



# 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 2024 | Workshop 2



# General Announcements

Special topics talk this Friday at 5:30PM

- Cyber Hygiene Talk presented by Krishna!
- Learn about protecting yourself online

Next week:

- Next week's talk (Wednesday the 16th) will be on XSS
- Alum panel and resume review planned Friday (the 18th)



# Internship Opportunity (!!!)

- Security Innovation
  - Seattle-based web pentesting firm
  - Buncha BK alums there, + Andrew
    - Dhruv & Daniel also interned here
  - Very cool
  - Guaranteed interview if you do their CTF thing
  - <https://www.securityinnovation.com/about/careers/>



# Introduction

- Credits to the presentation go to 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!

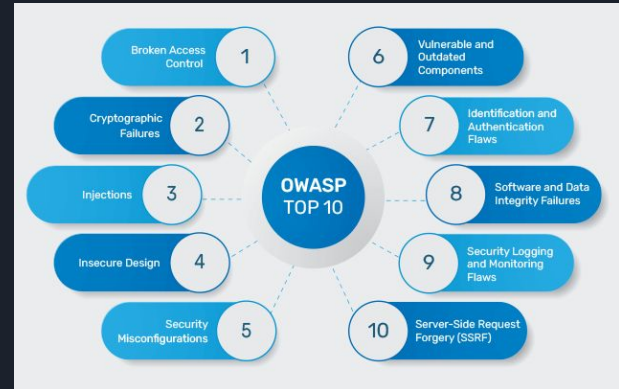


# What is Penetration Testing?

- 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

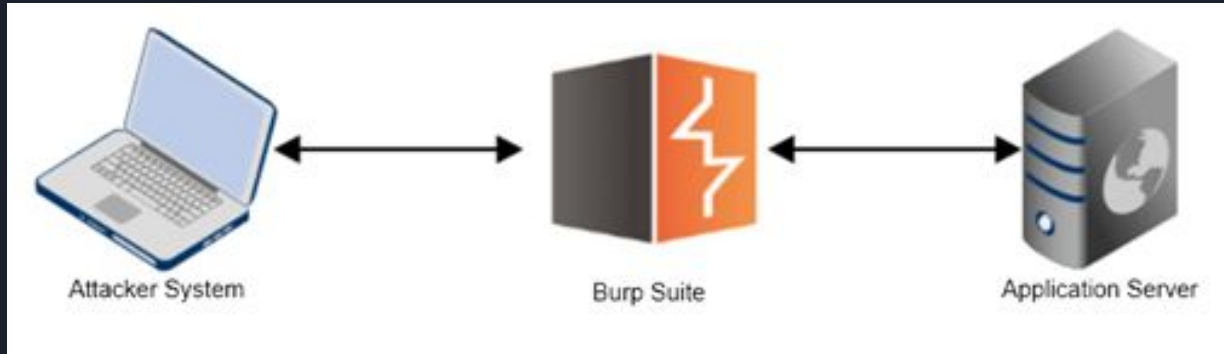
# Web application pentesting

- 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)

**Request**

Pretty Raw Hex

POST / HTTP/1.1

Host: titan.picoc.tf.net:64664  
Content-Length: 174  
Cache-Control: max-age=0  
Accept-Language: en-US,en;q=0.9  
Upgrade-Insecure-Requests: 1  
Origin: http://titan.picoc.tf.net:64664  
Content-Type: application/x-www-form-urlencoded  
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  
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://titan.picoc.tf.net:64664/  
Accept-Encoding: gzip, deflate, br  
Cookie: session=eyJjc3JmX3Rva2VuljoiOTESZTAyZWVmbWVY4NCU4OWZkNzkxYWNiNDY5ZWVlNjRjZjE5YTc5YyJ9.ZwLd8g.KCHHxLND174b9HGcQGBkEUCfXk  
Connection: keep-alive

csrf\_token=  
IjKx0WUwMmV1ZjVmODdlODlmZDc5MGRFjYjA2OWVjZTY0YzYwZmE3OWMi.ZwLd8g.SS  
jjma76DNVvrvBLaTZw-t0Hf2sfull\_name=l&username=l&phone\_number=l&  
city=l&password=l&submit=Register

