

Персональный проект. Этап №5

Основы информационной безопасности

Астраханцева А. А.

11 мая 2024

Российский университет дружбы народов, Москва, Россия

- Астраханцева Анастасия Александровна
- студентка НКАбд-01-22
- Студ. билет: 1132226437
- Российский университет дружбы народов
- <https://anastasiia7205.github.io/>

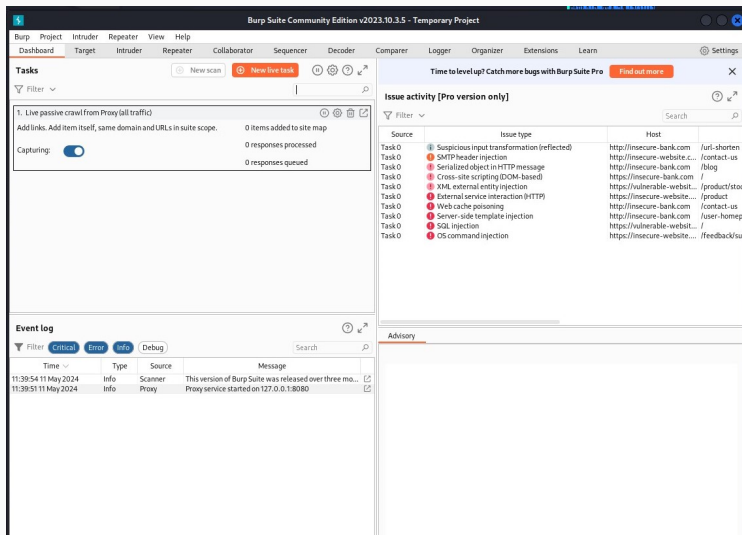


Знакомство с инструментами Burp Suite и их применение.

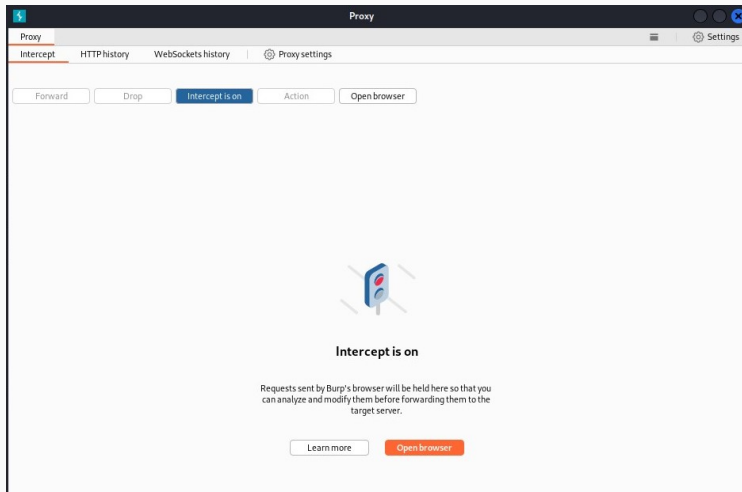
Выполнение работы

Окно Burp Suite

Находим Burp Suite среди встроенных приложения и открываем его.

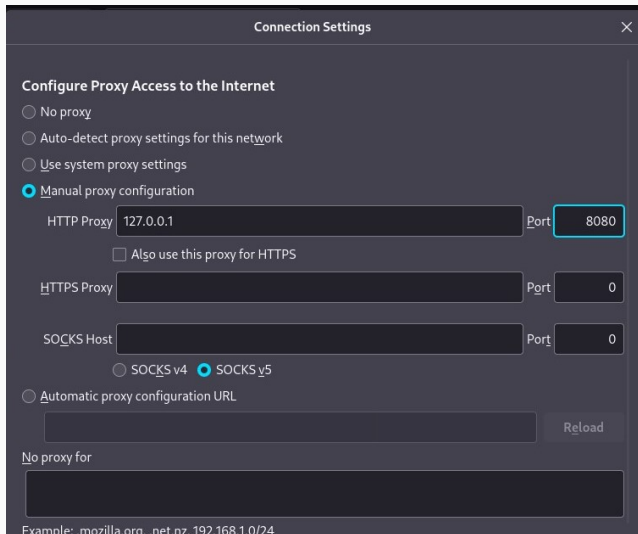


Будем производить взлома учетных данных, что-бы получить доступ к приложению DVWA.
Для этого сначала нужно настроить прокси-сервер.



