

CANDIDATE STUDY PLAN

Penetration Testing Resources

Abstract

This document will compile the results of the resources that I have been tasked to complete. It will contain screenshots from following along with the Beginner Web Application Hacking course, a breakdown of chapter 21 from 'A Web Application Hacker's Methodology' and some details of the things that I found useful within the other chapters. I will also include research of OWASP and MITRE common weaknesses, Portswigger Burpsuite, NMAP network scanning, and mobile application security. Lastly, I will include progress that I make in Portswigger Academy and TryHackMe hands on labs.

Rory James Murphy
roryjamesmurphy@hotmail.com

Table of Contents

Web Application.....	2
Beginner Web Application Hacking Course	2
Week 1: Reconnaissance.....	2
Week 2: Enumeration and XSS.....	9
Week 3: XSS, SQL Injection and Broken Access Control	14
Week 4: XXE, Input Validation, Broken Access Control and More XSS.....	19
Week 5: SQL Injections and Live Bug Bounty Hunting.....	24
A Web Application Hacker's Handbook	26
OWASP Top 10	28
MITRE Common Weaknesses	29
Portswigger Burpsuite.....	29
Network Security	30
NMAP Network Scanning.....	30
TCP and UDP	30
Port Scanning	30
Service Identification	32
Hands on Labs	33
Portswigger Academy	33
TryHackMe	34
References	35

Web Application

Beginner Web Application Hacking Course

<https://www.youtube.com/watch?v=24fHLWXGS-M>

Week 1: Reconnaissance

Target Validation

Important to validate that your target is indeed the target you are required to test.

Tools: WHOIS, nslookup, dnsrecon

Finding Subdomains

Useful information can be obtained by publicly known subdomains of your acquired target.

Tools: Google Fu, dig, Nmap, Sublist3r, Bluto, crt.sh

Fingerprinting

Find out what systems are running and what OS models are in use.

Tools: Nmap, Wappalyzer, WhatWeb, BuiltWith, Netcat

Data Breaches

Viable information through info dumps such as passwords or account names.

Tools: HaveIBeenPwned

Add scope: .*\url\com\$

Filter: show only in scope and remove any out of scope websites.

Burp Suite Community Edition v2020.4 - Temporary Project

Scan results for www.irobot.com - Mozilla Firefox

Security Headers
Sponsored by **Probely**

Scan your site now

www.irobot.com

Security Report Summary

F

Site: https://www.irobot.com/
IP Address: 23.74.44.179
Report Time: 10 Jan 2022 05:44:04 UTC
Headers: Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

Supported By

Probely Ouch, you should work on your security posture immediately! Start Now

Header issues are low priority but still noteworthy to add into a pen testing report.

iRobot: Vacuum & Mop - iRobot.com Technology Profile - Mozilla Firefox

Log In / Signup for Free

IROBOT.COM

Technology Profile Detailed Technology Profile Meta Data Profile Relationship Profile Redirect Profile Company Profile

Analytics and Tracking

Rapleaf Rapleaf Usage Statistics - Download List of All Websites using Rapleaf Marketing automation tools with the necessary data to help brands keep their customers engaged. Now TowerData. Marketing Automation

Eloqua Eloqua Usage Statistics - Download List of All Websites using Eloqua Marketing automation provider. Marketing Automation

Content Square Content Square Usage Statistics - Download List of All Websites using Content Square ContentSquare provides digital experience insights platform that tries to help businesses understand how and why users are interacting with their app, mobile and web sites. A/B Testing · Personalization · Site Optimization

CQuotient CQuotient Usage Statistics - Download List of All Websites using CQuotient Cross channel retail personalization - now part of Demandware/Salesforce

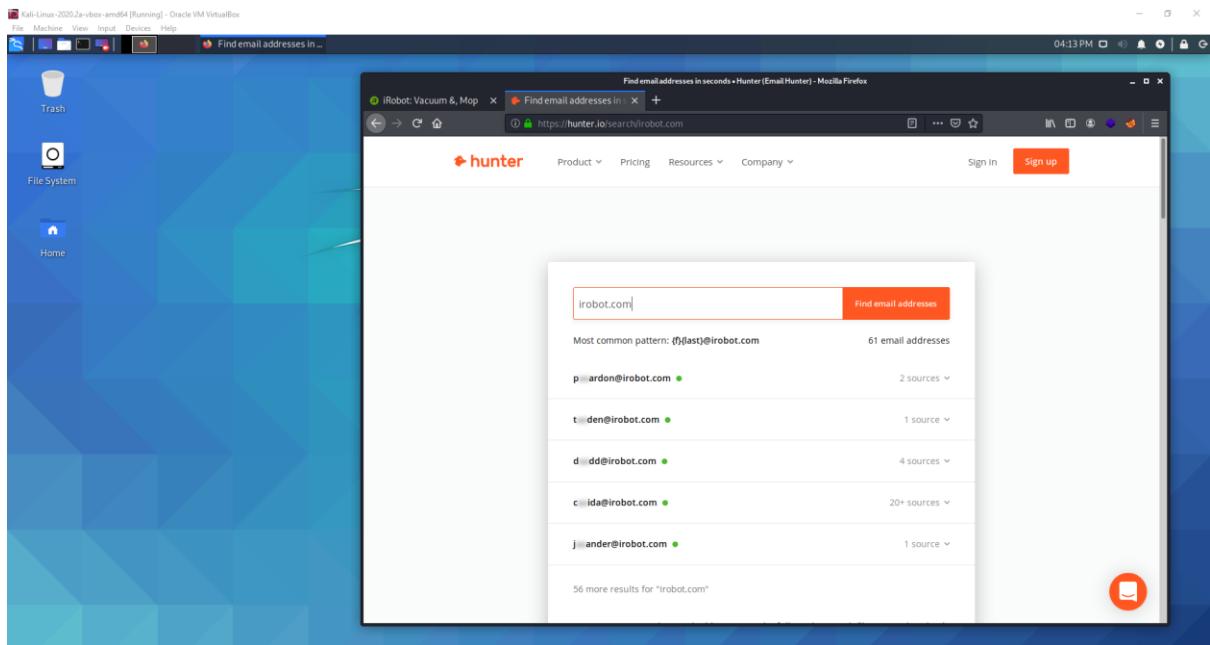
Profile Details Change Layout Last technology detected on 9th January 2022. We know of 178 technologies on this page and 125 technologies removed from irobot.com since 3rd January 2011. Link to this page.

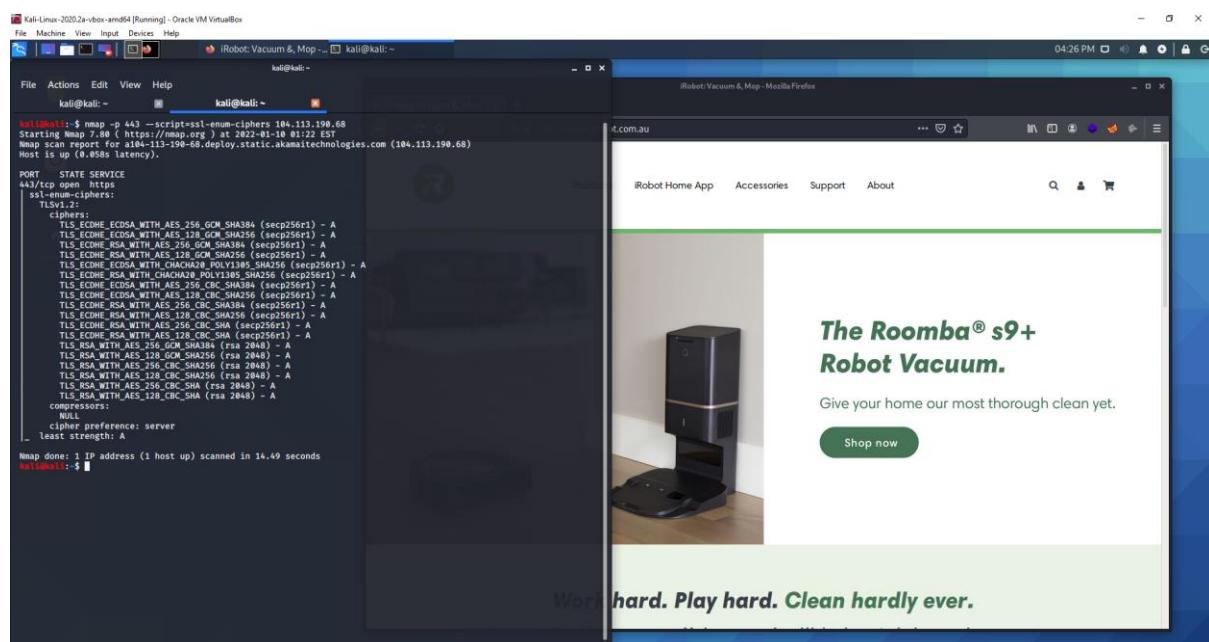
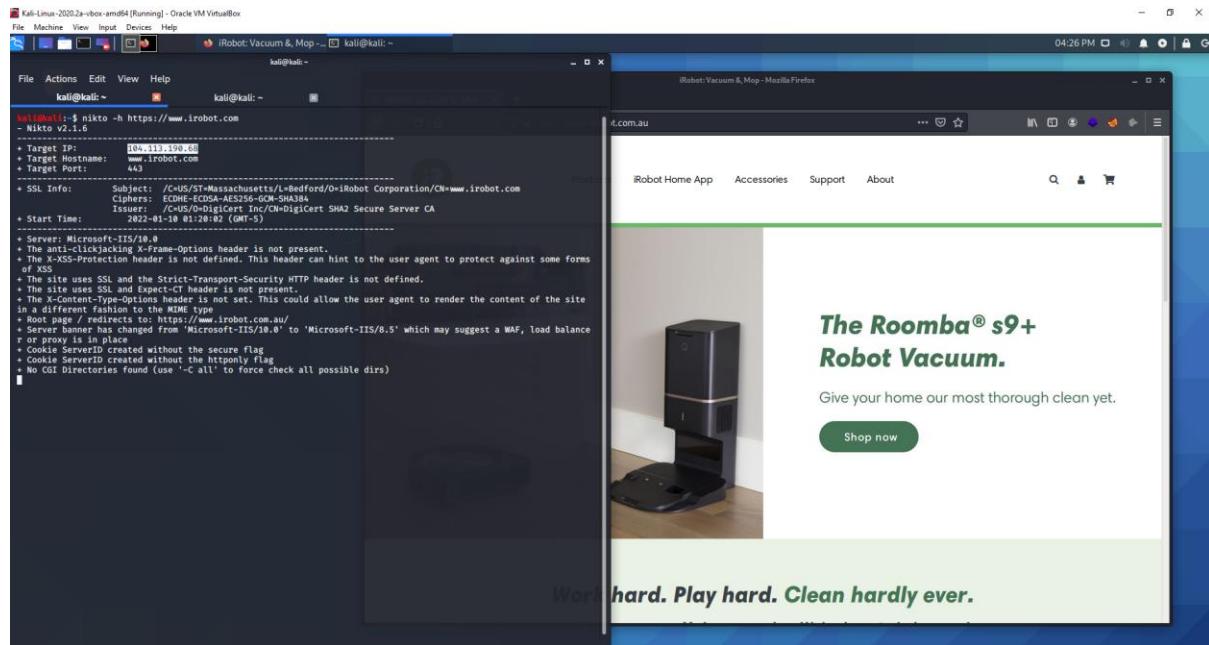
Add BuiltWith to Firefox for free! Get Lookups easily and quickly. Add to Firefox

Create Notification



This tutorial must be a bit dated by now, but I thought it was pretty funny that one of the tool domains got seized.





