

# Индивидуальный проект

## Этап 5. Использование Burp suite

---

Артамонов Т. Е.

12 октября 2024

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Артамонов Тимофей Евгеньевич
- студент группы НКНбд-01-21
- Российский университет дружбы народов
- <https://github.com/teartamonov>



Использовать Burp suite для перехвата запросов и атак.

Burp Suite — это проприетарное программное обеспечение для оценки безопасности и тестирования на проникновение веб-приложений. Примечательные возможности этого пакета включают функции прокси-сканирования веб-страниц (Burp Proxy), регистрировать HTTP-запросы / ответы (Burp Logger и HTTP History), захватывать / перехватывать текущие HTTP-запросы (Burp Intercept), и агрегировать отчеты, указывающие на слабые места (Burp Scanner). Это программное обеспечение использует встроенную базу данных, содержащую заведомо небезопасные синтаксические шаблоны и ключевые слова для поиска в захваченных HTTP-запросах / ответах.

## Выполнение лабораторной работы

---

В настройках браузера зададим прокси. (рис. 1)

The image shows a 'Connection Settings' dialog box with a close button (X) in the top right corner. The title is 'Connection Settings'. Below the title is the section 'Configure Proxy Access to the Internet'. There are 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'. Below this is a checkbox labeled 'Also use this proxy for HTTPS' which is unchecked. The second section is 'HTTPS Proxy' with an empty text field and a 'Port' field containing '0'. The third section 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 option 'Automatic proxy configuration URL' with an unchecked radio button, followed by an empty text field and a 'Reload' button. At the very bottom, there is a label 'No proxy for' followed by an empty text field. In the bottom right corner, there are two buttons: 'Cancel' and 'OK'.

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

Cancel OK

## Запустим Burp suite и включим Intercept. (рис. 2)

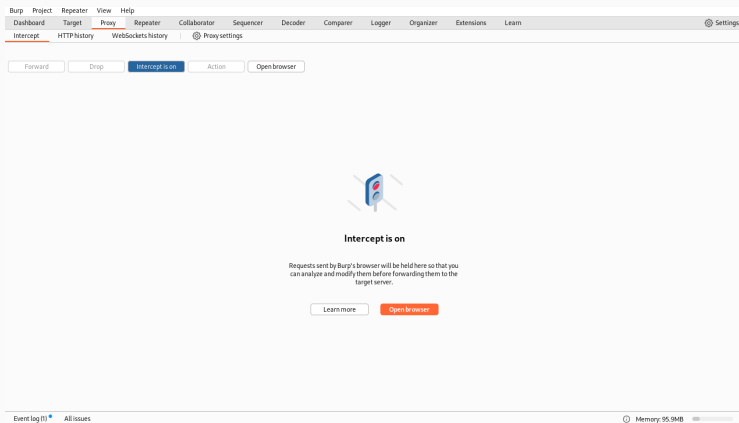


Figure 2: Intercept is on - теперь запросы будут перехватываться



## Пробуем открыть страницу в браузере. (рис. 3)

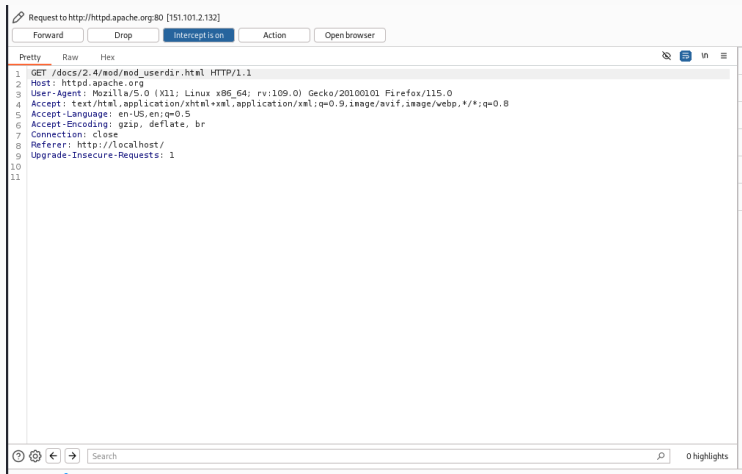


Figure 3: Нас перекидывает в Burp suite и показывает данные, которые мы перехватили вместе с запросом

