What Goes Wrong?

•••

Common Security Problems in Web Applications

Brian Myers PhD, CISSP, CCSK

Experience

- 20 years in software development
- 9 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
- Co-organizer, OWASP AppSec Days PNW

OWASP Top Ten Web App Risks

A01 – Broken Access Control

A02 – Cryptographic Failures

A03 – Injection

A04 – Insecure Design

A05 – Security Misconfiguration

A06 – Vulnerable & Outdated Components

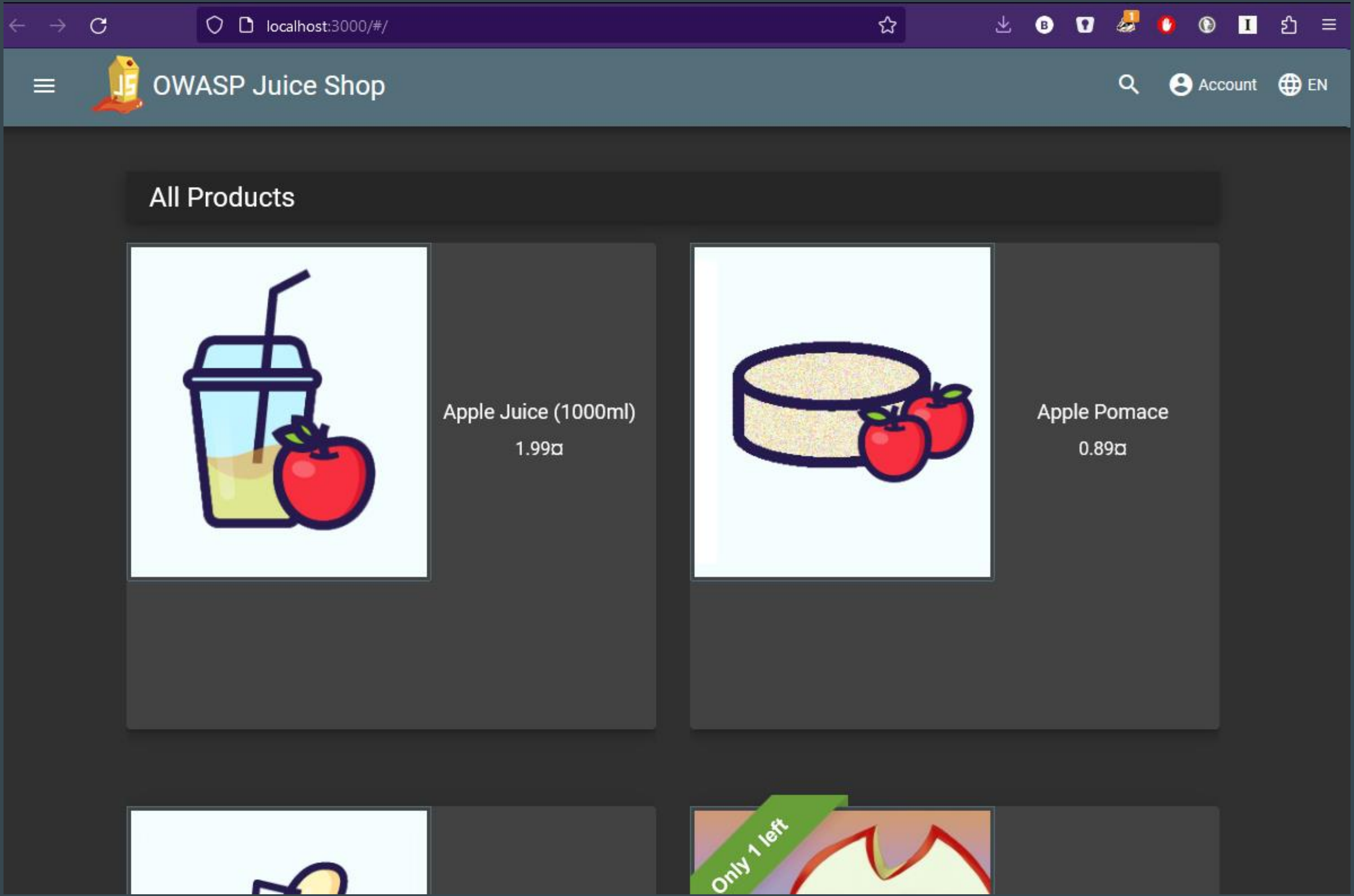
A07 – Identification & Authentication Failures

A08 – Software & Data Integrity Failures

A09 – Security Logging & Monitoring Failures

A10 – Server-Side Request Forgery (SSRF)

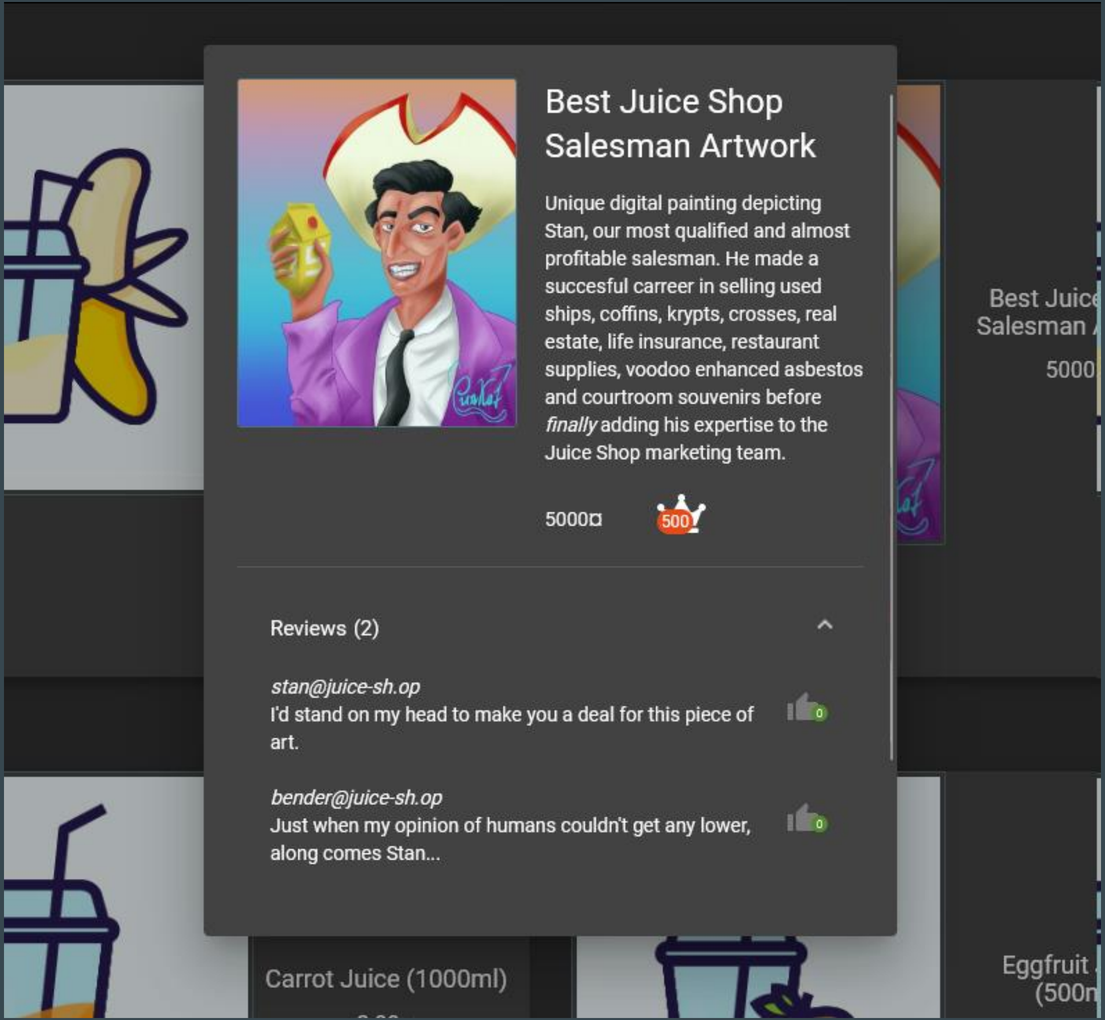
OWASP Juice Shop:
Reconnaissance



All Products

Apple Juice (1000ml)
1.99¤

Apple Pomace
0.89¤



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¤

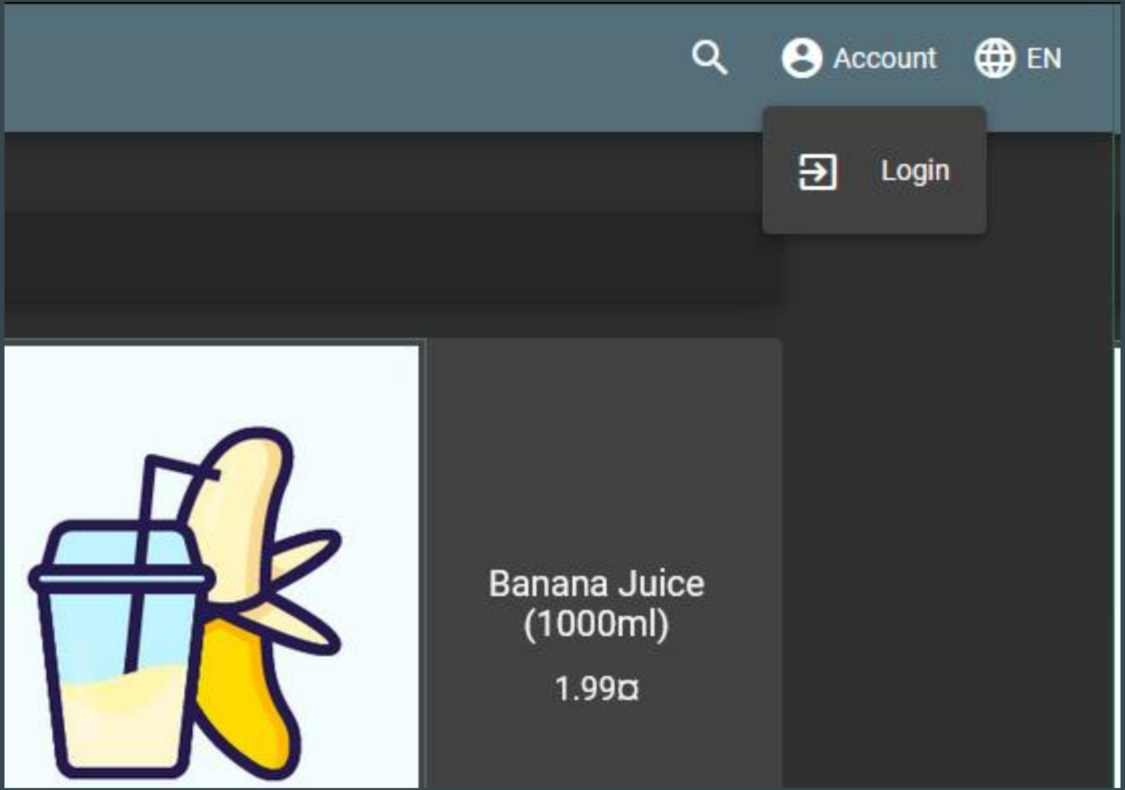
Reviews (2)

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

0

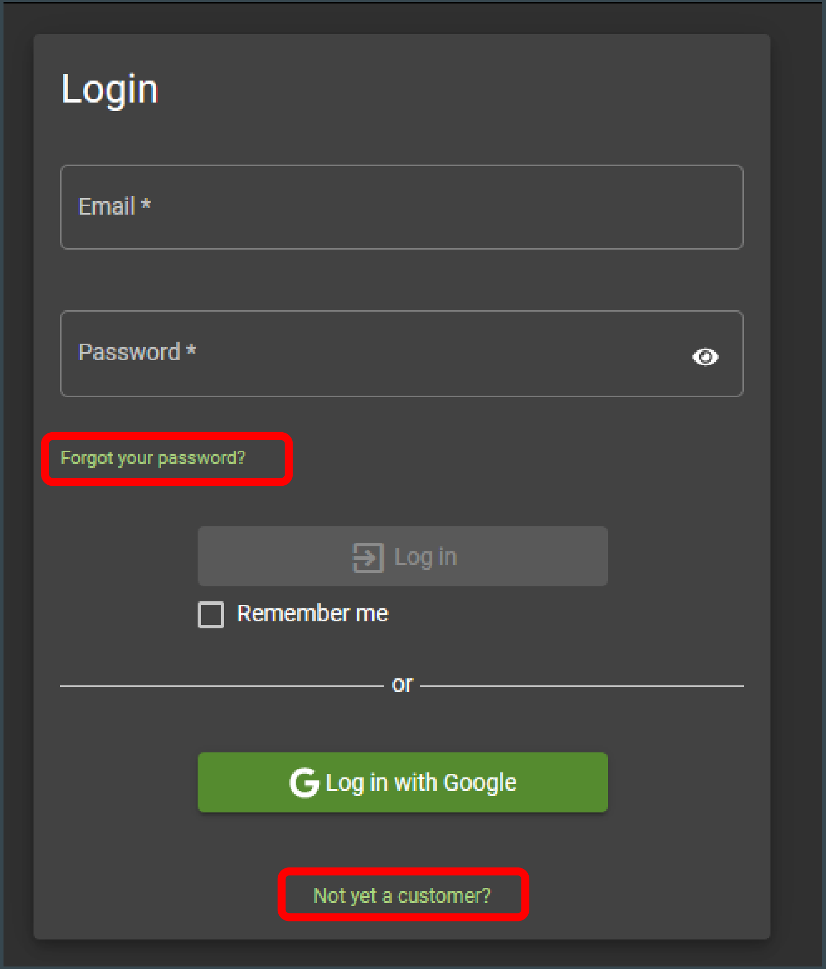
bender@juice-sh.op
Just when my opinion of humans couldn't get any lower, along comes Stan...

0



Banana Juice (1000ml)

1.99¤

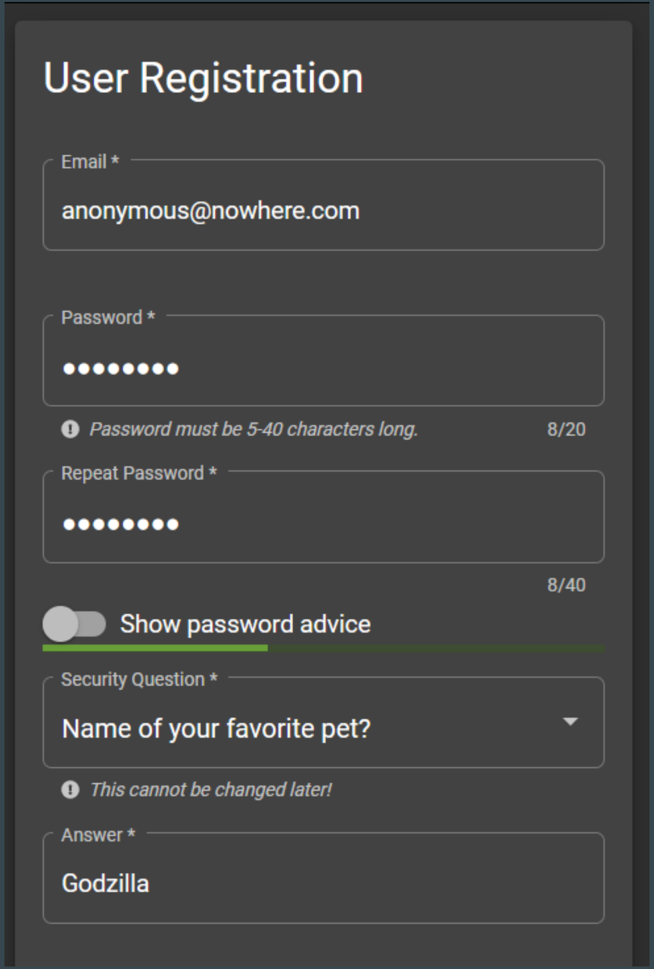


Login

Email *

Password *

□ Remember me



User Registration

Email *: anonymous@nowhere.com

Password *: ●●●●●●●●

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

Repeat Password *: ●●●●●●●●

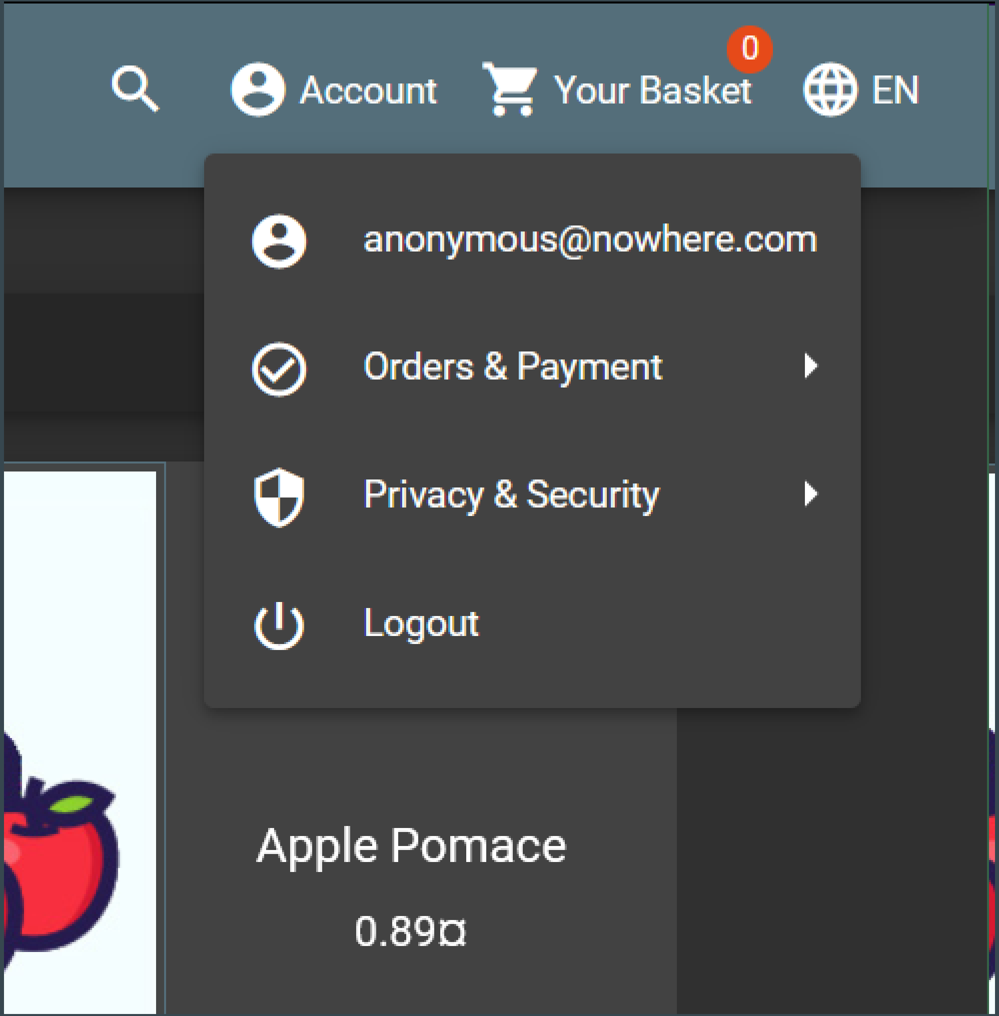
8/40

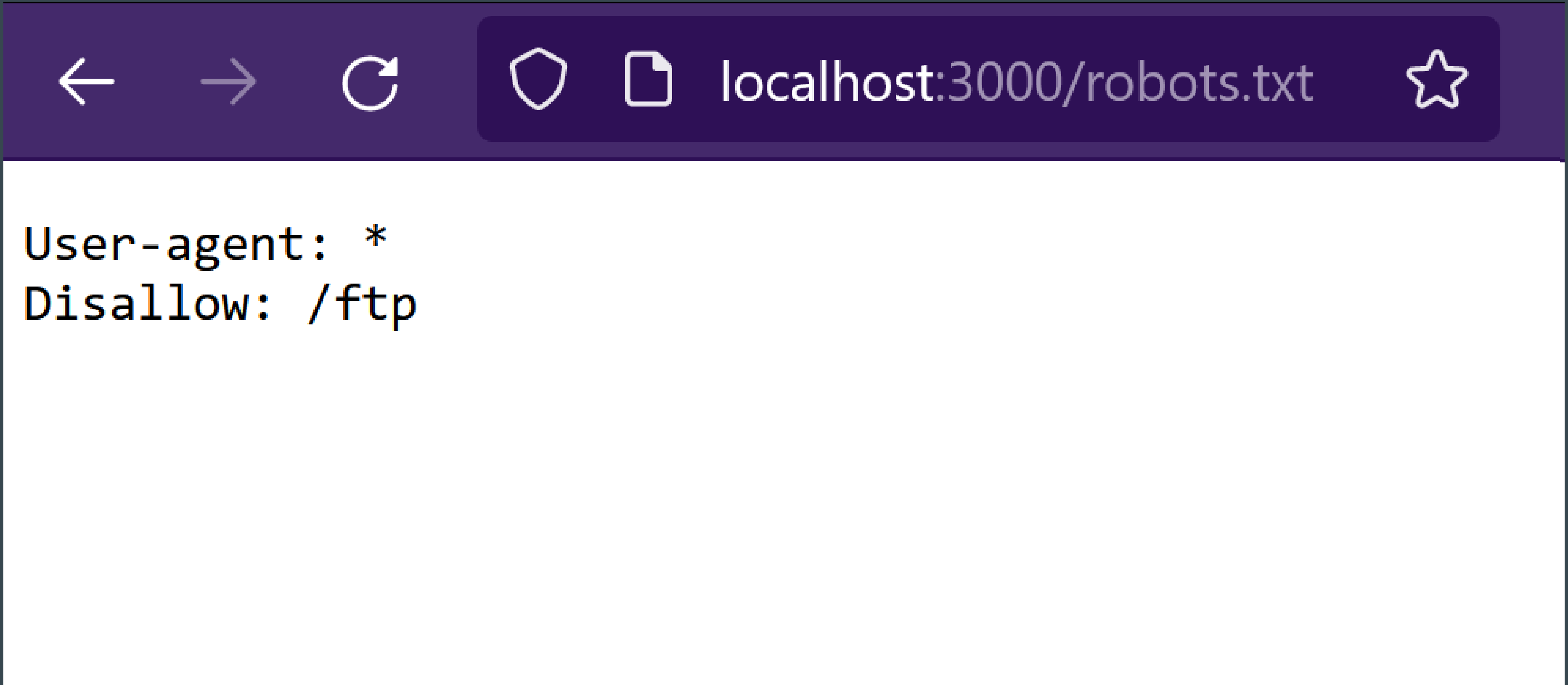
Show password advice

Security Question *: Name of your favorite pet?

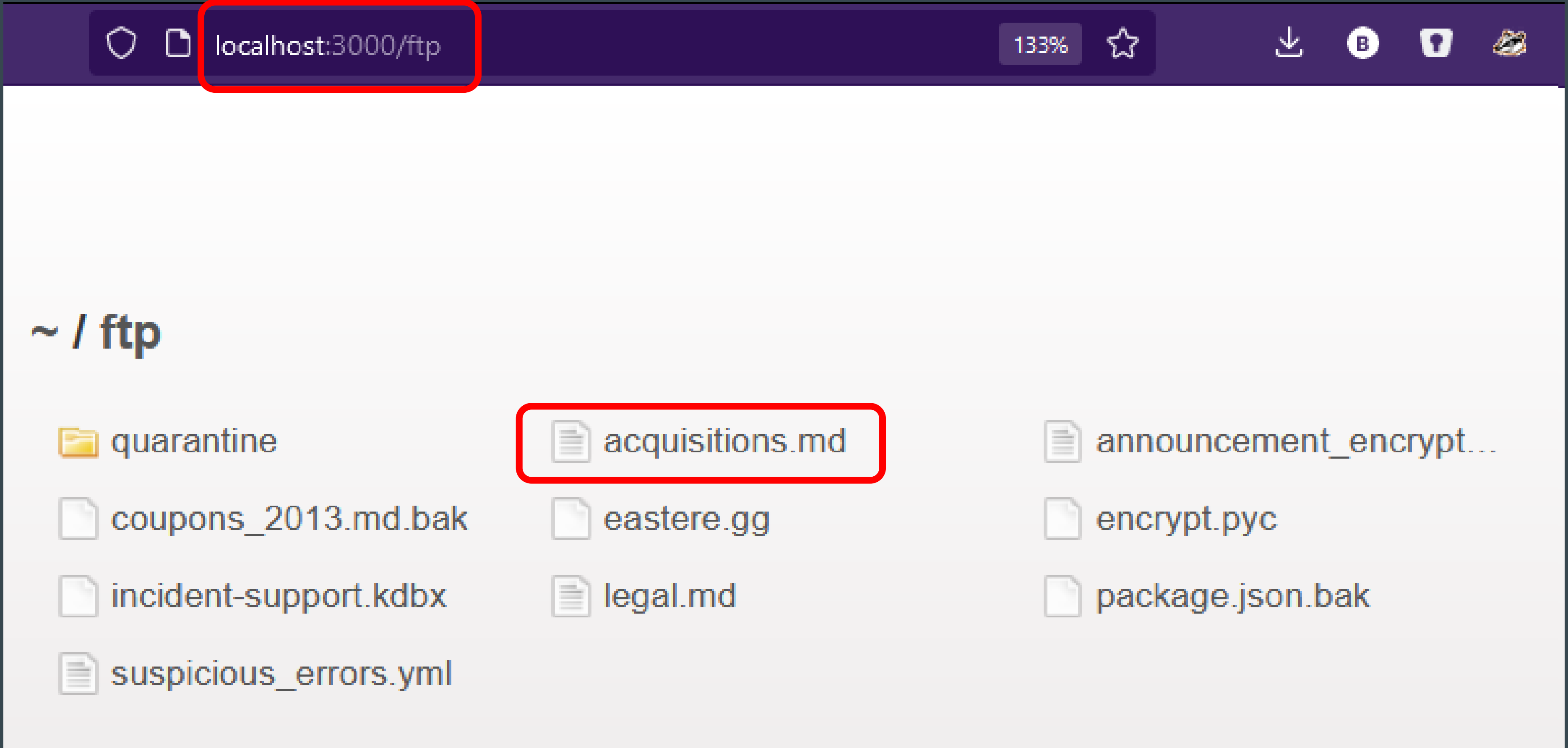
This cannot be changed later!

