

Before we begin...

Please have all of these set up on your device before we begin:

BurpSuite: <https://portswigger.net/burp/communitydownload>

Docker: <https://docs.docker.com/engine/install/>

OWASP Juice Shop: <https://owasp.org/www-project-juice-shop/>

If you need help, ask an officer!

```
docker pull bkimminich/juice-shop
```

```
docker run --rm -p 3000:3000 bkimminich/juice-shop
```

Introduction to Burp Suite

Batman's Kitchen 2025

Housekeeping

This Friday we are participating in [Hack.lu](#) CTF

- Great opportunity to get hands on experience
- Very beginner friendly

Next week:

- Next Wednesday we are doing an Introduction to Computer Networking

Introduction

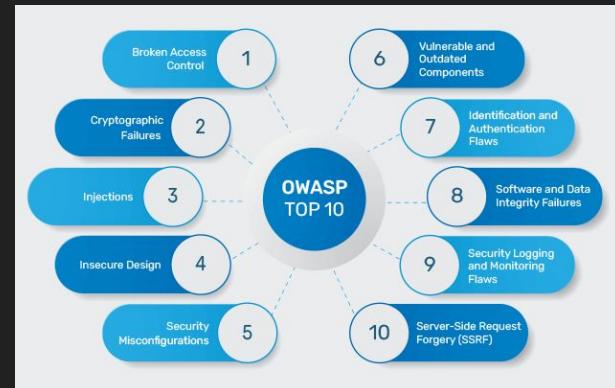
- These slides have been adapted from John Poch
 - Senior Security Consultant for ivision
 - .cosmic_panda on discord
 - Be sure to ask him if you have any questions about the pentesting industry as a whole!

What is Penetration Testing?

- White hat simulation of real-world attacks
 - Done by approved 3rd parties/security personnel
 - 3 types: White, gray, and black box assessments
- Various types for various systems
 - Web applications, mobile apps, IoT devices, ect
 - We will be focusing on web application pentesting

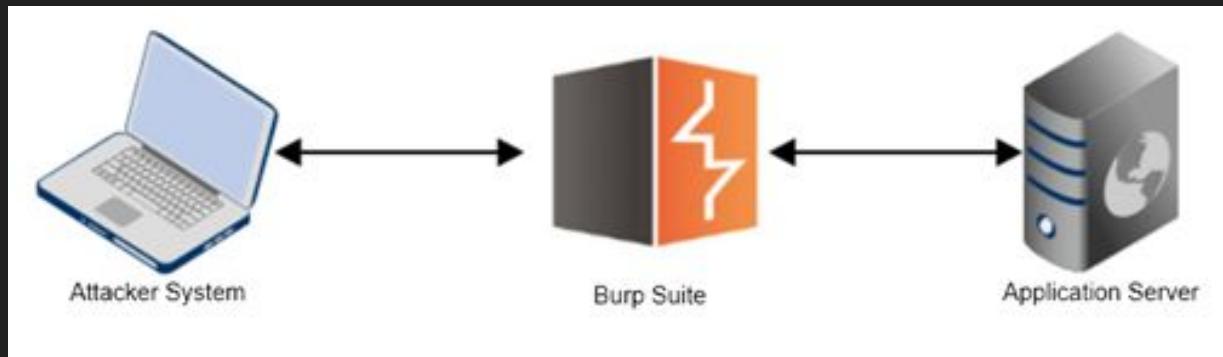
Web application pentesting

- Black box attacker with network access to the target web server
- Makes use of HTTP Proxies (like Burp) to view/modify requests
- Knowledge of threat modeling and OWASP Top 10!
 - Threat modeling: documenting and analyzing application so threats can be considered
 - OWASP Top 10 (Web):

