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

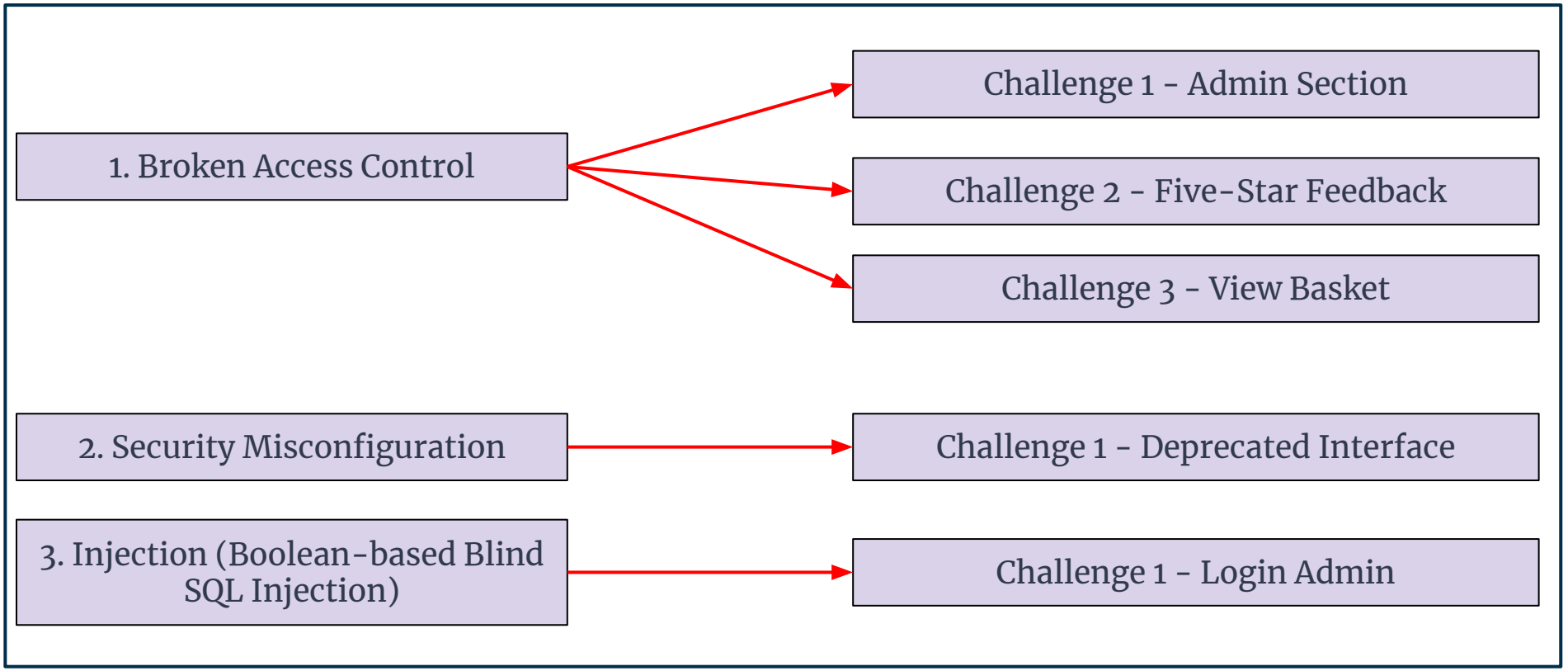
8. Reflected XSS

9. Security Policy

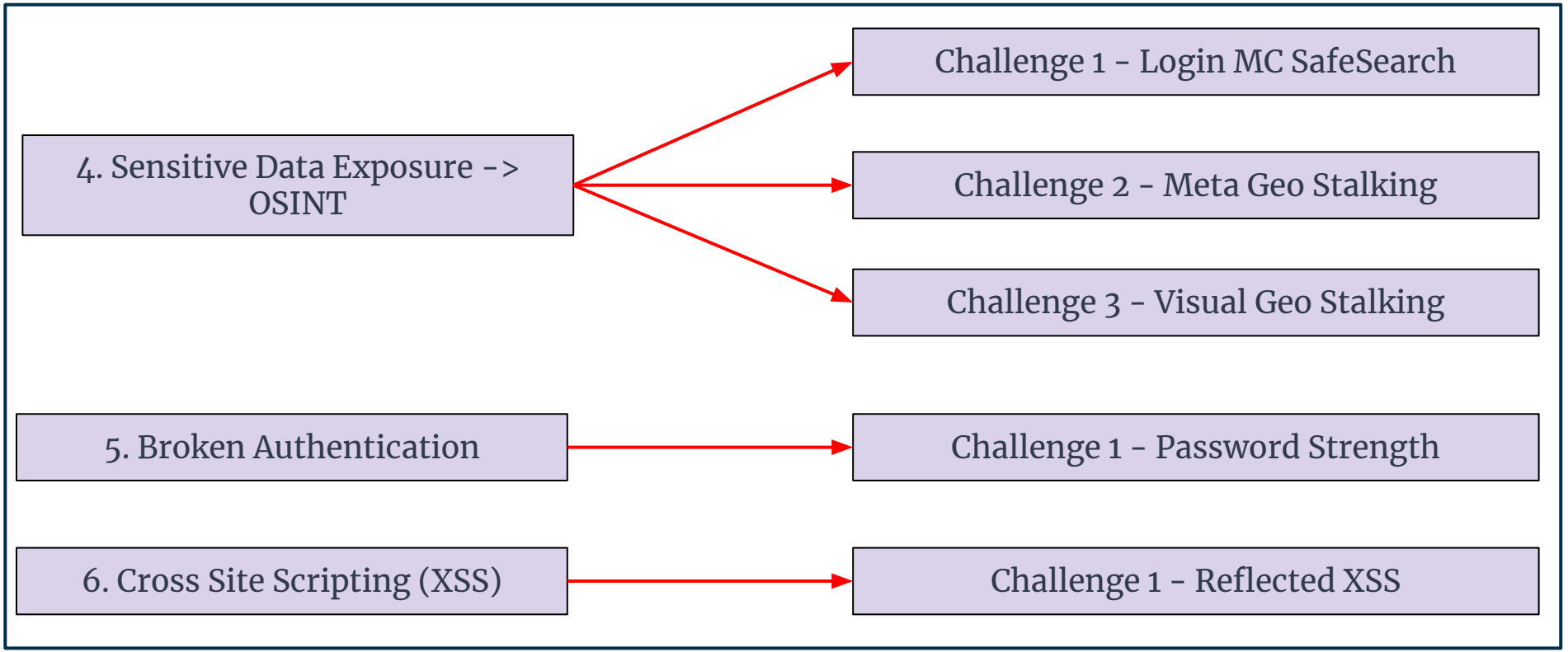
10. View Basket

11. Visual Geo Stalking

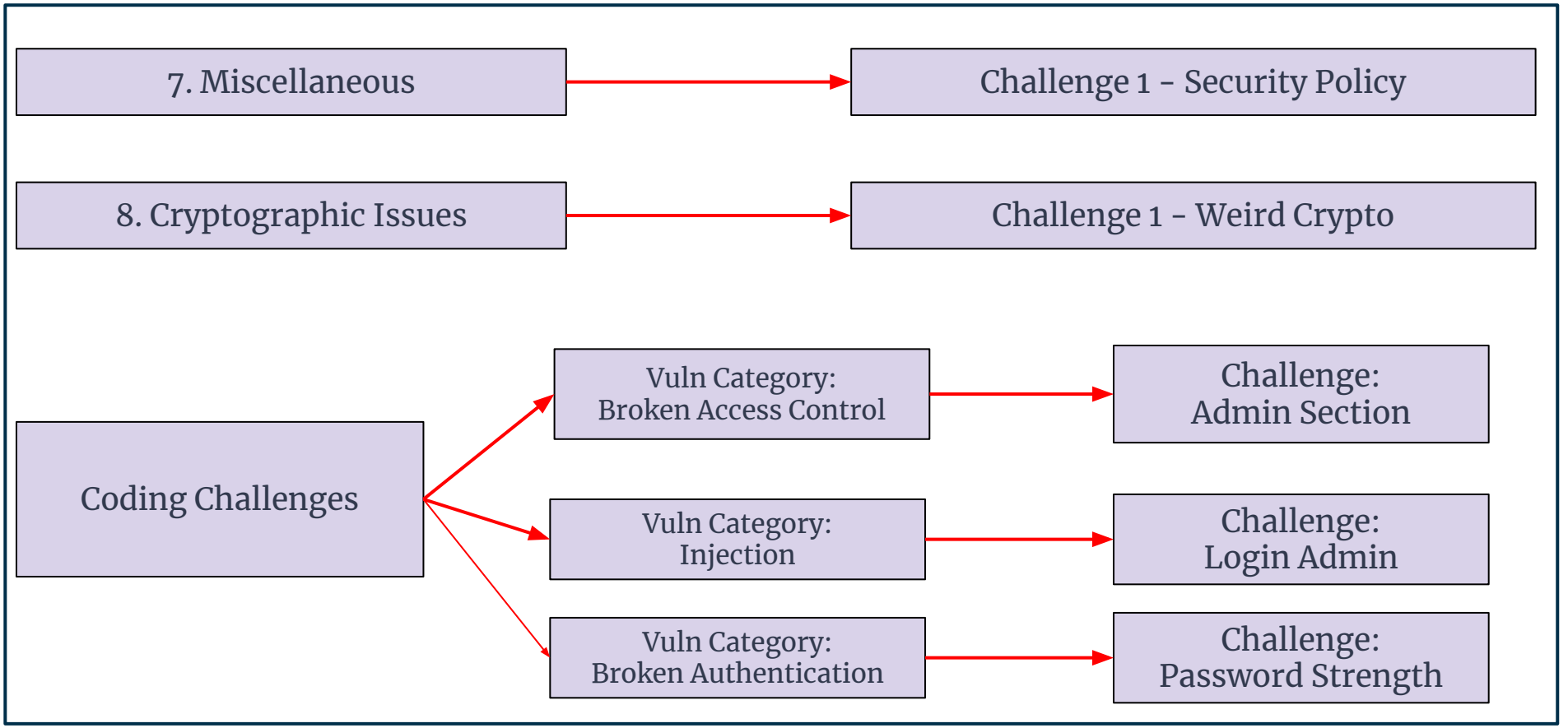
12. Weird Crypto



Challenges associated with each vulnerability category



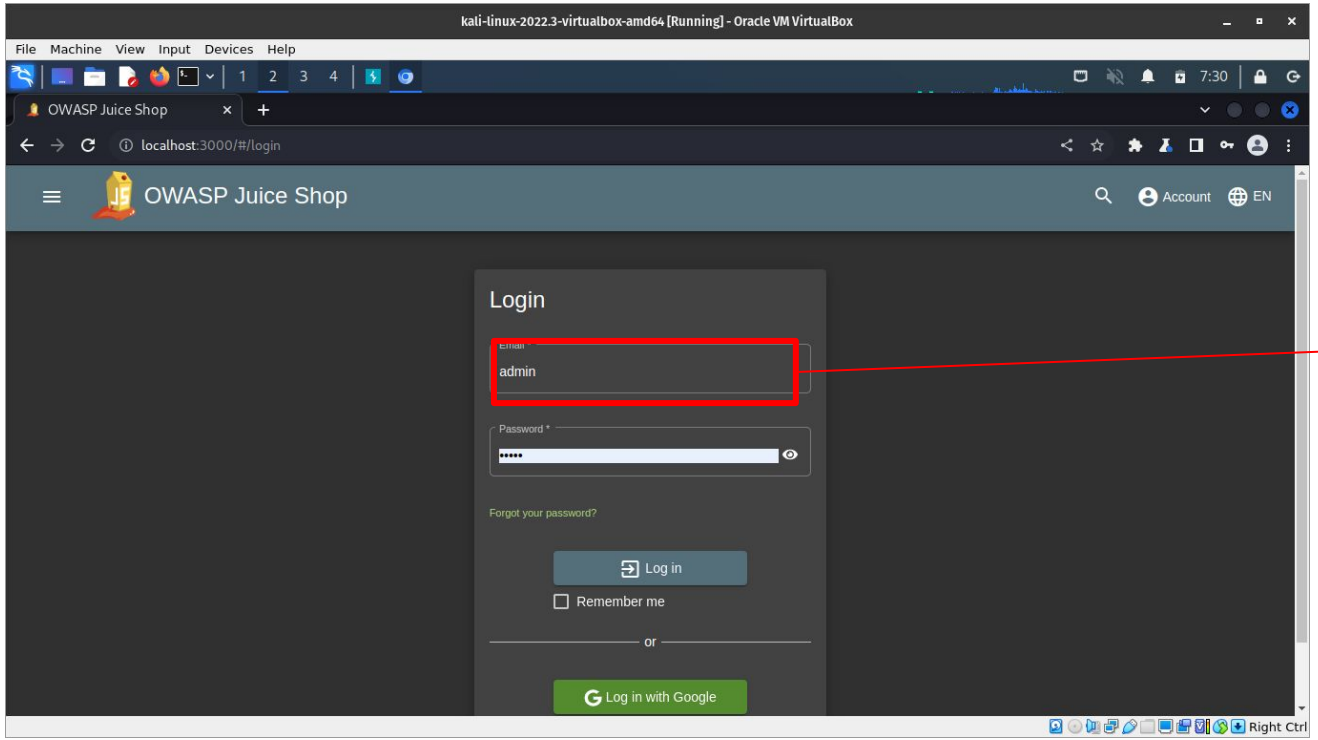
Challenges associated with each vulnerability category



Challenges associated with each vulnerability category + 3 Coding challenges

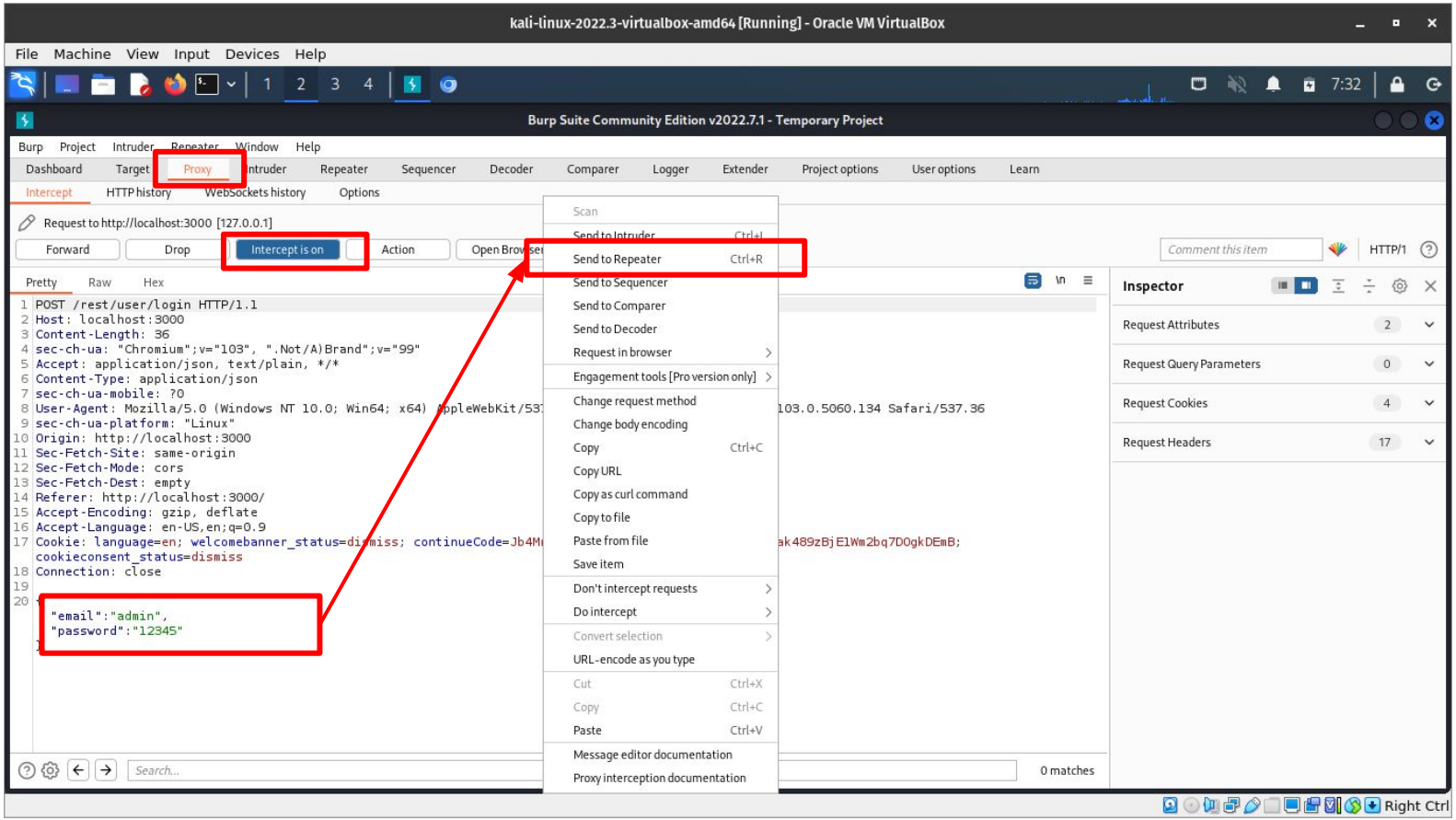
Injection (Boolean-based Blind SQL Injection)