Answer *: Godzilla


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



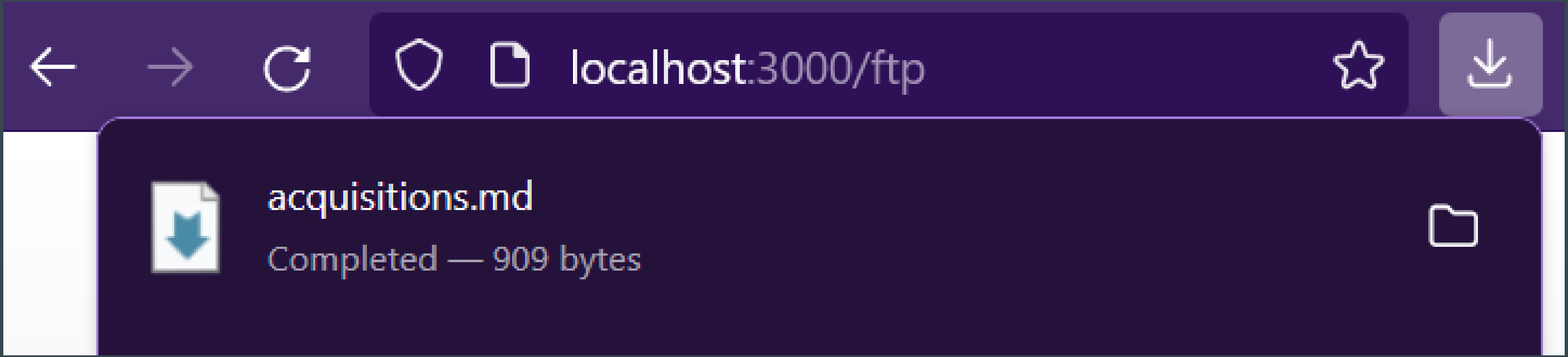
```
User-agent: *
Disallow: /ftp
```



localhost:3000/ftp

~ / ftp

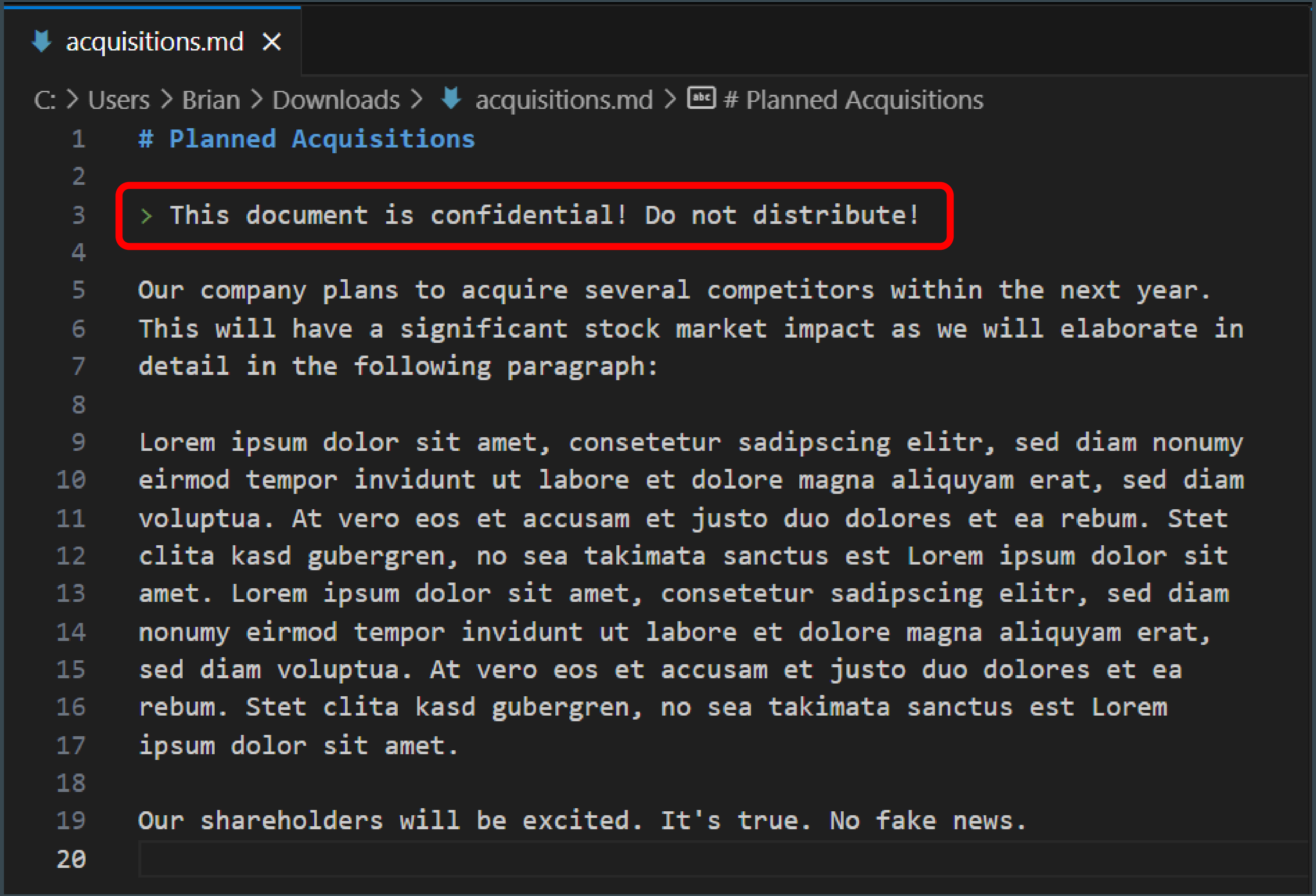
- quarantine
- acquisitions.md
- announcement_encrypt...
- coupons_2013.md.bak
- eastere.gg
- encrypt.pyc
- incident-support.kdbx
- legal.md
- package.json.bak
- suspicious_errors.yml



localhost:3000/ftp

acquisitions.md

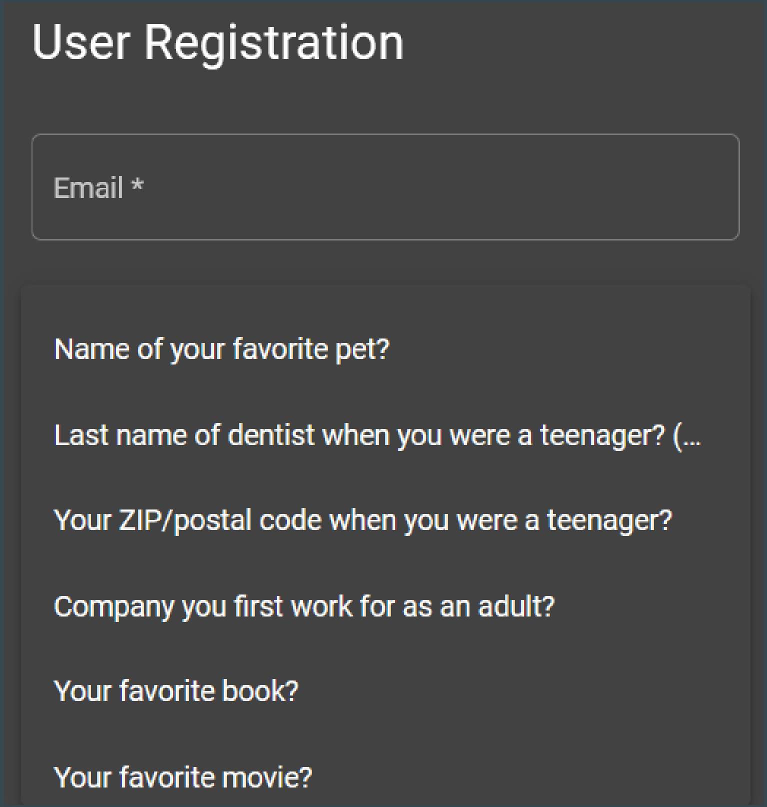
Completed — 909 bytes


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

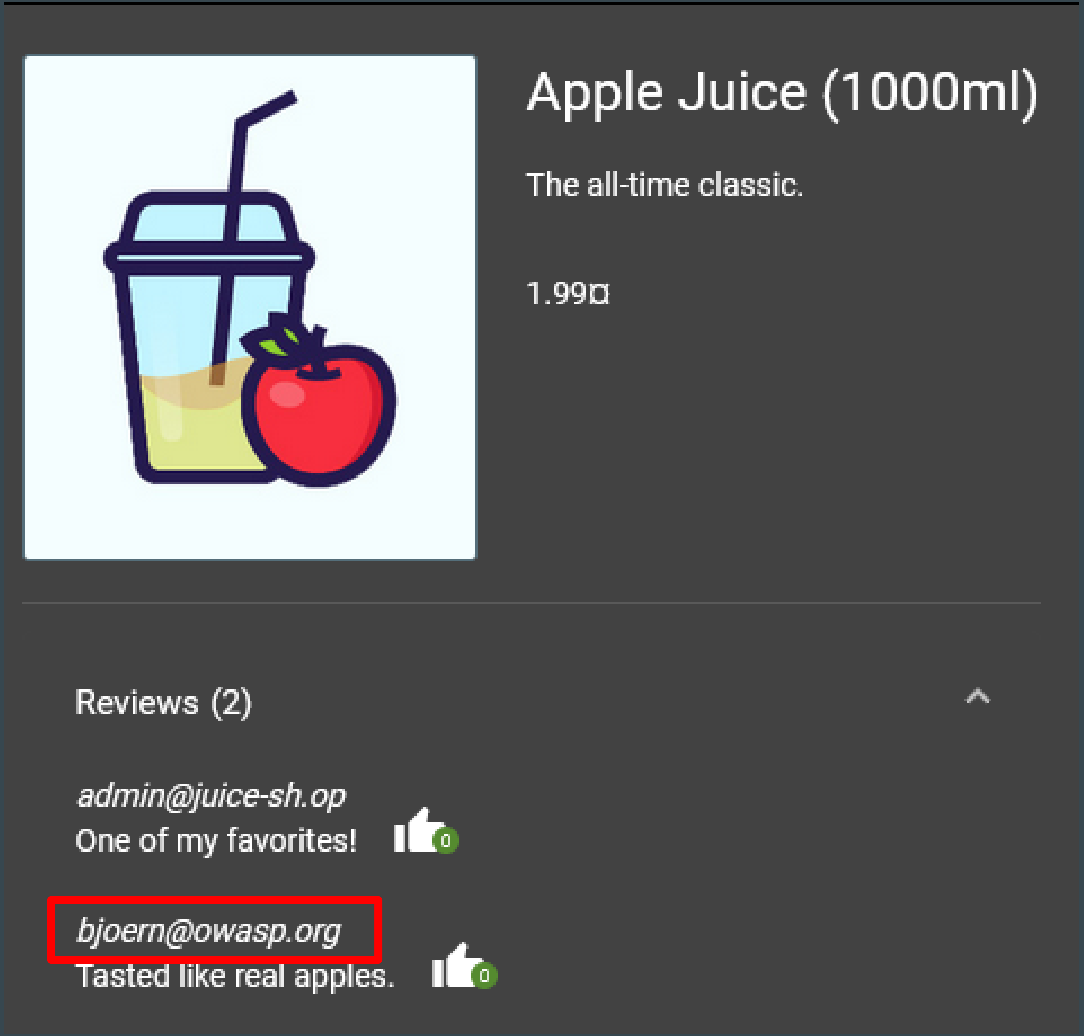
```markdown
# Planned Acquisitions

> 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.

```

A05 Security Misconfiguration

- Repeatable hardening process
- Removal of unneeded components
- Repeatable testing to verify effectiveness of configuration



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)

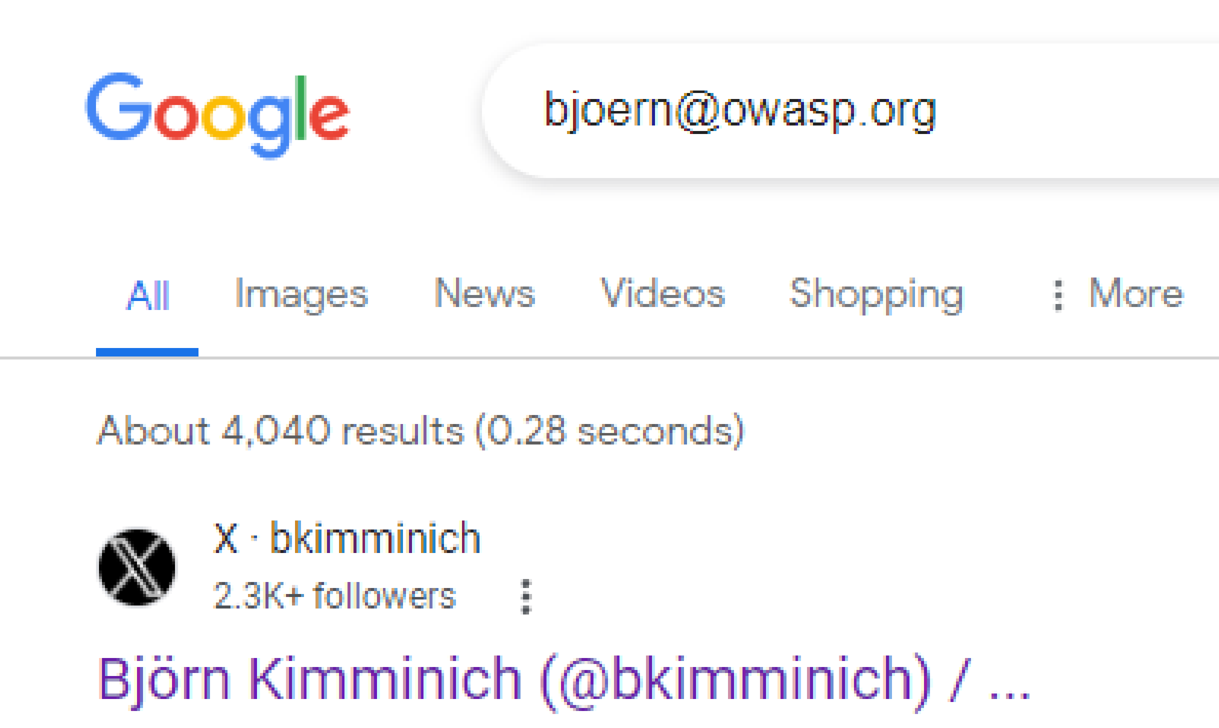
The all-time classic.

1.99¤

Reviews (2)

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

bjoern@owasp.org
Tasted like real apples. 👍 0



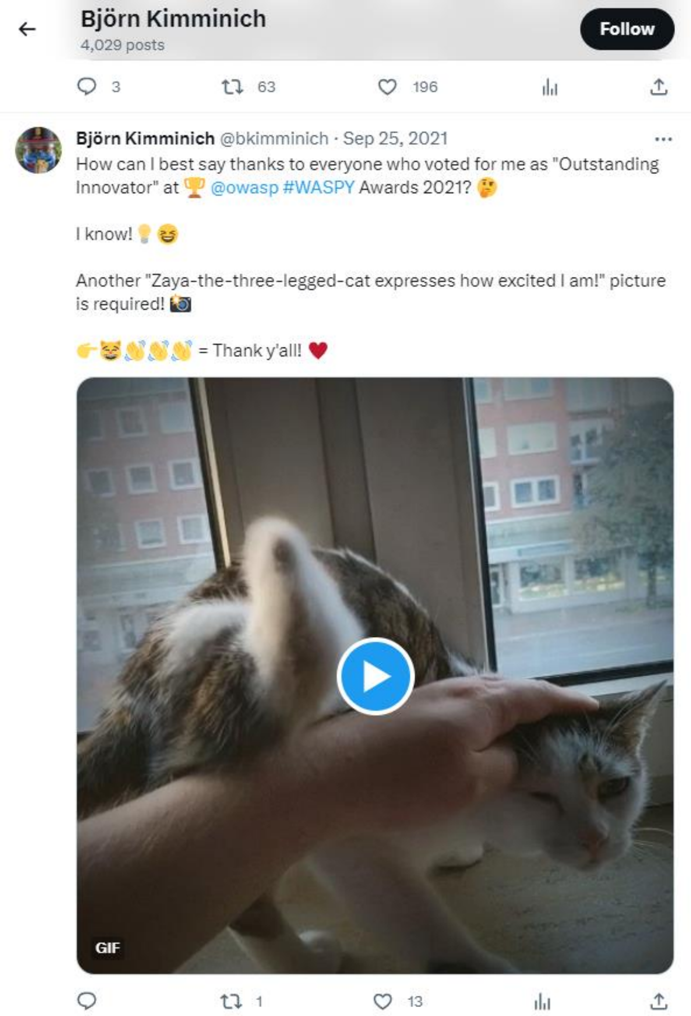
bjoern@owasp.org

About 4,040 results (0.28 seconds)

X · bkimminich

2.3K+ followers

Björn Kimminich (@bkimminich) / ...



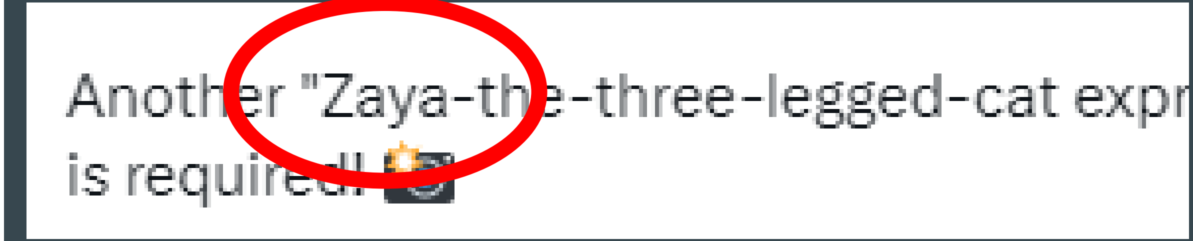
Björn Kimminich @bkimminich · Sep 25, 2021

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

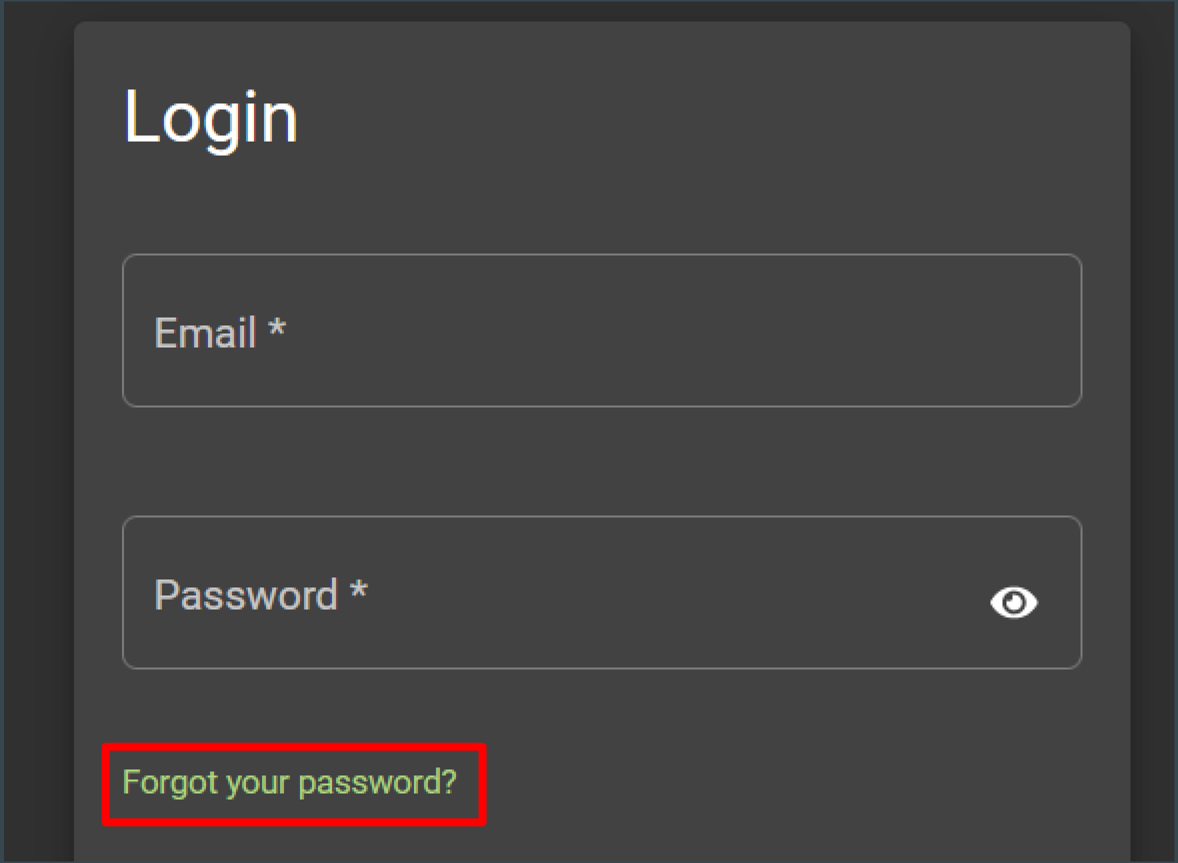
I know! 💡 😆

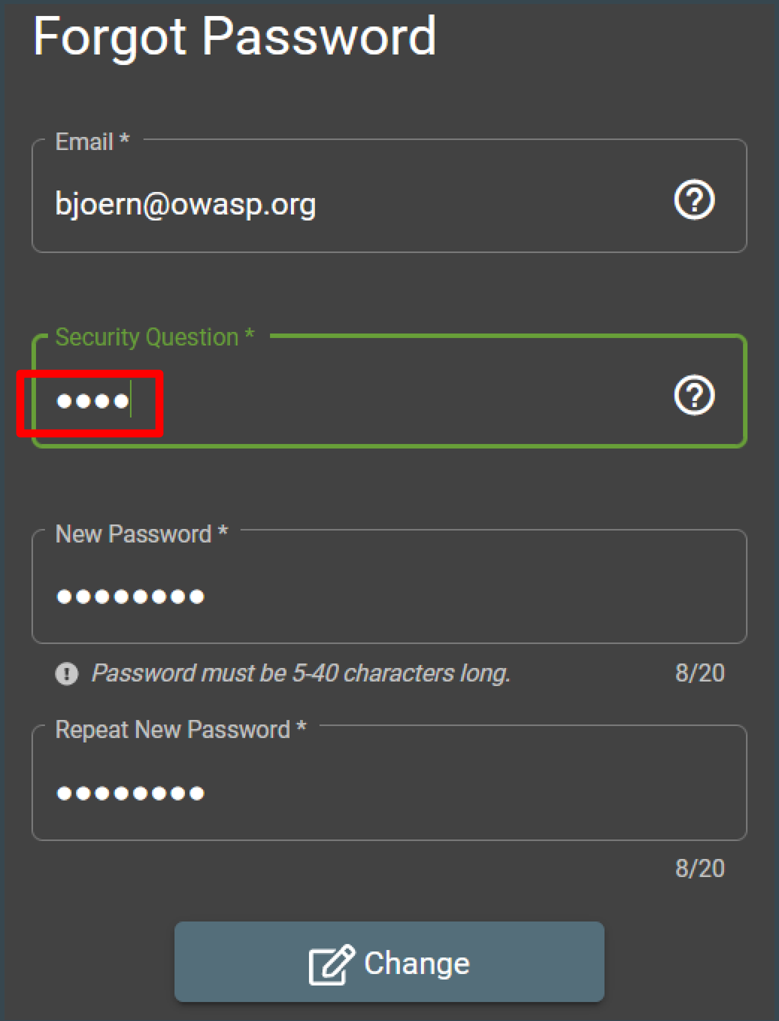
Another "Zaya-the-three-legged-cat expresses how excited I am!" picture is required! 📸

