Sri Lanka Institute of Information Technology

Cyber Security Assignment (2025)

Vulnerable Outdated Component

Bug Bounty Report- 07

IT23363366

TABLE OF CONTENT

1. Title

Report Title: Vulnerable Outdated Component
Reported By: Raahim Mahmooth
Date: April 23, 2025
Platform: https://hackerone
Tested On: mtn.com

2. Scope & Objective

The objective of this assessment was to identify **outdated software components** and vulnerable libraries used in the application and server infrastructure of mtn.com. By pinpointing deprecated or vulnerable versions of frontend libraries and server components, we can assess potential attack vectors such as XSS, RCE, or privilege escalation. This **report outlines the tools, methodologies, and outcomes of the analysis.**

3. Enumeration and Reconnaissance

3.1 Tools Used

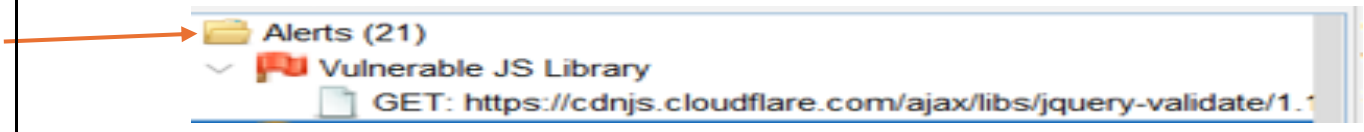
- Manual inspection via **Burp Suite**
- **OWASP ZAP** for passive and active scanning
- **Nikto** for web server vulnerability detection
- **Nmap**
- **XSStrike** for automated XSS testing
- Public vulnerability databases (Exploit-DB, CVE, Snyk)

3.2 Steps

Step 1: ZAP Scan: *to identify outdated component*

- Detected use of `jquery-validation@1.19.3`, known to have a vulnerability related to unsanitized dynamic error messages.

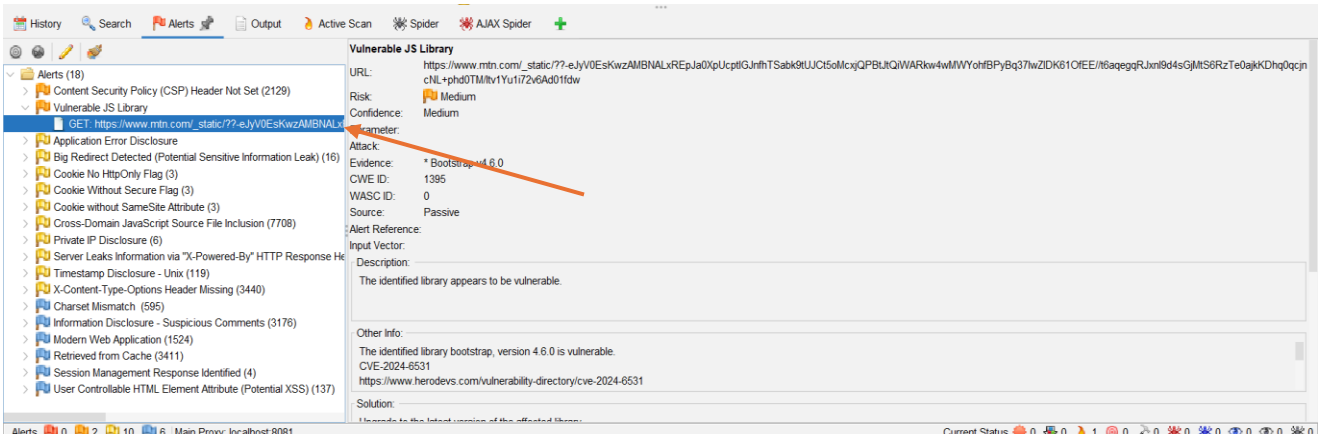
  This screenshot taken in my previous bugbounty

