Password cracking

ALIN ZAMFIROIU

What is Password cracking

- The process of attempting to gain unauthorized access to a system by using common passwords or algorithms that guess the password;

Password cracking is an ART

- The art of obtaining the correct password that gives access to a system protected by an authentication method

Techniques

- The most commonly techniques of password cracking are:
  - Dictionary attack
  - Brute force attack
  - Rainbow table attack
  - Guess
  - Spidering

Tools and instruments

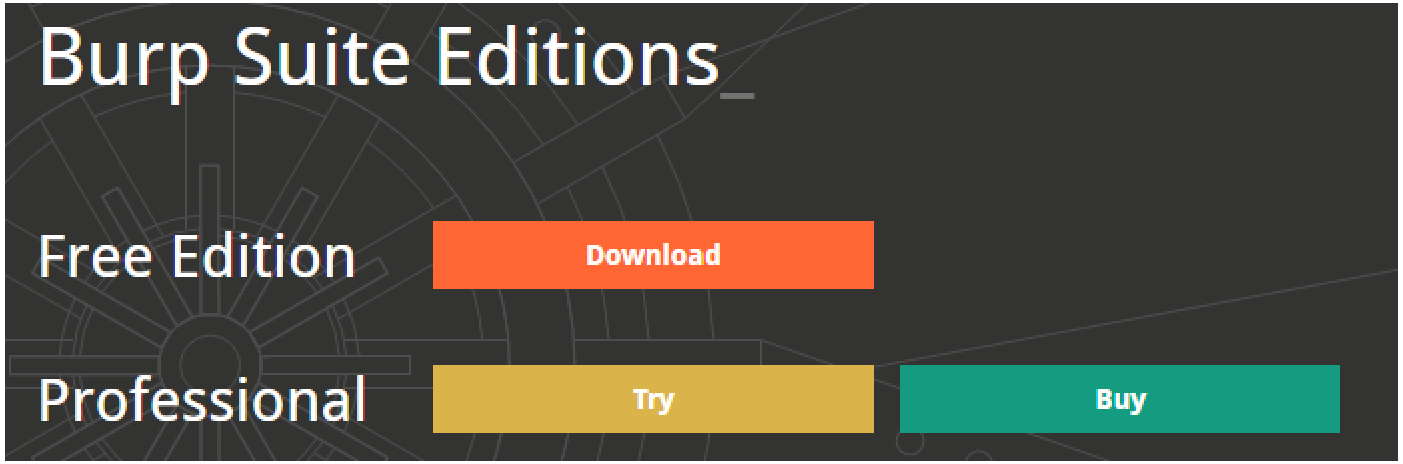
- The most used software tools to crack user passwords are:
  - **Brutus**
  - **Cain and abel**
  - **RainbowCrack**
  - **John the Ripper**
  - **Wfuzz**
  - **AirCrack NG**
  - **THC Hydra**
  - **Medusa**
  - **Burp Suite**