**Response**

Pretty Raw Hex Render

HTTP/1.1 302 FOUND

Server: Werkzeug/3.0.1 Python/3.8.10  
Date: Sun, 06 Oct 2024 18:59:02 GMT  
Content-Type: text/html; charset=utf-8  
Content-Length: 207  
Location: /dashboard  
Vary: Cookie  
Set-Cookie: session=eyJjc3JmX3Rva2VuljoiOTESZTAyZWVmbWVY4NCU4OWZkNzkxYWNiNDY5ZWVlNjRjZjE5YTc5YyJ9.ZwLd8g.KCHHxLND174b9HGcQGBkEUCfXk; Path=/  
Connection: close

<!doctype html>  
<html lang=en>  
<title>  
Redirecting...  
</title>  
<h1>  
Redirecting...  
</h1>  
<p>  
You should be redirected automatically to the target URL: <a href  
="/dashboard">  
/dashboard  
</a>  
</p>  
If not, click the link.

**Request Type/Protocol**

**Request Headers**

**Request Body**

**Response Status Code**



# 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

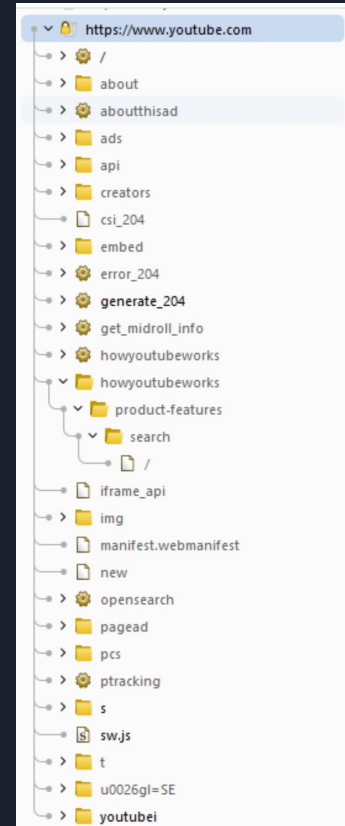


## Proxy (+ Demo)

- 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

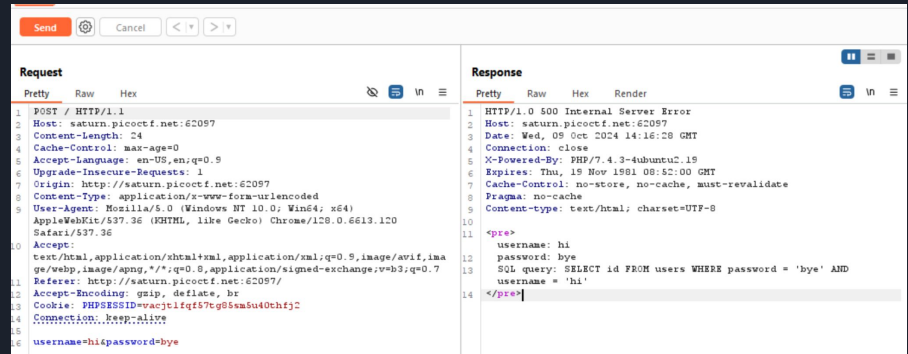
# Target

- 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 different inputs
  - Example repeater request:



The screenshot displays a network traffic analysis tool interface. At the top, there are buttons for 'Send', 'Cancel', and navigation arrows. The main area is divided into two panels: 'Request' on the left and 'Response' on the right. Both panels have tabs for 'Pretty', 'Raw', and 'Hex'. The 'Request' panel shows a POST request to 'http://saturn.picoctf.net:62097' with various headers and a body containing a SQL query. The 'Response' panel shows an HTTP 500 Internal Server Error response with a body containing a SQL query.

```
Request
Pretty Raw Hex
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=0.5
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 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120
11 Safari/537.36
12 Accept:
13 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
14 Referer: http://saturn.picoctf.net:62097/
15 Accept-Encoding: gzip, deflate, br
16 Cookie: PHPSESSID=wacltlfq657g85a5u40chtj2
17 Connection: keep-alive
18 username=hi&password=bye

Response
Pretty Raw Hex Render
1 HTTP/1.0 500 Internal Server Error
2 Host: saturn.picoctf.net:62097
3 Date: Wed, 09 Oct 2024 14:16:28 GMT
4 Connection: close
5 X-Powered-By: PHP/7.4.3-4ubuntu2.19
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Content-type: text/html; charset=UTF-8
10
11 <pre>
12 username: hi
13 password: bye
14 SQL query: SELECT id FROM users WHERE password = 'bye' AND
15 username = 'hi'
16 </pre>
```

