

# Индивидуальный проект. Этап 5.

Использование Burp Suite

---

Стариков Данила Андреевич

11 мая 2024

## Цели и задачи

---

- Познакомиться с экосистемой Burp Suite для поиска уязвимостей веб-приложений и демонстрации возможностей злоумышленника

## Результаты

---

# Знакомство с интерфейсом приложения

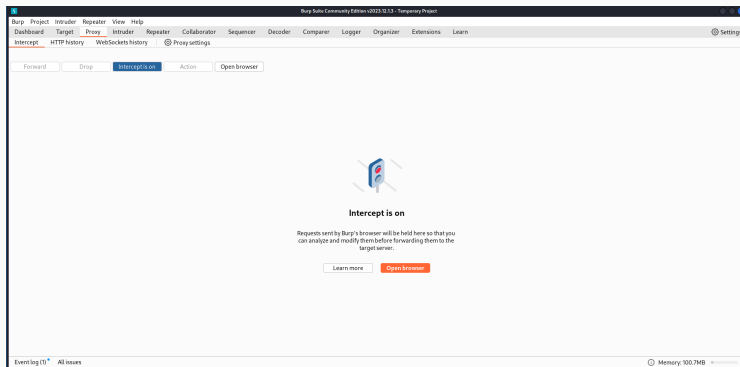


Figure 1: Окно приложения Burp Suite.

# Знакомство с интерфейсом приложения

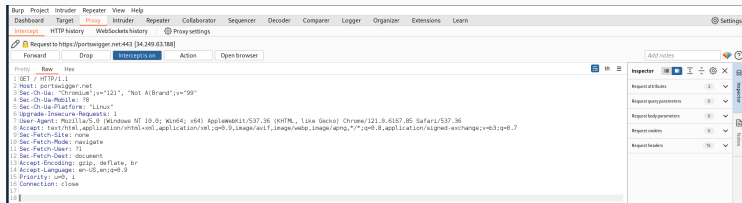


Figure 2: Представление перехваченного HTTP запроса.

# Знакомство с интерфейсом приложения

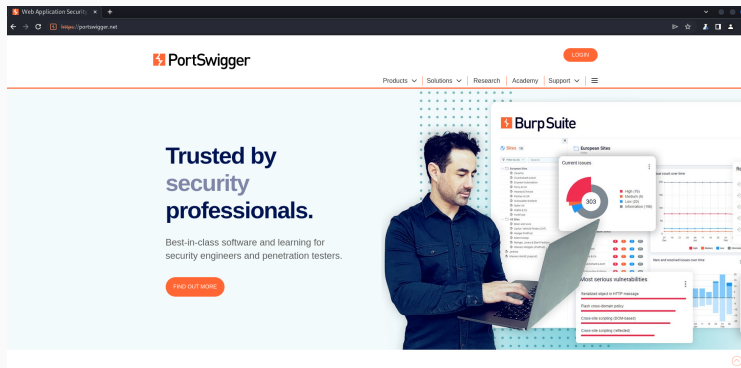


Figure 3: Сайт открыт через приложение.