Ciphers are hard to break into but noteworthy in adding into a report if they report back with a low grade

Loud scanning is an ideal way to pen test because if it is not picked up by security systems, it can be included within the report to help fine tune anti-intrusion software.

Enumerate Juice Shop

No results found on crt.sh, hunter.io, or builtwith.com

Kali-Linux-2020.2a-vbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

OWASP Juice Shop - Mo. 1 Burp Suite Community E... kali@kali: ~

Burp Suite Community Edition v2021.10.3 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Site map Scope Issue definitions

Filter: Hiding not found items. Hiding CSS, image and general binary content. hiding 4xx responses: hiding empty folders

http://localhost:3000

	Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
1	http://localhost:3000	GET	/socket.io-44trans...		200	119				22:58:45 16.J...
2	api	GET	/api/Challenge?username=...		200	2402	HTML	OWASP Juice Shop		22:58:42 16.J...
3	assets	GET	/api/Quantum...		200	987	JSON			22:58:46 16.J...
4	main.js	GET	/assets/main/en.js		200	JSON			22:58:43 16.J...	
5	polyfills.js	GET	/assets/polyfills/en.js		200	28686	JSON			22:58:44 16.J...
6	rest	GET	/main.js		200	402560	script			22:58:43 16.J...
7	runtime.js	GET	/polyfills.js		200	39456	script			22:58:43 16.J...
8	socket.io	GET	/rest/admin/application...		200	353	JSON			22:58:45 16.J...
9	socket.io	GET	/rest/products/search/#...		200	13213	JSON			22:58:45 16.J...
10	socket.io	GET	/rest/categories/...		200	3645	JSON			22:58:45 16.J...
11	socket.io	GET	/socket.io/EIO=4&trans...		200	232	JSON			22:58:44 16.J...
12	socket.io	POST	/socket.io/EIO=4&trans...		200	121	text			22:58:46 16.J...

Request

HTTP/1.1 200 OK

1 GET /socket.io/1/websocket?e3b0c44298fc12878ccf83e45bf0a9c1 HTTP/1.1

2 Host: localhost:3000

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0

4 Accept: */*

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Connection: upgrade

8 Origin: http://localhost:3000

9 Sec-WebSocket-Key: oJhRqBfPwspErdrclJUW=

10 Sec-WebSocket-Version: 13

11 Cookie: language=en

12 Upgrade: websocket

13 Cache-Control: no-cache

14 Upgrade: websocket

15

Search... 0 matches

Response

HTTP/1.1 101 Switching Protocols

1 Upgrade: websocket

2 Connection: Upgrade

3 Sec-WebSocket-Accept: n%BeiTgyl2ic2bE3kgzP032tIE=

4

5

6

7

8

9

10

11

12

13

14

15

Search... 0 matches

Kali-Linux-2020.2a-vbox-and84 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@kali:~

Scan results for https://juice-shop.herokuapp.com/ - Mozilla Firefox

OWASP Juice Shop | OWASP Juice Shop | Scan results for https://juice-shop.herokuapp.com/ - Mozilla Firefox

11:56 AM

File Actions Edit View Help

kali@kali:~

kali@kali:~\$ nikto -h https://juice-shop.herokuapp.com

- Nikto v2.1.6

+ Target IP: 54.73.53.134

+ Target Hostname: juice-shop.herokuapp.com

+ Target Port: 443

+ SSL Info: Subject: /CN=*.herokuapp.com Ciphers: ECDHE-RSA-AES128-GCM-SHA256 Issuer: /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon

+ Message: Multiple IP addresses found: 54.73.53.134, 46.137.15.86

+ Start Time: 2022-01-13 20:49:42 (GMT-5)

+ Server: Cowboy

+ Retrieved via header: 1.1 vegur

+ Retrieved access-control-allow-origin header: *

+ The X-XSS-Protection header is not defined. This header can hint to the use of XSS.

+ Uncommon header 'feature-policy' found, with contents: payment 'self'

+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.

+ The site uses SSL and Expect-CT header is not present.

[...]

OWASP Juice Shop | OWASP Juice Shop | Scan results for https://juice-shop.herokuapp.com/ - Mozilla Firefox

Security Headers Sponsored by Probely

Home About Donate

Scan your site now

https://juice-shop.herokuapp.com/#/ Scan

Hide results Follow redirects

Security Report Summary

D

Site: https://juice-shop.herokuapp.com/#/ IP Address: 54.73.53.134 Report Time: 14 Jan 2022 01:46:14 UTC

Headers: ✓ Content-Type Options ✓ X-Frame-Options ✘ Strict-Transport-Security ✘ Content-Security-Policy ✘ Reference-Policy ✘ Permissions-Policy

Kali-Linux-2020.2a-vbox-and84 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@kali:~

OWASP Juice Shop - Mozilla Firefox

OWASP Juice Shop - Mozilla Firefox

01:49 PM

File Actions Edit View Help

kali@kali:~

kali@kali:~\$ nikto -h https://juice-shop.herokuapp.com

- Nikto v2.1.6

+ Target IP: 54.73.53.134

+ Target Hostname: juice-shop.herokuapp.com

+ Target Port: 443

+ SSL Info: Subject: /CN=*.herokuapp.com Ciphers: ECDHE-RSA-AES128-GCM-SHA256 Issuer: /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon

+ Message: Multiple IP addresses found: 54.73.53.134, 46.137.15.86, 54.228.192.176

+ Start Time: 2022-01-13 20:49:42 (GMT-5)

+ Server: Cowboy

+ Retrieved via header: 1.1 vegur

+ Retrieved access-control-allow-origin header: *

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.

+ Uncommon header 'feature-policy' found, with contents: payment 'self'

+ The site uses SSL and the Strict-Transport-Security header is not defined.

+ The site uses SSL and Expect-CT header is not present.

+ No robots.txt file found. (It is recommended to have one to disallow all possible dirs)

+ Entry '/ftp/' in robots.txt returned a non-forbidden or redirect HTTP code (503)

+ 'robots.txt' contains 1 entry which should be manually viewed.

+ Server is using a wildcard certificate: *.herokuapp.com

+ Server banner has changed from 'Cowboy' to 'heroku router' which may suggest a WAF, load balancer or proxy is in place

+ The Content-Encoding header is set to 'deflate' this may mean that the server is vulnerable to the BREACH attack

+ /herokuapp.jks: Potentially interesting archive/cert file found.

+ /juice-shop.pem: Potentially interesting archive/cert file found.

+ /backup.tar.gz: Potentially interesting archive/cert file found.

+ /juice-shop.tar.gz: Potentially interesting archive/cert file found.

+ /com.cer: Potentially interesting archive/cert file found.

+ /herokuapp.tar.b2z: Potentially interesting archive/cert file found.

+ /herokuapp.tar.gz: Potentially interesting archive/cert file found.

+ /juice-shopherokuappcpcm.jks: Potentially interesting archive/cert file found.

+ /juice-shop.tar.b2z: Potentially interesting archive/cert file found.

+ /juice-shopherokuappcpcm.pem: Potentially interesting archive/cert file found.

+ /juice-shopherokuappcpcm.tar.gz: Potentially interesting archive/cert file found.

+ /com.tar: Potentially interesting archive/cert file found.

+ /com.pem: Potentially interesting archive/cert file found.

+ /juice-shopherokuappcpcm.war: Potentially interesting archive/cert file found.

+ /juice-shopherokuappcpcm.tar.gz: Potentially interesting archive/cert file found.

+ /site.jks: Potentially interesting archive/cert file found.

+ /juice-shop_herokuapp.com.war: Potentially interesting archive/cert file found.

+ /site.tar.lzma: Potentially interesting archive/cert file found.

+ /backup.tar.lzma: Potentially interesting archive/cert file found.

+ /juice-shop.herokuapp.com.tar: Potentially interesting archive/cert file found.

OWASP Juice Shop - Mozilla Firefox

Welcome to OWASP Juice Shop!

Being a web application with a vast number of intended security vulnerabilities, the **OWASP Juice Shop** is supposed to be the opposite of a best practice or template application for web developers: It is an awareness, training, demonstration and exercise tool for security risks in modern web applications. The **OWASP Juice Shop** is an open-source project hosted by the non-profit Open Web Application Security Project (OWASP) and is developed and maintained by volunteers. Check out the link below for more information and documentation on the project.

Apple Juice (1000ml) 1.99¤

Banana Juice (1000ml) 1.99¤

https://owasp-juice.shop

Help getting started Dismiss

Best Juice Shop Salesman Artwork 5000¤

Carrot Juice (1000ml) 2.99¤

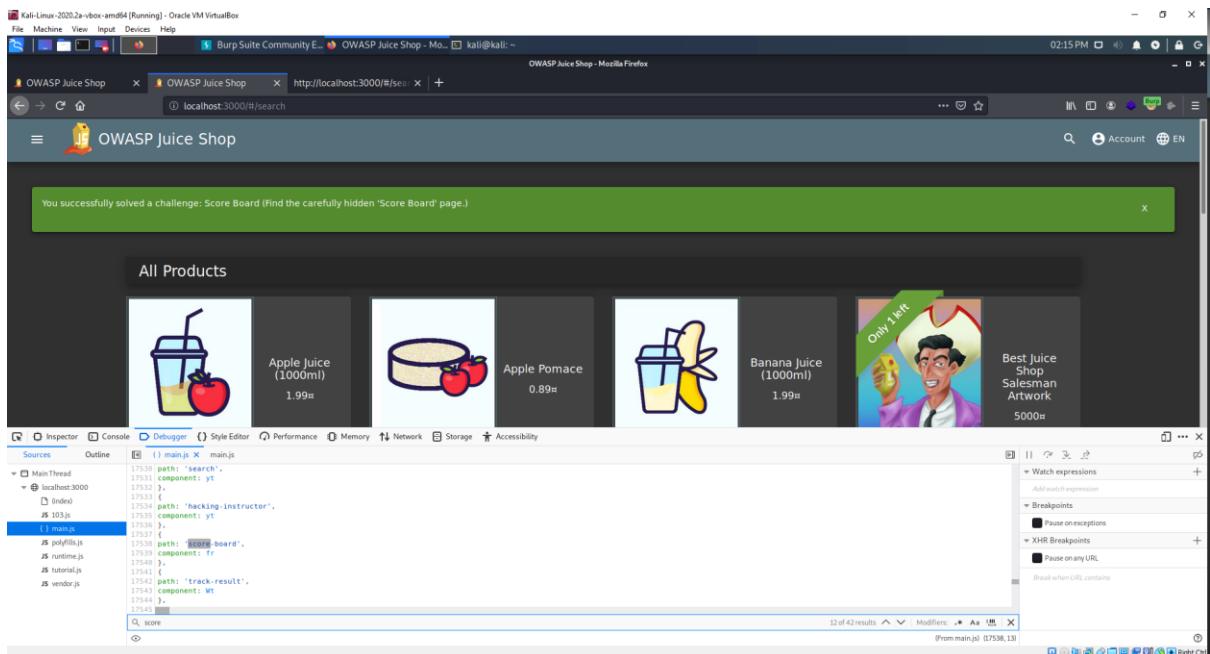
Eggfruit

This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

Me want it!

