INDUSFACE™

Monthly Zero-Day Vulnerability Coverage Report

June 2022

Total Zero-Day Vulnerabilities Found: 204

Command Injection	CSRF	Local File Inclusion	Cross-Site Scripting	SQL Injection
5	56	11	85	46

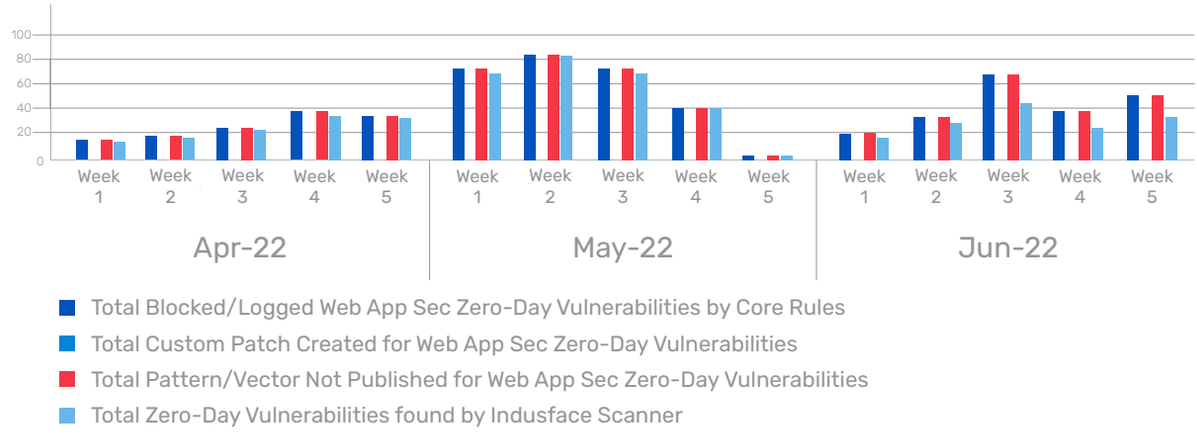
Zero-day vulnerabilities protected through core rules	203
Zero-day vulnerabilities protected through custom rules	0
Zero-day vulnerabilities for which protection can not be done	1
Zero-day vulnerabilities found by Indusface WAS	147

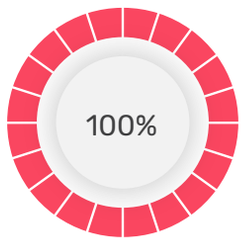
- To enable custom rules, please contact support@indusface.com
- Since the attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected.

Vulnerability Trend:

The weekly trend displays the total number of vulnerabilities discovered to the type of protection provided for the last quarter.

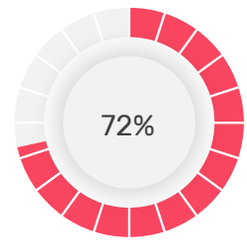
Weekly Vulnerability Trend of Last 3 Months





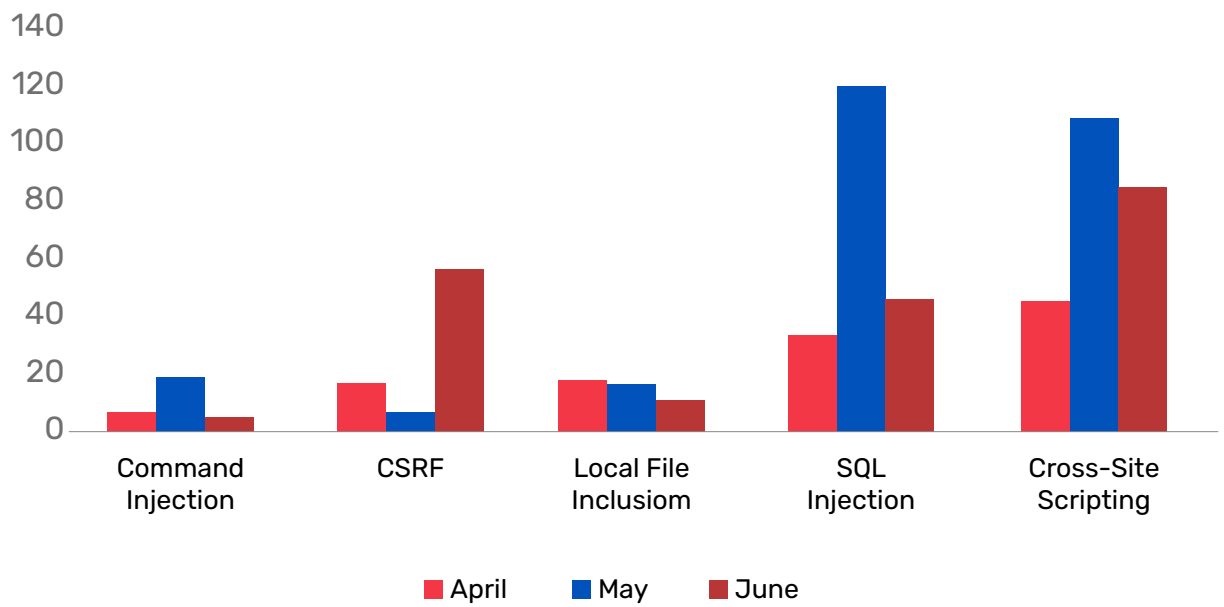
of the zero-day vulnerabilities were protected by the **core rules** in the last month.

of the zero-day vulnerabilities were protected by the **custom rules** in the last month.



of the zero-day vulnerabilities were reported by **Indusface Scanner** in the last month.

Top Five Vulnerability Categories



Command Injection Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2014	jgraph drawio up to 19.0.1 code injection	A vulnerability, which was classified as critical, was found in jgraph drawio up to 19.0.1. Affected is an unknown function. The manipulation leads to code injection. This vulnerability is traded as CVE-2022-2014. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2021-41738	ZeroShell 3.9.5 /cgi-bin/kerbynet IP os command injection	A vulnerability classified as critical has been found in ZeroShell 3.9.5. This affects an unknown part of the file /cgi-bin/kerbynet. The manipulation of the argument IP leads to os command injection. This vulnerability is uniquely identified as CVE-2021-41738. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-41421	MaianAffiliate up to 1.0 Admin Panel code injection	A vulnerability was found in MaianAffiliate up to 1.0. It has been declared as critical. This vulnerability affects unknown code of the component Admin Panel. The manipulation leads to code injection. This vulnerability was named CVE-2021-41421. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2022-31885	Marval MSM 14.19.0.12476 VBScript os command injection	A vulnerability was found in Marval MSM 14.19.0.12476. It has been classified as critical. This affects an unknown part of the component VBScript Handler. The manipulation leads to os command injection. This vulnerability is uniquely identified as CVE-2022-31885. Access to the local network is required for this attack to succeed. There is no exploit available.	Protected by core rules	Detected by scanner as command injection attack.
CVE-2022-2073	grav up to 1.7.33 code injection	A vulnerability which was classified as critical has been found in grav up to 1.7.33. Affected by this issue is some unknown functionality. The manipulation leads to code injection. This vulnerability is handled as CVE-2022-2073. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as command injection attack.

