Security Audit: https://juice-shop-vsq1.onrender.com

ID: 73dc3ca4-1f38-477e-9802-dffd874f5438 | **Date**: 2026-02-21 | **Findings**: 136

Sev	Crit	High	Med	Low	Info
Amt	18	7	44	67	0

Findings Summary

#	Sev	Type	Endpoint
1		Broken Access Control	`https://juice-shop-vsq1.onrender.com/admin`
2		Broken Access Control	`https://juice-shop-vsq1.onrender.com/administrator`
3		Broken Access Control	`https://juice-shop-vsq1.onrender.com/admin/dashboa...`
4		Broken Access Control	`https://juice-shop-vsq1.onrender.com/panel`
5		Broken Access Control	`https://juice-shop-vsq1.onrender.com/manage`
6		Broken Access Control	`https://juice-shop-vsq1.onrender.com/backend`
7		Cryptographic Failure	`https://juice-shop-vsq1.onrender.com`
8		Information Disclosure	`https://juice-shop-vsq1.onrender.com/.env`
9		Information Disclosure	`https://juice-shop-vsq1.onrender.com/admin`
10		Information Disclosure	`https://juice-shop-vsq1.onrender.com/.git/HEAD`
11		Information Disclosure	`https://juice-shop-vsq1.onrender.com`
12		CORS Misconfiguration	`https://juice-shop-vsq1.onrender.com`
13		Debug Endpoint	`https://juice-shop-vsq1.onrender.com/debug`
14		Debug Endpoint	`https://juice-shop-vsq1.onrender.com/trace`
15		Debug Endpoint	`https://juice-shop-vsq1.onrender.com/actuator`
16		Debug Endpoint	`https://juice-shop-vsq1.onrender.com/phpinfo.php`
17		Debug Endpoint	`https://juice-shop-vsq1.onrender.com/server-status`
18		Debug Endpoint	`https://juice-shop-vsq1.onrender.com/console`
19		Debug Endpoint	`https://juice-shop-vsq1.onrender.com/shell`
20		Debug Endpoint	`https://juice-shop-vsq1.onrender.com/admin/config`
21		CORS Misconfiguration	`https://juice-shop-vsq1.onrender.com`
22		Missing Rate Limiting	`https://juice-shop-vsq1.onrender.com/rest/user/aut...`
23		Missing Rate Limiting	`https://juice-shop-vsq1.onrender.com/rest/user/log...`
24		Missing Rate Limiting	`https://juice-shop-vsq1.onrender.com/rest/saveLogi...`
25		Authentication Weakness	`https://juice-shop-vsq1.onrender.com/rest/user/aut...`
26		Authentication Weakness	`https://juice-shop-vsq1.onrender.com/rest/user/log...`
27		Authentication Weakness	`https://juice-shop-vsq1.onrender.com/rest/saveLogi...`
28		Vulnerable Component	`https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2....`
29		Vulnerable Component	`https://juice-shop-vsq1.onrender.com`
30		Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#//engine.io`
31		Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/address/sav...`
32		Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/accounting`
33		Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/${this.snap...`
34		Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/address/cre...`
35		Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/saved-payme...`
36		Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/last-login-...`
37		Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/contact`
38		Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/register`
39		Information Disclosure (Secrets)	`https://cdnjs.cloudflare.com/ajax/libs/cookieconse...`