The figure shows a dual-monitor setup. The left monitor displays a Kali Linux terminal window titled 'File Machine View Input Devices Help' and 'OWASP Juice Shop - Mozilla Firefox'. The terminal window shows a network scan with the command 'nmap -p 3000 -A -T4 10.0.2.15'. It lists several open ports, including port 3000 (HTTP) which is described as 'Probably the most modern and sophisticated insecure web application'. The right monitor displays a Mozilla Firefox browser window titled 'OWASP Juice Shop - Mozilla Firefox' with the URL 'https://owasp-juice.shop'. The page title is 'Welcome to OWASP Juice Shop!'. It features a grid of juice products: Apple Juice (1000ml) at 1.99, Banana Juice (1000ml) at 1.99, Best Juice Shop Salesman Artwork (5000x), Carrot Juice (1000ml) at 2.99, and Eggfruit. A modal dialog box is visible, containing a 'Help getting started' button and a 'Dismiss' button.

Week 2: Enumeration and XSS



The screenshot shows a Kali Linux VM interface. At the top, there's a terminal window titled 'Kali-Linux-2020.2a-vbox-amd64 [Running] - Oracle VM VirtualBox'. Below it is a Firefox browser window with multiple tabs. One tab is titled 'listing directory /ftp - Mozilla Firefox' and shows a file list for the '/ftp' directory. Another tab is 'OWASP Juice Shop - Mozilla Firefox' showing a dashboard with various challenges. A third tab is 'listing directory /ftp - Mozilla Firefox' showing the same file list. A fourth tab is 'http://localhost:3000/#/se...'. The main content area displays a file browser interface for the '/ftp' directory. Inside, there's a 'mousepad' application window showing a document titled '# Planned Acquisitions' with sensitive information about company plans to acquire competitors.

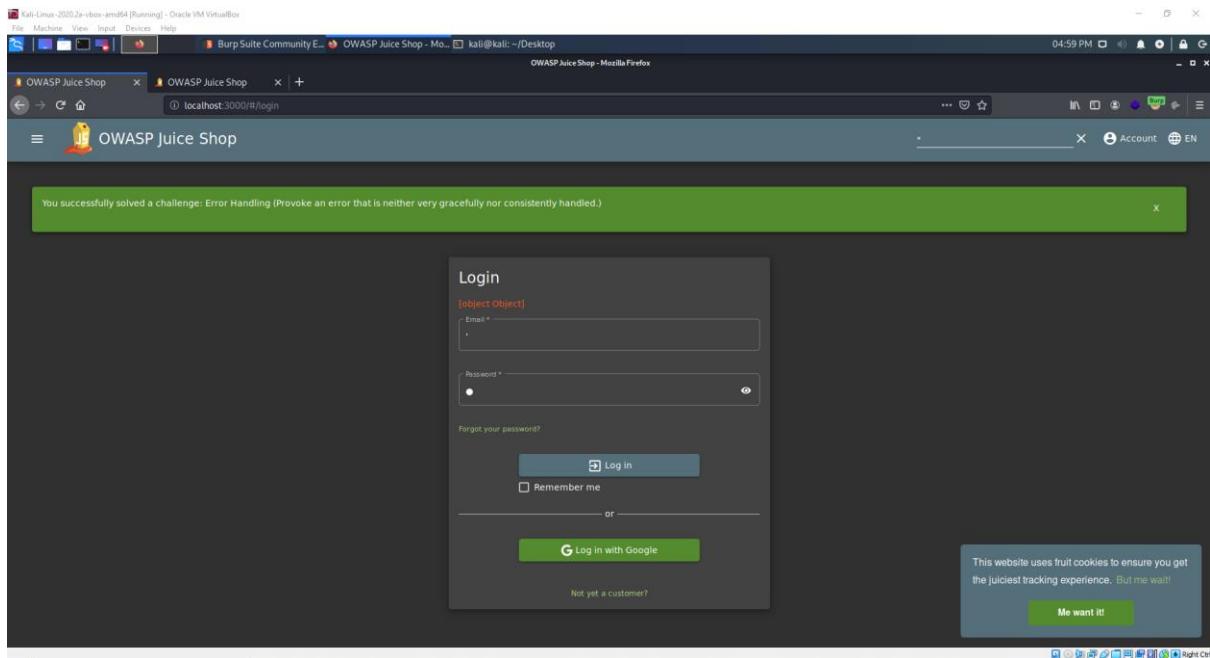
By filling in the user creation form, but returning to the first instance to change the password, Juice Shop does not register that you have two different passwords written in the form and completes the challenge; Repetitive Registration: Follow the DRY principle while registering a user.

```

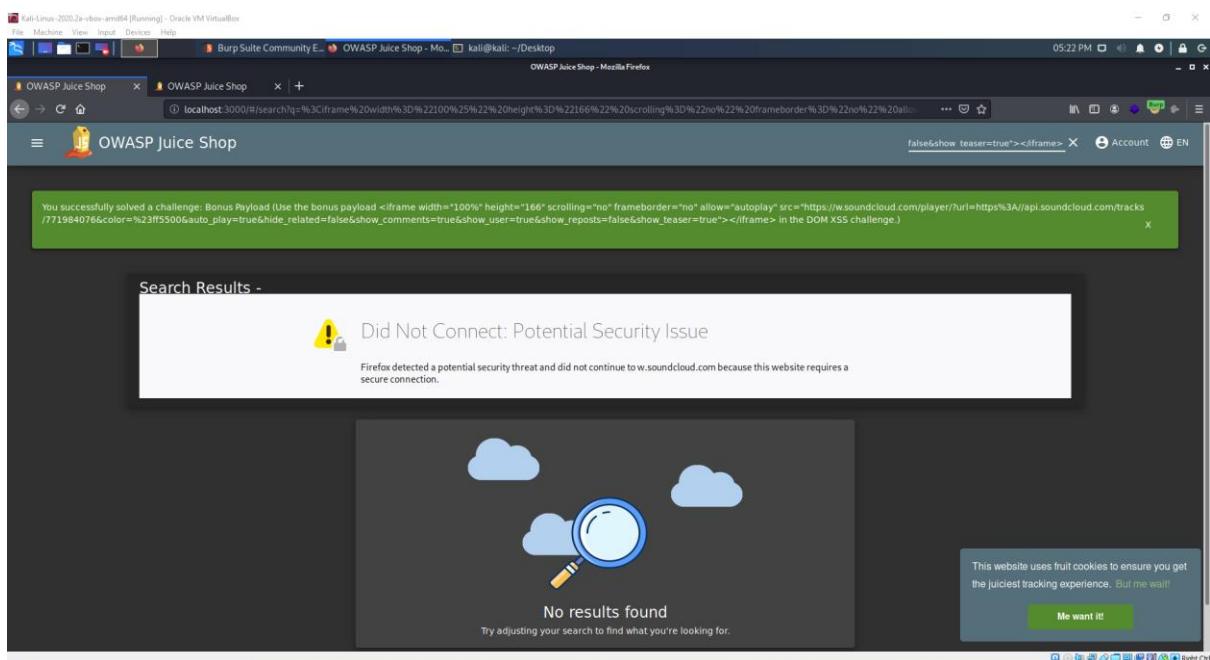
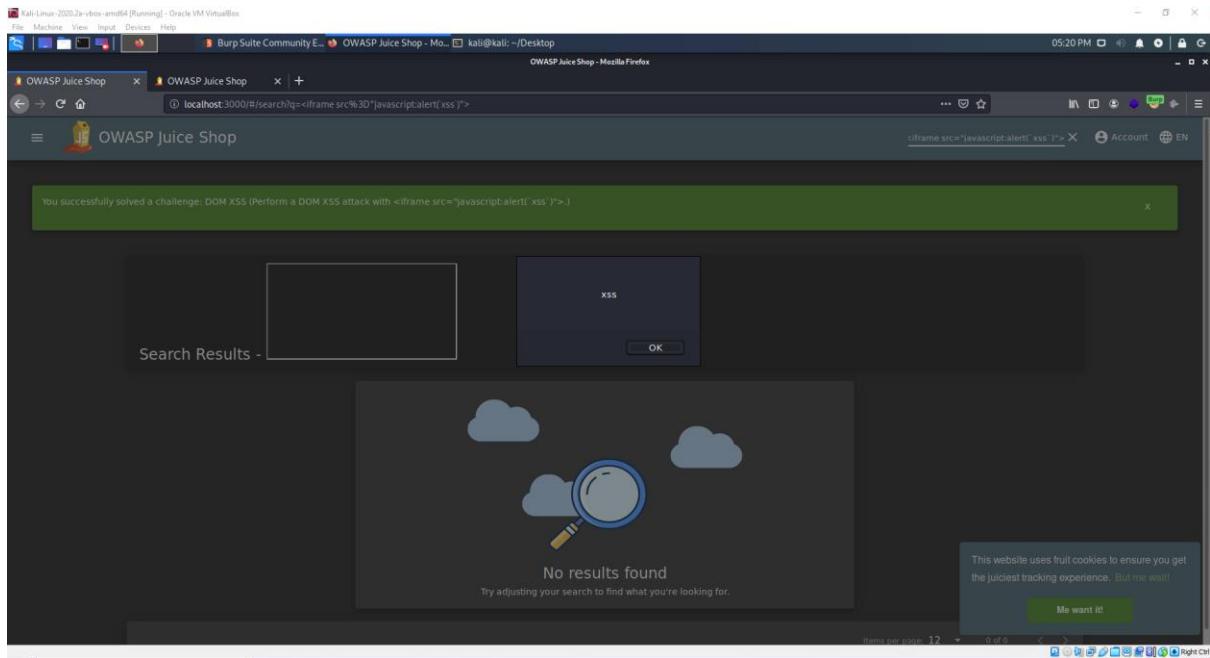
POST /api/Feedbacks/1 HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost:3000/
Content-Type: application/json
Content-Length: 72
Connection: close
Cookie: language=en; welcomebanner_status=dismiss; continueCode=3eVn1B3mPEPYlzz6jelolwH42jNc3nC2pOKYe6B7yrsDV95ZkO9ne0
12
13 {
  "captchaId": "5",
  "captcha": "0",
  "rating": "Comment (anonymous)",
  "ratingInt": 0
}

```

I have an updated version of Juice-Shop installed on my machine so instead of manipulating the source code through inspect element, I went and edited the post method through burpsuite since they changed the 0 rating challenge from a form input to a slider.



Using an apostrophe can fuzz to determine whether SQL injection is possible.



You successfully solved a challenge: Privacy Policy (Read our privacy policy.)

