



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!

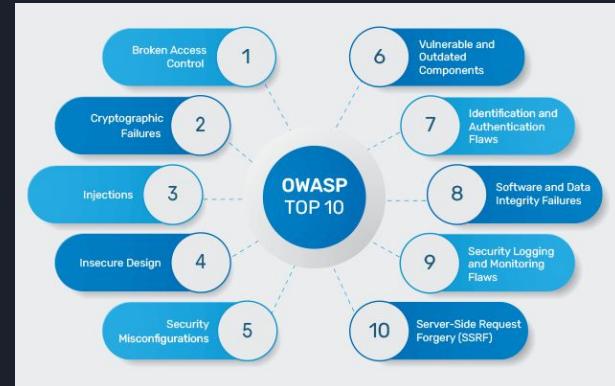


What is Penetration Testing?

- 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

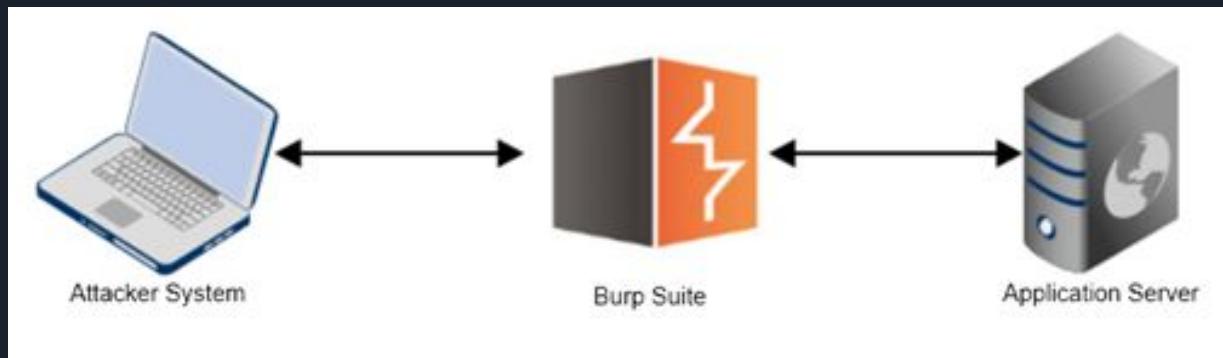
Web application pentesting

- 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):