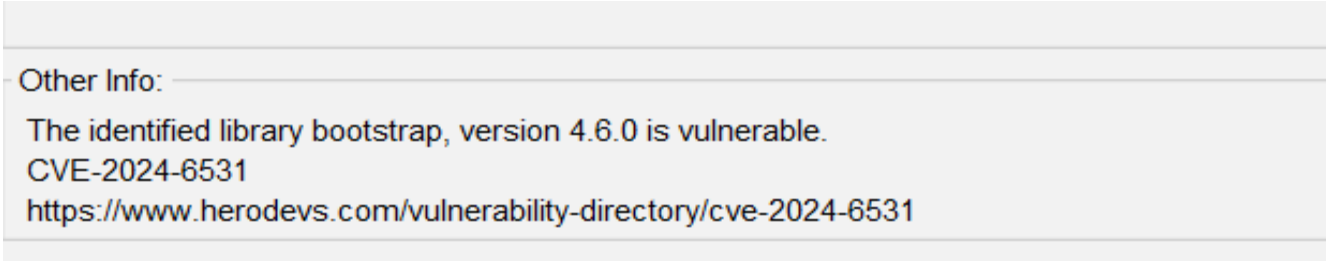


  Manually confirming by viewing the source code

```
<script src="https://code.jquery.com/jquery-1.11.1.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery-validate/1.19.3/jquery.validate.min.js"></script>
```

- Identified `Bootstrap v4.6.0`, which is vulnerable to XSS when used with HTML tooltips and popovers.





Step 2: Nmap Scan: *for OS fingerprinting and service enumeration*

- Server OS fingerprinted as **Linux 2.4.37 (DD-WRT v24-sp2)**.
- Detected open ports: 21 (FTP), 80, 554, and 1723 — all marked as "tcpwrapped", **indicating they are protected by a firewall or proxy**, limiting further service identification.

```
┌──(raahimmahmooth㉿kali)-[~]
└─$ nmap -sS -A 192.0.66.200 -T 4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-30 18:17 EDT
Nmap scan report for 192.0.66.200
Host is up (0.0059s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp?
80/tcp   open  tcpwrapped
|_http-server-header: nginx
|_http-title: 404 Not Found
443/tcp  open  tcpwrapped
|_ssl-date: TLS randomness does not represent time
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=go-vip.co
| Subject Alternative Name: DNS:*.go-vip.co, DNS:go-vip.co
| Not valid before: 2025-03-19T19:44:02
|_Not valid after:  2025-06-17T19:44:01
|_http-server-header: nginx
554/tcp  open  tcpwrapped
1723/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37
OS details: DD-WRT v24-sp2 (Linux 2.4.37)
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.38 ms 192.168.127.2
2   0.40 ms 192.0.66.200

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 234.03 seconds

┌──(raahimmahmooth㉿kali)-[~]
└─$
```

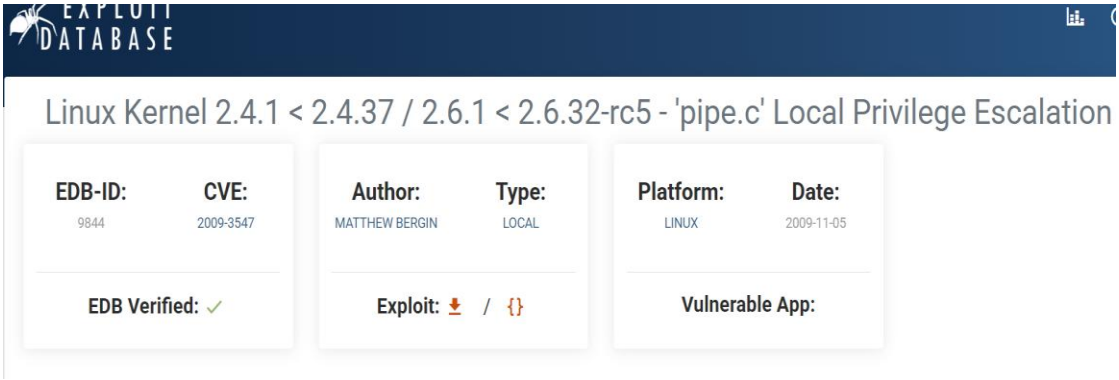
Step 3: OS Vulnerability Investigation

- The DD-WRT version v24-sp2 is known to be outdated.
- Metasploit module `linux/http/ddwrt_cgibin_exec` was found, but further details suggest it may require authenticated access or specific conditions.