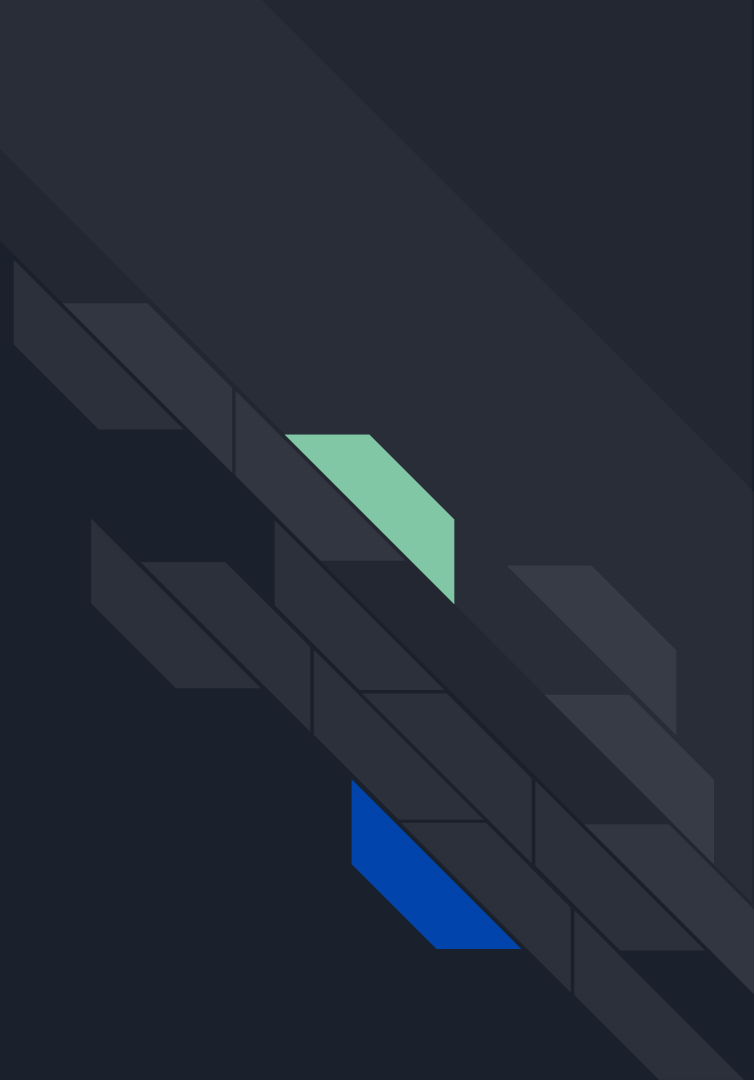
# Intruder

- 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 displays the Burp Suite Intruder tool interface. At the top, there are tabs for 'Positions', 'Payloads', 'Resource pool', and 'Settings'. The 'Positions' tab is active, showing a 'Choose an attack type' section with 'Attack type' set to 'Sniper'. Below this is the 'Payload positions' section, which includes a 'Target' field containing 'http://saturn.picocf.net:62097'. The main area shows a list of 16 lines of an HTTP request, with the last line being a payload template: 'username=\$user\$&password=\$pass\$'. The request details include: POST / HTTP/1.1, Host: saturn.picocf.net:62097, Content-Length: 24, Cache-Control: max-age=0, Accept-Language: en-US,en;q=0.9, Upgrade-Insecure-Requests: 1, Origin: http://saturn.picocf.net:62097, Content-Type: application/x-www-form-urlencoded, User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64), Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8, Referer: http://saturn.picocf.net:62097, Accept-Encoding: gzip, deflate, br, Cookie: PHPSESSID=vac4t1fq57tg05sm5u40chfj2, Connection: keep-alive.

```
1 POST / HTTP/1.1
2 Host: saturn.picocf.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.picocf.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;q=0.9,*/*;q=0.8
11 Referer: http://saturn.picocf.net:62097
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=vac4t1fq57tg05sm5u40chfj2
14 Connection: keep-alive
15
16 username=$user$&password=$pass$
```

# Juice Shop Challenges





# Challenges

- Put an additional product into another user's basket
- 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