Privacy Policy

Effective date: March 15, 2019

OWASP Juice Shop ("us", "we", or "our") operates the <http://localhost> website (the "Service").

This page informs you of our policies regarding the collection, use, and disclosure of personal data when you use our Service and the choices you have associated with respect to your personal data.

We use your data to provide and improve the Service. By using the Service, you agree to the collection and use of information in accordance with this policy. Policies used in this Privacy Policy have the same meanings as in our Terms and Conditions, accessible from <http://localhost>.

A. Information Collection And Use

We collect several different types of information for various purposes to provide and improve our Service to you.

A1. Types of Data Collected

A1.1 Personal Data

While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you ("Personal Data"). Personally identifiable information may include, but is not limited to:

- Email address
- Address, State, Province, ZIP/Postal code, City
- Cookies and Usage Data

A1.2 Usage Data

We may also collect information how the Service is accessed and used ("Usage Data"). This Usage Data may include information such as your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the page or our Service that you visit, the time and date of your visit, the time spent on those pages, unique device identifier, and other diagnostic data.

You successfully solved a challenge: Reflected XSS (Perform a reflected XSS attack with <iframe src="javascript:alert('xss')">.)

xss

OK

Search Results -

Expected Delivery

Ordered products

Product	Price	Quantity	Total Price
Bonus Points Earned: {{bonus}}			
(The bonus points from this order will be added 1:1 to your wallet & fund for future purchases!)			

This website uses fruit cookies to ensure you get the juiciest tracking experience... But me want!

Me want it!

XSS Prevention

Encoding

<script>

< == <

<script>

Filtering

Instead of replacing the script, it will remove them.

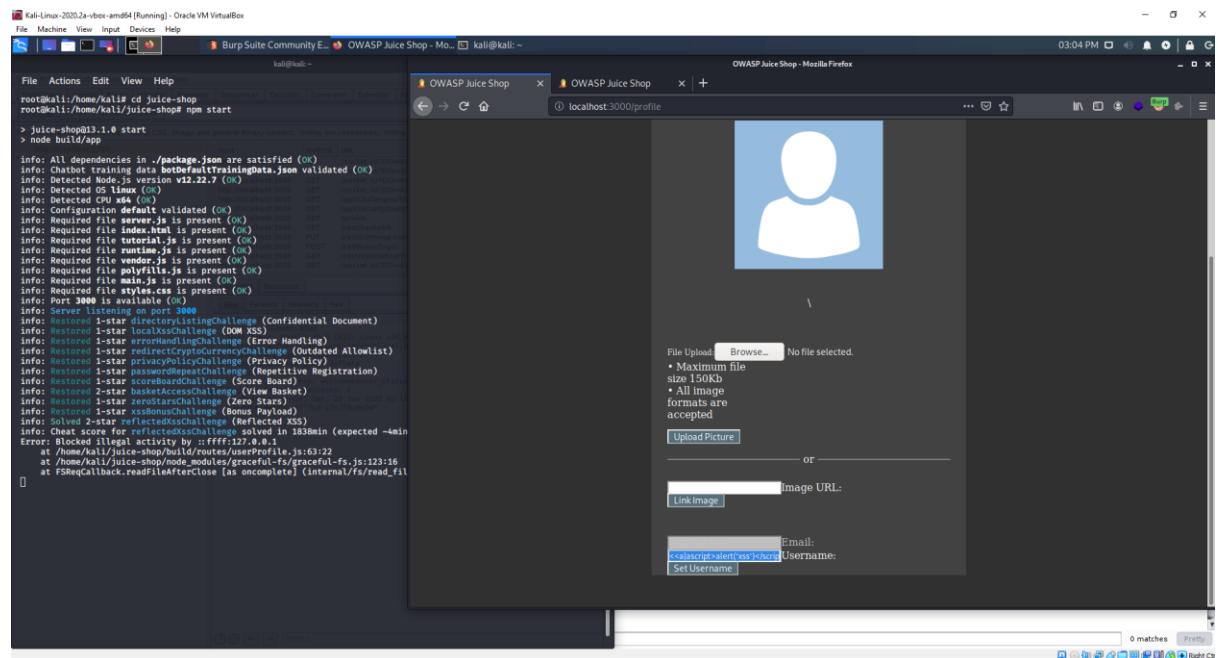
Validation

Comparison against a list or payloads. Can completely remove script tags.

Sanitisation

A mixture of all the previous methods of control.

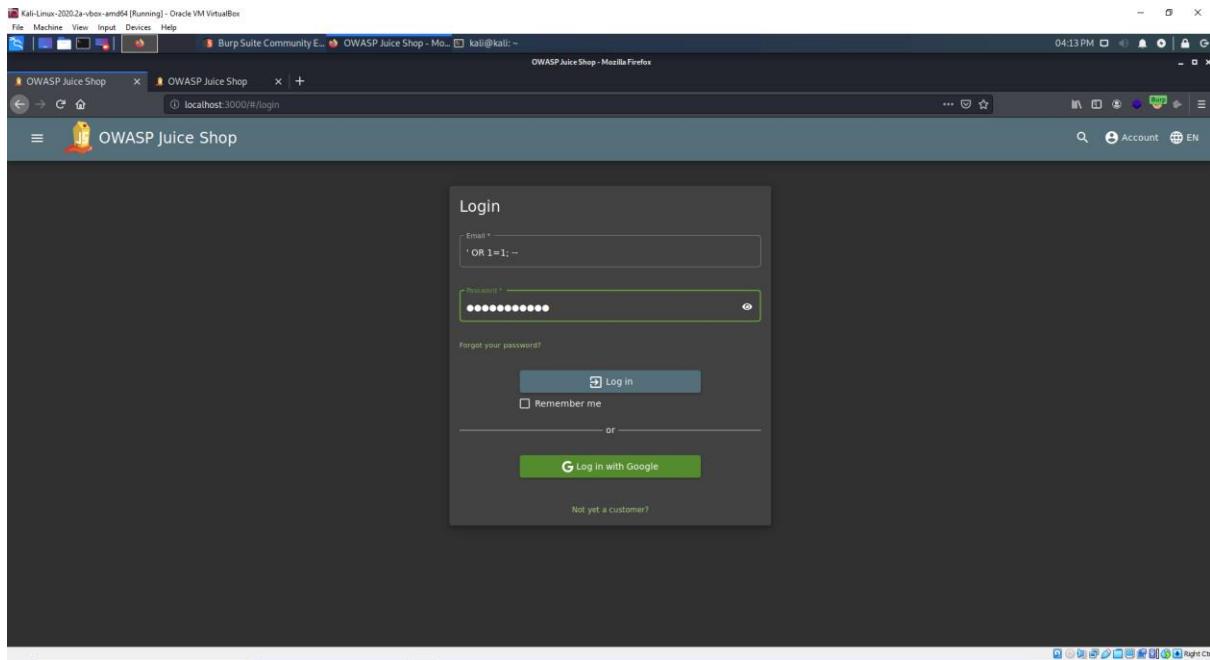
Week 3: XSS, SQL Injection and Broken Access Control



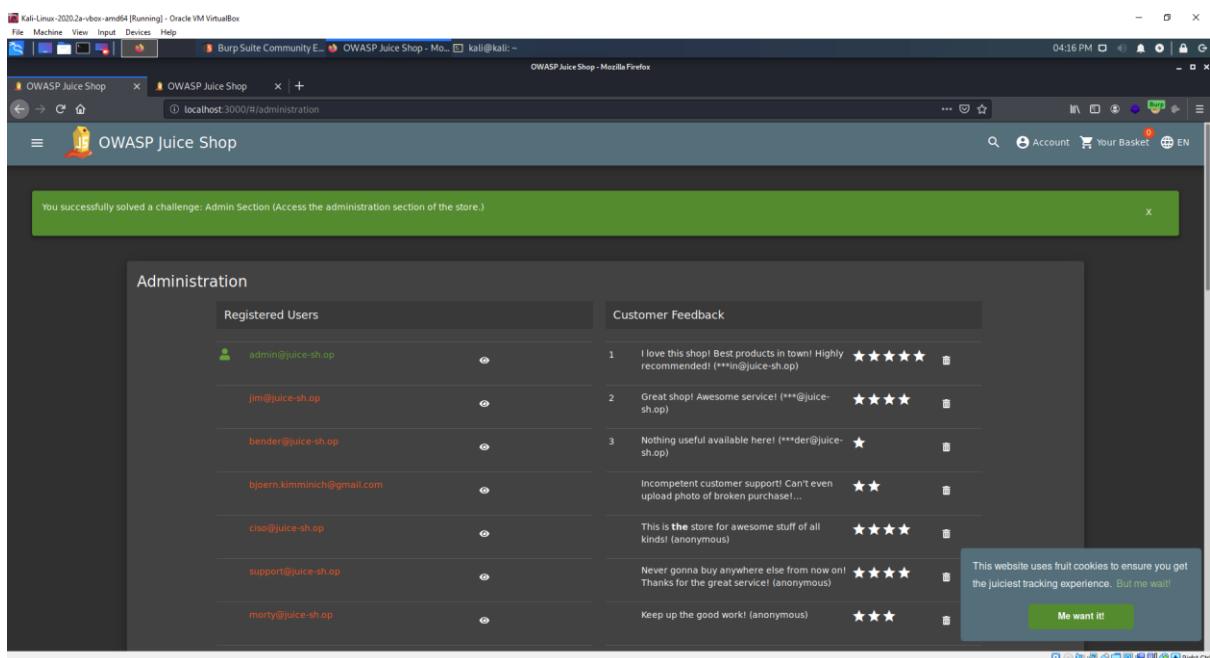
Can use a bitwise operation to bypass some sanitisation ie. a|a, a^a, a&a

Changing the buyer id (bid) in the session storage can allow you to view another customer's cart

Application allows for the upload of xml files, which can be used for xxe attacks



SQL injection to log in as the first user in the database which happens to be the admin account.



Admin page found through url /administration

Can also be found through debugger searching for admin pages.

The screenshot shows the OWASP Juice Shop administration page. On the left, a sidebar lists 'Registered Users' with entries for admin@juice-shop, jim@juice-shop, jbender@juice-shop, bjoern.kimminich@gmail.com, ciso@juice-shop, support@juice-shop, and morty@juice-shop. On the right, a 'Customer Feedback' section displays three reviews:

- Review 2: 'Great shop! Awesome service!' (admin@juice-shop) - ★★★★
- Review 3: 'Nothing useful available here!' (jim@juice-shop) - ★
- Review 4: 'Incompetent customer support! Can't even upload photo of broken purchase!' (jbender@juice-shop) - ★★
- Review 5: 'This is the store for awesome stuff of all kinds!' (anonymous) - ★★★★
- Review 6: 'Never gonna buy anywhere else from now on!' (ciso@juice-shop) - ★★★★
- Review 7: 'Thanks for the great service!' (anonymous) - ★★★★
- Review 8: 'Keep up the good work!' (anonymous) - ★★★

A green banner at the top of the main content area says: 'You successfully solved a challenge: Five-Star Feedback (Get rid of all 5-star customer feedback.)'. A tooltip on the right side of the page states: 'This website uses fruit cookies to ensure you get the juiciest tracking experience. But me waff! Me want it!'. The browser status bar shows 'localhost:3000/#/administration'.