  Searching for an exploit module

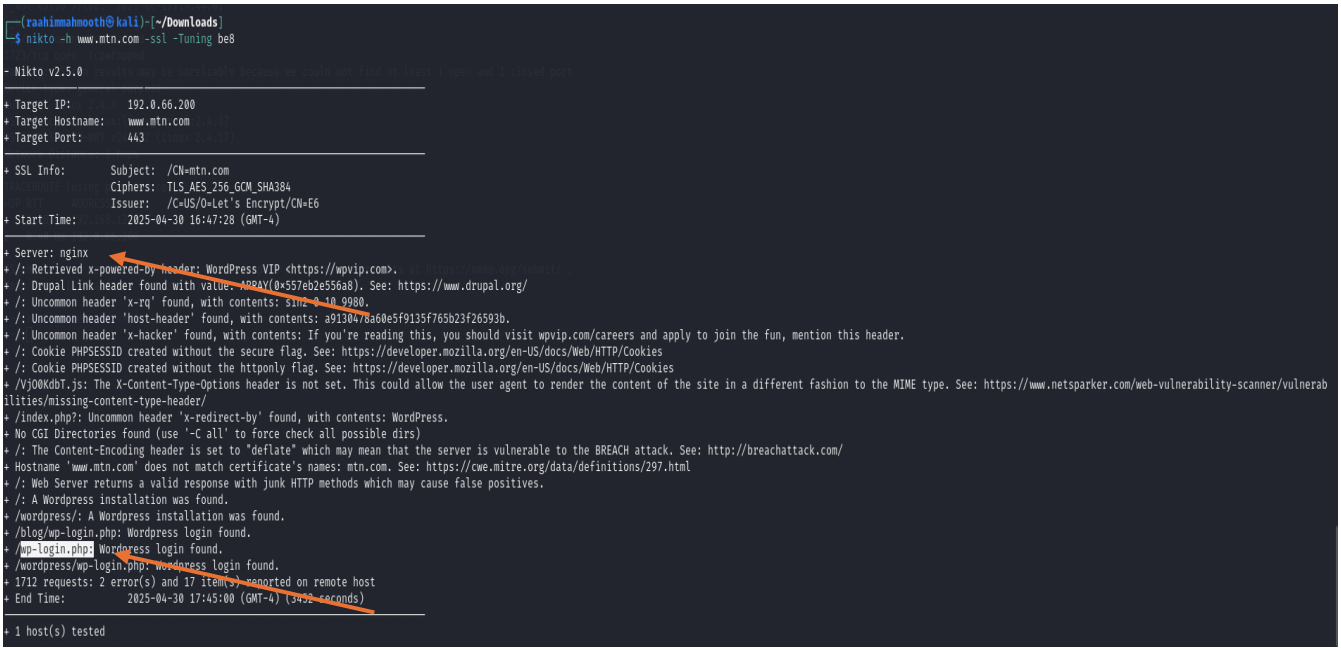
```
msf6 > search dd-wrt

Matching Modules
================

   #  Name                                    Disclosure Date  Rank       Check  Description
   -  ----                                    ---------------  ----       -----  -----------
   0  exploit/linux/http/ddwrt_cgibin_exec    2009-07-20       excellent  No     DD-WRT HTTP Daemon Arbitrary Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/http/ddwrt_cgibin_exec
```

- Exploit-DB shows CVE-2009-2692 — a **Local Privilege Escalation** vulnerability affecting the 2.4.x kernel. Since we don't have any local privileges



Step 4: Niko Scan

- Identified that the web server runs **Nginx** (version not detected).
- Found the presence of `/wp-login.php`, confirming WordPress is used.