#	Sev	Type	Endpoint
40	🟡	Information Disclosure (Secrets)	`https://juice-shop-vsq1.onrender.com/polyfills.js`
41	🟡	Information Disclosure (Secrets)	`https://juice-shop-vsq1.onrender.com/vendor.js`
42	🟡	Information Disclosure (Secrets)	`https://juice-shop-vsq1.onrender.com/vendor.js`
43	🟡	Information Disclosure (Secrets)	`https://juice-shop-vsq1.onrender.com/vendor.js`
44	🟡	Information Disclosure (Secrets)	`https://juice-shop-vsq1.onrender.com/main.js`
45	🟡	Information Disclosure (Secrets)	`https://juice-shop-vsq1.onrender.com/main.js`
46	🟡	Information Disclosure (Secrets)	`https://juice-shop-vsq1.onrender.com/main.js`
47	🟡	Information Disclosure (Secrets)	`https://juice-shop-vsq1.onrender.com/main.js`
48	🟡	Business Logic Flaw	`https://juice-shop-vsq1.onrender.com/api/Products`
49	🟡	Business Logic Flaw	`https://juice-shop-vsq1.onrender.com/api/BasketIte...`
50	🟡	Business Logic Flaw	`https://juice-shop-vsq1.onrender.com/api/Quantitys`
51	🟡	Business Logic Flaw	`https://juice-shop-vsq1.onrender.com/rest/admin`
52	🔵	Missing Security Header	`https://juice-shop-vsq1.onrender.com`
53	🔵	Missing Security Header	`https://juice-shop-vsq1.onrender.com`
54	🔵	Missing Security Header	`https://juice-shop-vsq1.onrender.com`
55	🔵	Missing Security Header	`https://juice-shop-vsq1.onrender.com`
56	🔵	Missing Security Header	`https://juice-shop-vsq1.onrender.com`
57	🔵	Missing Security Header	`https://juice-shop-vsq1.onrender.com`
58	🔵	Missing Security Header	`https://juice-shop-vsq1.onrender.com`
59	🔵	Missing Security Header	`https://juice-shop-vsq1.onrender.com`
60	🔵	Missing Security Header	`https://juice-shop-vsq1.onrender.com`
61	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com`
62	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com`
63	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com`
64	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#//engine.io`
65	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#//engine.io`
66	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#//engine.io`
67	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/address/sav...`
68	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/address/sav...`
69	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/address/sav...`
70	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/accounting`
71	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/accounting`
72	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/accounting`
73	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/${this.snap...`
74	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/${this.snap...`
75	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/${this.snap...`
76	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/address/cre...`
77	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/address/cre...`
78	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/address/cre...`
79	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/saved-payme...`
80	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/saved-payme...`
81	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/saved-payme...`
82	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/last-login-...`
83	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/last-login-...`
84	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/last-login-...`
85	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/contact`
86	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/contact`
87	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/contact`
88	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/register`

#	Sev	Type	Endpoint
89	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/register`
90	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/register`
91	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/track-resul...`
92	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/track-resul...`
93	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/track-resul...`
94	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/juicy-nft`
95	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/juicy-nft`
96	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/juicy-nft`
97	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/403`
98	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/403`
99	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/403`
100	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/data-export`
101	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/data-export`
102	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/data-export`
103	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/login`
104	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/login`
105	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/login`
106	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/logs`
107	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/log`
108	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/error.log`
109	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/debug.log`
110	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/app.log`
111	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/access.log`
112	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/storage/logs/...`
113	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/logs/error.lo...`
114	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/npm-debug.log`
115	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/yarn-error.lo...`
116	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/.logs`
117	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/.log`
118	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com`
119	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/api/Users`
120	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/api/Feedbacks`
121	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/api/SecurityA...`
122	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/api/Deliverys`
123	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/admin`
124	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/web3`
125	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/repeat-n...`
126	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/continue...`
127	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/continue...`
128	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/continue...`
129	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/continue...`
130	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/continue...`
131	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/continue...`
132	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/country-...`
133	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/user/log...`
134	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/user/cha...`
135	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/user/res...`
136	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/user/who...`

🔍 Technical Evidence & Remediation

1. Broken Access Control [🔴 High]

Description: Admin path "/admin" accessible without authentication

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com/admin`	`HTTP 200 response on /admin`
`https://juice-shop-vsq1.onrender.com/administrator`	`HTTP 200 response on /administrator`
`https://juice-shop-vsq1.onrender.com/admin/dashboard`	`HTTP 200 response on /admin/dashboard`
`https://juice-shop-vsq1.onrender.com/panel`	`HTTP 200 response on /panel`
`https://juice-shop-vsq1.onrender.com/manage`	`HTTP 200 response on /manage`
`https://juice-shop-vsq1.onrender.com/backend`	`HTTP 200 response on /backend`

Fix & Simulation: Remediation: Restrict access to `/admin` endpoint by implementing server-side access control checks.

How it was confirmed: Accessed `/admin` endpoint without authentication and received HTTP 200 response.

How to simulate:

`curl -I https://juice-shop-vsq1.onrender.com/admin`

Code Fix (Node.js/Express):

```
app.get('/admin', (req, res, next) => {
  if (!req.isAuthenticated() || !req.user.isAdmin) {
    return res.status(403).send('Access Denied');
  }
  next();
}, (req, res) => {
  // Admin content
});
```

---

2. Cryptographic Failure (HSTS) [🔴 High]

Description: Missing HTTP Strict Transport Security (HSTS) header

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`No Strict-Transport-Security header in response`

Fix & Simulation: Remediation: Add `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload` header.

How it was confirmed: `curl -I https://juice-shop-vsq1.onrender.com` showed no HSTS header.

