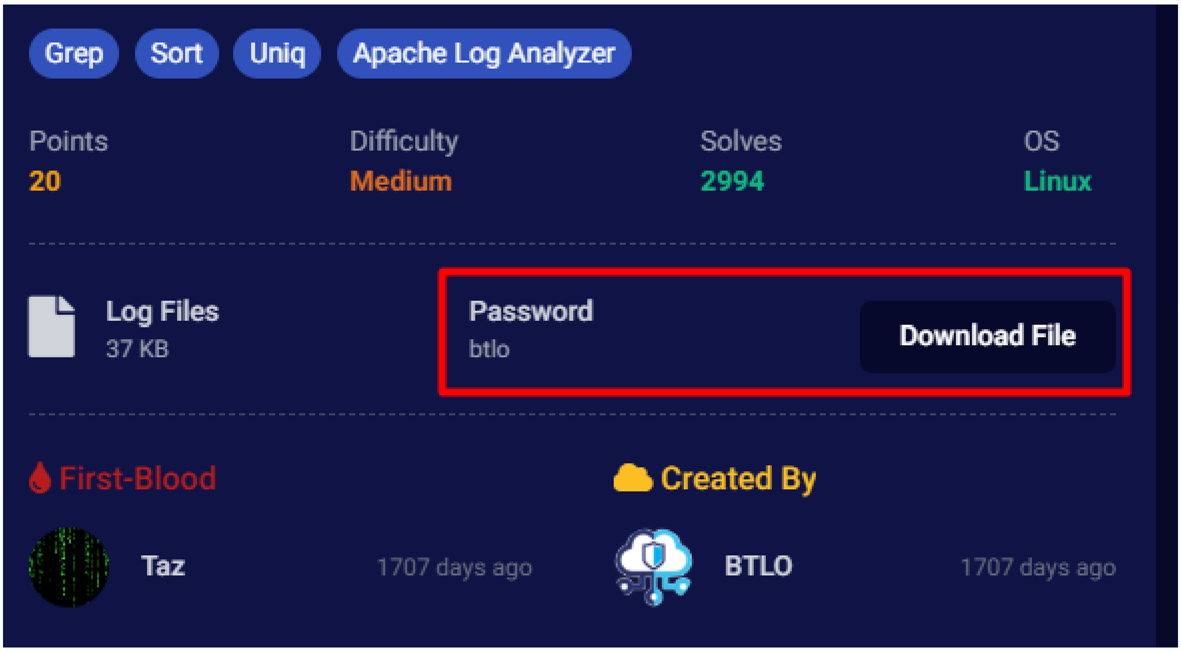
Reference: https://blueteamlabs.online/home/challenge/log-analysis-compromised-wordpress-ce000f5b59

Download the log file from the above link. The log file is **Apache log**.



