

Презентация по этапу №5

Основы информационной безопасности

Мишина Анастасия Алексеевна

9 мая 2024

- Мишина Анастасия Алексеевна
- НПИбд-02-22

- Научиться использовать Burp Suite для демонстрации реальных возможностей злоумышленников.

Выполнение работы

Burp Suite

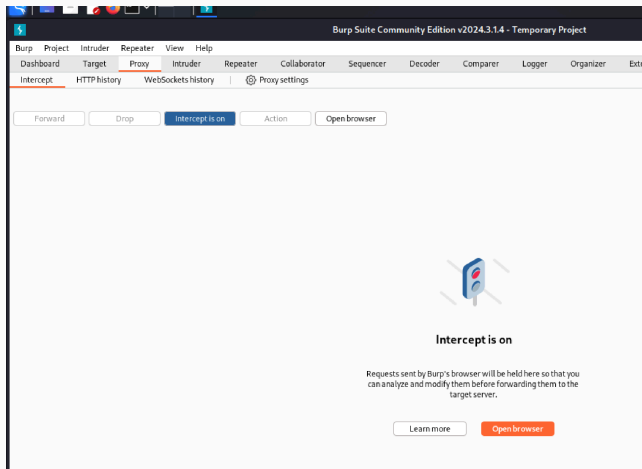


Рис. 1: Включение перехвата в прокси

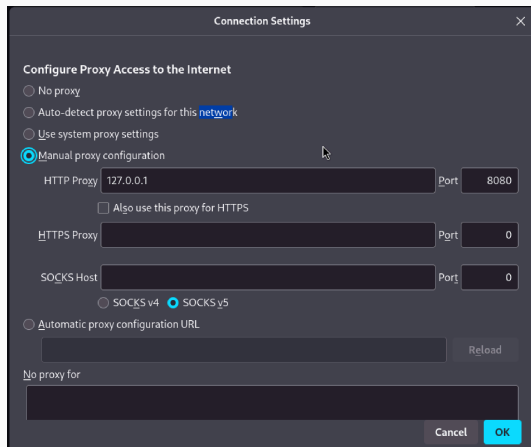


Рис. 2: Настройка прокси-сервера

Полученные данные

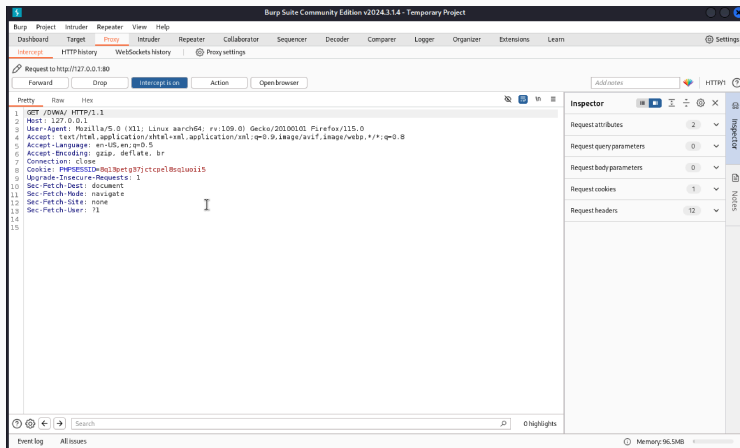


Рис. 3: Перехват данных веб-приложения

Ввод логина и пароля

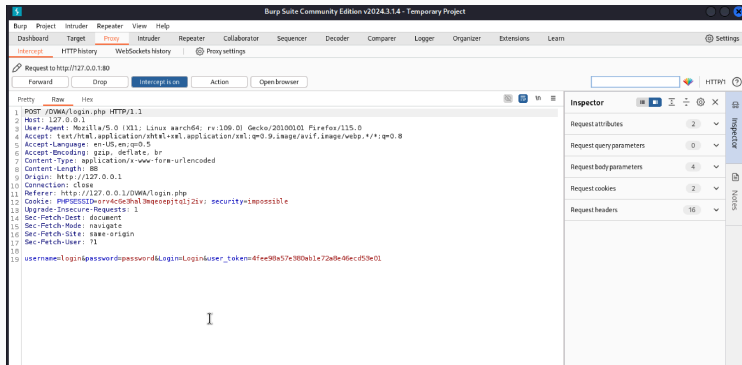


Рис. 4: Запрос для входа в веб-приложение

Попытка входа

The screenshot displays the Burp Suite Community Edition v2024.3.14 interface. The top menu bar includes options like Project, Intruder, Repeater, View, Help, and a tabbed interface with Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The 'Proxy' tab is active, showing 'Intercept' and 'HTTP history' sub-tabs. The 'HTTP history' tab is selected, displaying a table of intercepted requests.