👉😸👏👏👏 = 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 *

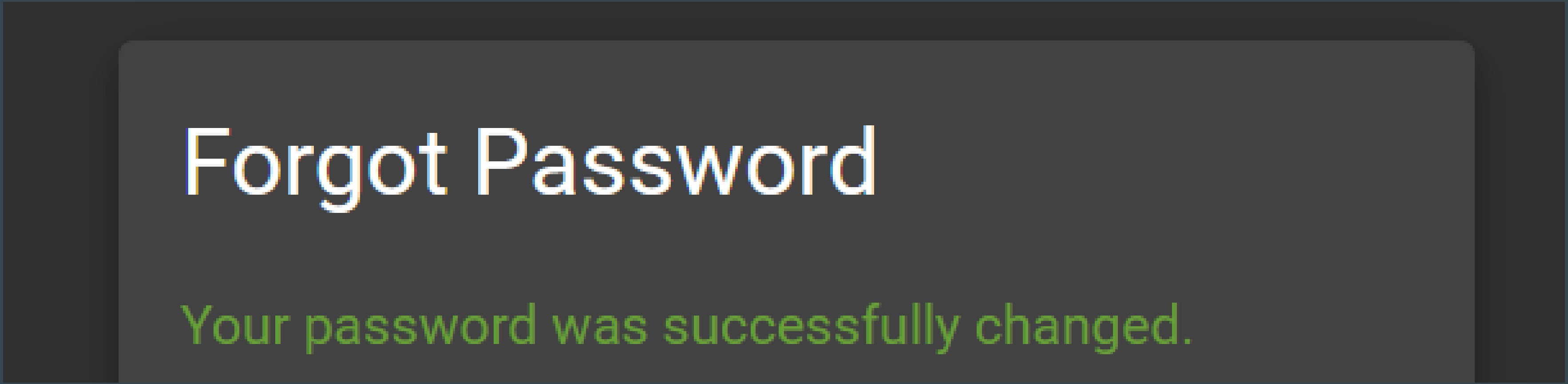
●●●●●●●●

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

Repeat New Password *

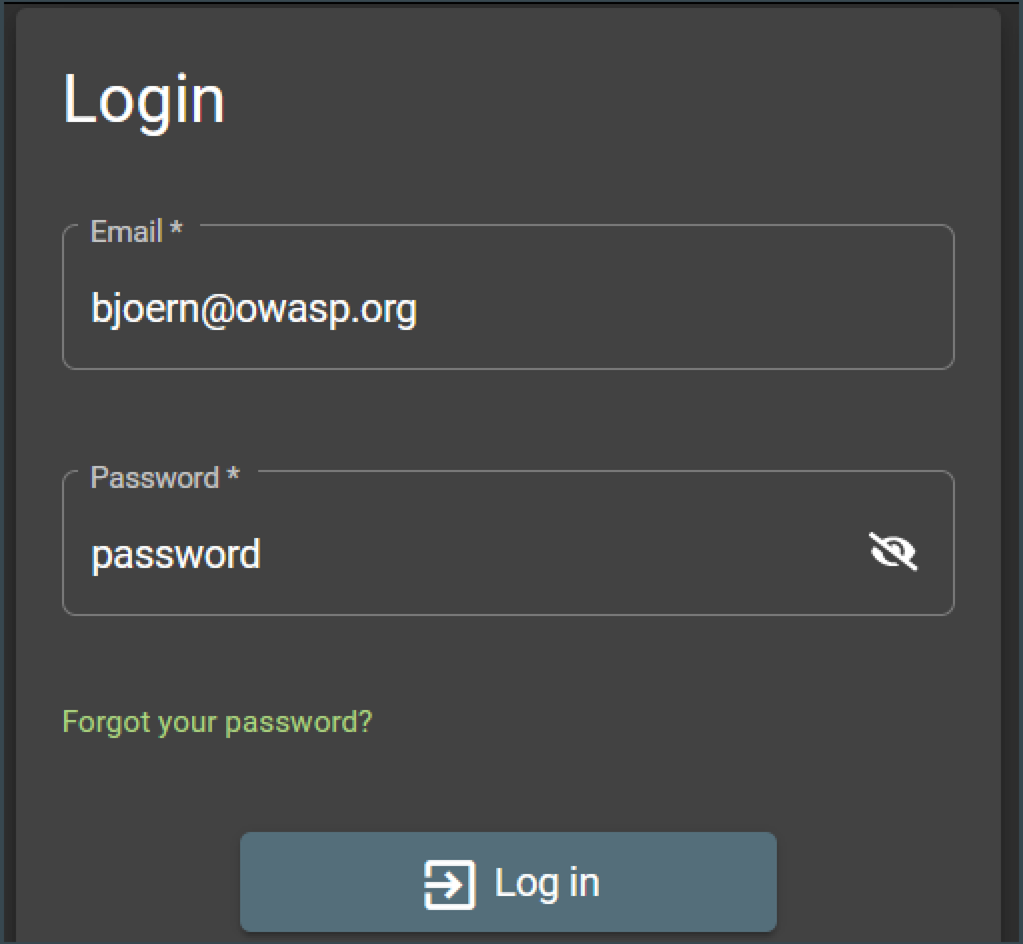
●●●●●●●●

8/20



Forgot Password

Your password was successfully changed.



Login

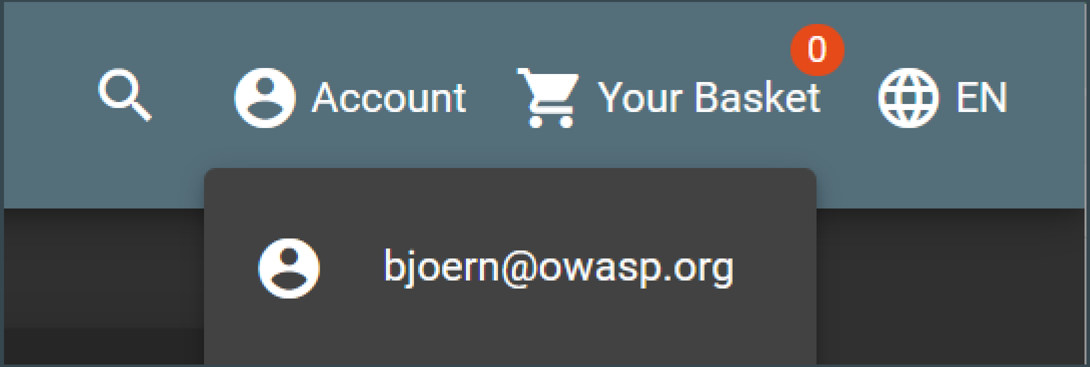
Email *

bjoern@owasp.org

Password *

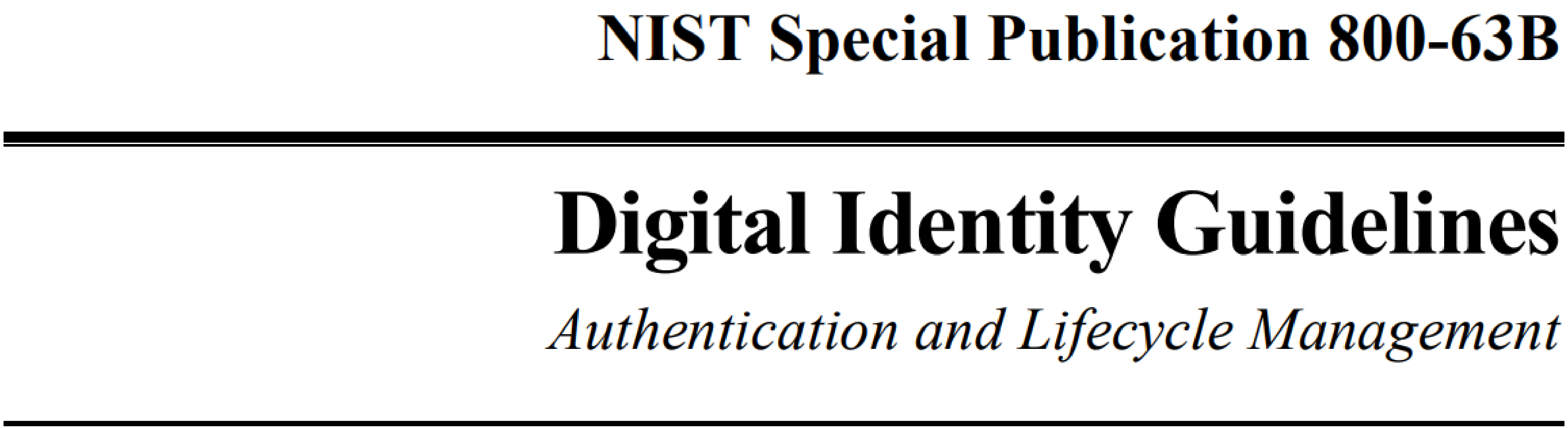
password

Forgot your password?



bjoern@owasp.org

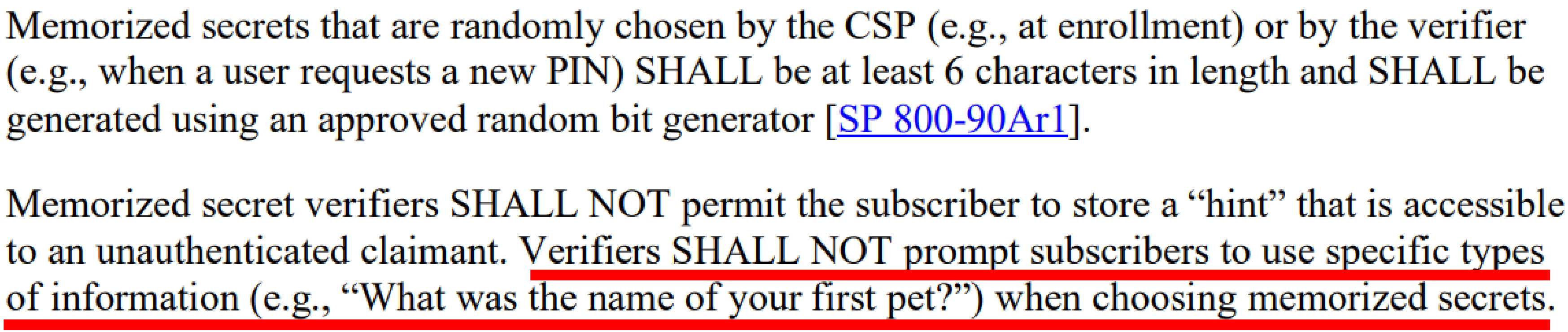
A04 Insecure Design



NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management



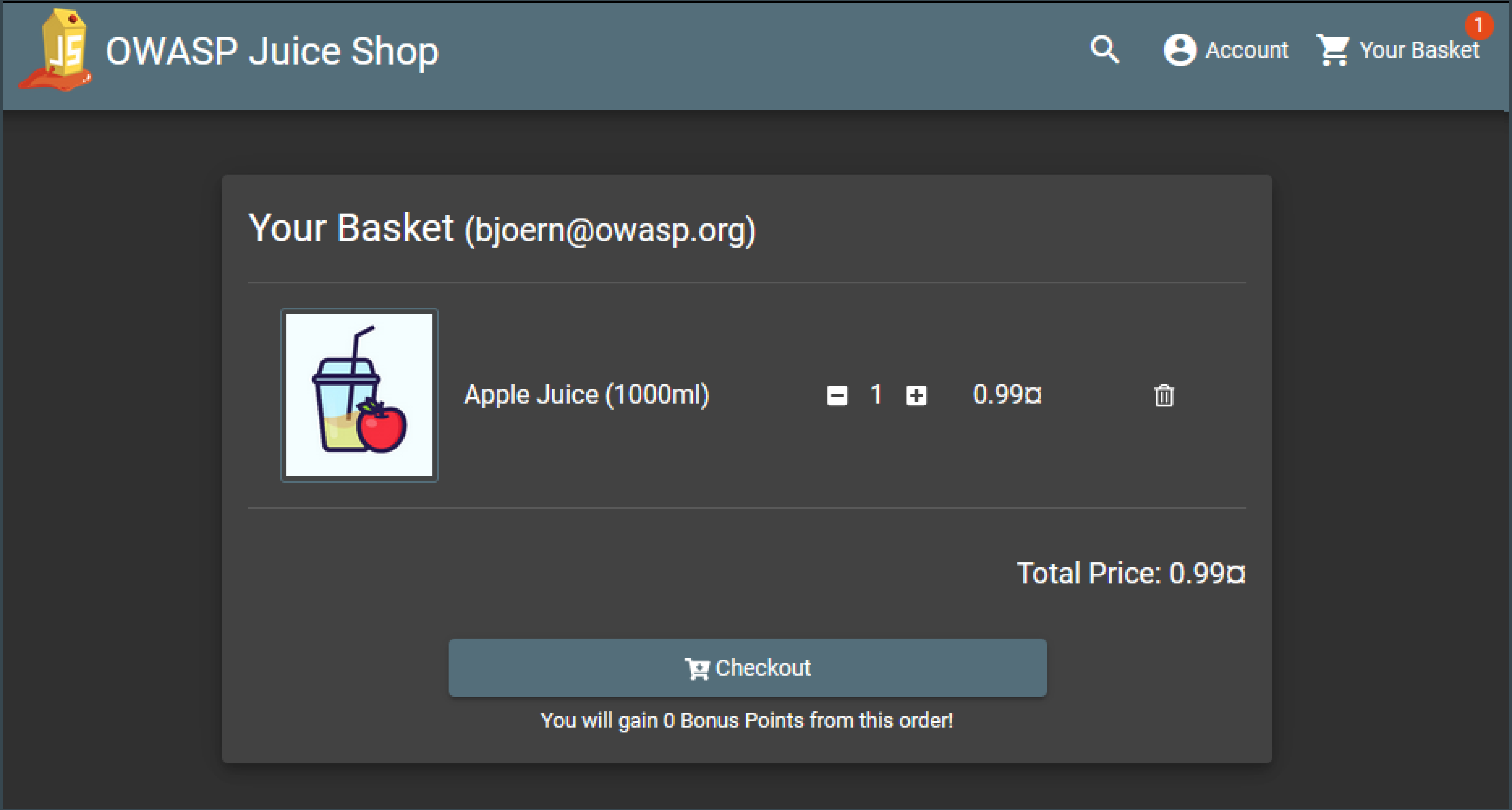
Memorized secrets that are randomly chosen by the CSP (e.g., at enrollment) or by the verifier (e.g., when a user requests a new PIN) SHALL be at least 6 characters in length and SHALL be generated using an approved random bit generator [SP 800-90Ar1].

Memorized secret verifiers SHALL NOT permit the subscriber to store a "hint" that is accessible to an unauthenticated claimant. Verifiers SHALL NOT prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing memorized secrets.

A04 Insecure Design

- Frameworks; design patterns; threat modeling; security testing; segregation & isolation

- Establish an SDLC using qualified professionals to help evaluate design security

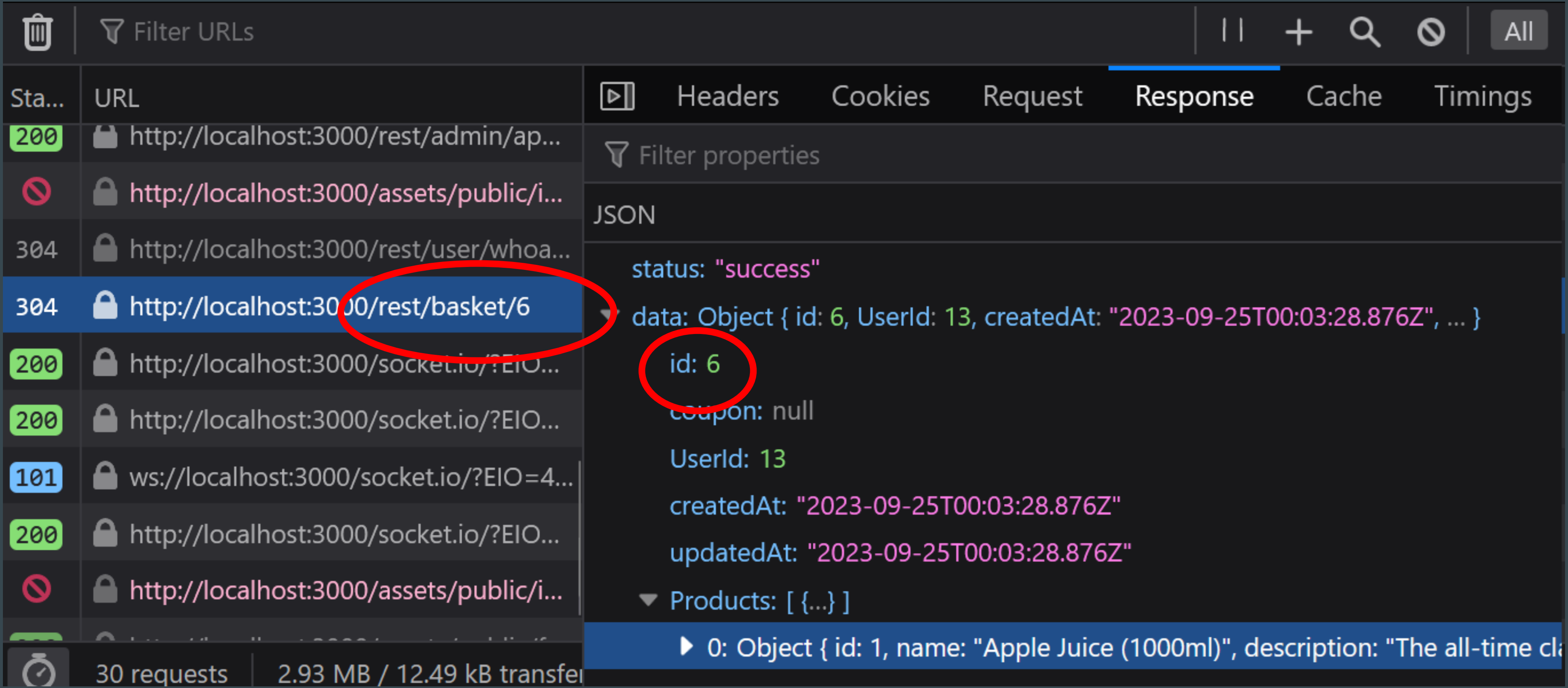


Your Basket (bjoern@owasp.org)

Apple Juice (1000ml)	1	0.99¤		

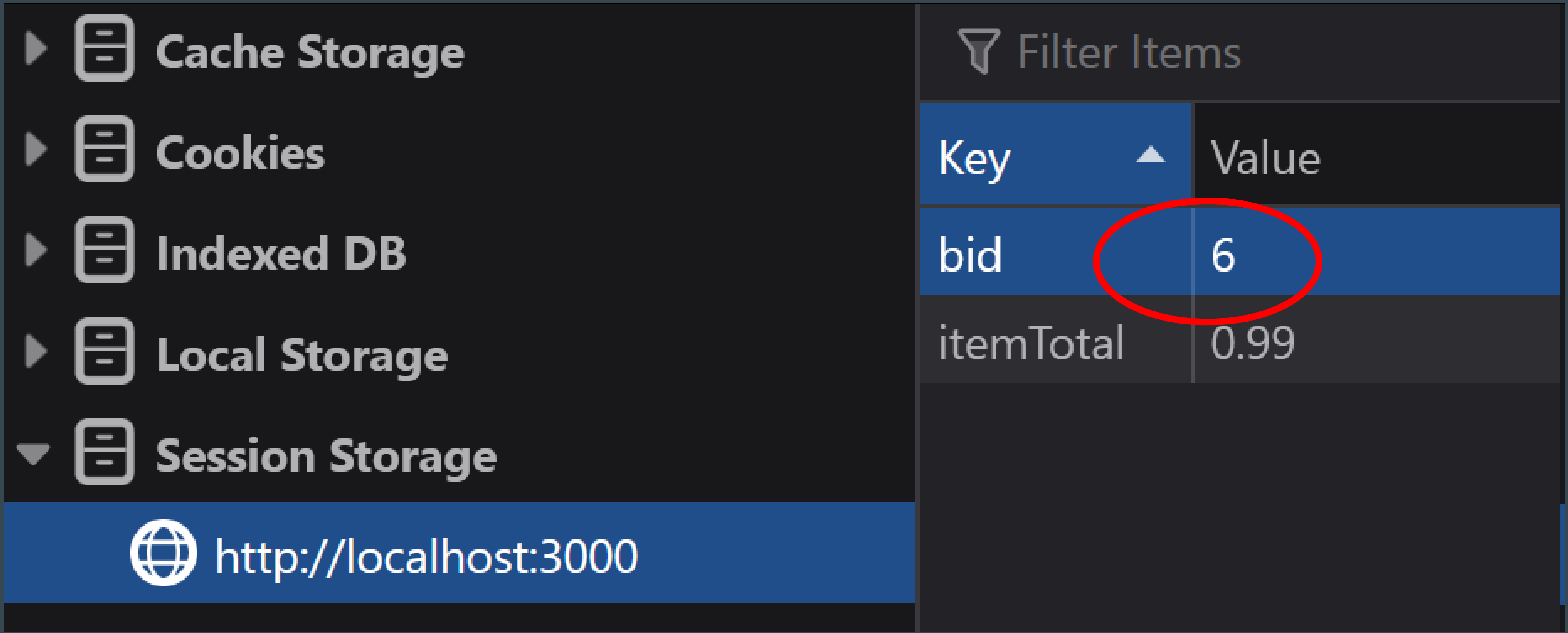
Total Price: 0.99¤

You will gain 0 Bonus Points from this order!