Challenge 1 - Login Admin

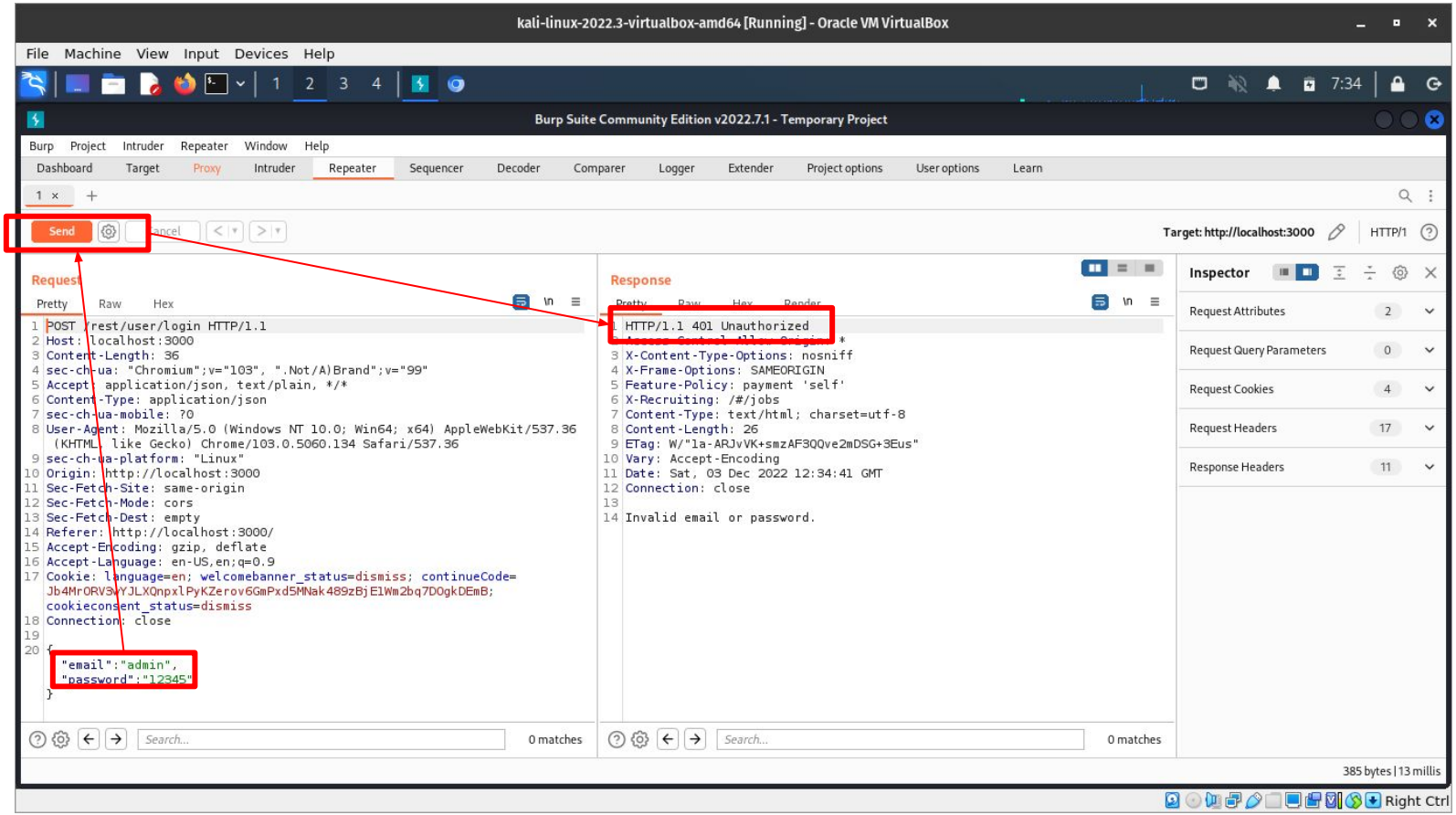


Capture the request on Burp Suite

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



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



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

Status Codes

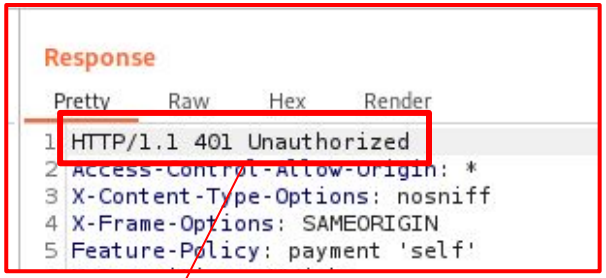
1xx - Informational

2xx - The request was successful

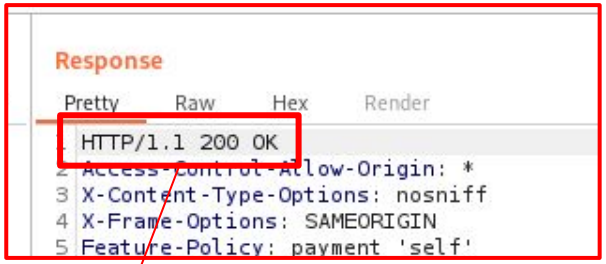
3xx - The client is redirected to a different resource

4xx - The request contains an error of some kind

5xx - The server encountered an error fulfilling the request

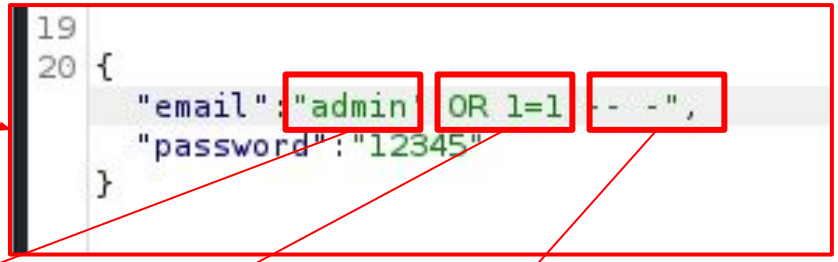


"401 Unauthorized" indicates that the server requires HTTP authentication before the request will be granted.



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

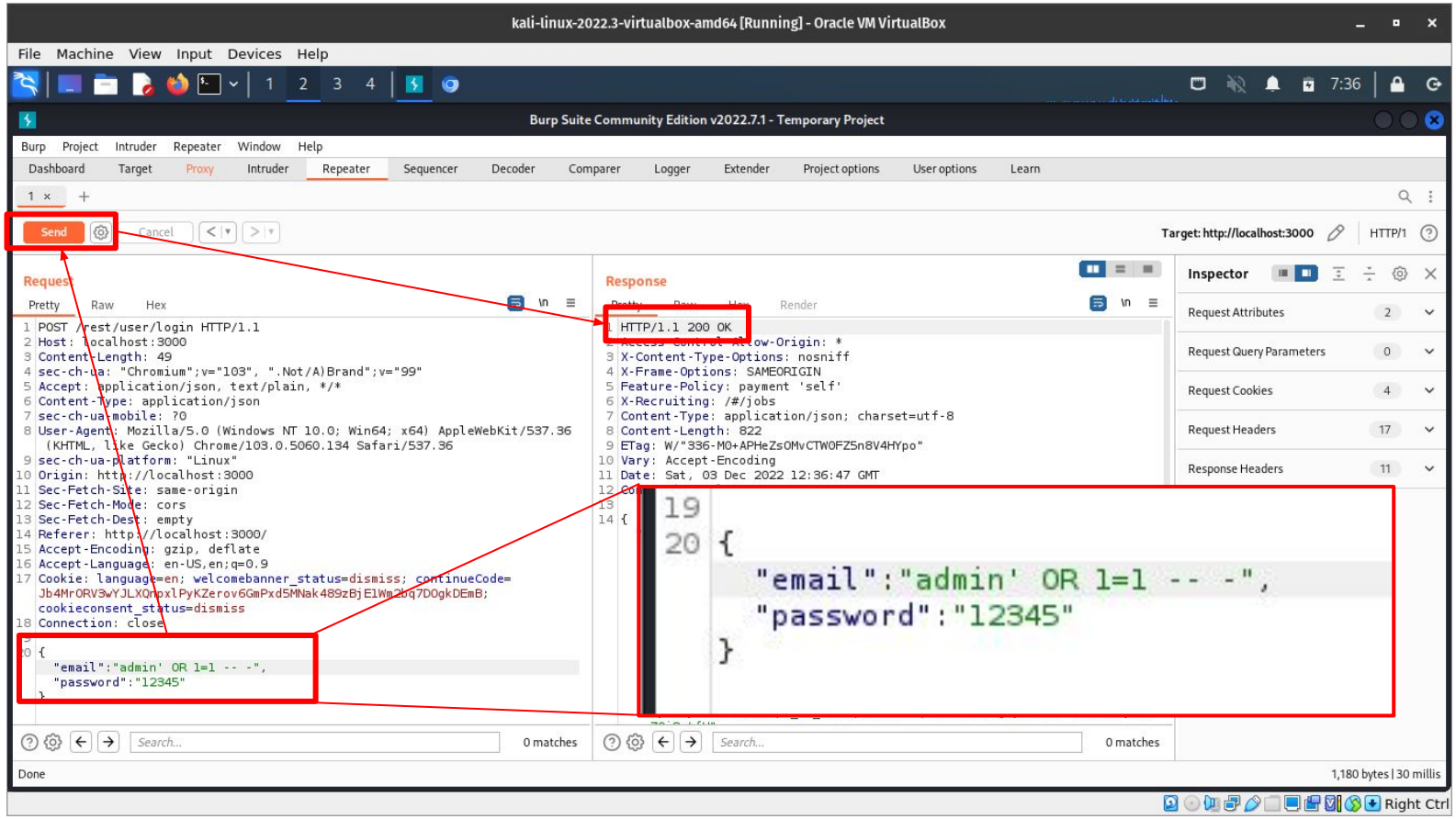
Injection (Boolean-based Blind SQL Injection)



“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



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

Status Codes

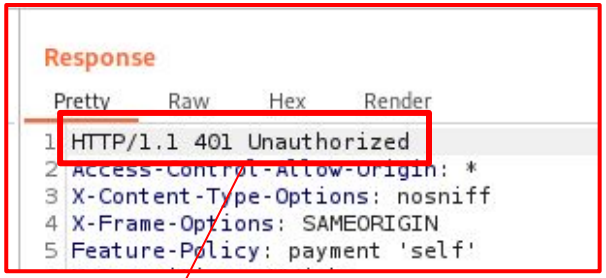
1xx - Informational

2xx - The request was successful

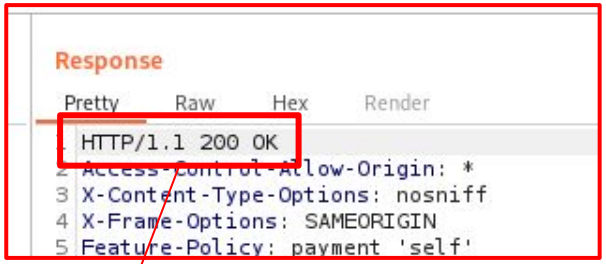
3xx - The client is redirected to a different resource

4xx - The request contains an error of some kind

5xx - The server encountered an error fulfilling the request



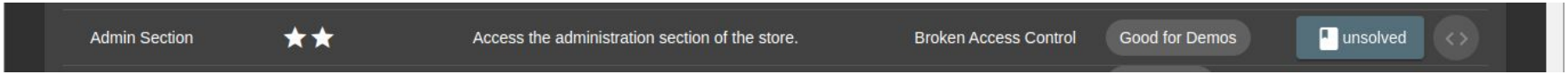
"401 Unauthorized" indicates that the server requires HTTP authentication before the request will be granted.



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

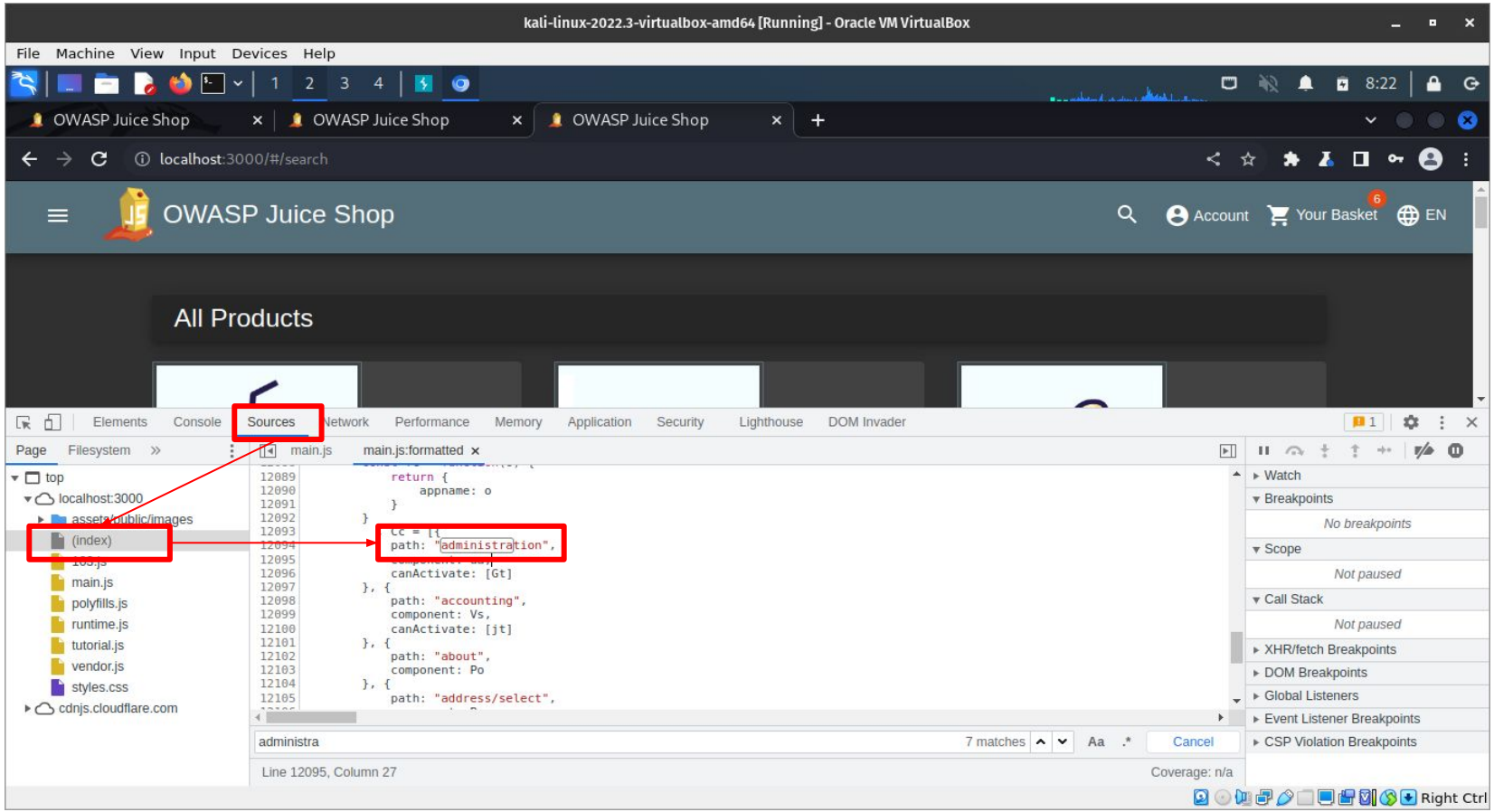
Broken Access Control

- Challenge 1 - Admin Section
- Challenge 2 - Five-Star Feedback
- Challenge 3 - View Basket