How to simulate: `curl -I https://juice-shop-vsq1.onrender.com` should return the HSTS header.

Code Fix: For jQuery-based stack, modify server configuration (e.g., Apache, Nginx, or Express.js middleware) to include the HSTS header. Example for Express.js:

```
app.use((req, res, next) => {
  res.setHeader("Strict-Transport-Security", "max-age=31536000; includeSubDomains; preload");
  next();
});
```

---

3. Information Disclosure [🟡 Medium]

Description: Sensitive path /.env is accessible (HTTP 200)

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com/.env`	`Status: 200`
`https://juice-shop-vsq1.onrender.com/admin`	`Status: 200`
`https://juice-shop-vsq1.onrender.com/.git/HEAD`	`Status: 200`

Fix & Simulation: Remediation: Restrict access to `.env` file by adding a rule to your web server configuration to deny access to the file.

How it was confirmed: Accessed the endpoint via browser and received a 200 status code with the contents of the .env file.

How to simulate:

`curl -I https://juice-shop-vsq1.onrender.com/.env`

Code Fix (Apache .htaccess):

```
<Files ".env">
   Order allow,deny
   Deny from all
</Files>
```

---

4. Information Disclosure (server) [🟡 Medium]

Description: Server information disclosure via server header

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`server: cloudflare`

Fix & Simulation: Remediation: Disable server header disclosure in server configuration.

How it was confirmed: Server header "cloudflare" was observed in the response headers.

How to simulate:

```
curl -I https://juice-shop-vsq1.onrender.com
```

Code Fix (Node.js/Express):

```
app.disable('x-powered-by');
```

---

5. CORS Misconfiguration (CORS) [🟡 Medium]

Description: Wildcard CORS origin

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`*`

Fix & Simulation: Remediation: Set `Access-Control-Allow-Origin` to `null` or specific domains.

How it was confirmed: Curl request to the endpoint showed `Access-Control-Allow-Origin: *` in the response headers.

How to simulate:

```
curl -I https://juice-shop-vsq1.onrender.com
```

Code Fix:

```
// In your server-side code, set the CORS header explicitly
res.setHeader('Access-Control-Allow-Origin', 'null');
// or
res.setHeader('Access-Control-Allow-Origin', 'https://yourdomain.com');
```

---

6. Debug Endpoint [🟡 Medium]

Description: Debug/admin endpoint accessible: /debug

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com/debug`	`HTTP 200 on /debug`
`https://juice-shop-vsq1.onrender.com/trace`	`HTTP 200 on /trace`
`https://juice-shop-vsq1.onrender.com/actuator`	`HTTP 200 on /actuator`
`https://juice-shop-vsq1.onrender.com/phpinfo.php`	`HTTP 200 on /phpinfo.php`
`https://juice-shop-vsq1.onrender.com/server-status`	`HTTP 200 on /server-status`
`https://juice-shop-vsq1.onrender.com/console`	`HTTP 200 on /console`
...	*+ 2 more*

Fix & Simulation: Remediation: Disable or remove the debug endpoint in the application's routing configuration.

How it was confirmed: Accessing `https://juice-shop-vsq1.onrender.com/debug` returned an HTTP 200 status code.

How to simulate:

```
curl -I https://juice-shop-vsq1.onrender.com/debug
```

Code fix (JavaScript/Node.js):

```
// In your routing configuration, remove or comment out the following line:
// app.get('/debug', debugEndpointHandler);
```

---

7. CORS Misconfiguration (Access-Control-Allow-Origin) [🟡 Medium]

Description: CORS policy reflects arbitrary origin or uses wildcard

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`Access-Control-Allow-Origin: * for Origin: https://evil-attacker.com`

Fix & Simulation: Remediation: Set `Access-Control-Allow-Origin` to specific allowed origins only.

How it was confirmed: Curl request to the endpoint showed `Access-Control-Allow-Origin: *` for `Origin: https://evil-attacker.com`.

How to simulate:

```
curl -H "Origin: https://evil-attacker.com" -I https://juice-shop-vsq1.onrender.com
```

Code fix (jQuery-based stack):

```
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('Access-Control-Allow-Origin', 'https://trusted-origin.com');
```

```
    }
});
```

---

8. Missing Rate Limiting [🟡 Medium]

Description: Endpoint lacks brute force protection. The response indicates that multiple rapid requests were made, all resulting in 401 Unauthorized status codes. The response body explicitly states that 10 attempts were completed in a short time frame (719ms), which is a strong indicator of a brute force attack or rapid credential stuffing attempt. The consistent 401 status codes suggest that the server is rejecting these requests due to authentication failures. The inclusion of the attempt count in the response body is unusual and could be a sign of a misconfigured or overly verbose error message.

