

Security Audit: <https://juice-shop-vsqa1.onrender.com>

ID: ae35210e-2fbd-4ae9-a589-5b45da7923e3 | Date: 2026-02-21 | Findings: 53

Sev	● Crit	● High	● Med	● Low	● Info
Amt	0	7	15	31	0

Findings Summary

#	Sev	Type	Endpoint
1	●	Broken Access Control	https://juice-shop-vsqa1.onrender.com/admin
2	●	Broken Access Control	https://juice-shop-vsqa1.onrender.com/administrator
3	●	Broken Access Control	https://juice-shop-vsqa1.onrender.com/admin/dashboa...
4	●	Broken Access Control	https://juice-shop-vsqa1.onrender.com/panel
5	●	Broken Access Control	https://juice-shop-vsqa1.onrender.com/manage
6	●	Broken Access Control	https://juice-shop-vsqa1.onrender.com/backend
7	●	Cryptographic Failure	https://juice-shop-vsqa1.onrender.com
8	●	Information Disclosure	https://juice-shop-vsqa1.onrender.com/.git/HEAD
9	●	Information Disclosure	https://juice-shop-vsqa1.onrender.com
10	●	CORS Misconfiguration	https://juice-shop-vsqa1.onrender.com
11	●	Debug Endpoint	https://juice-shop-vsqa1.onrender.com/debug
12	●	Debug Endpoint	https://juice-shop-vsqa1.onrender.com/trace
13	●	Debug Endpoint	https://juice-shop-vsqa1.onrender.com/actuator
14	●	Debug Endpoint	https://juice-shop-vsqa1.onrender.com/phpinfo.php
15	●	Debug Endpoint	https://juice-shop-vsqa1.onrender.com/server-status
16	●	Debug Endpoint	https://juice-shop-vsqa1.onrender.com/console
17	●	Debug Endpoint	https://juice-shop-vsqa1.onrender.com/shell
18	●	Debug Endpoint	https://juice-shop-vsqa1.onrender.com/admin/config
19	●	CORS Misconfiguration	https://juice-shop-vsqa1.onrender.com
20	●	Vulnerable Component	https://juice-shop-vsqa1.onrender.com/login
21	●	Vulnerable Component	https://juice-shop-vsqa1.onrender.com/.git/HEAD
22	●	Vulnerable Component	https://juice-shop-vsqa1.onrender.com/swagger.json
23	●	Missing Security Header	https://juice-shop-vsqa1.onrender.com
24	●	Missing Security Header	https://juice-shop-vsqa1.onrender.com
25	●	Missing Security Header	https://juice-shop-vsqa1.onrender.com
26	●	Missing Security Header	https://juice-shop-vsqa1.onrender.com
27	●	Missing Security Header	https://juice-shop-vsqa1.onrender.com
28	●	Missing Security Header	https://juice-shop-vsqa1.onrender.com
29	●	Missing Security Header	https://juice-shop-vsqa1.onrender.com
30	●	Missing Security Header	https://juice-shop-vsqa1.onrender.com
31	●	Missing Security Header	https://juice-shop-vsqa1.onrender.com
32	●	Missing SRI	https://juice-shop-vsqa1.onrender.com/login
33	●	Missing SRI	https://juice-shop-vsqa1.onrender.com/login
34	●	Missing SRI	https://juice-shop-vsqa1.onrender.com/login
35	●	Missing SRI	https://juice-shop-vsqa1.onrender.com/.git/HEAD
36	●	Missing SRI	https://juice-shop-vsqa1.onrender.com/.git/HEAD
37	●	Missing SRI	https://juice-shop-vsqa1.onrender.com/.git/HEAD
38	●	Missing SRI	https://juice-shop-vsqa1.onrender.com/swagger.json
39	●	Missing SRI	https://juice-shop-vsqa1.onrender.com/swagger.json