# Знакомство с интерфейсом приложения

The screenshot displays the Burp Suite Community Edition interface. The top menu bar includes Project, Intruder, Repeater, View, Help, Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The main toolbar shows Intercept, HTTP history, WebSockets history, and Proxy settings. The HTTP history tab is active, showing a list of requests. The selected request is a GET request to /content/images/svg/icons/enterprise.svg from https://portswigger.net. The details pane on the right shows the request and response. The response is an HTTP/2 200 OK status, with a Content-Type of image/svg+xml. The response body is a large base64-encoded string.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
1	https://portswigger.net	GET	/			200	48562	HTML		Web Application Secur...		✓	34.249.63.188	SessionId=CTDIEK...	17:09:44.11 M...
3	https://portswigger.net	GET	/content/images/svg/icons/enterprise...			200	2094	XML	svg			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:38.11 M...
4	https://portswigger.net	GET	/content/images/svg/icons/professio...			200	1938	XML	svg			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:38.11 M...
7	https://portswigger.net	GET	/content/images/svg/icons/communi...			200	2094	XML	svg			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:41.11 M...
8	https://portswigger.net	GET	/mega-nav/images/dastardly.svg			200	1914	XML	svg			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:41.11 M...
10	https://portswigger.net	GET	/bundles/public/statics/jchp2KAN...		✓	200	23942	script	js			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:41.11 M...
16	https://portswigger.net	GET	/images/company-logos/amazon.svg			200	6725	XML	svg			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:41.11 M...
17	https://portswigger.net	GET	/images/company-logos/hasa.svg			200	7252	XML	svg			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:42.11 M...
18	https://portswigger.net	GET	/content/images/logos/portswigger...			200	4797	XML	svg			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:42.11 M...
19	https://portswigger.net	GET	/images/company-logos/burclays.svg			200	6888	XML	svg			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:42.11 M...
20	https://portswigger.net	GET	/images/company-logos/fedex.svg			200	4173	XML	svg			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:42.11 M...
21	https://portswigger.net	GET	/images/company-logos/bsa.svg			200	2987	XML	svg			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:42.11 M...
24	https://portswigger.net	GET	/images/cademy-small.svg			200	17956	text	svg			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:42.11 M...
26	https://portswigger.net	GET	/images/burp-suite-small.svg			200	6203	XML	svg			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:42.11 M...
27	https://portswigger.net	GET	/images/research-small.svg			200	12391	text	svg			✓	34.240.117.4	ANVSALBAPP-05_f...	17:10:42.11 M...

**Request**

```
1 GET /content/images/svg/icons/enterprise.svg HTTP/2
2 Host: portswigger.net
3 Cookie: SessionId=CTDIEK...
4 Content-Type: image/svg+xml
5 Content-Length: 554
6 Server: Kestrel
7 Accept-Ranges: bytes
8 Cache-Control: must-revalidate, max-age=0
9 Etag: "1a9a697c945992a"
10 Last-Modified: Wed, 01 May 2024 07:18:38 GMT
11 Strict-Transport-Security: max-age=31536000; preload
12 X-Content-Type-Options: nosniff
13 X-Frame-Options: SAMEORIGIN
14 X-Kss-Protection: 1; mode=block
15 Content-Security-Policy: default-src 'none'; form-action 'self'; base-uri 'none'; child-src 'self' https://www.youtube.com/embed; connect-src 'self'
```

**Response**

```
1 HTTP/2 200 OK
2 Date: Sat, 11 May 2024 14:10:39 GMT
3 Content-Type: image/svg+xml
4 Content-Length: 554
5 Server: Kestrel
6 Accept-Ranges: bytes
7 Cache-Control: must-revalidate, max-age=0
8 Etag: "1a9a697c945992a"
9 Last-Modified: Wed, 01 May 2024 07:18:38 GMT
10 Strict-Transport-Security: max-age=31536000; preload
11 X-Content-Type-Options: nosniff
12 X-Frame-Options: SAMEORIGIN
13 X-Kss-Protection: 1; mode=block
14 Content-Security-Policy: default-src 'none'; form-action 'self'; base-uri 'none'; child-src 'self' https://www.youtube.com/embed; connect-src 'self'
```

Figure 4: История всех HTTP запросов.



# Перехват и модификация HTTP запроса

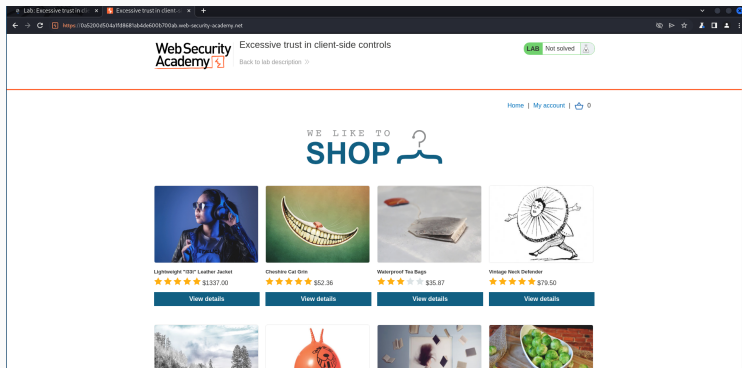


Figure 5: Тестовое приложение.