Real scenarios

- **Burp Suite + Firefox**

Burp Suite

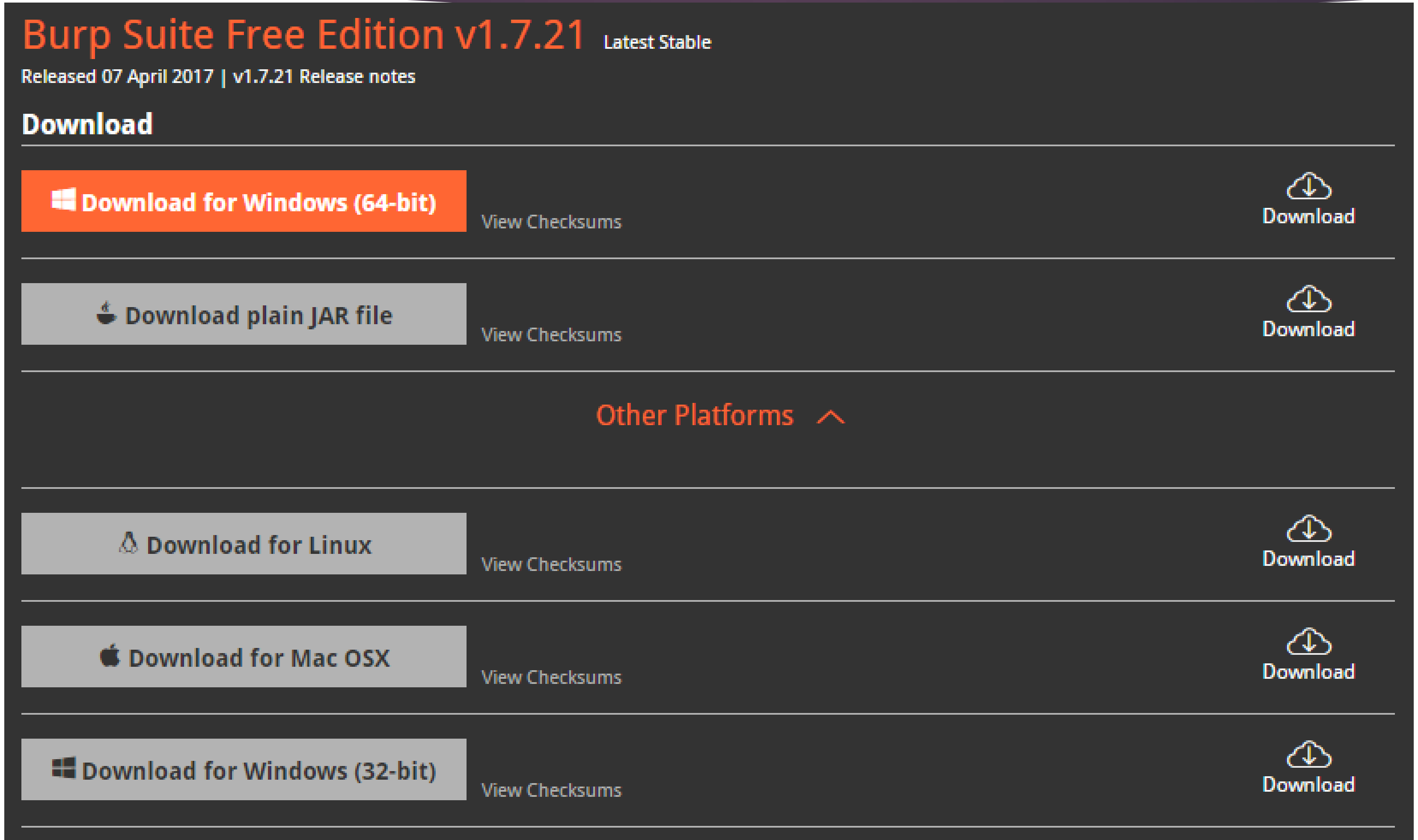
- Download the BurpSuite


Burp Suite Editions_

Free Edition

Professional

Burp Suite



Burp Suite Free Edition v1.7.21 Latest Stable

Released 07 April 2017 | v1.7.21 Release notes

Download

Download for Windows (64-bit) View Checksums Download

Download plain JAR file View Checksums Download

Other Platforms

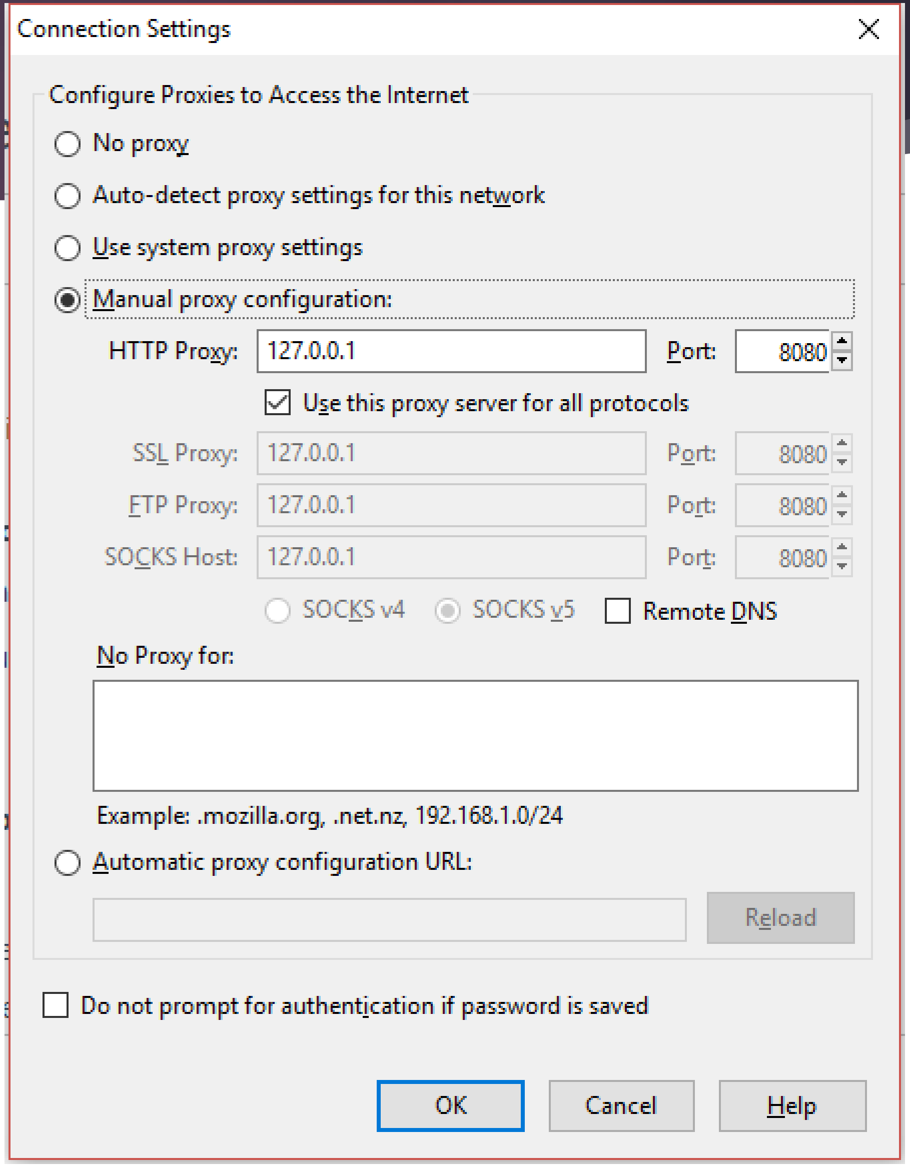
Download for Linux View Checksums Download

Download for Mac OSX View Checksums Download

Download for Windows (32-bit) View Checksums Download

Burp Suite

- Open Firefox and set the proxy to **127.0.0.1** and port: **8080**.