Can use admin privileges to remove 5 star reviews.

The screenshot shows the Burp Suite Community Edition v2020.4 - Temporary Project. The 'Intruder' tab is selected. In the 'Payload Positions' section, there is one payload position defined for the 'Sniper' attack type. The payload is a JSON object containing a login attempt:

```

1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:3000/
8 Content-Type: application/json
9 Content-Length: 40
10 Connection: close
11 Cookie: language=en; welcomebanner_status=dismiss; continueCode=35jaReBLY9dvJtVUHMrzTLF010v1ExHP9tLvcxZ54phMyh0QkxaPj2wZl
12 {
13     "email": "admin@juice-shop",
14     "password": "$1$29450"
15 }

```

The 'start attack' button is visible at the top right of the intruder panel. The browser status bar shows 'localhost:3000/#/administration'.

Using intruder to bruteforce the admin password

| Request | Payload | Status | Error | Timeout | Length | Comment |
|---------|------------|--------|-------|---------|--------|---------|
| 0 | | 401 | | | 362 | |
| 1 | admin | 401 | | | 362 | |
| 2 | admin1 | 401 | | | 362 | |
| 3 | admin2 | 401 | | | 362 | |
| 4 | admin3 | 401 | | | 362 | |
| 5 | admin123 | 200 | | | 1169 | |
| 6 | admin1234 | 401 | | | 362 | |
| 7 | admin12345 | 401 | | | 362 | |

Check status codes and length for outliers. Also check responses for “Invalid email OR password” for enumeration in professional tests. This is good security practice. Can also grep for invalid responses.

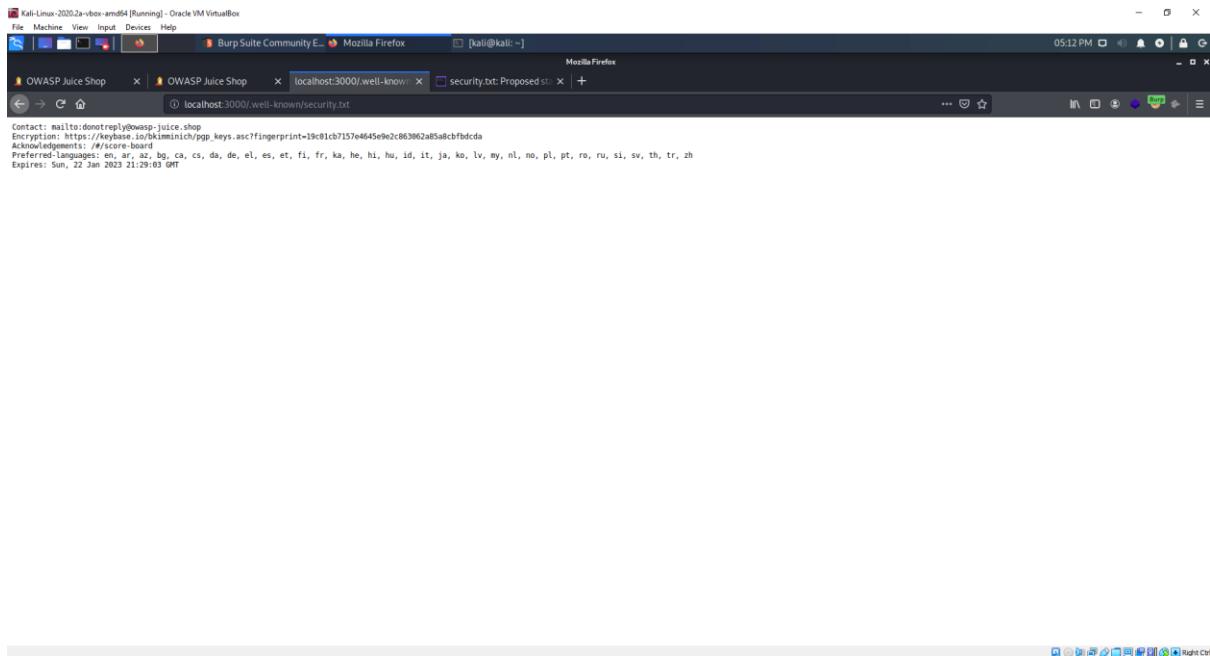
of your favorite mine's my dog mr.
noodles they don't

Rapper Who Is Very Concerned With Password Security

1,346,057 views • Oct 28, 2014

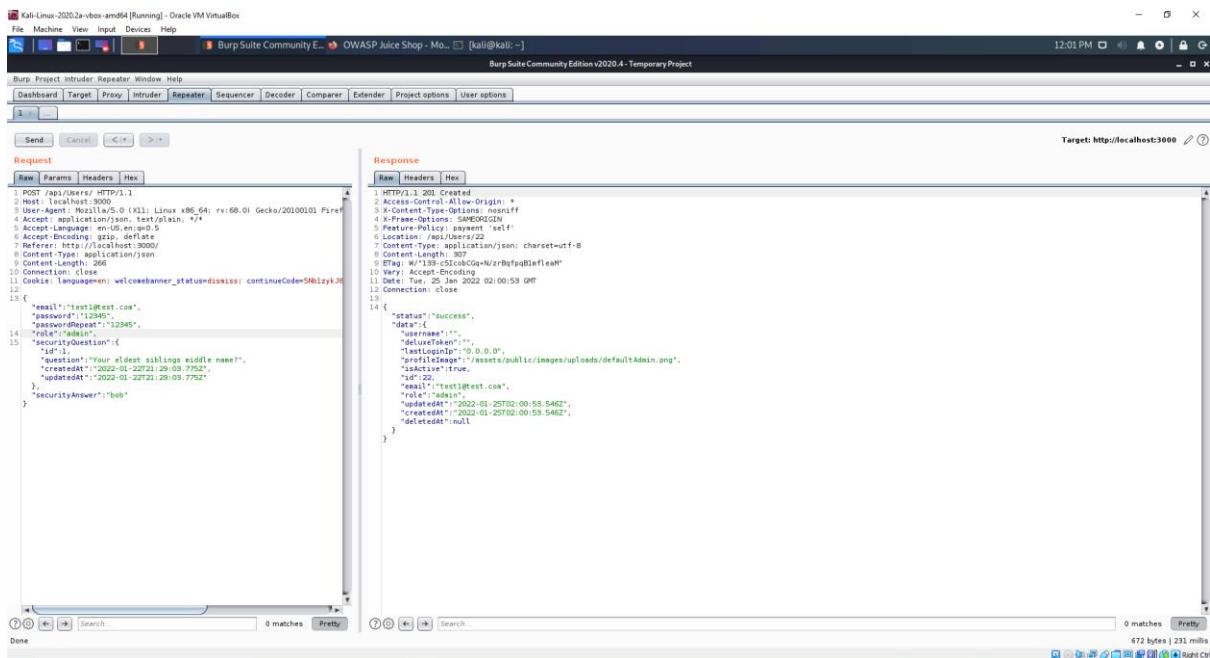
30K DISLIKE SHARE SAVE ...

Username: mc.safesearch@juice-sh.op Password: Mr. N00dles



Following the instructions at <https://securitytxt.org/>

Week 4: XXE, Input Validation, Broken Access Control and More XSS



Adding “role” : “admin” in the repeater will give the new user admin privileges.

Can bypass the captcha using the correct parameters in repeater as each captcha has a captcha ID tied to it.

Adding an additional BasketId in repeater can allow you to add another item to another user's basket.

```

Request
Raw Params Headers Hex
1 PUT /api/BasketItem/10 HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:3000/
8 Authorization: Bearer eyJhbGciOiJIWkIiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMIOiJzdmMjZKNl1wIzQF0YS16eyJpZC16HIsInVzZXJvYmQlIjoiIiwidWI
9 Content-Type: application/json
10 Content-Length: 17
11 Connection: close
12 Cookie: language=en; welcomebanner_status=dismiss; continueCode=0EG06h3tpEUphzhTBFEl4auRtag1#fn@0; JtHOCKySKLUXy1MBh3v0eV; token
13
14 {
    "quantity": -200
}

```

```

Response
Raw Headers Hex
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 Vary: Accept-Encoding
4 X-Content-Type-Options: nosniff
5 X-Frame-Options: SAMEORIGIN
6 Feature-Policy: payment 'self'
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 139
9 ETag: W/"9f-5wA21qLwLdS8SevnFJvnWkgp0"
10 Vary: Accept-Encoding
11 Date: Tue, 25 Jan 2022 02:50:26 GMT
12 Connection: close
13
14 {
    "status": "success",
    "data": {
        "id": 10,
        "quantity": -200,
        "createdAt": "2022-01-25T02:50:57.629Z",
        "updatedAt": "2022-01-25T02:50:26.918Z",
        "BasketId": 8,
        "ProductId": 25
    }
}

```

Can manipulate the quantity through repeater to give a negative value that will instead pay the user.

```

Request
Raw Params Headers Hex
1 PUT /api/Product/1/reviews HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:3000/
8 Authorization: Bearer eyJhbGciOiJIWkIiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMIOiJzdmMjZKNl1wIzQF0YS16eyJpZC16HIsInVzZXJvYmQlIjoiIiwidWI
9 Content-Type: application/json
10 Content-Length: 17
11 Connection: close
12 Cookie: language=en; welcomebanner_status=dismiss; continueCode=ADYh2tasAUlh2TIPripNu0#3aijfJzS0N#7tk1cp0PL0; 2wJhaM#; token
13
14 {
    "message": "Not actual apply.",
    "author": "adekingjuice-shop"
}

```

```

Response
Raw Headers Hex
1 HTTP/1.1 200 Created
2 Access-Control-Allow-Origin: *
3 Vary: Accept-Encoding
4 X-Content-Type-Options: nosniff
5 X-Frame-Options: SAMEORIGIN
6 Feature-Policy: payment 'self'
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 137
9 ETag: W/"13-7V20BNTenIRAD0OkrrrIwv705c"
10 Vary: Accept-Encoding
11 Date: Tue, 25 Jan 2022 03:07:09 GMT
12 Connection: Close
13
14 {
    "status": "success"
}

```

Adding a comment has an author parameter so you can change it to post as whoever you like.

```

POST /api/Feedbacks/1 HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Encoding: gzip, deflate
Referer: http://localhost:3000/
Content-Type: application/json
Connection: close
Cookie: language=en; welcomebanner_status=dismiss; continueCode=dv2h3tBz3jprgh1TWPkSk1JuvAtq1HfFP95aqH0Rg7cpH9V2JzzVh0; tokenkey)0eXai01KV1QLCjhGc101J9uI1NlJ9..eyJzdgP0dHMI01JzdnMjZNeIiwlZ0P0S16eyJpZCE0M; IsInVzXJwY1Iiolliv1Zh1heWv101J0Z9H9M80ZDNOlaWebSI;
...
14 {
    "userId": 2,
    "captchaId": 4,
    "captcha": "42",
    "comment": "Feedback (***@test.com).",
    "rating": 2
}

