

Log Analysis – Compromised WordPress | Forensic Case Report

1. Project Summary

This project presents a **comprehensive forensic investigation** of a compromised WordPress server.

The attacker likely exploited a vulnerable plugin, gaining remote code execution (RCE) and operating system access.

Using precise Apache log analysis and Linux CLI tools, we tracked the attacker's movements, identified exploited vulnerabilities, and uncovered a deployed PHP web shell.

2. Tools & Techniques

- `grep, sort, uniq` – Log parsing and pattern extraction
- DeepBlueCLI – Windows event log review (contextual support)
- WPScan – WordPress vulnerability enumeration
- `sqlmap` – SQL injection exploitation
- CVE Database Research – Vulnerability validation
- Manual timeline correlation

3. Case Overview

| Category | Detail |
|---------------------------------|--|
| Target | Compromised WordPress Server |
| OS | Linux |
| Primary Hypothesis | Plugin vulnerability exploited for RCE |
| Root Cause | Simple File List plugin vulnerability |
| Web Shell Deployed | <code>fr34k.php</code> |
| Final HTTP Response (Web Shell) | 404 Not Found |

4. Step-by-Step Investigation



Step 1: Identify Admin Login Panel

Command:

```
grep "wp-login.php" access.log
```

Finding:

```
GET /wp-login.php?itsec-hb-token=adminlogin
```

 **Key Insight:** Tokenized admin login URL was used to bypass traditional login defenses.

```

kali@kali: ~/Downloads
$ unzip SjuVmFhhCn5PEcmj5FMESd2FpEq9MT(1).zip
Archive: SjuVmFhhCn5PEcmj5FMESd2FpEq9MT(1).zip
SjuVmFhhCn5PEcmj5FMESd2FpEq9MT(1).zip access.log password:
password incorrect -reenter:
password incorrect -reenter:
replace access.log? [y]es, [n]o, [A]ll, [N]one, [r]ename: n

kali@kali: ~/Downloads
$ cat access.log | grep wp-login.php
172.21.0.1 - - [12/Jan/2021:15:53:22 +0000] "GET /wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin%2F&reauth=1 HTTP/1.1" 200 4633 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 - - [12/Jan/2021:15:53:22 +0000] "GET /wp-includes/css/buttons.min.css?ver=5.6 HTTP/1.1" 200 1788 "http://172.21.0.3/wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin%2F&reauth=1" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 - - [12/Jan/2021:15:53:22 +0000] "GET /wp-admin/css/login.min.css?ver=5.6 HTTP/1.1" 200 2296 "http://172.21.0.3/wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin%2F&reauth=1" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 - - [12/Jan/2021:15:53:22 +0000] "GET /wp-includes/js/zxcvbn-async.min.js?ver=1.0 HTTP/1.1" 200 608 "http://172.21.0.3/wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin%2F&reauth=1" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 - - [12/Jan/2021:15:53:22 +0000] "GET /wp-admin/css/forms.min.css?ver=5.6 HTTP/1.1" 200 6469 "http://172.21.0.3/wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin%2F&reauth=1" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 - - [12/Jan/2021:15:53:22 +0000] "GET /wp-admin/css/10n.min.css?ver=5.6 HTTP/1.1" 200 1022 "http://172.21.0.3/wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin%2F&reauth=1" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 - - [12/Jan/2021:15:53:22 +0000] "GET /wp-includes/js/wp-util.min.js?ver=5.6 HTTP/1.1" 200 940 "http://172.21.0.3/wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin%2F&reauth=1" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 - - [12/Jan/2021:15:53:22 +0000] "GET /wp-includes/js/underscore.min.js?ver=1.8.3 HTTP/1.1" 200 6056 "http://172.21.0.3/wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin%2F&reauth=1" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 - - [12/Jan/2021:15:53:22 +0000] "GET /wp-includes/js/dist/i18n.min.js?ver=326fe7fbfdb407b6edcbfa7e17f3909 HTTP/1.1" 200 4030 "http://172.21.0.3/wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin%2F&reauth=1" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 - - [12/Jan/2021:15:53:22 +0000] "GET /wp-admin/js/password-strength-meter.min.js?ver=5.6 HTTP/1.1" 200 971 "http://172.21.0.3/wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin%2F&reauth=1" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 - - [12/Jan/2021:15:53:22 +0000] "GET /wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=7.4.4 HTTP/1.1" 200 34595 "http://172.21.0.3/wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin%2F&reauth=1" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 - - [12/Jan/2021:15:53:22 +0000] "GET /wp-admin/js/user-profile.min.js?ver=5.6 HTTP/1.1" 200 2451 "http://172.21.0.3/wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin%2F&reauth=1" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 - - [12/Jan/2021:15:53:23 +0000] "POST /wp-login.php HTTP/1.1" 302 1136 "http://172.21.0.3/wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin%2F&reauth=1" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 - - [12/Jan/2021:15:53:31 +0000] "GET /wp-admin/ HTTP/1.1" 200 16408 "http://172.21.0.3/wp-login.php?redirect_to=http%3A%2F%2F172.21.0.3%2Fwp-admin"