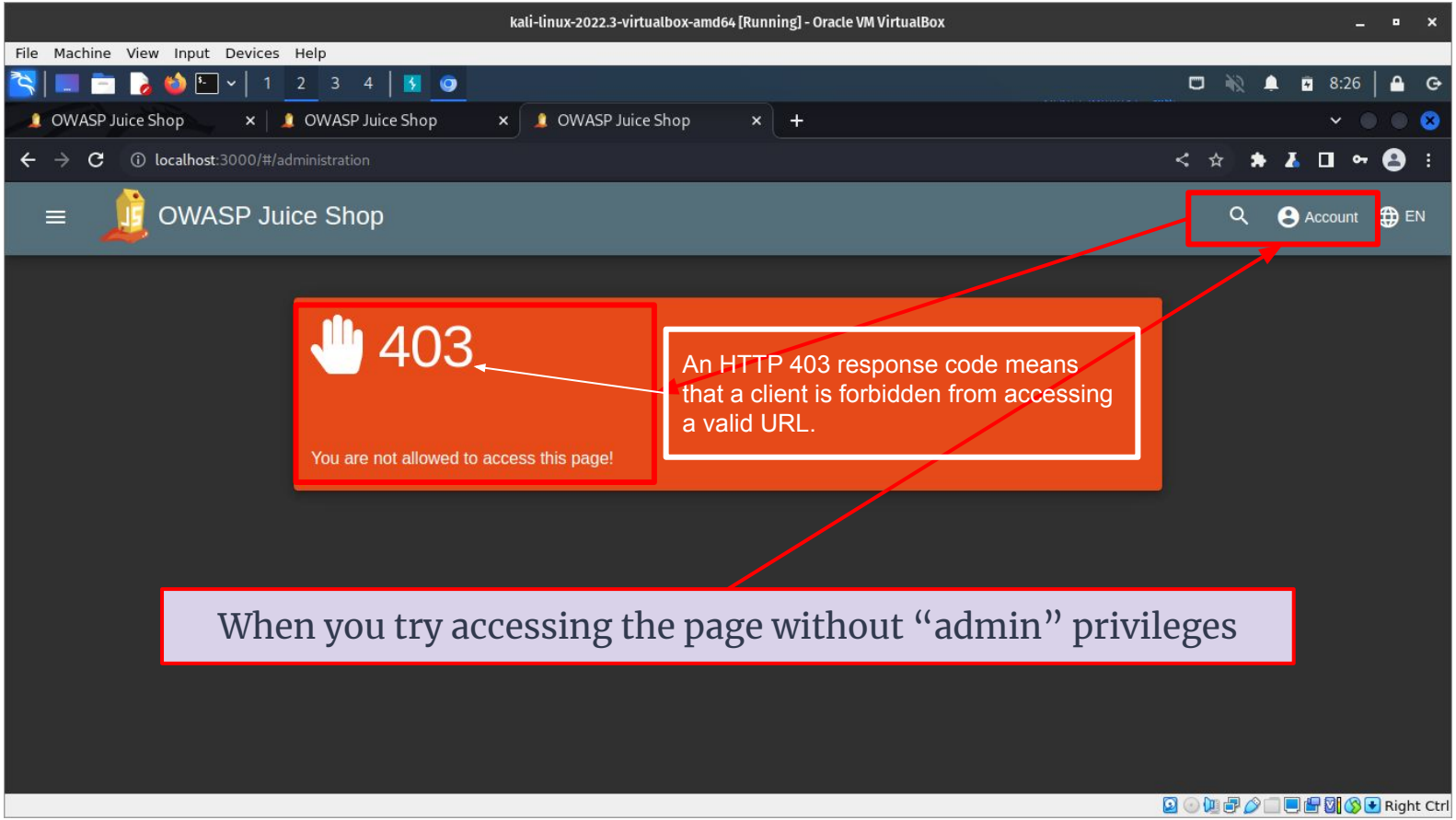


For this challenge you have to login as “admin”

Broken Access Control: #Challenge: 1. Admin Section



Broken Access Control: #Challenge: 1. Admin Section



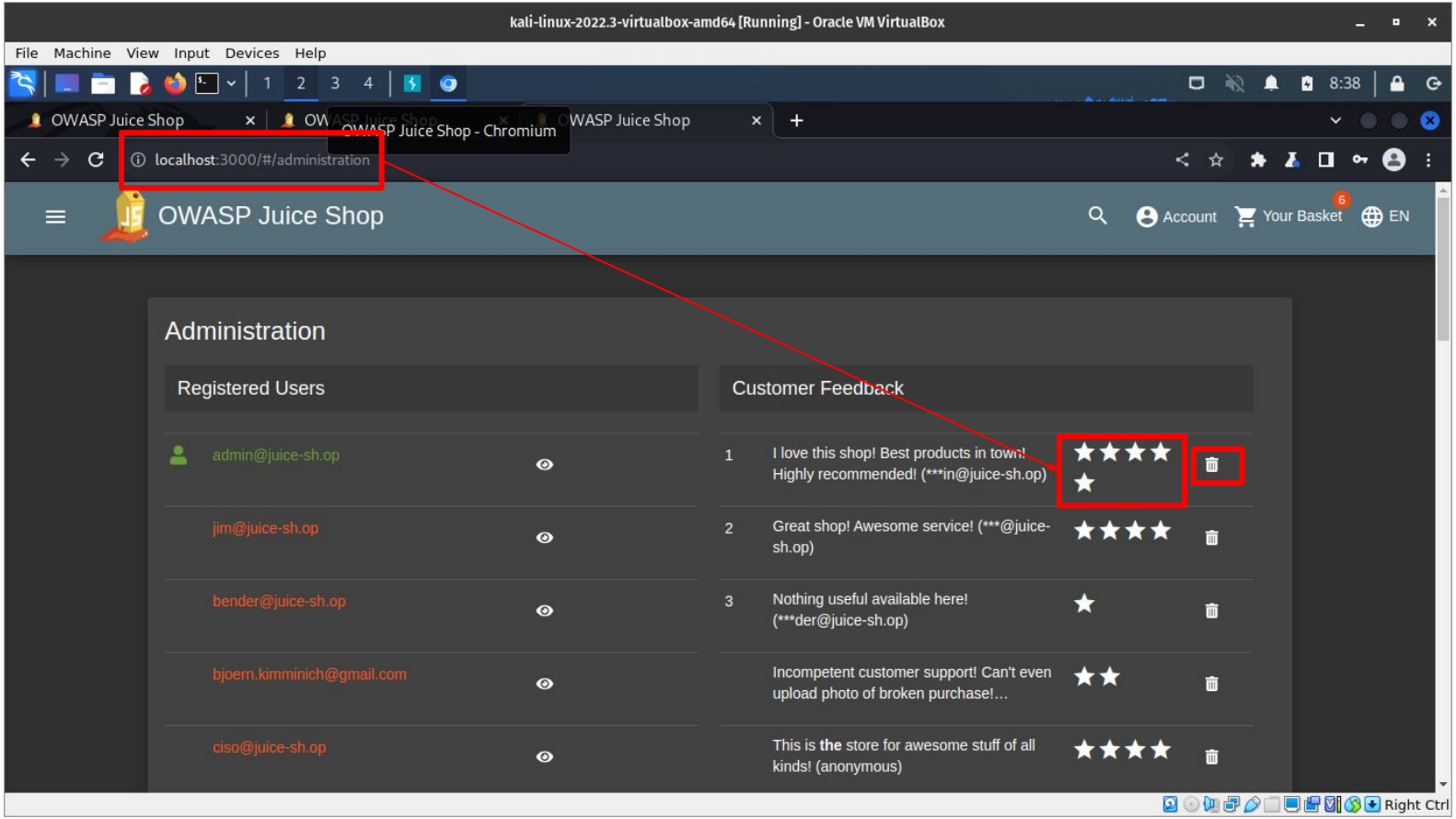
Broken Access Control: #Challenge: 1. Admin Section

1. Broken Access Control

- Challenge 1 - Admin Section
- Challenge 2 - Five-Star Feedback
- Challenge 3 - View Basket

For this challenge you have to login as “admin”

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

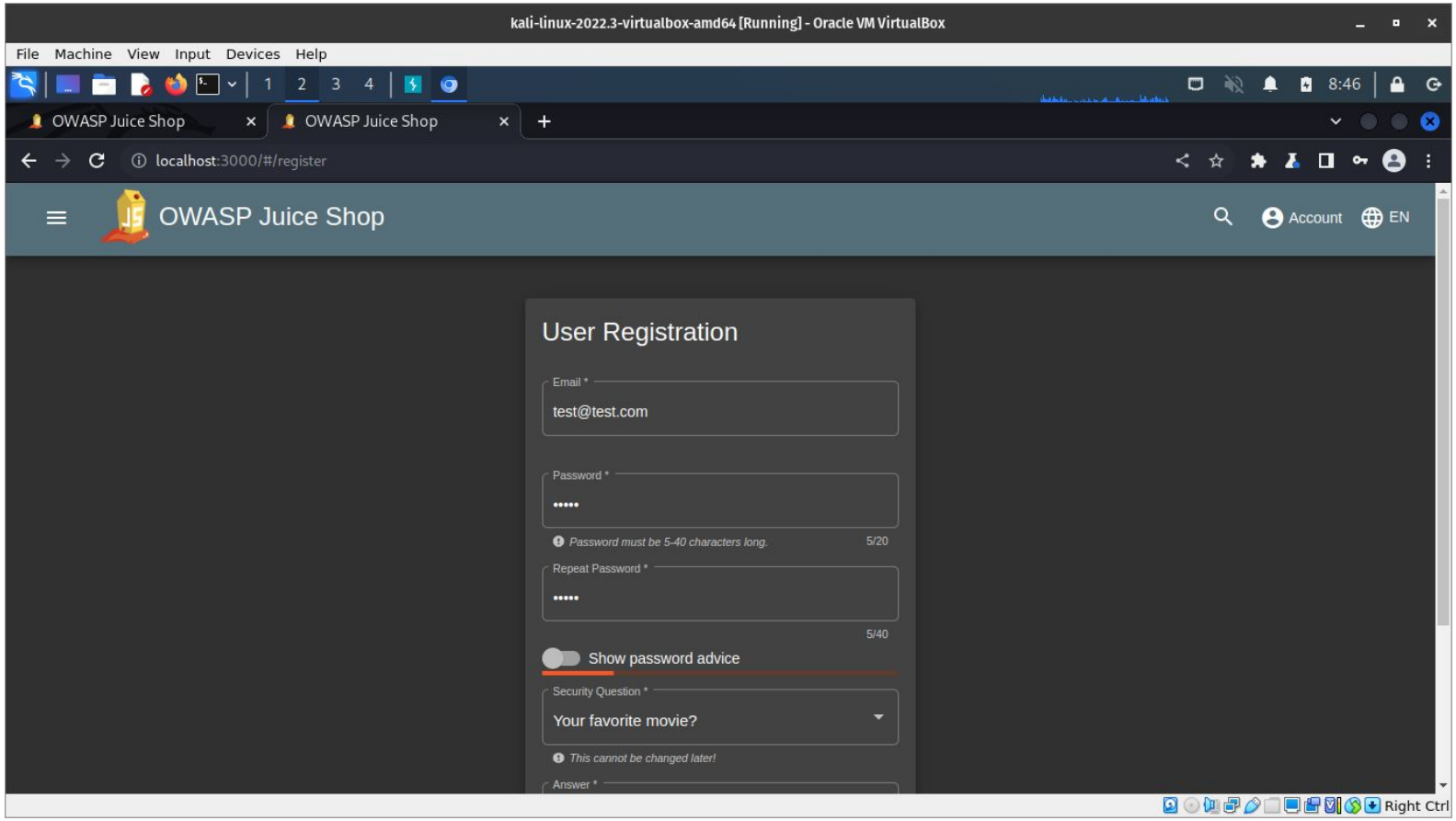


Broken Access Control: #Challenge: 2. Five-Star Feedback

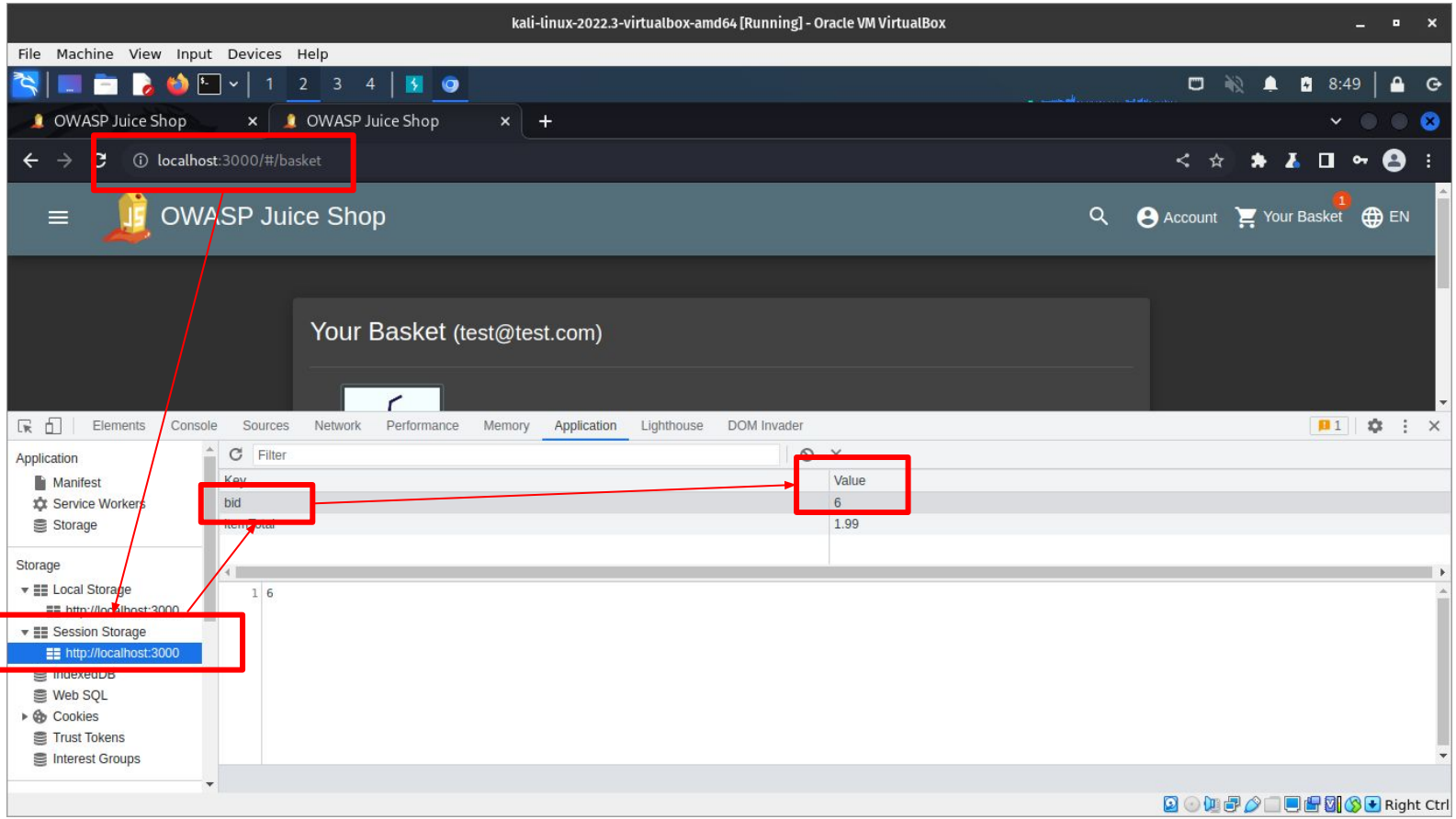
1. Broken Access Control

- Challenge 1 - Admin Section
- Challenge 2 - Five-Star Feedback
- Challenge 3 - View Basket

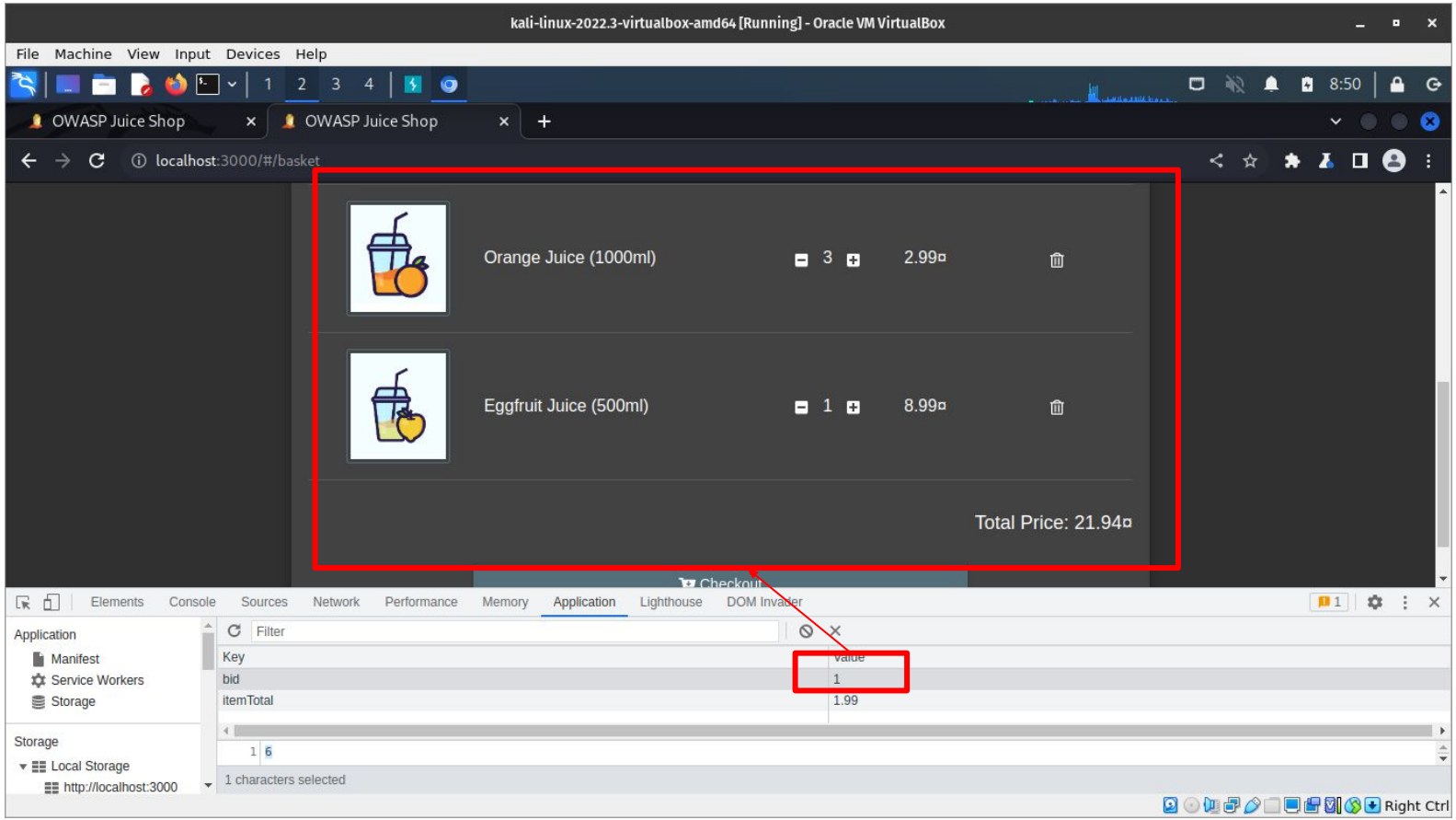
Broken Access Control: #Challenge: 3. View Basket