Grep Sort Uniq Apache Log Analyzer

Points 20

Difficulty Medium

Solves 2994

OS Linux

Log Files 37 KB

Password btlo

Download File

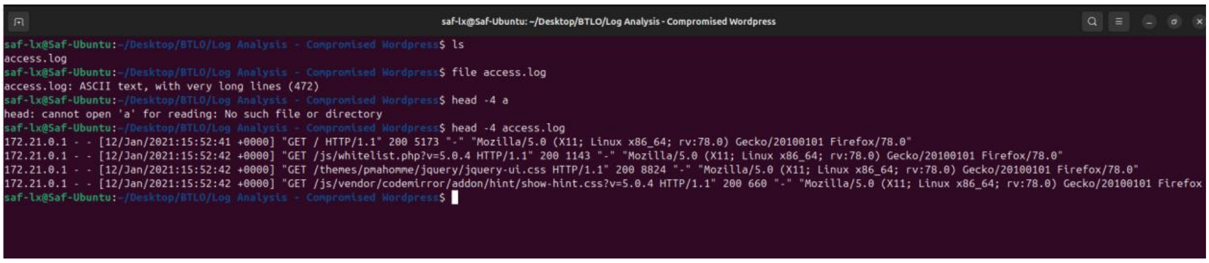
First-Blood

Taz 1707 days ago

Created By

BTLO 1707 days ago

Type of file in linux shell

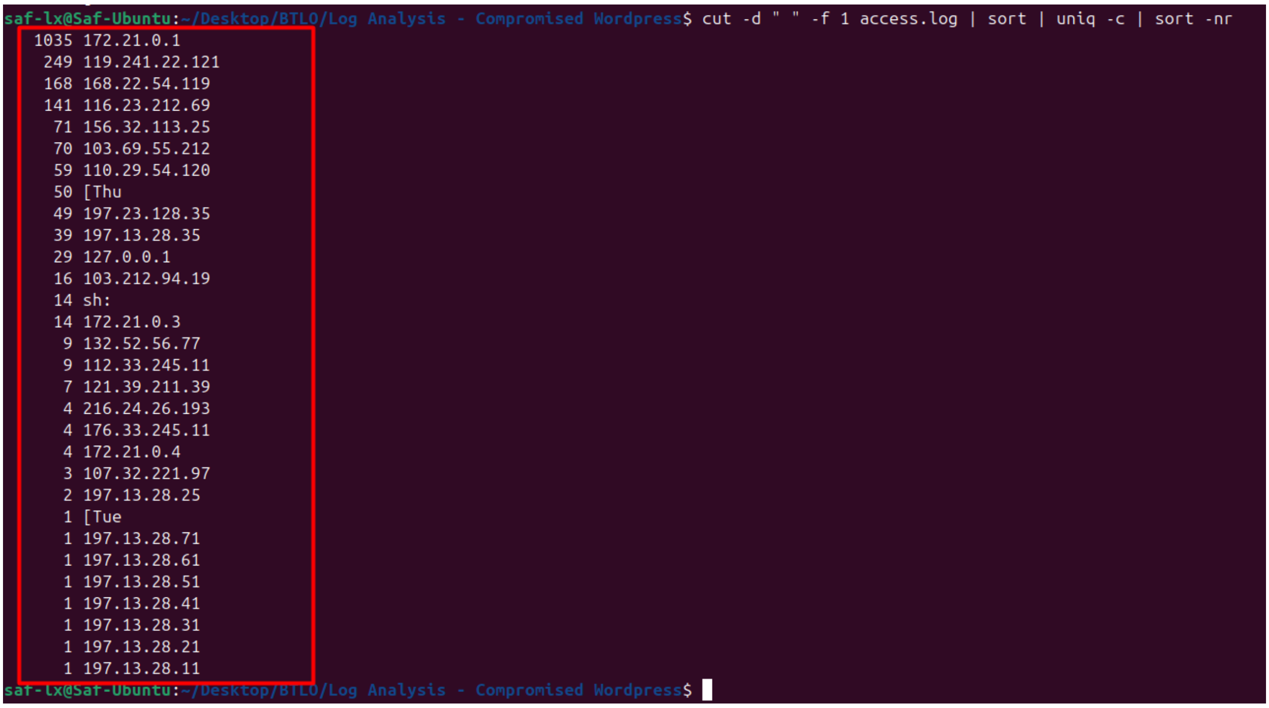


saf-lx@Saf-Ubuntu: ~/Desktop/BTLO/Log Analysis - Compromised Wordpress

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ ls
access.log
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ file access.log
access.log: ASCII text, with very long lines (472)
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ head -4 a
head: cannot open 'a' for reading: No such file or directory
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ head -4 access.log
172.21.0.1 - - [12/Jan/2021:15:52:41 +0000] "GET / HTTP/1.1" 200 5173 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
172.21.0.1 - - [12/Jan/2021:15:52:42 +0000] "GET /js/whitelist.php?v=5.0.4 HTTP/1.1" 200 1143 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
172.21.0.1 - - [12/Jan/2021:15:52:42 +0000] "GET /themes/pmahomme/jquery/jquery-ui.css HTTP/1.1" 200 8824 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
172.21.0.1 - - [12/Jan/2021:15:52:42 +0000] "GET /js/vendor/codemirror/addon/hint/show-hint.css?v=5.0.4 HTTP/1.1" 200 660 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$
```

Use of cut, grep, uniq and sort to filter out first the ip address.

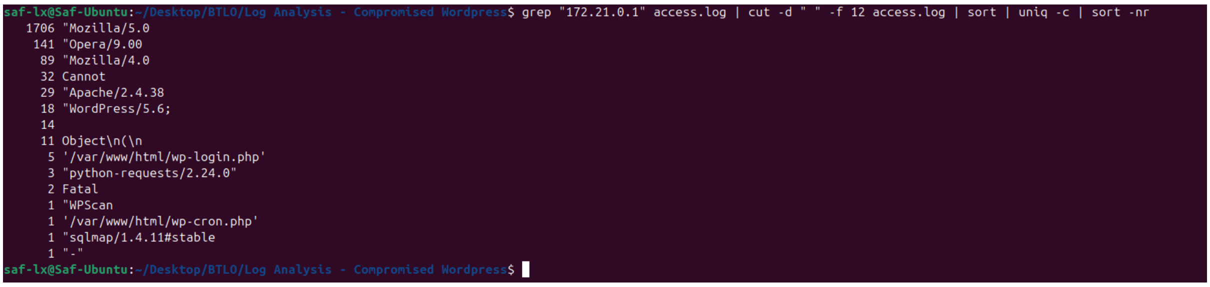
cut -d " " -f 1 access.log | sort | uniq -c | sort -nr



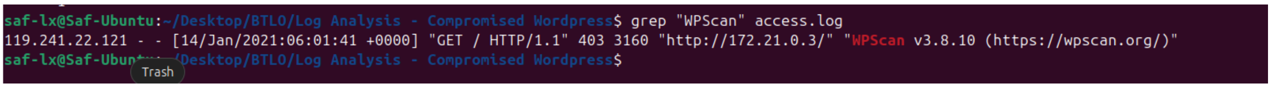
```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ cut -d " " -f 1 access.log | sort | uniq -c | sort -nr
   1035 172.21.0.1
    249 119.241.22.121
    168 168.22.54.119
    141 116.23.212.69
     71 156.32.113.25
     70 103.69.55.212
     59 110.29.54.120
     50 [Thu
     49 197.23.128.35
     39 197.13.28.35
     29 127.0.0.1
     16 103.212.94.19
     14 sh:
     14 172.21.0.3
      9 132.52.56.77
      9 112.33.245.11
      7 121.39.211.39
      4 216.24.26.193
      4 176.33.245.11
      4 172.21.0.4
      3 107.32.221.97
      2 197.13.28.25
      1 [Tue
      1 197.13.28.71
      1 197.13.28.61
      1 197.13.28.51
      1 197.13.28.41
      1 197.13.28.31
      1 197.13.28.21
      1 197.13.28.11
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$
```

Number of IP 172.21.0.1 is a lot so let’s investigate it.

grep "172.21.0.1" access.log | cut -d " " -f 12 access.log | sort | uniq -c | sort -nr

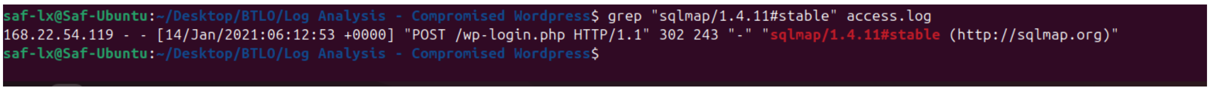