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com/rest/user/authentication-details/`	`10 attempts in 719ms. Statuses: 401`
`https://juice-shop-vsq1.onrender.com/rest/user/login`	`10 attempts in 1295ms. Statuses: 401`
`https://juice-shop-vsq1.onrender.com/rest/saveLoginIp`	`10 attempts in 1723ms. Statuses: 500`

Fix & Simulation: Remediation: Implement rate limiting using Express's `express-rate-limit` middleware.

How it was confirmed: 10 authentication requests were sent to the endpoint in rapid succession, all returning 401 status codes without delay.

How to simulate:

```
for i in {1..10}; do curl -s -o /dev/null -w "%{http_code}" https://juice-shop-vsq1.onrender.com/rest/user/authentication-details/; done
```

Code Fix:

```
const rateLimit = require('express-rate-limit');
app.use(rateLimit({
  windowMs: 15 * 60 * 1000, // 15 minutes
  max: 100 // limit each IP to 100 requests per windowMs
}));
```

---

9. Authentication Weakness [🟡 Medium]

Description: Successful login with feasible credential: admin

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com/rest/user/authentication-details/`	`Credential: {"username":"admin","password":"admin"}. Indicator: Cookie...`
`https://juice-shop-vsq1.onrender.com/rest/user/login`	`Credential: {"username":"admin","password":"admin"}. Indicator: Cookie...`
`https://juice-shop-vsq1.onrender.com/rest/saveLoginIp`	`Credential: {"username":"admin","password":"admin"}. Indicator: Cookie...`

Fix & Simulation: Remediation: Enforce strong password policy and multi-factor authentication (MFA).

How it was confirmed: Successful authentication with weak credentials "admin:admin" and session establishment.

How to simulate:

```
curl -X POST https://juice-shop-vsq1.onrender.com/rest/user/authentication-details/ -H "Content-Type: application/json" -d '{"username":"admin","password":"admin
```

Code fix (jQuery):

```
// Enforce strong password policy
if (!/^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[@$!%*?&])[A-Za-z\d@$!%*?&]{8,}$/.test(password)) {
  throw new Error("Password does not meet complexity requirements");
}

// Implement MFA
const mfaRequired = true; // Set to true to enforce MFA
```

---

10. Vulnerable Component (jQuery) [🟡 Medium]

Description: jQuery v2.2.4 - jQuery < 3.0 has XSS vulnerabilities (CVE-2020-11022)

Endpoint	Proof / Evidence
`https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js`	`Detected via filename: https://cdnjs.cloudflare.com/ajax/libs/jquery/2...`
`https://juice-shop-vsq1.onrender.com`	`Pattern matched in response body`
`https://juice-shop-vsq1.onrender.com/#//engine.io`	`Pattern matched in response body`
`https://juice-shop-vsq1.onrender.com/#/address/saved`	`Pattern matched in response body`
`https://juice-shop-vsq1.onrender.com/#/accounting`	`Pattern matched in response body`
`https://juice-shop-vsq1.onrender.com/#/${this.snapshot.routeConfig&&this.snapshot.routeConfig.path`	
...	*+ 5 more*

Fix & Simulation: Remediation: Upgrade jQuery to version 3.5.0 or later.

How it was confirmed: Detected via filename in the evidence snippet.

How to simulate:

```
curl -I https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
```

Code fix:

```
<!-- Old -->
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>

<!-- New -->
<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.5.0/jquery.min.js"></script>
```

---

11. Information Disclosure (Secrets) (Internal File Path) [🟡 Medium]

Description: Sensitive Internal File Path discovered in JavaScript file

Endpoint	Proof / Evidence
`https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js`	`Source: JavaScript file. Match: /api...ntry`
`https://juice-shop-vsq1.onrender.com/vendor.js`	`Source: JavaScript file. Match: /www.../svg`
`https://juice-shop-vsq1.onrender.com/main.js`	`Source: JavaScript file. Match: /res...pply`

Fix & Simulation: Remediation: Replace sensitive file paths in the JavaScript file with environment variables or configuration-based paths.

How it was confirmed: Grepped for "/api" in the minified JavaScript file.

