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

ID: 9f321b89-166d-4dde-bdda-8ff388499ec1 | **Date**: 2026-02-21 | **Findings**: 137

Sev	🔴 Crit	🟠 High	🟡 Med	🔵 Low	🟣 Info
Amt	18	7	45	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/#/${S.snapsho...`
33	🟡	Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/accounting`
34	🟡	Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/delivery-me...`
35	🟡	Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/complain`
36	🟡	Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/photo-wall`
37	🟡	Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/privacy-pol...`
38	🟡	Vulnerable Component	`https://juice-shop-vsq1.onrender.com/#/contact`
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/api/Challenge...`
52	🟠	Business Logic Flaw	`https://juice-shop-vsq1.onrender.com/rest/admin`
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 Security Header	`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`
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/#//engine.io`
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/#/address/sav...`
71	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/${S.snapsho...`
72	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/${S.snapsho...`
73	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/${S.snapsho...`
74	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/accounting`
75	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/accounting`
76	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/accounting`
77	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/delivery-me...`
78	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/delivery-me...`
79	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/delivery-me...`
80	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/complain`
81	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/complain`
82	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/complain`
83	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/photo-wall`
84	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/photo-wall`
85	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/photo-wall`
86	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/privacy-pol...`
87	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/privacy-pol...`
88	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/privacy-pol...`

#	Sev	Type	Endpoint
89	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/contact`
90	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/contact`
91	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/contact`
92	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/order-summa...`
93	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/order-summa...`
94	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/order-summa...`
95	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/about`
96	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/about`
97	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/about`
98	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/address/cre...`
99	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/address/cre...`
100	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/address/cre...`
101	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/address/sel...`
102	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/address/sel...`
103	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/address/sel...`
104	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/${this.snap...`
105	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/${this.snap...`
106	🔵	Missing SRI	`https://juice-shop-vsq1.onrender.com/#/${this.snap...`
107	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/logs`
108	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/log`
109	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/error.log`
110	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/debug.log`
111	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/app.log`
112	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/access.log`
113	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/storage/logs/...`
114	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/logs/error.lo...`
115	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/npm-debug.log`
116	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/yarn-error.lo...`
117	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/.logs`
118	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com/.log`
119	🔵	Logging Failure	`https://juice-shop-vsq1.onrender.com`
120	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/api/Users`
121	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/api/Feedbacks`
122	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/api/SecurityA...`
123	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/api/Deliverys`
124	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/admin`
125	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/web3`
126	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/repeat-n...`
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/continue...`
133	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/country-...`
134	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/user/log...`
135	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/user/cha...`
136	🔴	SQL Injection	`https://juice-shop-vsq1.onrender.com/rest/user/res...`
137	🔴	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) => {
  if (!req.isAuthenticated() || !req.user.isAdmin) {
    return res.status(403).send('Access Denied');
  }
  // 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 `Strict-Transport-Security` header.

How to simulate: `curl -I -H "Host: 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"
```

---

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: Accessing the endpoint directly returned the contents of the `.env` file with a 200 status code.

How to simulate:

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

Code Fix (Apache .htaccess):

```
<FilesMatch "\.env$">
    Order allow,deny
    Deny from all
</FilesMatch>
```

---

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: Upgrade to a modern web framework and implement proper server headers.

How it was confirmed: Server headers revealed "cloudflare" indicating potential outdated server configuration.

How to simulate:

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

Code Fix (Node.js/Express):

```
app.disable('x-powered-by');
app.use((req, res, next) => {
  res.set('X-Content-Type-Options', 'nosniff');
  res.set('X-Frame-Options', 'DENY');
  res.set('X-XSS-Protection', '1; mode=block');
  next();
});
```

---

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 returned `Access-Control-Allow-Origin: *`.

How to simulate:

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

Code Fix:

```
// In your server-side code, set the CORS header explicitly
res.setHeader('Access-Control-Allow-Origin', 'https://trusted-domain.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: Remove or restrict access to the `/debug` endpoint.

How it was confirmed: `curl -I https://juice-shop-vsq1.onrender.com/debug` returned HTTP 200.

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

Code Fix:

```
// In your server-side code (e.g., Express.js):
app.use('/debug', (req, res, next) => {
  if (!req.ip.includes('your_trusted_ip')) {
    return res.status(403).send('Access forbidden');
  }
  next();
});
```

---

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: Restrict `Access-Control-Allow-Origin` to specific trusted domains.

