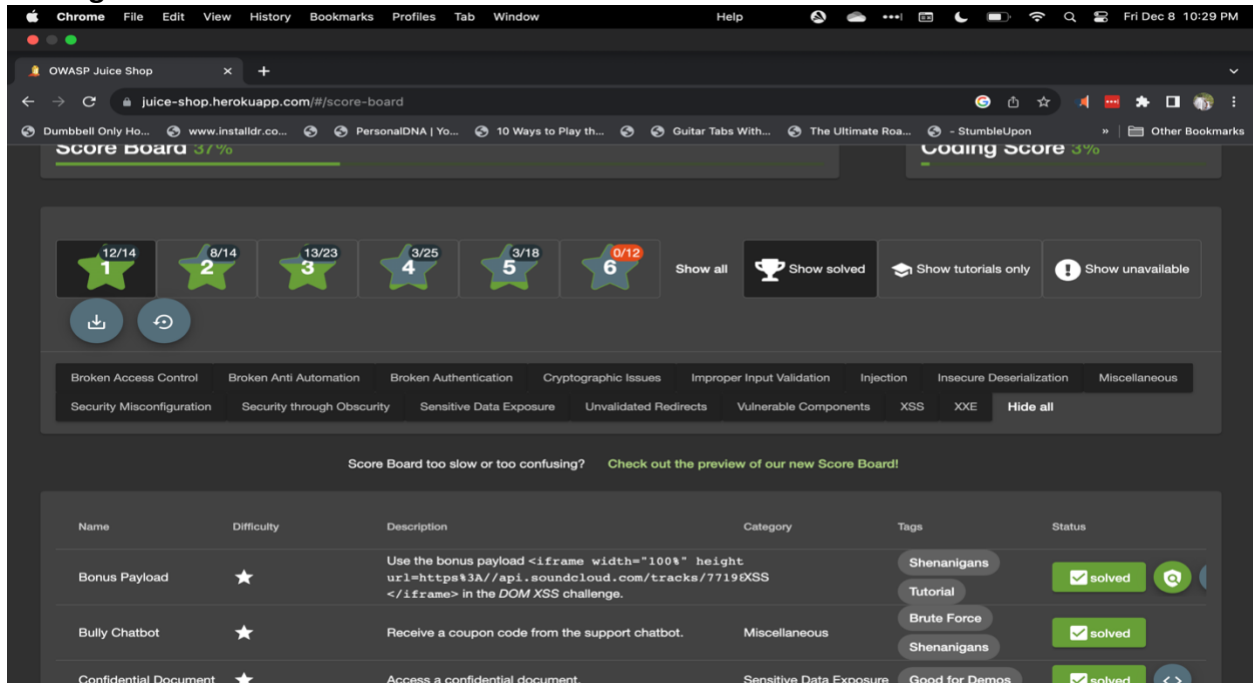


Week 3 LAB
Kyle Ford
12/15/2023

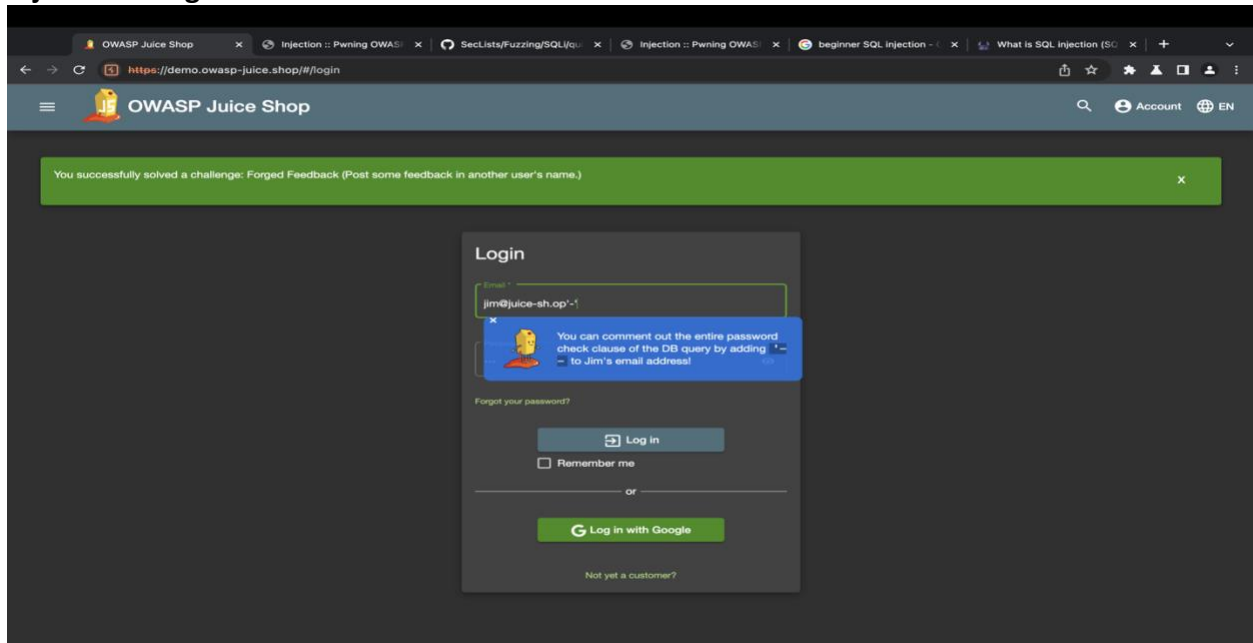
Finding the Score Board



The screenshot shows the OWASP Juice Shop Score Board in a Chrome browser. The URL is `juice-shop.herokuapp.com/#/score-board`. The page displays a progress bar for the "Score Board" at 37% and a "Coding Score" at 3%. Below the progress bar, there are six challenge cards numbered 1 to 6, each with a star icon and a difficulty level (e.g., 12/14, 8/14, 13/23, 3/25, 3/18, 0/12). To the right of the cards are buttons: "Show all", "Show solved", "Show tutorials only", and "Show unavailable". Below the cards are two circular icons: a download icon and a refresh icon. A category filter bar is visible with options: 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, and XXE. A message states: "Score Board too slow or too confusing? Check out the preview of our new Score Board!". Below this is a table of challenges.