```

You can alter the UserId parameter to post as someone else.

```

POST /api/Users/23 HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Encoding: gzip, deflate
Referer: http://localhost:3000/
Content-Type: application/json
Connection: close
Cookie: language=en; welcomebanner_status=dismiss; continueCode=SbNlzykJ0...
...
14 {
    "username": "admin",
    "password": "123456",
    "passwordRepeat": "123456",
    "role": "admin",
    "id": 23,
    "bio": "Your client skills are middle name",
    "streetAddress": "2022-01-22T21:29:09.775Z",
    "updatedAt": "2022-01-22T21:29:09.775Z"
},
"securityAnswer": "bab"
}

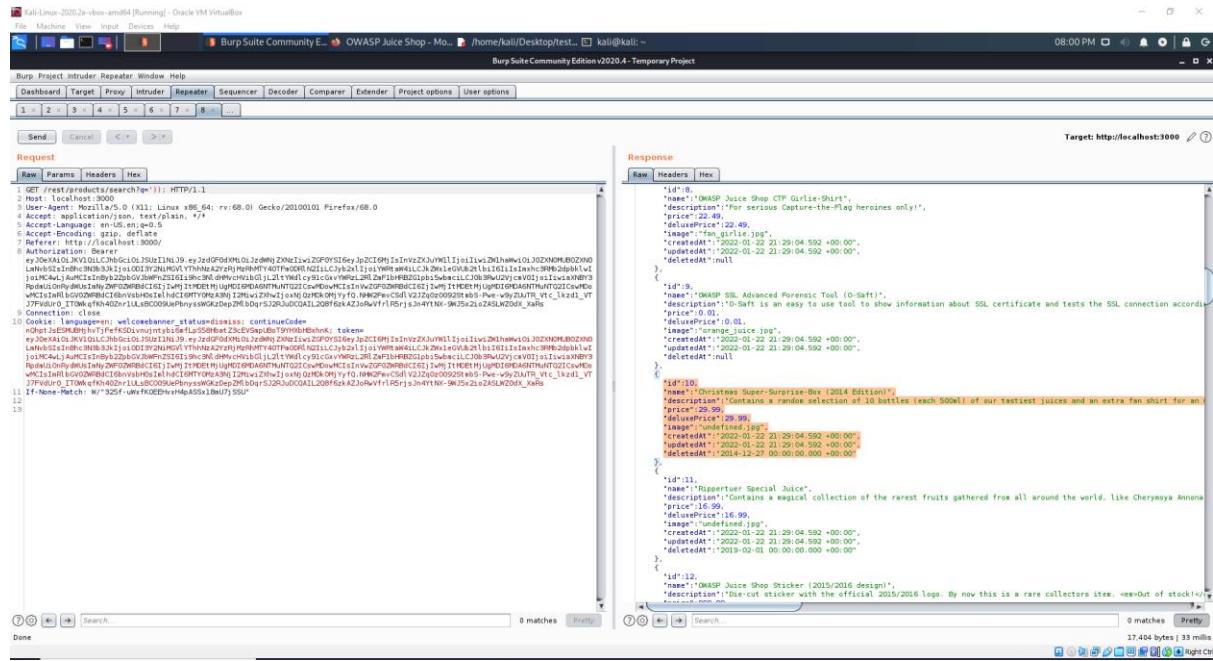
```

Can inject XSS through the API with repeater.

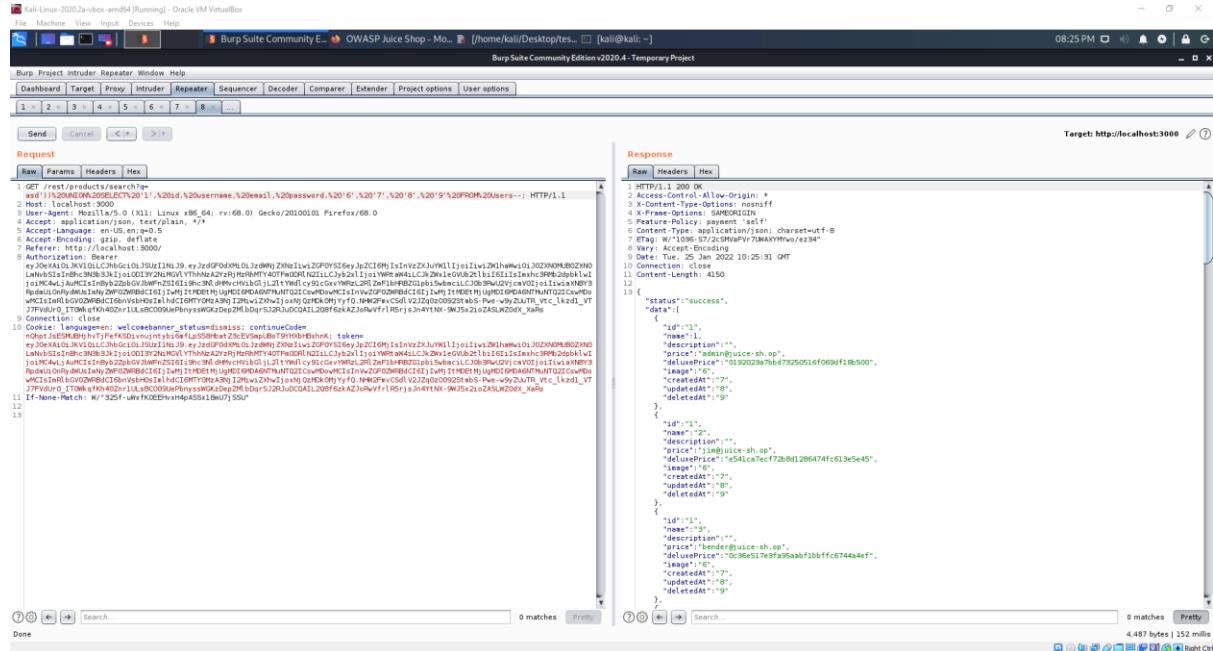
You can add onto the file you upload through intercept to exceed the file size limit.

Using XXE to show the passwd file. Prevented by disabling DTD's.

Week 5: SQL Injections and Live Bug Bounty Hunting

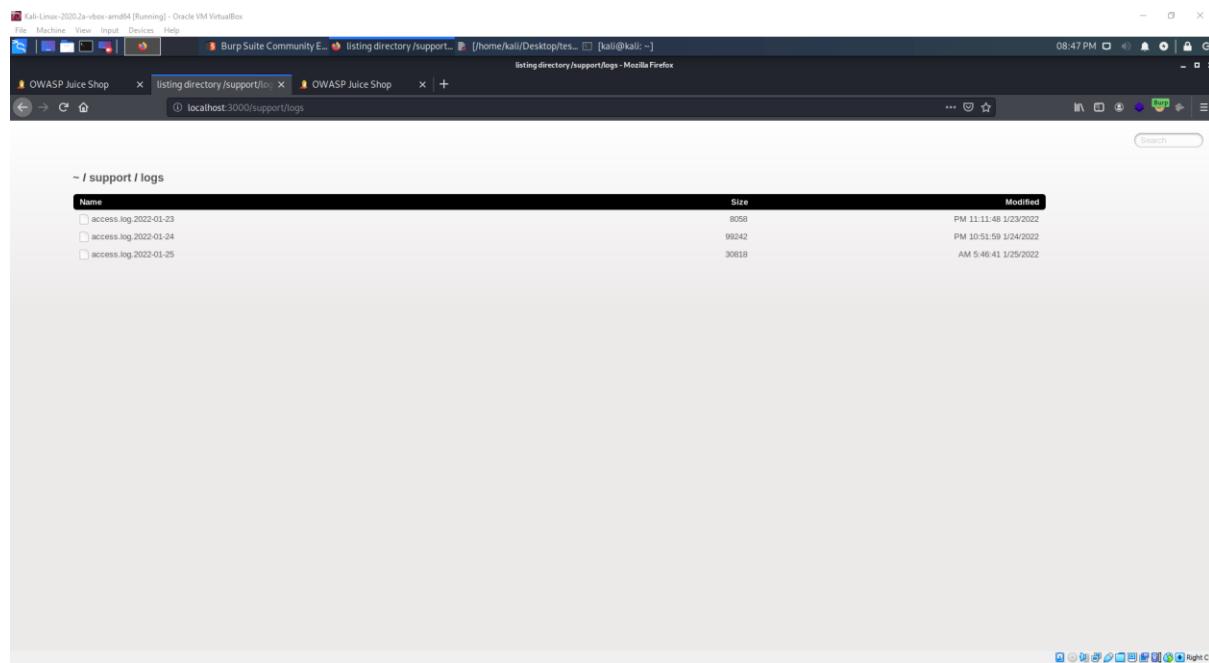


Using SQL injection with ')'; you can view the items in the database and find which items have been deleted and their time of deletion to use the item ID and add it to the basket through intercept.



Using SQL Injection to select information from the users table.

Using sleep can be a good indication of SQL injection when performing blind injections.



Using dirbuster can show hidden directories, one of which being the support logs.

Kali-Linux-2020.2a-vbox-amd64 [Running] - Oracle VM VirtualBox

Burp Suite Community Edition v2020.4 - Temporary Project

Request

```
Raw Params Headers Hex
1 GET /ftp/package.json.hak1250.ad HTTP/1.1
2 Host: localhost:3000
3 Date: Tue, 25 Jan 2022 10:49:19 GMT
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:3000/ftp
8 Connection: close
9 Content-Type: application/json; charset=UTF-8
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