How it was confirmed: `curl -I https://juice-shop-vsq1.onrender.com` showed `Access-Control-Allow-Origin: *`.

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

Code Fix:

```
// Replace:
res.setHeader('Access-Control-Allow-Origin', '*');

// With:
res.setHeader('Access-Control-Allow-Origin', 'https://trusted-domain.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 the number of attempts and the status codes, which is unusual and suggests that the server is tracking and potentially rate-limiting or blocking these requests. The consistent 401 status codes further suggest that the server is rejecting these requests due to authentication failures or rate limiting.

Endpoint	Proof / Evidence
`https://juice-shop-vsq1.onrender.com/rest/user/authentication-details/`	`10 attempts in 1029ms. Statuses: 401`
`https://juice-shop-vsq1.onrender.com/rest/user/login`	`10 attempts in 1530ms. Statuses: 401`
`https://juice-shop-vsq1.onrender.com/rest/saveLoginIp`	`10 attempts in 1112ms. Statuses: 500`

Fix & Simulation: Remediation: Implement rate limiting middleware in your jQuery-based stack to restrict authentication attempts.

How it was confirmed: 10 failed authentication attempts in under a second, all returning 401 status codes.

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:

```
// Add this middleware before your authentication routes
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 implement multi-factor authentication.

How it was confirmed: Successful authentication with weak credentials "admin:admin" observed.

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:

```
// Update password policy and add MFA
app.post('/rest/user/authentication-details', (req, res) => {
  if (!isStrongPassword(req.body.password) || !isMFAEnabled(req.user)) {
    return res.status(403).send('Weak password or MFA not enabled');
  }
  // ... rest of the code
});
```

---

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/#/${S.snapshot.routeConfig?.path	
`https://juice-shop-vsq1.onrender.com/#/accounting`	`Pattern matched in response body`
...	*+ 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 the exposed API path in the JavaScript file with a server-side generated path or use environment variables to store sensitive paths.

How it was confirmed: The exposed API path was found in the JavaScript file via a direct text search.

How to simulate:

```
curl -s https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js | grep -o '/api.*entry'
```

Code Fix (jQuery):

```
// Before
var apiPath = '/api/v1/entry';

// After
var apiPath = window.apiConfig.path || '/api/v1/entry';
```

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 (JavaScript):

```
// 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 credentials with environment variables or a secure secrets management system.

How it was confirmed: Inspected the JavaScript file at the given endpoint and found a hardcoded credential pattern.

How to simulate:

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

Code Fix (JavaScript):

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

// After
const apiKey = process.env.API_KEY || 'default-key-for-dev';
```

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 for a request that included a payload with a price of 0. This could suggest a business logic flaw where the server is not properly handling or validating the payload before checking for authorization. The detailed error message about the missing Authorization header is consistent with a 401 response, but the presence of a payload in the original request might indicate that the server is processing the request logic before checking for proper authorization, which could be a potential vulnerability.

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/api/Challenges/?key=nftMintChallenge`	`Accepted {"quantity":-1} with status 401`
`https://juice-shop-vsq1.onrender.com/rest/admin`	`Accepted {"quantity":-1} with status 500`

Fix & Simulation: Remediation: Validate and reject price updates with zero or negative values on the server-side.

How it was confirmed: Sent `{"price":0}` to the endpoint and received a 401 status code, indicating the server accepted the request.

How to simulate:

```
curl -X PUT https://juice-shop-vsq1.onrender.com/api/Products/1 -H "Content-Type: application/json" -d '{"price":0}'
```

Code Fix (jQuery/JavaScript):

```
if (price <= 0) {
  res.status(400).send({ error: "Price must be greater than zero" });
  return;
}
```

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 the following line to your server's configuration or relevant middleware to enable HSTS:

```
Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains; preload"
```

How it was confirmed: Checked response headers using `curl -I https://juice-shop-vsq1.onrender.com` and confirmed absence of `strict-transport-security`.

How to simulate:

```
curl -I https://juice-shop-vsq1.onrender.com | grep -i "strict-transport-security"
```

Code Fix (Express.js example):

```
const helmet = require('helmet');
app.use(helmet.hsts({ maxAge: 63072000, includeSubDomains: true, preload: true }));
```

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: `curl -I https://juice-shop-vsq1.onrender.com` showed no `X-XSS-Protection` header.