- Further scans on identified (via nmap) ports 554 and 1723 produced no actionable output.

4. Vulnerability Description

- **jquery-validation 1.19.3**: This version is susceptible to **unsanitized error messages**, which may lead to XSS if error messages are reflected or used insecurely.
- **Bootstrap 4.6.0**: Known to have issues with unescaped HTML in popovers/tooltips when combined with user input, increasing the risk of **Stored/Reflected XSS**.
- **Outdated Server OS**: Linux kernel 2.4.37 (DD-WRT v24-sp2) is no longer maintained and contains multiple **local privilege escalation vulnerabilities**, posing a significant risk if the server is compromised through another vector.

5. Affected Components

- **JavaScript Libraries:**
  - *https://cdnjs.cloudflare.com/ajax/libs/jquery-validate/1.19.3/jquery.validate.min.js*
  - *Bootstrap 4.6.0* from the site's static script bundler
- **Server OS:**
  - *Linux 2.4.37 (DD-WRT v24-sp2)*

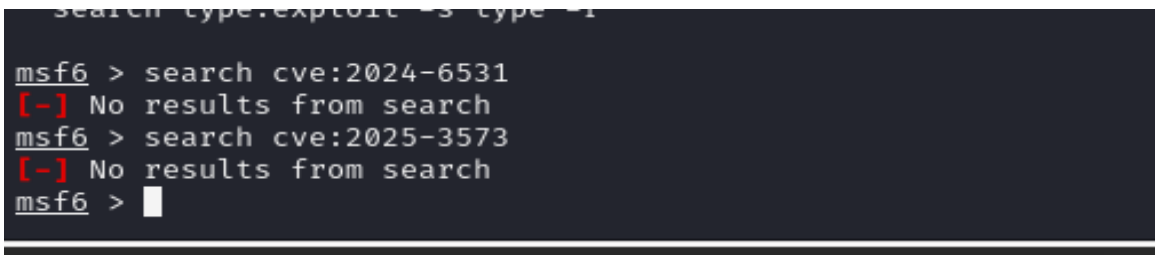
6. Impact Assessment

- **Frontend Libraries**: Outdated JS libraries like jQuery and Bootstrap are widely used, and known vulnerabilities can lead to **client-side attacks**, including **Reflected or Stored XSS**.
- **OS-Level Risks**: An outdated Linux kernel may provide attackers with ways to escalate **privileges if they gain any initial access to the system**.
- **Security Posture**: ***Using unsupported components*** reflects a **weak patch management** strategy, increasing the overall attack surface and likelihood of exploitation.