Broken Access Control: #Challenge: 3. View Basket



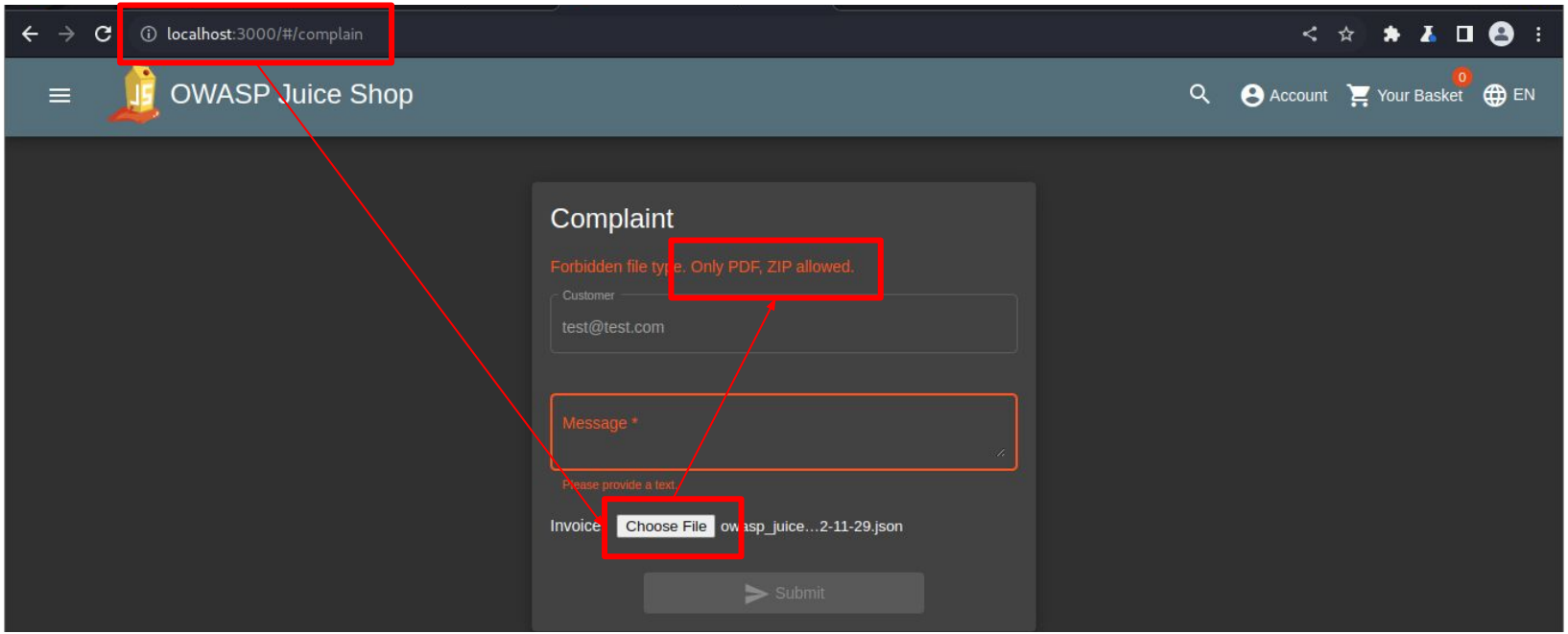
Broken Access Control: #Challenge: 3. View Basket



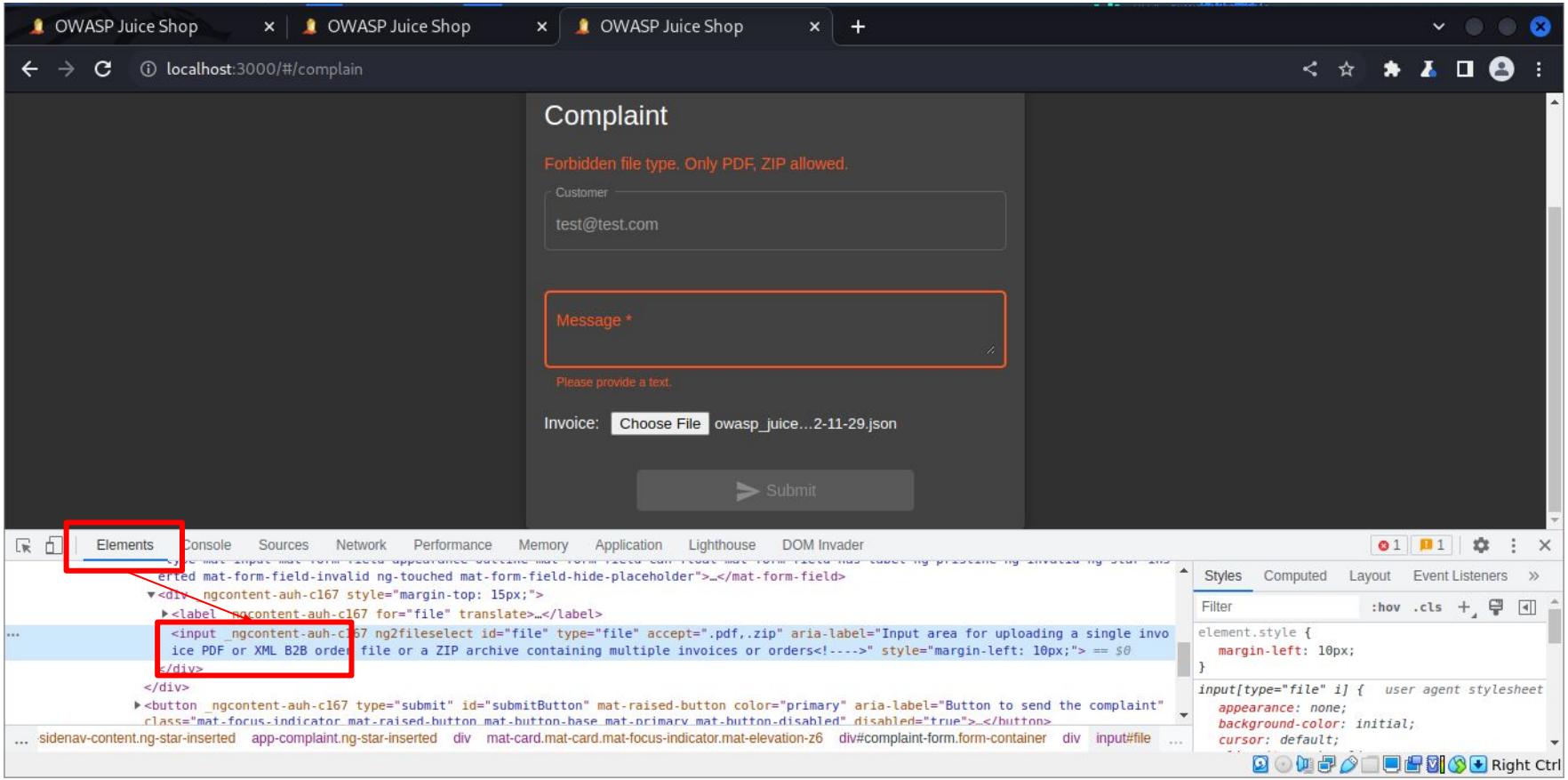
Broken Access Control: #Challenge: 3. View Basket

Security Misconfiguration → Challenge 1 - Deprecated Interface

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



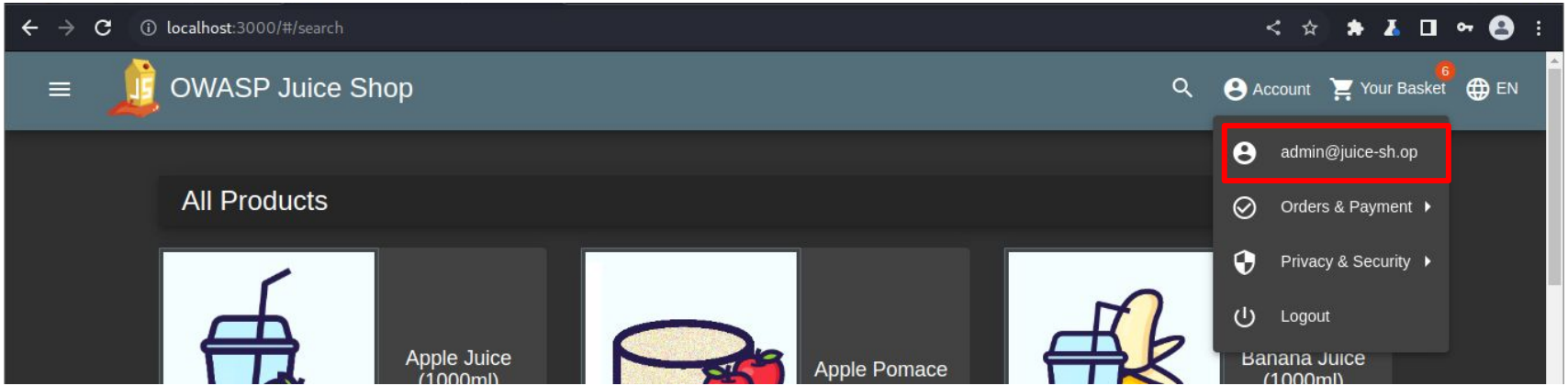
Security Misconfiguration: #Challenge: 1. Deprecated Interface



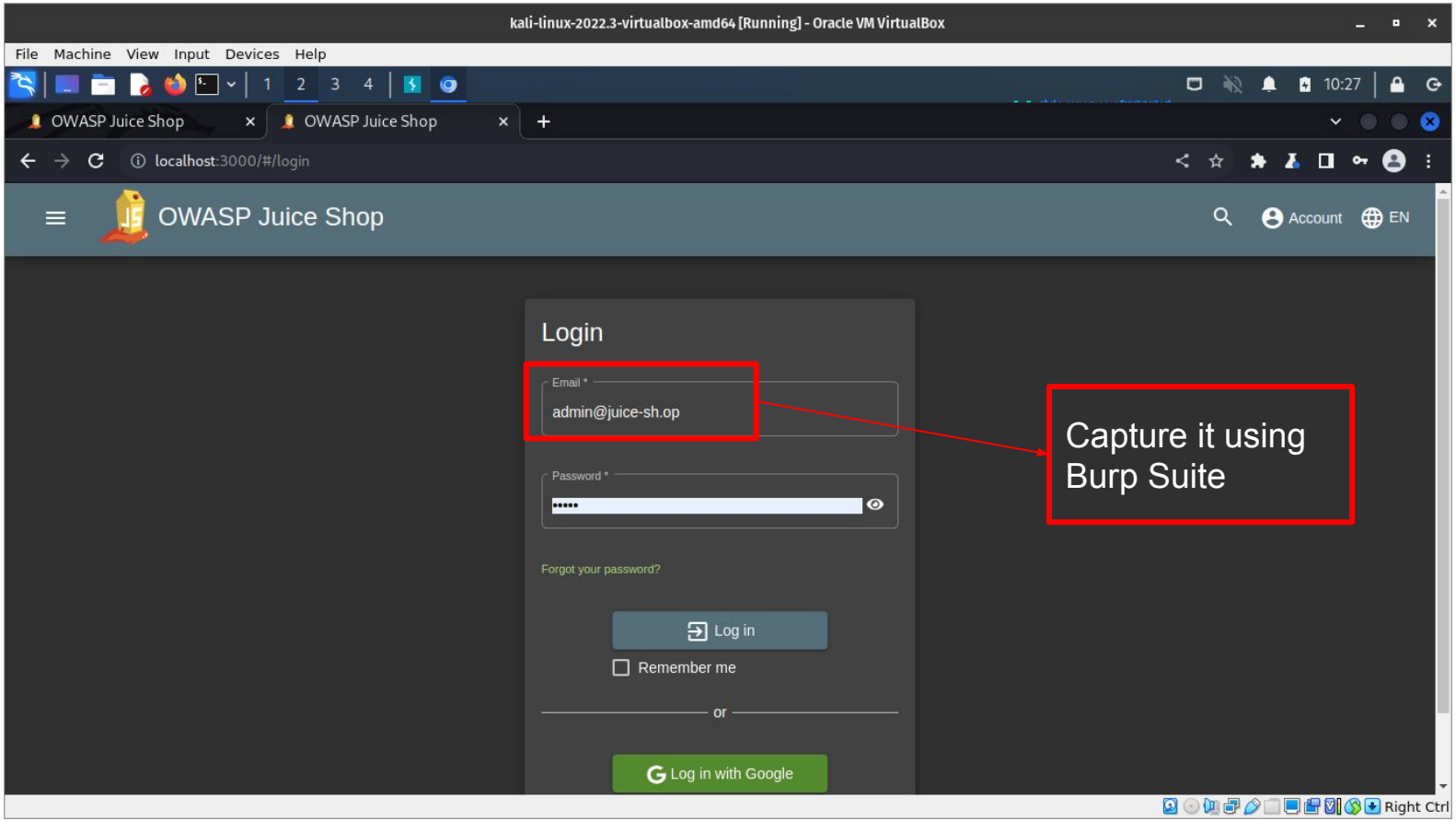
Security Misconfiguration: #Challenge: 1. Deprecated Interface

Sensitive Data Exposure -> OSINT

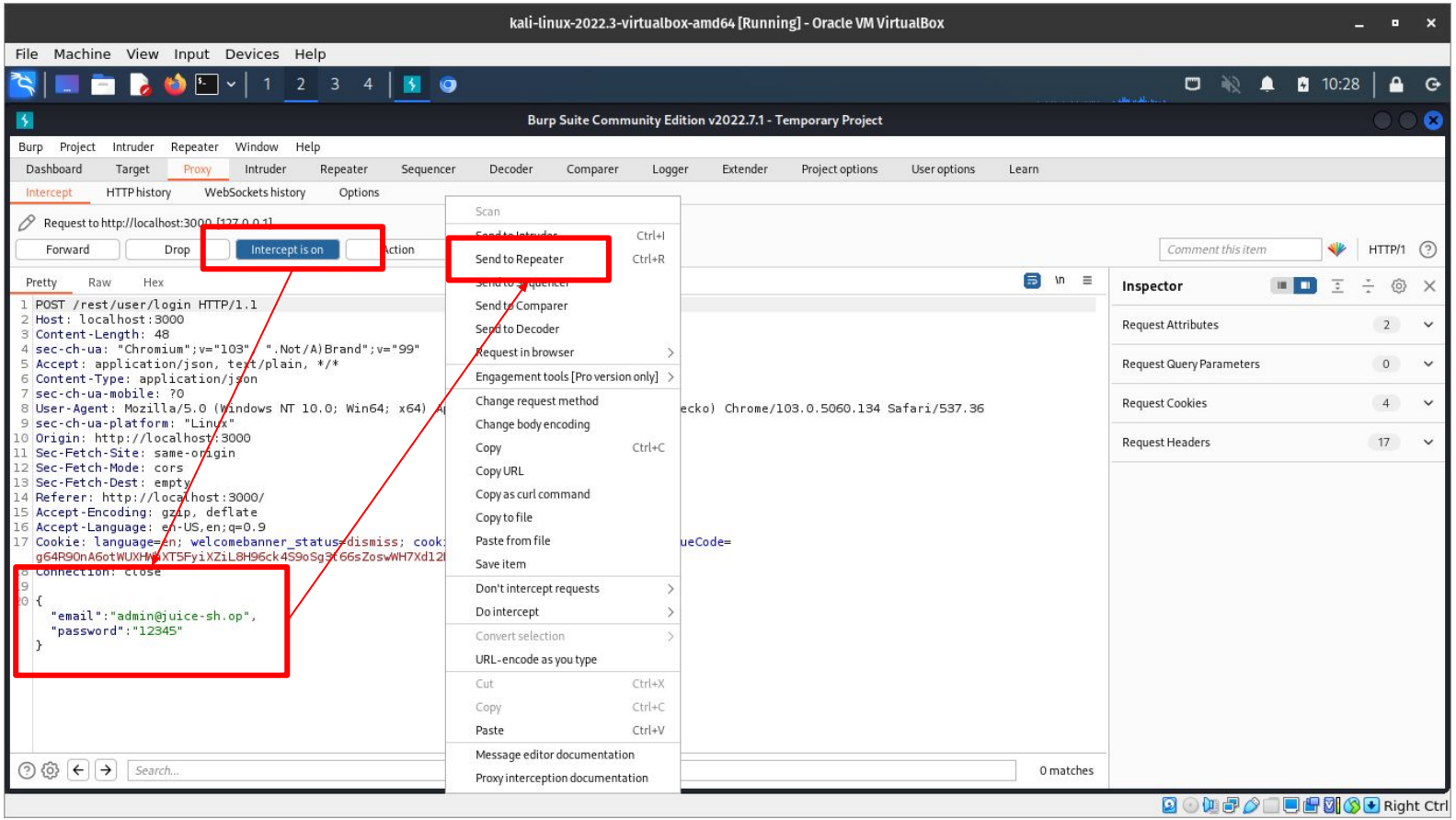
- Challenge 1 - Login MC SafeSearch
- Challenge 2 - Meta Geo Stalking
- Challenge 3 - Visual Geo Stalking



