

# **Индивидуальный проект**

**Этап 5. Использование Burp suite**

Артамонов Тимофей Евгеньевич

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Теоретическое введение</b>	<b>6</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>7</b>
<b>4</b>	<b>Выводы</b>	<b>10</b>
	<b>Список литературы</b>	<b>11</b>

## Список иллюстраций

3.1	HTTP Proxy . . . . .	7
3.2	Intercept is on - теперь запросы будут перехватываться . . . . .	8
3.3	Нас перекидывает в Burp suite и показывает данные, которые мы перехватили вместе с запросом . . . . .	8
3.4	Видим запрос который мы сюда перенаправили, справа внизу можно увидеть ответ на запрос . . . . .	9
3.5	Ссылки, методы запросов, код статуса и тд . . . . .	9

## **Список таблиц**

# 1 Цель работы

Использовать Burp suite для перехвата запросов и атак.

## 2 Теоретическое введение

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. [1]

### 3 Выполнение лабораторной работы

В настройках браузера зададим прокси. (рис. 3.1)

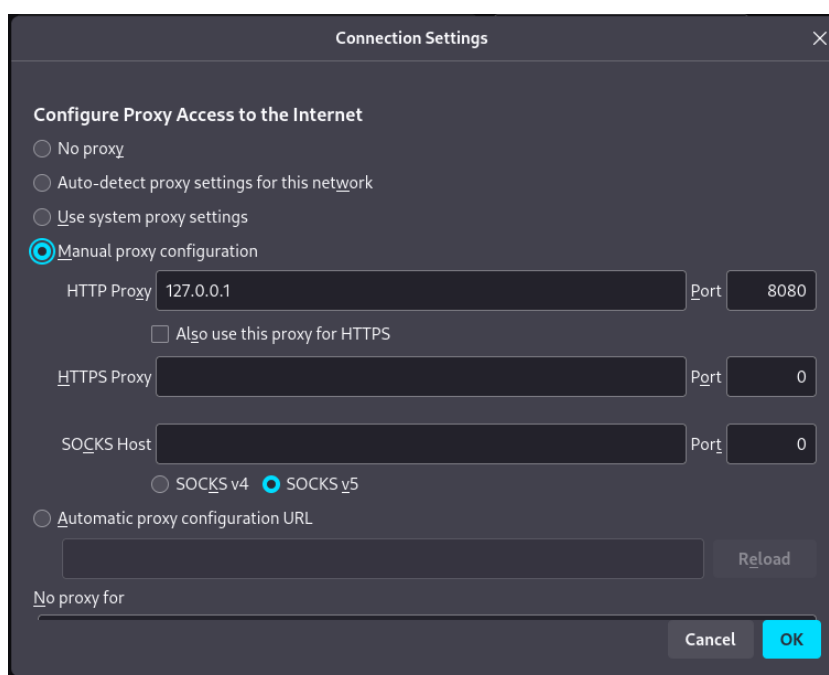


Рис. 3.1: HTTP Proxy

Запустим Burp suite и включим Intercept. (рис. 3.2)

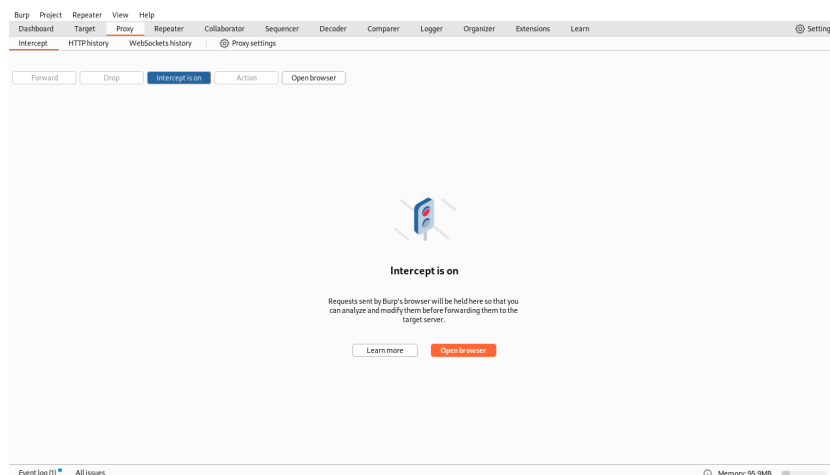


Рис. 3.2: Intercept is on - теперь запросы будут перехватываться

Пробуем открыть страницу в браузере. (рис. 3.3)



Рис. 3.3: Нас перекидывает в Burp suite и показывает данные, которые мы перехватили вместе с запросом

Нажимаем forward и заходим в раздел target. (рис. 3.4)



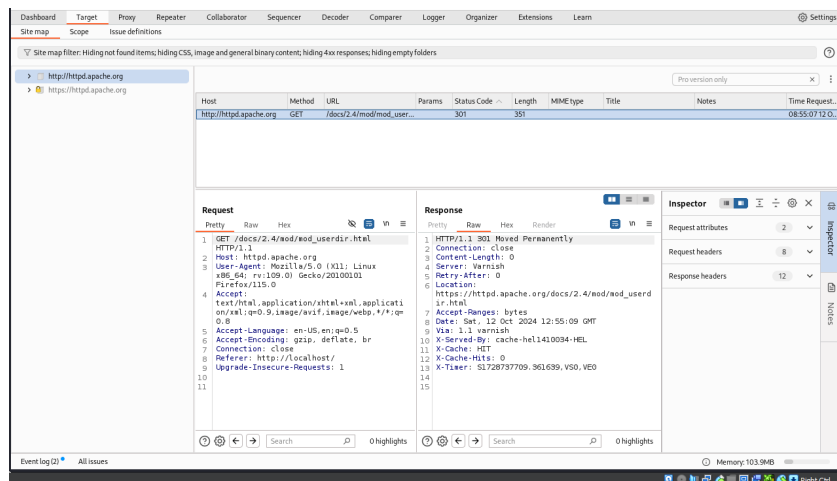


Рис. 3.4: Видим запрос который мы сюда перенаправили, справа внизу можно увидеть ответ на запрос

Зайдя обратно в раздел Прошу можем посмотреть историю http запросов. (рис. 3.5)

#	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://a.pk.goog	POST	/w2		✓	200	721	app					74.125.131.94	08:54:11'	
6	http://a.pk.goog	POST	/w2		✓	200	721	app					74.125.131.94	08:54:11'	
7	http://ocsp.sectigo.com	POST	/		✓	200	769	app					104.18.38.233	08:54:24'	
8	http://ocsp.sectigo.com	POST	/		✓	200	769	app					104.18.38.233	08:54:24'	
9	http://ocsp.sectigo.com	POST	/		✓	200	769	app					104.18.38.233	08:54:24'	
10	http://httpd.apache.org	GET	/docs/2.4/mod/mod_userdir.html			301	351	HTML	html				151.101.2.132	08:54:48'	

Рис. 3.5: Ссылки, методы запросов, код статуса и тд

## 4 Выводы

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

## Список литературы

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