7. Proof of Concept (PoC)

7.1 Library Exploitation

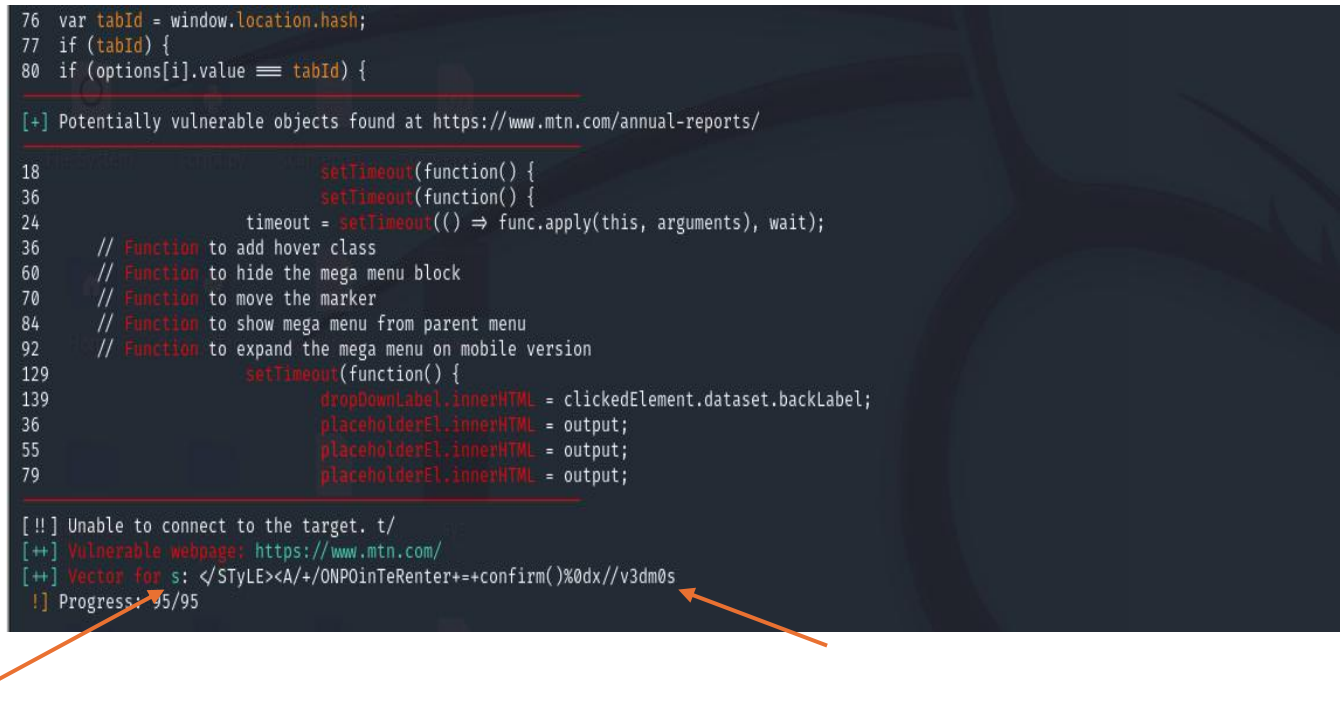
- Searched for known exploits:
  - CVE-2025-3573 (jQuery)
  - CVE-2024-6531 (Bootstrap)
  - No relevant remote exploits found in Metasploit.



- **XSStrike** found a reflected XSS payload on:

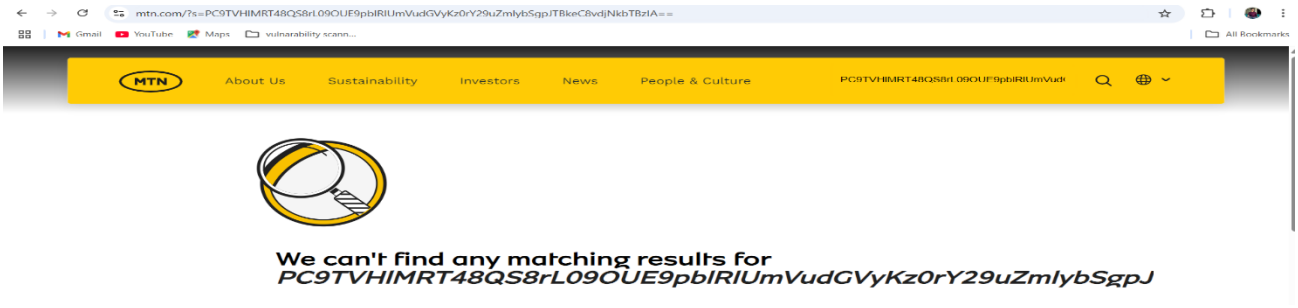
https://www.mtn.com/?s=</STyLE><A/+/ONPOinTeRenter+=+confirm()%0dx//v3dm0s

- Parameter *s=* appears vulnerable.