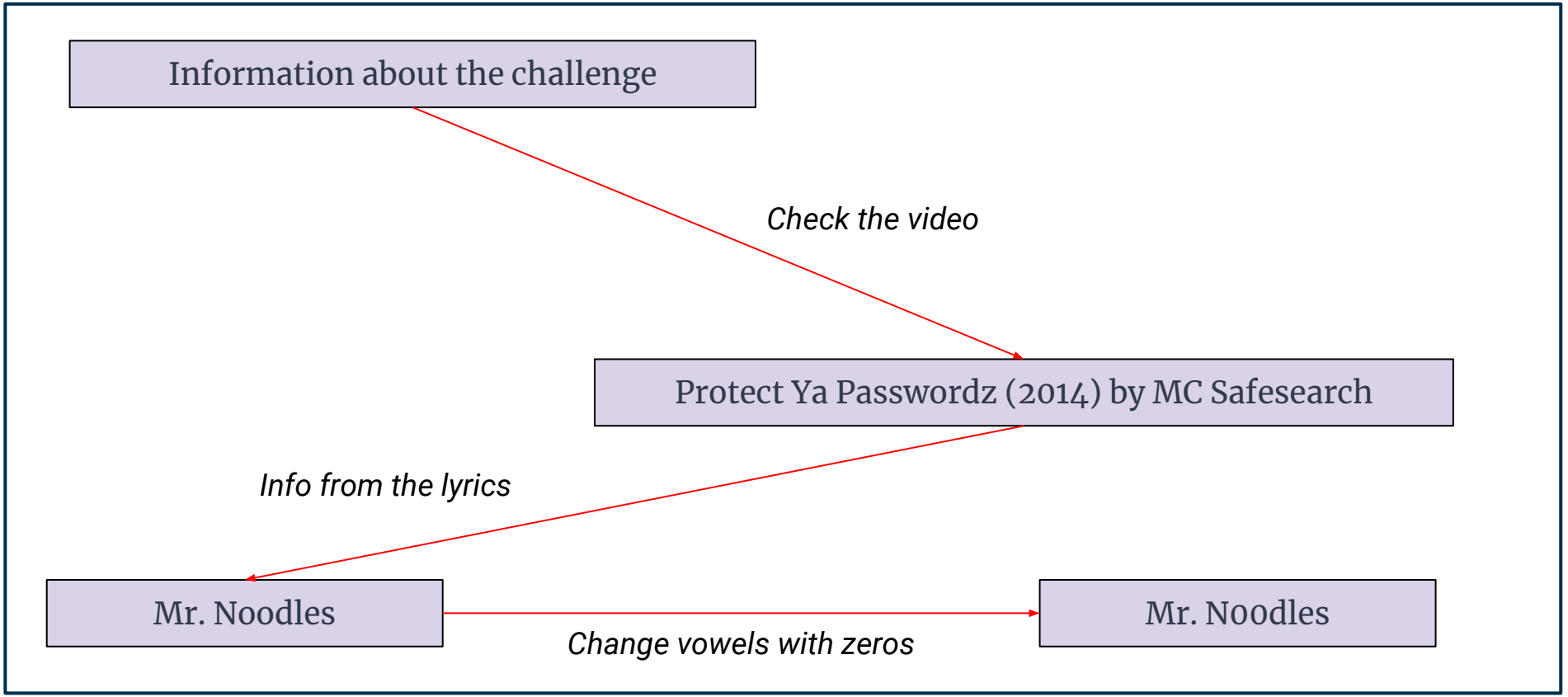
Sensitive Data Exposure -> OSINT: #Challenge: 1. Login MC SafeSearch



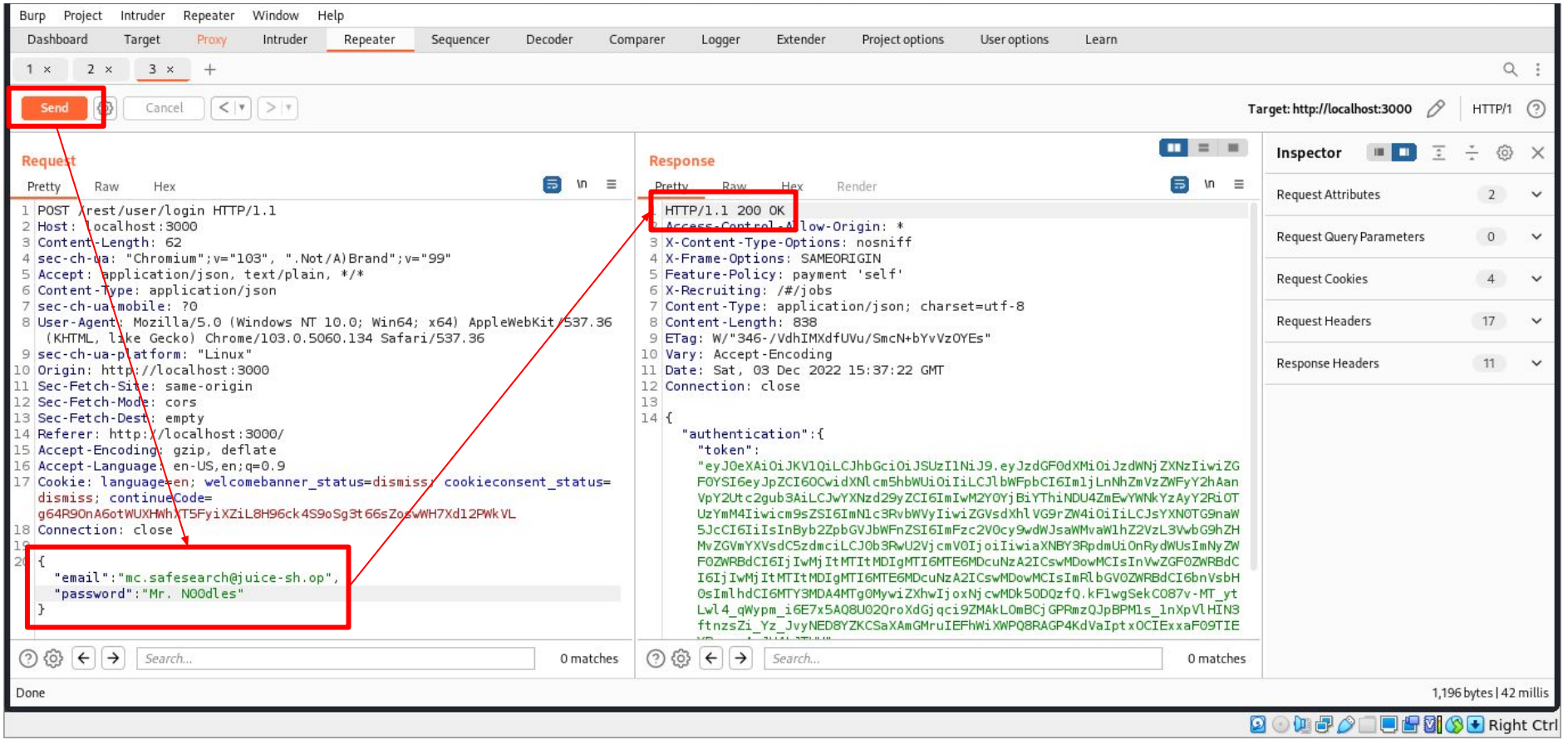
Sensitive Data Exposure -> OSINT: #Challenge: 1. Login MC SafeSearch



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



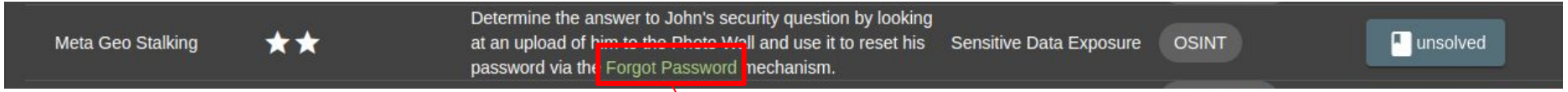
Sensitive Data Exposure -> OSINT: #Challenge: 1. Login MC SafeSearch



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

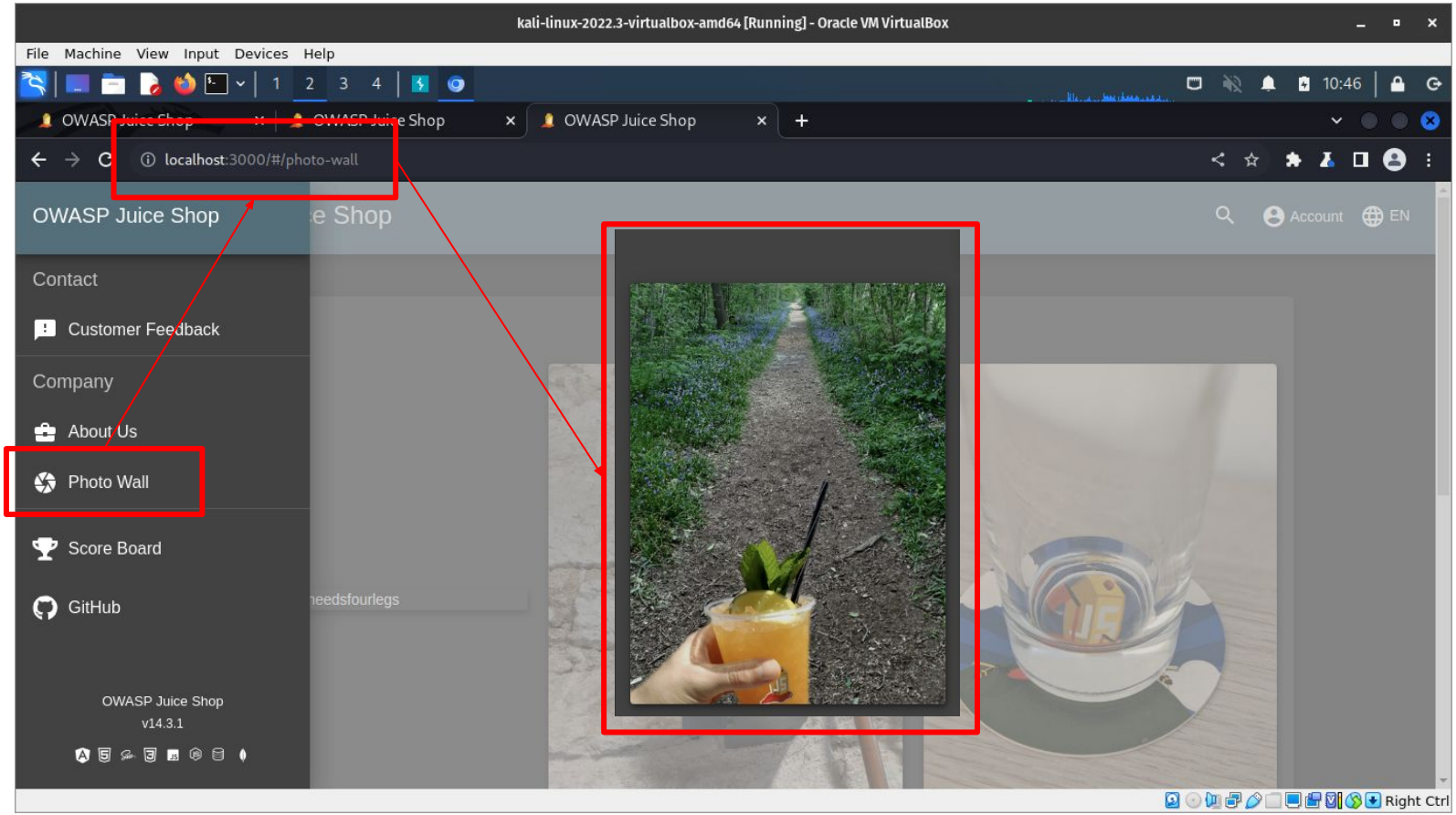
Sensitive Data Exposure -> OSINT

- Challenge 1 - Login MC SafeSearch
- Challenge 2 - Meta Geo Stalking
- Challenge 3 - Visual Geo Stalking



john@juice-sh.op

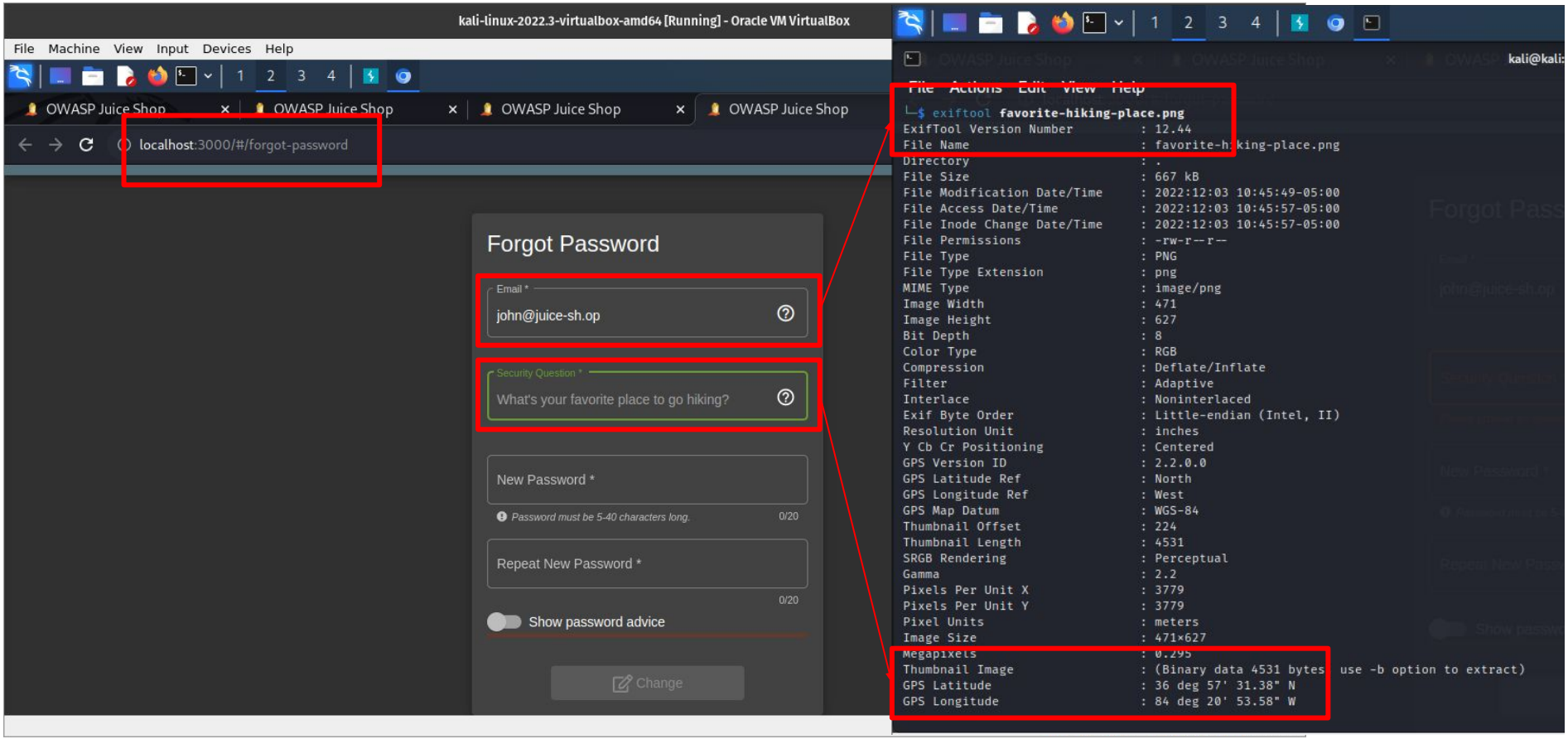
Sensitive Data Exposure -> OSINT: #Challenge: 2. Meta Geo Stalking