## Нажимаем forward и заходим в раздел target. (рис. 4)

The screenshot displays the Burp Suite interface with the 'Target' tab selected. The site map on the left shows the target URL `http://httpd.apache.org`. The main panel shows a list of requests, with the first one selected. Below the list, the 'Request' and 'Response' tabs are visible. The 'Request' tab shows the raw request details, and the 'Response' tab shows the raw response details. The 'Inspector' panel on the right shows the request and response headers.

**Request**

```
1 GET /docs/2.4/mod/mod_userdir.html
2 HTTP/1.1
3 Host: httpd.apache.org
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: close
9 Referer: http://localhost/
10 Upgrade-Insecure-Requests: 1
11
```

**Response**

```
1 HTTP/1.1 301 Moved Permanently
2 Connection: close
3 Content-Length: 0
4 Server: Varnish
5 Retry-After: 0
6 Location: https://httpd.apache.org/docs/2.4/mod/mod_userdir.html
7 Accept-Ranges: bytes
8 Date: Sat, 12 Oct 2024 12:55:09 GMT
9 Vary: 1.1 varnish
10 X-Served-By: cache-hel1410034-HEL
11 X-Cache: HIT
12 X-Cache-Hits: 0
13 X-Timer: S1728737709.361639,VSO,VED
14
15
```

**Inspector**

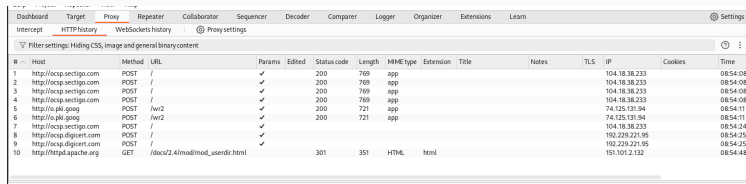
Request attributes: 2

Request headers: 8

Response headers: 12

Figure 4: Видим запрос который мы сюда перенаправили, справа внизу можно увидеть ответ на запрос

Зайдя обратно в раздел Proxy можем посмотреть историю http запросов. (рис. 5)



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
1	http://ocsp.sectigo.com	POST	/	✓		200	769	app					104.18.38.233		08:54:08
2	http://ocsp.sectigo.com	POST	/	✓		200	769	app					104.18.38.233		08:54:08
3	http://ocsp.sectigo.com	POST	/	✓		200	769	app					104.18.38.233		08:54:08
4	http://ocsp.sectigo.com	POST	/	✓		200	769	app					104.18.38.233		08:54:08
5	http://o.pki.goog	POST	/w2	✓		200	721	app					74.125.131.94		08:54:11
6	http://o.pki.goog	POST	/w2	✓		200	721	app					74.125.131.94		08:54:11
7	http://ocsp.sectigo.com	POST	/	✓									104.18.38.233		08:54:24
8	http://ocsp.digicert.com	POST	/	✓									192.229.221.95		08:54:25
9	http://ocsp.digicert.com	POST	/	✓									192.229.221.95		08:54:25
10	http://httpd.apache.org	GET	/docs/2.4/mod/mod_userdir.html			301	351	HTML	html				191.101.2.132		08:54:48

Figure 5: Ссылки, методы запросов, код статуса и тд

## Выводы

---

Использовали Burp suite для перехвата запросов, атаку провести не вышло тк отсутствует необходимый раздел.

1. Burp Suite [Электронный ресурс]. Wikimedia Foundation, Inc., 2024. URL: [https://en.wikipedia.org/wiki/Burp\\_Suite](https://en.wikipedia.org/wiki/Burp_Suite).