Name	Difficulty	Description	Category	Tags	Status
Bonus Payload	★	Use the bonus payload <code><iframe width=</code> "100%" height url=https%3A//api.soundcloud.com/tracks/77196XSS <code></iframe></code> in the DOM XSS challenge.		Shenanigans Tutorial	<input checked="" type="checkbox"/> solved
Bully Chatbot	★	Receive a coupon code from the support chatbot.	Miscellaneous	Brute Force Shenanigans	<input checked="" type="checkbox"/> solved
Confidential Document	★	Access a confidential document.	Sensitive Data Exposure	Good for Demos	<input checked="" type="checkbox"/> solved

Injection – Login as Jim



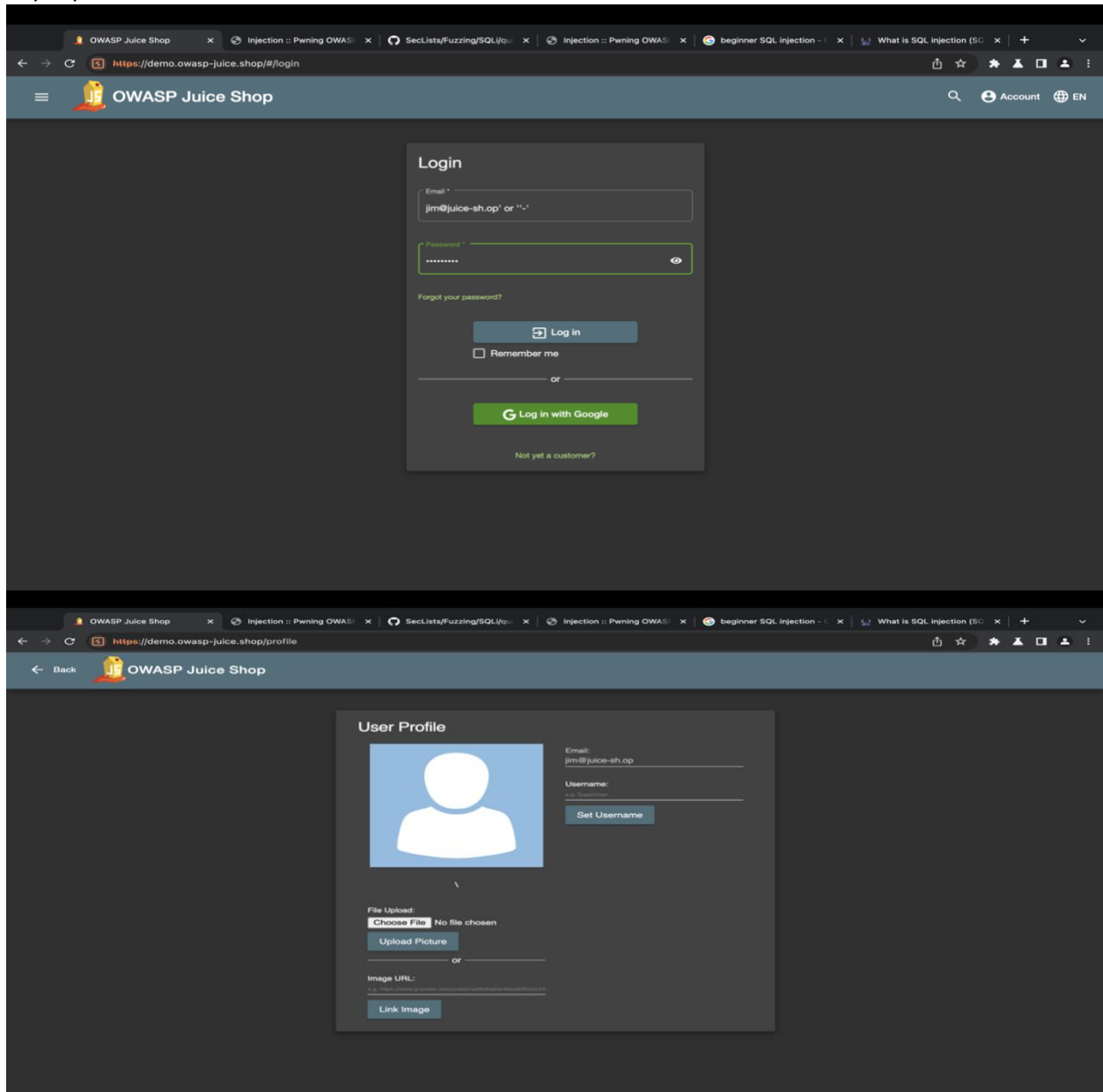
The screenshot shows the OWASP Juice Shop Login page in a Chrome browser. The URL is `https://demo.owasp-juice.shop/#/login`. A green notification banner at the top states: "You successfully solved a challenge: Forged Feedback (Post some feedback in another user's name.)". The login form is centered and contains the following elements:

- Login** header
- Email input field with the value `jim@juice-shop.org`
- A blue tooltip message: "You can comment out the entire password check clause of the DB query by adding `--` to Jim's email address!"
- Forgot your password? link
- Log in button
- Remember me checkbox
- or separator
- Log in with Google button
- Not yet a customer? link

Week 3 LAB

Kyle Ford

12/15/2023



Week 3 LAB
Kyle Ford
12/15/2023

Broken Authentication -

The screenshot shows the OWASP Juice Shop Score Board. At the top, the browser address bar displays `https://juice-shop.herokuapp.com/#/score-board`. The page features two progress bars: "Score Board 37%" and "Coding Score 10%". Below these are six challenge cards, each with a star icon and a progress indicator (e.g., 12/14, 8/14, 13/23, 3/25, 3/18, 0/12). A "Show all" button is next to the cards. Below the cards are three buttons: "Show solved", "Show tutorials only", and "Show unavailable". A navigation bar lists various categories: Broken Access Control, Broken Anti Automation, Broken Authentication (selected), Cryptographic Issues, Improper Input Validation, Injection, Insecure Deserialization, Miscellaneous, Security Misconfiguration, Security through Obscurity, Sensitive Data Exposure, Unvalidated Redirects, Vulnerable Components, XSS, and XXE. A message states: "Score Board too slow or too confusing? Check out the preview of our new Score Board!". Below this is a table with columns: Name, Difficulty, Description, Category, Tags, and Status. The first row shows "Password Strength" with a difficulty of two stars, a description about logging in with administrator credentials, a category of "Broken Authentication", and tags for "Brute Force" and "Tutorial". The status is "solved". A footer message encourages users to report new vulnerabilities via Gitter or GitHub.

Name	Difficulty	Description	Category	Tags	Status
Password Strength	★★	Log in with the administrator's user credentials without previously changing them or applying SQL Injection.	Broken Authentication	Brute Force Tutorial	solved

This screenshot shows the same OWASP Juice Shop Score Board, but with a "Coding Score 8%" and a modal window open for the "Fix 4" challenge. The modal displays a code diff for the `User.init()` method. The diff shows two lines added (marked with green '+' signs) to the password validation logic. Below the code diff, a green box contains a note about NIST-800-63B password requirements. The background shows the same navigation bar and challenge cards as the previous screenshot.

```
1 1 User.init(  
2 2     password: {  
3 3         type: DataTypes.STRING,  
4 4         set (clearTextPassword) {  
5 +             validatePasswordHasAtLeastTenChar(clearTextPassword)  
6 +             validatePasswordIsNotInTopOneMillionCommonPasswordsList(clearTextPassword)  
5 7         this.setDataValue('password', security.hash(clearTextPassword))  
6 8     }  
7 9 }  
7 9 },
```

According to NIST-800-63B, passwords (Memorized Secrets) should have at least eight characters to prevent 'online attacks'. Furthermore, NIST-800-63B requires that passwords don't appear in common dictionaries. If you want to have more fun with secrets, check out OWASP Wrong Secrets at <https://wrongsecrets.fly.dev/>, specially challenge 16 and 23.