```

```
[*] kali@kali: ~/Downloads
[*] rv:1.9.0.6) Gecko/2009020410 Fedora/3.0.6-1.fc10 Firefox/3.0.10
110.29.54.120 -- [14/Jan/2021:06:15:40 +0000] "POST /wp-login.php?itsec-hb-token=adminlogin HTTP/1.1" 403 3303 "-" Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.6) Gecko/2009020410 Fedora/3.0.6-1.fc10 Firefox/3.0.10
[Thu Jan 14 07:42:17.055410 2021] [php:error] [pid 22] [client 172.21.0.1:44924] script '/var/www/html/wp-login.php' not found or unable to stat
172.21.0.1 -- [14/Jan/2021:07:46:17 +0000] "GET /wp-login.php?itsec-hb-token=adminlogin HTTP/1.1" 404 489 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
[Thu Jan 14 07:42:19.321162 2021] [php:error] [pid 22] [client 172.21.0.1:44924] script '/var/www/html/wp-login.php' not found or unable to stat
172.21.0.1 -- [14/Jan/2021:07:46:19 +0000] "GET /wp-login.php?itsec-hb-token=adminlogin HTTP/1.1" 404 488 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
172.21.0.1 -- [14/Jan/2021:07:46:19 +0000] "GET /wp-login.php HTTP/1.1" 404 488 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
[Thu Jan 14 07:42:22.533632 2021] [php:error] [pid 22] [client 172.21.0.1:44924] script '/var/www/html/wp-login.php' not found or unable to stat
[Thu Jan 14 07:42:34.921671 2021] [php:error] [pid 26] [client 172.21.0.1:44944] script '/var/www/html/wp-login.php' not found or unable to stat
172.21.0.1 -- [14/Jan/2021:07:46:34 +0000] "GET /wp-login.php?itsec-hb-token=adminlogin HTTP/1.1" 404 489 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
[Thu Jan 14 07:42:37.012631 2021] [php:error] [pid 26] [client 172.21.0.1:44944] script '/var/www/html/wp-login.php' not found or unable to stat
172.21.0.1 -- [14/Jan/2021:07:46:37 +0000] "GET /wp-login.php?itsec-hb-token=adminlogin HTTP/1.1" 404 488 "-" Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
```

Step 2: Identify Attacker's Tools

Evidence:

- Log entries containing WPScan user agents.
- SQL injection attempts using sqlmap patterns.

- 🔑 **Key Insight:** WPScan for reconnaissance and sqlmap for SQL injection were confirmed as attacker tools.

```
(kali@kali)~[~/Downloads]
$ grep -i 'wpscan' access.log
grep -i 'sqlmap' access.log
grep -i 'curl' access.log
grep -i 'wget' access.log
grep -i 'nmap' access.log
grep -i 'burp' access.log

119.241.22.121 - - [14/Jan/2021:06:01:41 +0000] "GET / HTTP/1.1" 403 3160 "http://172.21.0.3/" "WPScan v3.8.10 (https://wpscan.org/)"
168.22.54.119 - - [14/Jan/2021:06:12:53 +0000] "POST /wp-login.php HTTP/1.1" 302 243 "-" "sqlmap/1.4.11#stable (http://sqlmap.org)"
```

Vulnerability Researcher

Step 1: Identify Exploited Plugin

Command:

```
grep "wp-content/plugins/" access.log | sort | uniq > plugin_access.log
```

Finding:

Heavy interactions with Simple File List plugin.

CVE Validation:

[CVE-2020-35489](#) – Simple File List 4.2.2 Remote Code Execution.