Method	URL	Params	Edited	Status code	Length	BMF type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
POST	/DWWA/login.php		✓	200	1672	HTML	php	Login: Damn Vulnera...			127.0.0.1		22:28:19.8...	8080	
GET	/DWWA/login.php			200	1672	HTML	php	Login: Damn Vulnera...			127.0.0.1		22:25:25.8...	8080	3
POST	/DWWA/login.php		✓	302	439	HTML	php				127.0.0.1	PHPSESSID=rv4...	22:25:09.8...	8080	3
GET	/DWWA/index.php			200	6394	HTML	php	Welcome: Damn Vul...			127.0.0.1		22:07:40.8...	8080	
POST	/DWWA/login.php		✓	302	439	HTML	php				127.0.0.1	PHPSESSID=im...	22:07:34.8...	8080	4
GET	/DWWA/login.php			200	1683	HTML	php	Login: Damn Vulnera...			127.0.0.1		22:06:40.8...	8080	4
POST	/DWWA/login.php		✓	302	439	HTML	php				127.0.0.1	PHPSESSID=itm...	21:57:46.8...	8080	2
POST	/		✓	200	883	app					188.43.76.83		21:28:41.8...	8080	36
POST	/		✓	200	883	app					188.43.76.83		21:28:39.8...	8080	47
POST	/		✓	200	883	app					188.43.76.83		21:28:32.8...	8080	84
POST	/		✓	200	883	app					188.43.76.83		21:28:32.8...	8080	55
GET	/DWWA/login.php			200	1633	HTML	php	Login: Damn Vulnera...			127.0.0.1		21:02:34.8...	8080	3
GET	/DWWA/setup.php			200	4588	HTML	php	Setup: Damn Vulnera...			127.0.0.1		21:02:28.8...	8080	
POST	/DWWA/setup.php		✓	302	306	HTML	php				127.0.0.1		21:02:26.8...	8080	42
GET	/DWWA/setup.php			200	3987	HTML	php	Setup: Damn Vulnera...			127.0.0.1		21:02:21.8...	8080	1
POST	/DWWA/setup.php		✓	500	295	HTML	php				127.0.0.1		21:01:34.8...	8080	1
GET	/DWWA/setup.php			200	3987	HTML	php	Setup: Damn Vulnera...			127.0.0.1		21:01:26.8...	8080	1
GET	/DWWA/login.php			500	295	HTML	php				127.0.0.1		21:01:09.8...	8080	1
POST	/DWWA/setup.php		✓	500	295	HTML	php				127.0.0.1		20:59:45.8...	8080	7
GET	/DWWA/setup.php			200	3987	HTML	php	Setup: Damn Vulnera...			127.0.0.1		20:58:48.8...	8080	4
GET	/DWWA/login.php			500	295	HTML	php				127.0.0.1		20:58:09.8...	8080	3
GET	/DWWA/login.php			403	410	HTML					127.0.0.1		20:47:48.8...	8080	14

The 'Request' tab is selected, showing the raw HTTP request details for the selected entry (index 19). The request is a POST to /DWWA/login.php with the following details:

- Content-Length: 188
- Origin: http://127.0.0.1
- Connection: close
- Referer: http://127.0.0.1/DWWA/login.php
- Cookie: PHPSESSID=rv4...; security=impossible
- Upgrade-Insecure-Requests: 1
- Sec-Fetch-Dest: document
- Sec-Fetch-Mode: navigate
- Sec-Fetch-Site: same-origin
- Sec-Fetch-User: ?1
- username=login&password=password&Login=Login&user_token=4fee98a57e380b1e72a8e46cc59e01

The 'Inspector' tab is also visible, showing request attributes, body parameters, cookies, and headers. The 'Request body parameters' section shows the login attempt details.