Local File Inclusion Vulnerabilities

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1743	Dominion Democracy Suite Voting System 5.5-A ImageCast X ../FILEDIR path traversal (icsa-22-154-01)	A vulnerability, which was classified as critical, has been found in Dominion Democracy Suite Voting System 5.5-A. Affected by this issue is some unknown functionality of the file ../FILEDIR of the component ImageCast X. The manipulation leads to path traversal. This vulnerability is handled as CVE-2022-1743. An attack has to be approached locally. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-32275	Grafana 8.4.3 Dashboard path-traversal	A vulnerability was found in Grafana 8.4.3. It has been declared as problematic. This vulnerability affects unknown code of the component Dashboard. The manipulation leads to relative path traversal. This vulnerability was named CVE-2022-32275. Access to the local network is required for this attack. There is no exploit available. The real existence of this vulnerability is still doubted at the moment.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-0779	User Meta Plugin upto 2.4.3 on-WordPress AJAX Action um_show_uploaded_file filepath path traversal	A vulnerability was found in User Meta Plugin up to 2.4.3. It has been classified as problematic. This affects the function um_show_uploaded_file of the component AJAX Action Handler. The manipulation of the argument filepath leads to path traversal. This vulnerability is uniquely identified as CVE-2022-0779. The attack needs to be approached within the local network. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
Null	convert-svg-core upto 0.6.3 SVG Tag pathname traversal (ID 86)	A vulnerability, which was classified as critical, was found in convert-svg-core up to 0.6.3. Affected is an unknown function of the component SVG Tag Handler. The manipulation leads to pathname traversal. This vulnerability is traded as CVE-2022-24278. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-1657	Jupiter Theme / JupiterX Theme on WordPress AJAX Action jupiterx_cp_load_pane_action path traversal	A vulnerability has been found in Jupiter Theme and JupiterX Theme and classified as critical. This vulnerability affects the function jupiterx_cp_load_pane_action of the component AJAX Action Handler. The manipulation leads to path traversal. This vulnerability was named CVE-2022-1657. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-26041	Generex RCCMD up to 4.26 pathname traversal	A vulnerability classified as problematic was found in Generex RCCMD up to 4.26. Affected by this vulnerability is an unknown functionality. The manipulation leads to pathname traversal. This vulnerability is known as CVE-2022-26041. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-29509	T&D Data Server/ Thermo Recorder Data Server pathname traversal	A vulnerability classified as critical has been found in T&D Data Server and Thermo Recorder Data Server. Affected is an unknown function. The manipulation leads to pathname traversal. This vulnerability is traded as CVE-2022-29509. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-25856	Argo Events up to 1.7.0 API GitArtifactReader. Read pathname-traversal (ID 1947)	A vulnerability has been found in Argo Events up to 1.7.0 and classified as critical. Affected by this vulnerability is the function GitArtifactReader. Read of the component API. The manipulation leads to pathname traversal. This vulnerability is known as CVE-2022-25856. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2013-1891	OpenCart up to1.5.5.1 filemanager.php path traversal	A vulnerability was found in OpenCart up to 1.5.5.1 and classified as critical. Affected by this issue is some unknown functionality of the file filemanager.php. The manipulation leads to path traversal. This vulnerability is handled as CVE-2013-1891. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-1953	ProductConfigurator for WooCommerce Plugin up to 1.2.31 on WordPress AJAX Action unlink path traversal	A vulnerability was found in Product Configurator for WooCommerce Plugin up to 1.2.31. It has been rated as critical. This issue affects the function unlink of the component AJAX Action Handler. The manipulation leads to path traversal. The identification of this vulnerability is CVE-2022-1953. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as local file inclusion attack.
CVE-2022-33116	GUnet Open eClass Platform up to 3.12.4 index.php jmpath pathname traversal	A vulnerability classified as problematic has been found in GUnet Open eClass Platform up to 3.12.4. This affects an unknown part of the file /modules/mindmap/index.php. The manipulation of the argument jmpath leads to pathname traversal. This vulnerability is uniquely identified as CVE-2022-33116. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as local file inclusion attack.

