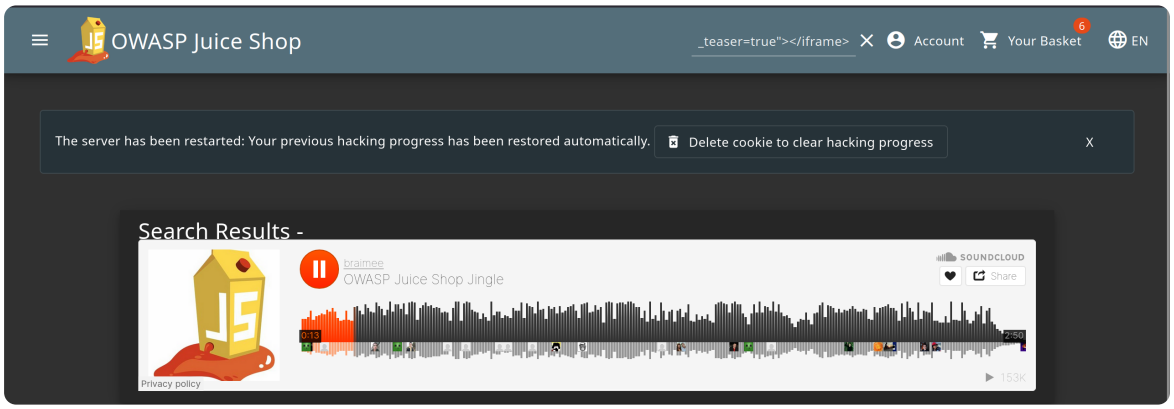
NASA Lab13

B11901164 陳秉緯

題目（除了 black list）

- Score Board (1 star):
  直接在網頁 URL 後面加上 score-board 搜尋即可找到 Score Board 頁面
- Bonus Payload (1 star):
  在 route = /search 頁面上方搜尋 `<iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe>` 則會出現



- Privacy Policy (1 star):
  點擊 Account > Privacy & Security > Privacy Policy
- Bully Chatbot (1 star):
  點擊 side menu 的 Support Chat，然後瘋狂發送 "Give me a coupon code"，最後他就會給我：Oooookay, if you promise to stop nagging me here's a 10% coupon code for you: o*l]qh7ZKp
- Error Handling (1 star):
  搜尋 `http://127.0.0.1:3000/rest`

OWASP Juice Shop (Express ^4.21.0)

500 **Error: Unexpected path: /rest**

```
at /juice-shop/build/routes/angular.js:42:18
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 Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:346:12)
at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /juice-shop/build/routes/verify.js:184:5
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 Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:346:12)
at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /juice-shop/build/routes/verify.js:111:5
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 Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:346:12)
at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)
at logger (/juice-shop/node_modules/morgan/index.js:144:5)
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
```

- Exposed Metrics (1 star):

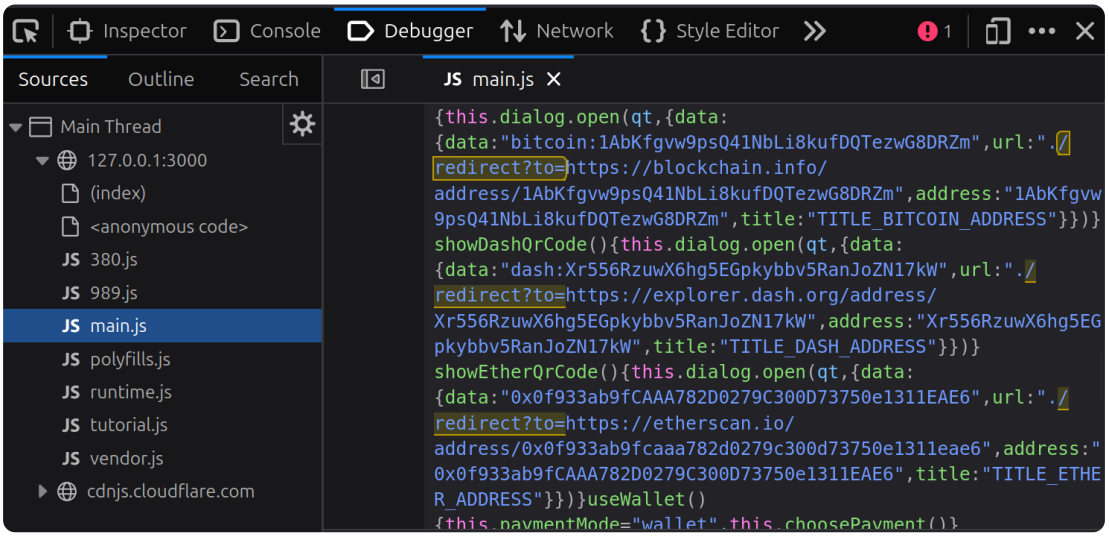
  去 `http://127.0.0.1:3000/metrics`

- Mass Dispel (1 star):

