

Структура научной презентации

Простейший шаблон

Карпачев Я. О.

Российский университет дружбы народов, Москва, Россия

Информация

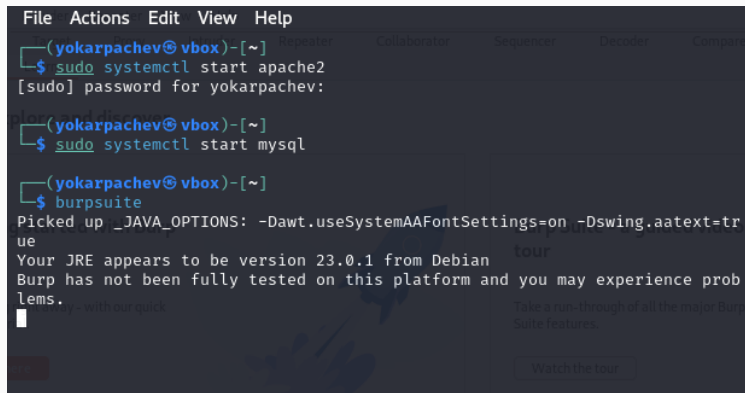
- Карпачев Я. О.
- студент
- Российский университет дружбы народов

Вводная часть

Взломать пароль с помощью Burp Suit

Выполнение лабораторной работы

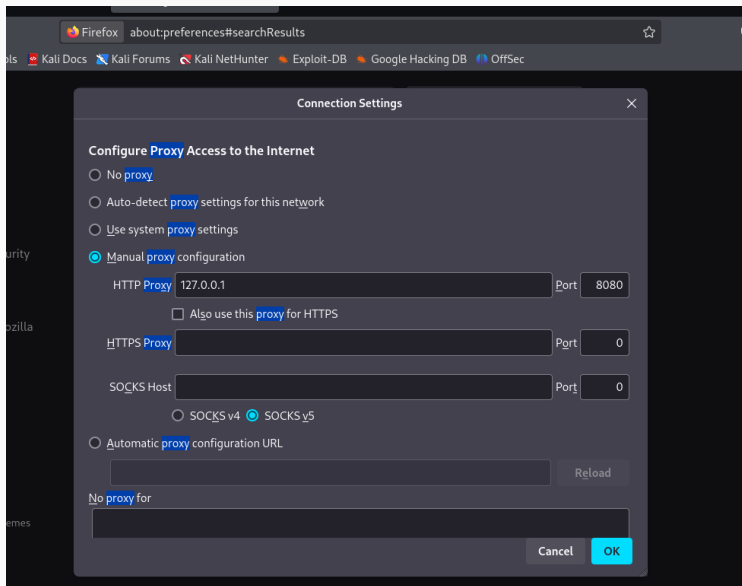
запускаем две команды одна для mysql, другая для apache2, а также сам Burp Suite



```
File Actions Edit View Help
(yokarpachev@vbox)-[~] Repeater Collaborator Sequencer Decoder Compare
$ sudo systemctl start apache2
[sudo] password for yokarpachev:
(yokarpachev@vbox)-[~]
$ sudo systemctl start mysql
(yokarpachev@vbox)-[~]
$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Your JRE appears to be version 23.0.1 from Debian
Burp has not been fully tested on this platform and you may experience problems.
[button: Watch the tour]
```

Рис. 1: Запуск команд

настраиваем окружение



перехватываем нужный запрос



```
1 POST /DWA/login.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 82
9 Origin: http://localhost
10 Connection: keep-alive
11 Referer: http://localhost/DWA/login.php
12 Cookie: security-impossible; PHPSESSID=7466dcbf35cafd9be537c6696141af3
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 username=aaa&password=aaaa&Login=Login&user_token=e8c970937e639fd22556fab1710b9de8
```

Рис. 5: запрос с неверными данными

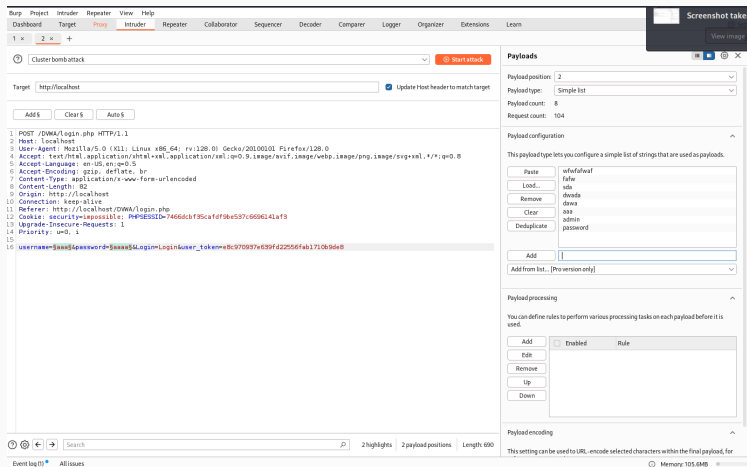


Рис. 6: готовим атаку

запускаем атаку

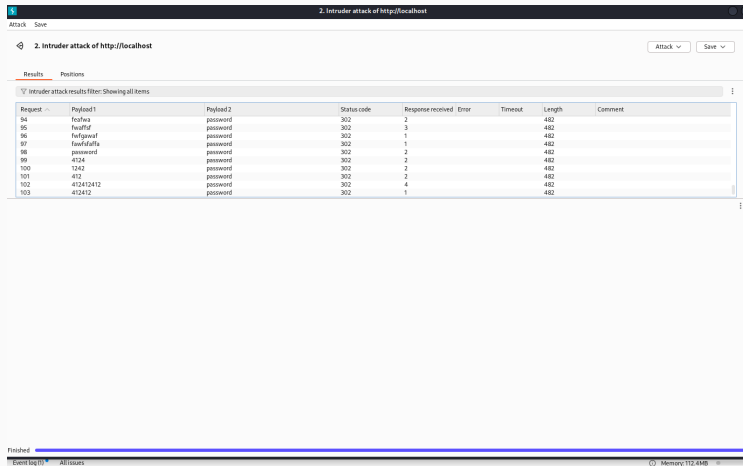


Рис. 7: пройденная атаку

находим запрос который отличается

```
1 HTTP/1.1 302 Found
2 Date: Mon, 21 Apr 2025 11:12:08 GMT
3 Server: Apache/2.4.62 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: PHPSESSID=dadea8b51365bb83d0f9d6578277f7e2; expires=Tue, 22 Apr 2025 11:12:08 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
8 Location: login.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13
14
```

Рис. 8: отличный запрос

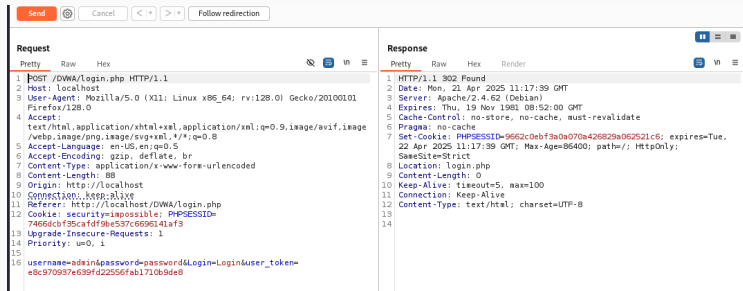


Рис. 9: ретрансляция верного пароля

я научился использовать burp suit для взлома паролей