

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](https://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

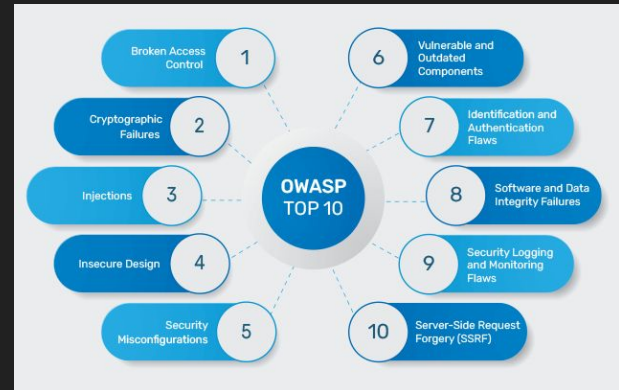
- These slides have been adapted from John Poch
 - Senior Security Consultant for ivision
 - .cosmic_panda on discord
 - Be sure to ask him if you have any questions about the pentesting industry as a whole!

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

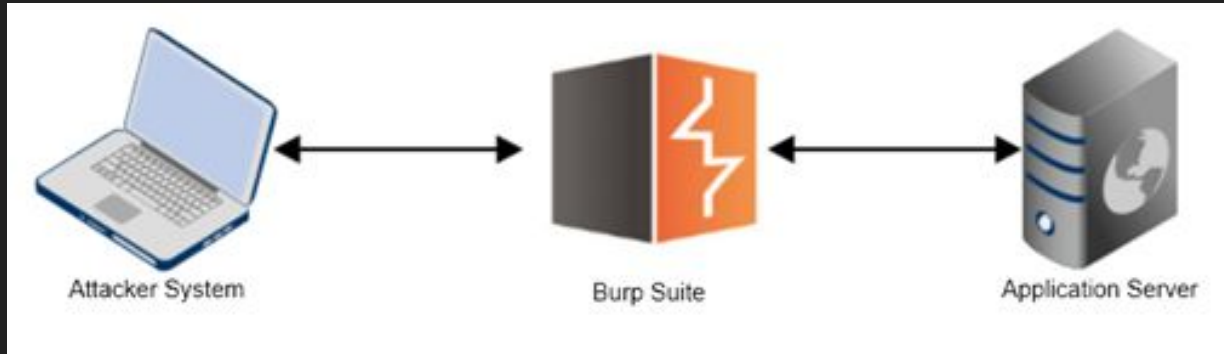
Web application pentesting

- 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)

Request
Type/Protocol

Request

Pretty	Raw	Hex
POST / HTTP/1.1		
Host: titan.picoctf.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.picoctf.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.picoctf.net:64664/		
Accept-Encoding: gzip, deflate, br		
Cookie: session=eyJjc3JmX3Rva2VuljoiOTESZTAyZWVmlWY4N2U4OWZkNzkxYWNlNDY5ZWVlNjRjZjBmYTc5YyJ9.ZwLd8g.KCHHxLNDI74b9HGcqGBkEUCfXk		
Connection: keep-alive		
csrf_token=IjKxWUwMmV1ZjVWm0Dd10D1mZDc5MGfjYjA20WVjZTY0Y2YwZmE30WMI.ZwLd8g.SSjjma76DNVvrvBLtZW-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=.eJwSjNsKwjAQRp9ln3lIrWmy_kxIt7sotkmIBRHx340QfJs5w5k30L2-4AoTnIBKFlfjg0MH0CGrM7NosYTYtmZQeVrVgky8XEiUeIPUPWn77oI_ePzEan5p1lbPvSZfyjPmbazpFg070I6V80CtcP77ny_ZzCwS.ZwLd8g.YlHbrtxWw98D34qYAWjq83ahA18; HttpOnly; Path=/			
Connection: close			
<!doctype html>			
<html lang=en>			
<title>			
Redirecting...			
</title>			
<h1>			
Redirecting...			
</h1>			
<p>			
You should be redirected automatically to the target URL: /dashboard			
			
. If not, click the link.			