Настройка прокси в браузере

Теперь нужно настроить браузер для своего прокси-сервера.



The screenshot shows a 'Connection Settings' dialog box with a close button (X) in the top right corner. The main section is titled 'Configure Proxy Access to the Internet'. It contains four radio button options: 'No proxy', 'Auto-detect proxy settings for this network', 'Use system proxy settings', and 'Manual proxy configuration'. The 'Manual proxy configuration' option is selected. Below these options are three proxy configuration sections. The first is 'HTTP Proxy', with a text field containing '127.0.0.1' and a 'Port' field containing '8080'. A checkbox labeled 'Also use this proxy for HTTPS' is unchecked. The second is 'HTTPS Proxy', with an empty text field and a 'Port' field containing '0'. The third is 'SOCKS Host', with an empty text field and a 'Port' field containing '0'. Below these are two radio button options: 'SOCKS v4' and 'SOCKS v5', with 'SOCKS v5' selected. At the bottom, there is an 'Automatic proxy configuration URL' section with an empty text field and a 'Reload' button. Below that is a 'No proxy for' section with an empty text field. At the very bottom, there is an example text: 'Example: mozilla.org, net.nz, 192.168.1.0/24'.

Connection Settings

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: Port: 0

SOCKS Host: Port: 0

- ☐ SOCKS v4
- ☒ SOCKS v5

☐ Automatic proxy configuration URL

Reload

No proxy for

Example: mozilla.org, net.nz, 192.168.1.0/24

Настройка прокси в браузере

Теперь нужно посетить целевой сайт. Браузер должен оставаться в режиме подключения.

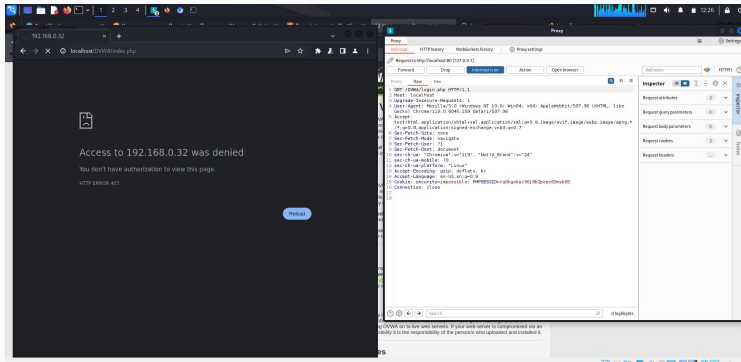


Рис. 4: Получение первых данных

На вкладке Target теперь будут некоторые данные на внутренней вкладке Site map.

The screenshot shows the Burp Suite Community Edition v2023.10.3.5 interface. The 'Target' tab is selected in the top menu. Below the menu, there is a filter bar that reads: 'Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders'. The main panel displays a list of hosts and their associated requests. The first host is 'http://localhost'. The requests are as follows:

Host	Method	URL	Params	Status code	Length	MIME type	Title
http://localhost	GET	/DWAA/login.php		200	1672	HTML	Login:: Damn Vulnerable ...
http://localhost	GET	/DWAA/index.php		302	629		
http://localhost	POST	/DWAA/login.php	✓	302	439		

The bottom panel shows the details of the selected request (GET /DWAA/index.php). The 'Request' tab is active, displaying the raw request data. The 'Response' tab is also visible, showing the raw response data. The 'Inspector' panel on the right shows the request attributes, headers, and response headers.

Request

```
1 GET /DWAA/index.php HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Chromium";v="119",
  "Not?A_Brand";v="24"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 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
8 Accept:
  text/html,application/xhtml+xml,
  application/xml;q=0.9,image/avif
  ,image/webp,image/png;q=0.8
  ,application/signed-exchange;v=b
  3;q=0.7
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate,
  br
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

Response

