

Индивидуальный проект №5

Основы информационной безопасности

Барсегян В.Л.

Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия

- Барсегян Вардан Леонович
- НПИБд-01-22
- Российский университет дружбы народов
- [1132222005@pfur.ru]
- https://github.com/VARdamn/study_2023-2024_infosec/tree/master/project-personal

Вводная часть

Знакомство с программой Burp Suite и изучение ее функционала.

Выполнение лабораторной работы

Открываю Burp Suite и во вкладке Proxy включаю перехват http-запросов

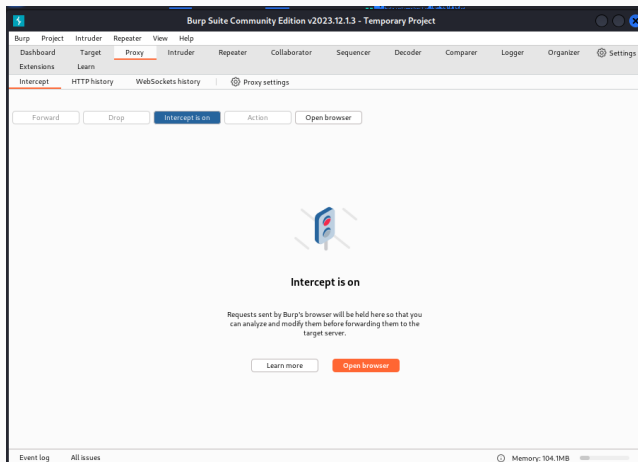


Figure 1: Перехват http-запросов

В настройках браузера настраиваю прокси-сервер

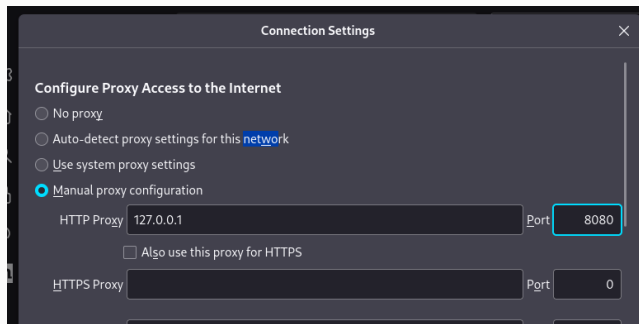


Figure 2: Настройка прокси-сервера

Теперь, трафик браузера перехватывается в программе Burp Suite. Например, при открытии веб-страницы мы видим GET-запрос к ней

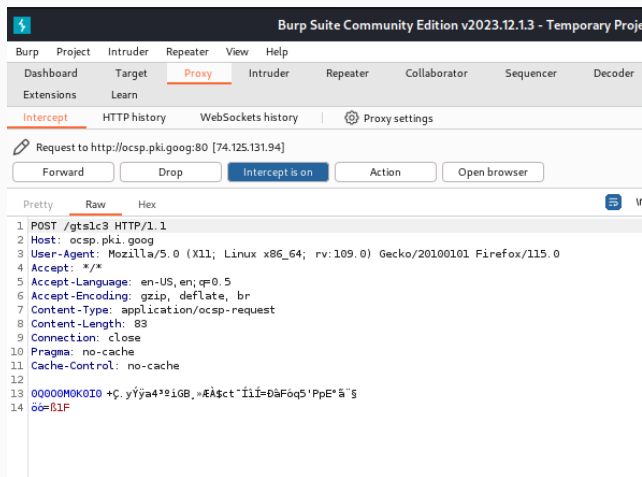
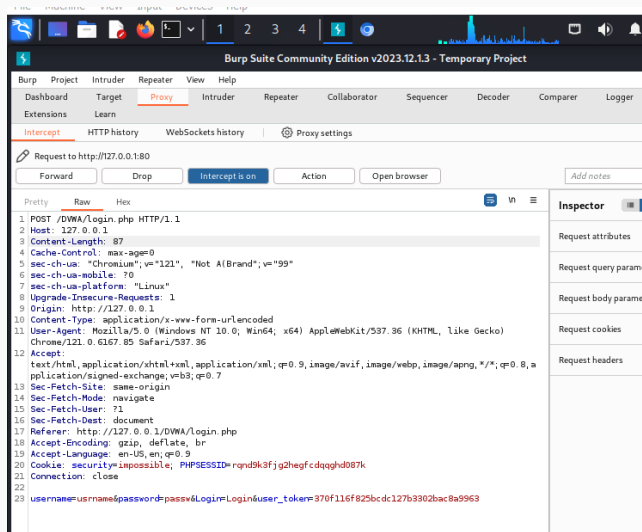


Figure 3: Перехват трафика

Отправляю POST-запрос к DVWA на авторизацию с логином *username* и паролем *passw*.