Week 3 LAB

Kyle Ford

12/15/2023

Sensitive Data Exposure

OWASP Juice Shop

https://juice-shop.herokuapp.com/#/score-board

Security Misconfiguration Security through Obscurity Sensitive Data Exposure Unvalidated Redirects Vulnerable Components XSS XXE Show all

Name	Confidential Docs	Exposed Metrics	Login MC SafeS	Meta Geo Stalk	NFT Takeover	Visual Geo Stalk
4	-	-	-	-	-	-
5	-	-	-	-	-	-
6	-	-	-	-	-	-
7	-	-	-	-	-	-
8	-	-	-	-	-	-
9	-	-	-	-	-	-
10	-	-	-	-	-	-
11	-	-	-	-	-	-
12	-	-	-	-	-	-
13	-	-	-	-	-	-
14	-	-	-	-	-	-
15	-	-	-	-	-	-
16	-	-	-	-	-	-
17	-	-	-	-	-	-
18	-	-	-	-	-	-

Getting rid of the /ftp folder entirely is the only way to plumb this data leakage for good. Valid static content in it needs to be moved to a more suitable location and order confirmation PDFs had no business to be placed there publicly accessible in the first place. Everything else in that folder was just accidentally put out there rather than secure.

Got an idea for a new challenge? Found a vulnerability that is not tracked here? Let us know via [Gitter.im](#) community chat or by opening a [GitHub](#) issue!

XML External Entities (XXE) - 16 challenges are unavailable on Heroku due to [security concerns](#) or technical incompatibility!

OWASP Juice Shop

https://juice-shop.herokuapp.com/#/score-board-preview?categories=XXE

Hacking Challenges Coding Challenges

Search Difficulty Status Tags

All XSS Sensitive Data Exposure Improper Input Validation Broken Access Control Unvalidated Redirects Vulnerable Components Broken Authentication Security through Obscurity Insecure Deserialization Miscellaneous Broken Anti Automation Injection Security Misconfiguration Cryptographic Issues XXE

This is a preview of the new Score Board. If you notice any bugs or have any feedback, please let us know! Reach out via our community channels. [Back to the old Score Board](#)

16 challenges are unavailable on Heroku due to security concerns or technical incompatibility! [Hide disabled challenges](#)

XXE XXE Data Access ★★★ Retrieve the content of C:\Windows\system, ini or /etc/passwd from the server. (This challenge is not available on Heroku) [Hint](#)

XXE XXE DoS ★★★★★ Give the server something to chew on for quite a while. (This challenge is not available on Heroku) [Hint](#)

12/15/2023

I used burp proxy to intercept the request. Then modified the “star” value to 0 and sent via repeater. I received a success response.