#	Sev	Type	Endpoint
40	●	Missing SRI	https://juice-shop-vsqa1.onrender.com/swagger.json
41	●	Logging Failure	https://juice-shop-vsqa1.onrender.com/logs
42	●	Logging Failure	https://juice-shop-vsqa1.onrender.com/log
43	●	Logging Failure	https://juice-shop-vsqa1.onrender.com/error.log
44	●	Logging Failure	https://juice-shop-vsqa1.onrender.com/debug.log
45	●	Logging Failure	https://juice-shop-vsqa1.onrender.com/app.log
46	●	Logging Failure	https://juice-shop-vsqa1.onrender.com/access.log
47	●	Logging Failure	https://juice-shop-vsqa1.onrender.com/storage/logs/...
48	●	Logging Failure	https://juice-shop-vsqa1.onrender.com/logs/error.lo...
49	●	Logging Failure	https://juice-shop-vsqa1.onrender.com/npm-debug.log
50	●	Logging Failure	https://juice-shop-vsqa1.onrender.com/yarn-error.lo...
51	●	Logging Failure	https://juice-shop-vsqa1.onrender.com/.logs
52	●	Logging Failure	https://juice-shop-vsqa1.onrender.com/.log
53	●	Logging Failure	https://juice-shop-vsqa1.onrender.com

Technical Evidence & Remediation

1. Broken Access Control [● High]

Description: Admin path "/admin" accessible without authentication

Endpoint	Proof / Evidence
https://juice-shop-vsqa1.onrender.com/admin	HTTP 200 response on /admin
https://juice-shop-vsqa1.onrender.com/administrator	HTTP 200 response on /administrator
https://juice-shop-vsqa1.onrender.com/admin/dashboard	HTTP 200 response on /admin/dashboard
https://juice-shop-vsqa1.onrender.com/panel	HTTP 200 response on /panel
https://juice-shop-vsqa1.onrender.com/manage	HTTP 200 response on /manage
https://juice-shop-vsqa1.onrender.com/backend	HTTP 200 response on /backend

Fix & Simulation: Remediation: Restrict access to /admin endpoint by implementing role-based access control (RBAC) checks.

How it was confirmed: Unauthorized access to /admin endpoint returned HTTP 200 response.

How to simulate:

```
curl -v https://juice-shop-vsqa1.onrender.com/admin
```

Code Fix (Node.js/Express):

```
// Add this middleware before your admin routes
app.use('/admin', (req, res, next) => {
  if (!req.user || req.user.role !== 'admin') {
    return res.status(403).send('Forbidden');
  }
  next();
});
```

2. Cryptographic Failure (HSTS) [● High]

Description: Missing HTTP Strict Transport Security (HSTS) header

Endpoint	Proof / Evidence
https://juice-shop-vsqa1.onrender.com	No Strict-Transport-Security header in response

Fix & Simulation: Remediation: Add HSTS header with Strict-Transport-Security: max-age=31536000; includeSubDomains; preload to server responses.

How it was confirmed: curl -I https://juice-shop-vsqa1.onrender.com showed no Strict-Transport-Security header.

How to simulate: curl -I https://juice-shop-vsqa1.onrender.com should return Strict-Transport-Security: max-age=31536000; includeSubDomains; preload.

Code Fix: For Node.js/Express:

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

3. Information Disclosure [● Medium]

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

Endpoint	Proof / Evidence
https://juice-shop-vsqli.onrender.com/.git/HEAD	Status: 200

Fix & Simulation: Remediation: Remove the exposed `.git` directory from the web root.

How it was confirmed: Accessed `.git/HEAD` and received a 200 status code.

How to simulate:

```
curl -I https://juice-shop-vsqli.onrender.com/.git/HEAD
```

Code Fix:

```
# For Apache, add to .htaccess:
RedirectMatch 404 /\.git|svn|hg)/
# For Nginx, add to config:
location ~ /\.git|svn|hg)/ { return 404; }
```

4. Information Disclosure (server) [🟡 Medium]

Description: Server information disclosure via server header

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

Fix & Simulation: Remediation: Implement server-side request forgery (SSRF) protection and disable server headers.

How it was confirmed: `curl -I https://juice-shop-vsqli.onrender.com` revealed "server: cloudflare" in response headers.

