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

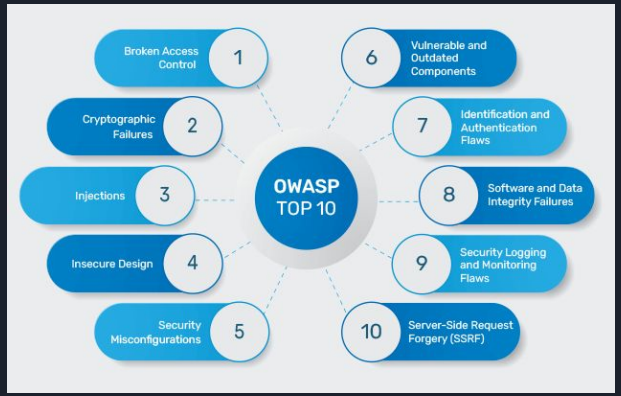
- Credits to the presentation go to John Poch
  - Senior Security Consultant for ivision
  - .cosmic_panda on discord
  - Be sure to ask him if you have any questions about the pentesting industry as a whole!

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

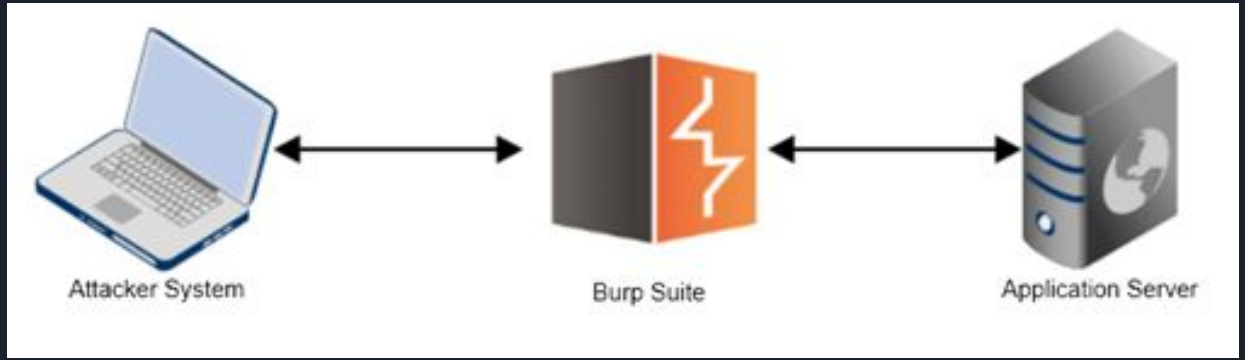
Web application pentesting

- 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

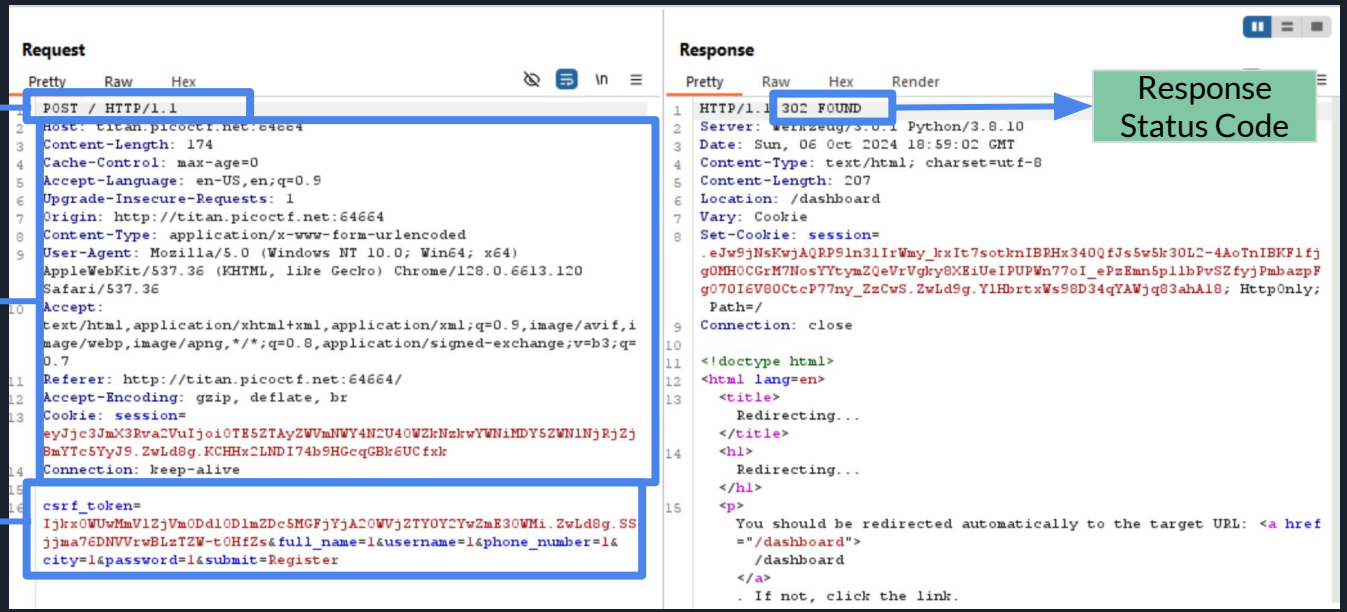


HTTP Request/Response Structure (as it appears in burp)

Request Type/Protocol

Request Headers

Request Body



Important Burpsuite Features