Cross-Site Request Forgery

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-33121	miniCMS 1.11 DAT File cross-site request forgery (ID 45)	A vulnerability has been found in miniCMS 1.11 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component DAT File Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-33121. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-31886	Marval MSM 14.19.0.12476 2FA crosssite request forgery	A vulnerability which was classified as problematic has been found in Marval MSM 14.19.0.12476. This issue affects some unknown processing of the component 2FA Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-31886. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-29647	MCMS 5.2.7 ms/basic/manager/save.do crosssiterequest forgery	A vulnerability was found in MCMS 5.2.7. It has been classified as problematic. Affected is an unknown function of the file ms/basic/manager/save.do. The manipulation leads to cross site request forgery. This vulnerability is traded as CVE-2022-29647. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-27174	Easy Blog up to 1.0.1 on EC-CUBE cross-site request forgery	A vulnerability, which was classified as problematic, was found in Easy Blog up to 1.0.1. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-27174. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-26173	JForum 2.8.0 jforum. page cross-site request forgery	A vulnerability was found in JForum 2.8.0. It has been declared as problematic. This vulnerability affects unknown code of the file jforum.page. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-26173. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1960	MyCSS Plugin up to 1.1 on WordPress Setting cross-site request forgery	A vulnerability was found in MyCSS Plugin up to 1.1. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-1960. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1918	ToolBar to Share Plugin up to 2.0 on WordPress plugin_toolbar_comparte-Page cross-site request forgery	A vulnerability, which was classified as problematic, has been found in ToolBar to Share Plugin up to 2.0. This issue affects some unknown processing of the component plugin_toolbar_comparte Page. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-1918. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1914	Clean-Contact Plugin up to 1.6 on WordPress-Setting cross-site request forgery	A vulnerability was found in Clean-Contact Plugin up to 1.6. It has been rated as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-1914. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1913	Add Post URL Plugin up to 2.1.0 on WordPress Setting cross-site request forgery	A vulnerability was found in Add Post URL Plugin up to 2.1.0. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-1913. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1900	Copify Plugin up to 1.3.0 on WordPress CopifySettings Page cross-site request forgery	A vulnerability classified as problematic was found in Copify Plugin up to 1.3.0. This vulnerability affects unknown code of the component CopifySettings Page. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-1900. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1895	underConstruction Plugin up to 1.19 on WordPress cross-site request forgery	A vulnerability, which was classified as problematic, was found in underConstruction Plugin up to 1.19. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-1895. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component	Protected by core rules	NA
CVE-2022-1885	Cimy Header Image Rotator Plugin up to 6.1.1 on WordPress Setting cross-site request forgery	A vulnerability has been found in Cimy Header Image Rotator Plugin up to 6.1.1 and classified as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-1885. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1846	Tiny Contact Form Plugin up to 0.7 on WordPress Setting crosssite request forgery	A vulnerability which was classified as problematic has been found in Tiny Contact Form Plugin up to 0.7. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-1846. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1845	WP Post Styling Plugin up to 1.3.0 on WordPress cross-site request forgery	A vulnerability classified as problematic was found in WP Post Styling Plugin up to 1.3.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-1845. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-1844	WP Sentry Plugin up to 1.0 on WordPress Setting cross-site request forgery	A vulnerability was found in WP Sentry Plugin up to 1.0. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-1844. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1843	MailPress Plugin up to 7.2.1 on WordPress Setting cross-site request forgery	A vulnerability classified as problematic has been found in MailPress Plugin up to 7.2.1. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-1843. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1842	OpenBook Book Data Plugin up to 3.5.2 on WordPress Setting crosssite request forgery	A vulnerability was found in OpenBook Book Data Plugin up to 3.5.2 and classified as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-1842. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1832	CaPa Protect Plugin up to 0.5.8.2 on WordPress Setting cross-site request forgery	A vulnerability classified as problematic was found in CaPa Protect Plugin up to 0.5.8.2. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-1832. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1831	WPlite Plugin up to 1.3.1 on WordPress Setting cross-site request forgery	A vulnerability classified as problematic has been found in WPlite Plugin up to 1.3.1. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-1831. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1830	Amazon Einzeltitellinks Plugin up to 1.3.3 on WordPress Setting crosssite request forgery	A vulnerability was found in Amazon Einzeltitellinks Plugin up to 1.3.3. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-1830. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1829	Inline Google Maps Plugin up to 5.11 on WordPress Setting crosssite request forgery	A vulnerability, which was classified as problematic, was found in Inline Google Maps Plugin up to 5.11. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-1829. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1828	PDF24 Articles to PDF Plugin up to 4.2.2 on WordPress cross-site request forgery	A vulnerability was found in PDF24 Articles to PDF Plugin up to 4.2.2. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-1828. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1827	PDF24 Article To PDF Plugin up to 4.2.2 on WordPress cross-site request forgery	A vulnerability was found in PDF24 Article To PDF Plugin up to 4.2.2. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-1827. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1826	Cross-Linker Plugin up to 3.0.1.9 on WordPress cross-site request forgery	A vulnerability was found in Cross-Linker Plugin up to 3.0.1.9. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-1826. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1793	Private Files Plugin up to 0.40 on WordPress crosssite request forgery	A vulnerability was found in Private Files Plugin up to 0.40. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-1793. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1792	Quick Subscribe Plugin up to 1.7.1 on WordPress Setting cross-site request forgery	A vulnerability, which was classified as problematic, was found in Quick Subscribe Plugin up to 1.7.1. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-1792. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1791	One Click Plugin Updater Plugin up to 2.4.14 on WordPress Setting cross-site request forgery	A vulnerability was found in One Click Plugin Updater Plugin up to 2.4.14. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-1791. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1790	New User Email Set Up Plugin up to 0.5.2 on WordPress Setting crosssite request forgery	A vulnerability was found in New User Email Set Up Plugin up to 0.5.2 and classified as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-1790. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1788	Change Uploaded File Permissions Plugin up to 4.0.0 on WordPress File Permission cross-site request forgery	A vulnerability has been found in Change Uploaded File Permissions Plugin up to 4.0.0 and classified as problematic. This vulnerability affects unknown code of the component File Permission Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-1788. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1779	Auto Delete Posts Plugin up to 1.3.0 on WordPress Setting cross-site request forgery	A vulnerability, which was classified as problematic, was found in Auto Delete Posts Plugin up to 1.3.0. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-1779. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1765	Hot Linked Image Cacher Plugin up to 1.16 on WordPress cross-site request forgery	A vulnerability classified as problematic was found in Hot Linked Image Cacher Plugin up to 1.16. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-1765. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1763	Static Page eXtended Plugin up to 2.1 on WordPress Setting crosssite request forgery	A vulnerability was found in Static Page eXtended Plugin up to 2.1. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-1763. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1761	Peters Collaboration Emails Plugin up to 2.2.0 on WordPress cross-site request forgery	A vulnerability classified as problematic has been found in Peters Collaboration E-mails Plugin up to 2.2.0. Affected is an unknown function. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-1761. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1759	RB Internal Links Plugin up to 2.0.16 on WordPress Setting crosssite request forgery	A vulnerability was found in RB Internal Links Plugin up to 2.0.16. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-1759. It is possible to initiate the attack remotely.There is no exploit available.	Protected by core rules	NA
CVE-2022-1758	Genki Pre-Publish Reminder Plugin up to 1.4.1 on WordPress cross-site request forgery	A vulnerability was found in Genki Pre-Publish Reminder Plugin up to 1.4.1 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-1758. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1749	WPMK Ajax Finder Plugin up to 1.0.1 on WordPress create-plug-inconfig.php createplugin_atf_admin_setting_page cross-site request forgery	A vulnerability, which was classified as problematic, was found in WPMK Ajax Finder Plugin up to 1.0.1. This affects the function createplugin_atf_admin_setting_page of the file ~/inc /config/create-plugin-config.php. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-1749. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1712	LiveSync for Plugin up to 1.0 on WordPress Setting cross-site request forgery	A vulnerability was found in LiveSync for Plugin up to 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-1712. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1695	WP Simple Adsense Insertion Plugin up to 2.0 on WordPress Admin Page cross-site request forgery	A vulnerability classified as problematic has been found in WP Simple Adsense Insertion Plugin up to 2.0. Affected is an unknown function of the component Admin Page. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-1695. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-1653	Supsystic Social Share Buttons Plugin up to 2.2.3 on WordPress Admin Page cross-site request forgery	A vulnerability was found in Supsystic Social Share Buttons Plugin up to 2.2.3. It has been declared as problematic. This vulnerability affects unknown code of the component Admin Page. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-1653. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-1630	WP-EMail Plugin up to 2.68.x on WordPress cross-site request forgery	A vulnerability has been found in WP-EMail Plugin up to 2.68.x and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-1630. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-1627	My Private Site Plugin up to 3.0.7 on WordPress Settings cross-site request forgery	A vulnerability was found in My Private Site Plugin up to 3.0.7. It has been classified as problematic. This affects an unknown part of the component Settings Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-1627. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1625	New User Approve Plugin up to 2.3 on WordPress Invitation Code cross-site request forgery	A vulnerability was found in New User Approve Plugin up to 2.3 and classified as problematic. Affected by this issue is some unknown functionality of the component Invitation Code Handler. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2022-1625. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-1610	Seamless Donations Plugin up to 5.1.8 on WordPress Setting crosssite request forgery	A vulnerability, which was classified as problematic, was found in Seamless Donations Plugin up to 5.1.8. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-1610. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-1605	Email Users Plugin up to 4.8.8 on WordPress Notification cross-site request forgery	A vulnerability, which was classified as problematic, has been found in Email Users Plugin up to 4.8.8. This issue affects some unknown processing of the component Notification Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-1605. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1603	Mail Subscribe List Plugin up to 2.1.3 on WordPress cross-site request forgery	A vulnerability, which was classified as problematic, has been found in Mail Subscribe List Plugin up to 2.1.3. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022-1603. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-1594	HC Custom WP-Admin URL Plugin up to 1.4 on WordPress Setting crosssite request forgery	A vulnerability classified as problematic has been found in HC Custom WP-Admin URL Plugin up to 1.4. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022-1594. It is possible to initiate the attack remotely.There is no exploit available.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1593	Site Offline or Coming Soon Plugin up to 1.6.6 on WordPress Setting cross-site request forgery	A vulnerability has been found in Site Offline or Coming Soon Plugin up to 1.6.6 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-1593. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1574	HTML2WP Plugin up to 1.0.0 on WordPress File Import cross-site request forgery	A vulnerability has been found in HTML2WP Plugin up to 1.0.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component File Import. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-1574. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1573	HTML2WP Plugin up to 1.0.0 on WordPress Setting cross-site request forgery	A vulnerability has been found in HTML2WP Plugin up to 1.0.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is known as CVE-2022-1573. The attack can be launched remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1572	HTML2WP Plugin up to 1.0.0 on WordPress AJAX Action cross-site request forgery	A vulnerability which was classified as problematic was found in HTML2WP Plugin up to 1.0.0. Affected is an unknown function of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-1572. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	NA
CVE-2022-1570	Files Download Delay Plugin up to 1.0.6 on WordPress Setting crosssite request forgery	A vulnerability, which was classified as problematic, was found in Files Download Delay Plugin up to 1.0.6. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability is uniquely identified as CVE-2022- 1570. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1424	Ask Me Theme up to 6.8.1 on WordPress AJAX Action cross-site request forgery	A vulnerability has been found in Ask Me Theme up to 6.8.1 and classified as problematic. This vulnerability affects unknown code of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-1424. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-1421	Discy Theme up to 5.1 on WordPress AJAX Action cross-site request forgery	A vulnerability, which was classified as problematic, was found in Discy Theme up to 5.1. Affected is an unknown function of the component AJAX Action Handler. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2022-1421. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-0875	Google Authenticator Plugin up to 1.0.4 on WordPress Setting crosssite request forgery	A vulnerability was found in Google Authenticator Plugin up to 1.0.4. It has been declared as problematic. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site request forgery. This vulnerability was named CVE-2022-0875. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2022-0444	Backup, Restore and Migrate WordPress Sites with the XCloner Plugin Setting cross-site request forgery	A vulnerability was found in Backup Restore and Migrate WordPress Sites with the XCloner Plugin up to 4.3.5 and classified as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site request forgery. The identification of this vulnerability is CVE-2022- 0444. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	NA
CVE-2021-44117	Daylight Studio Fuel CMS 1.5.0 4 cross-site request forgery	A vulnerability, which was classified as problematic, has been found in Daylight Studio Fuel CMS 1.5.0. Affected by this issue is some unknown functionality of the file /fuel/sitevariables/delete/4. The manipulation leads to cross-site request forgery. This vulnerability is handled as CVE-2021-44117. The attack may be launched remotely. There is no exploit available.	Protected by core rules	NA