```
1 HTTP/1.1 302 Found
2 Date: Sat, 11 May 2024 09:26:39
  GMT
3 Server: Apache/2.4.58 (Debian)
4 Set-Cookie: security=impossible;
  path=/; HttpOnly
5 Set-Cookie: PHPSESSID=
  h5ihsa35awfL2a6Cckepq3q179;
  expires=Sun, 12 May 2024
  09:26:39 GMT; Max-Age=86400;
  path=/; HttpOnly;
  SameSite=Strict
6 Expires: Thu, 19 Nov 1981
  08:52:00 GMT
7 Cache-Control: no-store,
  no-cache, must-revalidate
8 Pragma: no-cache
9 Set-Cookie: PHPSESSID=
  rq0kgokr30j8b2poo069nsb65;
  expires=Sun, 12 May 2024
  09:26:39 GMT; Max-Age=86400;
  path=/; HttpOnly;
  SameSite=Strict
10 Location: login.php
11 Content-Length: 0
12 Connection: close
13 Content-Type: text/html;
  charset=UTF-8
14
```

Inspector

Request attributes: 2

Request headers: 14

Response headers: 12

Заполнение перехватчиком данных

Сгенерируем трафик, которым воспользуется инструмент — нарушитель Burp Suite.

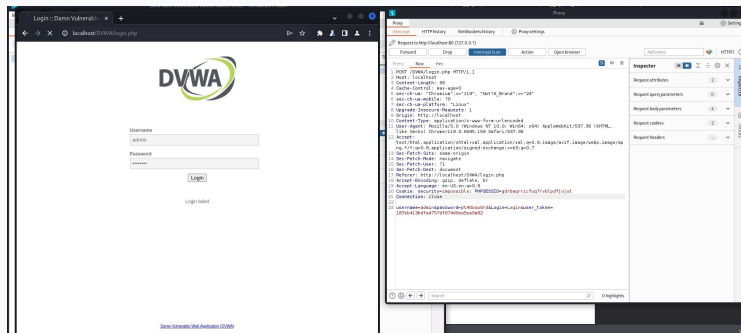
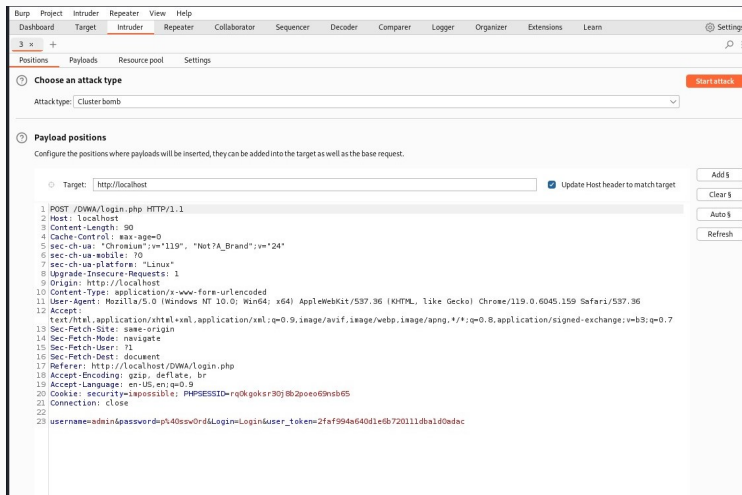


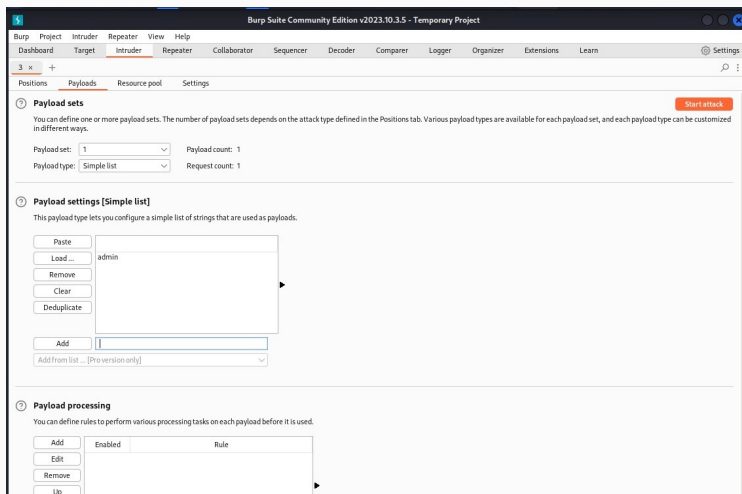
Рис. 6: Заполнение перехватчиком данных

Отправляем данные злоумышленнику. На вкладке Intruder переходим на вкладку Positions (Позиции).



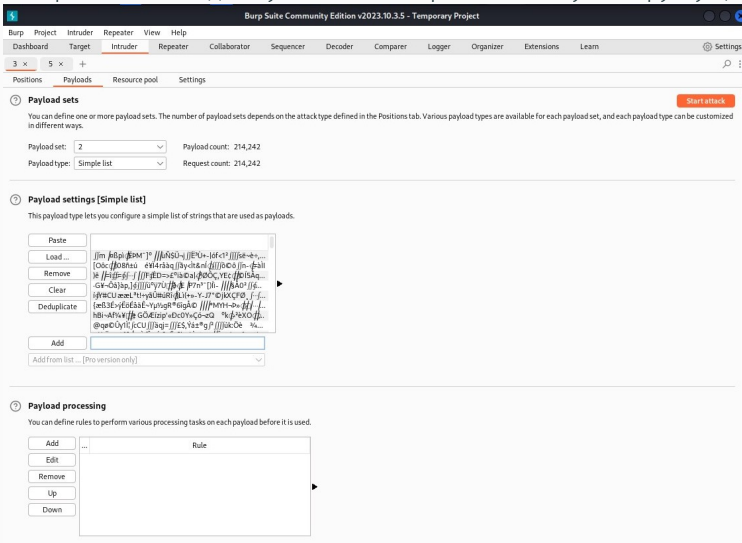
Вкладка Payload set 1

Если щелкнуть на Payload set (Набор полезных нагрузок), мы увидим количество позиций полезных нагрузок. Выбираем значение 1. Оно будет соответствовать полю username.



Вкладка Payload set 2

Теперь в поле ввода Payload set выбираем полезную нагрузку 2, отвечающую за поле пароля.



После этого появится окно с результатами (Results).

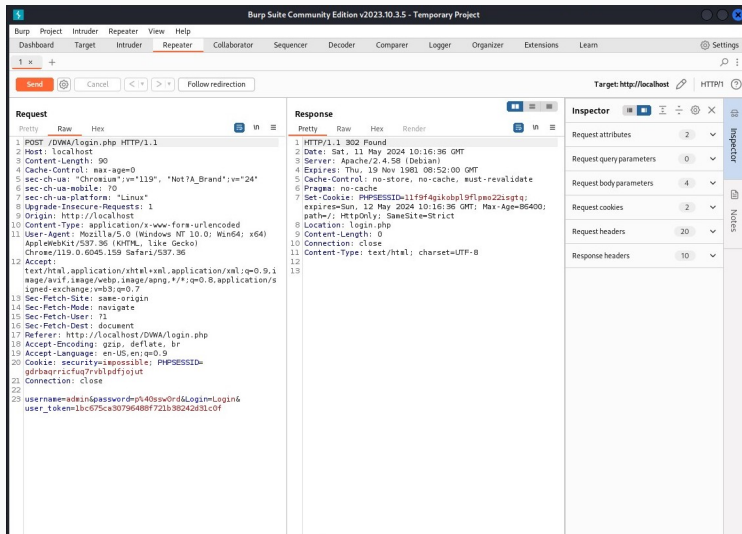
The screenshot shows the Burp Suite interface during an intruder attack. The main window is titled '2. Intruder attack of http://localhost - Temporary attack - Not saved to project file'. The 'Results' tab is active, displaying a table of attack results.

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
0	admin	12345678	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