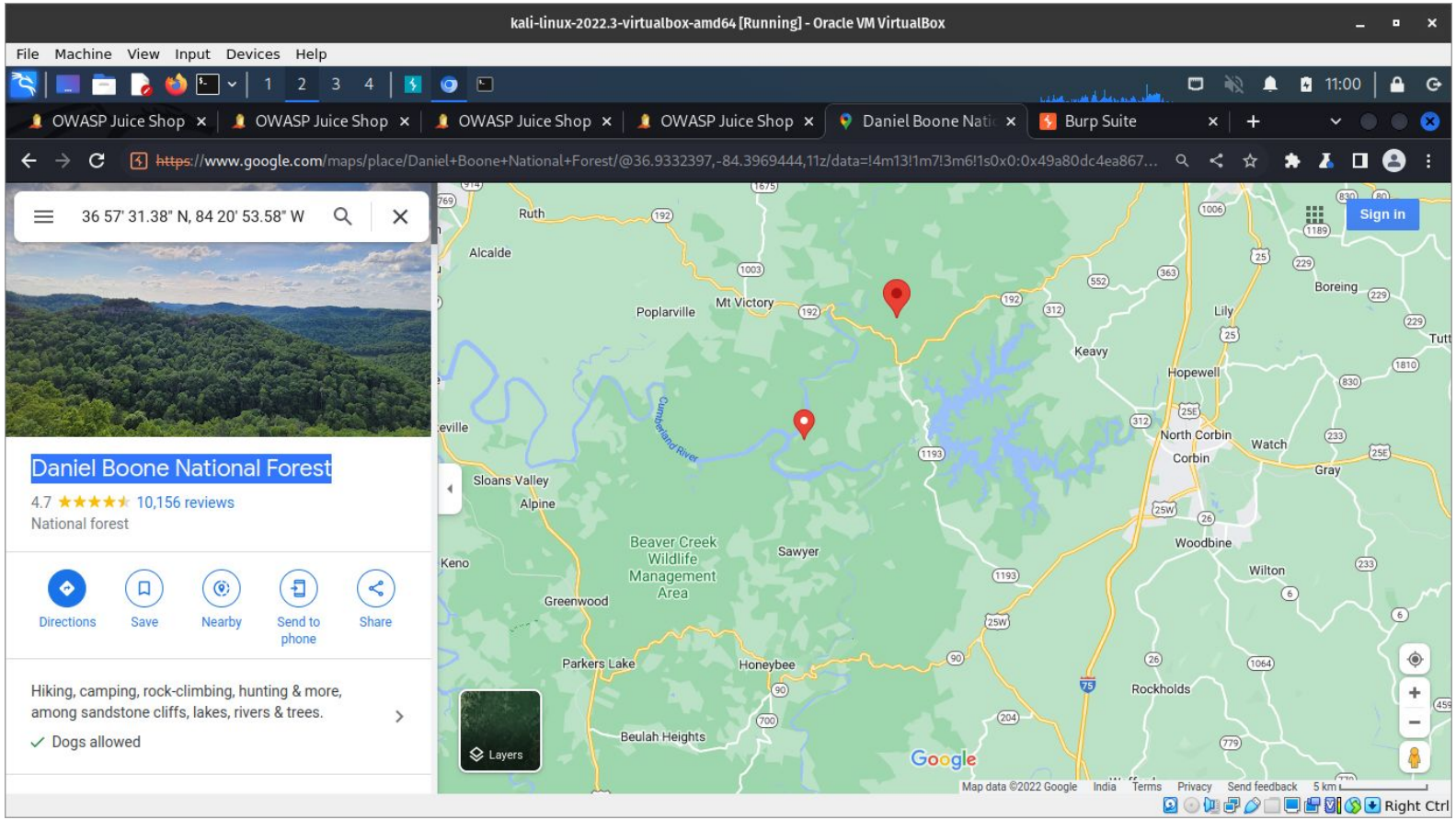
Sensitive Data Exposure -> OSINT: #Challenge: 2. Meta Geo Stalking

```
File  Actions  Edit  View  Help
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                      : 471×627
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



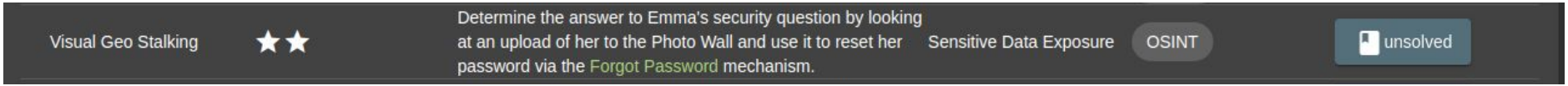
Sensitive Data Exposure -> OSINT: #Challenge: 2. Meta Geo Stalking



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

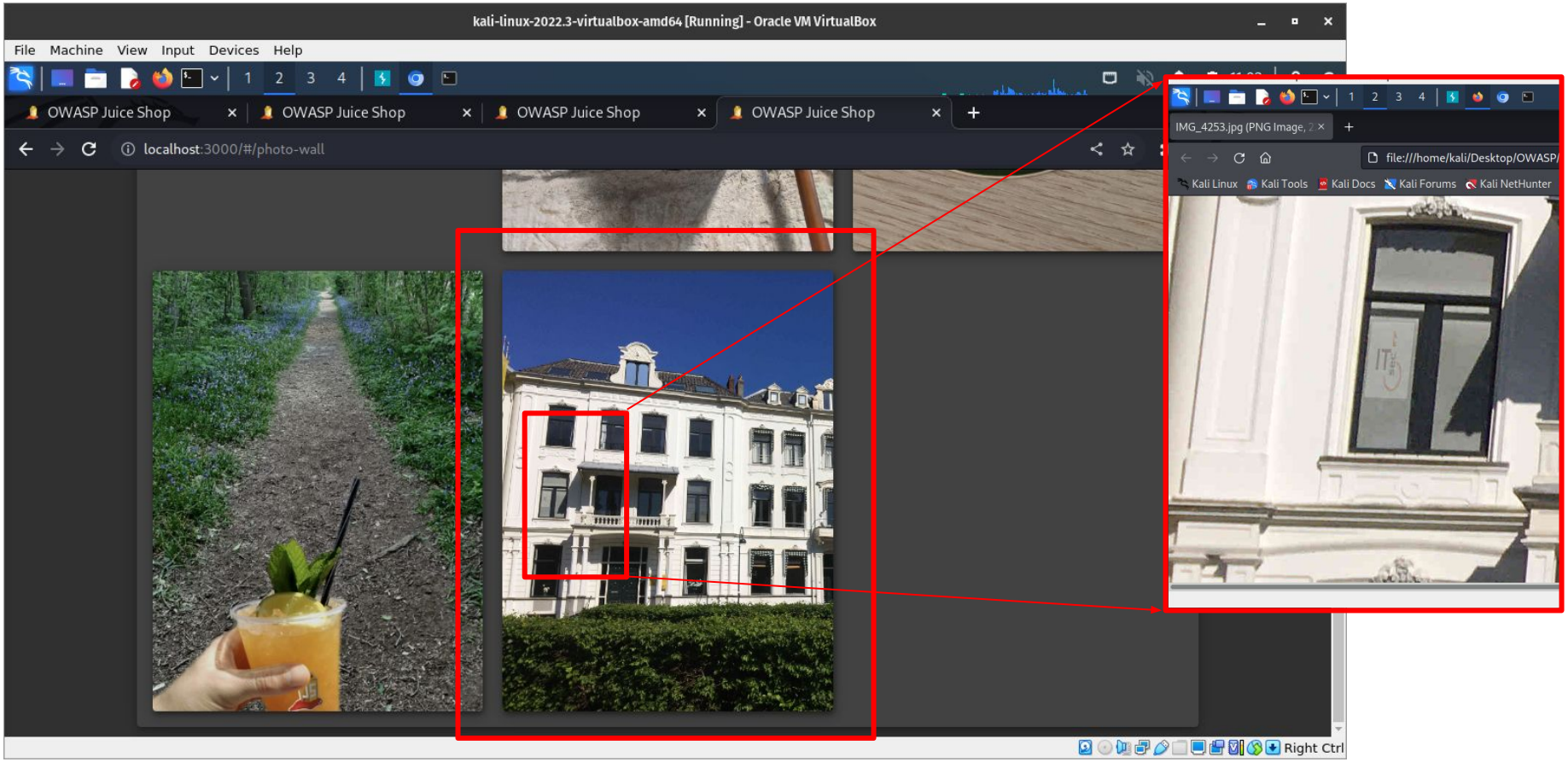
Sensitive Data Exposure -> OSINT

- Challenge 1 - Login MC SafeSearch
- Challenge 2 - Meta Geo Stalking
- Challenge 3 - Visual Geo Stalking

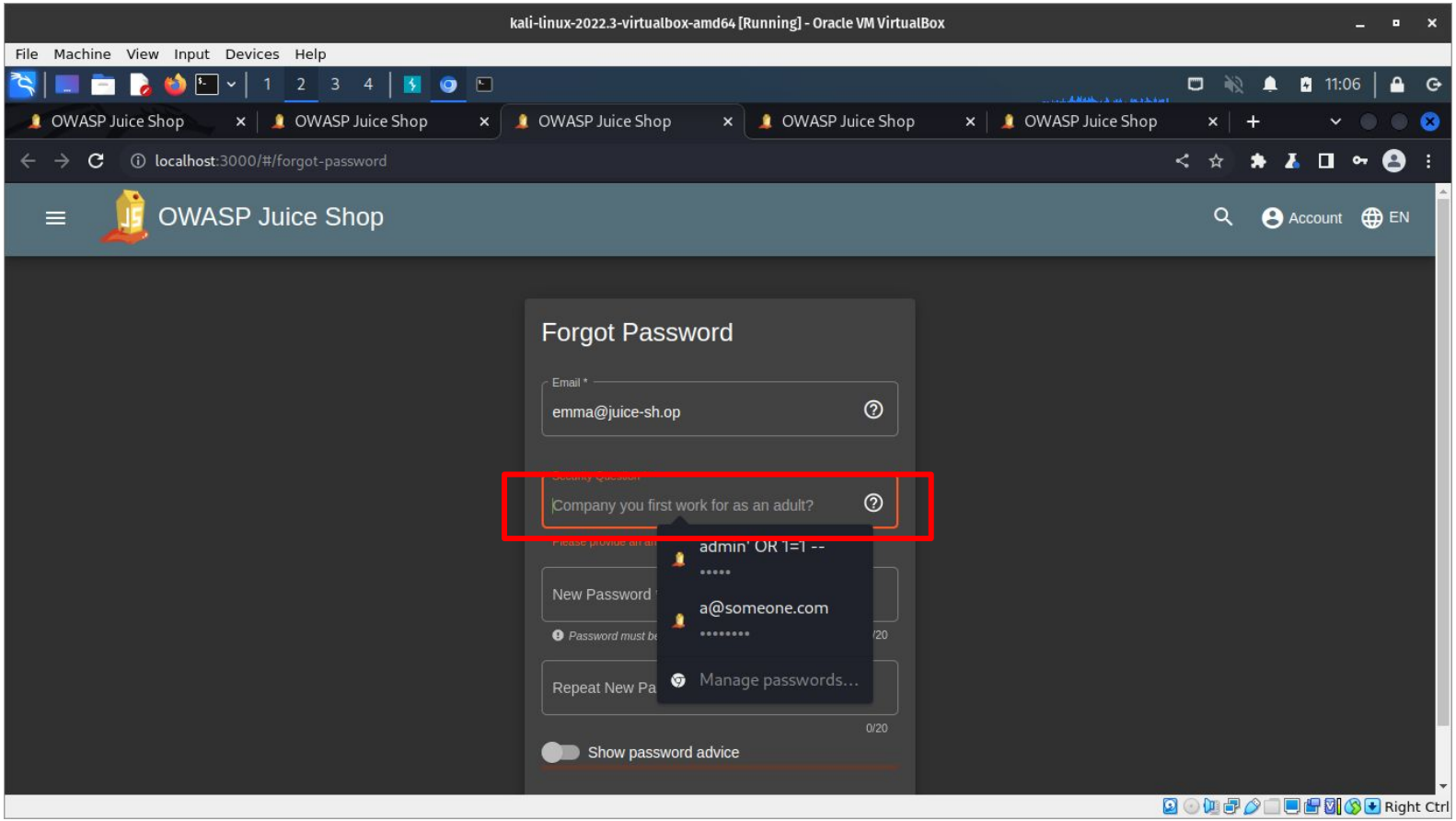


emma@juice-sh.op

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



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



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

Broken Authentication → Challenge 1 - Password Strength