```
Raw Headers Hex
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 Content-Type: application/json; charset=UTF-8
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Access-Control-Max-Age: 3600
7 Cache-Control: public, max-age=0
8 Last-Modified: Thu, 19 Jan 2022 21:50:43 GMT
9 ETag: 62-62-1642641140
10 Content-Type: application/octet-stream
11 Content-Length: 428
12 Date: Tue, 25 Jan 2022 10:49:19 GMT
13 Connection: close
14
15 {
16   "name": "Juice-Shop",
17   "version": "6.2.0-SNAPSHOT",
18   "description": "An intentionally insecure JavaScript Web Application",
19   "author": "Björn Kiaminich <juern.kiaminich@wasp.org> (https://kiaminich.de)",
20   "contributors": [
21     "Björn Kiaminich",
22     "Jennik Holtbach",
23     "Ashish089",
24     "t3m0n0n3bel",
25     "MarcelRe",
26     "sysoparist14",
27     "Scar26",
28     "CaptainFreak",
29     "HannsKraus",
30     "JuiceShopbot",
31     "the_gro",
32     "T3m0n0n3",
33     "AaryanD",
34     "RahulP",
35     "Take_Papel",
36     "...",
37   ],
38   "private": true,
39   "keywords": [
40     "security",
41     "vulnerability",
42     "web application security",
43     "webappsec",
44     "pentest",
45     "testing",
46     "security",
47     "vulnerable"
48   ],
49   "url": "https://www.wasp.juice-shop.de"
50 }
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
617
618
619
619
620
621
622
623
624
625
625
626
627
627
628
628
629
629
630
630
631
631
632
632
633
633
634
634
635
635
636
636
637
637
638
638
639
639
640
640
641
641
642
642
643
643
644
644
645
645
646
646
647
647
648
648
649
649
650
650
651
651
652
652
653
653
654
654
655
655
656
656
657
657
658
658
659
659
660
660
661
661
662
662
663
663
664
664
665
665
666
666
667
667
668
668
669
669
670
670
671
671
672
672
673
673
674
674
675
675
676
676
677
677
678
678
679
679
680
680
681
681
682
682
683
683
684
684
685
685
686
686
687
687
688
688
689
689
690
690
691
691
692
692
693
693
694
694
695
695
696
696
697
697
698
698
699
699
700
700
701
701
702
702
703
703
704
704
705
705
706
706
707
707
708
708
709
709
710
710
711
711
712
712
713
713
714
714
715
715
716
716
717
717
718
718
719
719
720
720
721
721
722
722
723
723
724
724
725
725
726
726
727
727
728
728
729
729
730
730
731
731
732
732
733
733
734
734
735
735
736
736
737
737
738
738
739
739
740
740
741
741
742
742
743
743
744
744
745
745
746
746
747
747
748
748
749
749
750
750
751
751
752
752
753
753
754
754
755
755
756
756
757
757
758
758
759
759
760
760
761
761
762
762
763
763
764
764
765
765
766
766
767
767
768
768
769
769
770
770
771
771
772
772
773
773
774
774
775
775
776
776
777
777
778
778
779
779
780
780
781
781
782
782
783
783
784
784
785
785
786
786
787
787
788
788
789
789
790
790
791
791
792
792
793
793
794
794
795
795
796
796
797
797
798
798
799
799
800
800
801
801
802
802
803
803
804
804
805
805
806
806
807
807
808
808
809
809
810
810
811
811
812
812
813
813
814
814
815
815
816
816
817
817
818
818
819
819
820
820
821
821
822
822
823
823
824
824
825
825
826
826
827
827
828
828
829
829
830
830
831
831
832
832
833
833
834
834
835
835
836
836
837
837
838
838
839
839
840
840
841
841
842
842
843
843
844
844
845
845
846
846
847
847
848
848
849
849
850
850
851
851
852
852
853
853
854
854
855
855
856
856
857
857
858
858
859
859
860
860
861
861
862
862
863
863
864
864
865
865
866
866
867
867
868
868
869
869
870
870
871
871
872
872
873
873
874
874
875
875
876
876
877
877
878
878
879
879
880
880
881
881
882
882
883
883
884
884
885
885
886
886
887
887
888
888
889
889
890
890
891
891
892
892
893
893
894
894
895
895
896
896
897
897
898
898
899
899
900
900
901
901
902
902
903
903
904
904
905
905
906
906
907
907
908
908
909
909
910
910
911
911
912
912
913
913
914
914
915
915
916
916
917
917
918
918
919
919
920
920
921
921
922
922
923
923
924
924
925
925
926
926
927
927
928
928
929
929
930
930
931
931
932
932
933
933
934
934
935
935
936
936
937
937
938
938
939
939
940
940
941
941
942
942
943
943
944
944
945
945
946
946
947
947
948
948
949
949
950
950
951
951
952
952
953
953
954
954
955
955
956
956
957
957
958
958
959
959
960
960
961
961
962
962
963
963
964
964
965
965
966
966
967
967
968
968
969
969
970
970
971
971
972
972
973
973
974
974
975
975
976
976
977
977
978
978
979
979
980
980
981
981
982
982
983
983
984
984
985
985
986
986
987
987
988
988
989
989
990
990
991
991
992
992
993
993
994
994
995
995
996
996
997
997
998
998
999
999
1000
1000
1001
1001
1002
1002
1003
1003
1004
1004
1005
1005
1006
1006
1007
1007
1008
1008
1009
1009
1010
1010
1011
1011
1012
1012
1013
1013
1014
1014
1015
1015
1016
1016
1017
1017
1018
1018
1019
1019
1020
1020
1021
1021
1022
1022
1023
1023
1024
1024
1025
1025
1026
1026
1027
1027
1028
1028
1029
1029
1030
1030
1031
1031
1032
1032
1033
1033
1034
1034
1035
1035
1036
1036
1037
1037
1038
1038
1039
1039
1040
1040
1041
1041
1042
1042
1043
1043
1044
1044
1045
1045
1046
1046
1047
1047
1048
1048
1049
1049
1050
1050
1051
1051
1052
1052
1053
1053
1054
1054
1055
1055
1056
1056
1057
1057
1058
1058
1059
1059
1060
1060
1061
1061
1062
1062
1063
1063
1064
1064
1065
1065
1066
1066
1067
1067
1068
1068
1069
1069
1070
1070
1071
1071
1072
1072
1073
1073
1074
1074
1075
1075
1076
1076
1077
1077
1078
1078
1079
1079
1080
1080
1081
1081
1082
1082
1083
1083
1084
1084
1085
1085
1086
1086
1087
1087
1088
1088
1089
1089
1090
1090
1091
1091
1092
1092
1093
1093
1094
1094
1095
1095
1096
1096
1097
1097
1098
1098
1099
1099
1100
1100
1101
1101
1102
1102
1103
1103
1104
1104
1105
1105
1106
1106
1107
1107
1108
1108
1109
1109
1110
1110
1111
1111
1112
1112
1113
1113
1114
1114
1115
1115
1116
1116
1117
1117
1118
1118
1119
1119
1120
1120
1121
1121
1122
1122
1123
1123
1124
1124
1125
1125
1126
1126
1127
1127
1128
1128
1129
1129
1130
1130
1131
1131
1132
1132
1133
1133
1134
1134
1135
1135
1136
1136
1137
1137
1138
1138
1139
1139
1140
1140
1141
1141
1142
1142
1143
1143
1144
1144
1145
1145
1146
1146
1147
1147
1148
1148
1149
1149
1150
1150
1151
1151
1152
1152
1153
1153
1154
1154
1155
1155
1156
1156
1157
1157
1158
1158
1159
1159
1160
1160
1161
1161
1162
1162
1163
1163
1164
1164
1165
1165
1166
1166
1167
1167
1168
1168
1169
1169
1170
1170
1171
1171
1172
1172
1173
1173
1174
1174
1175
1175
1176
1176
1177
1177
1178
1178
1179
1179
1180
1180
1181
1181
1182
1182
1183
1183
1184
1184
1185
1185
1186
1186
1187
1187
1188
1188
1189
1189
1190
1190
1191
1191
1192
1192
1193
1193
1194
1194
1195
1195
1196
1196
1197
1197
1198
1198
1199
1199
1200
1200
1201
1201
1202
1202
1203
1203
1204
1204
1205
1205
1206
1206
1207
1207
1208
1208
1209
1209
1210
1210
1211
1211
1212
1212
1213
1213
1214
1214
1215
1215
1216
1216
1217
1217
1218
1218
1219
1219
1220
1220
1221
1221
1222
1222
1223
1223
1224
1224
1225
1225
1226
1226
1227
1227
1228
1228
1229
1229
1230
1230
1231
1231
1232
1232
1233
1233
1234
1234
1235
1235
1236
1236
1237
1237
1238
1238
1239
1239
1240
1240
1241
1241
1242
1242
1243
1243
1244
1244
1245
1245
1246
1246
1247
1247
1248
1248
1249
1249
1250
1250
1251
1251
1252
1252
1253
1253
1254
1254
1255
1255
1256
1256
1257
1257
1258
1258
1259
1259
1260
1260
1261
1261
1262
1262
1263
1263
1264
1264
1265
1265
1266
1266
1267
1267
1268
1268
1269
1269
1270
1270
1271
1271
1272
1272
1273
1273
1274
1274
1275
1275
1276
1276
1277
1277
1278
1278
1279
1279
1280
1280
1281
1281
1282
1282
1283
1283
1284
1284
1285
1285
1286
1286
1287
1287
1288
1288
1289
1289
1290
1290
1291
1291
1292
1292
1293
1293
1294
1294
1295
1295
1296
1296
1297
1297
1298
1298
1299
1299
1300
1300
1301
1301
1302
1302
1303
1303
1304
1304
1305
1305
1306
1306
1307
1307
1308
1308
1309
1309
1310
1310
1311
1311
1312
1312
1313
1313
1314
1314
1315
1315
1316
1316
1317
1317
1318
1318
1319
1319
1320
1320
1321
1321
1322
1322
1323
1323
1324
1324
1325
1325
1326
1326
1327
1327
1328
1328
1329
1329
1330
1330
1331
1331
1332
1332
1333
1333
1334
1334
1335
1335
1336
1336
1337
1337
1338
1338
1339
1339
1340
1340
1341
1341
1342
1342
1343
1343
1344
1344
1345
1345
1346
1346
1347
1347
1348
1348
1349
1349
1350
1350
1351
1351
1352
1352
1353
1353
1354
1354
1355
1355
1356
1356
1357
1357
1358
1358
1359
1359
1360
1360
1361
1361
1362
1362
1363
1363
1364
1364
1365
1365
1366
1366
1367
1367
1368
1368
1369
1369
1370
1370
1371
1371
1372
1372
1373
1373
1374
1374
1375
1375
1376
1376
1377
1377
1378
1378
1379
1379
1380
1380
1381
1381
1382
1382
1383
1383
1384
1384
1385
1385
1386
1386
1387
1387
1388
1388
1389
1389
1390
1390
1391
1391
1392
1392
1393
1393
1394
1394
1395
1395
1396
1396
1397
1397
1398
1398
1399
1399
1400
1400
1401
1401
1402
1402
1403
1403
1404
1404
1405
1405
1406
1406
1407
1407
1408
1408
1409
1409
1410
1410
1411
1411
1412
1412
1413
1413
1414
1414
1415
1415
1416
1416
1417
1417
1418
1418
1419
1419
1420
1420
1421
1421
1422
1422
1423
1423
1424
1424
1425
1425
1426
1426
1427
1427
1428
1428
1429
1429
1430
1430
1431
1431
1432
1432
1433
1433
1434
1434
1435
1435
1436
1436
1437
1437
1438
1438
1439
1439
1440
1440
1441
1441
1442
1442
1443
1443
1444
1444
1445
1445
1446
1446
1447
1447
1448
1448
1449
1449
1450
1450
1451
1451
1452
1452
1453
1453
1454
1454
1455
1455
1456
1456
1457
1457
1458
1458
1459
1459
1460
1460
1461
1461
1462
1462
1463
1463
1464
1464
1465
1465
1466
1466
1467
1467
1468
1468
1469
1469
1470
1470
1471
1471
1472
1472
1473
1473
1474
1474
1475
1475
1476
1476
1477
1477
1478
1478
1479
1479
1480
1480
1481
1481
1482
1482
1483
1483
1484
1484
1485
1485
1486
1486
1487
1487
1488
1488
1489
1489
1490
1490
1491
1491
1492
1492
1493
1493
1494
1494
1495
1495
1496
1496
1497
1497
1498
1498
1499
1499
1500
1500
1501
1501
1502
1502
1503
1503
1504
1504
1505
1505
1506
1506
1507
1507
1508
1508
1509
1509
1510
1510
1511
1511
1512
1512
1513
1513
151
```

1. Explore visible content. Use a passive sitemap like Burp Suite.
2. Consult public resources. (wayback machine, google site:)
3. Discover hidden content. Check requests for non-existent items.
4. Discover default content. Run nikto, dirbuster.
5. Enumerate identifier-specified functions. Request parameters.
6. Test for debug parameters.
7. Identify application functionality
8. Identify data entry points
9. Identify technologies used. Wappalyzer, Nmap
10. Map the attack surface.
11. Test data transmission via the client
12. Test client-side controls over user input
13. Test browser extension components
14. Understand the mechanism. (forms, certificates, multifactor)
15. Test password quality
16. Test username enumeration
17. Test resilience to password guessing
18. Test account recovery functions
19. Test “Remember me” functions
20. Test username uniqueness
21. Test predictability of autogenerated credentials
22. Check for unsafe transmission of credentials
23. Check for unsafe distribution of credentials
24. Test for insecure storage
25. Test for logic flaws
26. Test tokens
27. Check session data
28. Check for CSRF
29. Check cookie scope
30. Test access controls
31. Test with multiple accounts
32. Test with limited access
33. Test for insecure access control methods
34. Test for input vulnerabilities. (fuzz all request parameters, SQL injection, XSS, OS commands, path traversal, script injection, file inclusion)
35. Test for function specific input vulnerabilities. (SMTP injection, SOAP injection, LDAP injection, XPath injection, XXE injection)
36. Test for logic flaws
37. Test for shared hosting vulnerabilities
38. Test for application server vulnerabilities
39. Misc checks (DOM-based, local privacy, weak SSL ciphers, same-origin policy)
40. Follow up on any information leakage

