

Индивидуальный проект этап №5

Основы информационной безопасности

Павлюченков С.В.

07 сентября 25

Российский университет дружбы народов, Москва, Россия

- Павлюченков Сергей Витальевич
- Студент ФФМиЕН
- Российский университет дружбы народов
- 1132237372@pfur.ru
- <https://serapshi.github.io/svpavliuchenkov.github.io/>



Использование Burp Suite Burp Suite представляет собой набор мощных инструментов безопасности веб-приложений, которые демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения

Выполнение лабораторной работы

Занык Burp Suite

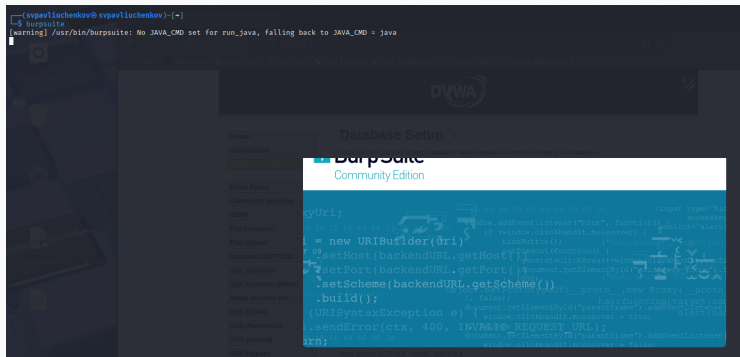
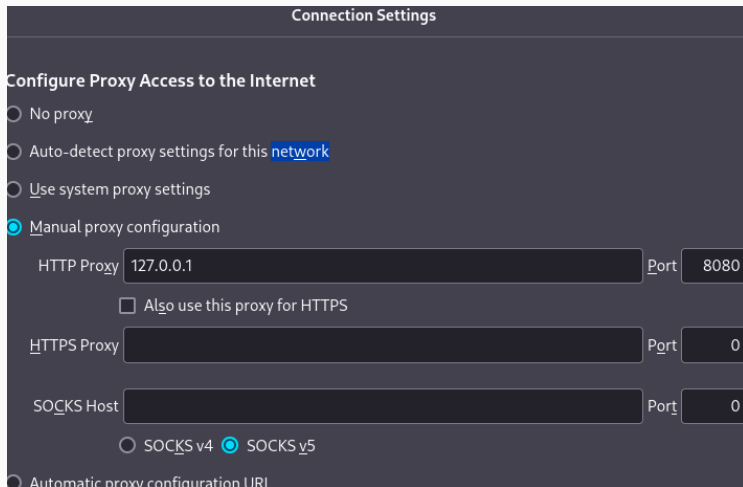


Рис. 1: Запуск через консоль

Конфигурация прокси для работы



The image shows a 'Connection Settings' window with the following configuration:

- Configure Proxy Access to 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
 - ☐ Also use this proxy for HTTPS
- HTTPS Proxy**: (empty), Port: 0
- SOCKS Host**: (empty), Port: 0
 - ☐ SOCKS v4
 - ☒ SOCKS v5
- ☐ Automatic proxy configuration URL

Рис. 2: Конфигурация ip и порта

Включаем перехват запросов

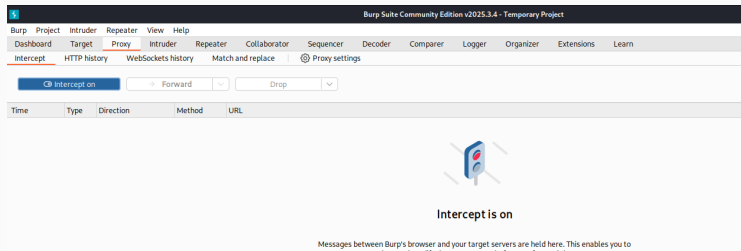


Рис. 3: intercept on

Перехват запроса

Time	Type	Direction	Method	URL
10:13:22.14 S...	HTTP	→ Request	GET	http://127.0.0.1/dvwa/setup.php