SQL Injection

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-30833	Wedding Management System 1.0 client_edit.php user_id sql injection	A vulnerability was found in Wedding Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /Wedding-Management/admin/client_edit.php?booking=31. The manipulation of the argument user_id leads to sql injection. This vulnerability is traded as CVE-2022-30833. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2019-12350	ZZCMS 2019 Comma dl/dl_download.php id sql injection	A vulnerability classified as critical has been found in ZZCMS 2019. This affects an unknown part of the file dl/dl_download.php of the component Comma Handler. The manipulation of the argument id leads to sql injection. This vulnerability is uniquely identified as CVE-2019-12350. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-30817	Boo Simple Bus Ticket Booking System 1.0 index.php sql injection	A vulnerability classified as critical has been found in Boo Simple Bus Ticket Booking System 1.0. This affects an unknown part of the file /SimpleBusTicket/index.php. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-30817. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-30799	oretnom23 Online Ordering System 1.0 store/orderpage.php sql injection	A vulnerability was found in oretnom23 Online Ordering System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file store/orderpage.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-30799. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-30352	phpABook 0.9i index.php auth_user sql injection (ID 54518 / EDB-50071)	A vulnerability was found in phpABook 0.9i. It has been rated as critical. This issue affects some unknown processing of the file index.php. The manipulation of the argument auth_user leads to sql injection. The identification of this vulnerability is CVE-2022-30352. The attack may be initiated remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-44095	Project Worlds Hospital Management System in PHP 1.0 Login Page sql injection	A vulnerability classified as critical has been found in Project Worlds Hospital Management System in PHP 1.0. Affected is an unknown function of the component Login Page. The manipulation leads to sql injection. This vulnerability is traded as CVE-2021-44095. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-30496	IDCE MV 1.0 Logon Page user sql injection	A vulnerability has been found in IDCE MV 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the component Logon Page. The manipulation of the argument user leads to sql injection. This vulnerability is known as CVE-2022-30496. Access to the local network is required for this attack. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2021-37589	Virtua Cobranca prior 12R Login Page sql injection	A vulnerability has been found in Virtua Cobranca and classified as critical. Affected by this vulnerability is an unknown functionality of the component Login Page. The manipulation leads to sql injection. This vulnerability is known as CVE-2021-37589. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-30927	oretnom23 Simple Task Scheduling System up to 1.0 id sql injection	A vulnerability classified as critical was found in oretnom23 Simple Task Scheduling System up to 1.0. Affected by this vulnerability is an unknown functionality. The manipulation of the argument id leads to sql injection. This vulnerability is known as CVE-2022-30927. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-0788	WP Fundraising Donation and Crowdfunding Platform Plugin REST Route sql injection	A vulnerability classified as critical was found in WP Fundraising Donation and Crowdfunding Platform Plugin up to 1.4.2. Affected by this vulnerability is an unknown functionality of the component REST Route Handler. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-0788. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1689	Note Press Plugin up to 0.1.10 on WordPress Admin Dashboard Update sql injection	A vulnerability, which was classified as critical, has been found in Note Press Plugin up to 0.1.10. This issue affects some unknown processing of the component Admin Dashboard. The manipulation of the argument Update leads to sql injection. The identification of this vulnerability is CVE-2022-1689. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-1685	Five Minute Webshop Plugin up to 1.3.2 on WordPress Manage Products Admin Page orderby sql injection	A vulnerability was found in Five Minute Webshop Plugin up to 1.3.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Manage Products Admin Page. The manipulation of the argument orderby leads to sql injection. This vulnerability is known as CVE-2022-1685. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-1684	Cube Slider Plugin up to 1.2 on WordPress idslider sql injection	A vulnerability was found in Cube Slider Plugin up to 1.2. It has been classified as critical. Affected is an unknown function. The manipulation of the argument idslider leads to sql injection. This vulnerability is traded as CVE-2022-1684. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-1687	Logo Slider Plugin up to 1.4.8 on WordPress Manage Slider Images Admin Page lsp_slider_id sql injection	A vulnerability classified as critical has been found in Logo Slider Plugin up to 1.4.8. This affects an unknown part of the component Manage Slider Images Admin Page. The manipulation of the argument lsp_slider_id leads to sql injection. This vulnerability is uniquely identified as CVE-2022-1687. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-1688	Note Press Plugin up to 0.1.10 on WordPress Admin Dashboard id sql injection	A vulnerability classified as critical was found in Note Press Plugin up to 0.1.10. This vulnerability affects unknown code of the component Admin Dashboard. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-1688. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1683	amtyThumb Plugin up to 4.2.0 on WordPress Shortcode a sql injection	A vulnerability was found in amtyThumb Plugin up to 4.2.0 and classified as critical. This issue affects some unknown processing of the component Shortcode Handler. The manipulation of the argument a leads to sql injection. The identification of this vulnerability is CVE-2022-1683. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-1691	Realty Workstation Plugin up to 1.0.6 on WordPress Agent Edit trans_edit sql injection	A vulnerability has been found in Realty Workstation Plugin up to 1.0.6 and classified as critical. Affected by this vulnerability is an unknown functionality of the component Agent Edit Handler. The manipulation of the argument trans_edit leads to sql injection. This vulnerability is known as CVE-2022-1691. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-1692	CP Image Store with Slideshow Plugin up to 1.0.67 Query Parameter ordering_by sql injection	A vulnerability was found in CP Image Store with Slideshow Plugin up to 1.0.67 and classified as critical. Affected by this issue is some unknown functionality of the component Query Parameter Handler. The manipulation of the argument ordering_by leads to sql injection. This vulnerability is handled as CVE-2022-1692. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-31325	ChurchCRM 4.4.5 WhyCameEditor.php PersonID sql injection (ID 6005)	A vulnerability was found in ChurchCRM 4.4.5 and classified as critical. This issue affects some unknown processing of the file /churchcrm/WhyCameEditor.php. The manipulation of the argument PersonID leads to sql injection. The identification of this vulnerability is CVE-2022-31325. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2021-40961	CMS Made Simple up to 2.2.15 function.admin_articlestab.php sortby/query1 sql injection	A vulnerability classified as critical has been found in CMS Made Simple up to 2.2.15. This affects an unknown part of the file modules/News/function.admin_articlestab.php. The manipulation of the argument sortby/query1 leads to sql injection. This vulnerability is uniquely identified as CVE-2021-40961. The attack can only be done within the local network. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31788	IdeaLMS 2022 6 ClassID sql injection	A vulnerability was found in IdeaLMS 2022. It has been classified as critical. Affected is an unknown function of the file IdeaLMS/ChatRoom/ClassAccessControl/6? isBigBlueButton=0. The manipulation of the argument ClassID leads to sql injection. This vulnerability is traded as CVE-2022-31788. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-2067	RosarioSIS up to 8.x sql injection	A vulnerability was found in RosarioSIS up to 8.x. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-2067. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-1800	Export any WordPress data to XML-CSV Plugin up to 1.3.4 on WordPress POST Parameter cpt sql injection	A vulnerability was found in Export any WordPress data to XML-CSV Plugin up to 1.3.4. It has been rated as critical. Affected by this issue is some unknown functionality of the component POST Parameter Handler. The manipulation of the argument cpt leads to sql injection. This vulnerability is handled as CVE-2022-1800. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-1768	RSVPMaker Plugin up to 9.3.2 on WordPress ~/rsvpmakeremail.php sql injection	A vulnerability, which was classified as critical, has been found in RSVPMaker Plugin up to 9.3.2. Affected by this issue is some unknown functionality of the file ~/rsvpmaker-email.php. The manipulation leads to sql injection. This vulnerability is handled as CVE-2022-1768. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-0827	Bestbooks Plugin up to 2.6.3 on WordPress sql injection	A vulnerability classified as critical was found in Bestbooks Plugin up to 2.6.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to sql injection. This vulnerability is known as CVE-2022-0827. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-32336	Fast Food Ordering System 1.0 view_menu.php id sql injection	A vulnerability, which was classified as critical, has been found in Fast Food Ordering System 1.0. This issue affects some unknown processing of the file /ffos/admin/menus /view_menu.php. The manipulation of the argument id leads to sql injection. The identification of this vulnerability is CVE-2022-32336. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-32992	Online Tours and Travels Management System 1.0 tax.php tname sql injection	A vulnerability, which was classified as critical, has been found in Online Tours and Travels Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/operations/tax.php. The manipulation of the argument tname leads to sql injection. This vulnerability is handled as CVE-2022-32992. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-32301	YoudianCMS 9.5.0 ApiAction.class.php IdList sql injection	A vulnerability classified as critical has been found in YoudianCMS 9.5.0. This affects an unknown part in the library /App/Lib/Action/Home/ApiAction.class.php. The manipulation of the argument IdList leads to sql injection. This vulnerability is uniquely identified as CVE-2022-32301. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-32302	SourceCodester Theme Park Ticketing System 1.0 edit_ticket. php id sql injection	A vulnerability has been found in SourceCodester Theme Park Ticketing System 1.0 and classified as critical. This vulnerability affects unknown code of the file edit_ticket.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-32302. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-32101	kkcms 1.3.7 vlist.php cid sql injection	A vulnerability was found in kkcms 1.3.7. It has been classified as critical. Affected is an unknown function of the file /template/wapian/vlist.php. The manipulation of the argument cid leads to sql injection. This vulnerability is traded as CVE-2022-32101. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-32991	Web Based Quiz System 1.0 welcome.php eid sql injection	A vulnerability was found in Web Based Quiz System 1.0 and classified as critical. This issue affects some unknown processing of the file welcome.php. The manipulation of the argument eid leads to sql injection. The identification of this vulnerability is CVE-2022-32991. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-32370	itsourcecode School Management System 1.0 get_classroom.php id sql injection	A vulnerability was found in itsourcecode School Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /school/model/get_classroom.php. The manipulation of the argument id leads to sql injection. This vulnerability was named CVE-2022-32370. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31912	Online Tutor Portal Site 1.0 Master.php sql injection	A vulnerability, which was classified as critical, was found in Online Tutor Portal Site 1.0. This affects an unknown part of the file /otps/classes/Master.php?f=delete_team. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-31912. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-31908	Student Registration and Fee Payment System 1.0 /scms/student.php sql injection	A vulnerability was found in Student Registration and Fee Payment System 1.0 and classified as critical. This issue affects some unknown processing of the file /scms/student.php. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2022-31908. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2021-41654	Wuzhicms 4.1.0 index.php keyValue sql injection (ID 198)	A vulnerability was found in Wuzhicms 4.1.0 and classified as critical. Affected by this issue is some unknown functionality of the file/coreframe/app/pay/admin/index.php. The manipulation of the argument keyValue leads to sql injection. This vulnerability is handled as CVE-2021-41654. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-31384	Directory Management System 1.0 add-directory.php fullname sql injection	A vulnerability, which was classified as critical, has been found in Directory Management System 1.0. Affected by this issue is some unknown functionality of the file adddirectory.php. The manipulation of the argument fullname leads to sql injection. This vulnerability is handled as CVE-2022-31384. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-31911	Online Discussion Forum Site 1.0 Master.php sql injection	A vulnerability was found in Online Discussion Forum Site 1.0. It has been classified as critical. This affects an unknown part of the file /odfs/classes/Master.php?f=delete_team. The manipulation leads to sql injection. This vulnerability is uniquely identified as CVE-2022-31911. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2020-35597	Victor CMS 1.0 admin_edit_comment.php c_id sql injection (ID 16 / EDB-49282)	A vulnerability was found in Victor CMS 1.0. It has been classified as critical. This affects an unknown part of the file admin_edit_comment.php. The manipulation of the argument c_id leads to sql injection. This vulnerability is uniquely identified as CVE-2020-35597. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2021-41408	VoIPmonitor up to 24.61 Web GUI api.php user sql injection	A vulnerability was found in VoIPmonitor up to 24.61. It has been classified as critical. This affects an unknown part of the file api.php of the component Web GUI. The manipulation of the argument user leads to sql injection. This vulnerability is uniquely identified as CVE-2021-41408. It is possible to initiate the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-1905	Events Made Easy Plugin up to 2.2.80 on WordPress sql injection	A vulnerability was found in Events Made Easy Plugin up to 2.2.80. It has been classified as critical. Affected is an unknown function. The manipulation leads to sql injection. This vulnerability is traded as CVE-2022-1905. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-1472	Better Find and Replace Plugin up to 1.3.5 on WordPress sql injection	A vulnerability has been found in Better Find and Replace Plugin up to 1.3.5 and classified as critical. This vulnerability affects unknown code. The manipulation leads to sql injection. This vulnerability was named CVE-2022-1472. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-33055	oretnom23 Online Railway Reservation System 1.0 manage_train.php id sql injection	A vulnerability was found in oretnom23 Online Railway Reservation System 1.0. It has been classified as critical. Affected is an unknown function of the file /orrs/admin/trains/manage_train.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-33055. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-40956	LaikeTui up to 3.5.0 Menu Management sql injection (ID 13)	A vulnerability, which was classified as critical, has been found in LaikeTui up to 3.5.0. This issue affects some unknown processing of the component Menu Management. The manipulation leads to sql injection. The identification of this vulnerability is CVE-2021-40956. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-33114	Jfinal CMS 5.1.0 list attrVal sql injection (ID 38)	A vulnerability was found in Jfinal CMS 5.1.0. It has been classified as critical. Affected is an unknown function of the file /jfinal_cms/system/dict/list. The manipulation of the argument attrVal leads to sql injection. This vulnerability is traded as CVE-2022-33114. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2021-40955	LaikeTui 3.5.0 Background Administrator List sql injection (ID 12)	A vulnerability classified as critical was found in LaikeTui 3.5.0. This vulnerability affects unknown code of the component Background Administrator List. The manipulation leads to sql injection. This vulnerability was named CVE-2021-40955. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as SQL injection attack
CVE-2022-34132	Benjamin Balet Jorani 1.0 Leaves.php id sql injection (ID 369)	A vulnerability was found in Benjamin Balet Jorani 1.0. It has been classified as critical. Affected is an unknown function of the file application/controllers /Leaves.php. The manipulation of the argument id leads to sql injection. This vulnerability is traded as CVE-2022-34132. It is possible to launch the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as SQL injection attack