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 □ Remote DNS

No Proxy for:

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

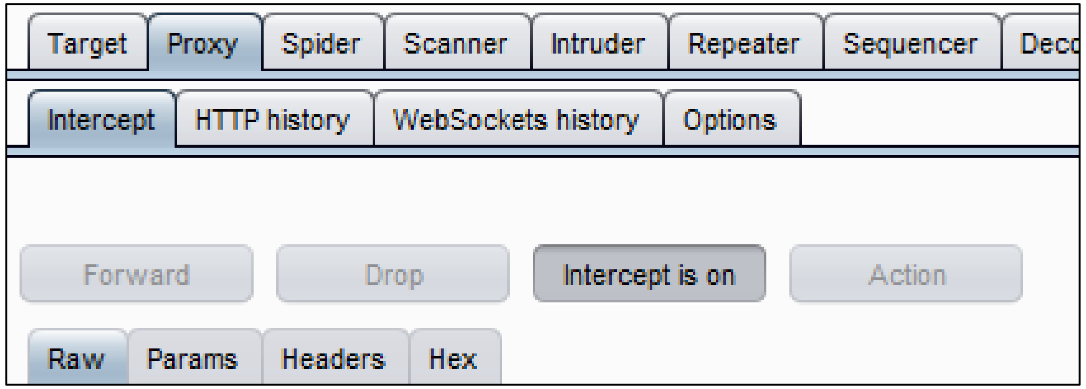
○ Automatic proxy configuration URL:

□ Do not prompt for authentication if password is saved

Burp Suite

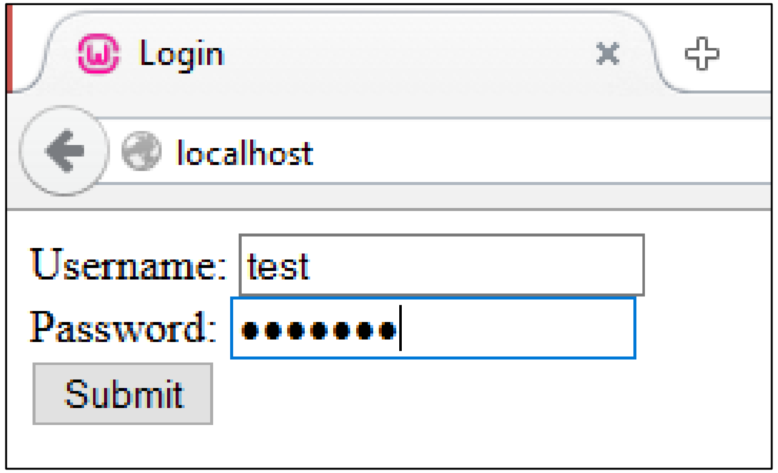
- In Proxy Tab we have the **Intercept is on** button.

- That means that our Burp will intercept our requests from the proxy.



Burp Suite

- Now we have to request the web site with a test user a test password.