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings

Target: https://demo.owasp-juice.shop HTTP/2

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
<pre> 1 POST /api/renewals/n/r/z 200 2 Host: demo.owasp-juice.shop 3 Cookie: language=en; cookieconsent_status=dismiss; welcomebanner_status=dismiss; continueCode[1]=toRyZdnLwV0S43bbJMjOmPKrTqgAXunAd7p6E3NVLvvgG6A2E9mKzQ; continueCode= Mhh3tYv5btvCZF2XIn24et6Ia7Hn3YtJlVPpMetkKckyFxoSHzU3QTGXW52is0aTpxCj0; token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpzZW50dXkiLCJ1eWUiOiJ1ZDdhbmQ1LjZmZDZlZWZlY2F0OTY5eGpZCjE2LW1udW1lc3NoNW0iO11CLlBWPWF6PC16mpbbBqdWljZS1zaC5vcC1lc2lnbmh3b3B3Ikljo1ZTU0MHNNHNZVjZjcyHTMTANiIQ3MGZjNjEzZTU0NDULCjY2bzIljo1Y3VzdG9PZXI1LLCjZkNmVmdVB2b21ib161ElIiwiaXNjaW5kaWQ6NGRkZAwJAwJiwidGVzZXRLZEFlbjIudXBkx5SwlaWFRBTjo1bnZyAGNOIDNIY0FoLXltY4tQL_85zy2MUgIMhX4G3glTrXRAsKYtp_z_-SP3GLV1daKnIOplLdb07FtsghLVtc7FDuGS5BASwhTRYMP6P-sfgx_nLHFVJ5CuKEQIWinrlJINjOMN38FGGIQAe4LK0U1TAkuLUJFBYXChYZSOBKtaIIlBK 4 Content-Length: 98 5 Sec-Ch-Ua: "Not-A Brand";v="8", "Chromium";v="128" 6 Accept: application/json, text/plain, */* 7 Content-Type: application/json 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 Safari/537.36 9 Origin: https://demo.owasp-juice.shop 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: cors 12 Sec-Fetch-Dest: empty 13 Referer: https://demo.owasp-juice.shop/ 14 Accept-Encoding: gzip, deflate, br 15 Accept-Language: en-US,en;q=0.9 16 Priority: u=1, i 17 18 { 19 "userId":2, 20 "captcha":"11371", 21 "captcha":"21", 22 "comment":"NOW (**@juice-sh.op)", 23 "rating":8 24 } </pre>			<pre> 1 HTTP/2 201 Created 2 Server: Cowboy 3 Report-To: {"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?ts=1702674327&sid=812dc77-8bd08-43b1-a5f1-b25750382959&s=GYSB4MMH2J3Rbid&sMs3NovvUlHzUz2b4sGoZiqkZBSbW4h3D"}]} 4 Reporting-Endpoints: heroku-nelhttps://nel.heroku.com/reports?ts=1702674327&sid=812dc77-8bd08-43b1-a5f1-b25750382959&s=GYSB4MMH2J3Rbid&sMs3NovvUlHzUz2b4sGoZiqkZBSbW4h3D 5 Nel: {"report-to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"response_headers":["Via"]} 6 Access-Control-Allow-Origin: * 7 X-Content-Type-Options: nosniff 8 X-Frame-Options: SAMEORIGIN 9 Feature-Policy: payment "self" 10 X-Recruiting: //jobs 11 Location: /api/feedbacks/111 12 Content-Type: application/json; charset=utf-8 13 Content-Length: 172 14 Etag: W/"ac-cj/GapOERfp28Q5BFqJPBfabXo" 15 Vary: Accept-Encoding 16 Date: Fri, 15 Dec 2023 21:05:27 GMT 17 Via: 1.1 vegur 18 19 { 20 "status":"success", 21 "data":{ 22 "id":111, 23 "userId":2, 24 "comment":"NOW (**@juice-sh.op)", 25 "rating":8, 26 "updatedAt":"2023-12-15T21:05:27.740Z", 27 "createdAt":"2023-12-15T21:05:27.740Z" 28 } 29 } </pre>		