Рис. 5: HTTP history

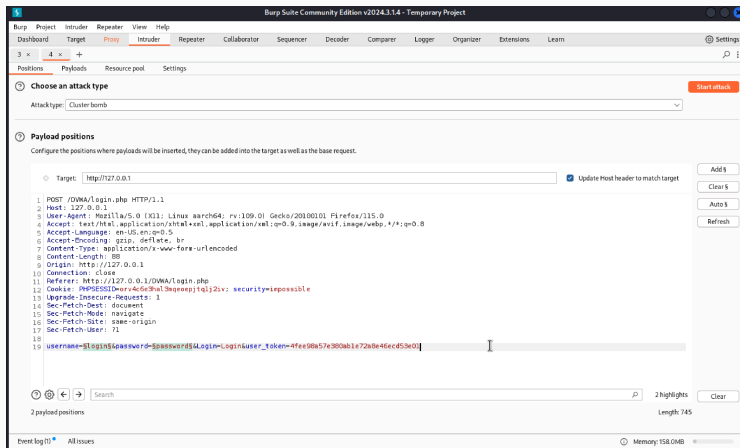


Рис. 6: Выбор позиций в Intruder

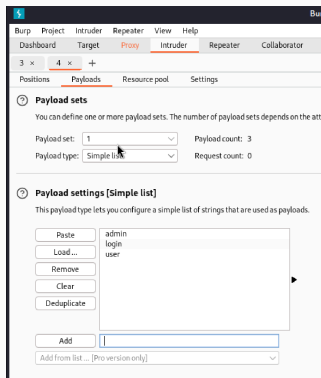


Рис. 7: Заполнение нагрузки username

Возможные пароли

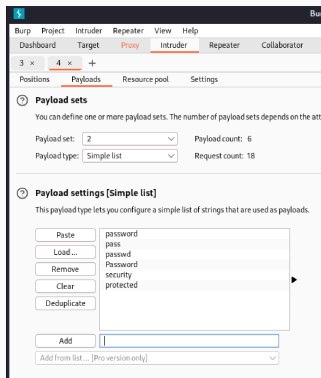


Рис. 8: Заполнение нагрузки password

Результаты атаки

The screenshot shows the Burp Suite interface during an intruder attack. The title bar indicates the target is '6. Intruder attack of http://127.0.0.1'. The main window has tabs for 'Results', 'Positions', 'Payloads', 'Resource pool', and 'Settings'. The 'Results' tab is active, showing a table of intruder attack results. The table has columns: Request, Payload 1, Payload 2, Status code, Response received, Error, Timeout, Length, and Comment. The table contains 10 rows of data, with the first row (index 1) selected. Below the table, there are tabs for 'Request' and 'Response'. The 'Response' tab is active, showing the raw response data in a text area. The response starts with 'HTTP/1.1 302 Found' and includes various headers like 'Date', 'Server', 'Expires', 'Cache-Control', 'Pragma', 'Set-Cookie', 'Location', 'Content-Length', 'Keep-Alive', and 'Content-Type'.

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
0			302	2			476	
1	admin	password	302	2			475	
2	login	password	302	1			476	
3	user	password	302	1			475	
4	admin	pass	302	1			476	
5	login	pass	302	2			475	
6	user	pass	302	2			476	
7	admin	passwd	302	1			475	
8	login	passwd	302	2			476	
9	user	passwd	302	2			475	

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Wed, 08 May 2024 21:30:01 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=ejb32sggd52vs2q1fupagnb98; expires=Thu, 09 May 2024 21:30:01 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
12 Content-Type: text/html; charset=UTF-8
13
14
```

Рис. 9: Результаты атаки

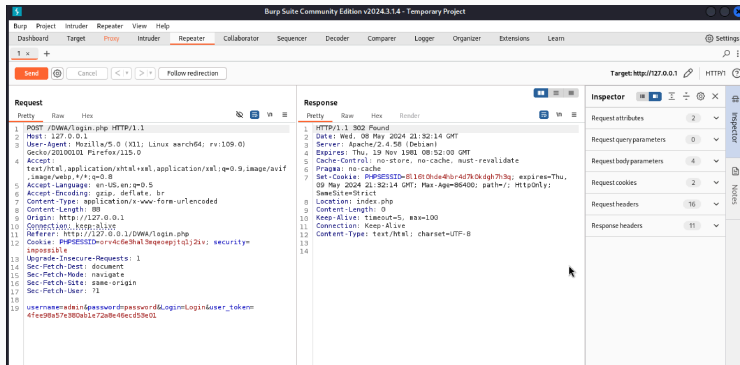


Рис. 10: Использование Repeater

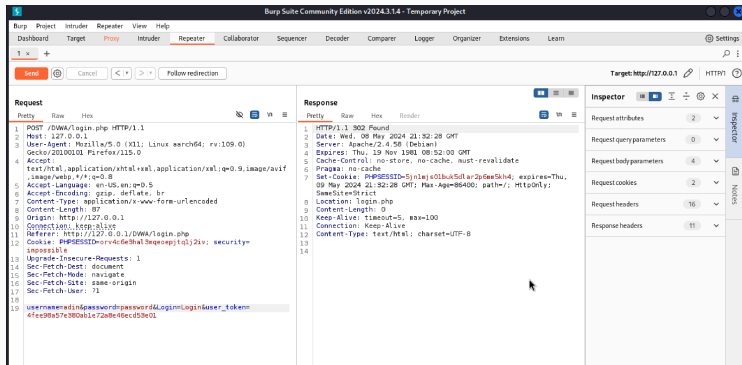


Рис. 11: Использование Repeater

- В ходе выполнения данной работы, я научилась использовать набор инструментов Burp Suite. Данный набор инструментов безопасности приложений является мощной платформой для атаки веб-приложений.