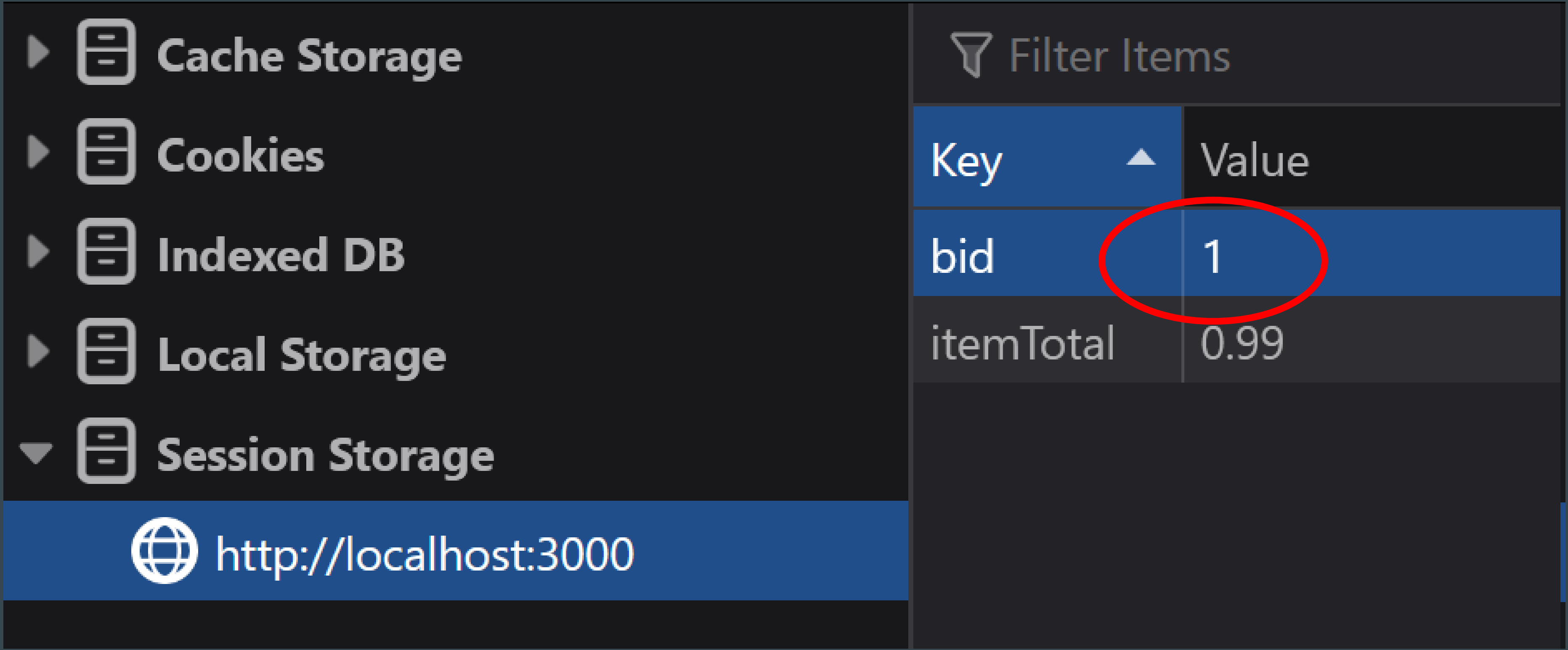


```
Sta...  URL
200     http://localhost:3000/rest/admin/ap...
        http://localhost:3000/assets/public/i...
304     http://localhost:3000/rest/user/whoa...
304     http://localhost:3000/rest/basket/6
200     http://localhost:3000/socket.io/?EIO...
200     http://localhost:3000/socket.io/?EIO...
101     ws://localhost:3000/socket.io/?EIO=4...
200     http://localhost:3000/socket.io/?EIO...
        http://localhost:3000/assets/public/i...

30 requests    2.93 MB / 12.49 kB transfer
```

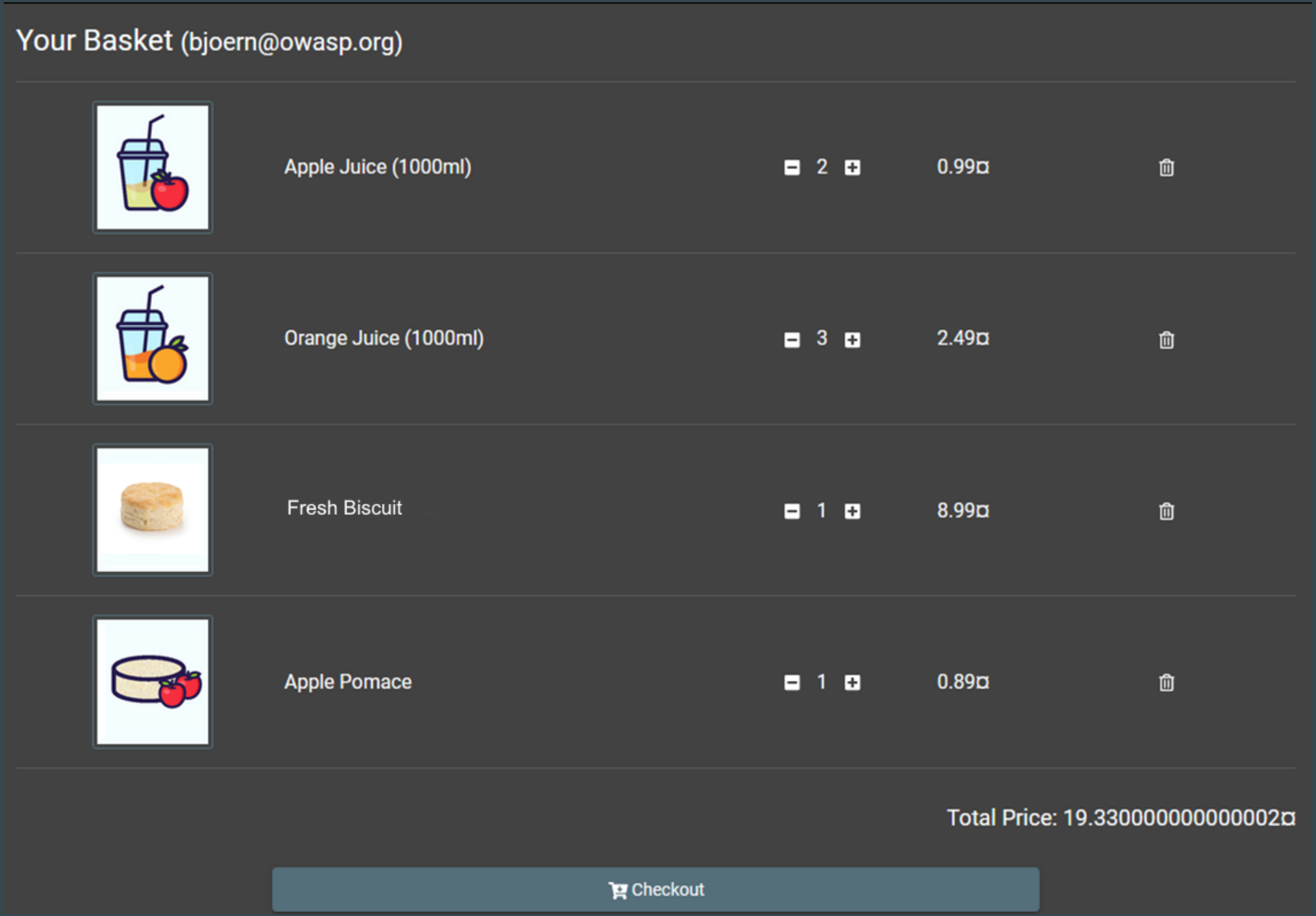
```
JSON
  status: "success"
▼ data: Object { id: 6, UserId: 13, createdAt: "2023-09-25T00:03:28.876Z", ... }
    id: 6
    coupon: null
    UserId: 13
    createdAt: "2023-09-25T00:03:28.876Z"
    updatedAt: "2023-09-25T00:03:28.876Z"
  ▼ Products: [ {...} ]
    ▶ 0: Object { id: 1, name: "Apple Juice (1000ml)", description: "The all-time cla
```



Key	Value
bid	6
itemTotal	0.99



Key	Value
bid	1
itemTotal	0.99



Your Basket (bjoern@owasp.org)

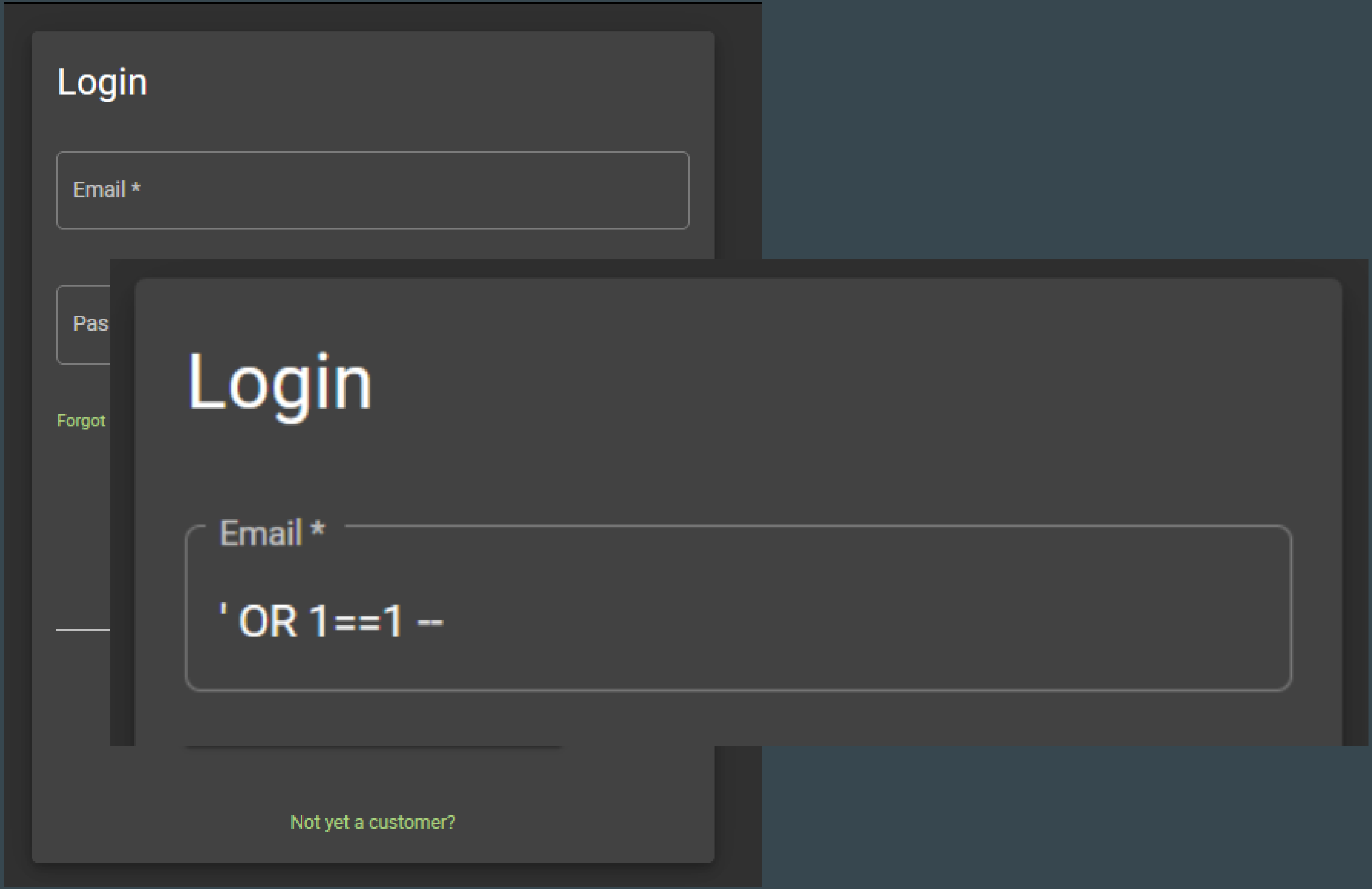
Apple Juice (1000ml)	2	0.99¤
Orange Juice (1000ml)	3	2.49¤
Fresh Biscuit	1	8.99¤
Apple Pomace	1	0.89¤

Total Price: 19.330000000000002¤

A01 Broken Access Control

- Sanitize user input
- Whitelist allowed characters
- Log access control failures
- Implement access control in one place and re-use it
- Deny by default

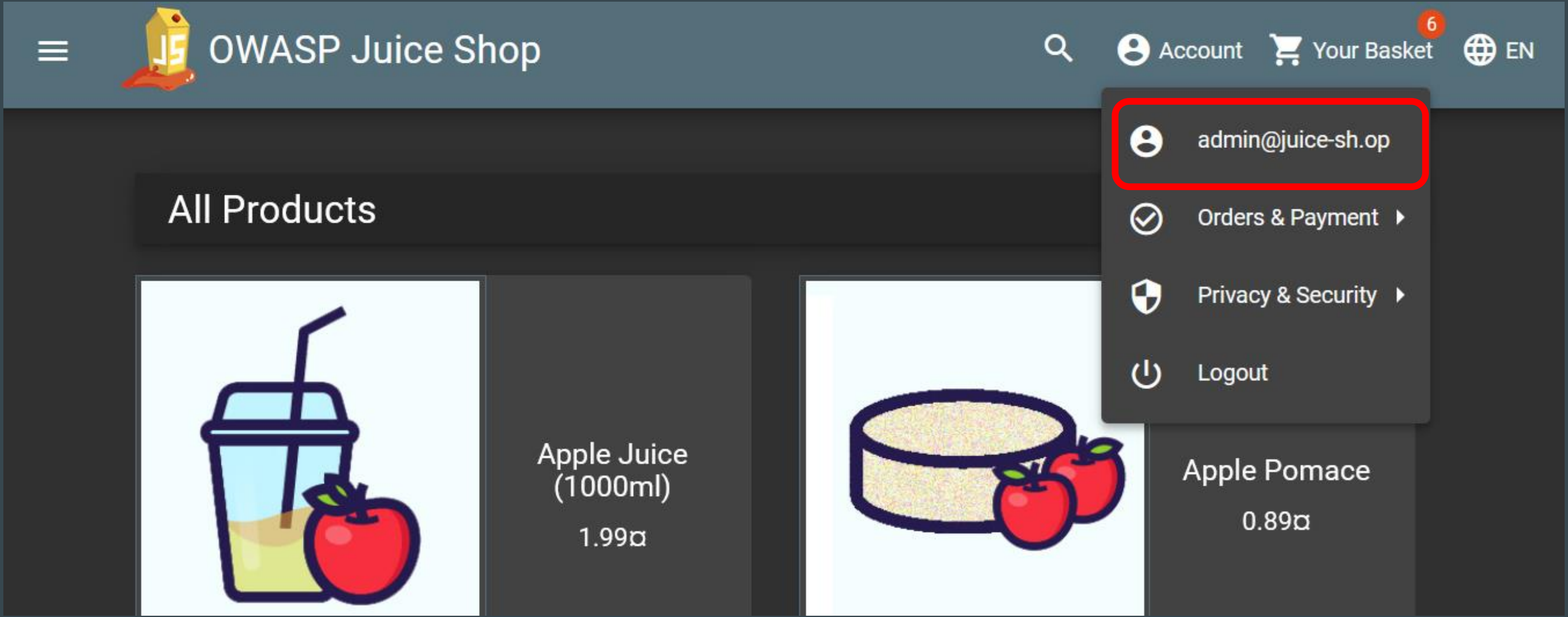
… all server side!

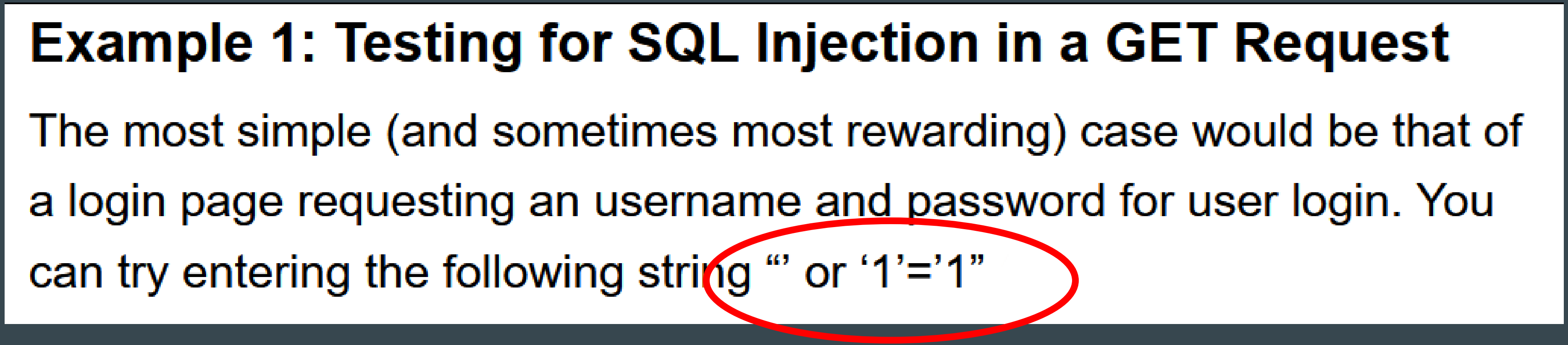


Login

Email *

' OR 1==1 --


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

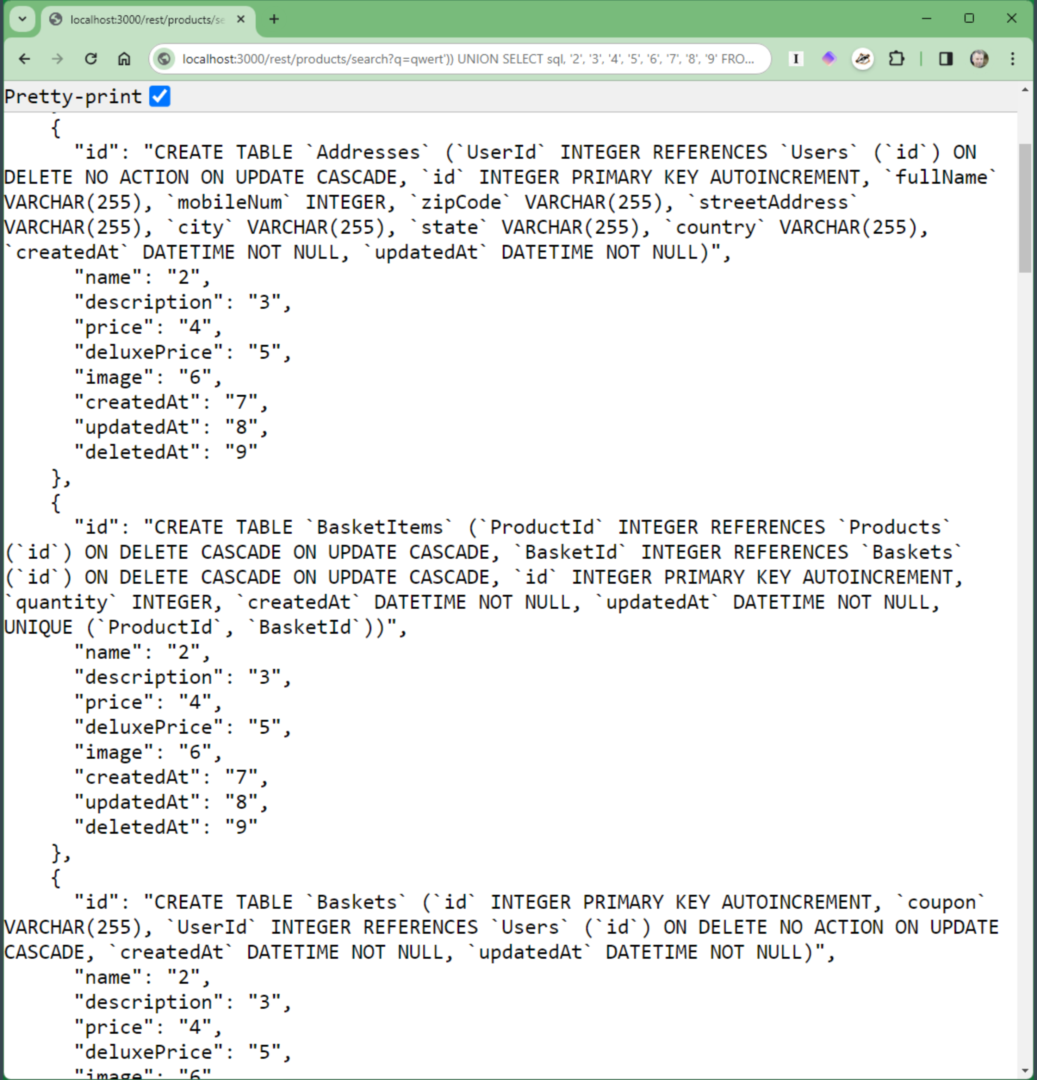


Example 1: Testing for SQL Injection in a GET Request

The most simple (and sometimes most rewarding) case would be that of a login page requesting an username and password for user login. You can try entering the following string “’ or ‘1’=’1”

Source: OWASP Web Application Security Testing Guide

```
http://localhost:3000/rest/products/search?q=

    qwert')) UNION SELECT sql, '2', '3', '4', '5', '6', '7', '8', '9' FROM sqlite_master--
```



localhost:3000/rest/products/search?q=qwert')) UNION SELECT sql, '2', '3', '4', '5', '6', '7', '8', '9' FRO...

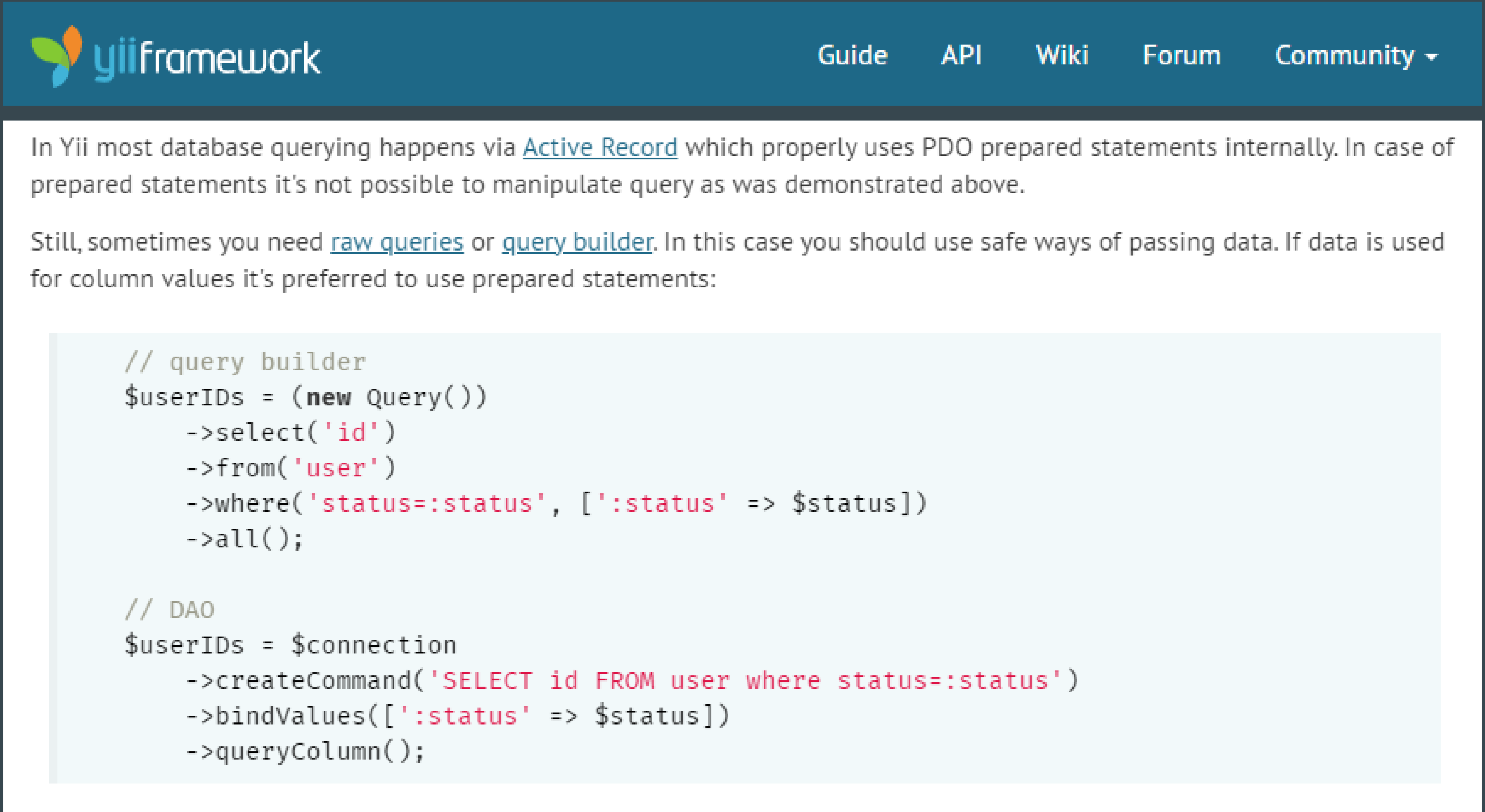
Pretty-print ☑

```
  {
    "id": "CREATE TABLE `Addresses` (`UserId` INTEGER REFERENCES `Users` (`id`) ON
DELETE NO ACTION ON UPDATE CASCADE, `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)",
    "name": "2",
    "description": "3",
    "price": "4",
    "deluxePrice": "5",
    "image": "6",
    "createdAt": "7",
    "updatedAt": "8",
    "deletedAt": "9"
  },
  {
    "id": "CREATE TABLE `BasketItems` (`ProductId` INTEGER REFERENCES `Products`
(`id`) ON DELETE CASCADE ON UPDATE CASCADE, `BasketId` INTEGER REFERENCES `Baskets`
(`id`) ON DELETE CASCADE ON UPDATE CASCADE, `id` INTEGER PRIMARY KEY AUTOINCREMENT,
`quantity` INTEGER, `createdAt` DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL,
UNIQUE (`ProductId`, `BasketId`))",
    "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), `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",
```

A03 Injection (SQL)

- Safe API
  (e.g. parameterized queries)
- Server-side input validation

```php
<?php
$query = "UPDATE usertable SET pwd='$pwd' WHERE uid='$uid';";
?>
```



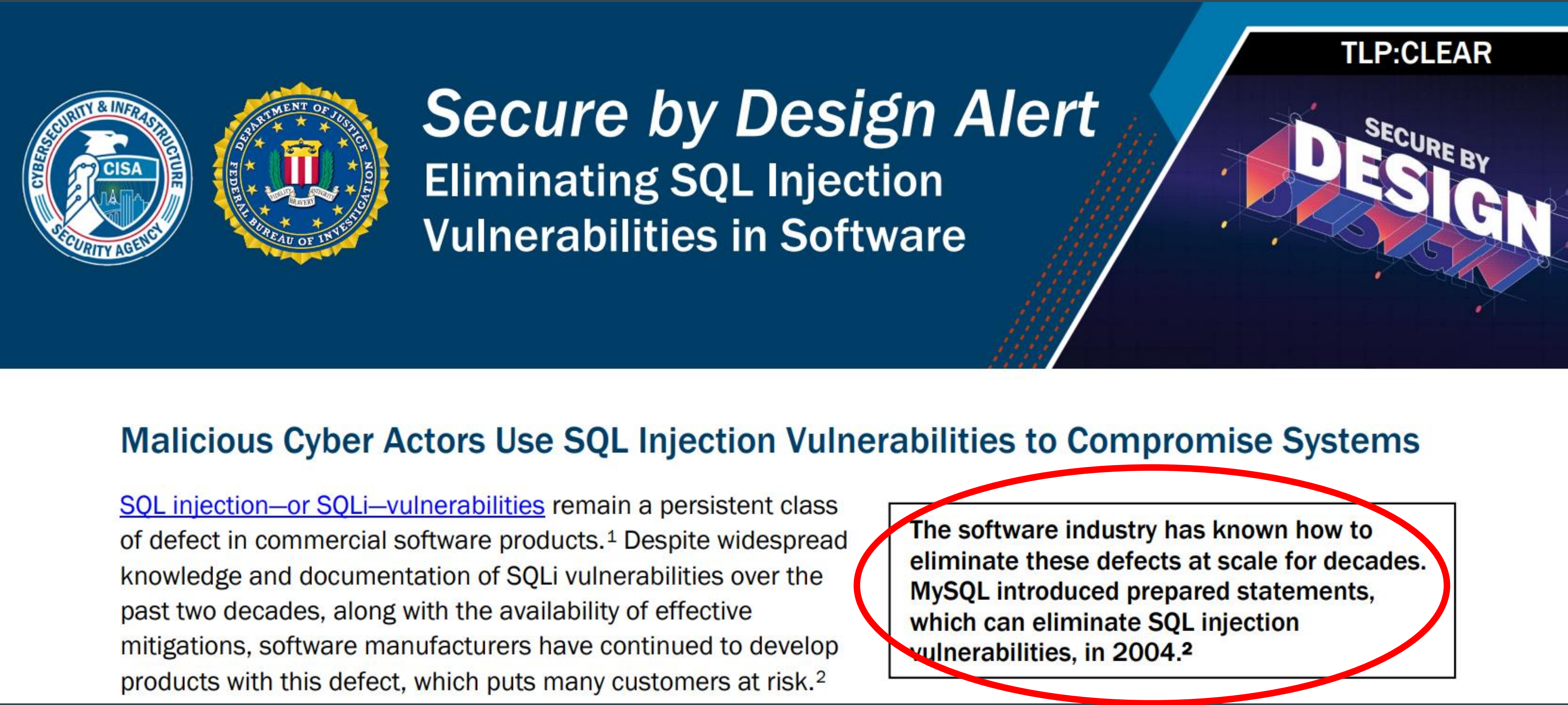
In Yii most database querying happens via Active Record which properly uses PDO prepared statements internally. In case of prepared statements it's not possible to manipulate query as was demonstrated above.