1	admin	qwerly	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
2	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
3	admin	p@ssword	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
4	admin	p@sswOrd	302	<input type="checkbox"/>	<input type="checkbox"/>	476	
5	admin	p@sswOrd	302	<input type="checkbox"/>	<input type="checkbox"/>	476	

Below the table, the 'Request' and 'Response' details are visible. The request is a POST to /DWA/Login.php with the following headers:

```
1 POST /DWA/Login.php HTTP/1.1
2 Host: localhost
3 Content-Length: 88
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://localhost
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
```

Теперь мы можем перейти на страницу входа DVWA и предоставить доступ к сайту.



Вкладка Repeater Render

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Dashboard Target Intruder Repeater Sequencer Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

5 x +

Send Cancel < >

Target: http://localhost HTTP/1


Request

Pretty Raw Hex

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: localhost
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
7 Upgrade-Insecure-Requests: 1
8 Origin: http://localhost
9 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
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,
  image/avif,image/webp,image/apng,*/*;q=0.8,application/
  signed-exchange;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://localhost/DVWA/login.php
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Cookie: security=impossible; PHPSESSID=
  qdrbaqrricfuq7rvblpdfjojut
19 Connection: close
20
21
```

Response

Pretty Raw Hex Render



Username

Password

Login

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 2

Request headers 18

Response headers 9

Inspector Notes

Done

1,633 bytes 10 millis

Познакомилась с инструментами Burp Suite и применила их для атаки на целевой сайт.

Спасибо за внимание