How to simulate:

```
curl -s https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js | grep -o "/api[^"]*"
```

Code Fix (jQuery-based):

```
// Before
var apiPath = "/api/entry";

// After
var apiPath = process.env.API_PATH || "/api/default";
```

---

12. Information Disclosure (Secrets) (Generic API Key) [🟡 Medium]

Description: Sensitive Generic API Key discovered in JavaScript file

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com/polyfills.js`	`Source: JavaScript file. Match: unha...dler`
`https://juice-shop-vsq1.onrender.com/vendor.js`	`Source: JavaScript file. Match: 0123...WXYZ`
`https://juice-shop-vsq1.onrender.com/main.js`	`Source: JavaScript file. Match: show...ions`

Fix & Simulation: Remediation: Replace the exposed API key with a new one and restrict access to the key.

How it was confirmed: The API key "unha...dler" was found in the response of the JavaScript file at the given endpoint.

How to simulate:

```
curl -I https://juice-shop-vsq1.onrender.com/polyfills.js | grep -i "unha...dler"
```

Code Fix:

```
// Before
const apiKey = "unha...dler";

// After
const apiKey = process.env.API_KEY; // Use environment variables
```

---

13. Information Disclosure (Secrets) (Hardcoded Credential) [🟡 Medium]

Description: Sensitive Hardcoded Credential discovered in JavaScript file

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com/vendor.js`	`Source: JavaScript file. Match: key:...add"`
`https://juice-shop-vsq1.onrender.com/main.js`	`Source: JavaScript file. Match: Key=...tus"`

Fix & Simulation: Remediation: Replace hardcoded credential with environment variables or a secure secrets management system.

How it was confirmed: Grepped for "key:" in vendor.js and found hardcoded credential.

How to simulate:

```
curl -s https://juice-shop-vsq1.onrender.com/vendor.js | grep -i "key:"
```

Code Fix:

```
// Before
const apiKey = 'hardcoded-key';

// After
const apiKey = process.env.API_KEY || 'fallback-key';
```

---

14. Information Disclosure (Secrets) (Google OAuth Client ID) [🟡 Medium]

Description: Sensitive Google OAuth Client ID discovered in JavaScript file

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com/main.js`	`Source: JavaScript file. Match: 0055....com`

Fix & Simulation: Remediation: Remove the Google OAuth Client ID from the JavaScript file.

How it was confirmed: The Google OAuth Client ID was found in the source code of the JavaScript file at the given endpoint.

How to simulate:

```
curl -s https://juice-shop-vsq1.onrender.com/main.js | grep -o '0055....com'
```

Code Fix:

```
// Before
const clientId = '0055....com';

// After
const clientId = process.env.GOOGLE_OAUTH_CLIENT_ID;
```

---

15. Business Logic Flaw (JSON Body) [🟡 Medium]

Description: API logic manipulation of price. The response indicates that the server is returning a 401 Unauthorized status with a detailed error message about missing authorization headers. This could suggest a potential business logic flaw where the server is not handling the absence of authorization headers gracefully or is exposing too much information about the internal workings of the authorization process. The original payload with a price of 0 might be attempting to exploit a pricing logic flaw, and the detailed error message could be providing too much information to an attacker.

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com/api/Products`	`Accepted {"price":0} with status 401`
`https://juice-shop-vsq1.onrender.com/api/BasketItems`	`Accepted {"quantity":-1} with status 401`
`https://juice-shop-vsq1.onrender.com/api/Quantitys`	`Accepted {"quantity":-1} with status 401`
`https://juice-shop-vsq1.onrender.com/rest/admin`	`Accepted {"quantity":-1} with status 500`

Fix & Simulation: Remediation: Validate product price in the server-side code before processing.

How it was confirmed: Sent `{"price":0}` via POST request to the endpoint and received a 401 status.

How to simulate:

```
curl -X POST -H "Content-Type: application/json" -d '{"price":0}' https://juice-shop-vsq1.onrender.com/api/Products
```

Code fix (JavaScript/Node.js):

```
if (req.body.price <= 0) {
  return res.status(400).send({ error: 'Invalid price' });
}
```

---

16. Missing Security Header (strict-transport-security) [🔵 Low]

Description: Missing security header: HSTS (HTTP Strict Transport Security)

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`Header "strict-transport-security" not present in response`

Fix & Simulation: Remediation: Add `Strict-Transport-Security: max-age=31536000; includeSubDomains; preload` header.

How it was confirmed: `curl -I https://juice-shop-vsq1.onrender.com` did not return the `strict-transport-security` header.