Still, sometimes you need raw queries or query builder. In this case you should use safe ways of passing data. If data is used for column values it's preferred to use prepared statements:

```
// query builder
$userIDs = (new Query())
    ->select('id')
    ->from('user')
    ->where('status=:status', [':status' => $status])
    ->all();

// DAO
$userIDs = $connection
    ->createCommand('SELECT id FROM user where status=:status')
    ->bindValues([':status' => $status])
    ->queryColumn();
```

History of Injection in OWASP top 10

2004	A6 Injection Flaws
2007	A2 Injection Flaws
2010	A1 Injection
2013	A1 Injection
2017	A1 Injection
2021	A3 Injection



TLP:CLEAR

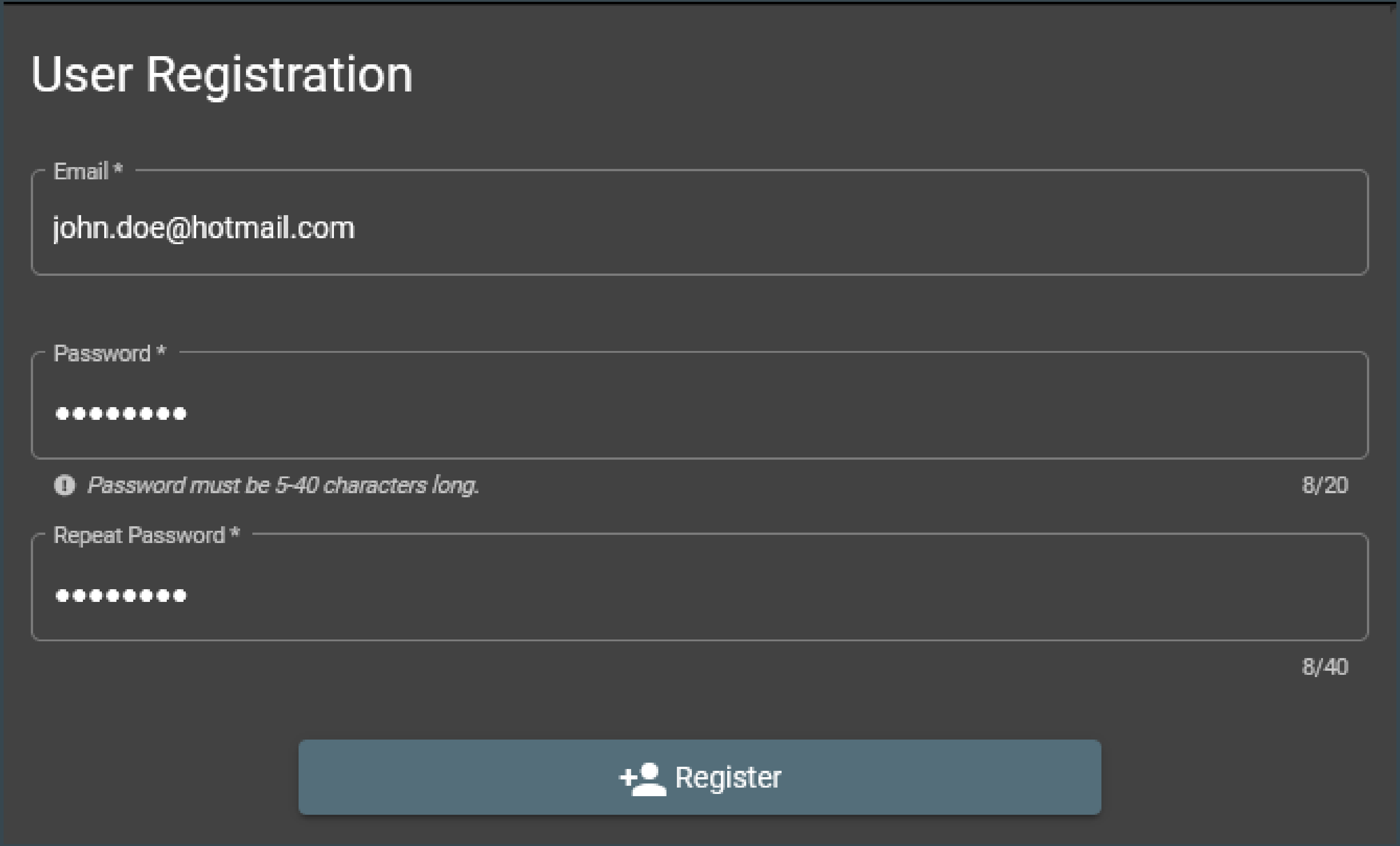
Secure by Design Alert

Eliminating SQL Injection Vulnerabilities in Software

Malicious Cyber Actors Use SQL Injection Vulnerabilities to Compromise Systems

SQL injection—or SQLi—vulnerabilities remain a persistent class of defect in commercial software products.[1] Despite widespread knowledge and documentation of SQLi vulnerabilities over the past two decades, along with the availability of effective mitigations, software manufacturers have continued to develop products with this defect, which puts many customers at risk.[2]

The software industry has known how to eliminate these defects at scale for decades. MySQL introduced prepared statements, which can eliminate SQL injection vulnerabilities, in 2004.[2]



User Registration

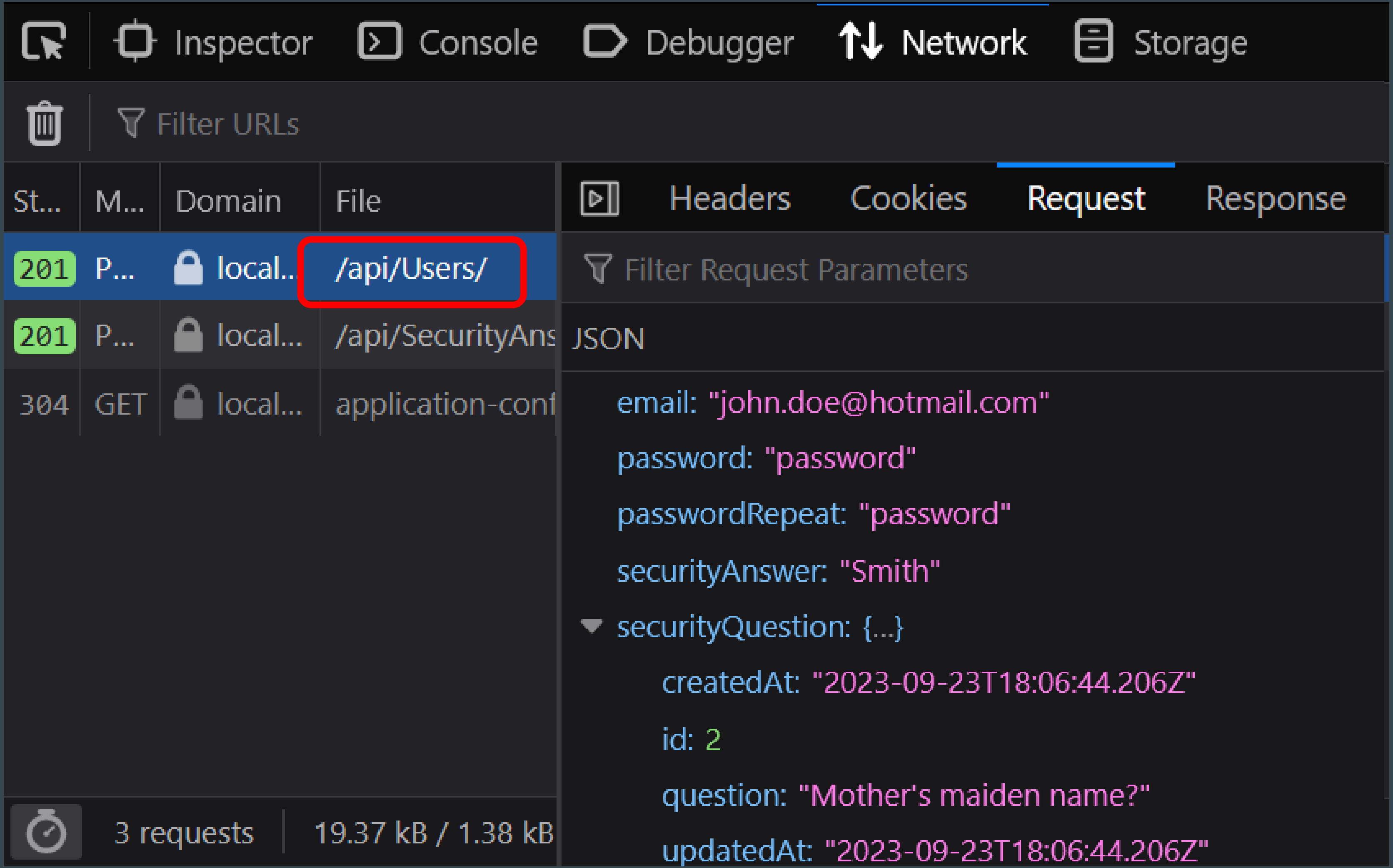
Email * john.doe@hotmail.com

Password * ••••••••

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

Repeat Password * ••••••••

8/40

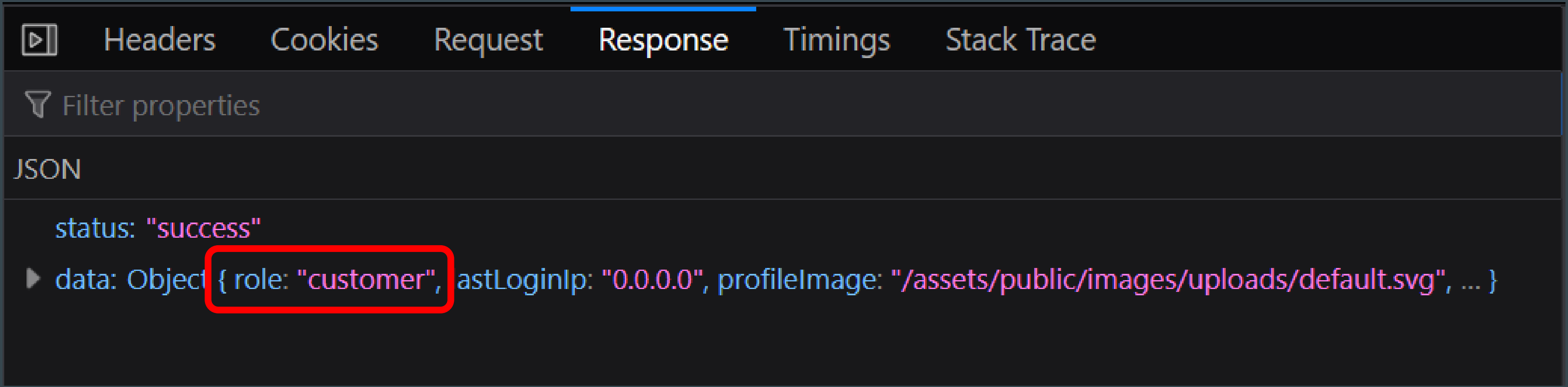


St...	M...	Domain	File
201	P...	local...	/api/Users/
201	P...	local...	/api/SecurityAns
304	GET	local...	application-conf

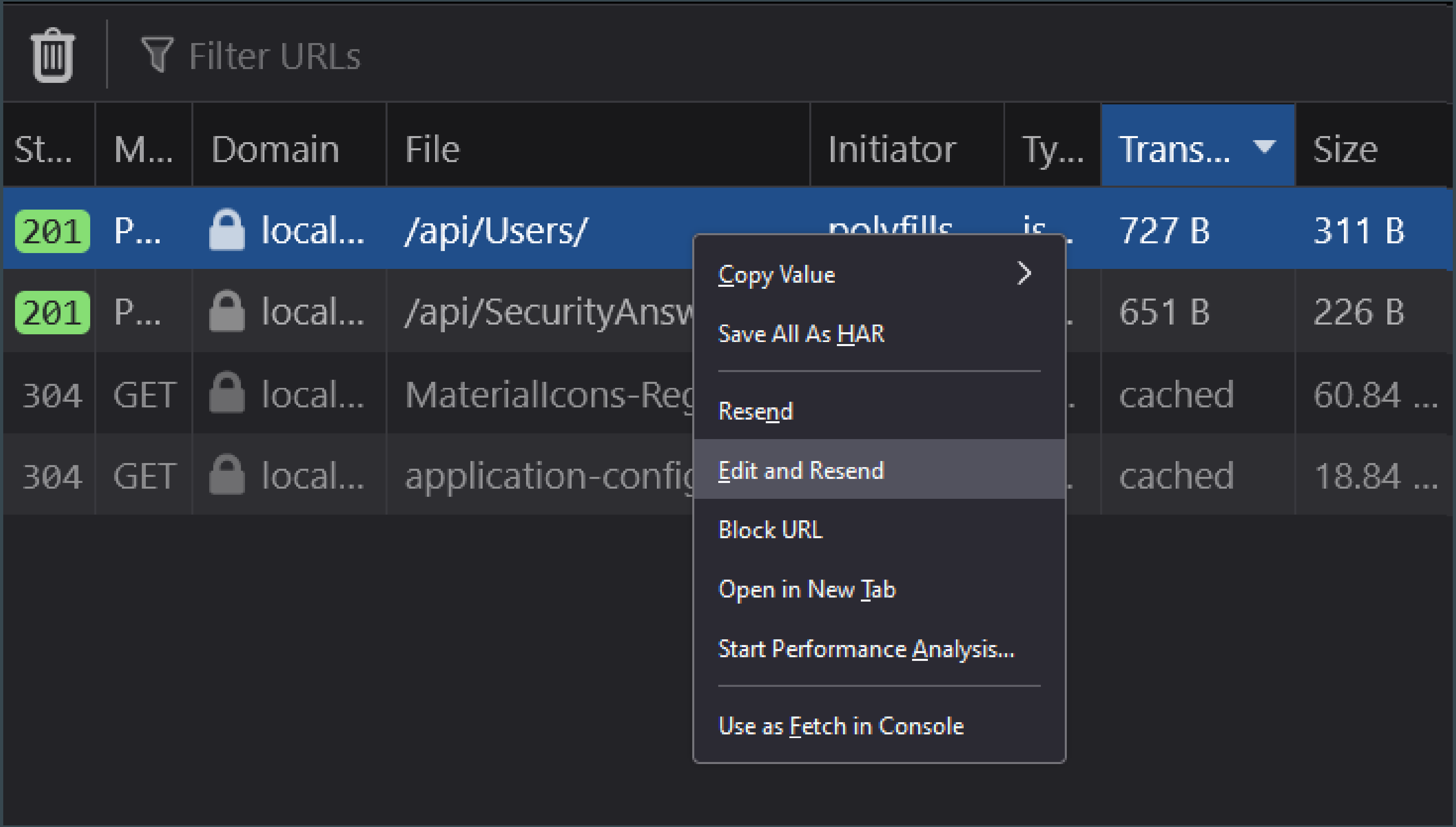
3 requests | 19.37 kB / 1.38 kB

JSON

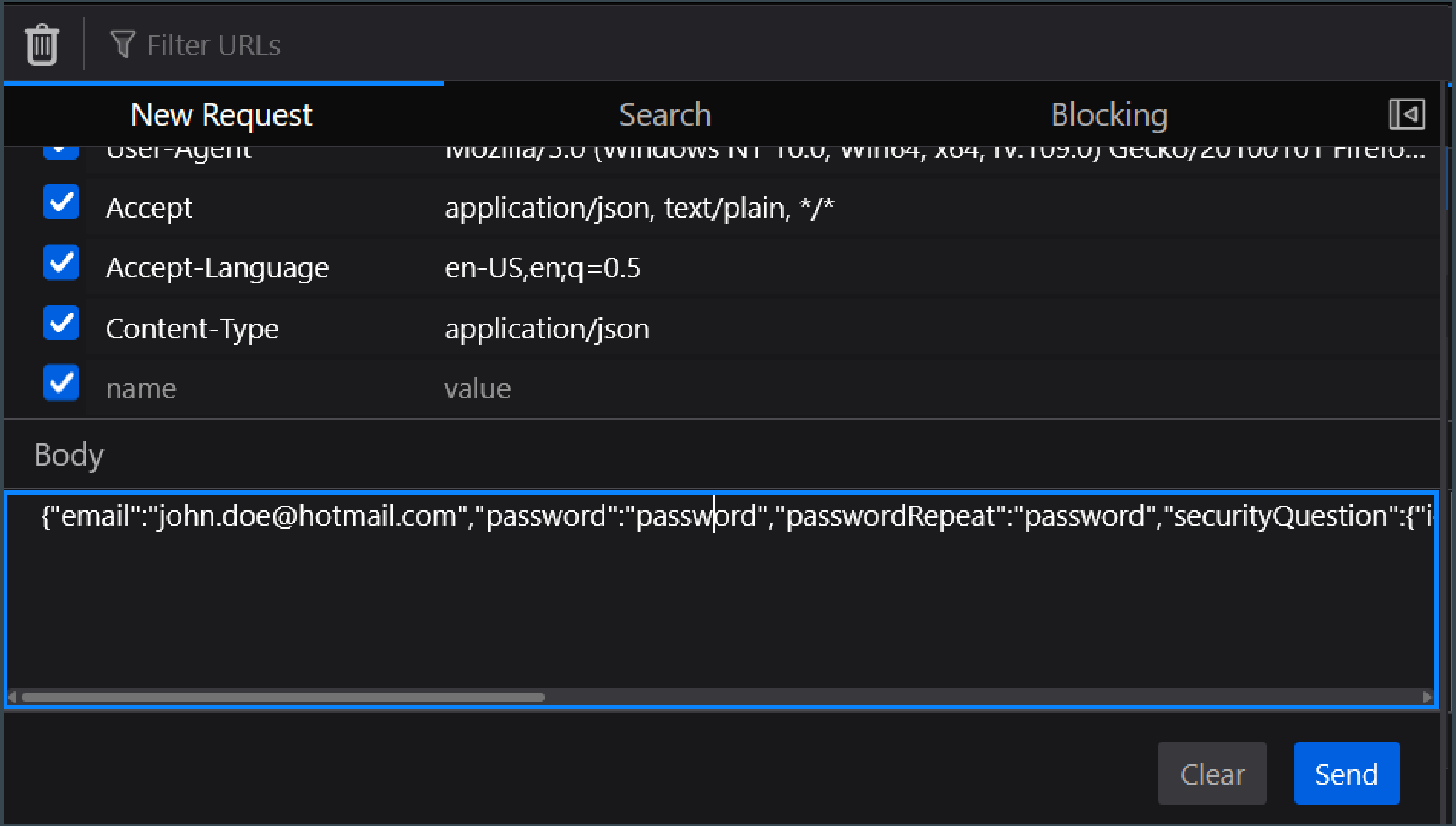
```
email: "john.doe@hotmail.com"
password: "password"
passwordRepeat: "password"
securityAnswer: "Smith"
▾ securityQuestion: {...}
    createdAt: "2023-09-23T18:06:44.206Z"
    id: 2
    question: "Mother's maiden name?"
    updatedAt: "2023-09-23T18:06:44.206Z"
```



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

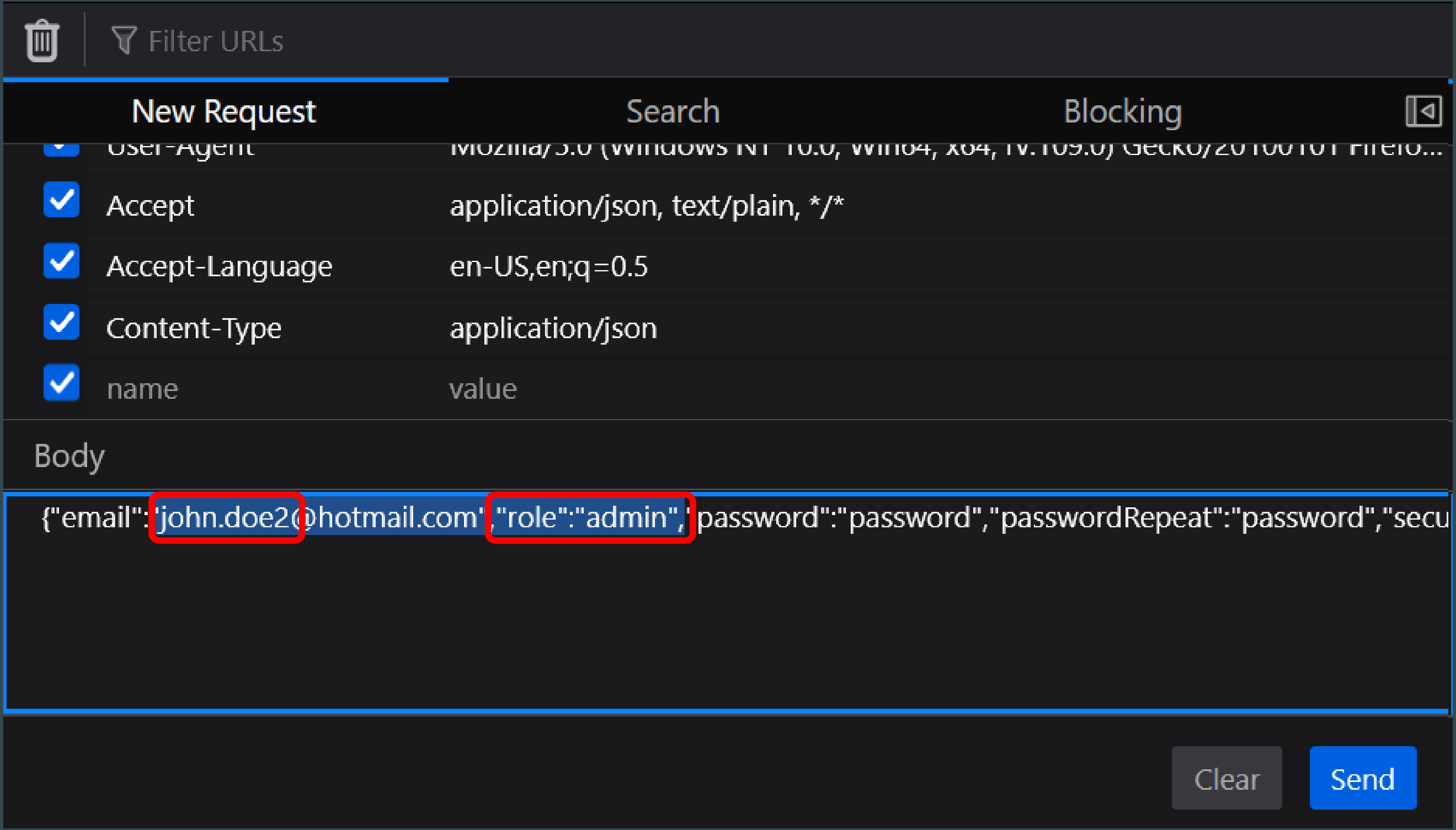


St...	M...	Domain	File	Initiator	Ty...	Trans...	Size
201	P...	local...	/api/Users/	polyfills	js...	727 B	311 B
201	P...	local...	/api/SecurityAnsw		.	651 B	226 B
304	GET	local...	MaterialIcons-Reg		.	cached	60.84 ...
304	GET	local...	application-config		.	cached	18.84 ...