```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ grep "172.21.0.1" access.log | cut -d " " -f 12 access.log | sort | uniq -c | sort -nr
   1706 "Mozilla/5.0
    141 "Opera/9.00
     89 "Mozilla/4.0
     32 Cannot
     29 "Apache/2.4.38
     18 "WordPress/5.6;
     14
     11 Object\n(\n
      5 '/var/www/html/wp-login.php'
      3 "python-requests/2.24.0"
      2 Fatal
      1 "WPScan
      1 '/var/www/html/wp-cron.php'
      1 "sqlmap/1.4.11#stable
      1 "-"
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$
```



```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ grep "WPScan" 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/)"
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$
```

The client is making a request. The client is WPScan running on a machine with 119.241.22.121.

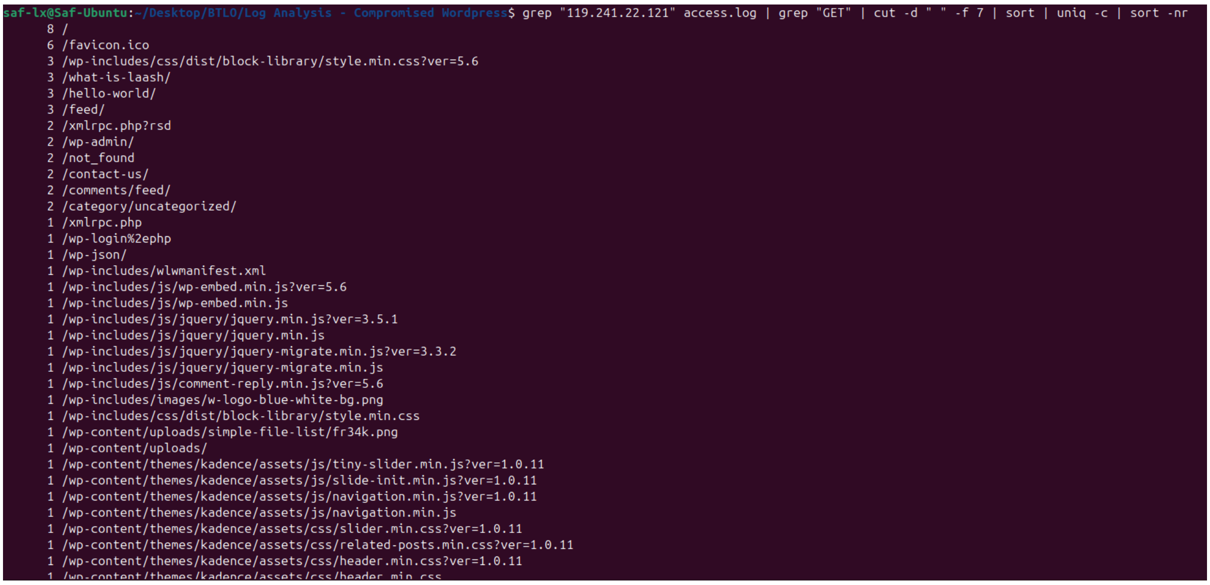


```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ grep "sqlmap/1.4.11#stable" access.log
168.22.54.119 - - [14/Jan/2021:06:12:53 +0000] "POST /wp-login.php HTTP/1.1" 302 243 "-" "sqlmap/1.4.11#stable (http://sqlmap.org)"
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$
```

Seems like the client at 168.22.54.119 sent a POST request to WordPress Login Page. The request is made using sqlmap, designed to find SQL injection.

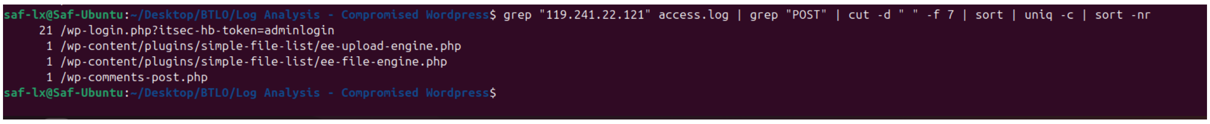
The two IP address: 119.241.22.121 and 168.22.54.119 looks suspicious. Let’s carry out investigation by grep command.

grep "119.241.22.121" access.log | grep "GET" | cut -d " " -f 7 | sort | uniq -c | sort -nr