Request

PrettyRawHex

1GET /dvwa/setup.php HTTP/1.1

2Host: 127.0.0.1

3User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0

4Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

5Accept-Language: en-US,en;q=0.5

6Accept-Encoding: gzip, deflate, br

7Referer: http://127.0.0.1/dvwa/setup.php

8Connection: keep-alive

9Cookie: security=impossible; PHPSESSID=0a442a2b72d2de9571d219602ce51bfe

10Upgrade-Insecure-Requests: 1

11Sec-Fetch-Dest: document

12Sec-Fetch-Mode: navigate

13Sec-Fetch-Site: same-origin

14Sec-Fetch-User: ?1

15Priority: u=0, i

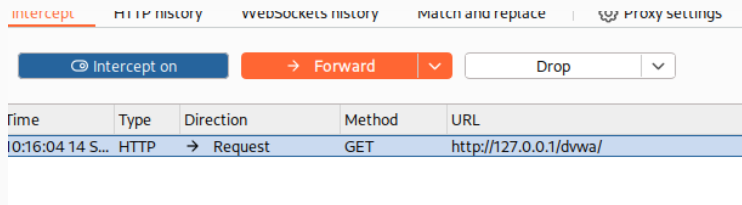


Рис. 5: Кнопка forward

Подробная информации по запросам

The screenshot displays the 'Network' tab of a web browser's developer tools. At the top, a table lists several requests to a host at 127.0.0.1. The first request, 'http://127.0.0.1/dwa/setup.php', is selected. Below the table, the 'Request' and 'Response' panels are visible. The 'Request' panel shows the raw HTTP request, including headers like 'Host: 127.0.0.1', 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0', and 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8'. The 'Response' panel shows the raw HTTP response, including headers like 'HTTP/1.1 200 OK', 'Date: Sun, 14 Sep 2025 14:14:31 GMT', and 'Server: Apache/2.4.63 (Debian)'. The 'Inspector' panel on the right shows the rendered HTML content, which is a document titled 'Setup: Damn Vulnerable W...'. The 'Request attributes' panel on the right shows the request's status as 200.

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
http://127.0.0.1	GET	/dwa/setup.php		200	6729	HTML	Setup: Damn Vulnerable W...		10:14:35 14 Sep.
http://127.0.0.1	GET	/dwa/dwa/js/add_event_li...		200	911	script			10:14:45 14 Sep.
http://127.0.0.1	GET	/dwa/dwa/js/dwaPage.js		200	1560	script			10:14:51 14 Sep.
http://127.0.0.1	GET	/dwa/favicon.ico							
http://127.0.0.1	GET	/dwa/instructions.php							
http://127.0.0.1	GET	/dwa/vulnerabilities/brute/							
http://127.0.0.1	GET	/dwa/vulnerabilities/exec/							
http://127.0.0.1	GET	/dwa/vulnerabilities/csrf/							

Request

Pretty Raw Hex

```
1 GET /dwa/setup.php HTTP/1.1
2 Host: 127.0.0.1
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,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://127.0.0.1/dwa/setup.php
8 Connection: keep-alive
9 Cookie: security=impossible; PHPSESSID=
  0a442a2b72d2de9671d219602ce51bfa
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Priority: u=0, i
16
17
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sun, 14 Sep 2025 14:14:31 GMT
3 Server: Apache/2.4.63 (Debian)
4 Expires: Tue, 23 Jun 2009 12:00:00 GMT
5 Cache-Control: no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 6401
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html; charset=utf-8
12
13 <!DOCTYPE html>
14
15 <html lang="en-GB">
16
17 <head>
18 <meta http-equiv="Content-Type" content="
  text/html; charset=UTF-8" />
19
20 <title>
```