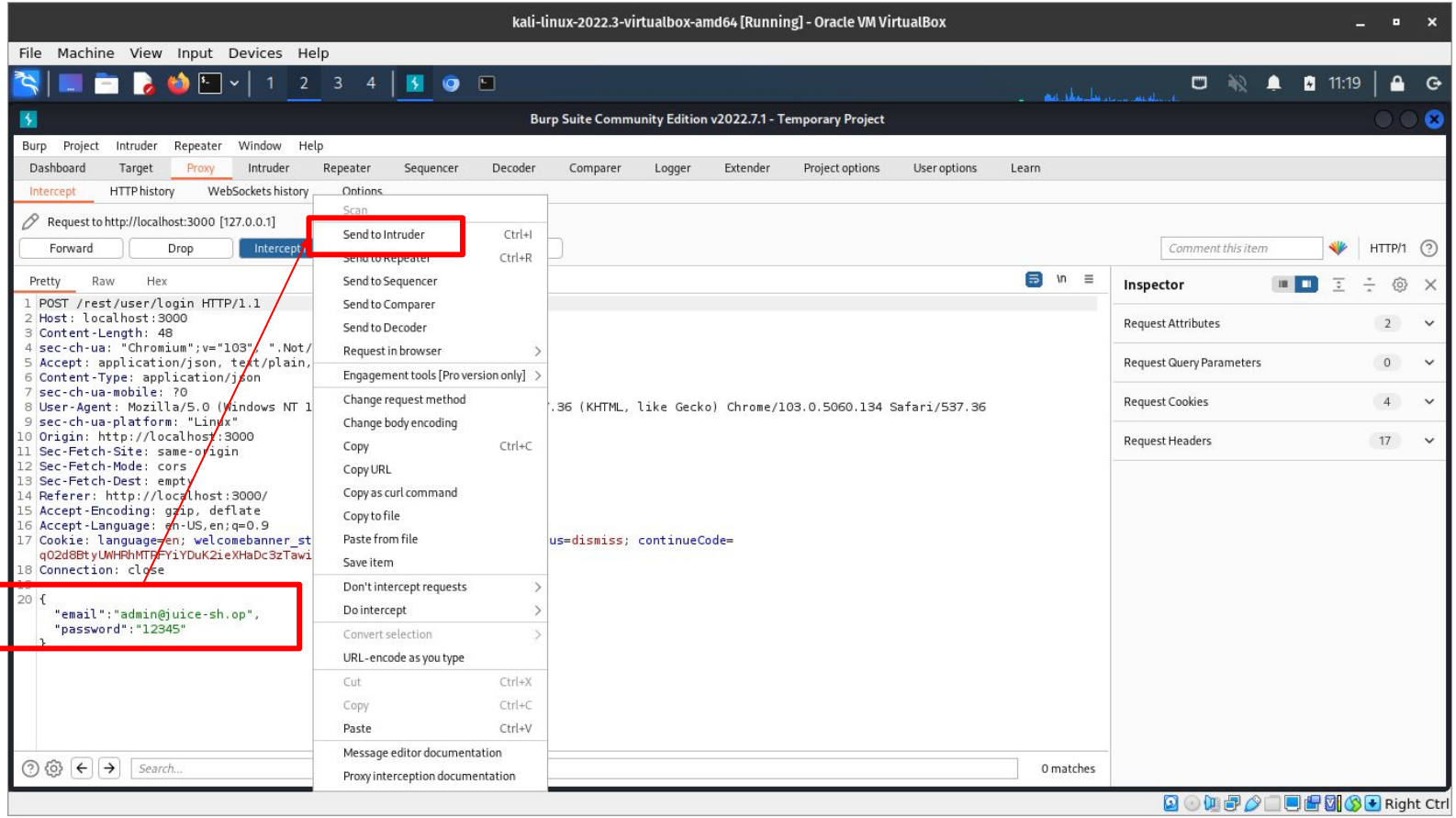
admin@juice-sh.op

Payload:

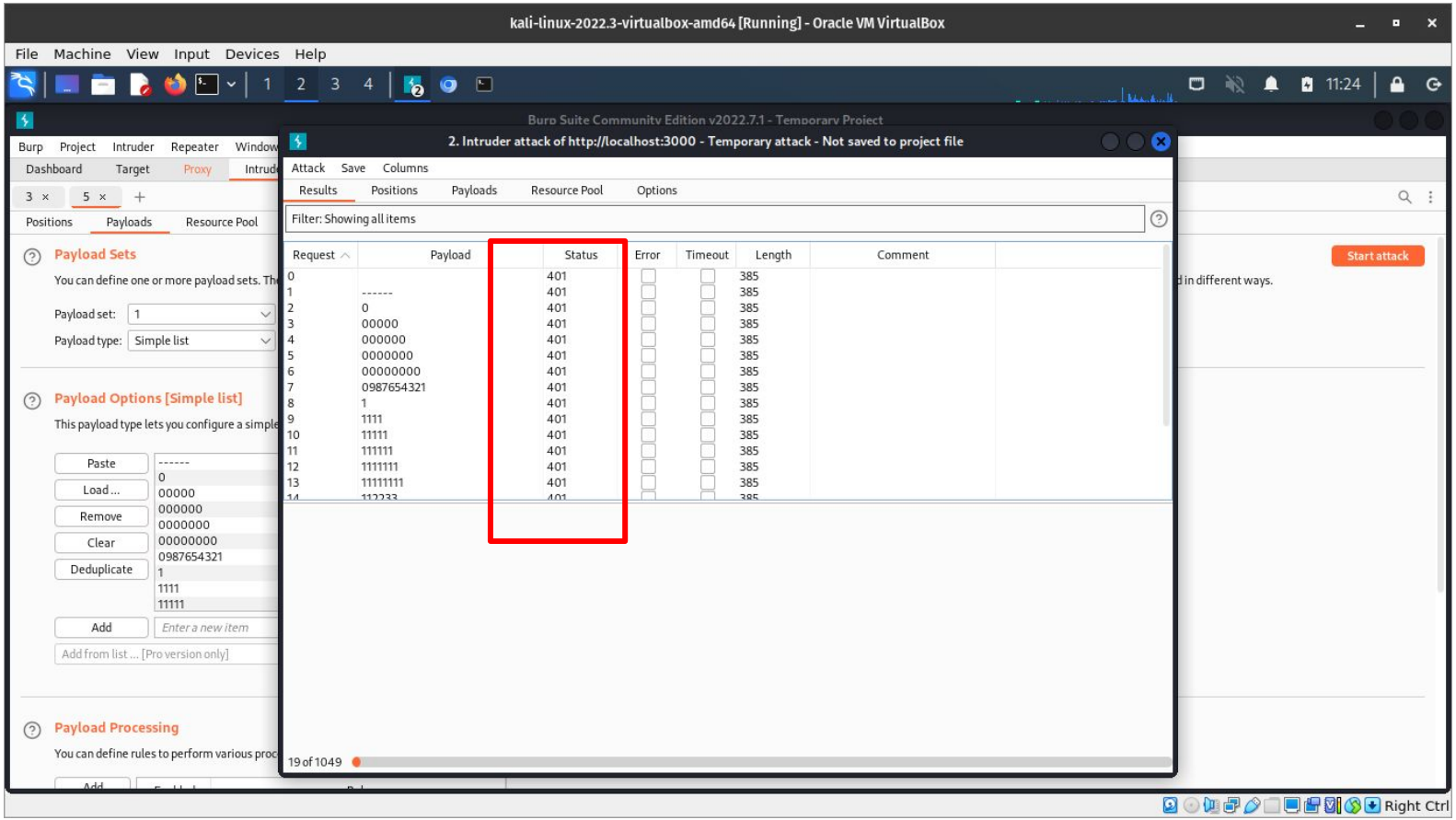
https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/best1050.txt

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

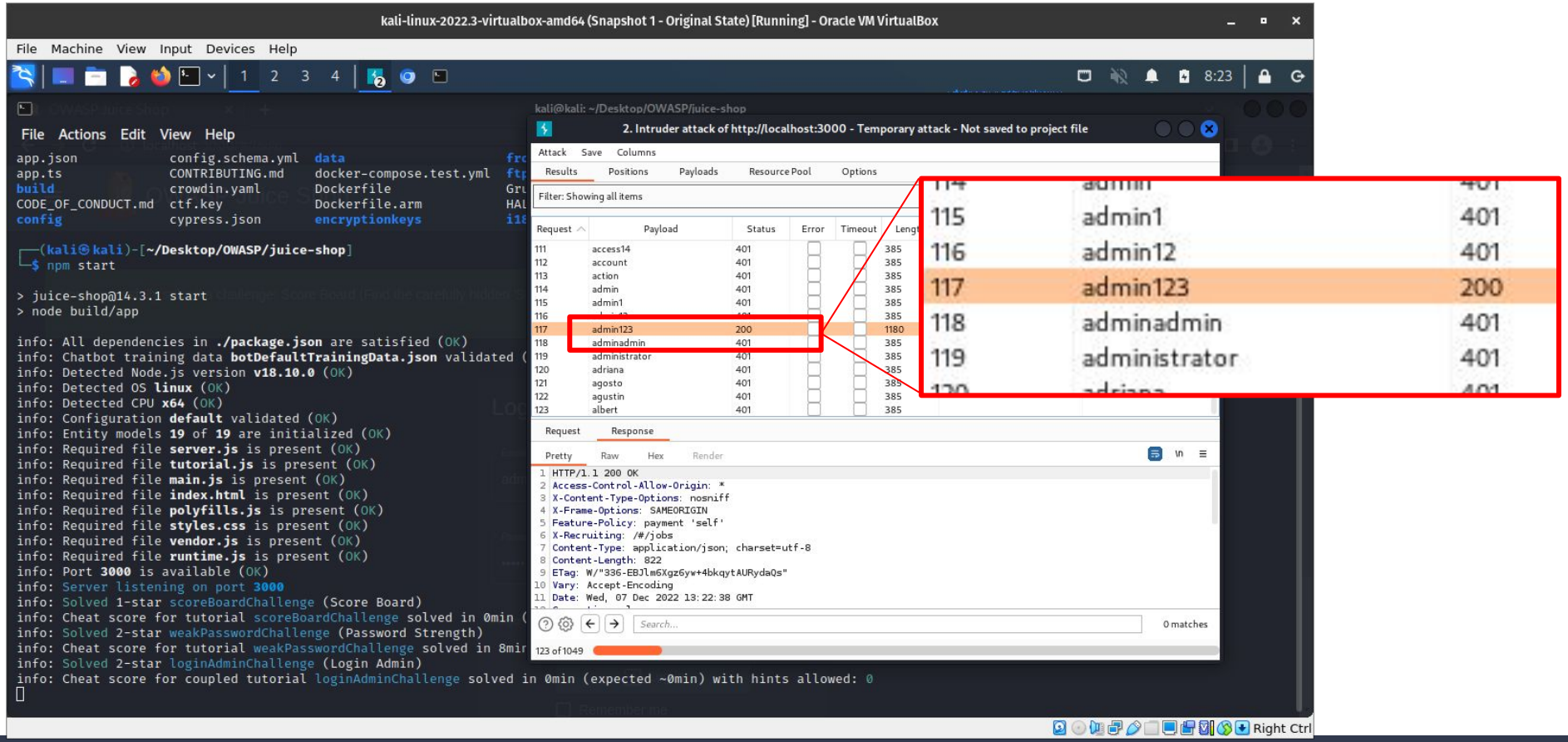
Broken Authentication: #Challenge: 1. Password Strength



Broken Authentication: #Challenge: 1. Password Strength



Broken Authentication: #Challenge: 1. Password Strength

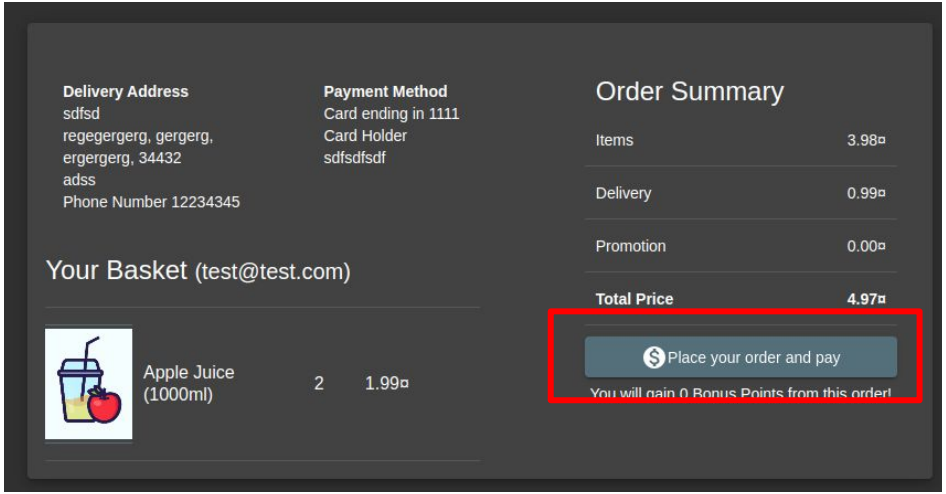


Broken Authentication: #Challenge: 1. Password Strength

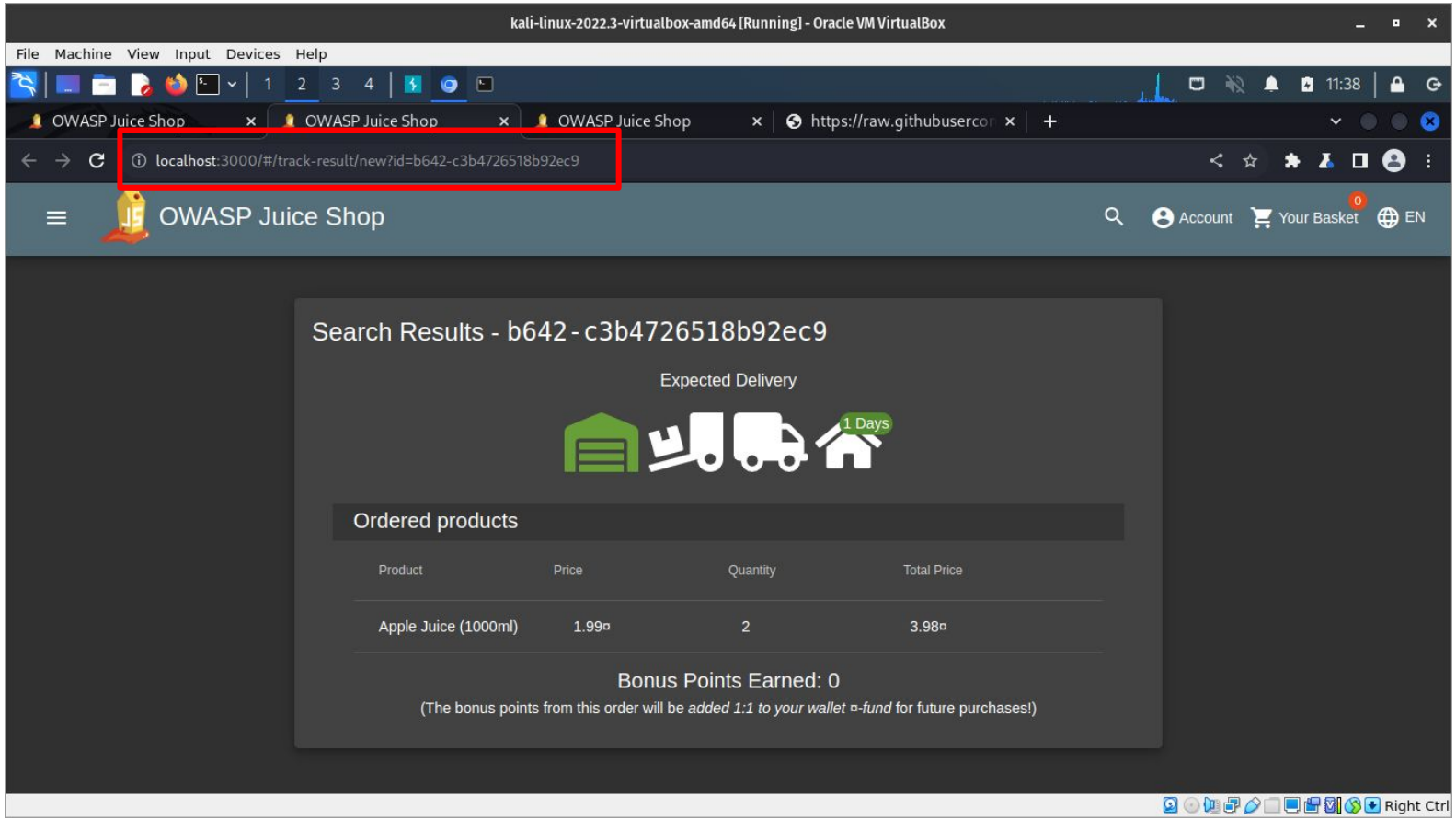
Cross Site Scripting (XSS) → Challenge 1 - Reflected XSS

Reflected XSS	★★	Perform a *reflected* XSS attack with `<iframe src="javascript:alert(`xss`)">`.	XSS	Danger Zone Good for Demos	unsolved

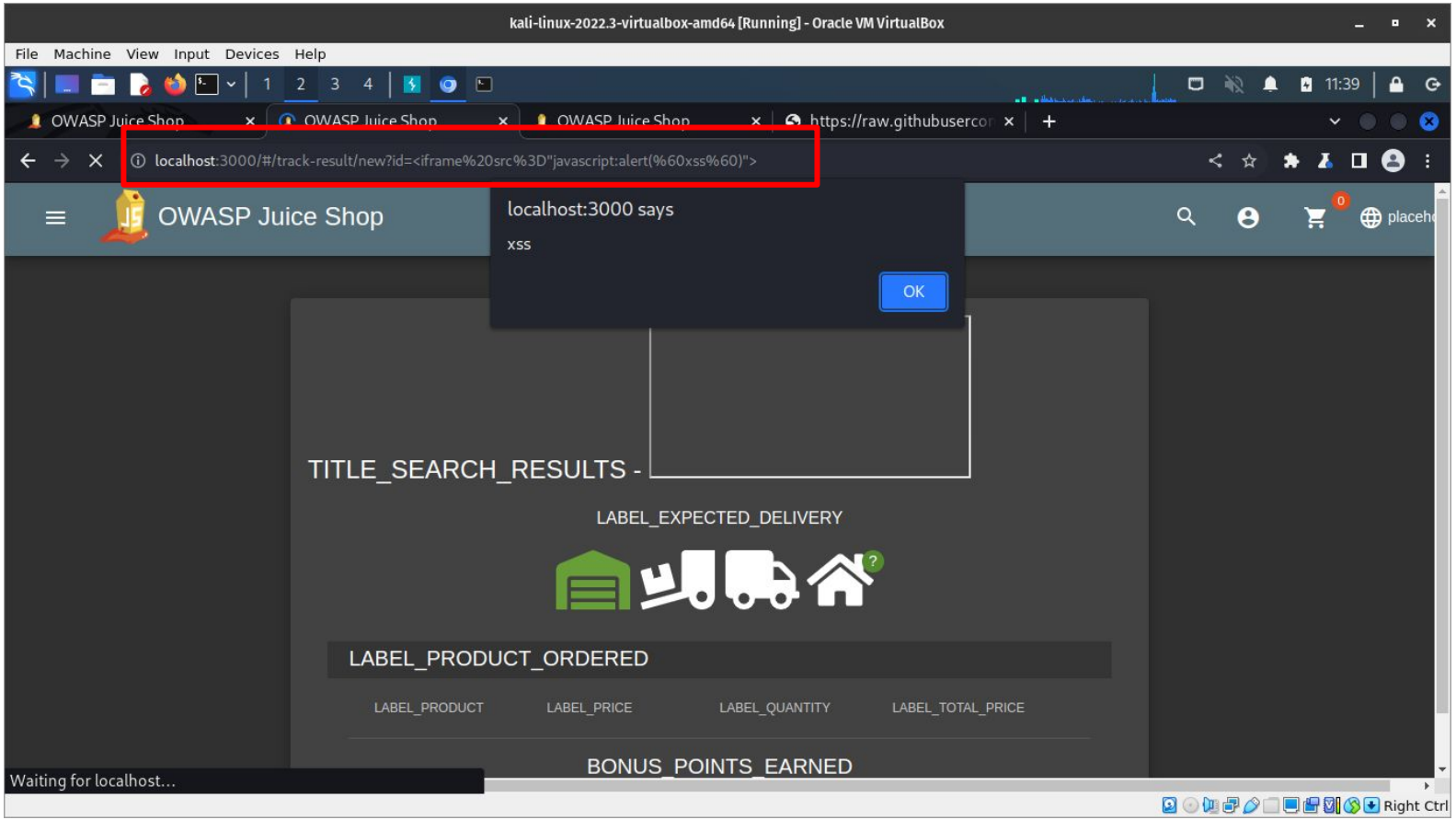
test@test.com



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