Перехожу во вкладку intruder, выбираю тип атаки Cluster bomb. Копирую POST-запрос к DVWA из прошлого пункта и параметры username и password оборачиваю в переменные

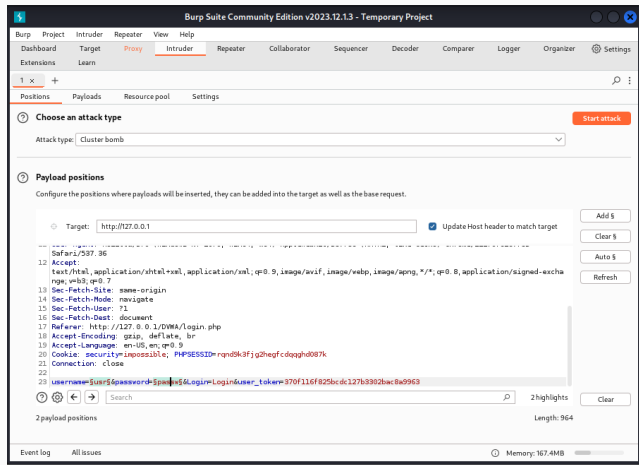
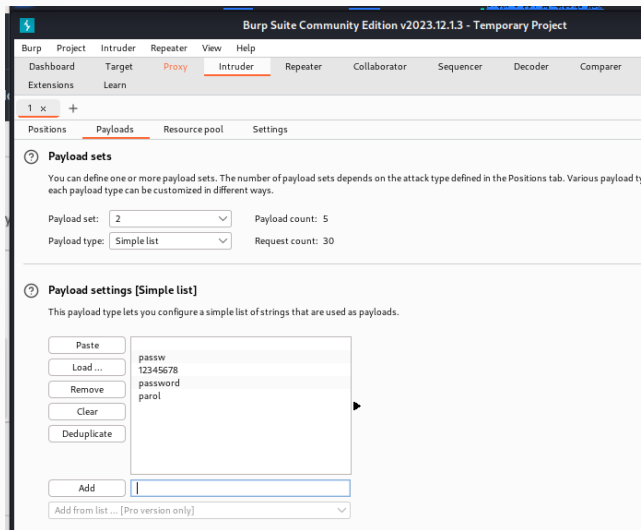


Figure 5: Создание атаки Cluster bomb

Перехожу во вкладку Payloads, и для переменной 1 (username) добавляю несколько значений. Аналогично делаю для переменной 2 (login)



Нажимаю на кнопку *Start attack*, после чего посылаются POST-запросы со всеми комбинациями переменных username и password. Например, для комбинации логина и пароля user:12345678 запрос перенаправляется на страницу /login.php - значит, данная комбинация неверная

2. Intruder attack of http://127.0.0.1

Attack Save Columns

2. Intruder attack of http://127.0.0.1 Attack Save

Results Positions Payloads Resource pool Settings

Filter: Showing all items


Requ...	Payload 1	Payload 2	Status code	Error	Timeout	Length	Comment
12	login	passw	302			475	
13		12345678	302			476	
14	username	12345678	302			475	
15		12345678	302			476	
16	admin	12345678	302			475	
17	user	12345678	302			475	
18	login	12345678	302			476	
19		password	302			476	
20	username	password	302			476	
21		password	302			476	
22	admin	password	302			476	
23	user	password	302			476	
24	login	password	302			476	

Request Response


Pretty Raw Hex Render

```
7 Set-Cookie: PHPSESSID=go14stfbklbgbpse5tqludud6d1; expires=Sat, 20 Apr 2024 11:51:35 GMT; Max-Age=86400; path=/; HttpOnly
8 Location: login.php
9 Content-Length: 0
10 Keep-Alive: timeout=5, max=99
```

Все комбинации, кроме admin:password, перенаправляются на /login.php. Комбинация admin:password перенаправляет на страницу /index.php - значит, комбинация admin:password верная

 2. Intruder attack of http

Attack Save Columns

 2. Intruder attack of http://127.0.0.1

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Requ...	Payload 1	Payload 2	Status code	Error
18	login	12345678	302	<input type="checkbox"/>
19		password	302	<input type="checkbox"/>
20	username	password	302	<input type="checkbox"/>
21		password	302	<input type="checkbox"/>
22	admin	password	302	<input checked="" type="checkbox"/>
23	user	password	302	<input type="checkbox"/>
24	login	password	302	<input type="checkbox"/>
25		parol	302	<input type="checkbox"/>
26	username	parol	302	<input type="checkbox"/>
27		parol	302	<input type="checkbox"/>
28	admin	parol	302	<input type="checkbox"/>
29	user	parol	302	<input type="checkbox"/>
30	login	parol	302	<input type="checkbox"/>

Request Response

Pretty Raw Hex Render

```
7 Set-Cookie: PHPSESSID=v4pto2j9ima4viiheillqjjpqa; expires=Sat, 20 Apr :
  SameSite=Strict
8 Location: index.php
9 Content-Length: 0
```

Я познакомился с Burp Suite и научился его применять на практике.

Список литературы