Done

0 highlights

Inspector

Notes

0 highlights

Week 3 LAB

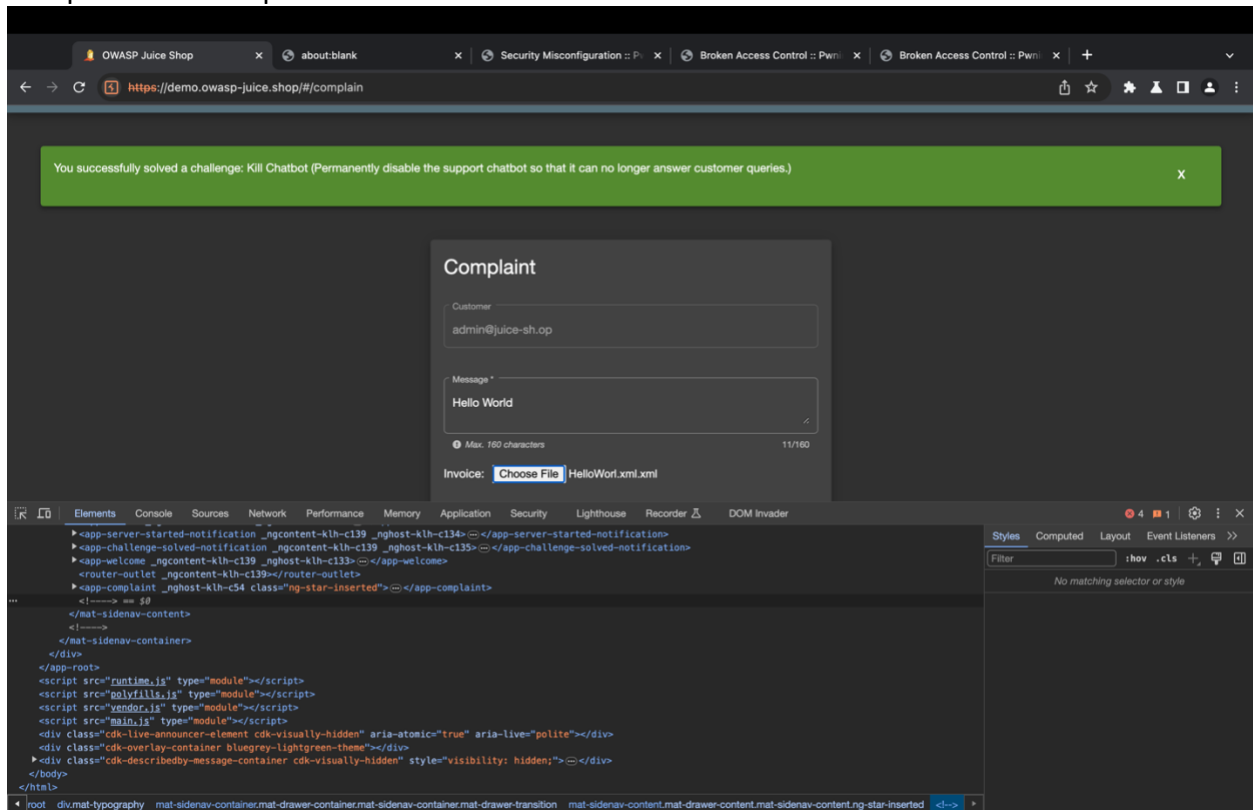
Kyle Ford

12/15/2023

Security Misconfiguration - Deprecated Interface

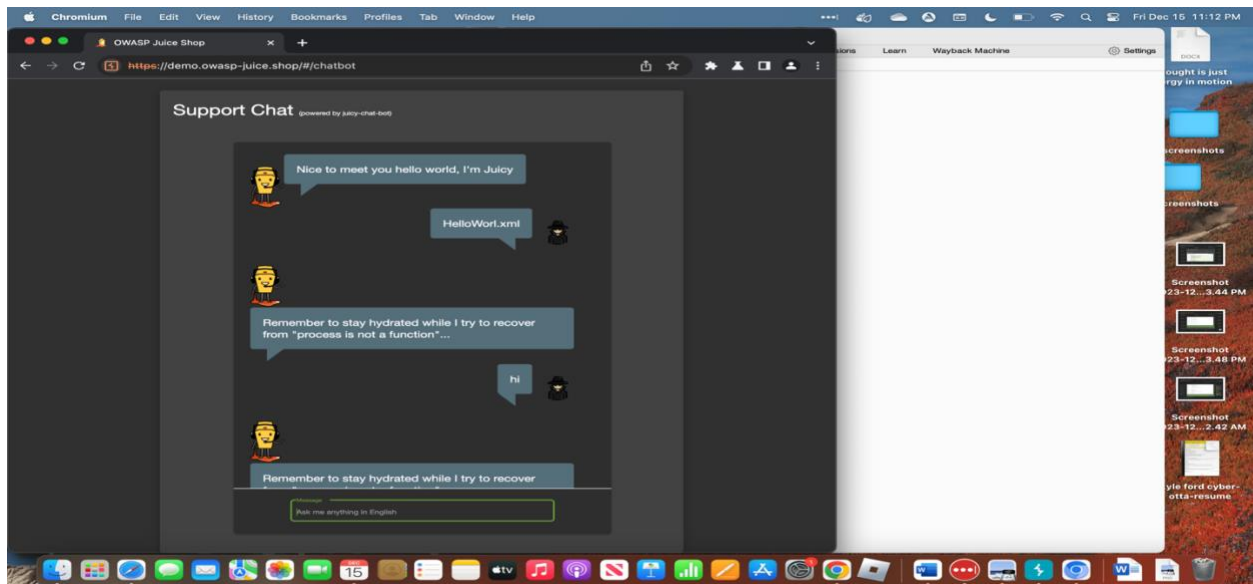
I tried to solve the Use deprecated interface challenge by doing the following:

Complaint menu> upload . XML file > submit.