```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ grep "119.241.22.121" access.log | grep "GET" | cut -d " " -f 7 | sort | uniq -c | sort -nr
      8 /
      6 /favicon.ico
      3 /wp-includes/css/dist/block-library/style.min.css?ver=5.6
      3 /what-is-laash/
      3 /hello-world/
      3 /feed/
      2 /xmlrpc.php?rsd
      2 /wp-admin/
      2 /not_found
      2 /contact-us/
      2 /comments/feed/
      2 /category/uncategorized/
      1 /xmlrpc.php
      1 /wp-login%2ephp
      1 /wp-json/
      1 /wp-includes/wlwmanifest.xml
      1 /wp-includes/js/wp-embed.min.js?ver=5.6
      1 /wp-includes/js/wp-embed.min.js
      1 /wp-includes/js/jquery/jquery.min.js?ver=3.5.1
      1 /wp-includes/js/jquery/jquery.min.js
      1 /wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2
      1 /wp-includes/js/jquery/jquery-migrate.min.js
      1 /wp-includes/js/comment-reply.min.js?ver=5.6
      1 /wp-includes/images/w-logo-blue-white-bg.png
      1 /wp-includes/css/dist/block-library/style.min.css
      1 /wp-content/uploads/simple-file-list/fr34k.png
      1 /wp-content/uploads/
      1 /wp-content/themes/kadence/assets/js/tiny-slider.min.js?ver=1.0.11
      1 /wp-content/themes/kadence/assets/js/slide-init.min.js?ver=1.0.11
      1 /wp-content/themes/kadence/assets/js/navigation.min.js?ver=1.0.11
      1 /wp-content/themes/kadence/assets/js/navigation.min.js
      1 /wp-content/themes/kadence/assets/css/slider.min.css?ver=1.0.11
      1 /wp-content/themes/kadence/assets/css/related-posts.min.css?ver=1.0.11
      1 /wp-content/themes/kadence/assets/css/header.min.css?ver=1.0.11
      1 /wp-content/themes/kadence/assets/css/header.min.css
```

We couldn’t see anything when we grep with GET. Let’s do with POST.

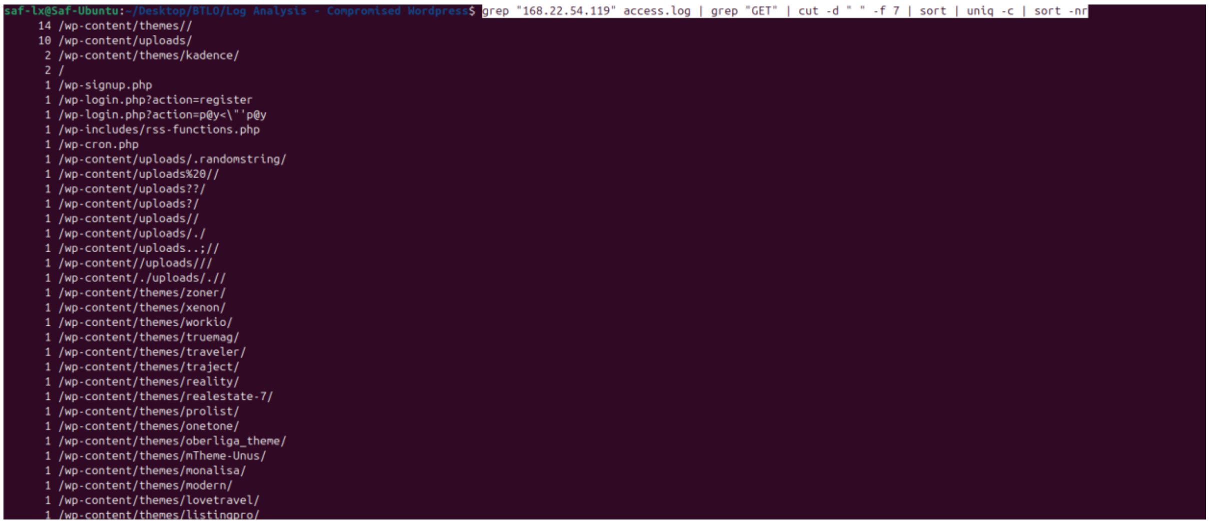


```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ grep "119.241.22.121" access.log | grep "POST" | cut -d " " -f 7 | sort | uniq -c | sort -nr
     21 /wp-login.php?itsec-hb-token=adminlogin
      1 /wp-content/plugins/simple-file-list/ee-upload-engine.php
      1 /wp-content/plugins/simple-file-list/ee-file-engine.php
      1 /wp-comments-post.php
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$
```

So, count 21 with /wp-login.php?itsec-hb-token=adminlogin, which is interesting in wordpress login php. The client (IP 119.241.22.121) made a **POST request** to your WordPress login page. Seems like the attacker is trying to gain access to.

With another IP, let’s extract with GET request.

grep "168.22.54.119" access.log | grep "GET" | cut -d " " -f 7 | sort | uniq -c | sort -nr

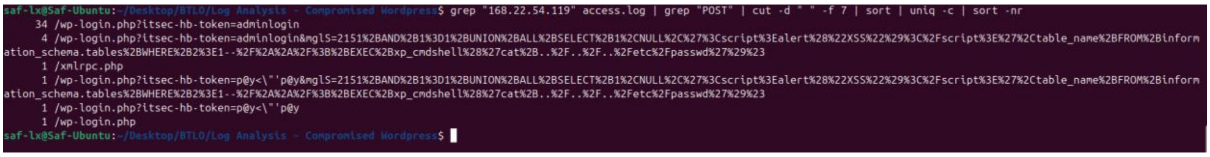