☑	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

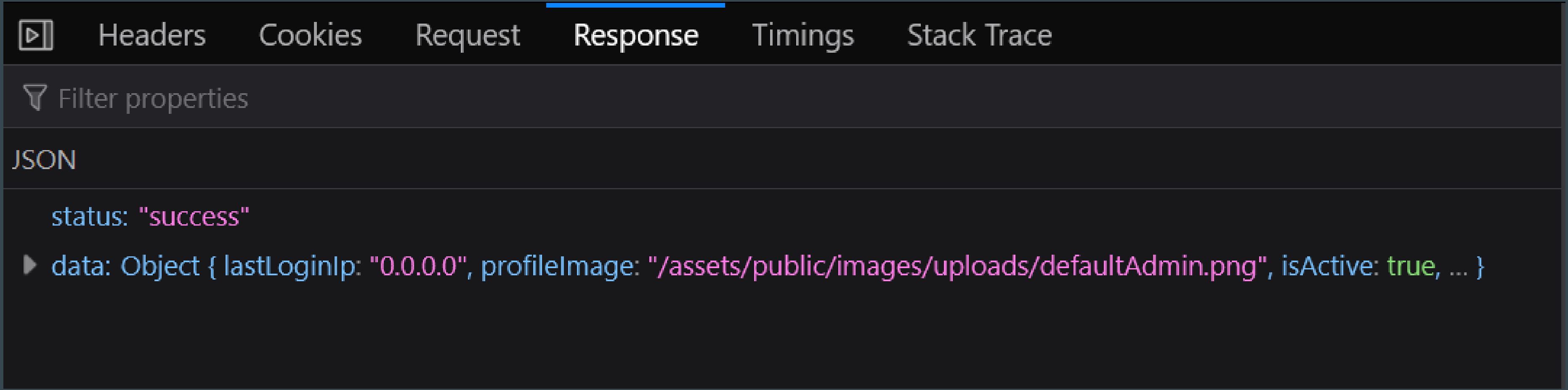
```
{"email":"john.doe@hotmail.com","password":"password","passwordRepeat":"password","securityQuestion":{"i
```



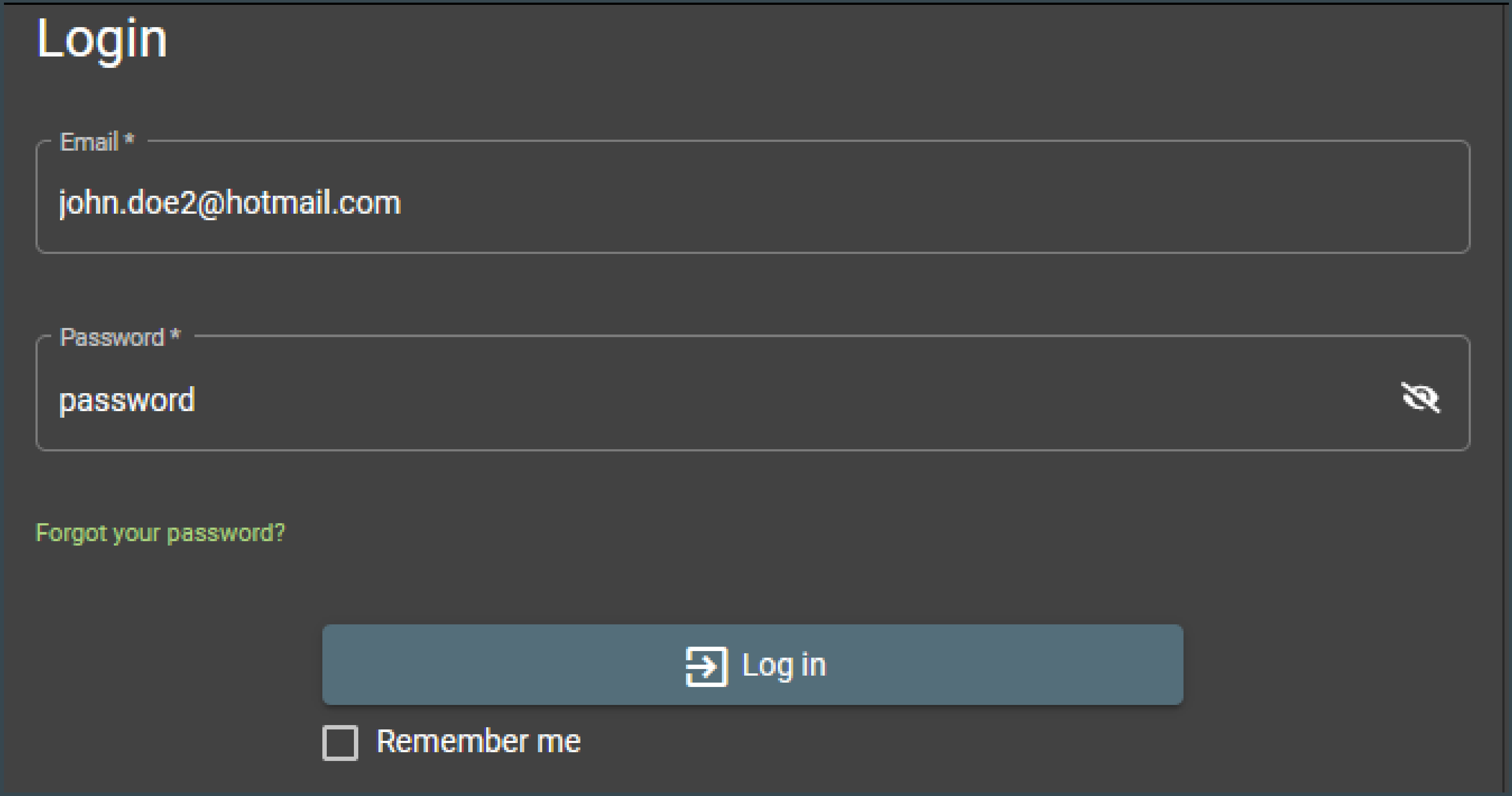
☑	User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefo...
☑	Accept	application/json, text/plain, */*
☑	Accept-Language	en-US,en;q=0.5
☑	Content-Type	application/json
☑	name	value

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, … }
```



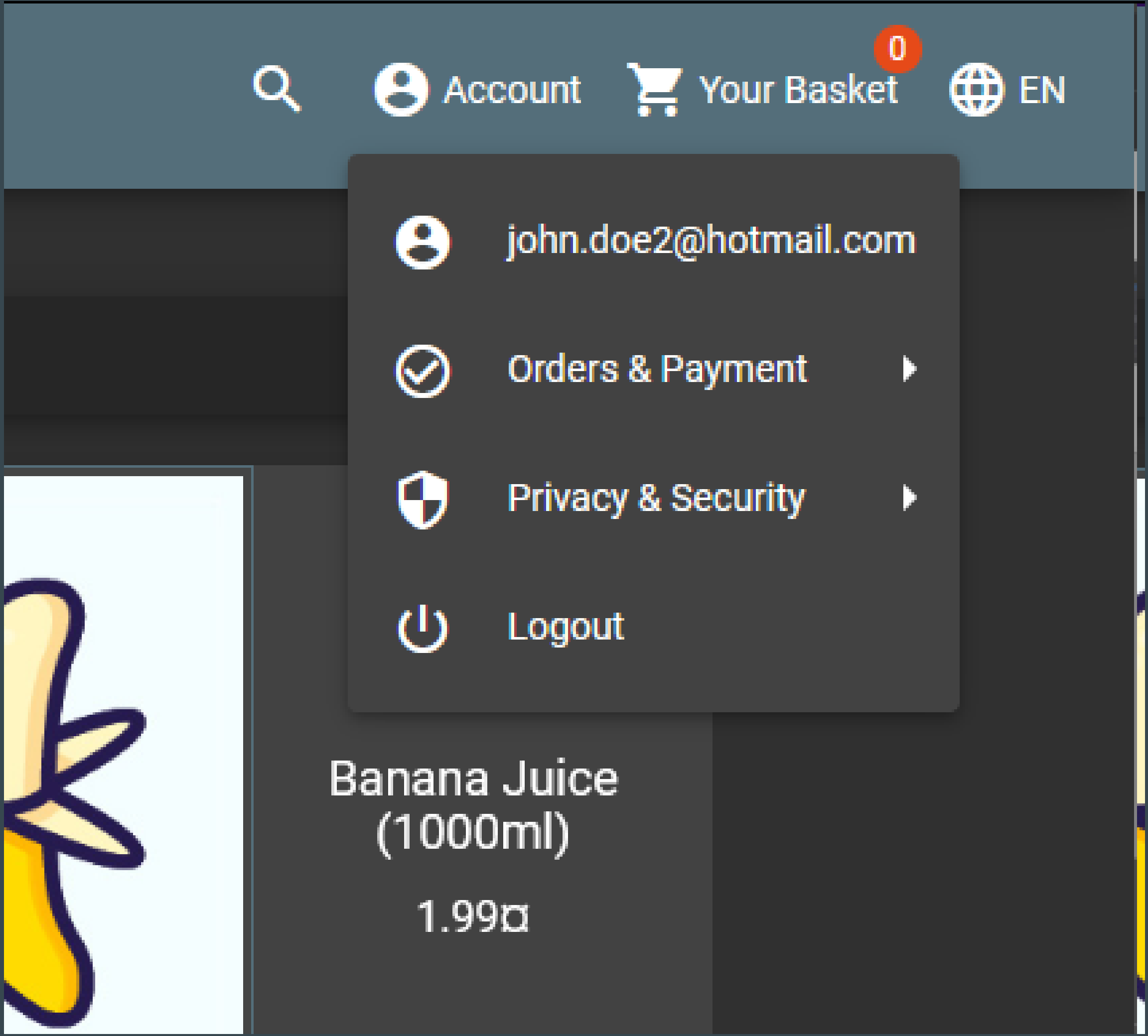
Login

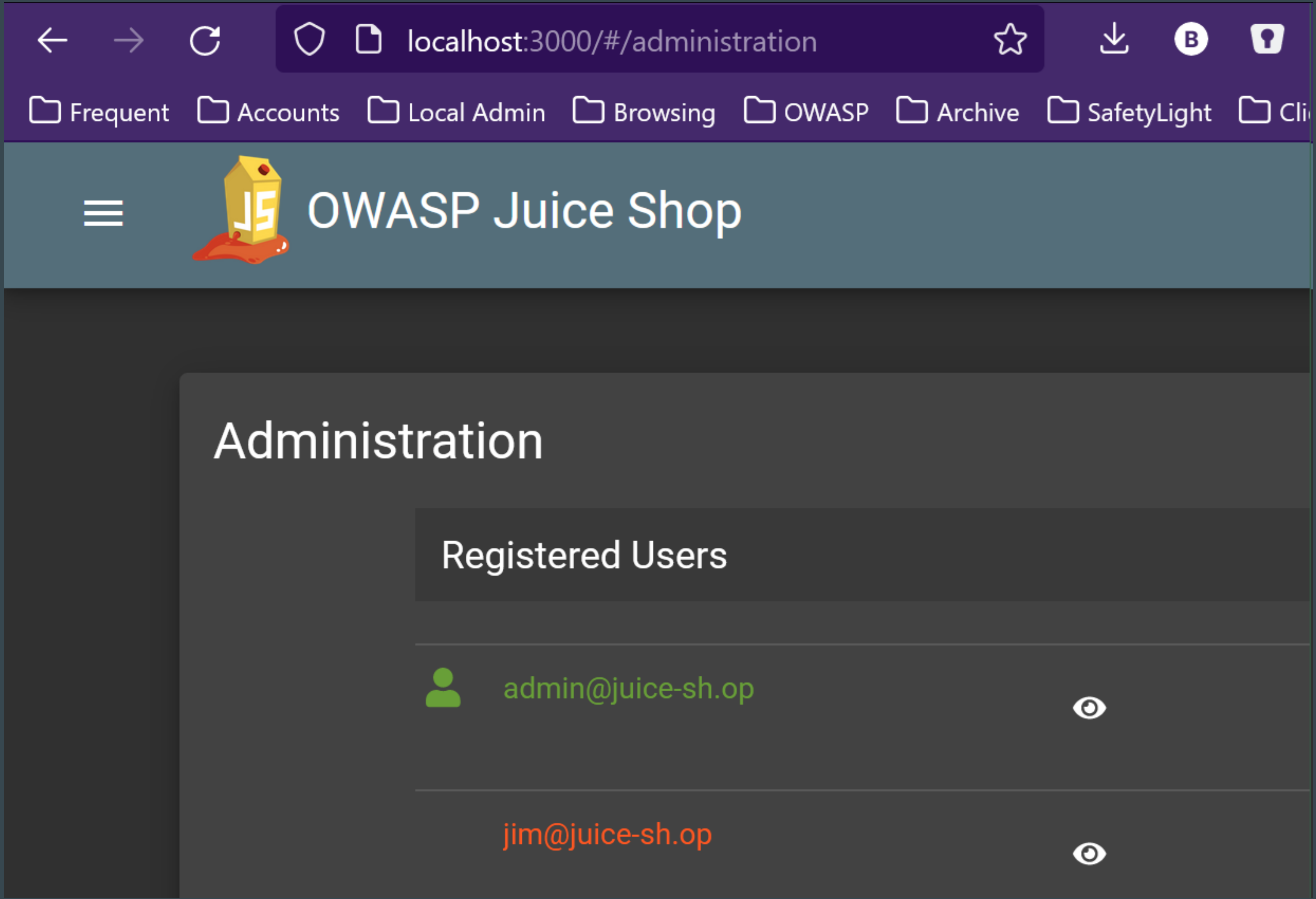
Email *

john.doe2@hotmail.com

Password *

password


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



OWASP Juice Shop

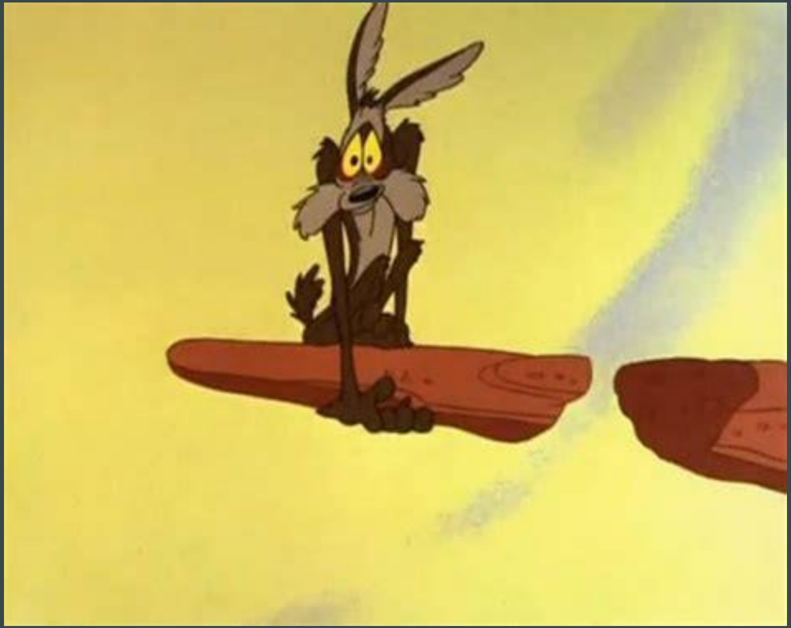
Administration

Registered Users

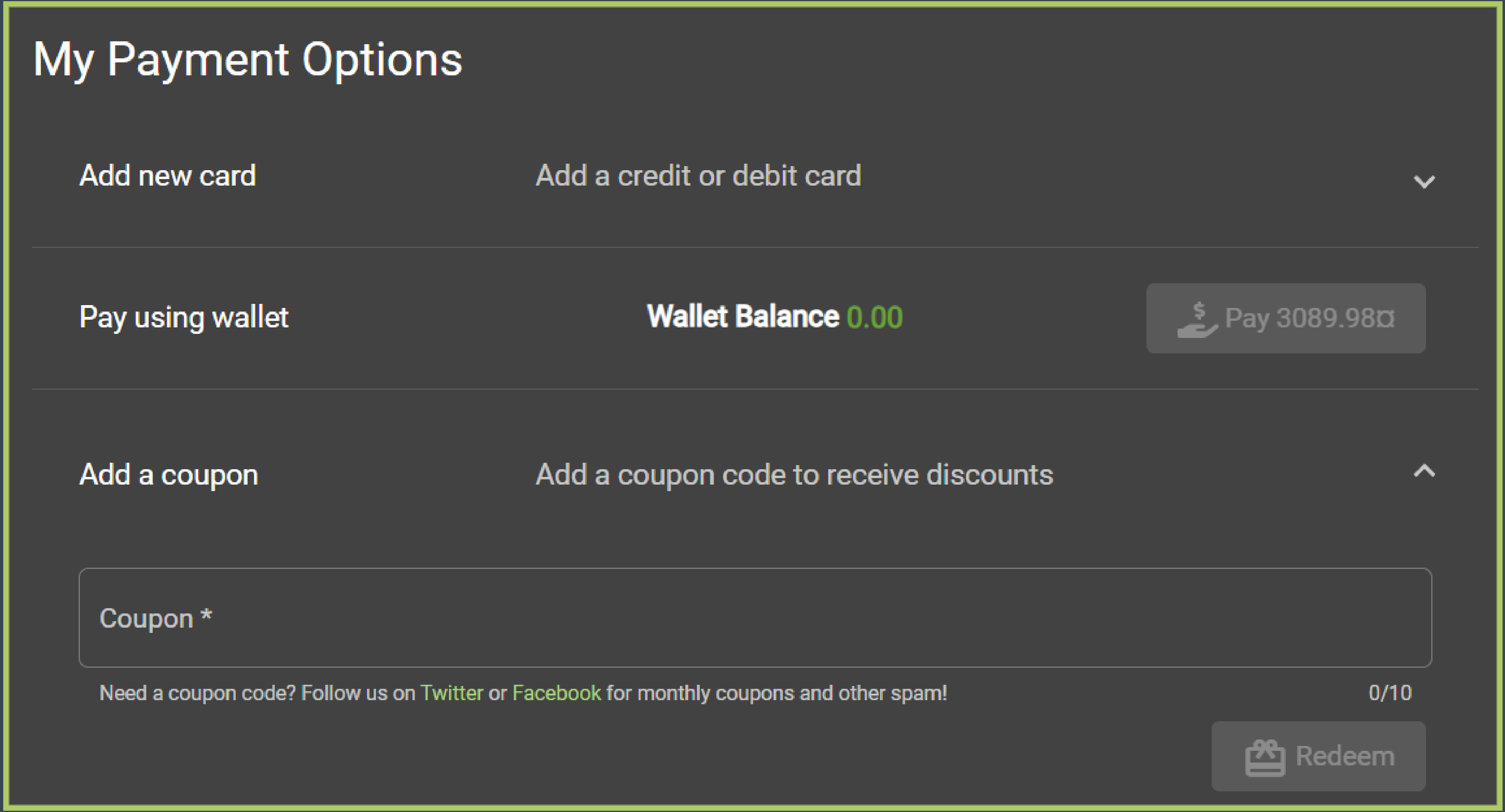
admin@juice-sh.op

jim@juice-sh.op

A07 Identification & Authentication Failures



- Validate user input
- Implement MFA
- Change default credentials
- Require strong passwords
- Limit failed log-in attempts



My Payment Options

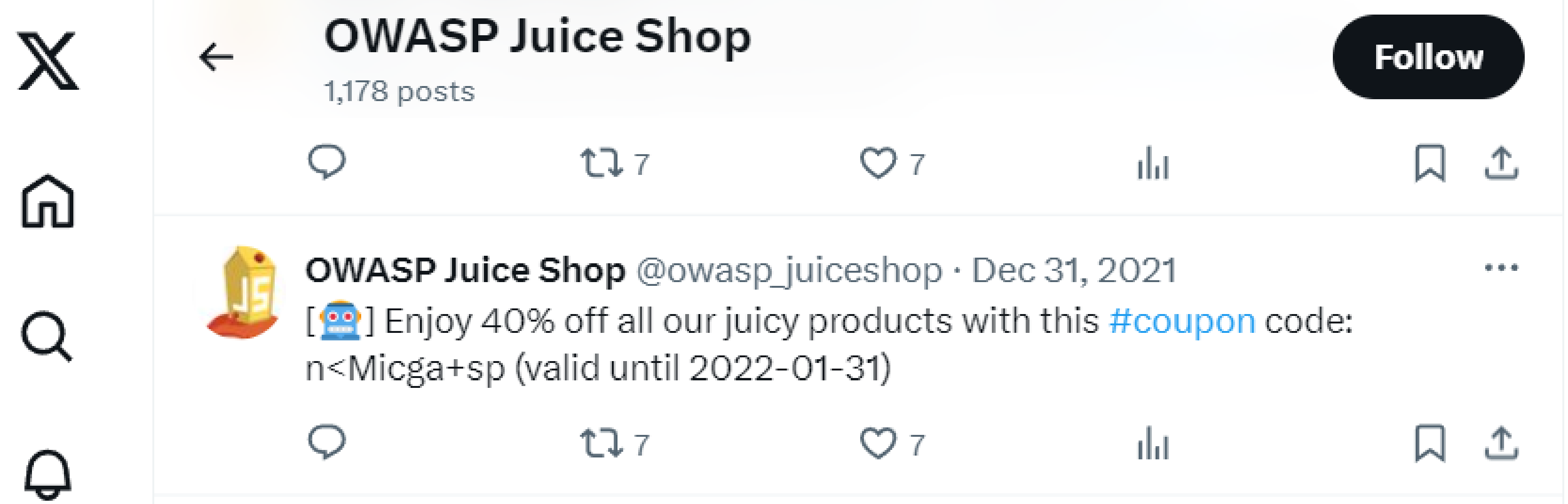
Add new card — Add a credit or debit card

Pay using wallet — **Wallet Balance** 0.00

Add a coupon — Add a coupon code to receive discounts

Coupon *

Need a coupon code? Follow us on Twitter or Facebook for monthly coupons and other spam! 0/10

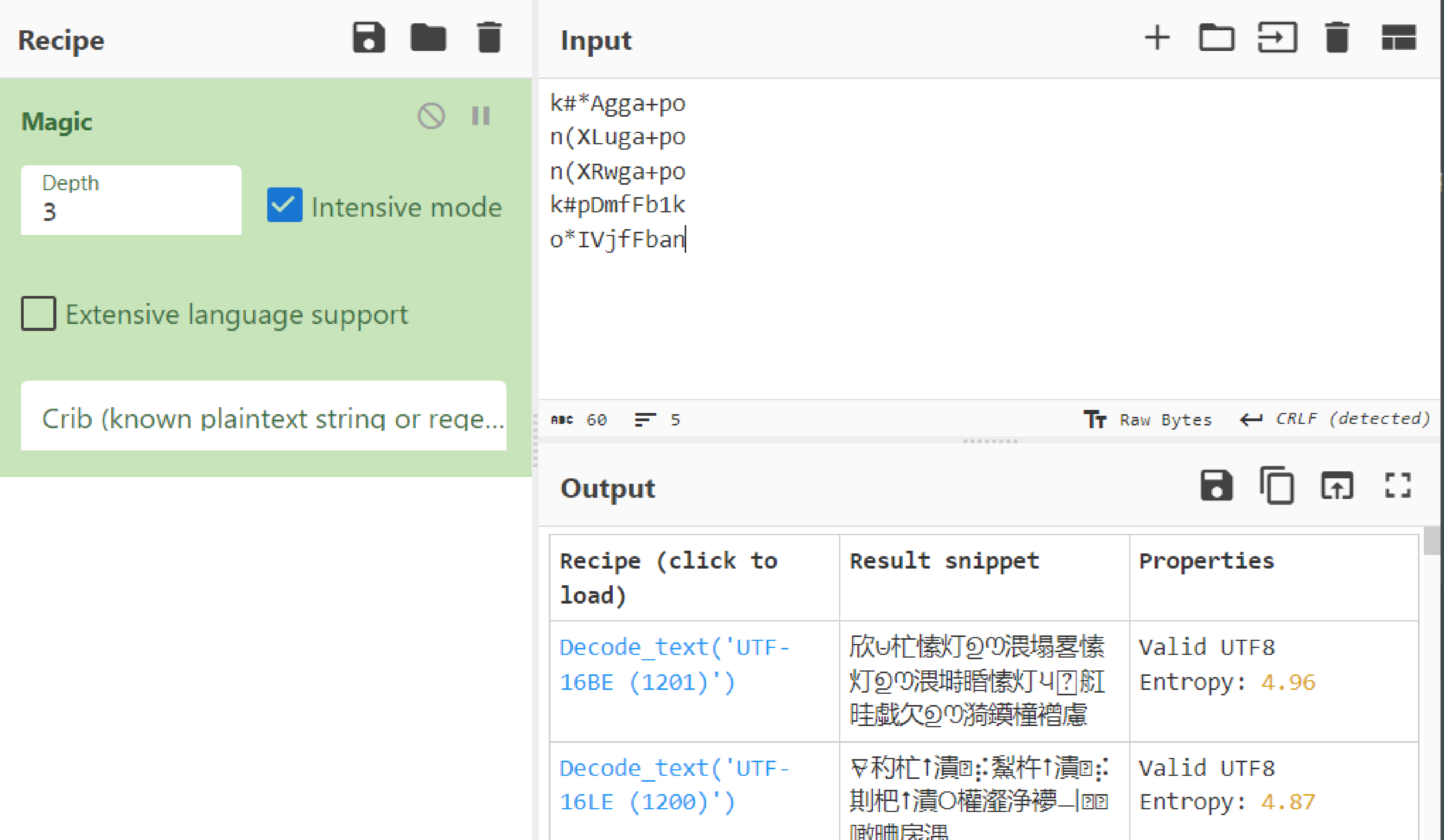


OWASP Juice Shop @owasp_juiceshop · Dec 31, 2021

[🤖] Enjoy 40% off all our juicy products with this #coupon code: n<Micga+sp (valid until 2022-01-31)

Some Old Coupons

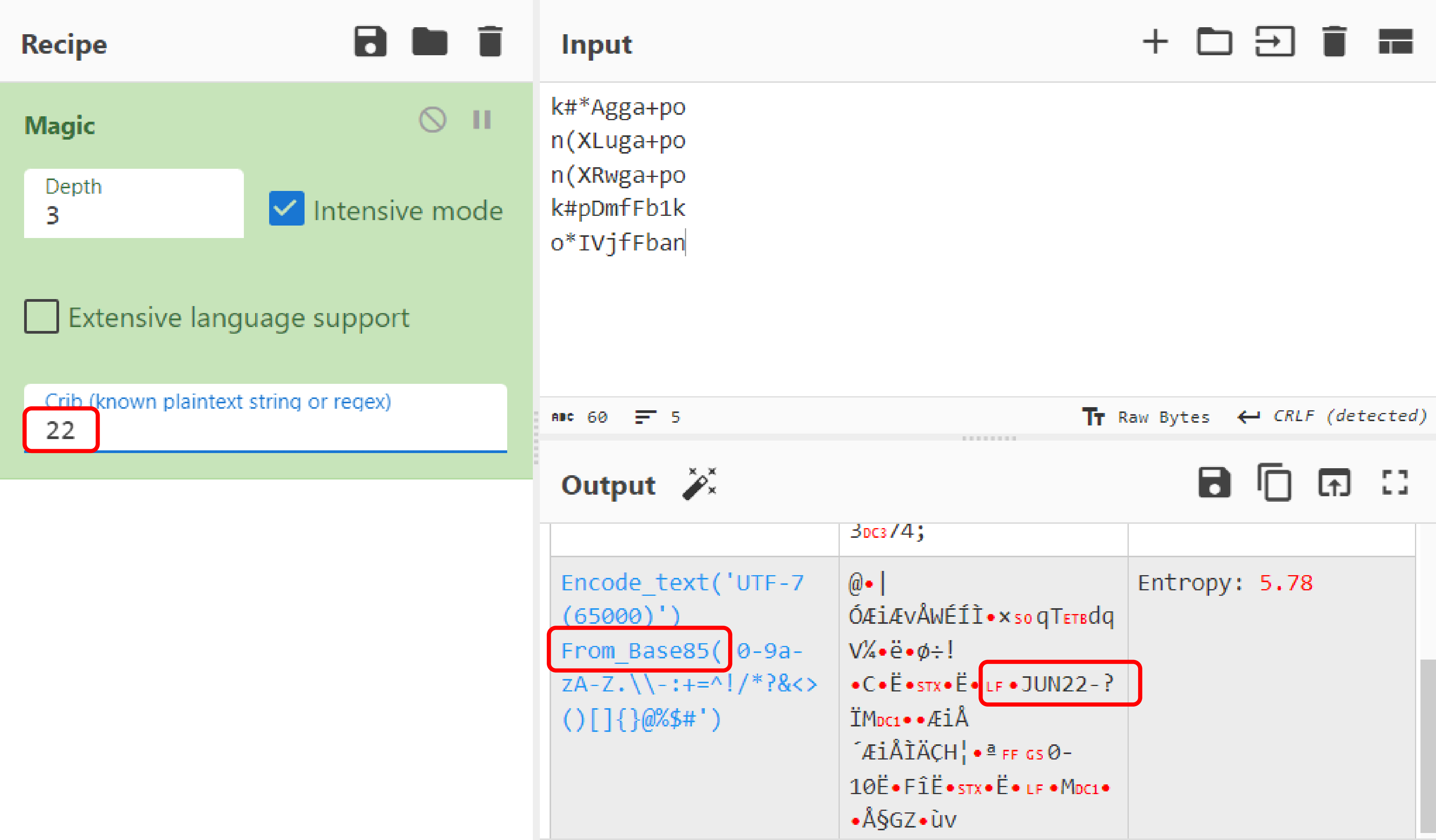
Coupon Code	Discount	Date
k#*Agga+po	30%	2022-08-31
n(XLuga+po	30%	2022-07-31
n(XRwga+po	30%	2022-06-30
k#pDmfFb1k	10%	2020-04-30
o*IVjfFban	40%	2020-03-31



Recipe
Magic
Depth
3
☑ Intensive mode
□ Extensive language support
Crib (known plaintext string or rege...
Input
Output

