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 Outdated WordPress Core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Detected WordPress version: **6.7.2** (Outdated)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94    "status": "outdated",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/`

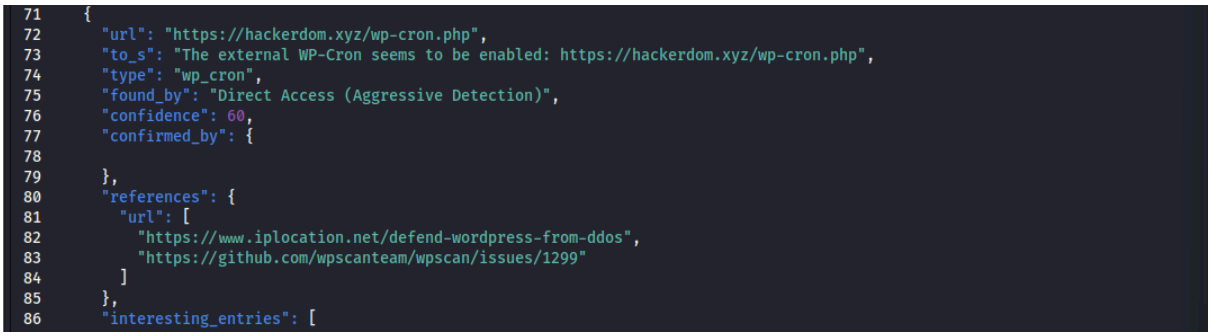
Fix:

- 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.



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.

```
"users": {
  "user": {
    "id": null,
    "found_by": "Rss Generator (Aggressive Detection)",
    "confidence": 50,
    "interesting_entries": [

    ],
    "confirmed_by": {
```

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