```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ grep "168.22.54.119" access.log | grep "GET" | cut -d " " -f 7 | sort | uniq -c | sort -nr
     14 /wp-content/themes//
     10 /wp-content/uploads/
      2 /wp-content/themes/kadence/
      2 /
      1 /wp-signup.php
      1 /wp-login.php?action=register
      1 /wp-login.php?action=p@y<\"'p@y
      1 /wp-includes/rss-functions.php
      1 /wp-cron.php
      1 /wp-content/uploads/.randomstring/
      1 /wp-content/uploads%20//
      1 /wp-content/uploads??/
      1 /wp-content/uploads?/
      1 /wp-content/uploads//
      1 /wp-content/uploads/./
      1 /wp-content/uploads..;//
      1 /wp-content//uploads///
      1 /wp-content/./uploads/.//
      1 /wp-content/themes/zoner/
      1 /wp-content/themes/xenon/
      1 /wp-content/themes/workio/
      1 /wp-content/themes/truemag/
      1 /wp-content/themes/traveler/
      1 /wp-content/themes/traject/
      1 /wp-content/themes/reality/
      1 /wp-content/themes/realestate-7/
      1 /wp-content/themes/prolist/
      1 /wp-content/themes/onetone/
      1 /wp-content/themes/oberliga_theme/
      1 /wp-content/themes/mTheme-Unus/
      1 /wp-content/themes/monalisa/
      1 /wp-content/themes/modern/
      1 /wp-content/themes/lovetravel/
      1 /wp-content/themes/listingpro/
```

Also, with POST

grep "168.22.54.119" access.log | grep "POST" | cut -d " " -f 7 | sort | uniq -c | sort -nr

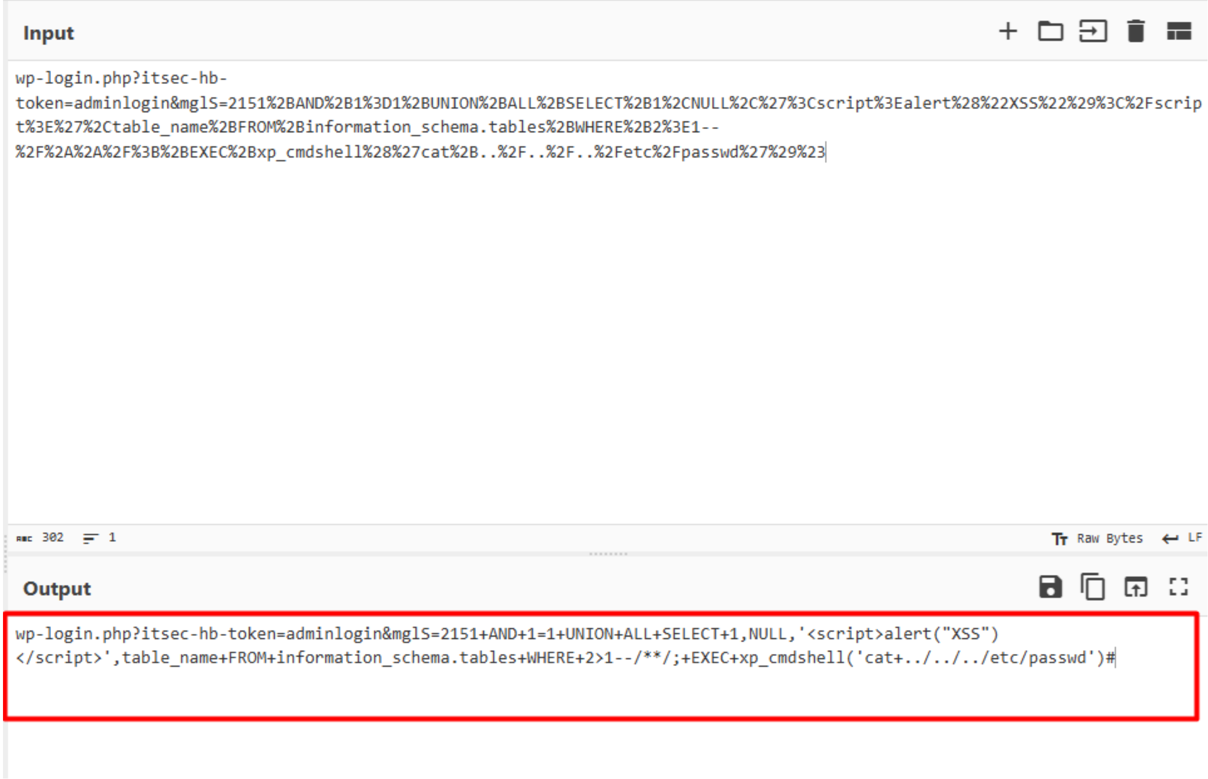
We found some interesting output here as