- 🔑 **Key Insight:** Simple File List plugin was the initial attack vector.

```
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"

(kali@kali)~[~/Downloads]
$ cat access.log | grep "/wp-content/plugins/"

172.21.0.1 - - [12/Jan/2021:15:53:50 +0000] "GET /wp-content/plugins/akismet/inc/akismet.js?ver=4.1.7 HTTP/1.1" 200 4139 "http://172.21.0.3/wp-admin/options-general.php?page=akismet-key-config&view=start" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
172.21.0.1 - - [12/Jan/2021:15:53:50 +0000] "GET /wp-content/plugins/akismet/inc/akismet.css?ver=4.1.7 HTTP/1.1" 200 3487 "http://172.21.0.3/wp-admin/options-general.php?page=akismet-key-config&view=start" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
172.21.0.1 - - [12/Jan/2021:15:53:50 +0000] "GET /wp-content/plugins/akismet/inc/img/logo-full-2x.png HTTP/1.1" 200 5338 "http://172.21.0.3/wp-admin/options-general.php?page=akismet-key-config&view=start" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
172.21.0.1 - - [12/Jan/2021:15:57:28 +0000] "GET /wp-content/plugins/better-wp-security/dist/core/admin-notices.min.css?ver=d035a754e0e995d7f2a8 HTTP/1.1" 200 2294 "http://172.21.0.3/wp-admin/plugins.php?plugin_status=all&paged=15s" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
172.21.0.1 - - [12/Jan/2021:15:57:28 +0000] "GET /wp-content/plugins/better-wp-security/lib/icon-fonts/icon-fonts.css?ver=5.6 HTTP/1.1" 200 896 "http://172.21.0.3/wp-admin/plugins.php?plugin_status=all&paged=15s" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
172.21.0.1 - - [12/Jan/2021:15:57:29 +0000] "GET /wp-content/plugins/better-wp-security/dist/vendors/core/admin-notices-api-api-settings.min.js?ver=c5d904b2839be81df49e HTTP/1.1" 200 4119 "http://172.21.0.3/wp-admin/plugins.php?plugin_status=all&paged=15s" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
172.21.0.1 - - [12/Jan/2021:15:57:29 +0000] "GET /wp-content/plugins/better-wp-security/dist/core/admin-notices-api.min.js?ver=347f2aa808de04b456c5 HTTP/1.1" 200 4932 "http://172.21.0.3/wp-admin/plugins.php?plugin_status=all&paged=15s" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
172.21.0.1 - - [12/Jan/2021:15:57:29 +0000] "GET /wp-content/plugins/better-wp-security/dist/core/admin-notices.min.js?ver=2cfla195a17e8ff8a47d HTTP/1.1" 200 3703 "http://172.21.0.3/wp-admin/plugins.php?plugin_status=all&paged=15s" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
172.21.0.1 - - [12/Jan/2021:15:57:30 +0000] "GET /wp-content/plugins/better-wp-security/lib/icon-fonts/fonts/itthemes-icons.woff HTTP/1.1" 200 2725 "http://172.21.0.3/wp-content/plugins/better-wp-security/lib/icon-fonts/icon-fonts.css?ver=5.6" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

Step 2: Analyze Exploitation Path

Evidence:

```
/wp-content/plugins/simple-file-list/
```

- 🔑 **Key Insight:** Exploit path directly targeted plugin's upload interface.

Threat Hunter

Step 1: Locate Web Shell

Command:

```
grep "uploads/*.php" access.log
```

Finding:

```
GET /wp-content/uploads/fr34k.php
```



Key Insight: Attacker uploaded PHP web shell to uploads directory.