  在有很多通過的訊息的時候，按住 shift 並點其中一個訊息叉叉，則能一次關掉所有通過訊息

- Outdated Allowlist (1 star):

  1. 在登入後要買東西選擇 My Payment Options 的時候打開瀏覽器 dev tool > Debugger > main.js
  2. 搜尋 `/redirect?to=` 則可以找到

  3. 把第一個 `/redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm` 複製貼到 `http://127.0.0.1:3000/` 之後搜尋

- Web3 Sandbox (1 star):

  直接搜尋 `http://127.0.0.1:3000/#/web3-sandbox`

- Admin Section (2 stars):

  以 admin 帳號登入後 直接搜尋 `http://127.0.0.1:3000/#/administration`

- Empty User Registration (2 stars):
    1. 在 Brup Suite > Proxy 打開 Browser 並搜尋 `http://127.0.0.1:3000/#/register` 頁面
    2. 正常填寫 email 跟 password，隨便選一個 Security Question 也隨便填 Answer
    3. 在按下 Register 前，先在 Brup Suite 點擊 Intercept off 改成 on
    4. 點 Register 後，更改 request：把 email, password, repeat password 都清空
    5. 最後在 Brup Suite 點擊 Intercept on 改成 off，送出 request
- Forged Feedback (3 stars):
    1. 在 Brup Suite > Proxy 打開 Browser 並登入後搜尋 `http://127.0.0.1:3000/#/contact` 頁面
    2. 隨便寫 Comment 與調整 Rating，並填寫正確的 CAPTCHA 的 Result
    3. 在 Submit 之前，先在 Brup Suite 點擊 Intercept off 改成 on
    4. 點 Submit 後，更改 request：把 "UserId": 1, 改成 2
    5. 最後在 Brup Suite 點擊 Intercept on 改成 off，送出 request
- CAPTCHA Bypass (3 stars):
    1. 在瀏覽器登入帳號後同時打開 11 個 `http://127.0.0.1:3000/#/contact` 頁面
    2. 填寫完所有 Comment 與調整 Rating，並填寫正確的 CAPTCHA 的 Result
    3. 快速重複以下動作：固定滑鼠游標位置在 Submit 上，點擊 Submit，打 Ctrl + w 關閉已經點過 Submit 的頁面
- Forged Review (3 stars):
    1. 在 Brup Suite > Proxy 打開 Browser 並登入後點擊任意 product
    2. 填寫 Review，在 Submit 之前，先在 Brup Suite 點擊 Intercept off 改成 on
    3. 點 Submit 後，更改 request：把 "author": "admin@juice-sh.op" 改成在 `http://127.0.0.1:3000/#/administration` 看到 valid 的除了 admin@juice-sh.op 的 email
    4. 最後在 Brup Suite 點擊 Intercept on 改成 off，送出 request
- Forged Coupon (6 stars):

1. 登入之後在 `/basket` route 頁面點 Checkout
2. Select an address，點 Continue
3. 任意 Choose a delivery speed，點 Continue
4. 任意選擇一張卡
5. 在 Add a coupon 的下方有 BlueSky 的連結點進去
6. 複製做新一篇貼文內的 coupon code: o*l]qh7ZKp，貼到 Coupon，點 Continue
7. 點 Place your order and pay，然後就顯示解鎖這題
8. 但是我發現只有 10% off，並不是此題要求的 80% off，所以我覺得這題網站的判斷可能有 bug

- Multiple Likes (6 stars):
  1. 下載瀏覽器的 auto clicker 的 extension，並把 interval 改成 0.001 seconds
  2. 把游標放在任意 product 的尚未點過 like 的 review
  3. 啟動 extension 則解鎖此題

Total: 34 stars

截圖score-board