```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ grep "168.22.54.119" access.log | grep "POST" | cut -d " " -f 7 | sort | uniq -c | sort -nr
     34 /wp-login.php?itsec-hb-token=adminlogin
      4 /wp-login.php?itsec-hb-token=adminlogin&mglS=2151%2BAND%2B1%3D1%2BUNION%2BALL%2BSELECT%2B1%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%2BFROM%2Binform
ation_schema.tables%2BWHERE%2B2%3E1--%2F%2A%2A%2F%3B%2BEXEC%2Bxp_cmdshell%28%27cat%2B..%2F..%2F..%2Fetc%2Fpasswd%27%29%23
      1 /xmlrpc.php
      1 /wp-login.php?itsec-hb-token=p@y<\"'p@y&mglS=2151%2BAND%2B1%3D1%2BUNION%2BALL%2BSELECT%2B1%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%2BFROM%2Binform
ation_schema.tables%2BWHERE%2B2%3E1--%2F%2A%2A%2F%3B%2BEXEC%2Bxp_cmdshell%28%27cat%2B..%2F..%2F..%2Fetc%2Fpasswd%27%29%23
      1 /wp-login.php?itsec-hb-token=p@y<\"'p@y
      1 /wp-login.php
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$
```

168.22.54.119 - - [14/Jan/2021:06:14:00 +0000] "POST /wp-login.php?itsec-hb-token=adminlogin&mglS=2151%2BAND%2B1%3D1%2BUNION%2BALL%2BSELECT%2B1%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%2BFROM%2Binformation_schema.tables%2BWHERE%2B2%3E1--%2F%2A%2A%2F%3B%2BEXEC%2Bxp_cmdshell%28%27cat%2B..%2F..%2F..%2Fetc%2Fpasswd%27%29%23 HTTP/1.1" 200 2831 "-" "Mozilla/5.0 (X11; U; Linux i686 (x86_64); ru; rv:1.8.0.3) Gecko/20060425 SUSE/1.5.0.3-7 Firefox/1.5.0.3"

The client at 168.22.54.119 is making post request in login page with some string. Decode the string in cyberchef.



```
wp-login.php?itsec-hb-token=adminlogin&mglS=2151%2BAND%2B1%3D1%2BUNION%2BALL%2BSELECT%2B1%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27%2Ctable_name%2BFROM%2Binformation_schema.tables%2BWHERE%2B2%3E1--%2F%2A%2A%2F%3B%2BEXEC%2Bxp_cmdshell%28%27cat%2B..%2F..%2F..%2Fetc%2Fpasswd%27%29%23
```

```
wp-login.php?itsec-hb-token=adminlogin&mglS=2151+AND+1=1+UNION+ALL+SELECT+1,NULL,'<script>alert("XSS")</script>',table_name+FROM+information_schema.tables+WHERE+2>1--/**/;+EXEC+xp_cmdshell('cat+../../../etc/passwd')#
```

Decoded Version:

wp-login.php?itsec-hb-token=adminlogin&mglS=2151 AND 1=1 UNION ALL SELECT 1,NULL,'<script>alert("XSS")</script>',table_name FROM information_schema.tables WHERE 2>1--/**/; EXEC xp_cmdshell('cat ../../../etc/passwd')#

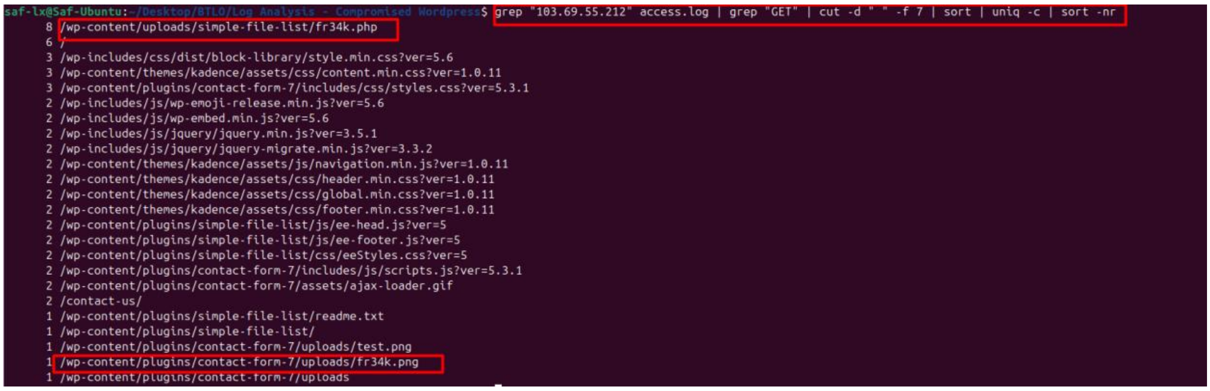
Here, this code is malicious, the attacker:

1. Detect SQL injection vulnerability and exploit it.
2. Extract dabase metadata.
3. Inject javascript. An attacker sends JavaScript code (like <script>alert("XSS")</script>) as part of input to a website.

4. Execute command like cat /etc/password and escalate to RCE or to theft data.
5. Basically, the payload mixes DBMS/OS-specific element to increase chance of success against unknown targets. Multi-vector probing.

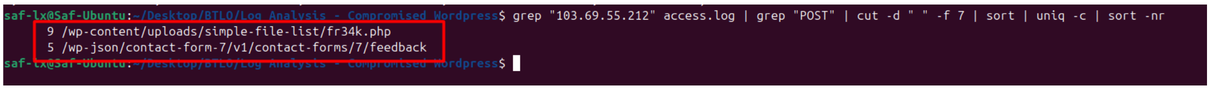
Let’s grep GET and POST with another IP address 103.69.55.212 then,

grep "103.69.55.212" access.log | grep "GET" | cut -d " " -f 7 | sort | uniq -c | sort -nr