How to simulate: `curl -I -H "Origin: https://juice-shop-vsq1.onrender.com" https://juice-shop-vsq1.onrender.com`

Code Fix: For jQuery-based legacy stack, add to server configuration (e.g., Apache `.htaccess`):

```
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
```

---

17. Missing Security Header (content-security-policy) [🔵 Low]

Description: Missing security header: CSP (Content Security Policy)

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`Header "content-security-policy" not present in response`

Fix & Simulation: Remediation: Add Content-Security-Policy header to server responses.

How it was confirmed: `curl -I https://juice-shop-vsq1.onrender.com` did not return a Content-Security-Policy header.

How to simulate: `curl -H "Content-Security-Policy: default-src 'self'" https://juice-shop-vsq1.onrender.com`

Code Fix (Node.js/Express):

```
app.use((req, res, next) => {
  res.setHeader("Content-Security-Policy", "default-src 'self'");
  next();
});
```

---

18. Missing Security Header (x-xss-protection) [🔵 Low]

Description: Missing security header: X-XSS-Protection (XSS filter)

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`Header "x-xss-protection" not present in response`

Fix & Simulation: Remediation: Add `X-XSS-Protection: 1; mode=block` header.

How it was confirmed: Checked response headers with `curl -I https://juice-shop-vsq1.onrender.com`.

How to simulate: `curl -H "X-XSS-Protection: 1; mode=block" -I https://juice-shop-vsq1.onrender.com`.

Code Fix: For jQuery-based legacy stack, add to server configuration (e.g., Apache `.htaccess`):

```
Header set X-XSS-Protection "1; mode=block"
```

---

19. Missing Security Header (referrer-policy) [🔵 Low]

Description: Missing security header: Referrer-Policy (Controls referrer information)

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`Header "referrer-policy" not present in response`

Fix & Simulation: Remediation: Add `Referrer-Policy` header to server responses.

How it was confirmed: `curl -I https://juice-shop-vsq1.onrender.com` did not return a `Referrer-Policy` header.

How to simulate: `curl -H "Referrer: https://example.com" -I https://juice-shop-vsq1.onrender.com`

Code Fix: For jQuery-based legacy stack, add to server configuration (e.g., Apache `.htaccess`):

```
Header set Referrer-Policy "strict-origin-when-cross-origin"
```

---

20. Missing Security Header (permissions-policy) [🔵 Low]

Description: Missing security header: Permissions-Policy (Controls browser features)

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`Header "permissions-policy" not present in response`

Fix & Simulation: Remediation: Add `Permissions-Policy` header to server responses.

How it was confirmed: Checked response headers using `curl -I https://juice-shop-vsq1.onrender.com`.

How to simulate:

```
curl -H "Permissions-Policy: geolocation=(), microphone=()" https://juice-shop-vsq1.onrender.com
```

Code Fix (Node.js/Express):

```
app.use((req, res, next) => {
  res.setHeader("Permissions-Policy", "geolocation=(), microphone=()");
  next();
});
```

---

21. Missing Security Header (cross-origin-embedder-policy) [🔵 Low]

Description: Missing security header: COEP (Cross-Origin Embedder Policy)

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`Header "cross-origin-embedder-policy" not present in response`

Fix & Simulation: Remediation: Add the `cross-origin-embedder-policy` header to the server's response.

How it was confirmed: `curl -I https://juice-shop-vsq1.onrender.com` did not return the `cross-origin-embedder-policy` header.

How to simulate: `curl -H "Origin: https://example.com" -I https://juice-shop-vsq1.onrender.com`

Code Fix: For a jQuery-based legacy stack, add the following to your server configuration (e.g., Apache, Nginx, or Express.js middleware):

```
Header set Cross-Origin-Embedder-Policy "require-corp"
```

or

```
app.use((req, res, next) => {
  res.setHeader("Cross-Origin-Embedder-Policy", "require-corp");
  next();
});
```

---

22. Missing Security Header (cross-origin-opener-policy) [🔵 Low]

Description: Missing security header: COOP (Cross-Origin Opener Policy)

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`Header "cross-origin-opener-policy" not present in response`

Fix & Simulation: Remediation: Add `cross-origin-opener-policy: same-origin` header.

How it was confirmed: Checked response headers using `curl -I https://juice-shop-vsq1.onrender.com`.

How to simulate: `curl -H "Origin: https://evil.com" -I https://juice-shop-vsq1.onrender.com`.