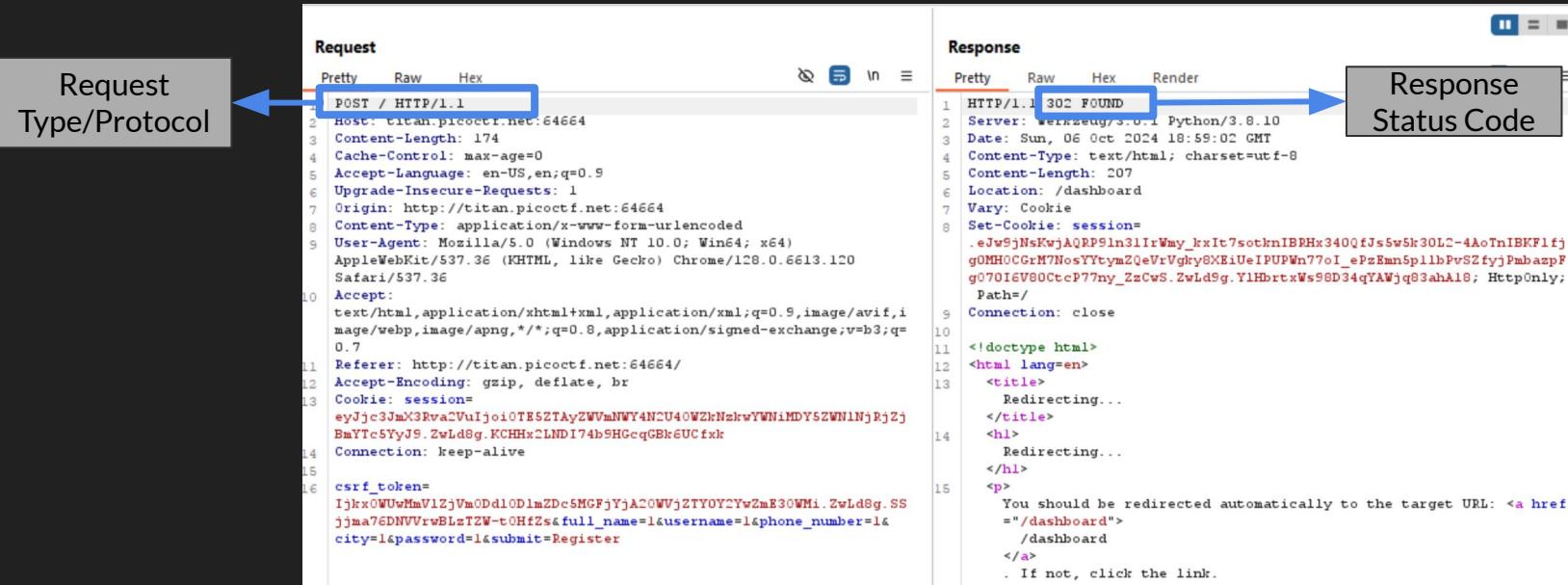


What is BurpSuite?

- Web application pentesting tool
- Acts as a middleman between an attacker system and application server
- Requests can be modified viewed before being sent to the server or displayed on the system



HTTP Request/Response Structure (as it appears in burp)



HTTP Request/Response Structure (as it appears in burp)

Request Headers

Request Body

Response Headers

Response Body

```
Request
Pretty Raw Hex
1 POST / HTTP/1.1
2 Host: titan.picoctf.net:64664
3 Content-Length: 174
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Upgrade-Insecure-Requests: 1
7 Origin: http://titan.picoctf.net:64664
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120
Safari/537.36
10 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://titan.picoctf.net:64664/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: session=eyJjc3JmX3Rva2VuIjoiOTF5ZTAyZWVmNWy4N2U40WZkNmkwYWNiMDY5ZWN1NjRjZjBmYtcsYyj9.ZwLd8g.KCCHh2LND174b9HGcqGBk6UCfxk
14 Connection: keep-alive
15
16 csrf_token=IjhxOWUmMv1ZjVmODdlODlmZDc5MGFjYjA20WVjZTY0Y2YwZmE30WMi.ZwLd8g.SSjma7EDNVVrwBlzTzW-t0HfZs&full_name=1&username=1&phone_number=1&city=1&password=1&submit=Register
```