Response
Status Code

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

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,i
  mage/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=
  eyJjc3JmX3Rva2VuIjo0TE5ZTAyZWVmbWY4N2U4OWZkNzkxYWNiNDY5ZWVlNjRjZj
  SmYtc5YyJ9.ZwLd8g.KCHHxLND174b9HGqQGBk6UCfxk
14 Connection: keep-alive
15
  csrf_token=
  IjxxQUwMmVlZjVwODdlODlmZDc5MGRFjYjA2OWVjZTY0Y2YwZmE3OWMi.ZwLd8g.SS
  jja76DNVrvwBLtZW-tCHf2sfull_name=l&username=l&phone_number=l&
  city=l&password=l&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=
  .eJwSjNsKwjAQRp9ln3lIrWmy_kxIt7sotkmIBRHx340QfJs5w5k30L2-4AoTnIBKFlfj
  gOMH0CGcM7NosYtYtmZQeVrVgky8XEiUeIPUPWn77oI_ePzEan5p1lbPvSZfyjPmbazpF
  g070I6V80CtcP77ny_ZzCwS.ZwLd8g.YlHbrtxWs98D34qYAWjq83ahA18; HttpOnly;
  Path=/
9 Connection: close
10
11 <!doctype html>
12 <html lang=en>
13 <title>
  Redirecting...
14 </title>
15 <h1>
  Redirecting...
16 </h1>
17 <p>
  You should be redirected automatically to the target URL: <a href
  ="/dashboard">
  /dashboard
18 </a>
19 . If not, click the link.
```

Request Headers

Request Body

Response Headers

Response 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

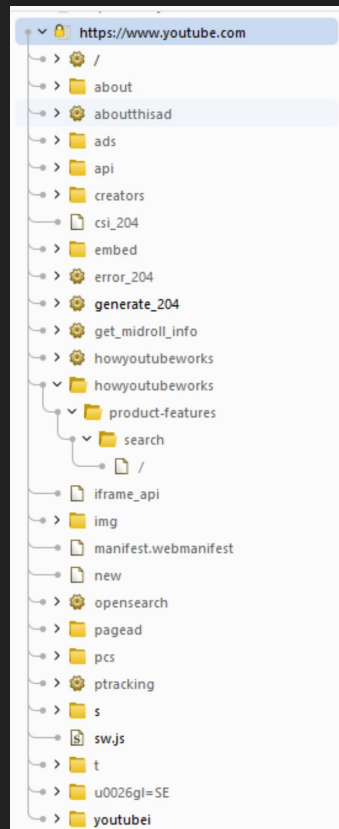
- Proxy: Intercept, view, and manipulate requests
- Target: Site mapping
- Repeater: Manual request modification
- Intruder: Automated request modification
- Other useful modules as well (Decoder, Organizer, etc)
 - But we'll focus on the first 4

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

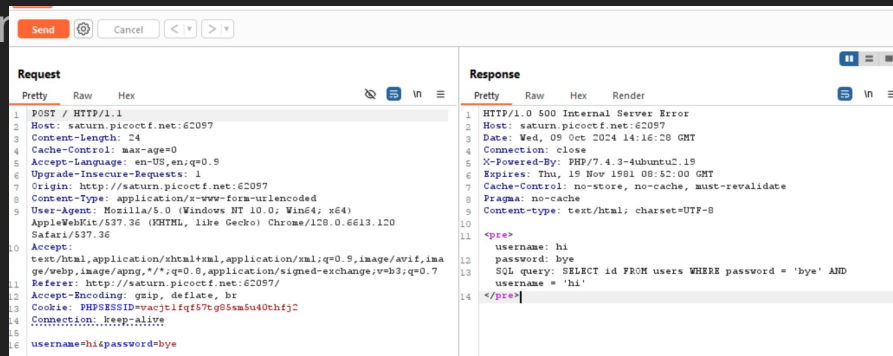
Target

- 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:



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 Burp Suite Intruder tool interface. At the top, there are tabs for 'Positions', 'Payloads', 'Resource pool', and 'Settings'. The 'Positions' tab is active. Below the tabs, there are two sections: 'Choose an attack type' and 'Payload positions'. In the 'Choose an attack type' section, the 'Attack type' is set to 'Sniper'. In the 'Payload positions' section, there is a 'Target' field with the value 'http://saturn.picoctf.net:62097'. Below the target field, there is a list of HTTP request details, including the method (POST), host (saturn.picoctf.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.picoctf.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.picoctf.net:62097/), accept encoding (gzip, deflate, br), cookie (PHPSESSID=vacjtlfq57tg05smSu40chfj2), connection (keep-alive), and the payload (username=\$user\$&password=\$pass\$).

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added in

Target: http://saturn.picoctf.net:62097

```
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;q=0.9,*/*;q=0.8
11 Referer: http://saturn.picoctf.net:62097/
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=vacjtlfq57tg05smSu40chfj2
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