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

Code fix (Node.js/Express):

```
app.use((req, res, next) => {
  res.setHeader("X-XSS-Protection", "1; mode=block");
  next();
});
```

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 the `Referrer-Policy` header to the server's response.

How it was confirmed: Checked response headers using `curl -I https://juice-shop-vsq1.onrender.com` and confirmed the absence of `Referrer-Policy`.

How to simulate:

```
curl -I -H "Referer: https://example.com" https://juice-shop-vsq1.onrender.com
```

Code Fix (Node.js/Express):

```
app.use((req, res, next) => {
  res.setHeader('Referrer-Policy', 'strict-origin-when-cross-origin');
  next();
});
```

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 the `Permissions-Policy` header to the server's response.

How it was confirmed: `curl -I https://juice-shop-vsq1.onrender.com | grep -i "permissions-policy"`

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

Code Fix (Node.js/Express):

```
app.use((req, res, next) => {
  res.setHeader("Permissions-Policy", "geolocation=(), microphone=(), camera=()");
  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 `cross-origin-embedder-policy: require-corp` header.

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

How to simulate: `curl -I -H "Origin: https://example.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 Cross-Origin-Embedder-Policy "require-corp"
```

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 the `cross-origin-opener-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 -I -H "Origin: https://example.com" https://juice-shop-vsq1.onrender.com
```

Code Fix (Node.js/Express):

```
app.use((req, res, next) => {
  res.setHeader("Cross-Origin-Opener-Policy", "same-origin");
  next();
});
```

---

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 the `cross-origin-resource-policy` header to the server response.

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

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

Code Fix (Node.js/Express):

```
app.use((req, res, next) => {
  res.setHeader('Cross-Origin-Resource-Policy', 'same-site');
  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: Checked response headers using `curl -I https://juice-shop-vsq1.onrender.com` .

How to simulate: `curl -I https://juice-shop-vsq1.onrender.com | grep "x-permitted-cross-domain-policies"`

Code Fix (Node.js/Express):

```
app.use((req, res, next) => {
  res.setHeader('x-permitted-cross-domain-policies', 'none');
  next();
});
```

---

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/#/${S.snapshot.routeConfig?.path	
`https://juice-shop-vsq1.onrender.com/#/accounting`	`Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/cookiecons...`
`https://juice-shop-vsq1.onrender.com/#/delivery-method`	`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 (jQuery):

```
// Update the script tag in your HTML or JS file
var script = document.createElement('script');
script.src = "//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js";
script.integrity = "sha384-...";
script.crossOrigin = "anonymous";
document.head.appendChild(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/#/${S.snapshot.routeConfig?.path	
`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/#/delivery-method`	`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="sha384-KJ3o2DKtIkvYIK3UENzmM7KCkRr/rE9/Qpg6aAZGJwFDMVNA/GpGFF93hXpG5KkN" crossorigin="anonymous"></script>`

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

How to simulate:

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

Code Fix:

```
// Update the script tag in your HTML file
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js" integrity="sha384-KJ3o2DKtIkvYIK3UENzmM7KCkRr/rE9/Qpg6aAZGJwFDMVNA/GpGFF93hXpG5KkN" cros
```

---

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/#/${S.snapshot.routeConfig?.path	
`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/#/delivery-method`	`<link href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cook...`
...	*+ 9 more*

Fix & Simulation: How it was confirmed: Inspected the HTML source and found the `<link>` tag without the `integrity` attribute.

How to simulate:

```
curl -I https://juice-shop-vsq1.onrender.com | grep -o '<link href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css">'
```

Fix:

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

---

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: Disable log access to unauthorized users.

How it was confirmed: Accessed `/logs` endpoint without authentication, received HTTP 200 with log data.

How to simulate:

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

Code fix (jQuery/Node.js):

```
// Add authentication check in the route handler
app.get('/logs', (req, res) => {
  if (!req.isAuthenticated()) {
    return res.status(403).send('Forbidden');
  }
  // Rest of the log handling code
});
```

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, // 15 minutes
  max: 100 // limit each IP to 100 requests per windowMs
}));
```

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: 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:

```
// Use parameterized queries with jQuery.ajax
$.ajax({
  url: '/api/Users',
  type: 'POST',
  data: JSON.stringify({ username: username, password: password }),
  contentType: 'application/json',
  success: function(data) {
    // handle success
  },
  error: function(xhr, status, error) {
    // handle error
  }
});
```

💡 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