```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ grep "103.69.55.212" access.log | grep "GET" | cut -d " " -f 7 | sort | uniq -c | sort -nr
      8 /wp-content/uploads/simple-file-list/fr34k.php
      6 /
      3 /wp-includes/css/dist/block-library/style.min.css?ver=5.6
      3 /wp-content/themes/kadence/assets/css/content.min.css?ver=1.0.11
      3 /wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.3.1
      2 /wp-includes/js/wp-emoji-release.min.js?ver=5.6
      2 /wp-includes/js/wp-embed.min.js?ver=5.6
      2 /wp-includes/js/jquery/jquery.min.js?ver=3.5.1
      2 /wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2
      2 /wp-content/themes/kadence/assets/js/navigation.min.js?ver=1.0.11
      2 /wp-content/themes/kadence/assets/css/header.min.css?ver=1.0.11
      2 /wp-content/themes/kadence/assets/css/global.min.css?ver=1.0.11
      2 /wp-content/themes/kadence/assets/css/footer.min.css?ver=1.0.11
      2 /wp-content/plugins/simple-file-list/js/ee-head.js?ver=5
      2 /wp-content/plugins/simple-file-list/js/ee-footer.js?ver=5
      2 /wp-content/plugins/simple-file-list/css/eeStyles.css?ver=5
      2 /wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.3.1
      2 /wp-content/plugins/contact-form-7/assets/ajax-loader.gif
      2 /contact-us/
      1 /wp-content/plugins/simple-file-list/readme.txt
      1 /wp-content/plugins/simple-file-list/
      1 /wp-content/plugins/contact-form-7/uploads/test.png
      1 /wp-content/plugins/contact-form-7/uploads/fr34k.png
      1 /wp-content/plugins/contact-form-7/uploads
```

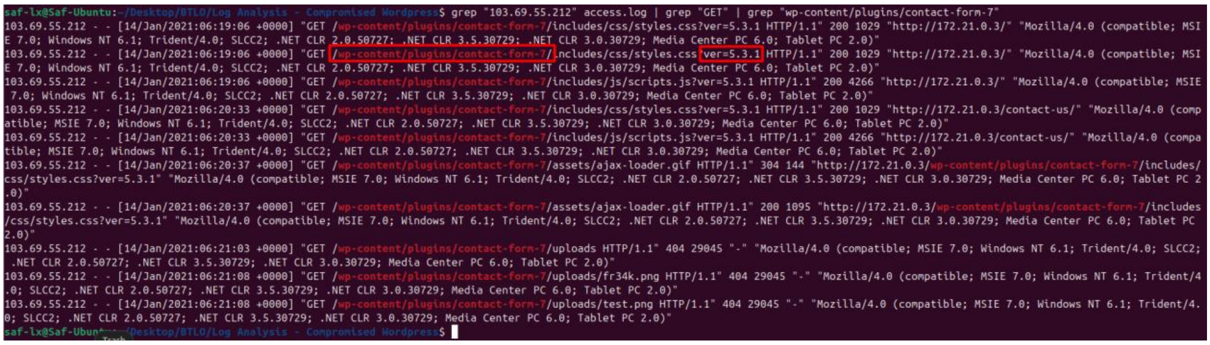
grep "103.69.55.212" access.log | grep "POST" | cut -d " " -f 7 | sort | uniq -c | sort -nr