- However, manual **testing failed** to execute payload in the browser.no popup reflected

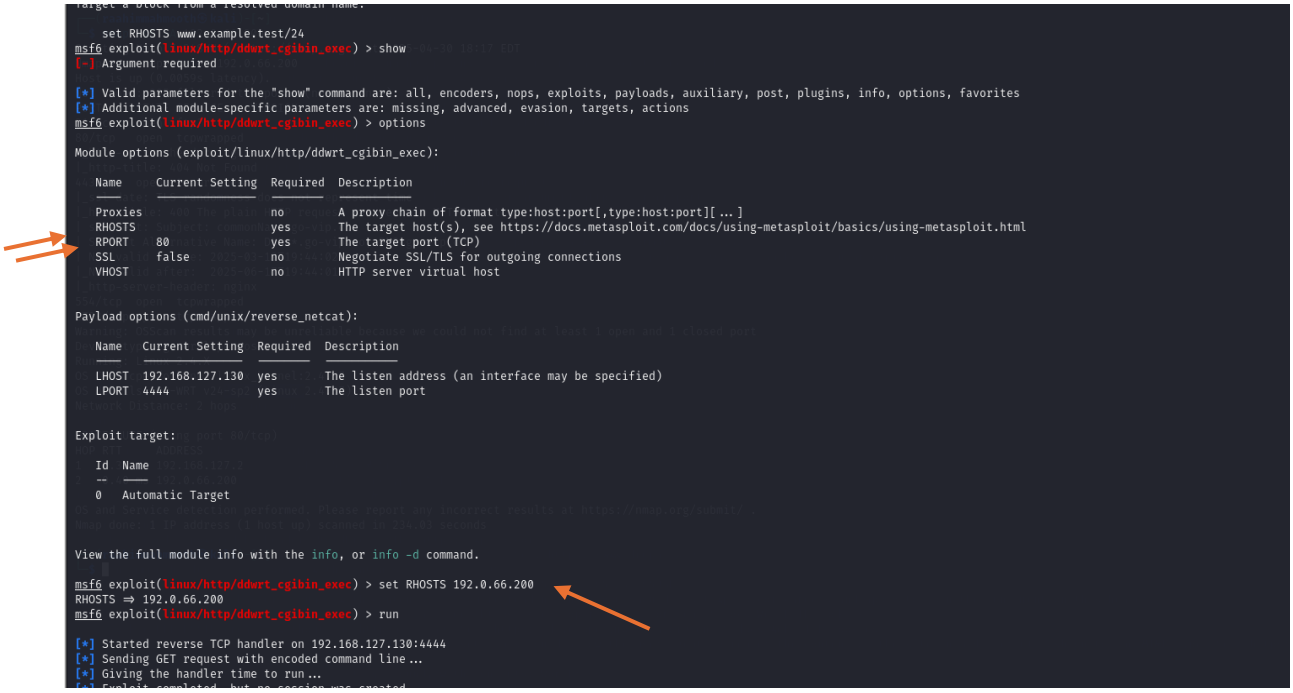
Try with base64 encoded payload.

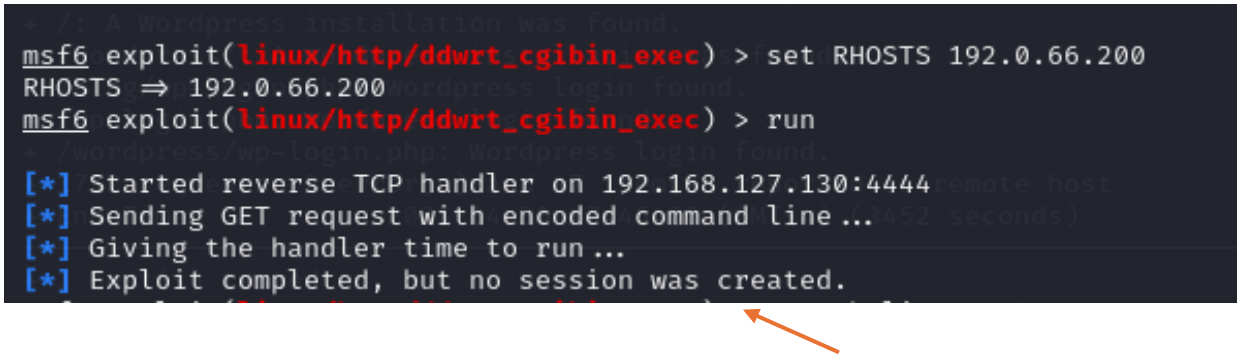


- Result: **Potential vulnerability exists**, but not confirmed exploitable under current conditions. May be vulnerable libraries not actively present on the specific page