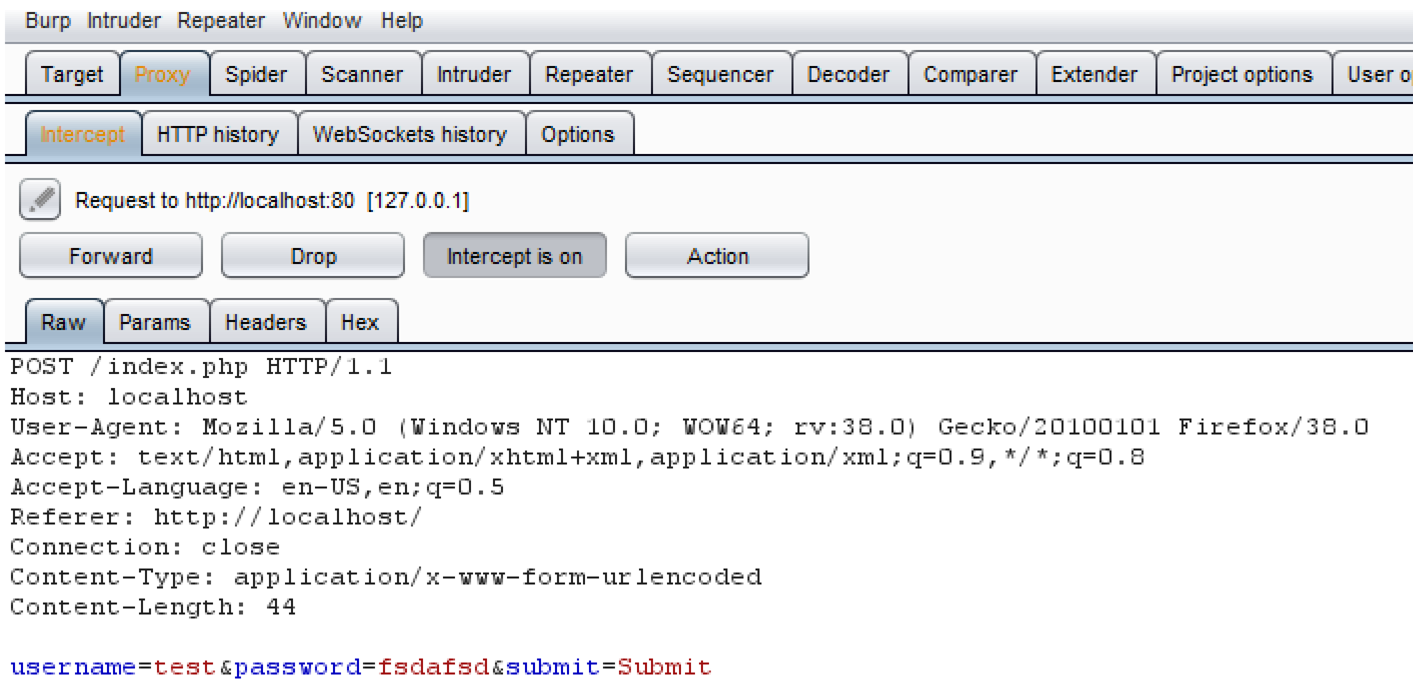
Username: test

Password: ●●●●●●●

Burp Suite

- Burp will intercept our request to the web site.

- In this request we have our parameters: username and password.



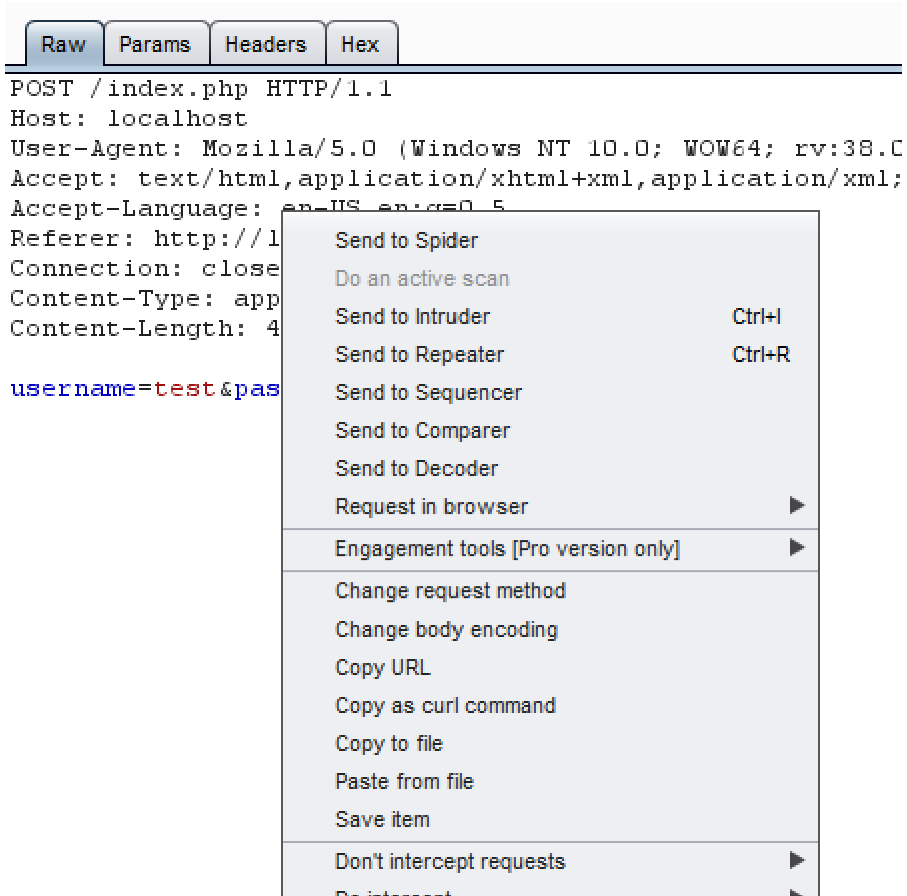
Request to http://localhost:80 [127.0.0.1]

```
POST /index.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost/
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

username=test&password=fsdafsd&submit=Submit
```

Burp Suite

- This request we will **Send to Intruder** (CTRL + I)