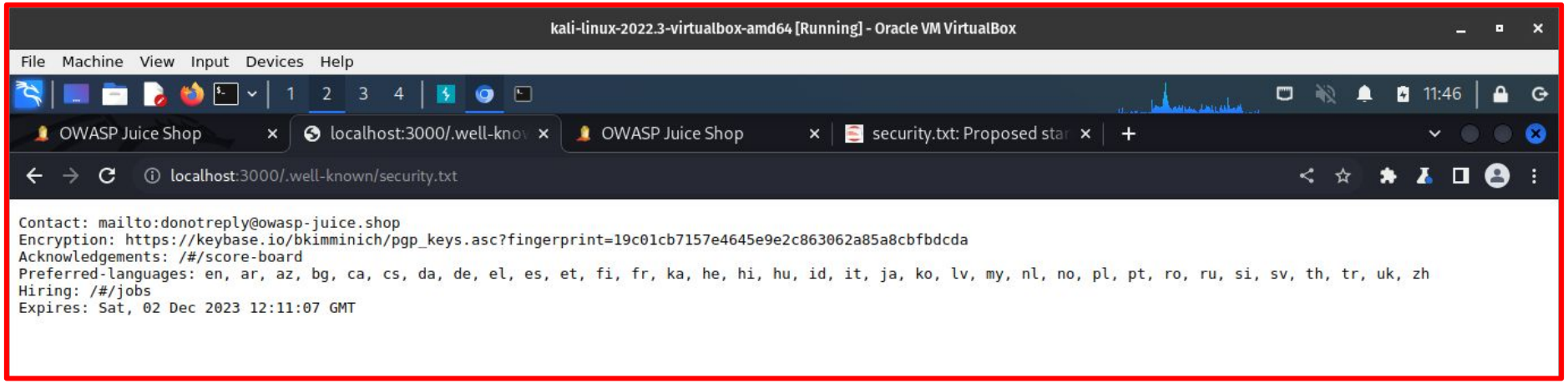
Cross Site Scripting (XSS): #Challenge: 1. Reflected XSS



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

Miscellaneous → Challenge 1 - Security Policy

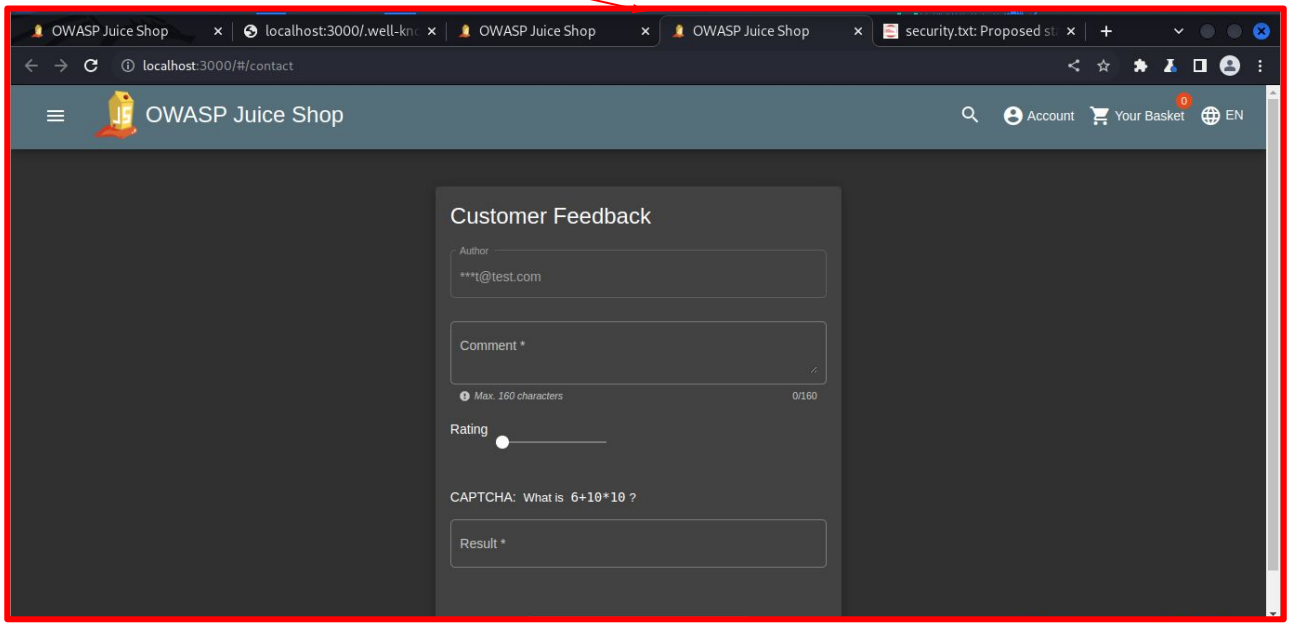
securitytxt.org



Miscellaneous: #Challenge: 1. Security Policy

Cryptographic Issues → Challenge 1 - Weird Crypto

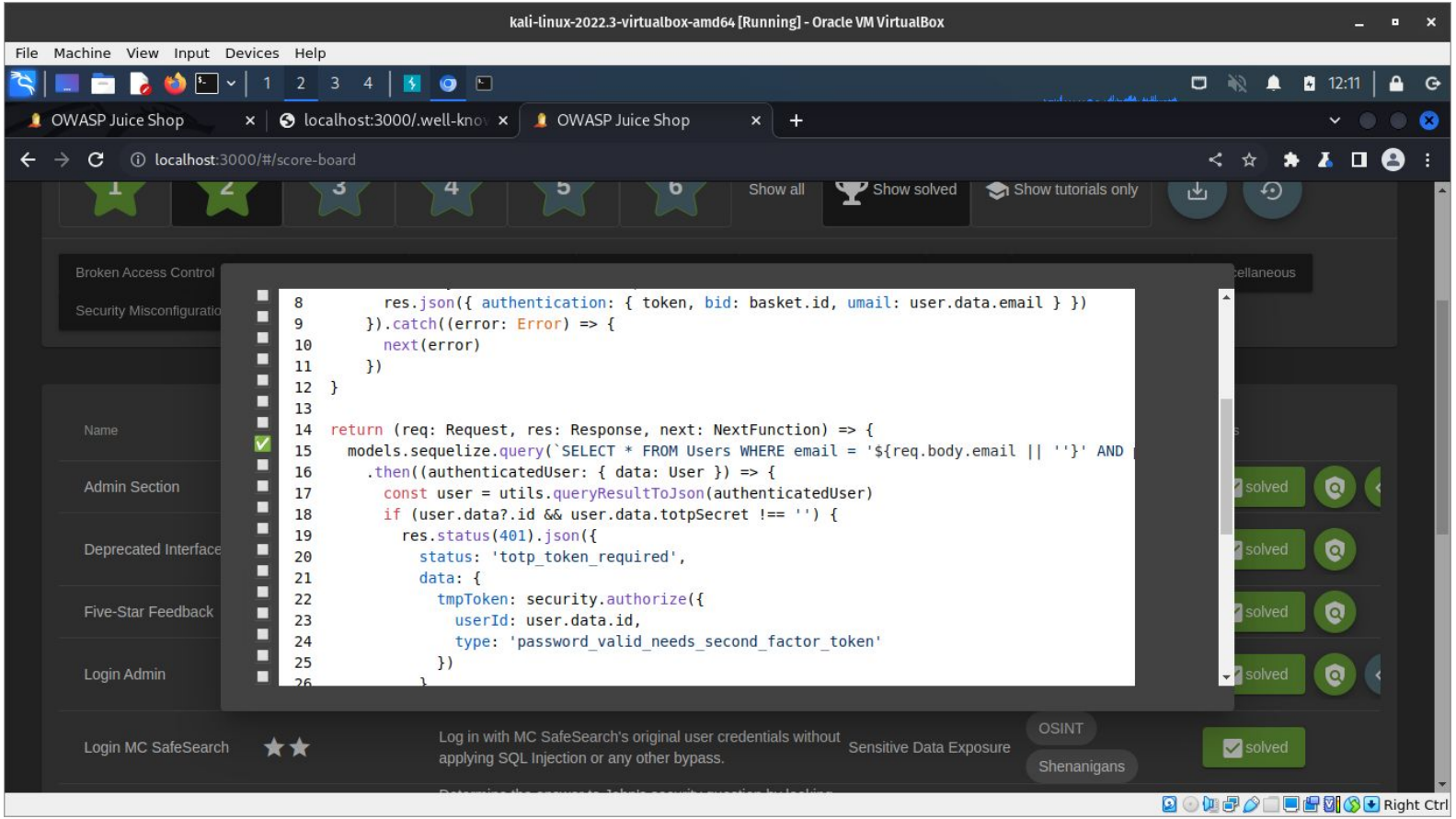
Weird Crypto ★★ Inform the shop about an algorithm or library it should definitely not use the way it does. Cryptographic Issues unsolved



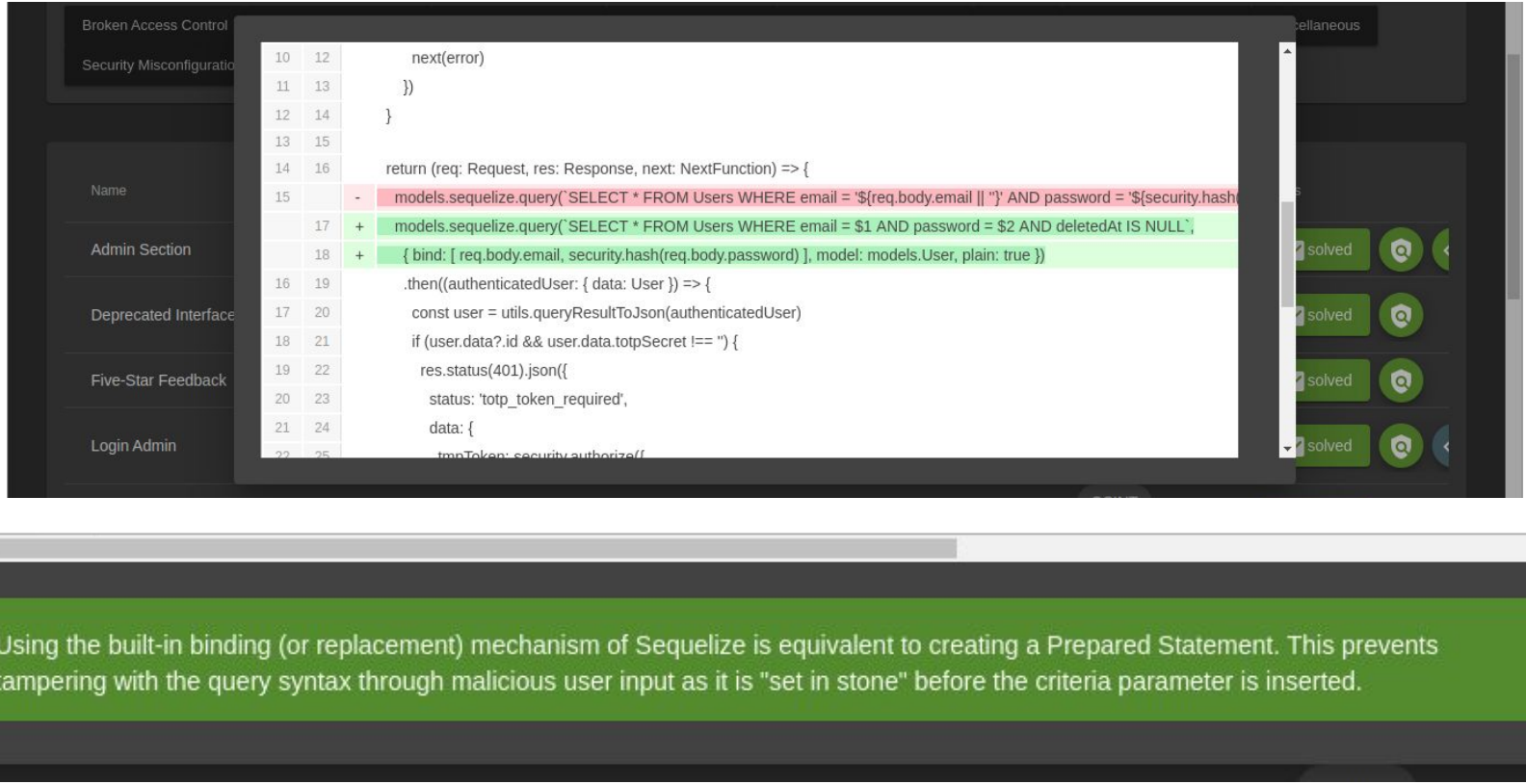
Miscellaneous: #Challenge: 1. Security Policy

Miscellaneous: #Coding Challenge 1: Admin Section

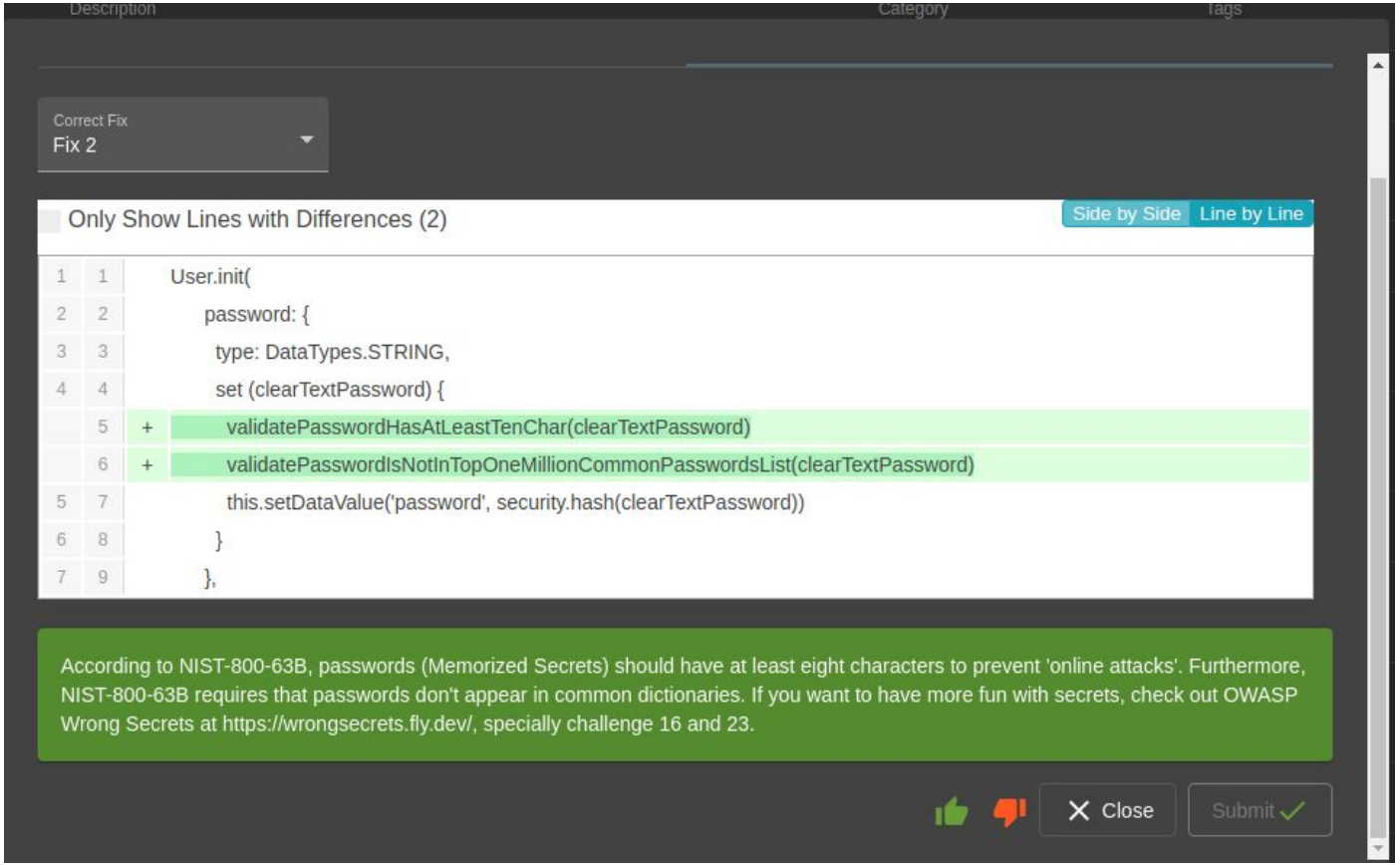
Miscellaneous: #Coding Challenge 1: Admin Section



Miscellaneous: #Coding Challenge 2: Login Admin



Miscellaneous: #Coding Challenge 2: Login Admin



Miscellaneous: #Coding Challenge 3: Password Strength