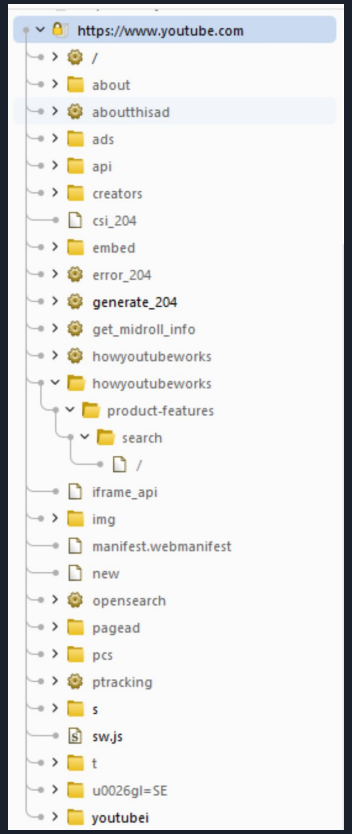
- Proxy: Intercept, view, and manipulate requests
- Target: Site mapping
- Repeater: Manual request modification
- Intruder: Automated request modification
- Other useful modules as well (Decoder, Organizer, etc)
    - But we'll focus on the first 4

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

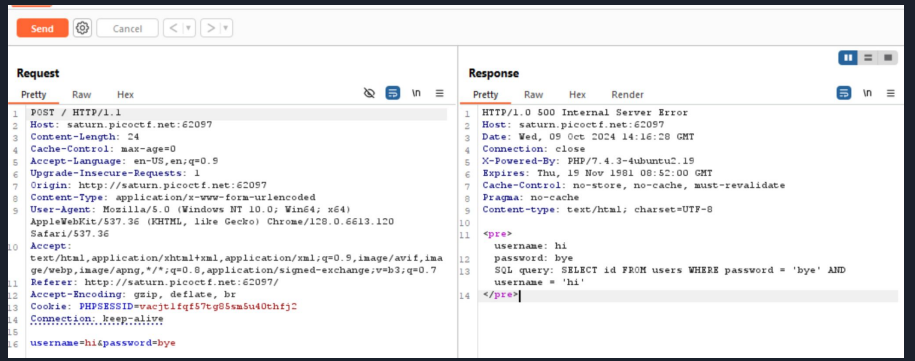
Target

- 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



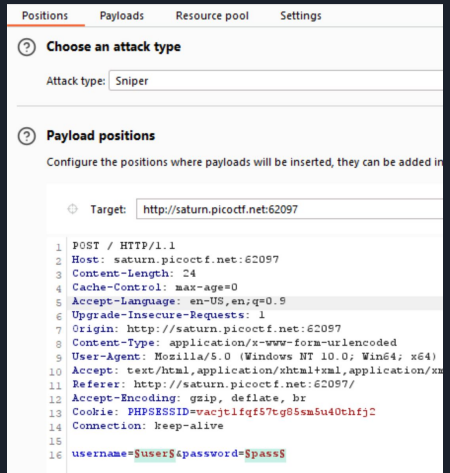
Repeater

- 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:



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:



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