

WPScan Vulnerability Report

Target Website: <https://hackerdom.xyz/>

Scan Tool: WPScan 3.8.28

Scan Date: April 20, 2025

Vulnerability Summary and Fixes

1. Outdated WordPress Core

Vulnerability:

Detected WordPress version: **6.7.2** (Outdated)

Detected via RSS feed and CSS version leaks.

```
90 ],
91 "version": {
92   "number": "6.7.2",
93   "release_date": "2025-02-11",
94   "status": "outdated",
95   "found_by": "Most Common Wp Includes Query Parameter In Homepage (Passive Detection)",
96   "confidence": 100,
97   "interesting_entries": [
98     "https://hackerdom.xyz/wp-includes/css/dist/block-library/style.min.css?ver=6.7.2"
99   ],
```

Fix:

Update WordPress to the latest stable version using the admin dashboard or CLI.

2. Publicly Accessible Sensitive Files

Vulnerability:

- `/readme.html` is accessible: discloses WP version.
- `/robots.txt` lists sensitive directories:
 - `/wp-admin/`
 - `/wp-content/uploads/wc-logs/`
 - `/wp-content/uploads/woocommerce_uploads/`

```

35 {
36   "url": "https://hackerdom.xyz/robots.txt",
37   "to_s": "robots.txt found: https://hackerdom.xyz/robots.txt",
38   "type": "robots_txt",
39   "found_by": "Robots Txt (Aggressive Detection)",
40   "confidence": 100,
41   "confirmed_by": {
42   },
43 },
44 "references": {
45 },
46 },
47 "interesting_entries": [
48   "/wp-content/uploads/wc-logs/",
49   "/wp-content/uploads/woocommerce_transient_files/",
50   "/wp-content/uploads/woocommerce_uploads/",
51   "/wp-admin/",
52   "/wp-admin/admin-ajax.php"
53 ]
54 },
55 {
56   "url": "https://hackerdom.xyz/readme.html",
57   "to_s": "WordPress readme found: https://hackerdom.xyz/readme.html",
58   "type": "readme",
59   "found_by": "Direct Access (Aggressive Detection)",
60   "confidence": 100,
61   "confirmed_by": {

```

Fix:

- Delete `readme.html` from root directory.
- Restrict access or clean up sensitive entries in `robots.txt`.

3. External WP-Cron Access

Vulnerability:

<https://hackerdom.xyz/wp-cron.php> is publicly accessible.

Can be abused for **DDoS** or high resource usage.

```

71 {
72   "url": "https://hackerdom.xyz/wp-cron.php",
73   "to_s": "The external WP-Cron seems to be enabled: https://hackerdom.xyz/wp-cron.php",
74   "type": "wp_cron",
75   "found_by": "Direct Access (Aggressive Detection)",
76   "confidence": 60,
77   "confirmed_by": {
78   },
79 },
80 "references": {
81   "url": [
82     "https://www.iplocation.net/defend-wordpress-from-ddos",
83     "https://github.com/wpscanteam/wpscan/issues/1299"
84   ]
85 },
86 "interesting_entries": [

```

Fix:

1. Disable external WP-Cron:

In `wp-config.php`

```
define('DISABLE_WP_CRON', true);
```

2. Use server-side cron job:

```
* /5 * * * * wget -q -O - https://hackerdom.xyz/wp-cron.php?doing_wp_cron >/dev/null 2>&1
```

4. WordPress User Enumeration

Vulnerability:

Username user discovered via RSS feed and passive detection.

```
170 "users": {
171   "user": {
172     "id": null,
173     "found_by": "Rss Generator (Aggressive Detection)",
174     "confidence": 50,
175     "interesting_entries": [
176     ],
177     "confirmed_by": {
178     }
179   }
180 }
```

Fix:

- Install plugin: **Stop User Enumeration**
- Restrict /wp-json/wp/v2/users and /?author=1 access via .htaccess:

```
<IfModule mod_rewrite.c>
RewriteCond %{QUERY_STRING} author=
RewriteRule ^ /? [L,R=302]
</IfModule>
```

5. Theme Detected

Theme: HackDome (v1.0)

Status: Up-to-date, no known vulnerabilities

Fix: No action needed. Continue monitoring theme updates.

6. Plugin Vulnerabilities

Status: No plugins listed in this scan.

May be blocked or not publicly accessible.

Fix: Confirm plugin visibility or scan using alternative methods (e.g., logged-in scan).

General Security Recommendations

- Use strong admin passwords and rotate them regularly.
- Keep WordPress, plugins, and themes updated.
- Enable two-factor authentication (2FA).
- Install a WAF plugin like **Wordfence** or **iThemes Security**.

Report Prepared By:

Pradip Sapkota

Cybersecurity Audit using WPScan

April 20, 2025