```
k#*Agga+po
n(XLuga+po
n(XRwga+po
k#pDmfFb1k
o*IVjfFban
```

Recipe (click to load)	Result snippet	Properties
Decode_text('UTF-16BE (1201)')	欣⩁杧愫灯ഊ渨塌畧愫灯ഊ渨塒睧愫灯ч?舡畦戲欠ഊ漪鐨橦禬慮	Valid UTF8 Entropy: 4.96
Decode_text('UTF-16LE (1200)')	⍫䄪杧⭡潰?⡮䱘杵⭡潰?⡮剘杷⭡潰○權瀣浄褸—|??瞰聃戻渪	Valid UTF8 Entropy: 4.87



Magic

Depth
3

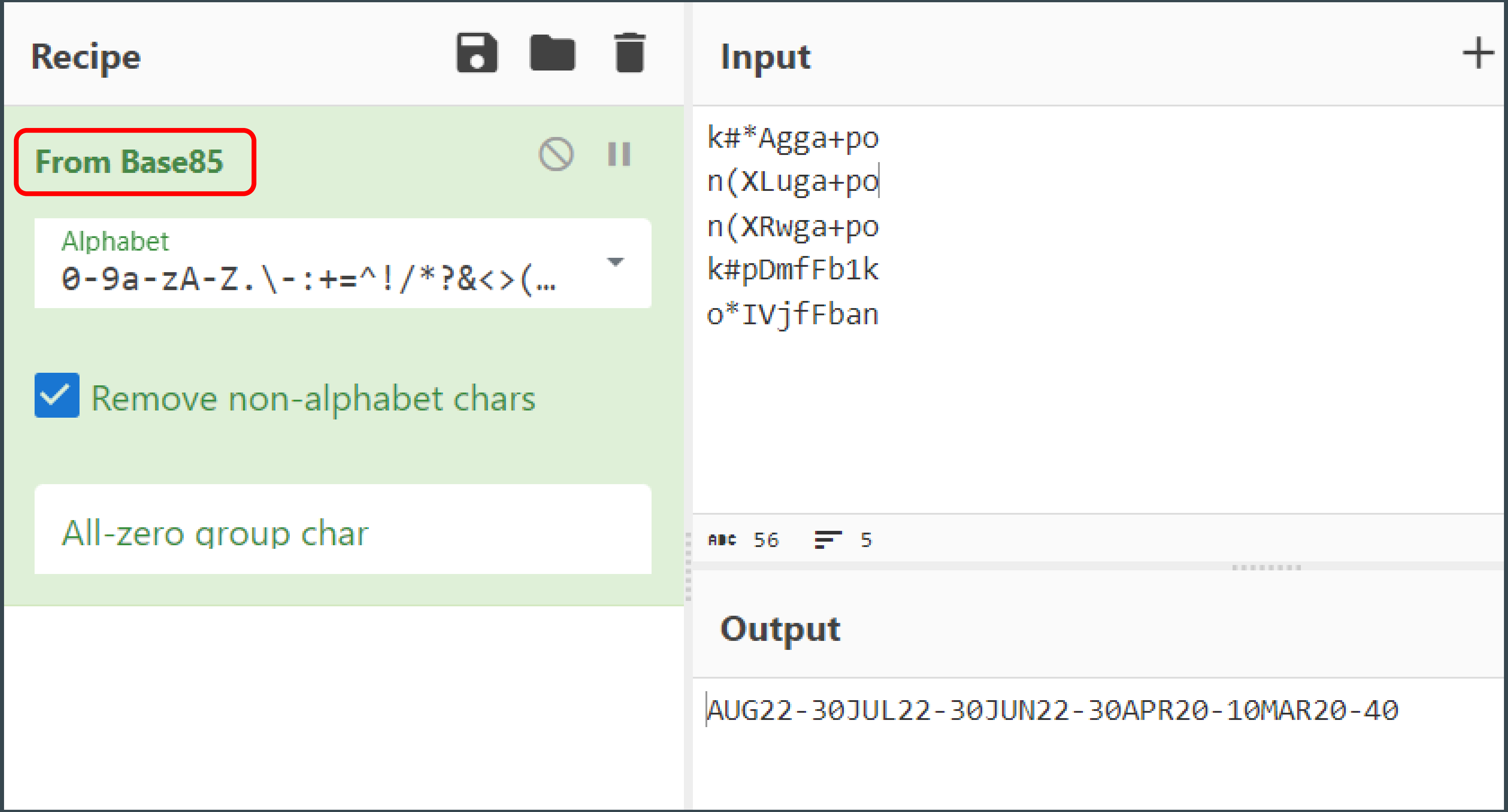
☑ Intensive mode

□ Extensive language support

Crib (known plaintext string or regex)
22

```
k#*Agga+po
n(XLuga+po
n(XRwga+po
k#pDmfFb1k
o*IVjfFban
```

```
3DC3/4;

Encode_text('UTF-7     @•|                          Entropy: 5.78
(65000)')              ÓÆiÆvÅWÉÍÌ•×SOqTETBdq
From_Base85('0-9a-     V¼•ë•ø÷!
zA-Z.\\-:+=^!/*?&<>    •C•Ë•STX•Ë•LF•JUN22-?
()[]{}@%$#')           ÏMDC1••ÆiÅ
                       ´ÆiÅÌÄÇH¦•ª FF GS 0-
                       10Ë•FîË•STX•Ë•LF•MDC1•
                       •Å§GZ•ùv
```



From Base85

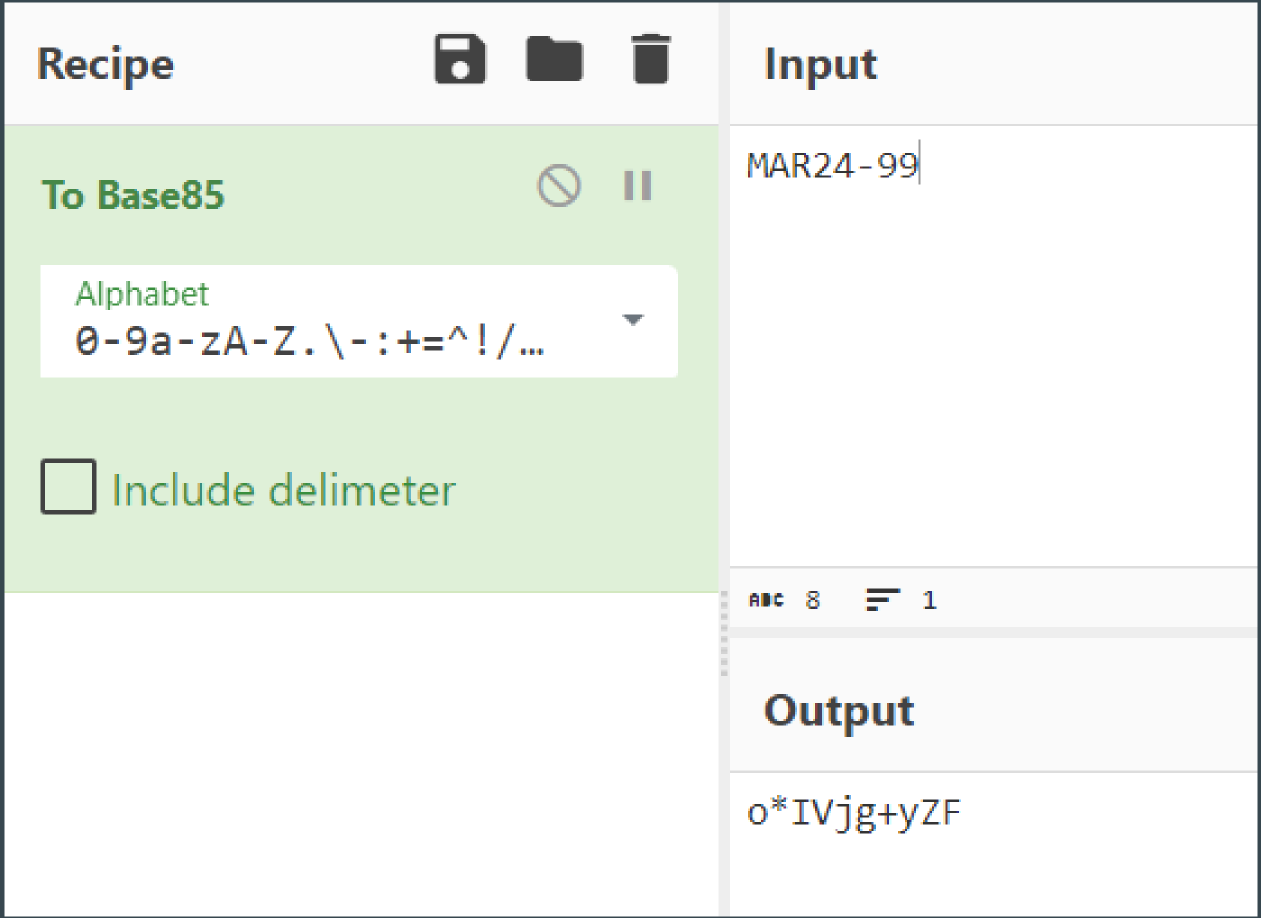
Alphabet
0-9a-zA-Z.\-:+=^!/*?&<>(…

☑ Remove non-alphabet chars

All-zero group char

```
k#*Agga+po
n(XLuga+po
n(XRwga+po
k#pDmfFb1k
o*IVjfFban
```

```
AUG22-30JUL22-30JUN22-30APR20-10MAR20-40
```



Recipe

To Base85

Alphabet
0-9a-zA-Z.\-:+=^!/…

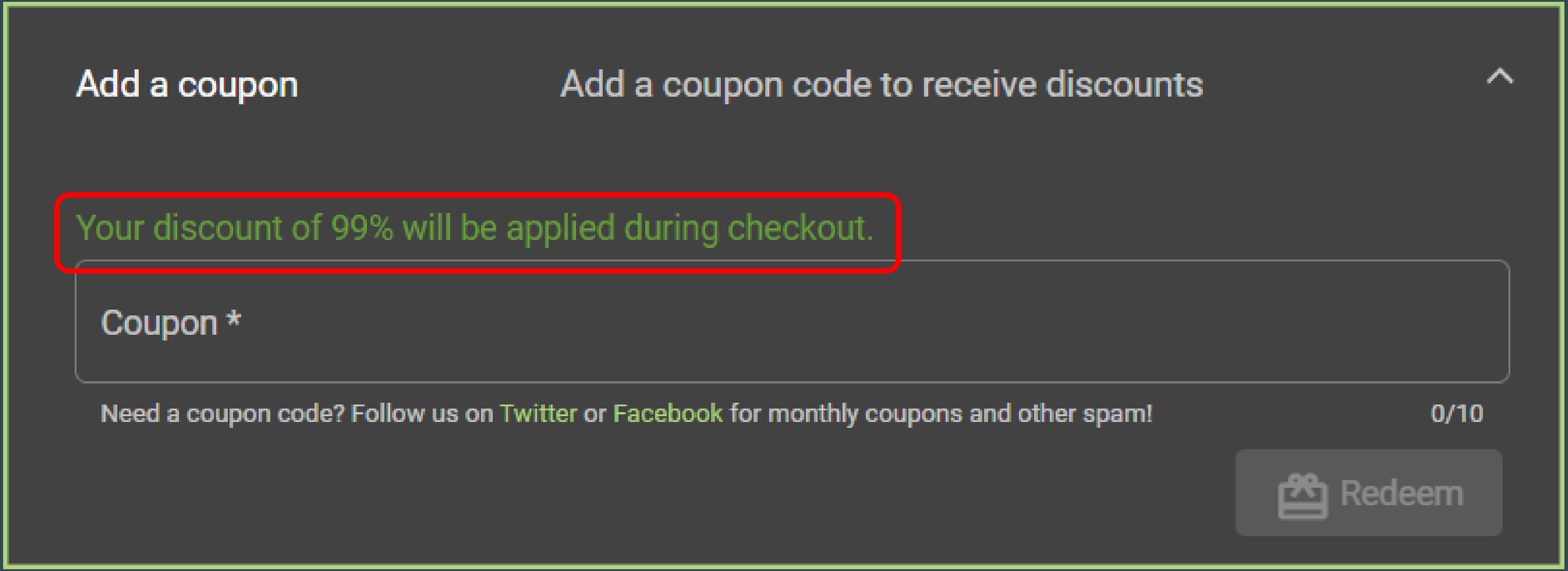
□ Include delimeter

Input

```
MAR24-99
```

Output

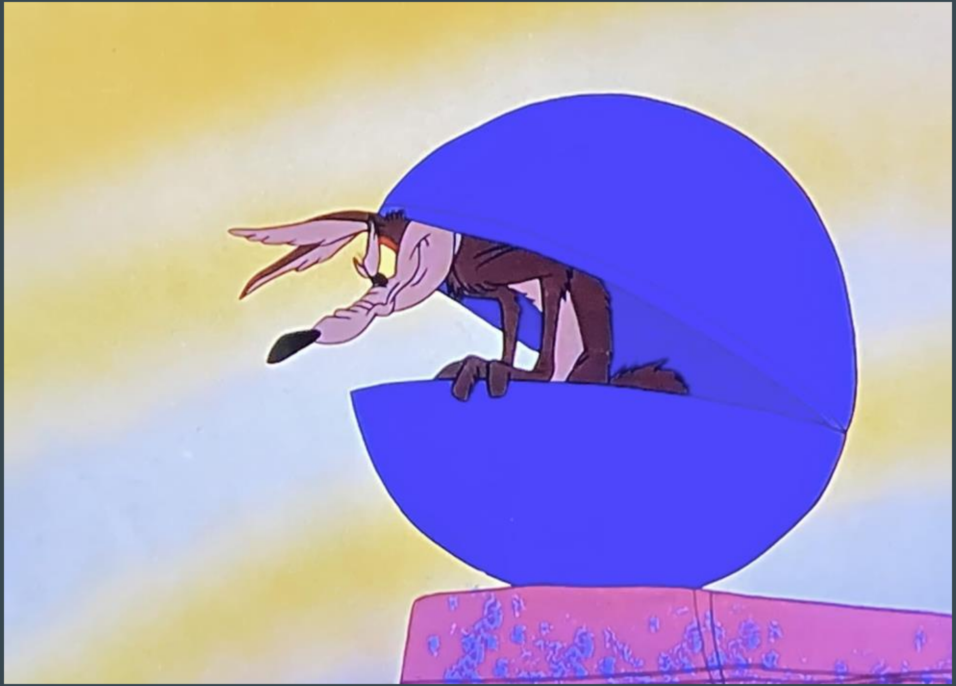
```
o*IVjg+yZF
```



Your discount of 99% will be applied during checkout.

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

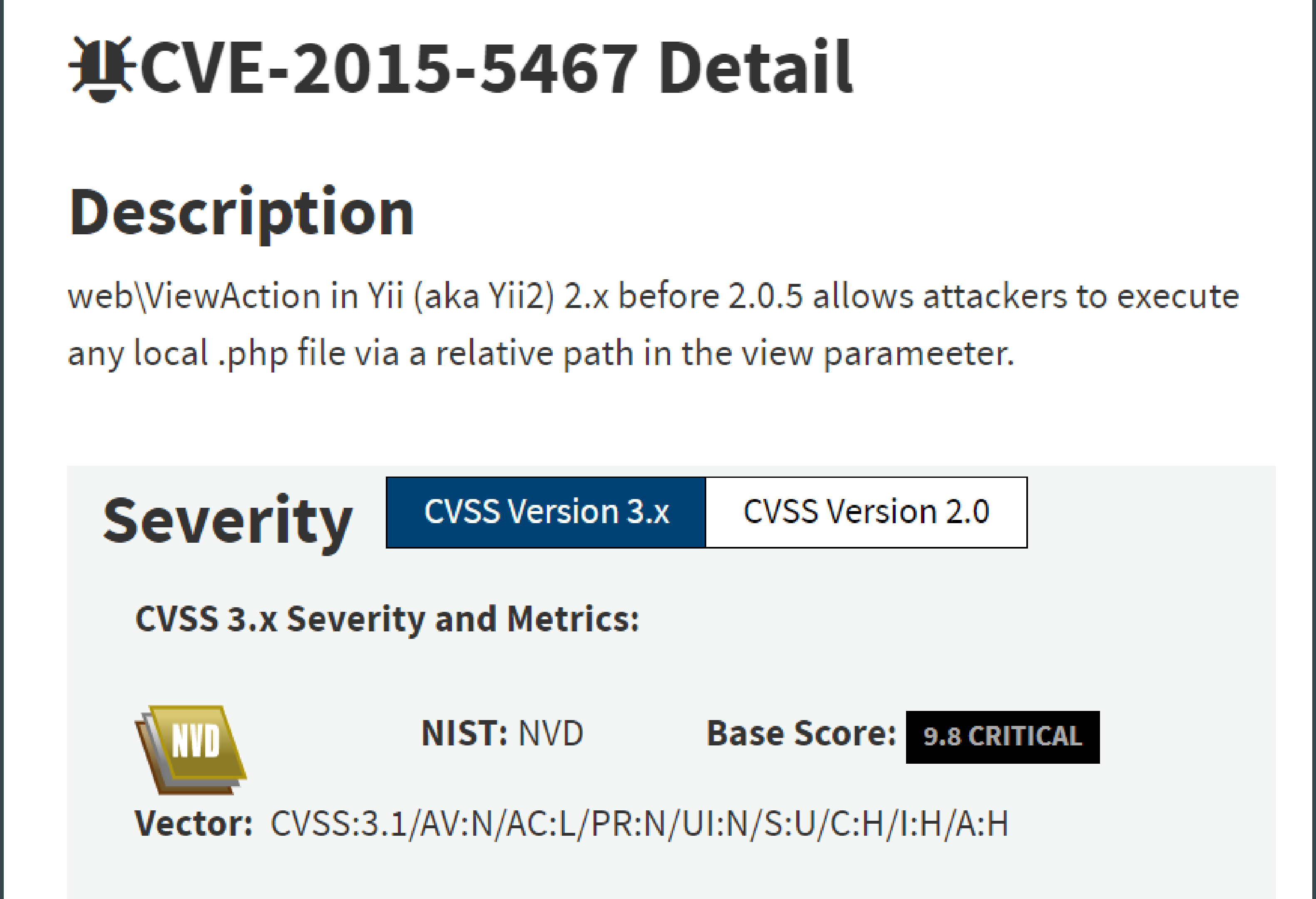
A02 Cryptographic Failures



- Use strong, standard algorithms
- Manage keys properly
- Encrypt all data in transit
- Store passwords with salts and a delay factor
- Ensure high entropy for crypto-graphic randomness

A06 Vulnerable and Outdated Components

Problem	Vulnerable component creates a path for attackers
Concerns	libraries, modules, snippets, infrastructure; nested dependencies.
Incidents	Equifax (unpatched Struts) Numerous IoT examples WannaCry, Heartbleed...
Mitigation	Apply patches Use a SCA scanner Manage third-party components (evaluate, inventory, monitor, scan, sunset)



CVE-2015-5467 Detail

Description

web\ViewAction in Yii (aka Yii2) 2.x before 2.0.5 allows attackers to execute any local .php file via a relative path in the view parameeter.

Severity

CVSS 3.x Severity and Metrics:

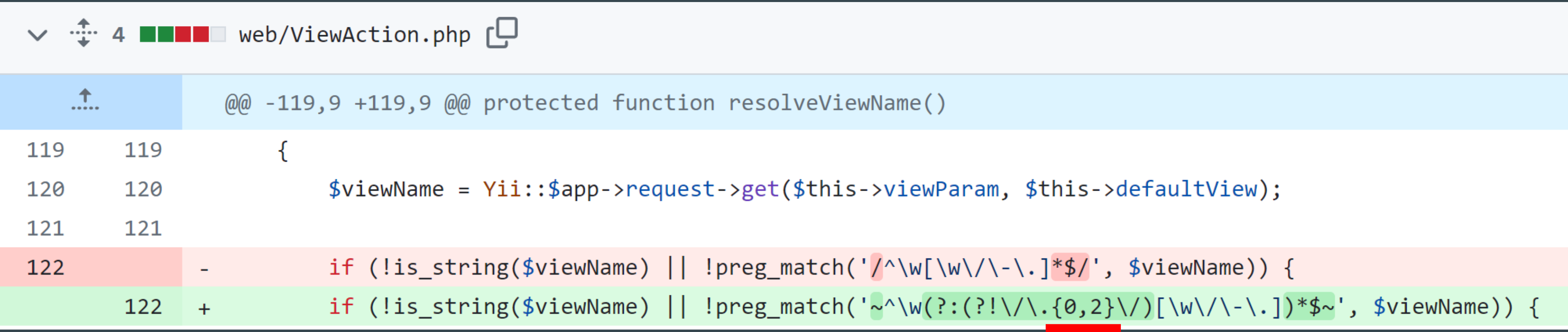
NIST: NVD **Base Score:** 9.8 CRITICAL

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

What Could You Do With This?