Cross-Site Scripting Vulnerability

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29628	Online Market Place Site 1.0 payload / omps/seller Page cross-site scripting	A vulnerability, which was classified as problematic, has been found in Online Market Place Site 1.0. This issue affects some unknown processing of the file / omps/seller of the component payload Handler. The manipulation of the argument Page leads to crosssite scripting. The identification of this vulnerability is CVE-2022-29628. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1991	Fast Food Ordering System 1.0 Master List Master.php Description cross-site scripting	A vulnerability classified as problematic has been found in Fast Food Ordering System 1.0. Affected is an unknown function of the file Master.php of the component Master List. The manipulation of the argument Description with the input foo "><img src=" " onerror="alert (document.cookie)"> leads to cross-site scripting. This vulnerability is traded as CVE-2022-1991. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1988	neorazorx facturascripts prior 2022.09 cross-site scripting	A vulnerability has been found in neorazorx facturascripts and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1988. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-30349	SiteServer SSCMS 6.15.51 cross-site scripting (ID 3238)	A vulnerability was found in SiteServer SSCMS 6.15.51. It has been classified as problematic. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-30349. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-38221	bbs-go up to 3.3.0 cross-site scripting (ID 112)	A vulnerability, which was classified as problematic, was found in bbs-go up to 3.3.0. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2021-38221. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to apply a patch to fix this issue.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29648	Jfinal CMS 5.1.0 HTTP Header X-Forwarded-For cross-site scripting (ID 34)	A vulnerability was found in Jfinal CMS 5.1.0 and classified as problematic. Affected by this issue is some unknown functionality of the component HTTP Header Handler. The manipulation of the argument X-Forwarded-For leads to cross-site scripting. This vulnerability is handled as CVE-2022-29648. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-29598	Solutions Atlantic Regulatory Reporting System v500 ShowDocument.aspx cross-site scripting	A vulnerability classified as problematic was found in Solutions Atlantic Regulatory Reporting System v500. This vulnerability affects unknown code of the file RRSWeb/maint/ShowDocument/ShowDocument. aspx. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-29598. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-30429	Neos CMS 3.3.29/8.0.1 crosssite scripting	A vulnerability was found in Neos CMS 3.3.29/8.0.1. It has been declared as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-30429. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-29770	XXL-Job 2.3.0 / xxl-job-admin/ jobinfo cross-site scripting (ID 2836)	A vulnerability has been found in XXL-Job 2.3.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file / xxl-jobadmin/ jobinfo. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-29770. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1647	FormCraft Plugin up to 1.2.5 on WordPress Field Label cross-site scripting	A vulnerability was found in FormCraft Plugin up to 1.2.5 and classified as problematic. This issue affects some unknown processing of the component Field Label Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1647. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1241	Ask Me Theme up to 6.8.1 on Word-Press Edit Profile Page cross-site scripting	A vulnerability, which was classified as problematic, was found in Ask Me Theme up to 6.8.1. This affects an unknown part of the component Edit Profile Page. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1241. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1469	FiboSearch Plugin up to 1.16.x on WordPress Setting cross-site scripting	A vulnerability was found in FiboSearch Plugin up to 1.16. x. It has been rated as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1469. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1005	WP Statistics Plugin up to 13.2.1 on WordPress REQUEST_URI cross-site script-ing	A vulnerability was found in WP Statistics Plugin up to 13.2.1. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument REQUEST_URI leads to crosssite scripting. This vulnerability is handled as CVE-2022-1005. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1569	Pie Forms prior 1.4.9.4 on WordPress Field cross-site scripting	A vulnerability, which was classified as problematic, has been found in Pie Forms Forms. Affected by this issue is some unknown functionality of the component Field Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1569. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-2015	jgraph drawio up to 19.0.1 crosssite scripting	A vulnerability, which was classified as problematic, has been found in jgraph drawio up to 19.0.1. Affected by this issue is some unknown functionality. The manipulation leads to crosssite scripting. This vulnerability is handled as CVE-2022-2015. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-29455	Elementor Website Builder Plugin up to 3.5.5 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in Elementor Website Builder Plugin up to 3.5.5. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-29455. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-2066	neorazorx facturascripts prior 2022.06 cross-site scripting	A vulnerability was found in neorazorx facturascripts and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2066. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1773	WP Athletics Plugin up to 1.1.7 on WordPress Admin Page cross-site scripting	A vulnerability, which was classified as problematic, has been found in WP Athletics Plugin up to 1.1.7. Affected by this issue is some unknown functionality of the component Admin Page. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1773. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1814	WP Admin Style Plugin up to 0.1.2 on WordPress cross-site scripting	A vulnerability was found in WP Admin Style Plugin up to 0.1.2. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1814. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-2065	neorazorx facturascripts prior 2022.06 cross-site scripting	A vulnerability has been found in neorazorx facturascripts and classified as problematic. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-2065. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-0209	Mitsol Social Post Feed Plugin up to 1.10 on WordPress crosssite scripting	A vulnerability was found in Mitsol Social Post Feed Plugin up to 1.10. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-0209. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1532	Themify Plugin up to 1.3.7 on WordPress Admin Page page cross-site scripting	A vulnerability was found in Themify Plugin up to 1.3.7. It has been rated as problematic. This issue affects some unknown processing of the component Admin Page. The manipulation of the argument page leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1532. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1961	Google Tag Manager Plugin up to 1.15.1 on WordPress ~/public/frontend.php gtm4wp-options [scroller-contentid] cross-site scripting	A vulnerability classified as problematic was found in Google Tag Manager Plugin up to 1.15.1. Affected by this vulnerability is an unknown functionality of the file ~/public/frontend.php. The manipulation of the argument gtm4wp-options [scroller-contentid] leads to crosssite scripting. This vulnerability is known as CVE-2022-1961. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1604	MailerLite Plugin up to 1.5.3 on WordPress cross-site scripting	A vulnerability classified as problematic was found in MailerLite Plugin up to 1.5.3. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-1604. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-41663	MiniCMS 1.11 Article post-edit.php cross-site scripting (ID 41)	A vulnerability has been found in MiniCMS 1.11 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file post-edit.php of the component Article Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2021-41663. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-40678	Piwigo 11.5.0 admin.php crosssite scripting (ID 1476)	A vulnerability classified as problematic was found in Piwigo 11.5.0. This vulnerability affects unknown code of the file /admin.php?page=batch_manager&mode=unit. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2021-40678. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-27859	Nicdark Travel Management Plugin up to 2.0 on WordPress cross-site scripting	A vulnerability classified as problematic has been found in Nicdark Travel Management Plugin up to 2.0. This affects an unknown part. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-27859. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-31914	Zoo Management System 1.0 save_animal cross-site scripting	A vulnerability, which was classified as problematic, was found in Zoo Management System 1.0. Affected is an unknown function of the file zms /admin/public_html/save_animal? an_id=24. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-31914. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-24127	REDCap 12.0.11 Project edit_project_settings.php app_title cross-site scripting	A vulnerability has been found in REDCap 12.0.11 and classified as problematic. This vulnerability affects unknown code of the file ProjectGeneral/edit_project_settings.php of the component Project Handler. The manipulation of the argument app_title leads to cross-site scripting. This vulnerability was named CVE-2022-24127. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-24004	REDCap 12.0.11 messenger_ajax.php new_title cross-site scripting	A vulnerability, which was classified as problematic, was found in REDCap 12.0.11. This affects an unknown part of the file Messenger/messenger_ajax.php. The manipulation of the argument new_title leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-24004. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-41420	MaianAffiliate up to 1.0 Admin Panel cross-site scripting	A vulnerability was found in MaianAffiliate up to 1.0 and classified as problematic. This issue affects some unknown processing of the component Admin Panel. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2021-41420. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31910	Online Tutor Portal Site 1.0 /otps /classes/Master.php cross-site scripting	A vulnerability was found in Online Tutor Portal Site 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /otps /classes/Master.php. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-31910. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-31913	Online Discussion Forum Site 1.0 Master.php name cross-site scripting	A vulnerability has been found in Online Discussion Forum Site 1.0 and classified as problematic. This vulnerability affects unknown code of the file /odfs/classes/Master.php? f=save_category. The manipulation of the argument name leads to cross-site scripting. This vulnerability was named CVE-2022-31913. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-36609	webTareas 2.2p1 editfolder.php Name cross-site scripting (ID 43)	A vulnerability was found in webTareas 2.2p1. It has been rated as problematic. This issue affects some unknown processing of the file /linkedcontent/editfolder.php. The manipulation of the argument Name leads to crosssite scripting. The identification of this vulnerability is CVE-2021-36609. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-33295	Joplin Desktop App up to 1.8.4 cross-site scripting	A vulnerability was found in Joplin Desktop App up to 1.8.4 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2021-33295. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-36827	Saturday Drive Ninja Forms Contact Form Plugin up to 3.6.9 on WordPress label cross-site scripting	A vulnerability was found in Saturday Drive Ninja Forms Contact Form Plugin up to 3.6.9. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument label leads to cross-site scripting. This vulnerability is handled as CVE-2021-36827. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-32442	u5cms 8.3.5/127.0.0.1 Default Home Page cross-site scripting (ID 49)	A vulnerability classified as problematic has been found in u5cms 8.3.5/127.0.0.1. Affected is an unknown function of the component Default Home Page. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-32442. It is possible to launch the attack remotely. Furthermore, there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-31875	Trendnet IP-110wn 1.2.2.68/admin/schepro-file.cgi proname-cross-site scripting	A vulnerability was found in Trendnet IP-110wn 1.2.2.68. It has been rated as problematic. This issue affects some unknown processing of the file /admin / scheprofile.cgi. The manipulation of the argument proname leads to cross-site scripting. The identification of this vulner-ability is CVE-2022-31875. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-31873	Trendnet IP-110wn 1.2.2.68/admin/general.cgi prefix cross-site scripting	A vulnerability was found in Trendnet IP-110wn 1.2.2.68. It has been declared as problem-atic. This vulnerability affects unknown code of the file /admin/general.cgi. The manipulation of the argument prefix leads to cross-site scripting. This vulnerability was named CVE-2022-31873. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1266	Post Grid, Slider & Carousel Ulti-mate Plugin up to 1.4.x on Word-Press Header Title crosssite scripting	A vulnerability classified as problematic was found in Post Grid, Slider & Carousel Ultimate Plugin up to 1.4.x. This vulnera-bility affects unknown code. The manipulation of the argument Header Title leads to cross-site scripting. This vulnerability was named CVE-2022-1266. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1717	Custom Share Buttons with Floating Sidebar Plugin up to 4.1 on WordPress cross-site script-ing	A vulnerability was found in Custom Share Buttons with Floating Sidebar Plugin up to 4.1 and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1717. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-25104	Ocean Extra Plugin up to 1.9.4 on Word-Press cross-site scripting	A vulnerability was found in Ocean Extra Plugin up to 1.9.4. It has been rated as problematic. Affected by this issue is some unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2021-25104. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-0663	PrintFriendly Print, PDF, Email Plugin up to 5.2.2 on WordPress Custom Button Text Setting cross-site scripting	A vulnerability classified as problematic has been found in PrintFriendly Print, PDF, Email Plugin up to 5.2.2. This affects an unknown part of the component Custom Button Text Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-0663. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1945	Colorlib Coming Soon & Maintenance Mode Plugin up to 1.0.98 on WordPress Setting cross-site scripting	A vulnerability was found in Colorlib Coming Soon & Maintenance Mode Plugin up to 1.0.98. It has been classified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1945. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-25088	XML Sitemaps Plugin up to 4.1.2 on WordPress Debug Page cross-site scripting	A vulnerability was found in XML Sitemaps Plugin up to 4.1.2. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Debug Page. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2021-25088. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1889	Newsletter Plugin up to 7.4.5 on WordPress preheader_text cross-site scripting	A vulnerability, which was classified as problematic, has been found in Newsletter Plugin up to 7.4.5. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation of the argument preheader_text leads to crosssite scripting. This vulnerability is handled as CVE-2022-1889. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-2130	microweber up to 1.2.16 crosssite scripting	A vulnerability, which was classified as problematic, was found in microweber up to 1.2.16. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2130. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1915	WP Zillow Review Slider Plugin up to 2.3 on WordPress Setting cross-site scripting	A vulnerability was found in WP Zillow Review Slider Plugin up to 2.3 and classified as problematic. This issue affects some unknown processing of the component Setting Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1915. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1896	underConstruction Plugin up to 1.20 on WordPress Display a custom page using your own HTML cross-site scripting	A vulnerability has been found in underConstruction Plugin up to 1.20 and classified as problematic. This vulnerability affects unknown code of the component Display a custom page using your own HTML. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-1896. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-25585	Unioncms 1.0.13 Default Setting cross-site scripting	A vulnerability classified as problematic was found in Unioncms 1.0.13. Affected by this vulnerability is an unknown functionality of the component Default Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-25585. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-23056	Frappe ERPNext 13.30.0 Patient History Page cross-site	A vulnerability, which was classified as problematic, was found in Frappe ERPNext 13.30.0. This affects an unknown part of the component Patient History Page. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-23056. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-31786	IdeaLMS 2022 PATH_INFO cross-site scripting	A vulnerability was found in IdeaLMS 2022. It has been rated as problematic. This issue affects some unknown processing of the file IdeaLMS /Class/Assessment/. The manipulation of the argument PATH_INFO leads to cross-site scripting. The identification of this vulnerability is CVE-2022-31786. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-34328	jenaye PMB 7.3.10 index.php id cross-site scripting	A vulnerability was found in jenaye PMB 7.3.10 and classified as problematic. Affected by this issue is some unknown functionality of the file index.php. The manipulation of the argument id leads to crosssite scripting. This vulnerability is handled as CVE-2022-34328. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2021-29055	SourceCodester School File Management System 1.0 Update Account Form student_profile.php Firtstname cross-site scripting (ID 161394)	A vulnerability, which was classified as problematic, has been found in SourceCodester School File Management System 1.0. This issue affects some unknown processing of the file student_profile.php of the component Update Account Form. The manipulation of the argument Firtstname leads to cross-site scripting. The identification of this vulnerability is CVE-2021-29055. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-32987	Simple Bakery Shop Management 1.0 Username/Full Name cross-site scripting	A vulnerability was found in Simple Bakery Shop Management 1.0 and classified as problematic. This issue affects some unknown processing of the file /bsms/?page=manage_account. The manipulation of the argument Username/Full Name leads to cross-site scripting. The identification of this vulnerability is CVE-2022-32987. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-33910	MantisBT up to 2.25.4 SVG Document file_download.php cross-site scripting	A vulnerability has been found in MantisBT up to 2.25.4 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file file_download.php of the component SVG Document Handler. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-33910. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-32209	CRuby/JRuby SanitizerThere cross-site scripting	A vulnerability classified as problematic was found in CRuby and JRuby. This vulnerability affects the function Rails::Html::SanitizerThere. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-32209. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2021-39408	Online Student Rate System 1.0 index.php page cross-site scripting	A vulnerability was found in Online Student Rate System 1.0. It has been classified as problematic. Affected is an unknown function of the file index.php. The manipulation of the argument page leads to cross-site scripting. This vulnerability is traded as CVE-2021-39408. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-2040	Brizy Plugin up to 2.4.1 on WordPress URL cross-site scripting	A vulnerability which was classified as problematic has been found in Brizy Plugin up to 2.4.1. This issue affects some unknown processing of the component URL Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-2040. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-2218	ionicabizau parse-url up to 6.x cross-site scripting	A vulnerability which was classified as problematic was found in ionicabizau parse-url up to 6.x. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2218. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1995	Malware Scanner Plugin up to 4.5.1 on WordPress Setting cross-site scripting	A vulnerability classified as problematic was found in Malware Scanner Plugin up to 4.5.1. This vulnerability affects unknown code of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-1995. The attack can be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1990	Nested Pages Plugin up to 3.1.20 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in Nested Pages Plugin up to 3.1.20. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1990. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-2217	ionicabizau parse-url up to 7.0.0 cross-site scripting	A vulnerability was found in ionicabizau parse-url up to 7.0.0. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2217. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-2213	SourceCodester Library Management System 1.0 edit_admin_details.php Name cross-site scripting	A vulnerability was found in SourceCodester Library Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/edit_admin_details.phpidadmin. The manipulation of the argument Name leads to cross-site scripting. This vulnerability is known as CVE-2022-2213. The attack can be launched remotely. Furthermore there is an exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1964	Easy SVG Support Plugin up to 3.2.x on WordPress cross-site scripting	A vulnerability was found in Easy SVG Support Plugin up to 3.2.x. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1964. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1904	Pricing Tables Plugin up to 3.2.0 on WordPress cross-site scripting	A vulnerability was found in Pricing Tables Plugin up to 3.2.0 and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1904. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1971	NextCellent Gallery Plugin up to 1.9.35 on WordPress Image Setting cross-site scripting	A vulnerability was found in NextCellent Gallery Plugin up to 1.9.35. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Image Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1971. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1776	Popups, Welcome Bar, Optins and Lead Generation Plugin Campaign cross-site scripting	A vulnerability was found in Popups Welcome Bar Optins and Lead Generation Plugin up to 2.1.7. It has been rated as problematic. This issue affects some unknown processing of the component Campaign Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1776. The attack may be initiated remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-2041	Brizy Plugin up to 2.4.1 on WordPress cross-site scripting	A vulnerability which was classified as problematic was found in Brizy Plugin up to 2.4.1. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-2041. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1095	Mihdan No External Links Plugin up to 4.8.0 on WordPress Setting cross-site scripting	A vulnerability was found in Mihdan No External Links Plugin up to 4.8.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1095. The attack may be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1994	Login With OTP Over SMS, Email, WhatsApp and Google Authenticator Plugin Setting cross-site scripting	A vulnerability was found in Login With OTP Over SMS Email WhatsApp and Google Authenticator Plugin up to 1.0.7. It has been classified as problematic. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1994. It is possible to initiate the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1113	Florist One Flower Delivery Plugin up to 3.5.10 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in Florist One Flower Delivery Plugin up to 3.5.10. This affects an unknown part of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is uniquely identified as CVE-2022-1113. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1326	Contact Form Plugin up to 1.2.0 on WordPress Custom Text Field cross-site scripting	A vulnerability classified as problematic was found in Contact Form Plugin up to 1.2.0. This vulnerability affects unknown code of the component Custom Text Field Handler. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-1326. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1028	Security Firewall, Malware Scanner, Secure Login and Backup Plugin cross-site scripting	A vulnerability was found in Security Firewall Malware Scanner Secure Login and Backup Plugin up to 4.2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1028. The attack can be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1327	Grid Gallery Plugin up to 1.1.1 on WordPress Image Field cross-site scripting	A vulnerability which was classified as problematic has been found in Grid Gallery Plugin up to 1.1.1. This issue affects some unknown processing of the component Image Field Handler. The manipulation leads to cross-site scripting. The identification of this vulnerability is CVE-2022-1327. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1029	Limit Login Attempts Plugin up to 4.0.71 on WordPress Setting cross-site scripting	A vulnerability classified as problematic has been found in Limit Login Attempts Plugin up to 4.0.71. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1029. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2020-21161	Ruckus Wireless ZoneDirector 9.8.3.0 cross-site scripting	A vulnerability classified as problematic has been found in Ruckus Wireless ZoneDirector 9.8.3.0. Affected is an unknown function. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2020-21161. It is possible to launch the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-1470	Ultimate Woo-Commerce CSV Importer Plugin up to 2.0 on WordPress cross-site scripting	A vulnerability classified as problematic was found in Ultimate WooCommerce CSV Importer Plugin up to 2.0. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross-site scripting. This vulnerability is known as CVE-2022-1470. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1916	Active Prod-ucts Tables for WooCommerce up to 1.0.4 on WordPress AJAX Action crosssite scripting	A vulnerability which was classified as problematic has been found in Active Products Tables for WooCommerce up to 1.0.4. Affected by this issue is some unknown functionality of the component AJAX Action Handler. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1916. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1321	miniOrange Google Authenti-cator Plugin up to 5.5.5 on Word-Press cross-site scripting	A vulnerability was found in miniOrange Google Authenticator Plugin up to 5.5.5 and classified as problematic. Affected by this issue is some unknown function-ality. The manipulation leads to cross-site scripting. This vulnerability is handled as CVE-2022-1321. The attack may be launched remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-1010	Login using WordPress Users Plugin up to 1.13.3 on WordPress Set-ting cross-site scripting	A vulnerability was found in Login using WordPress Users Plugin up to 1.13.3. It has been clas-sified as problematic. Affected is an unknown function of the component Setting Handler. The manipulation leads to cross-site scripting. This vulnerability is traded as CVE-2022-1010. It is possible to launch the attack remotely. There is no exploit available. It is recommended to upgrade the affected component.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-33009	LightCMS 1.3.11 PDF File crosssite scripting (ID 30)	A vulnerability which was classi-fied as problematic was found in LightCMS 1.3.11. This affects an unknown part of the component PDF File Handler. The manipula-tion leads to crosssite scripting. This vulnerability is uniquely identified as CVE-2022-33009. It is possible to initiate the attack remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack

Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage	Indusface WAS Coverage
CVE-2022-23896	Admidio 4.1.2 cross-site scripting	A vulnerability classified as problematic was found in Admidio 4.1.2. This vulnerability affects unknown code. The manipulation leads to cross-site scripting. This vulnerability was named CVE-2022-23896. The attack can be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2020-19897	wuzhicms 4.1.0 imgurl cross-site scripting (ID 183)	A vulnerability was found in wuzhicms 4.1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument imgurl leads to cross-site scripting. This vulnerability is known as CVE-2020-19897. The attack can be launched remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack
CVE-2022-31897	SourceCodester Zoo Management System 1.0 register_visitor msg cross-site scripting (ID 167572)	A vulnerability was found in SourceCodester Zoo Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file public_html /register_visitor. The manipulation of the argument msg leads to cross-site scripting. The identification of this vulnerability is CVE-2022-31897. The attack may be initiated remotely. There is no exploit available.	Protected by core rules	Detected by scanner as cross-site scripting attack

Indusface is a leading application security SaaS company that secures critical Web, Mobile & API applications of 3000+ global customers using its award-winning fully managed platform that integrates a web application scanner, web application firewall, DDoS &, BOT Mitigation, CDN, and threat intelligence engine. The company has been funded by Tata Capital Growth Fund, is Great Place to Work certified, mentioned by analysts like Gartner, Forrester, etc in their reports, and has been the recipient of many awards such as the Economic Times Top 25, NASSCOM DSCI Top Security Company, Deloitte Asia Top 100 , and several other such prestigious recognitions.

CONTACT US - +91 265 6133021 | +1 866 537 8234
EMAIL - sales@indusface.com

Indusface is the Only Vendor To Be Named Gartner® Peer Insights™ Customers' Choice in All the 7 Segments of Voice of Customer WAAP 2022 Report.