```
(kali@kali) ~/Downloads
$ grep "uploads/*.php" access.log

Thu Jan 14 06:03:49.745554 2021 [autoindex:error] [pid 88] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:49.758020 2021 [autoindex:error] [pid 87] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:49.760732 2021 [autoindex:error] [pid 89] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:49.773617 2021 [autoindex:error] [pid 83] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:49.958274 2021 [autoindex:error] [pid 83] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:49.962993 2021 [autoindex:error] [pid 92] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:50.070529 2021 [autoindex:error] [pid 85] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:50.073138 2021 [autoindex:error] [pid 88] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:50.177985 2021 [autoindex:error] [pid 83] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:50.182871 2021 [autoindex:error] [pid 99] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:50.186417 2021 [autoindex:error] [pid 84] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:50.189607 2021 [autoindex:error] [pid 92] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:50.193185 2021 [autoindex:error] [pid 85] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:50.196027 2021 [autoindex:error] [pid 88] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
Thu Jan 14 06:03:50.199521 2021 [autoindex:error] [pid 86] [client 168.22.54.119:0] AH01276: Cannot serve directory /var/www/html/wp-content/uploads/: No
matching DirectoryIndex (index.php,index.html) found, and server-generated directory index forbidden by Options directive, referer: http://172.21.0.3/
03.69.55.212 - - [14/Jan/2021:06:27:04 +0000] "GET /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 1295 "-" Mozilla/4.0 (compatible; MSIE 7.
; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
03.69.55.212 - - [14/Jan/2021:06:27:06 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 1213 "http://172.21.0.3/wp-content/upload
/simple-file-list/fr34k.php" Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.
```

Step 2: Validate Final Response Code

Finding:

HTTP response code: 404 Not Found (shell likely removed post-compromise or cleaned by defender).



Key Insight: Final shell access attempt returned 404, indicating post-attack cleanup or shell deletion.

```
File Actions Edit View Help
s/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
103.69.55.212 - - [14/Jan/2021:06:28:02 +0000] "GET /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 5356 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
103.69.55.212 - - [14/Jan/2021:06:28:11 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 5588 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
103.69.55.212 - - [14/Jan/2021:06:28:12 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 4672 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
103.69.55.212 - - [14/Jan/2021:06:28:41 +0000] "GET /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 5357 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
103.69.55.212 - - [14/Jan/2021:06:28:57 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 5754 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
103.69.55.212 - - [14/Jan/2021:06:29:02 +0000] "GET /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 5356 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
103.69.55.212 - - [14/Jan/2021:06:29:09 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 6513 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
103.69.55.212 - - [14/Jan/2021:06:29:09 +0000] "GET /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 5357 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
103.69.55.212 - - [14/Jan/2021:06:29:35 +0000] "GET /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 5357 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
103.69.55.212 - - [14/Jan/2021:06:29:41 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 4789 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
103.69.55.212 - - [14/Jan/2021:06:29:59 +0000] "GET /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 5357 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
103.69.55.212 - - [14/Jan/2021:06:30:01 +0000] "POST /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 200 215 "http://172.21.0.3/wp-content/uploads/simple-file-list/fr34k.php" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
103.69.55.212 - - [14/Jan/2021:06:30:05 +0000] "GET /wp-content/uploads/simple-file-list/fr34k.php HTTP/1.1" 404 488 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; Tablet PC 2.0)"
(kali@kali) - [~/Downloads]
```

5. Final Consensus Solution

| Investigation Objective | Answer |
|---|---|
| Admin Login Panel URI | GET /wp-login.php?itsec-hb-token=adminlogin |
| Tools Used by Attacker | WPScan, sqlmap |
| Exploited Plugin | Simple File List 4.2.2 |
| Exploited Plugin CVE | CVE-2020-35489 |
| PHP Web Shell File | fr34k.php |
| Final HTTP Response Code (Web Shell Access) | 404 Not Found |

6. Sample Commands

```
# Command: Find login attempts
grep "wp-login.php" access.log

# Command: Find plugin interactions
grep "wp-content/plugins/" access.log | sort | uniq > plugin_access.log
```






Command: Search for web shells in uploads directory

```
grep "uploads/*.php" access.log
```

Command: Search for sqlmap SQL injection attempts

```
grep -i "sqlmap" access.log
```

7. Lessons Learned

-  Vet and minimize third-party plugin usage.
-  Maintain regular patch cycles for all plugins and themes.
-  Monitor upload directories for PHP files and unauthorized changes.
-  Enforce directory browsing restrictions.
-  Conduct periodic log reviews to detect early signs of compromise.

8. Project Impact

This forensic analysis provided a **clear attack timeline and root cause assessment**.

It not only uncovered the breach but established a repeatable methodology to harden WordPress deployments and enhance incident response capabilities.

9. Acknowledgements

- The forensic investigation team.
- BTLO platform for creating this challenge.
- Community write-ups that supported cross-verification.

10. References

- [CVE-2020-35489 – NVD Entry](#)
- Simple File List Plugin – WordPress
- BTLO Challenge: Log Analysis – Compromised WordPress