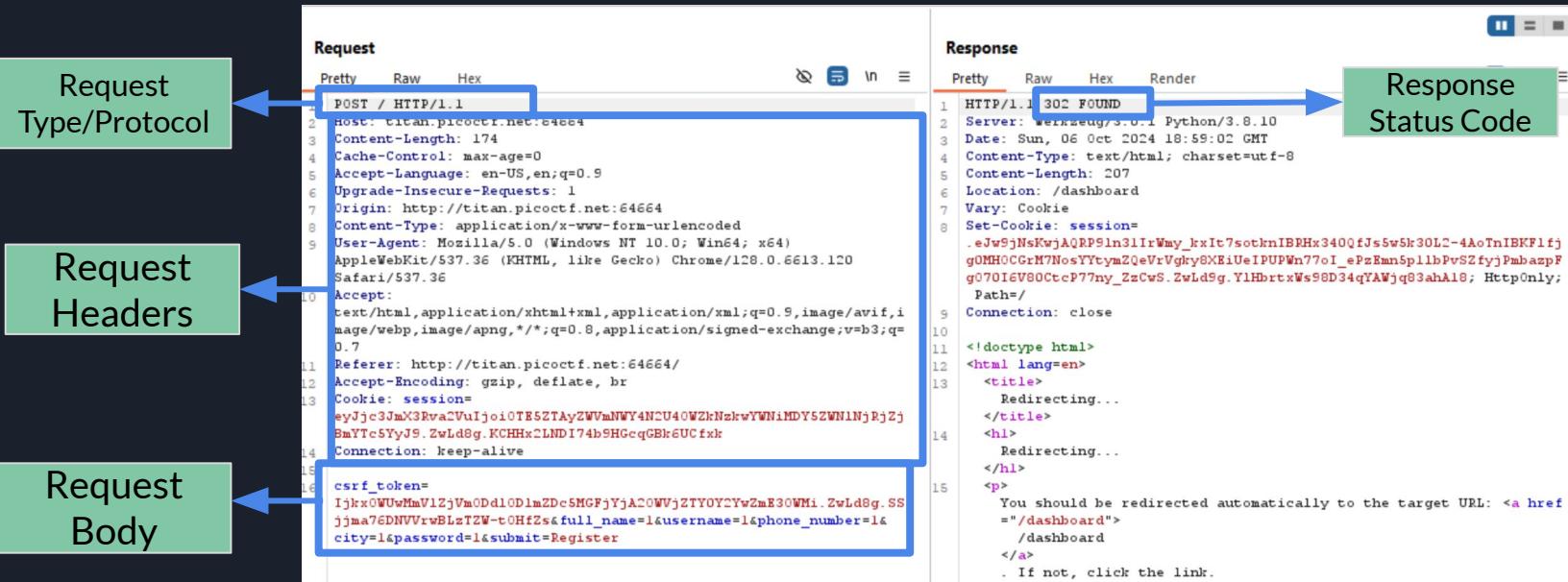


What is Burpsuite?

- 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)





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

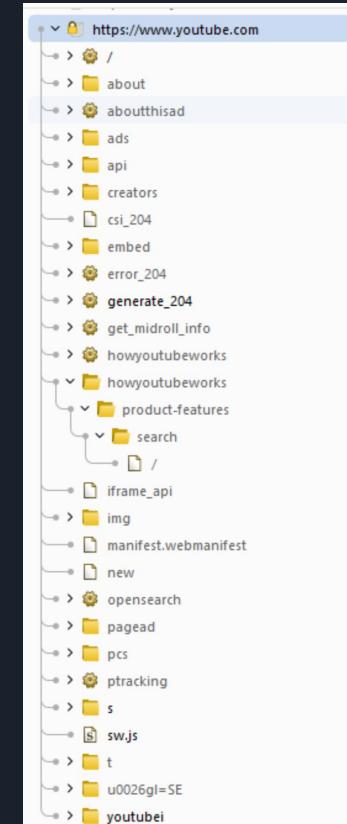


Proxy (+ Demo)

- 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

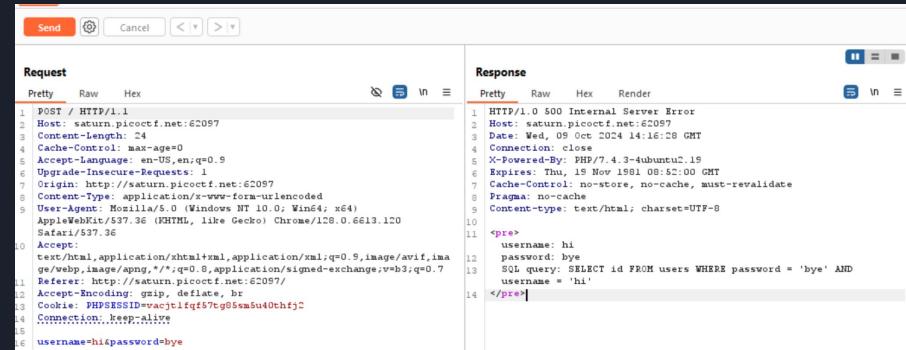
Target

- 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:

