Lab 12

CYL2002 Digital Forensics - Lab

Name : Mirza Humayun Masood(i22-1749)

Section : CY-A

Submitted to: Sir Ubaid Ullah

Department of Cyber Security BS(CY)

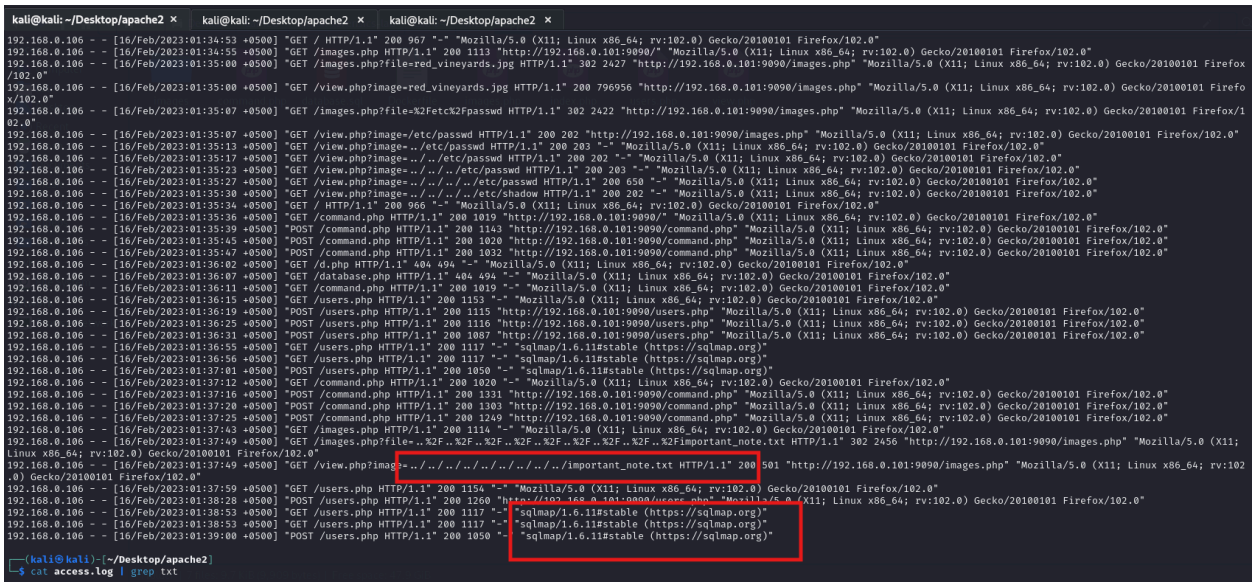
FAST-NUCES Islamabad

What IP address does the attack seem to be originating from?

The ip address of the attacker is 192.168.0.106 as it was given in the access.log file.

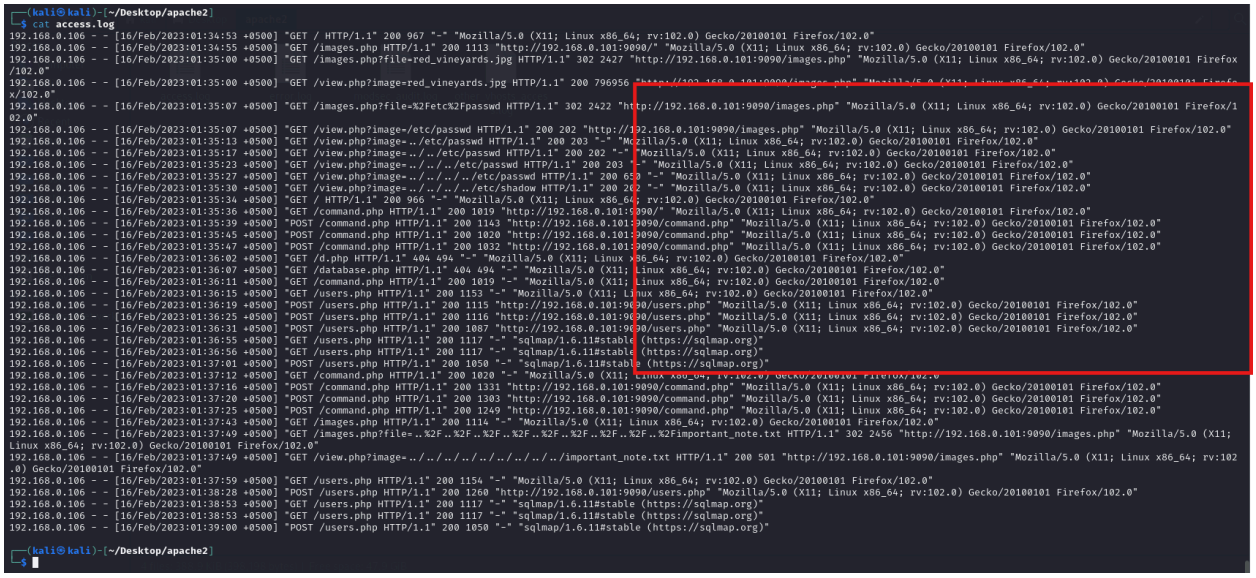
Which vulnerabilities do you think are being exploited, and what evidence do you have to support your findings?

