

BLM4011

Security of Computer Systems

Project

COURSE NAME: Security of Computer Systems

COURSE GROUP: 3

INSTRUCTOR NAME: Prof. Dr. Hasan Hüseyin BALIK

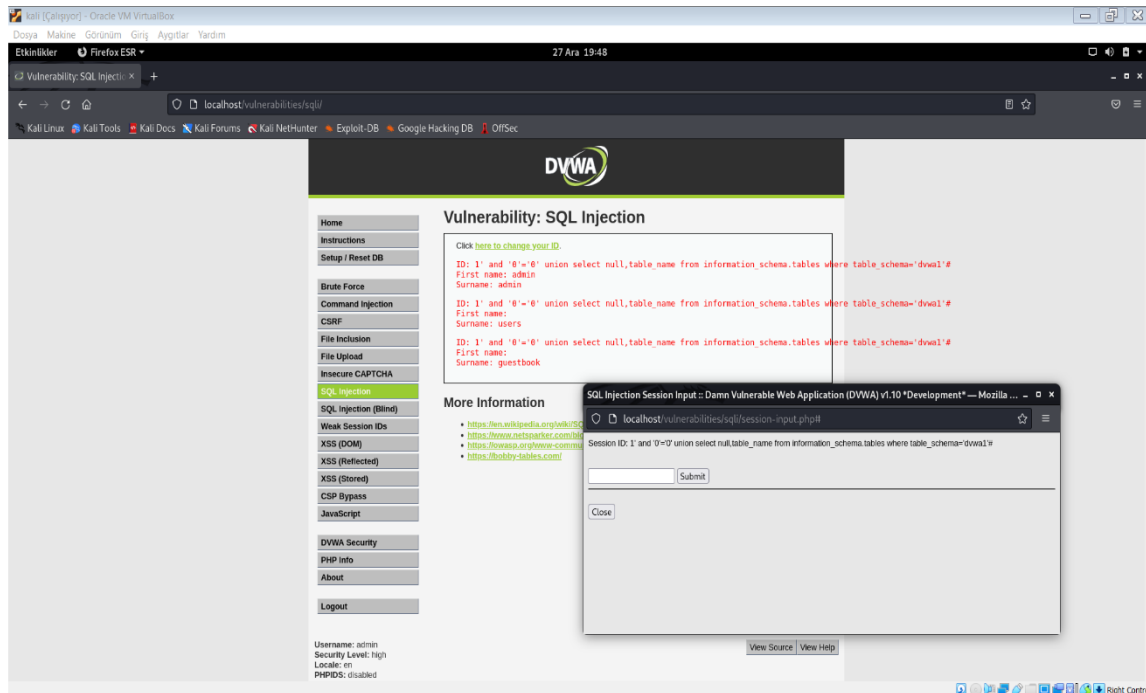
STUDENT ID: 16011038

STUDENT NAME AND SURNAME: TALHA BACAK

SUBJECT: SQL Injection & Password cracking

1 SQL Injection

With the '1'' sign, 1 was given to the SQL parameter, then we are able to write SQL. Afterwards, I wrote a SQL code that learns the names of the tables in the database with the command I wrote. By typing '#' at the end, I have made comment line the rest of the operations. When I submitted it, it returned the information I wanted and showed it.



2 Password Cracking

I wrote the given hash to dosya.txt. Since it is understood that the hash type is md5, I wrote format=md5* to find it faster. I have added the rockyou.txt that will help us decrypt it to wordlist. Password is '?:jolly.'.

```
kali@kali: ~/Downloads
(kali@kali)~[~/Downloads]
$ sudo cat dosya.txt
[sudo] password for kali:
$1$hCuyQvFA$JHo/oX9fIm6RDhp8N9hJg1

(kali@kali)~[~/Downloads]
$ sudo john --format=md5* dosya.txt --wordlist rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Warning: invalid UTF-8 seen reading rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)

(kali@kali)~[~/Downloads]
$ sudo john --show --format=md5crypt dosya.txt
?:jolly.

1 password hash cracked, 0 left

(kali@kali)~[~/Downloads]
$
```