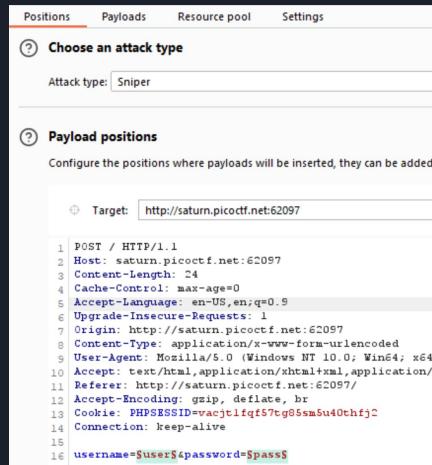


```
POST / HTTP/1.1
Host: saturn.picocft.net:62097
Content-Length: 24
Content-Type: application/json
Accept: */*
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
Origin: http://saturn.picocft.net:62097
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6613.120 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=vacj1fqf57tg05xm5u40thfj2
Connection: keep-alive
username:hi
password:bye
SQL query: SELECT id FROM users WHERE password = 'bye' AND username = 'hi'

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
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

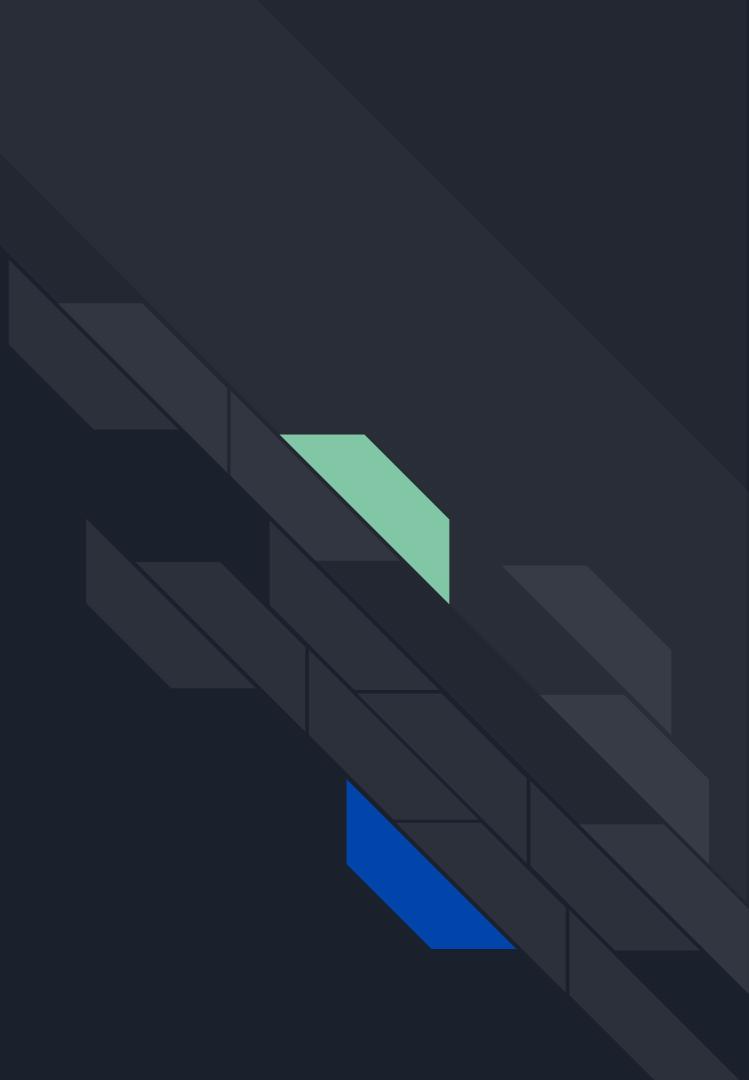
- Automate sending requests with modified parameters
 - “Send to intruder”
 - Makes brute-forcing attacks much easier
 - Can also be used for Denial of Service
- Specify payload locations/types
 - Example intruder request:



The screenshot shows the OWASP ZAP Intruder tool's payload configuration interface. The 'Payloads' tab is selected. Under 'Choose an attack type', 'Sniper' is selected. In the 'Payload positions' section, the 'Target' is set to 'http://saturn.picoctf.net:62097'. The 'Payload' field contains a multi-line HTTP POST request with a password parameter. The request is as follows:

```
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=vacl1f1gf57tg05sm5u40thfj2
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