Inspector

Request attributes 2

Request cookies 2

Request headers 14

Response headers 10

Рис. 6: Список запросов

Попытка авторизации

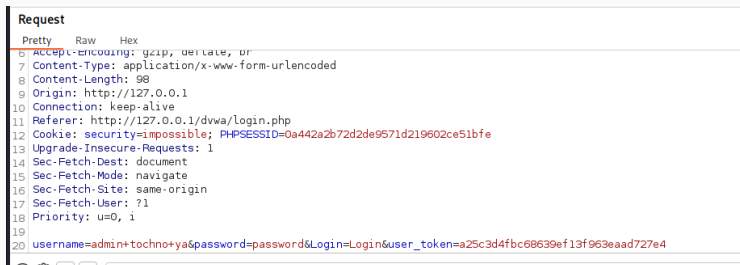


Рис. 7: Запрос авторизации

Передача запроса в секцию злоумышленника

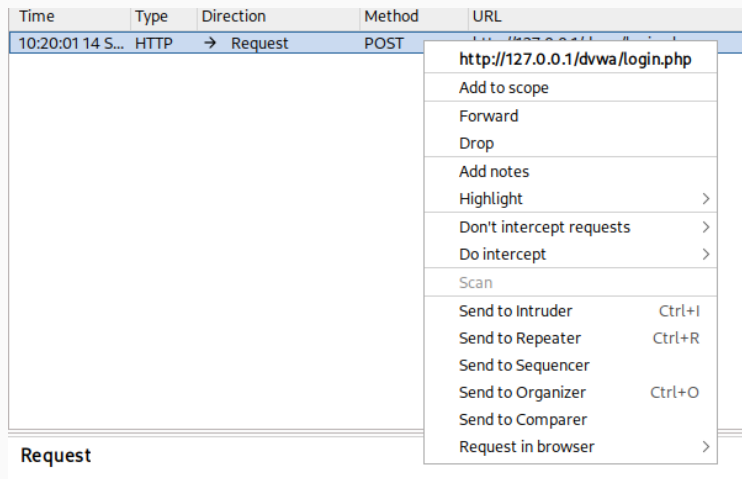


Рис. 8: Send to intruder

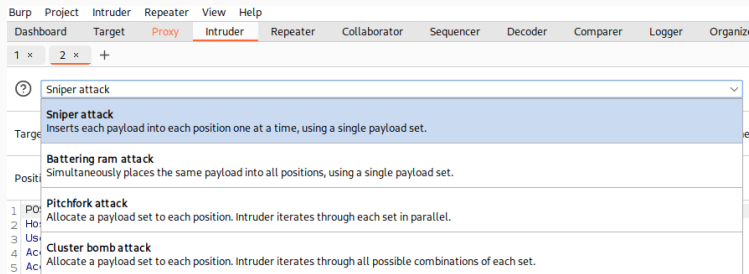


Рис. 9: Доступные методы атак

Создание списка для атаки (Sniper attack)

Payloads

Payload position:

All payload positions

Payload type:

Simple list

Payload count:

7

Request count:

35

Payload configuration

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

Paste

admin

Load...

svpavliuchenkov

Remove

321user

Clear

1234

Deduplicate

123

password

Add

Add from list... [Pro version only]

Запуск атаки на localhost:80

2. Intruder attack of http://localhost:80

Results Positions

▼ Capture filter: Capturing all items

▼ View filter: Showing all items

Request ^v	Position	Payload	Status code	Response received	Error	Timeout	Length	Comment
0	0		404	7			488	
1	1	admin	404	0			487	
2	1		404	9			488	
3	1	svpavluchenkov	404	1			488	
4	1	32user	404	1			488	
5	1	1234	404	25			488	
6	1	123	404	57			488	
7	1	password	404	0			488	
8	2	admin	404	0			488	

Рис. 11: Запросы при атаке

Выбор подстановки значений из списка

Positions

```
1 POST /dvwa/login.php HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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: 98
9 Origin: http://127.0.0.1
10 Connection: keep-alive
11 Referer: http://127.0.0.1/dvwa/login.php
12 Cookie: security=impossible; PHPSESSID=0a442a2b72d2
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 Priority: u=0, i
19
20 username=admin+techno+ya&password=password&Login
```


Пример запросы при атаке DVWA

Index	Position	Payload	Status Code
1	1	123	302
1	1	svpavliuchenkov	302
1	1		302
1	1	http://127.0.0.1	302
1	1	http://127.0.0.1	302
2	2		302
2	2	admin	302
2	2	password	302
2	2	123	302

Response

Raw	Hex
<pre>/dvwa/login.php HTTP/1.1 127.0.0.1 Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0 t: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 t-Language: en-US,en;q=0.5 t-Encoding: gzip, deflate, br nt-Type: application/x-www-form-urlencoded nt-Length: 97 n: http://127.0.0.1 ction: keep-alive er: http://127.0.0.1/dvwa/login.php e: security=impossible; PHPSESSID=0a442a2b72d2de9571d219602ce51bfe de-Insecure-Requests: 1 etch-Dest: document etch-Mode: navigate etch-Site: same-origin etch-User: ?1 ity: u=0, i</pre>	

В этом этапе я научился пользоваться Burp Suite, а именно мощных инструментов безопасности веб-приложений, который демонстрируют реальные возможности злоумышленника, проникающего в веб-приложения и позволяет моделировать события заранее позволяя найти уязвимости.