Sql injection and Path Traversal.



How can we determine what web browser the attacker is using?

The attacker was using Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 , as we can see from the access.log file.

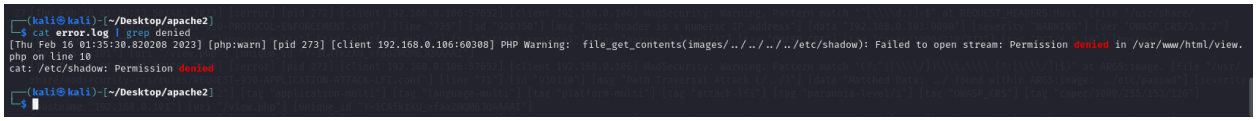


Did the attacker use any automated tools during the attack? If so, can you identify the name of the tool and its purpose?

The attacker used sqlmap for sql injection, and exposed some confidential data.

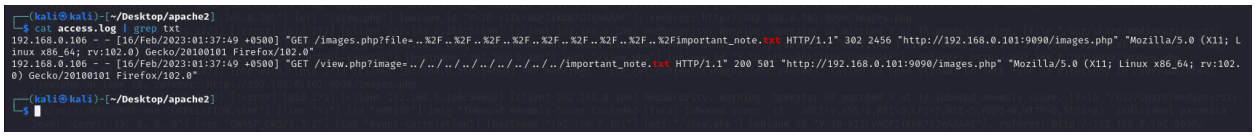
Which file was the attacker trying to access but couldn’t due to limited server access?

The attacker was trying to access the etc/shadows file but could not due to less Access to the server.



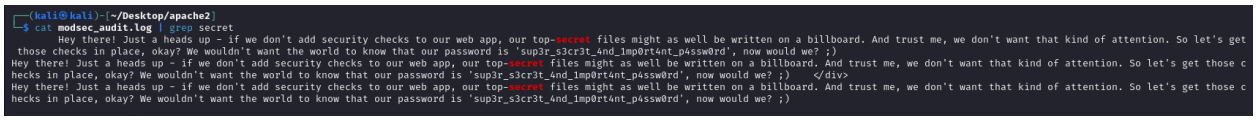
Did the attacker gain access to any confidential data? If yes, how much data was compromised?

Yes he got important.txt and 501 bytes of data was requested.



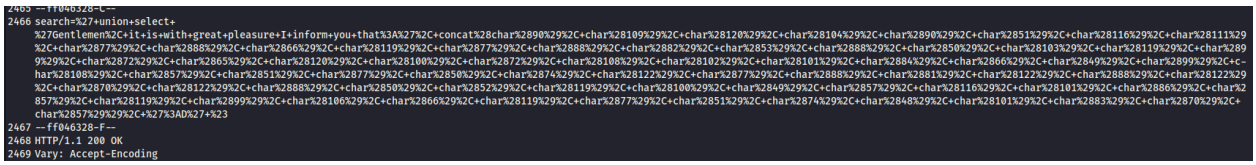
An important secret was compromised. Can you figure it out? Hint: The secret you're looking for is not in a .sql or a .php file.

The password of root was ‘sup3r_s3cr3t_4nd_1mp0rt4nt_p4ssw0rd’



The attacker left a message for the server administrator. Find out what the message said, and also mention how you were able to find it.