```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ grep "103.69.55.212" access.log | grep "POST" | cut -d " " -f 7 | sort | uniq -c | sort -nr
      9 /wp-content/uploads/simple-file-list/fr34k.php
      5 /wp-json/contact-form-7/v1/contact-forms/7/feedback
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ 
```

The attacker tried to do post request with this two link and try to upload php web shell file.

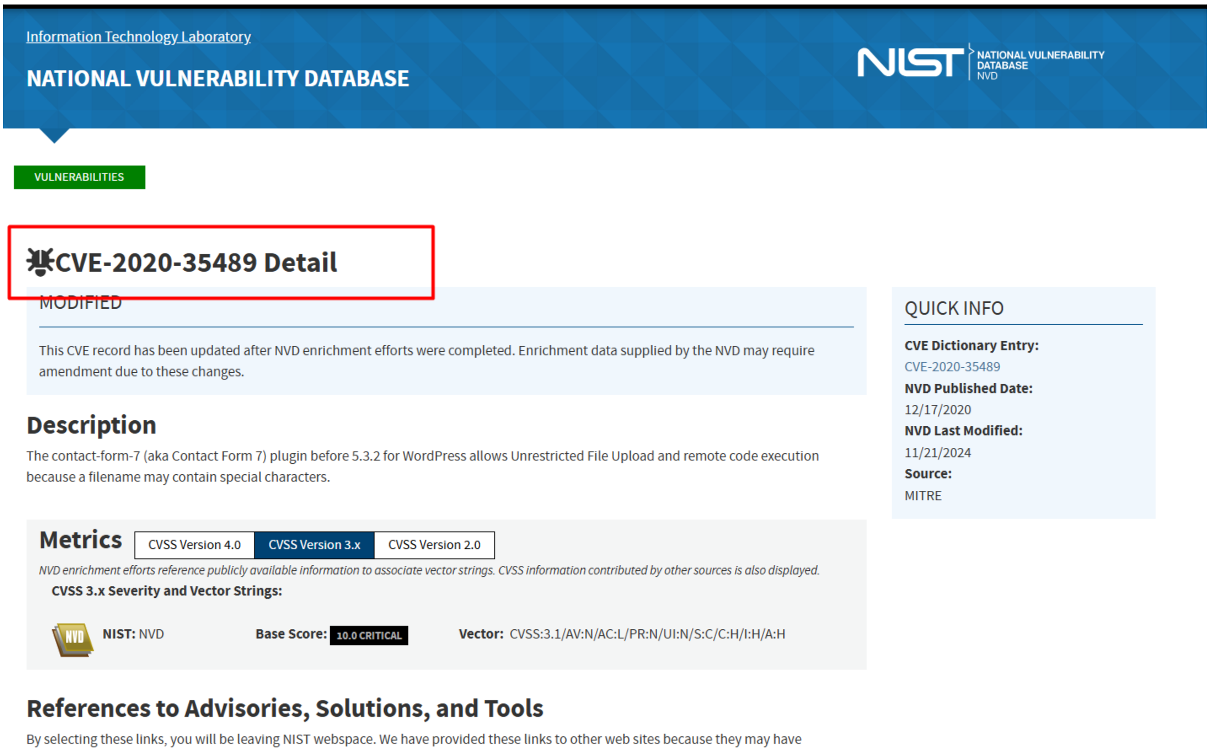
These two looks suspicious.



```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ grep "103.69.55.212" access.log | grep "GET" | grep "wp-content/plugins/contact-form-7"
103.69.55.212 - - [14/Jan/2021:06:19:06 +0000] "GET /wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.3.1 HTTP/1.1" 200 1029 "http://172.21.0.3/" "Mozilla/4.0 (compatible; MSI
E 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/2021:06:19:06 +0000] "GET /wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.3.1 HTTP/1.1" 200 1029 "http://172.21.0.3/" "Mozilla/4.0 (compatible; MSI
E 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/2021:06:19:06 +0000] "GET /wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.3.1 HTTP/1.1" 200 4266 "http://172.21.0.3/" "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/2021:06:20:33 +0000] "GET /wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.3.1 HTTP/1.1" 200 1029 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (comp
atible; 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/2021:06:20:33 +0000] "GET /wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.3.1 HTTP/1.1" 200 4266 "http://172.21.0.3/contact-us/" "Mozilla/4.0 (compa
tible; 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/2021:06:20:37 +0000] "GET /wp-content/plugins/contact-form-7/assets/ajax-loader.gif HTTP/1.1" 304 144 "http://172.21.0.3/wp-content/plugins/contact-form-7/includes/
css/styles.css?ver=5.3.1" "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/2021:06:20:37 +0000] "GET /wp-content/plugins/contact-form-7/assets/ajax-loader.gif HTTP/1.1" 200 1095 "http://172.21.0.3/wp-content/plugins/contact-form-7/includes
/css/styles.css?ver=5.3.1" "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/2021:06:21:03 +0000] "GET /wp-content/plugins/contact-form-7/uploads HTTP/1.1" 404 29045 "-" "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/2021:06:21:08 +0000] "GET /wp-content/plugins/contact-form-7/uploads/fr34k.png HTTP/1.1" 404 29045 "-" "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/2021:06:21:08 +0000] "GET /wp-content/plugins/contact-form-7/uploads/test.png HTTP/1.1" 404 29045 "-" "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)"
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Log Analysis - Compromised Wordpress$ 
```

https://nvd.nist.gov/vuln/detail/cve-2020-35489

The contact-form-7 (aka Contact Form 7) plugin before 5.3.2 for WordPress allows Unrestricted File Upload and remote code execution because a filename may contain special characters. -> Vulnerability details.



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

CVE-2020-35489 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

The contact-form-7 (aka Contact Form 7) plugin before 5.3.2 for WordPress allows Unrestricted File Upload and remote code execution because a filename may contain special characters.

Metrics

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 10.0 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have

QUICK INFO

CVE Dictionary Entry:
CVE-2020-35489
NVD Published Date:
12/17/2020
NVD Last Modified:
11/21/2024
Source:
MITRE

Analysis

1. Attacker use the vulnerability to exploit wordpress website.
2. Attacker entertain multiple IP address for http GET and POST request. Multiple IP addresses has been used.
3. Attacker uploaded a web shell to get reverse shell to remotely control the web server.