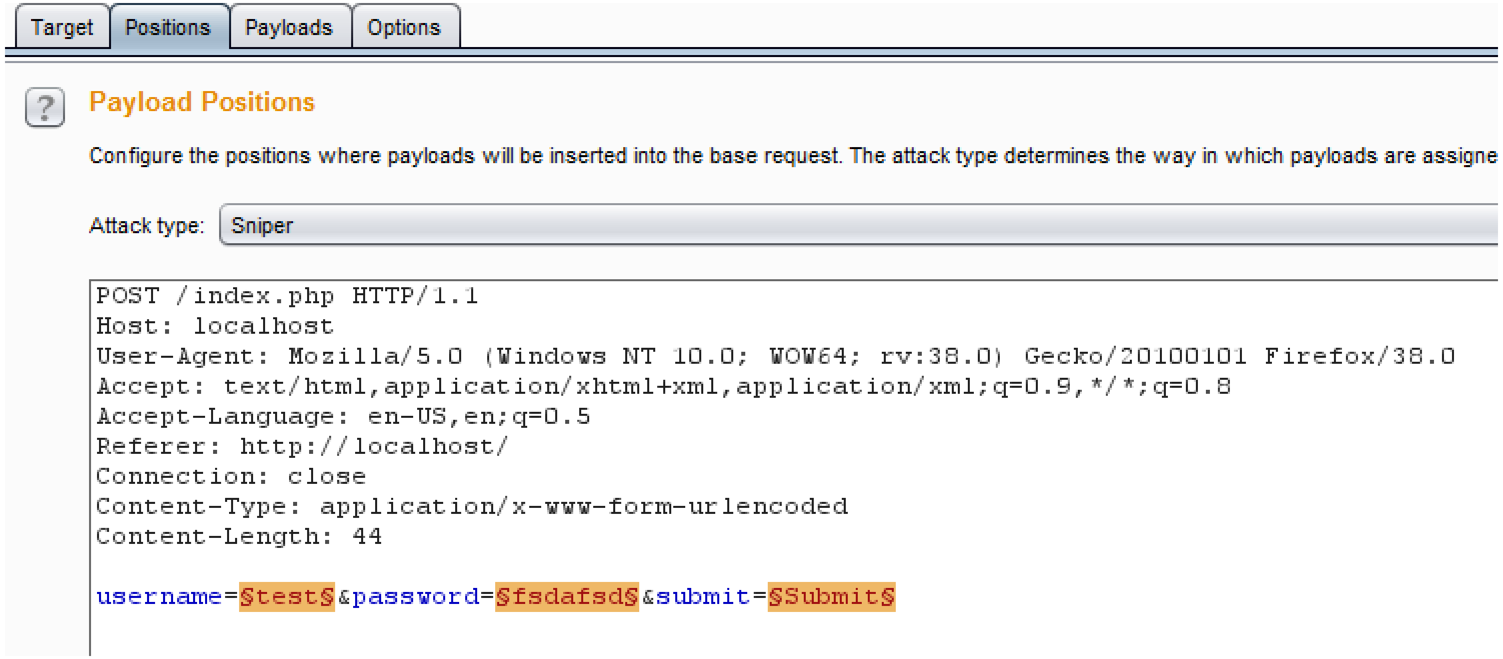


```
POST /index.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:38.C
Accept: text/html,application/xhtml+xml,application/xml;
Accept-Language: en-US,en;q=0.5
Referer: http://l
Connection: close
Content-Type: app
Content-Length: 4

username=test&pas
```

Burp Suite

- In Intruder tab, we have four tabs: **Target**, **Positions**, **Payloads** and **Options.**
- In Target tab we have only or target and the port.
- In the Positions tab we have to set our modified positions (in our case only the **username** and the **password**)



Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigne

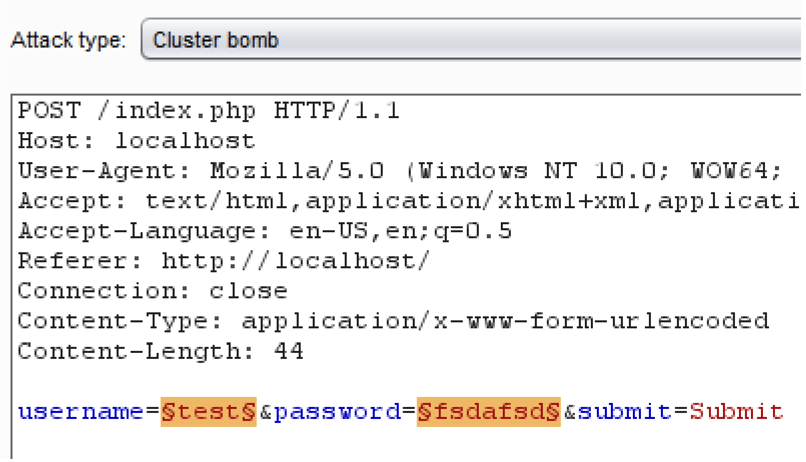
Attack type: Sniper

```
POST /index.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost/
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

username=§test§&password=§fsdafsd§&submit=§Submit§
```

Burp Suite

- Also, in the Position tab we have to select the attack type:
  - Snipper
  - Battering ram
  - Pitch fork
  - Cluster bomb



Attack type: Cluster bomb

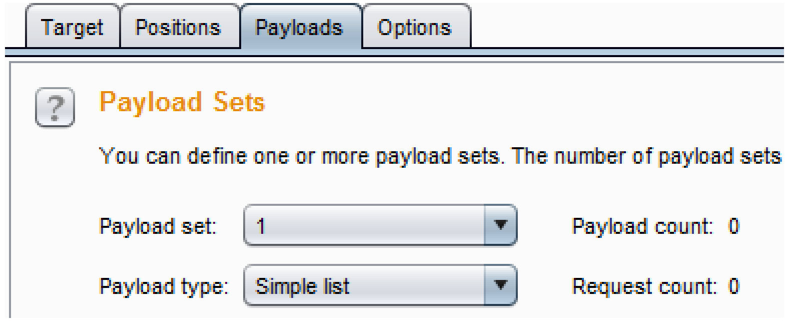
```
POST /index.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
Accept: text/html,application/xhtml+xml,applicati
Accept-Language: en-US,en;q=0.5
Referer: http://localhost/
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

username=§test§&password=§fsdafsd§&submit=Submit
```

Burp Suite

- In Payloads tab we have to set our payload lists, for two positions: username and password.