7.2 Server Exploitation Attempt

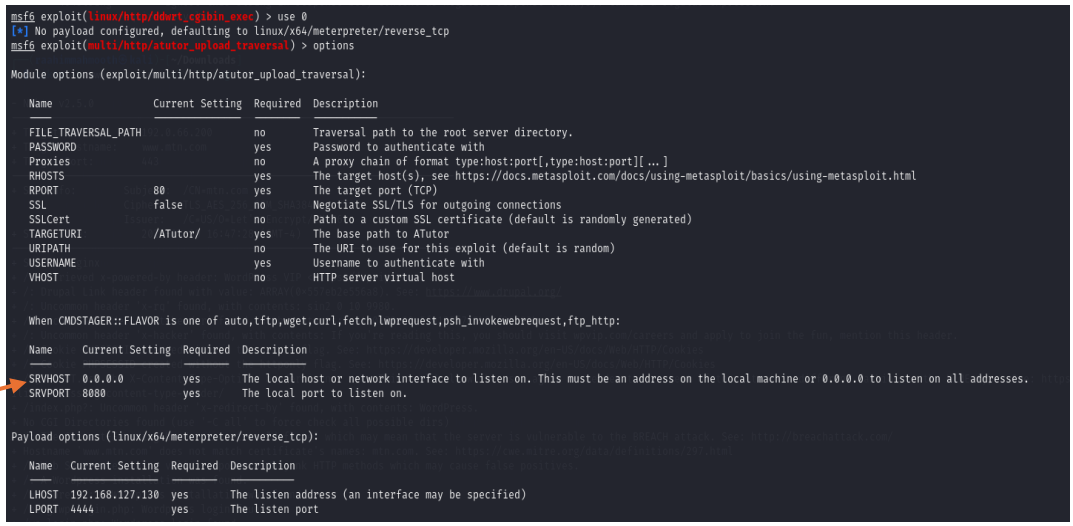
- **DD-WRT Exploit Module** (`linux/http/ddwrt_cgibin_exec`) in Metasploit appeared applicable. But no sessions was created after the exploit





- Attempted testing on *Linux kernel 2.4.37* was inconclusive:
    - The module required parameters suggesting **local access or authenticated context**.
    - Given the **web app context**, local privilege escalation is **not directly exploitable** without another foothold.

Needed a **local access for** this type of exploit



8. Proposed Mitigation

- **Upgrade jQuery-Validate to 1.19.5 or latest** to address error message sanitization flaws.
- **Upgrade Bootstrap to version 5.x or above** to avoid XSS risks via tooltip/popover mechanisms.
- Implement **Content Security Policy (CSP)** headers and input sanitization to mitigate XSS.
- **Update or migrate away from DD-WRT v24-sp2**. Consider using a supported router firmware or upgrading the Linux kernel to a maintained version.
- Conduct regular vulnerability scans and dependency audits using tools like `npm audit`, `Retire.js`, or `OWASP Dependency-Check`.

9. Conclusion

The assessment revealed outdated and potentially vulnerable libraries in the frontend stack and an outdated operating system on the backend. While no confirmed exploitation was achieved, the risks are real, particularly in long-term exposure scenarios.

Efforts were made to test various endpoints, exploit PoCs, and identify outdated components. Some vectors (e.g., the DD-WRT exploit) were not applicable without a local shell or deeper access. Still, these findings suggest the need for a better patch management process.

Note: Full exploitation was not guaranteed, but the environment presents multiple potential attack surfaces worth addressing.

10. References

- *jQuery-Validate Vulnerability – Snyk*
- *Bootstrap 4.6.0 Vulnerability – Snyk*
- *Exploit-DB – Linux Kernel 2.4.37 LPE*
- *OWASP A06:2021 – Vulnerable and Outdated Components*