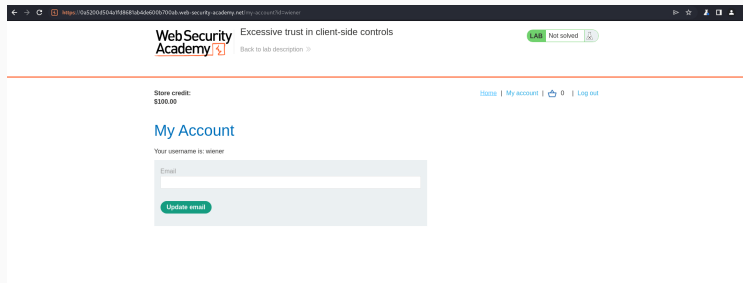


Figure 6: Личный кабинет с 100 долларами на счету.

# Перехват и модификация HTTP запроса

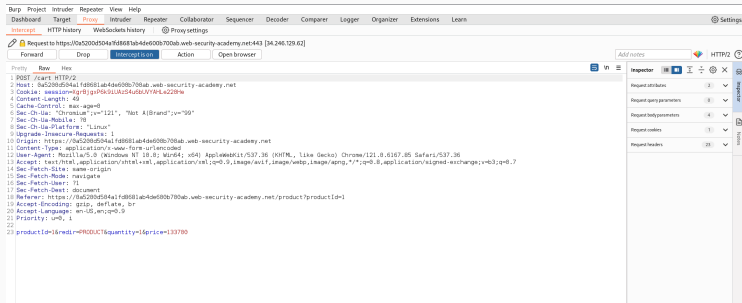


Figure 7: Перехват HTTP запроса при добавлении товара в корзину.

# Перехват и модификация HTTP запроса

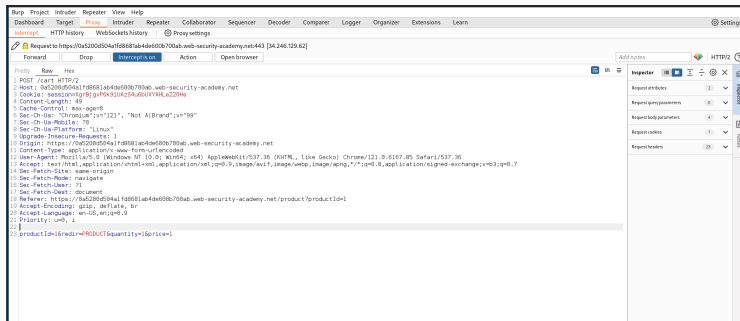


Figure 8: Запрос после изменения цены.

# Перехват и модификация HTTP запроса

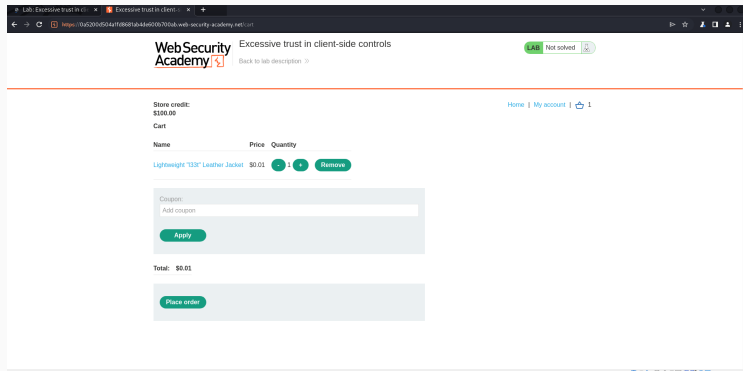


Figure 9: Корзина с измененной ценой товара.

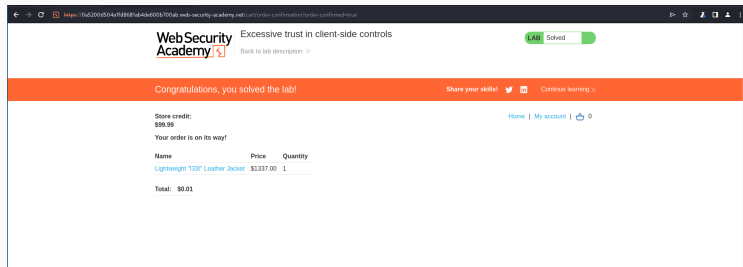


Figure 10: Итоговый счет на аккаунте после оплаты заказа.

ИТОГ



- В результате работы познакомились с экосистемой **Burp Suite** и продемонстрировали ее работу при перехвате и модификации HTTP запроса.