- We choose the set and the type of the payload:
  - Simple list
  - Runtime file
  - Custom iterator
  - Character substitution
  - Case modification
  - Recursive grep
  - Illegal Unicode
  - Character blocks
  - Numbers
  - Dates
  - Brute Forcer
  - Null payloads
  - Character frobber
  - Bit flipper
  - Username generator
  - ECB block shuffler
  - Extention-generated



Payload Sets

You can define one or more payload sets. The number of payload sets

Payload set: 1

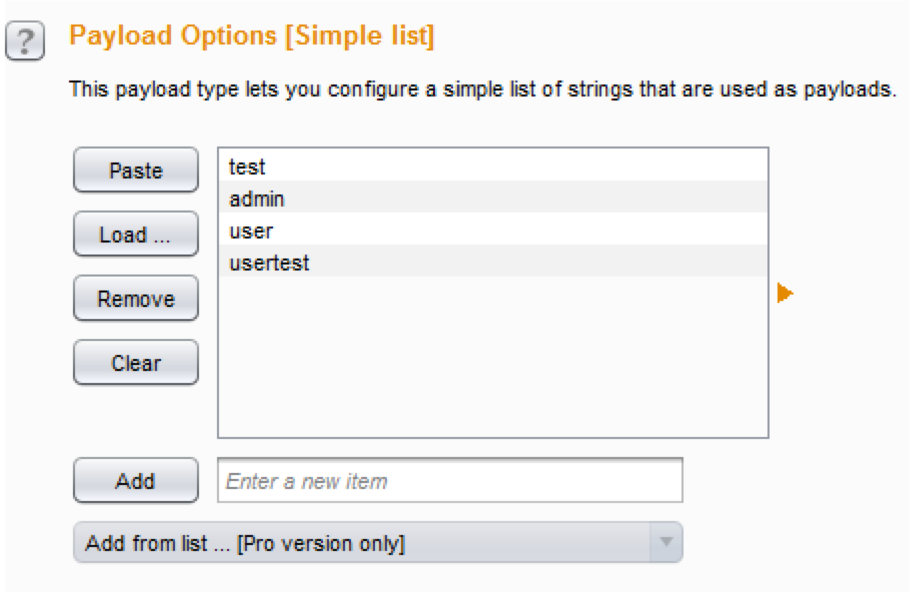
Payload count: 0

Payload type: Simple list

Request count: 0

Burp Suite

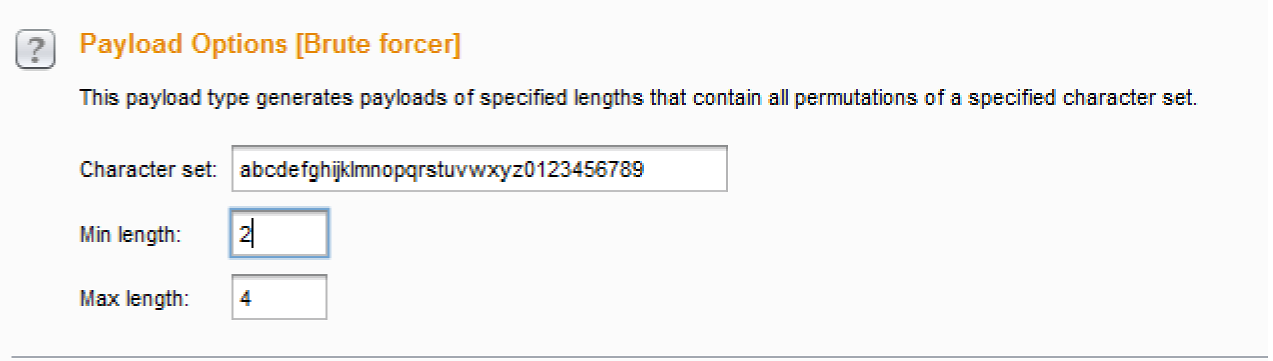
- For **Simple list**, we have to create a list with usernames and a list with passwords.
- For Brute forcer, we have to take the set of characters to create passwords and the possible length



Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

test
admin
user
usertest



Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

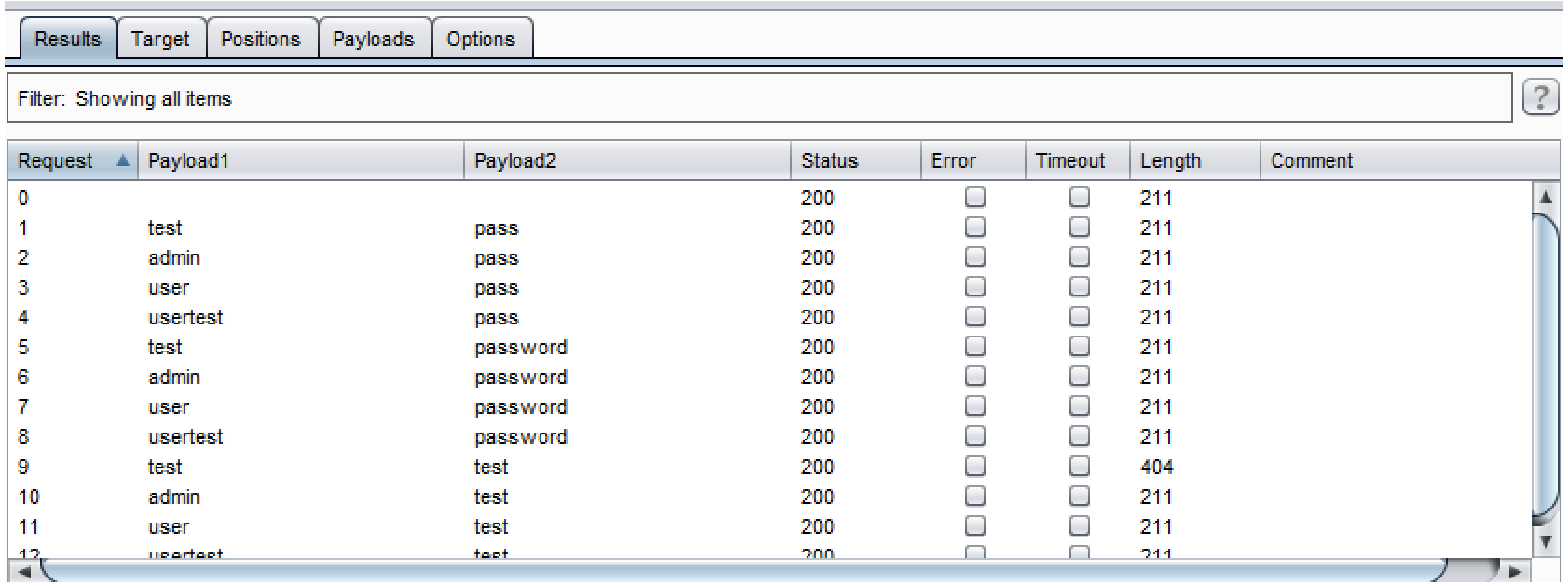
Character set: abcdefghijklmnopqrstuvwxyz0123456789

Min length: 2

Max length: 4

Burp Suite

- The result presents the length of the HTTP response.
- The correct pair is that with the different length.
- In our case: **test** with **test**.



Filter: Showing all items

Request ▲	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200	☐	☐	211	
1	test	pass	200	☐	☐	211	
2	admin	pass	200	☐	☐	211	
3	user	pass	200	☐	☐	211	
4	usertest	pass	200	☐	☐	211	
5	test	password	200	☐	☐	211	
6	admin	password	200	☐	☐	211	
7	user	password	200	☐	☐	211	
8	usertest	password	200	☐	☐	211	
9	test	test	200	☐	☐	404	
10	admin	test	200	☐	☐	211	
11	user	test	200	☐	☐	211	
12	usertest	test	200	☐	☐	211	

Password strength

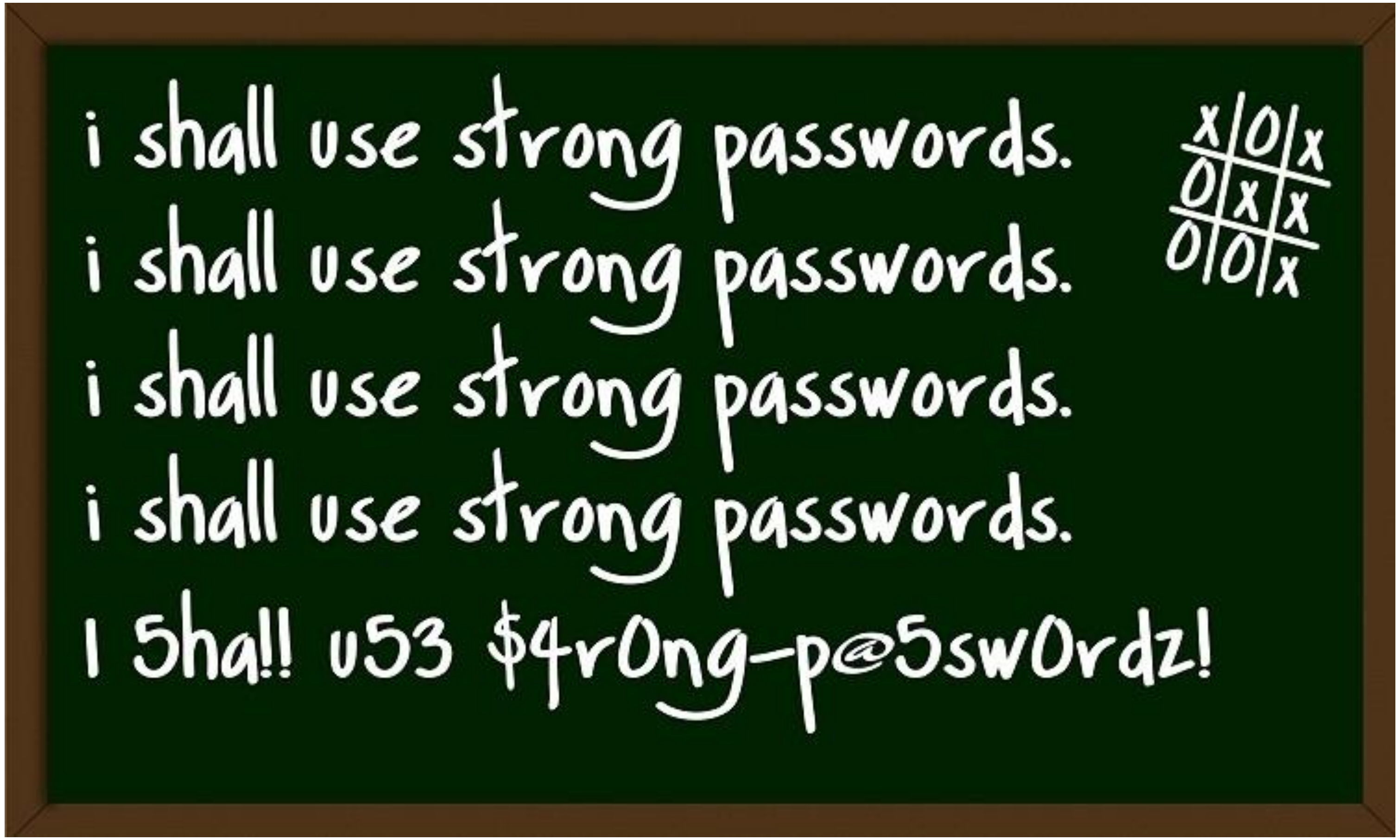
- To resist to a password cracking attack, the password should be strength. The strength of a password is determined by:
  - Length
  - Complexity
  - Unpredictability