OWASP Top 10

A01:2021 – Broken Access Control

Broken access control commonly leads to unauthorised information disclosure, modification or destruction of all data or performing a business function outside of the user's limits.

A02:2021 – Cryptographic Failures

Cryptographic failures compromise the protection needs of data in transit and at rest. Examples include passwords, credit card numbers, health records, personal information, and business secrets.

A03:2021 – Injection

Injection includes attacks such as cross site scripting, SQL injection and external control of file names or paths. These attacks can occur when an application hasn't been validated, filtered, or sanitized correctly.

A04:2021 – Insecure Design

This is a broad category representing different weaknesses expressed as missing or ineffective control design. These include generating error messages containing sensitive information, unprotected storage of credentials, trust boundary violation and insufficiently protected credentials.

A05:2021 – Security Misconfiguration

Misconfiguration includes missing appropriate security hardening across the application stack, the inclusion of unnecessary features, default accounts and passwords, and poorly configured security headers. Notable CWEs include improper restriction of XML eternal entity reference and configurations.

A06:2021 – Vulnerable and Outdated Components

You can be vulnerable if you do not know what versions you are running, your nested dependencies, out of date software, unsupported software, etc.

A07:2021 – Identification and Authentication Failures

Authentication weaknesses can occur when an application permits automated attacks, permits brute force attacks, uses weak or ineffective credential recovery processes, uses default or well-known passwords, uses plain text or weakly hashed passwords, has missing multi-factor authentication, exposes identifiers in the URL or does not correctly invalidate session IDs.

A08:2021 – Software and Data Integrity Failures

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks. Prevention methods include using digital signatures to verify the integrity of the software or data, ensure libraries and dependencies are using trusted repositories and ensure that unsigned or unencrypted data is not sent to untrusted clients without a form of integrity check.

A09:2021 – Security Logging and Monitoring Failures

Insufficient logging, detection, monitoring and active response occurs when logs of applications are not monitored for suspicious activity, logs are only stored locally, warnings generate inadequate or unclear logs and if penetration tests and scans do not trigger alerts.

A10:2021 – Server-Side Request Forgery

SSRF flaws occur whenever a web application is fetching a remote resource without validating the user supplied URL allowing an attacker to coerce the application to send a crafted request to an unexpected destination.

MITRE Common Weaknesses

Common Weakness Enumeration (CWE) is a community developed list of common software and hardware security weaknesses. Weaknesses are flaws, faults, bugs or other errors in software or hardware implementation, code, design, or architecture that if left unaddressed could result in systems, networks or hardware being vulnerable to attack.

CWEs help developers and security practitioners to describe and discuss software and hardware weaknesses in a common language, check for weaknesses in existing software and hardware products, evaluate coverage of tools targeting these weaknesses, leverage a common baseline standard for weakness identification, mitigation, and prevention and prevent software and hardware vulnerabilities prior to deployment.

Portswigger Burpsuite

Portswigger's Burpsuite is a web application testing tool that helps users find a wide range of vulnerabilities in applications automatically and manually. It can crawl applications and create a site map, find issues within pages, includes essential tools like the interception proxy, repeater, intruder, decoder, sequencer, and comparer.

The interception proxy acts as proxy between you and the application, capturing packets sent to the application and displaying them in raw text. This can be used to view, manipulate, alter, or remove data from the packet before it reaches the application's server. It is set up on the host machine on a given port (usually 8080) and can be switched on and off. This can be useful in testing vulnerabilities

and creating exploits within the application API as noted in the beginner's web application hacking tutorial above.

Network Security

NMAP Network Scanning

TCP and UDP

TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol and while more popular services on the internet run over the TCP protocol, UDP services are still widely deployed.

TCP requires an established connection to transmit data and the connection should be closed once transmission is complete. It is also able to sequence data, guarantees the delivery of data to the destination, can retransmit lost packets, has an extensive error checking and acknowledgement of data and is read as a byte stream. Common uses for TCP are HTTPS, HTTP, SMTP, POP, and FTP.

UDP is a connectionless protocol with no requirements for opening, maintaining, or terminating a connection. It is unable to sequence data, cannot guarantee the delivery of data and has no ability to retransmit lost packets. It uses a basic error checking mechanism using checksums and its packets are sent with defined boundaries, sent individually, and checked for integrity on arrival. Common uses for UDP are video conferencing, streaming, DNS, and VoIP.

Port Scanning

The port scanner is the core function of Nmap and unless instructed otherwise, scans the most used 1000 TCP ports on a host. Port scanning will classify each port into the state open, closed filtered, unfiltered, open|filtered or closed|filtered.

The open state means that an application is actively accepting TCP connections or UDP packets on this port. Finding these is often the primary goal of port scanning.

The closed state means that the port is accessible but there is no application listening on it.

The filtered state means Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port.

The unfiltered state means that the port is accessible, but Nmap is unable to determine whether it is opened or closed. This is only seen within an ACK scan.

The open|filtered state occurs when Nmap is unable to determine whether it is opened or filtered. This is seen in UDP, IP protocol, FIN, NULL and Xmas scans.

The closed|filtered state occurs when Nmap is unable to determine whether the port is closed or filtered. This is only seen in an ID idle scan.

Ports are simply software abstraction, used to distinguish between communication channels. Like how IP addresses identify machines on a network, ports identify specific applications used on a single machine.

Top 20 most common TCP ports

80 – HTTP

23 – Telnet

443 – HTTPS

21 – FTP

22 – SSH

25 – SMTP

3389 – ms-term-server

110 – POP3

445 – Microsoft-DS

139 – NetBIOS-SSN

143 – IMAP

53 – Domain

135 – MSRPC

3306 – MySQL

8080 – HTTP Proxy

1723 – PPTP

111 – RPCBind

995 – POP3S

993 – IMAPS

5900 – VNC

Top 20 most common UDP ports

631 – IPP
161 – SNMP
137 – NETBIOS-SN
123 – NTP
138 – NETBIOS-DGM
1434 – MS-SQL-DS
445 – Microsoft-DS
135 – MSRPC
67 – DHCP-S
53 – Domain
139 – NETBIOS-SSN
500 – ISAKMP
68 – DHCPC
520 – Route
1900 – UPNP
4500 – nat-t-ike
524 – Syslog
49152 – IANA specified ports
162 – SNMPTrap
69 – TFTP

Service Identification

Using its nmap-services database of more than 2,200 well-known services and while this information is usually accurate, there are often times when hosts run applications from different ports. Nmap also has the ability to fingerprint which version of applications are running which can help dramatically in determining which exploits an application is vulnerable to however, keep in mind that security fixes are often back-ported to earlier versions of software so you cannot rely solely on the version number to prove a service is vulnerable.

Some service scans can sometimes reveal information about a target beyond the service type and version number. They can also include SSH protocol numbers, Apache modules and more. The

version detection can also discover operating systems and device types and a scan can be used in fingerprinting a system with the `-O` flag.

Useful Nmap flags

`-p`: port selection

`-A`: aggressive detection mode

`-O`: OS fingerprinting

`-T4`: Timing, increases the speed of scan. The faster the more noise it makes.

`-sV`: service scan

`-sS`: stealth TCP scan

`-sU`: UDP scan

Hands on Labs

Portswigger Academy

The screenshot shows the Portswigger Academy dashboard. At the top, there's a navigation bar with tabs like 'Dashboard' and 'Community'. Below the navigation, the main content area is titled 'Your learning progress'. It features several sections: 'Your level' (NEWBIE, Solve 31 more labs to become an apprentice), 'Level progress' (Apprentice: 19 of 50, Practitioner: 24 of 131, Expert: 1 of 30), 'Learning materials' (progress 13%), and 'Vulnerability labs' (progress 20%). Each section has a 'VIEW ALL' button. The bottom of the page includes a footer with various icons and links.

TryHackMe

The second section (Security Tools) focuses on learning how to use Industry Standard tooling to interact with your targets.

The third section (Vulnerabilities) covers various vulnerabilities found in web applications today. This section will go over root causes of these vulnerabilities and give you hands on experience on exploiting them.

The final section (Practise Makes Perfect) will help you apply what you've learnt in previous sections.

After completing this path, you should be able to:

- understand how web applications work
- utilise industry standard tooling when attacking web applications
- explain and exploit common web vulnerabilities
- apply this knowledge to other targets (be it within an interview or a professional web applications security assessment)

Web Fundamentals
Before attacking web applications, it's important to understand how the internet and web applications work.

BurpSuite & OWASP Zap
Burp Suite is the industry standard tool for web application hacking, and is essential in any web penetration test.

Vulnerabilities
Explore common web application security vulnerabilities. Understand how they work, the context in which they can be found and how to exploit them.

Practice Makes Perfect
Now that you've seen common vulnerabilities, reinforce this knowledge by solving some web application security challenges.

Certificate
In order to get your certificate you should complete the course. Certificates allow you to prove your education.
Path Progress (100%)

Next Achievement (2/2)
No badges left to earn in this path.



References

- Lindsay, J., Chell, D., Erasmus, T., Colley, S., & Whitehouse, O. (2015). *The Mobile Application Hacker's Handbook* (1st ed.). Wiley Publishing.
- Scambray, J., McClure, S., & Kurtz, G. (2012). *Hacking Exposed 7: Network Security Secrets and Solutions* (7th ed.). McGraw-Hill Education.
- Stuttard, D., & Pinto, M. (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws* (2nd ed.). Wiley Publishing.