```
http://example.com/index.php?
    r=site/page&view=../../private.php
```

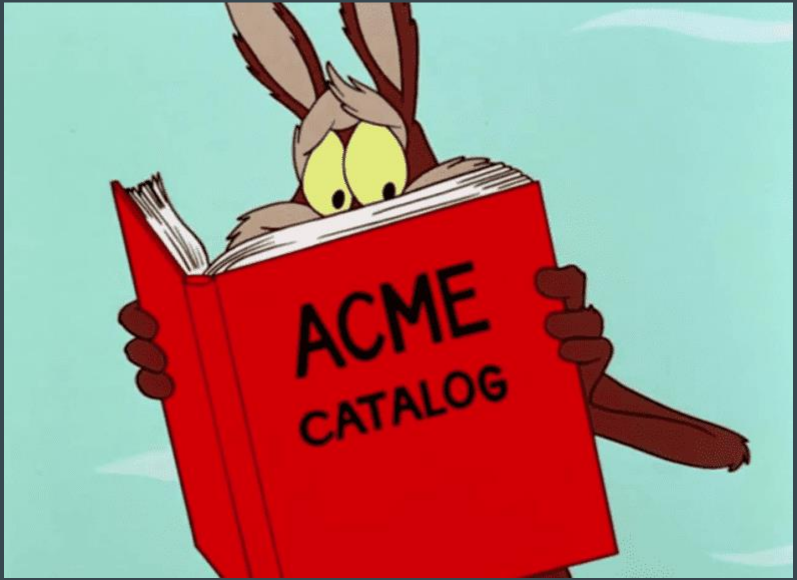
What Was the Fix?

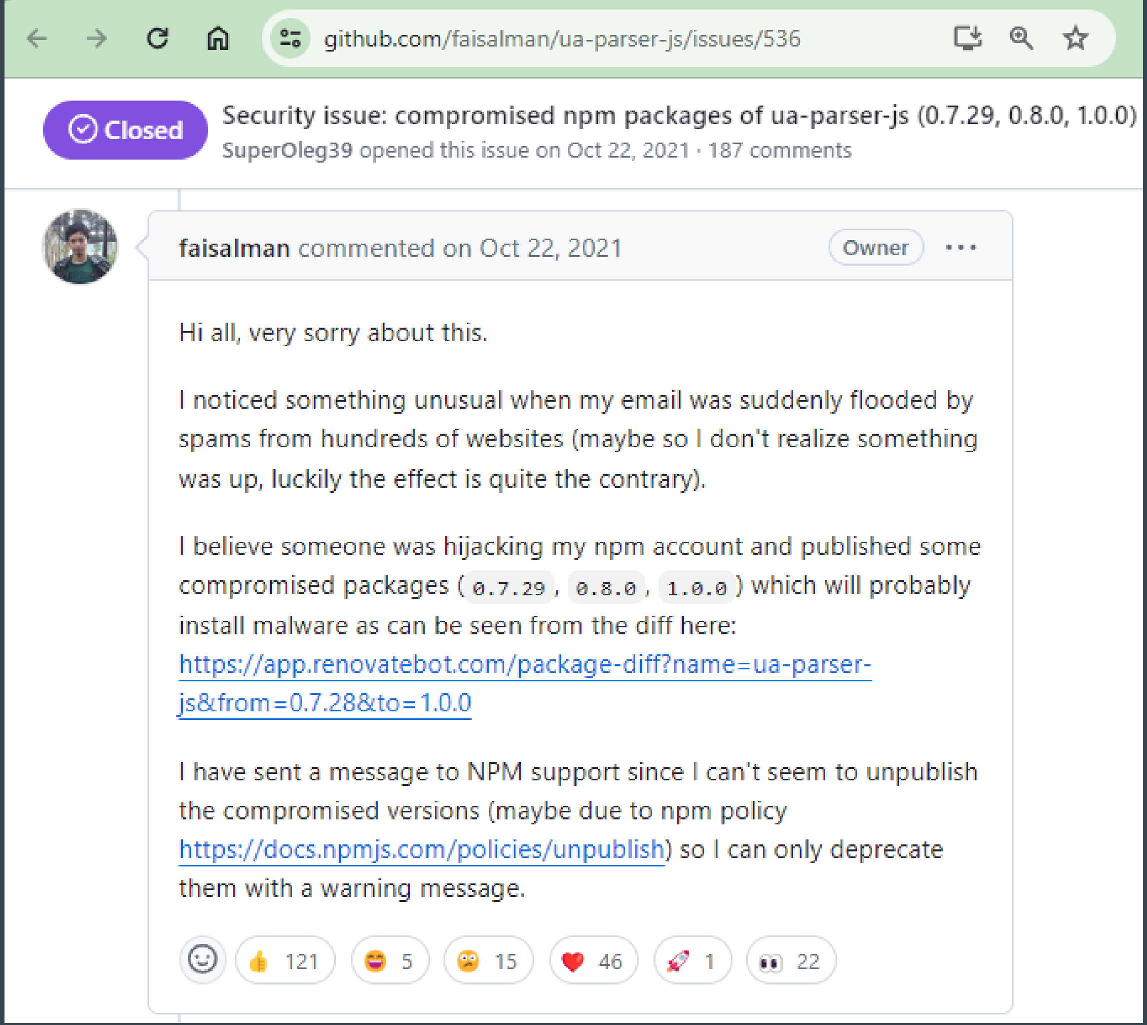


```
@@ -119,9 +119,9 @@ protected function resolveViewName()
        {
            $viewName = Yii::$app->request->get($this->viewParam, $this->defaultView);

-           if (!is_string($viewName) || !preg_match('/^\w[\w\/\-\.]*$/', $viewName)) {
+           if (!is_string($viewName) || !preg_match('~^\w(?:(?!\/\.{0,2}\/)[\w\/\-\.])*$~', $viewName)) {
```

A08 Software & Data Integrity

Problem	Failure to validate integrity of incoming code, components.
Concerns	Third-party channels including source repos, tool suppliers, data channels...
Incidents	• SolarWinds • Home router firmware updates
Mitigation	Digital signatures, trusted repos, SCA scanning, CI/CD pipeline access control, encryption for data in transit...





Closed Security issue: compromised npm packages of ua-parser-js (0.7.29, 0.8.0, 1.0.0)

SuperOleg39 opened this issue on Oct 22, 2021 · 187 comments

faisalman commented on Oct 22, 2021 Owner

Hi all, very sorry about this.

I noticed something unusual when my email was suddenly flooded by spams from hundreds of websites (maybe so I don't realize something was up, luckily the effect is quite the contrary).

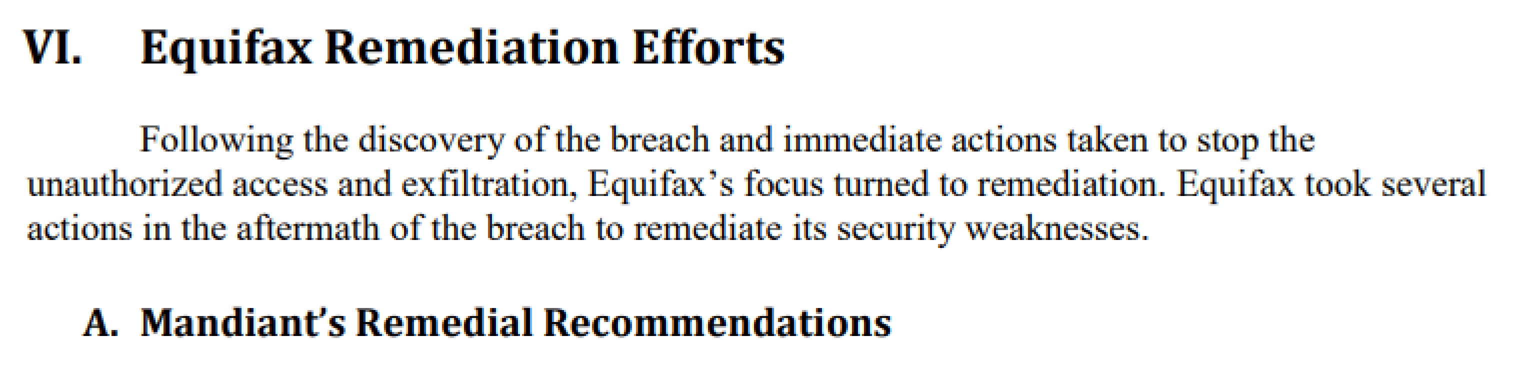
I believe someone was hijacking my npm account and published some compromised packages (`0.7.29`, `0.8.0`, `1.0.0`) which will probably install malware as can be seen from the diff here: https://app.renovatebot.com/package-diff?name=ua-parser-js&from=0.7.28&to=1.0.0

I have sent a message to NPM support since I can't seem to unpublish the compromised versions (maybe due to npm policy https://docs.npmjs.com/policies/unpublish) so I can only deprecate them with a warning message.

A09 Logging & Monitoring Failures

Problem	Inadequate detective and forensic log data
Concerns	Detecting attacks in progress Blocking attack vectors after an incident Determining exposure precisely
Incidents	SolarWinds Home router firmware updates
Mitigation	Log for forensics, not just debugging Ensure logs can be correlated Monitor logs regularly

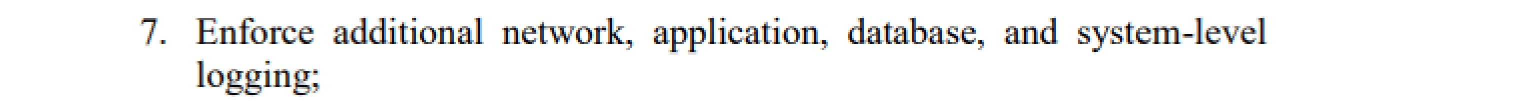
MANDIANT



VI. Equifax Remediation Efforts

Following the discovery of the breach and immediate actions taken to stop the unauthorized access and exfiltration, Equifax's focus turned to remediation. Equifax took several actions in the aftermath of the breach to remediate its security weaknesses.

A. Mandiant's Remedial Recommendations



7. Enforce additional network, application, database, and system-level logging;

- Local logs not forwarded to the SIEM
- Inaccurate field mapping
- Application updates sometimes affected SIEM ingestion and parsing
- Time zone misconfigured
- Log retention time too short
- Source IP addresses of users masked by a load balancer
- No documentation of log fields or sources
- No playbooks for investigating issues consistently and reliably
- Application logs designed for troubleshooting, not investigating

Recommendation

Run mock forensic incidents to confirm:

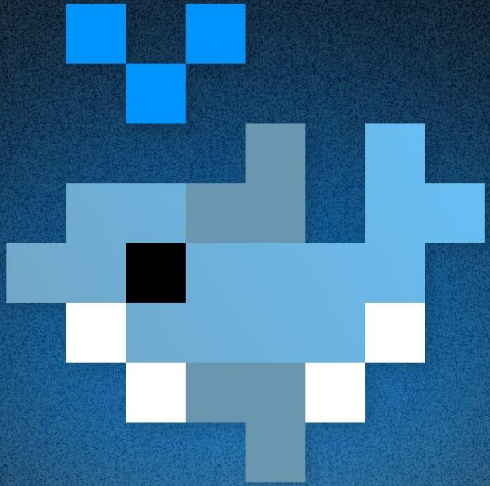
- You are logging the right things.
- Your logs are configured correctly.
- You know how to find the info you need reliably.

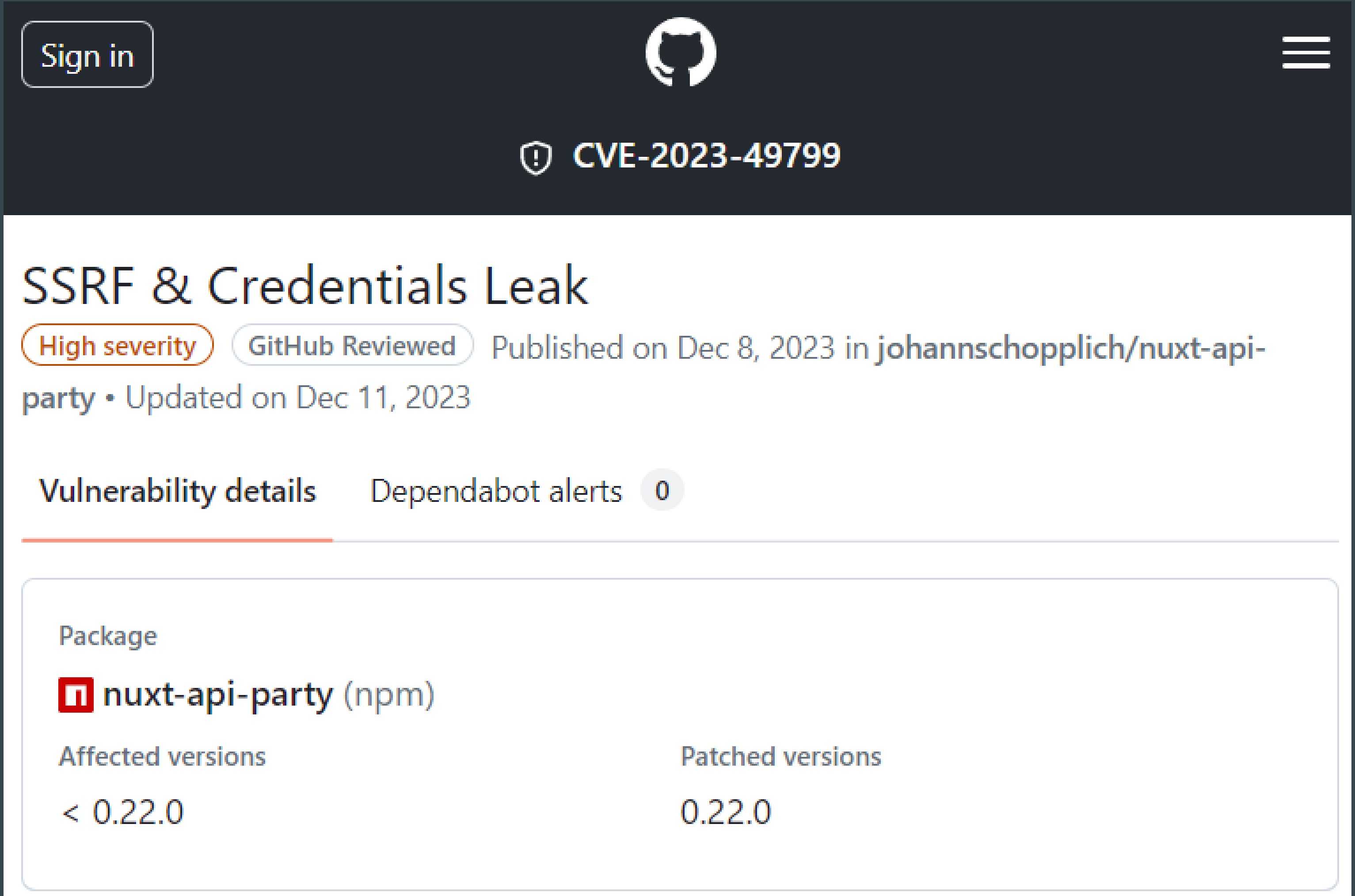
A10 Server-Side Request Forgery (SSRF)

Problem	Web app fetches remote resource without validating URL
Concerns	Fetching malicious resources Exposing local resources
Incidents	Tesla (2018) Capital One (2019)
Mitigation	Validate all user-supplied input Whitelist allowed schema/domains

Nuxt API Party

Connect to APIs securely with a server proxy and dynamic composables





CVE-2023-49799

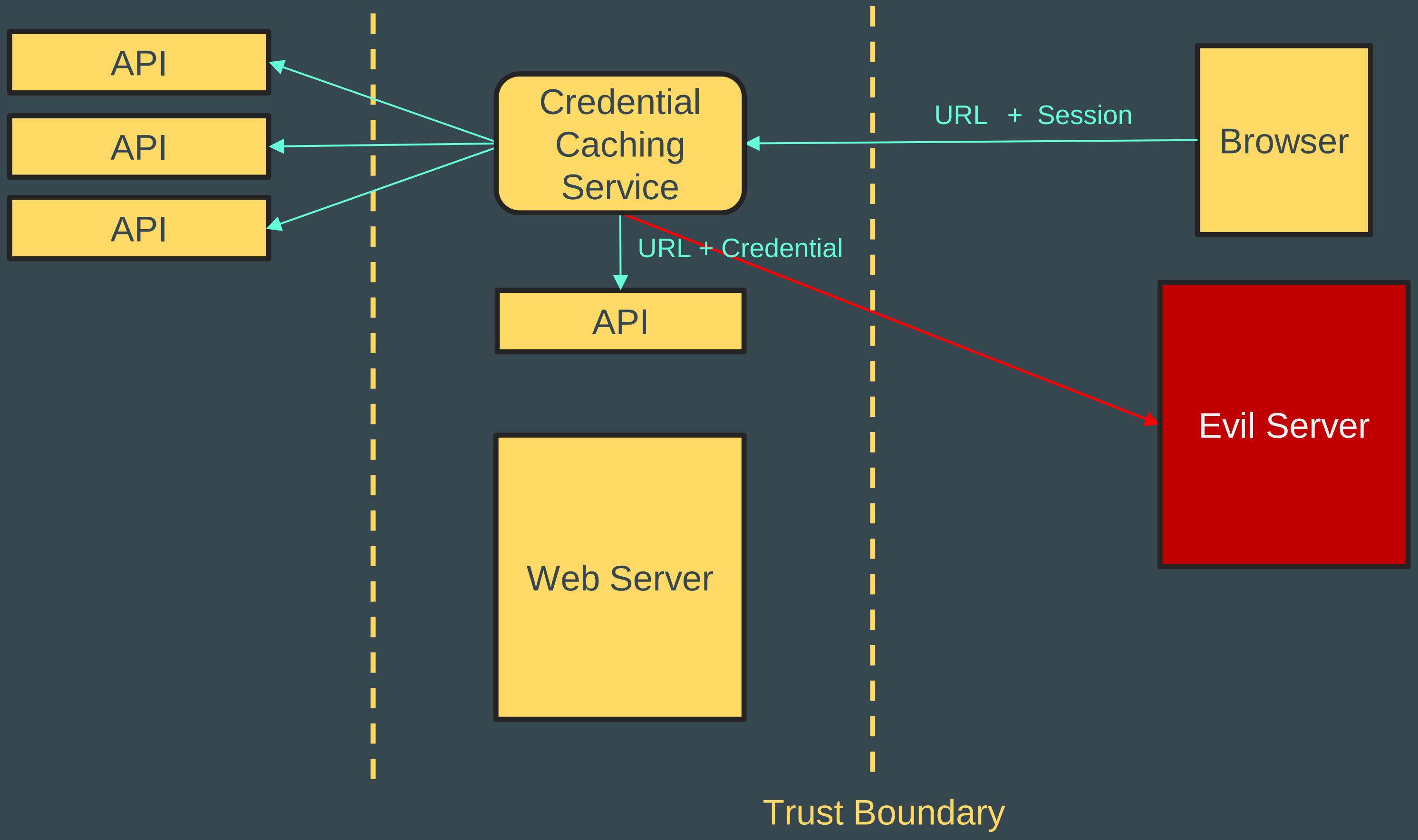
SSRF & Credentials Leak

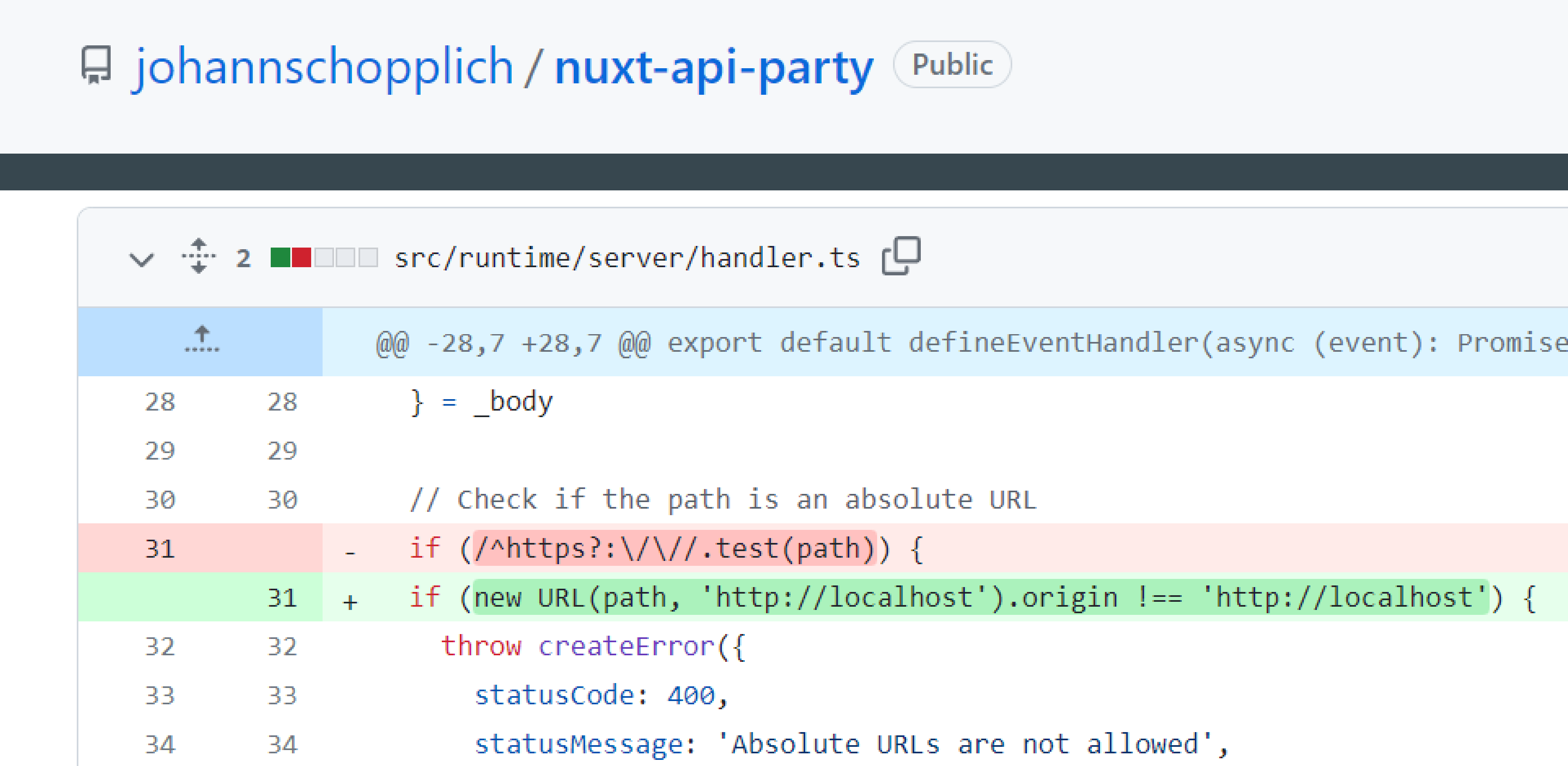
High severity GitHub Reviewed Published on Dec 8, 2023 in **johannschopplich/nuxt-api-party** • Updated on Dec 11, 2023

Package

nuxt-api-party (npm)

Affected versions	Patched versions
< 0.22.0	0.22.0


API
API
API
Credential Caching Service
URL + Session
Browser
URL + Credential
API
Evil Server
Web Server
Trust Boundary



johannschopplich / nuxt-api-party Public

2 src/runtime/server/handler.ts

```diff
@@ -28,7 +28,7 @@ export default defineEventHandler(async (event): Promise
     } = _body
 
     // Check if the path is an absolute URL
-    if (/^https?:\/\//.test(path)) {
+    if (new URL(path, 'http://localhost').origin !== 'http://localhost') {
       throw createError({
         statusCode: 400,
         statusMessage: 'Absolute URLs are not allowed',
```

What We Saw

Security Misconfiguration	Exposed ftp directory
Insecure Design	Use of security questions
Broken Access Control	Unauthorized access to cart via IDOR
Injection (SQL)	Logged in as admin; fetched schema
Identity & Authorization Failures	Created an unauthorized admin user
Cryptographic Failures	Forged a discount coupon
Vulnerable & Outdated Components	Directory traversal in Yii
Software & Data Integrity	ua-parser-js compromised by Monero mining code
Logging & Monitoring Failures	Forensic recommendations from Mandiant
Server Side Request Forgery (SSRF)	Credential leak in nux-api-party

Resources

From OWASP

Cheat Sheets

Testing Guide

OWASP Juice Shop

Vulnerable Web Applications

Other Favorites

FireFox
Developer Tools

PortSwigger
Web Security Academy (free online training)

SafetyLight LLC

brian@safetylight.dev

License and Attribution