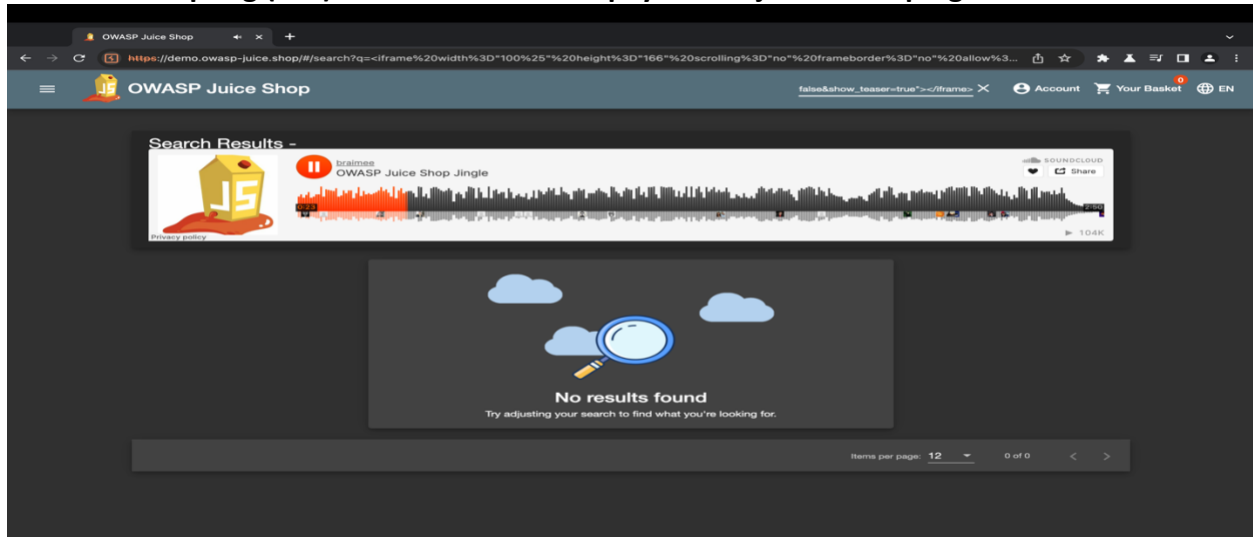
Break the Chatbot

I entered "HelloWorl.xml" into the chat and rendered the chatbot useless.

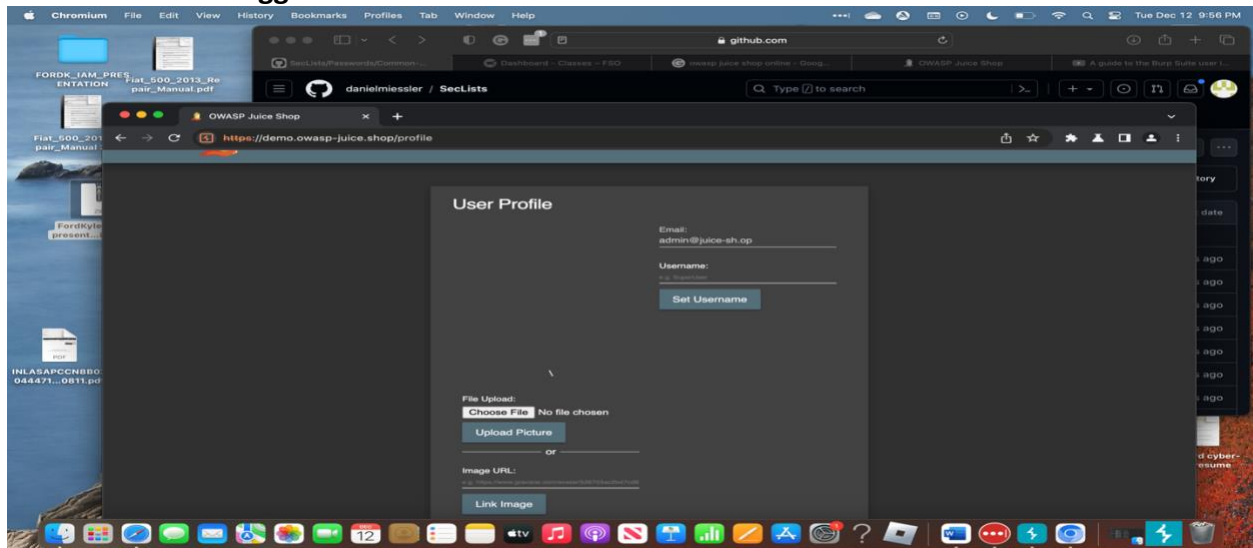


Week 3 LAB
Kyle Ford
12/15/2023

Cross Site Scripting (XSS) – Bonus DOM – XSS payload- injected in top right search box



Weak Password -logged into admin account



Week 3 LAB
Kyle Ford
12/15/2023
Admin Section Coding challenge

The screenshot shows the OWASP Juice Shop Admin Section Coding Challenge interface. The browser address bar displays `https://demo.owasp-juice.shop/#/score-board-preview`. The interface features a sidebar on the left with various security categories and a main area with a coding challenge. The challenge is titled "Coding Challenge: Admin Section" and includes a "Find It" button and a "Fix It" button. The challenge content shows a code diff for the `routes` object, with changes highlighted in green and red. The diff shows the addition of a new route for the `administration` endpoint, which is protected by `canActivate: [AuthGuard]`. The challenge also includes a "Hint" button and a "Submit" button.