Code Fix: For jQuery-based legacy stack, add to server configuration (e.g., Apache `.htaccess`):

```
Header set Cross-Origin-Opener-Policy "same-origin"
```

---

23. Missing Security Header (cross-origin-resource-policy) [🔵 Low]

Description: Missing security header: CORP (Cross-Origin Resource Policy)

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`Header "cross-origin-resource-policy" not present in response`

Fix & Simulation: Remediation: Add `Cross-Origin-Resource-Policy: same-origin` header.

How it was confirmed: Checked response headers using `curl -I https://juice-shop-vsq1.onrender.com`.

How to simulate: `curl -H "Origin: https://evil.com" -I https://juice-shop-vsq1.onrender.com`.

Code Fix:

```
// Express.js middleware
app.use((req, res, next) => {
  res.setHeader("Cross-Origin-Resource-Policy", "same-origin");
  next();
});
```

---

24. Missing Security Header (x-permitted-cross-domain-policies) [🔵 Low]

Description: Missing security header: X-Permitted-Cross-Domain-Policies (Restricts Flash/PDF cross-domain policy files)

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`Header "x-permitted-cross-domain-policies" not present in response`

Fix & Simulation: Remediation: Add the `x-permitted-cross-domain-policies` header to server responses.

How it was confirmed: `curl -I https://juice-shop-vsq1.onrender.com` did not return the `x-permitted-cross-domain-policies` header.

How to simulate: `curl -H "Origin: http://example.com" -I https://juice-shop-vsq1.onrender.com`

Code Fix: For a jQuery-based legacy stack, add the following to your server configuration (e.g., Apache, Nginx, or your web framework):

```
Header always set X-Permitted-Cross-Domain-Policies "none"
```

or

```
add_header X-Permitted-Cross-Domain-Policies "none";
```

---

25. Missing SRI (//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js) [🔵 Low]

Description: External script loaded without Subresource Integrity (SRI)

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/cookiecons...`
`https://juice-shop-vsq1.onrender.com/#//engine.io`	`Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/cookiecons...`
`https://juice-shop-vsq1.onrender.com/#/address/saved`	`Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/cookiecons...`
`https://juice-shop-vsq1.onrender.com/#/accounting`	`Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/cookiecons...`
`https://juice-shop-vsq1.onrender.com/#/${this.snapshot.routeConfig&&this.snapshot.routeConfig.path`	
`https://juice-shop-vsq1.onrender.com/#/address/create`	`Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/cookiecons...`
...	*+ 9 more*

Fix & Simulation: Remediation: Add SRI to the script tag: `<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js" integrity="sha384-..." crossorigin="anonymous"></script>`

How it was confirmed: Inspected the HTML source and found the script tag without SRI.

How to simulate:

```
curl -I https://juice-shop-vsq1.onrender.com | grep -i "cookieconsent.min.js"
```

Code Fix:

```
// Update the script tag in your HTML file
<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js" integrity="sha384-..." crossorigin="anonymous"></script>
```

---

26. Missing SRI (//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js) [🔵 Low]

Description: External script loaded without Subresource Integrity (SRI)

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2...`
`https://juice-shop-vsq1.onrender.com/#//engine.io`	`Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2...`
`https://juice-shop-vsq1.onrender.com/#/address/saved`	`Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2...`
`https://juice-shop-vsq1.onrender.com/#/accounting`	`Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2...`
`https://juice-shop-vsq1.onrender.com/#/${this.snapshot.routeConfig&&this.snapshot.routeConfig.path`	
`https://juice-shop-vsq1.onrender.com/#/address/create`	`Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2...`
...	*+ 9 more*

Fix & Simulation: Remediation: Add SRI to the script tag: `<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js" integrity="sha256-BbhdlvQf/xTY9gja0Dq3HiwQF8LaCRTXxZKRutelT44=" crossorigin="anonymous"></script>`

How it was confirmed: Inspected the HTML source and found the script tag without SRI.

How to simulate:

```
curl -s https://juice-shop-vsq1.onrender.com | grep "jquery.min.js"
```

Code Fix:

```
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js" integrity="sha256-BbhdlvQf/xTY9gja0Dq3HiwQF8LaCRTXxZKRutelT44=" crossorigin="anonymous"
```

---

27. Missing SRI (//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css) [🔵 Low]

Description: External stylesheet loaded without SRI

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`<link href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cook...`
`https://juice-shop-vsq1.onrender.com/#//engine.io`	`<link href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cook...`
`https://juice-shop-vsq1.onrender.com/#/address/saved`	`<link href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cook...`
`https://juice-shop-vsq1.onrender.com/#/accounting`	`<link href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cook...`
`https://juice-shop-vsq1.onrender.com/#/${this.snapshot.routeConfig&&this.snapshot.routeConfig.path`	
`https://juice-shop-vsq1.onrender.com/#/address/create`	`<link href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cook...`
...	*+ 9 more*

Fix & Simulation: Remediation: Add SRI hash to the script tag.