Password strength - length

Password strength - complexity

"I just hacked a billion passwords by guessing 1-2-3-4-5."

Password strength - unpredictability



i shall use strong passwords.

i shall use strong passwords.

i shall use strong passwords.

i shall use strong passwords.

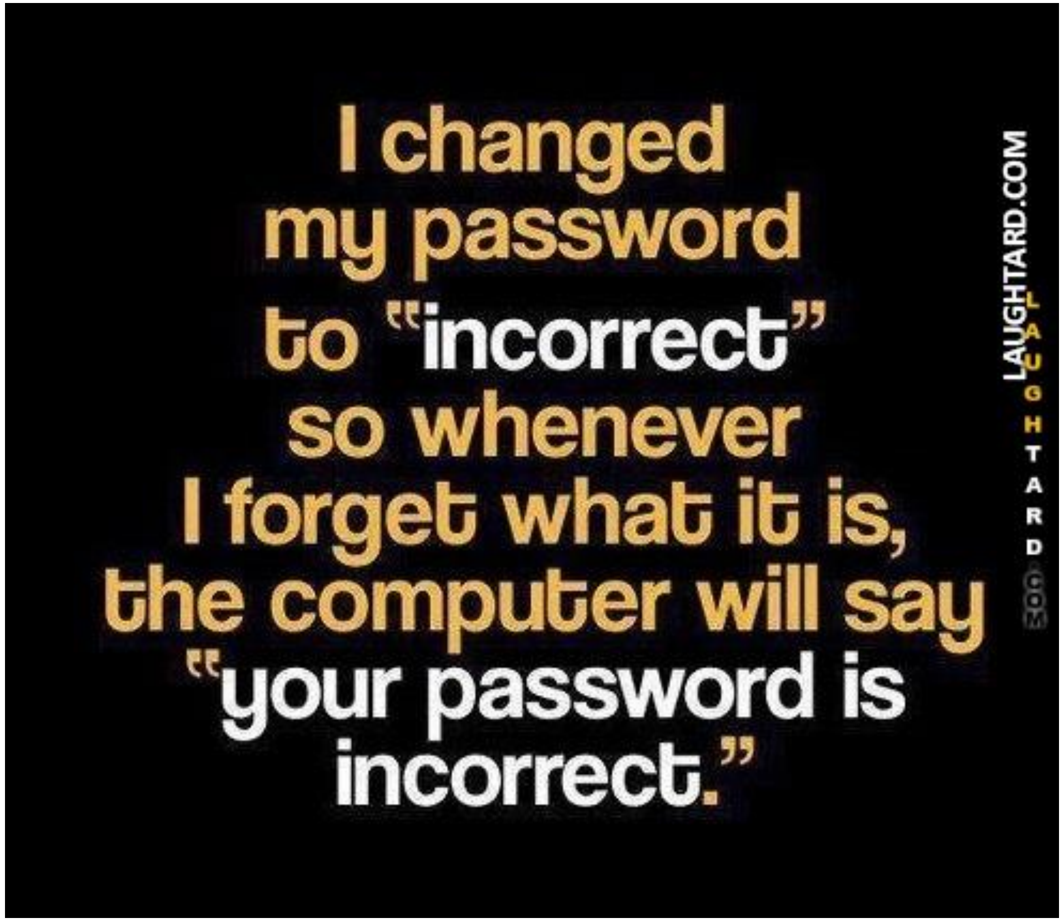
I 5ha!! u53 $4r0ng-p@5sw0rdz!

X	O	X
O	X	X
O	O	X

Recommendations

- Avoid short and easily passwords;
- Avoid using passwords with predicable patterns;
- Stored passwords should be encrypted;
- Using the strength indicators of the registration systems.

Recommendations



I changed my password to "incorrect" so whenever I forget what it is, the computer will say "your password is incorrect."

References

- Chrysanthou Yiannis, Allan Tomlinson , Modern Password Cracking: A hands-on approach to creating an optimised and versatile attack, Technical Report, 2013, Information Security Group, Royal Holloway, University of London .

- Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, The design and analysis of graphical passwords, Proceedings of the 8th USENIX Security Symposium.

- https://portswigger.net/burp/
- https://www.techworm.net/2016/08/top-10-popular-password-cracking-tools.html
- https://www.privacyrights.org/blog/10-rules-creating-hacker-resistant-password

Password cracking