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 302 FOUND
2 Server: Werkzeug/3.0.1 Python/3.8.10
3 Date: Sun, 06 Oct 2024 18:59:02 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 207
6 Location: /dashboard
7 Vary: Cookie
8 Set-Cookie: session=.eJw9jNsKwjAQRP9ln3l1rWmy_kxit7sothniIBRHx340QfJs5w5k30L2-4AoTnIBKf1fjgOMH0Gr7TNosYttymZQeVgkry8xEiUeIPUPWn77oi_ePzEan5p11bPvSZfyjPmbazpFg070IEV80CtcP77ny_ZzCwS.ZwLd8g.Y1HbrtzWs98D34qYAWjq83ahA18; HttpOnly; Path/
9 Connection: close
10
11 <!doctype html>
12 <html lang=en>
13   <title>
14     Redirecting...
15   </title>
16   <h1>
17     Redirecting...
18   </h1>
19   <p>
20     You should be redirected automatically to the target URL: <a href="/dashboard">/dashboard</a>
21     . If not, click the link.
22   </p>
```

Request
Body

ZAP and Caido

Zed Attack Proxy (ZAP) by OWASP/Checkmarx

- Open Source Attack Proxy

Caido

- Allegedly better automation and workflow tools
- Access to pro for students

Important BurpSuite Features

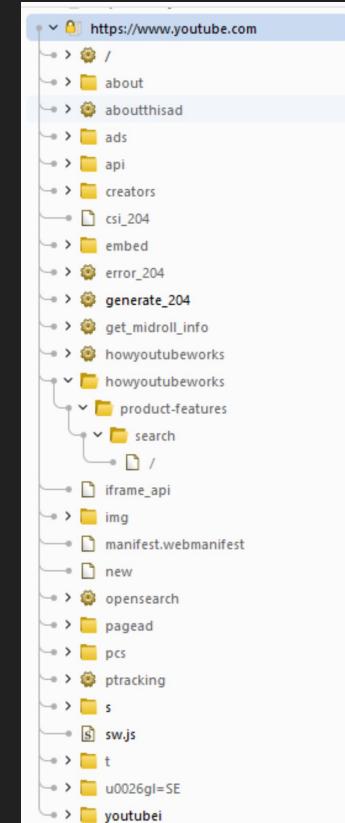
- Proxy: Intercept, view, and manipulate requests
- Target: Site mapping
- Repeater: Manual request modification
- Intruder: Automated request modification
- Other useful modules as well (Decoder, Organizer, etc)
 - But we'll focus on the first 4

Proxy (+ Demo)

- BurpSuite's own browser with more features
 - Intercept: view and modify requests before they get sent to the server
 - HTTP History: Shows all HTTP requests made by the browser and their responses
 - WebSocket History: Shows all the data sent and received via websockets

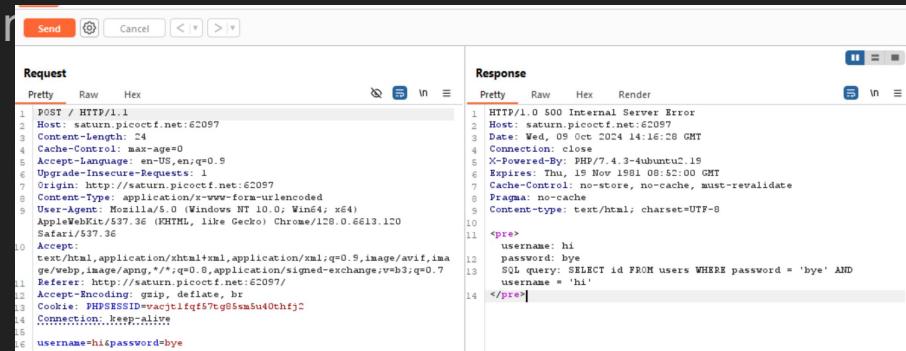
Target

- Site mapping
- Scope definition
 - Allows marking of what domains are “in scope” when pentesting
 - Can then be used to filter out requests to sites you don’t care about



Repeater

- Modify previously sent requests before sending
 - “Send to repeater”
 - See how changing specific aspects of the request (headers, body content, ect) changes the server’s response
 - Allows for easily testing
 - Example repeater request:



The screenshot shows a browser developer tools Network tab with two panels: Request and Response.

Request:

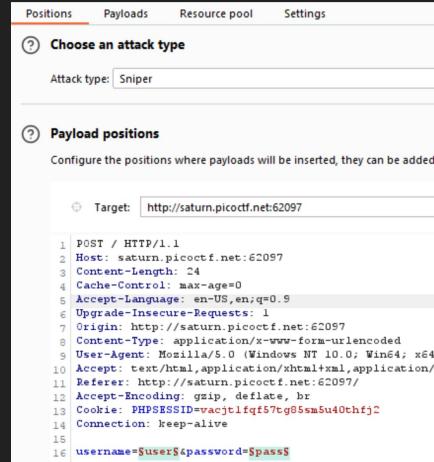
```
POST / HTTP/1.1
Host: saturn.picocft.net:62097
Content-Length: 24
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
Origin: http://saturn.picocft.net:62097
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6613.120
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://saturn.picocft.net:62097
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=vacj1fq57tg05xm5u40thfj2
Connection: keep-alive
username=hi&password=bye
```

Response:

```
HTTP/1.0 500 Internal Server Error
Host: saturn.picocft.net:62097
Date: Wed, 09 Oct 2024 14:16:28 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 14
X-Powered-By: PHP/7.4.3-4ubuntu2.19
Expires: Thu, 15 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-type: text/html; charset=UTF-8
<pre>
username: hi
password: bye
SQL query: SELECT id FROM users WHERE password = 'bye' AND
username = 'hi'
</pre>
```

Intruder

- Automate sending requests with modified parameters
 - “Send to intruder”
 - Makes brute-forcing attacks much easier
 - Can also be used for Denial of Service
- Specify payload locations/types
 - Example intruder request:



The screenshot shows the OWASP ZAP Intruder tool's configuration interface. The top navigation bar includes 'Positions', 'Payloads', 'Resource pool', and 'Settings'. The 'Payloads' tab is active, showing the sub-section 'Choose an attack type' with 'Sniper' selected. Below this is the 'Payload positions' section, which includes a 'Target' field set to 'http://saturn.picoctf.net:62097'. A code editor displays a POST request template with various headers and a payload section. The payload section contains the following code:

```
1 POST / HTTP/1.1
2 Host: saturn.picoctf.net:62097
3 Content-Length: 24
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Upgrade-Insecure-Requests: 1
7 Origin: http://saturn.picoctf.net:62097
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
10 Accept: text/html,application/xhtml+xml,application/xml
11 Referer: http://saturn.picoctf.net:62097/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=vactlfqf57cg05sm5u40thfj2
14 Connection: keep-alive
15
16 username=$user$&password=$pass$
```

Juice Shop Challenges

Challenges

- Submit 10 or more customer feedbacks within 10 seconds
- Post some feedback in another user's name
- Post a product review as another user or edit another user's review
- Place an order that makes you rich
- Upload a file larger than 100 kb
- Upload a file that isn't a .pdf or .zip
- Register as a user with admin privileges
- Put an additional product into another user's basket (HARD)

Recommended Extensions

Extensions make Burp way more powerful

- Auth Analyzer
- Hackverter
- JWT Editor