First i was going through the modsec_audit.log file, there i saw this sql squery of search and select, i went to cyber chef there it gave me some characters, and i gpt the characters to get the flag the attacker left for server administrator.



Input

```
search=%27+union+select+%27Gentlemen%2C+it+is+with+great+pleasure+I+inform+you+that%3A%27%2C+concat%28char%2890%29%2C+char%28109%29%2C+char%28120%29%2C+char%28104%29%2C+char%2890%29%2C+char%2851%29%2C+char%28116%29%2C+char%28111%29%2C+char%2877%29%2C+char%2888%29%2C+char%2866%29%2C+char%28119%29%2C+char%2877%29%2C+char%2888%29%2C+char%2882%29%2C+char%2853%29%2C+char%2888%29%2C+char%2850%29%2C+char%28103%29%2C+char%28119%29%2C+char%2899%29%2C+char%2872%29%2C+char%2865%29%2C+char%28120%29%2C+char%28100%29%2C+char%2872%29%2C+char%28108%29%2C+char%28102%29%2C+char%28101%29%2C+char%2884%29%2C+char%2866%29%2C+char%2849%29%2C+char%2899%29%2C+char%28108%29%2C+char%2857%29%2C+char%2851%29%2C+char%2877%29%2C+char%2850%29%2C+char%2874%29%2C+char%28122%29%2C+char%2877%29%2C+char%2888%29%2C+char%2881%29%2C+char%28122%29%2C+char%2888%29%2C+char%28122%29%2C+char%2870%29%2C+char%28122%29%2C+char%2888%29%2C+char%2850%29%2C+char%2852%29%2C+char%28119%29%2C+char%28100%29%2C+char%2849%29%2C+char%2857%29%2C+char%28116%29%2C+char%28101%29%2C+char%2886%29%2C+char%2857%29%2C+char%28119%29%2C+char%2899%29%2C+char%28106%29%2C+char%2866%29%2C+char%28119%29%2C+char%2877%29%2C+char%2851%29%2C+char%2874%29%2C+char%2848%29%2C+char%28101%29%2C+char%2883%29%2C+char%2870%29%2C+char%2857%29%29%2C+%27%3AD%27+%23
```

ABC 1297 1 Raw Bytes LF

Output

```
search=' union select 'Gentlemen, it is with great pleasure I inform you that:', concat(char(90), char(109), char(120), char(104), char(90), char(51), char(116), char(111), char(77), char(88), char(66), char(119), char(77), char(88), char(82), char(53), char(88), char(50), char(103), char(119), char(99), char(72), char(65), char(120), char(100), char(72), char(108), char(102), char(101), char(84), char(66), char(49), char(99), char(108), char(57), char(51), char(77), char(50), char(74), char(122), char(77), char(88), char(81), char(122), char(88), char(122), char(70), char(122), char(88), char(50), char(52), char(119), char(100), char(49), char(57), char(116), char(101), char(86), char(57), char(119), char(99), char(106), char(66), char(119), char(77), char(51), char(74), char(48), char(101), char(83), char(70), char(57)), ':D' #
```

ABC 841 1 1ms Raw Bytes LF

Earlier, we decoded this sequence, which resulted in the secret message:

`flag{h1pp1ty_h0pp1ty_y0ur_w3bs1t3_1s_n0w_my_pr0p3rty!}`

So, this payload would return:

> **"Gentlemen, it is with great pleasure I inform you that:**
> **flag{h1pp1ty_h0pp1ty_y0ur_w3bs1t3_1s_n0w_my_pr0p3rty!}**
> **"**

This type of payload is commonly used to test for SQL injection vulnerabilities by embedding a message or flag if successful.

Gentlemen, it is with great pleasure I inform you that:
flag{h1pp1ty_h0pp1ty_y0ur_w3bs1t3_1s_n0w_my_pr0p3rty!}
:D

What were some indicators that confirmed that an attack had taken place? What were your key takeaways from this attack?

The etc/passwd file and important.txt file were extracted, Sql injection was done to see the passwords of the users and The attacker left the flag for the server administrator as well. To mitigate it there should be more critical checks, and there should be mitigations against sql injection.

Based on this attack, what indicators of compromise can be used to detect future attacks?

We can detect Sql injection, and path traversal, also the key words like etc, passwd,shadow , so by that we can monitor logs, and can tell if an attack has been performed or not.