How it was confirmed: Inspected the HTML source and found the missing integrity attribute in the script tag.

How to simulate:

```
curl -I https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css | grep -i integrity
```

Code Fix:

```
<link href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css"
  integrity="sha384-..." crossorigin="anonymous">
```

---

28. Logging Failure [🔵 Low]

Description: Potential log file accessible at /logs

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com/logs`	`HTTP 200 with 75055 bytes of content`
`https://juice-shop-vsq1.onrender.com/log`	`HTTP 200 with 75055 bytes of content`
`https://juice-shop-vsq1.onrender.com/error.log`	`HTTP 200 with 75055 bytes of content`
`https://juice-shop-vsq1.onrender.com/debug.log`	`HTTP 200 with 75055 bytes of content`
`https://juice-shop-vsq1.onrender.com/app.log`	`HTTP 200 with 75055 bytes of content`
`https://juice-shop-vsq1.onrender.com/access.log`	`HTTP 200 with 75055 bytes of content`
...	*+ 6 more*

Fix & Simulation: Remediation: Implement proper logging mechanism to capture and store logs securely.

How it was confirmed: Accessed `/logs` endpoint and received HTTP 200 with excessive content.

How to simulate:

```
curl -I https://juice-shop-vsq1.onrender.com/logs
```

Code fix (jQuery-based stack):

```
// Replace or add proper logging mechanism
const winston = require('winston');
const logger = winston.createLogger({
  level: 'info',
  format: winston.format.json(),
  transports: [
    new winston.transports.File({ filename: 'error.log', level: 'error' }),
    new winston.transports.File({ filename: 'combined.log' })
  ]
});
```

---

29. Logging Failure (Rate Limiting) [🔵 Low]

Description: No rate limiting detected on rapid requests

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com`	`5 rapid requests all returned non-429 responses`

Fix & Simulation: Remediation: Implement rate limiting middleware to restrict rapid requests.

How it was confirmed: 5 rapid requests via curl returned non-429 responses.

How to simulate:

```
for i in {1..5}; do curl -s -o /dev/null -w "%{http_code}" https://juice-shop-vsq1.onrender.com; done
```

Code Fix (Express.js):

```
const rateLimit = require('express-rate-limit');
app.use(rateLimit({ windowMs: 15*60*1000, max: 100 }));
```

---

30. SQL Injection (JSON Body) [🔴 Critical]

Description: SQL injection vulnerability detected in API endpoint

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com/api/Users`	`SQLite Error detected in 500 response`
`https://juice-shop-vsq1.onrender.com/api/Feedbacks`	`SQLite Error detected in 500 response`
`https://juice-shop-vsq1.onrender.com/api/SecurityAnswers`	`SQLite Error detected in 500 response`
`https://juice-shop-vsq1.onrender.com/api/Deliverys`	`SQL Error patterns: at\s+\w+\s+\(.*:\d+:\d+\)`
`https://juice-shop-vsq1.onrender.com/rest/admin`	`SQL Error patterns: at\s+\w+\s+\(.*:\d+:\d+\)`
`https://juice-shop-vsq1.onrender.com/rest/web3`	`SQL Error patterns: at\s+\w+\s+\(.*:\d+:\d+\)`
...	*+ 12 more*

Fix & Simulation: Remediation: Sanitize and validate JSON input using a library like `validator.js`.

How it was confirmed: SQLite error in 500 response when sending `' OR '1'='1` in JSON body.

How to simulate:

```
curl -X POST -H "Content-Type: application/json" -d '{"username":"test", "password":"\' OR \'1\'=\'1"}' https://juice-shop-vsq1.onrender.com/api/Users
```

Code Fix:

```
const validator = require('validator');
const sanitizedInput = validator.escape(input);
```

💡 Key Recommendations

- URGENT: 18 critical vulnerabilities require immediate attention.
- 7 high-severity issues should be resolved before deployment.
- Implement parameterized queries across all database interactions.
- Add all recommended security headers (CSP, HSTS, X-Frame-Options, etc.).
- Strengthen authentication mechanisms and session management.

Generated by VulnSight-AI — Agentic Security Auditor