OWASP Juice Shop

order_5267-6781bc49acda2

https://demo.owasp-juice.shop/#/score-board-preview

Improper Input Validation

Missing Encoding

Retrieve the photo of Bjørn's cat in "melee combat-mode".

Unvalidated Redirects

Outdated Allowlist

Let us redirect you to one of our crypto currency addresses which are not promoted any longer.

Improper Input Validation

Repetitive Registration

Follow the DRY principle while registering a user.

Coding Challenge: Admin Section

Find It

Fix It

Correct Fix

Fix 2

Only Show Lines with Differences (8)

Side by Side

Line by Line

```
1 1 const routes: Routes = [  
2 2   {  
3 3     // TODO: Externalize admin functions into separate application  
4 4     path: 'administration',  
5 5     // that is only accessible inside corporate network,  
6 6     component: AdministrationComponent,  
7 7     canActivate: [AuthGuard]  
8 8   },  
9 9   // ...  
10 10  { path: 'administration',  
11 11    component: AdministrationComponent,  
12 12  }  
13 13 ]
```

Hint

Submit

The screenshot shows the OWASP Juice Shop Admin Section Coding Challenge interface with the solution displayed. The browser address bar displays `https://demo.owasp-juice.shop/#/score-board-preview`. The interface features a sidebar on the left with various security categories and a main area with a coding challenge. The challenge is titled "Coding Challenge: Admin Section" and includes a "Find It" button and a "Fix It" button. The challenge content shows a code diff for the `routes` object, with changes highlighted in green and red. The diff shows the addition of a new route for the `administration` endpoint, which is protected by `canActivate: [AuthGuard]`. The challenge also includes a "Hint" button and a "Submit" button.

OWASP Juice Shop

order_5267-6781bc49acda2

https://demo.owasp-juice.shop/#/score-board-preview

Improper Input Validation

Missing Encoding

Retrieve the photo of Bjørn's cat in "melee combat-mode".

Unvalidated Redirects

Outdated Allowlist

Let us redirect you to one of our crypto currency addresses which are not promoted any longer.

Improper Input Validation

Repetitive Registration

Follow the DRY principle while registering a user.

Coding Challenge: Admin Section

Find It

Fix It

Correct Fix

Fix 2

Only Show Lines with Differences (8)

Side by Side

Line by Line

```
177 180 component: OAuthComponent  
178 181 },  
179 182 {  
180 183   matcher: tokenMatcher,  
181 184   component: TokenSaleComponent  
182 185 },  
183 186 {  
184 187   path: '403',  
185 188   component: ErrorPageComponent  
186 189 },  
187 190 {  
188 191   path: '',  
189 192   component: SearchResultComponent  
190 193 }  
191 194 ]
```

Hint

Submit

While attempts could be made to limit access to administrative functions of a web shop through access control, it is definitely safer to apply the "separation of concerns" pattern more strictly by internally hosting a distinct admin backend application with no internet exposure.

Week 3 LAB

Kyle Ford

12/15/2023

Broken Access Control

Access Administration section – opened dev tools > located path to administration > typed path into browser.

The screenshot shows a web application interface with a dark theme. The main content area is titled "Administration" and is divided into two sections: "Registered Users" and "Customer Feedback".

Registered Users:

Username	Avatar
admin@juice-sh.op	
jim@juice-sh.op	
bender@juice-sh.op	
bjoern.kimminich@gmail.com	
cisco@juice-sh.op	
support@juice-sh.op	
morty@juice-sh.op	

Customer Feedback:

ID	Feedback	Rating	Action
1	I love this shop! Best products in town! Highly recommended! ("in@juice-sh.op)	★★★★★	
2	Great shop! Awesome service! ("@juice-sh.op)	★★★★★	
3	Nothing useful available here! ("der@juice-sh.op)	★	
21	Please send me the juicy chatbot NFT in my wallet at /juicy-nft: "purpose betray marriage bla...	★	
	Incompetent customer support! Can't even upload photo of broken purchase!	★★	
	This is the store for awesome stuff of all kinds! (anonymous)	★★★★★	
	Never gonna buy anywhere else from now on! Thanks for the great service! (anonymous)	★★★★★	

The browser's developer tools are open, showing the Sources panel. The file "main.js" is selected, and the variable "path" is highlighted in the code editor. The console shows a message: "Line 1, Column 433077".