How to simulate: `curl -v https://juice-shop-vsqli.onrender.com --header "Host: evil.com"`

Code Fix (Node.js/Express):

```
app.disable('x-powered-by');
app.use((req, res, next) => {
  if (req.headers.host !== 'juice-shop-vsqli.onrender.com') {
    return res.status(400).send('Bad Request');
  }
  next();
});
```

5. CORS Misconfiguration (CORS) [🟡 Medium]

Description: Wildcard CORS origin

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

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

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

How to simulate:

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

Code Fix (Node.js/Express):

```
app.use((req, res, next) => {
  res.setHeader('Access-Control-Allow-Origin', 'https://yourdomain.com');
  next();
});
```

6. Debug Endpoint [🟡 Medium]

Description: Debug/admin endpoint accessible: `/debug`

Endpoint	Proof / Evidence
https://juice-shop-vsqli.onrender.com/debug	HTTP 200 on /debug
https://juice-shop-vsqli.onrender.com/trace	HTTP 200 on /trace
https://juice-shop-vsqli.onrender.com/actuator	HTTP 200 on /actuator
https://juice-shop-vsqli.onrender.com/phpinfo.php	HTTP 200 on /phpinfo.php
https://juice-shop-vsqli.onrender.com/server-status	HTTP 200 on /server-status
https://juice-shop-vsqli.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-vsqli.onrender.com/debug` returned HTTP 200.

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

Code fix (Node.js/Express):

```
// Remove or comment out the following line in your route definitions:
app.get('/debug', (req, res) => res.send('Debug info'));
// Or restrict access with middleware:
app.get('/debug', authenticateAdmin, (req, res) => res.send('Debug info'));
```

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

Description: CORS policy reflects arbitrary origin or uses wildcard

Endpoint	Proof / Evidence
https://juice-shop-vsqli.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-vsqli.onrender.com -H "Origin: https://evil-attacker.com" returned Access-Control-Allow-Origin: *.

How to simulate: curl -I https://juice-shop-vsqli.onrender.com -H "Origin: https://trusted-domain.com"

Code fix (Node.js/Express):

```
app.use((req, res, next) => {
  const allowedOrigins = ['https://trusted-domain1.com', 'https://trusted-domain2.com'];
  const origin = req.headers.origin;
  if (allowedOrigins.includes(origin)) {
    res.setHeader('Access-Control-Allow-Origin', origin);
  }
  next();
});
```

8. Vulnerable Component (jQuery) [🟡 Medium]

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

Endpoint	Proof / Evidence
https://juice-shop-vsqli.onrender.com/login	Pattern matched in response body
https://juice-shop-vsqli.onrender.com/.git/HEAD	Pattern matched in response body
https://juice-shop-vsqli.onrender.com/swagger.json	Pattern matched in response body

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

How it was confirmed: Pattern "jquery.min.js" with version < 3.5.0 found in response body.

How to simulate:

```
curl -I https://juice-shop-vsqli.onrender.com/login | grep -i "jquery"
```

Code fix (JavaScript):

```
<!-- Replace with -->
<script src="https://code.jquery.com/jquery-3.5.1.min.js"></script>
```

9. Missing Security Header (strict-transport-security) [🟢 Low]

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

Endpoint	Proof / Evidence
https://juice-shop-vsqli.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: Checked response headers using curl -I https://juice-shop-vsqli.onrender.com .

How to simulate: curl -I -H "Host: juice-shop-vsqli.onrender.com" https://juice-shop-vsqli.onrender.com .

Code Fix: For Node.js/Express:

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

10. Missing Security Header (content-security-policy) [🟢 Low]

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

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

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

How it was confirmed: curl -I https://juice-shop-vsqli.onrender.com | grep -i "content-security-policy"

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

Code Fix (Node.js/Express):

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

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

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

Endpoint	Proof / Evidence
https://juice-shop-vsqli.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-vsqli.onrender.com did not return x-xss-protection header.

How to simulate: curl -H "X-XSS-Protection: 0" https://juice-shop-vsqli.onrender.com

Code Fix: For Node.js/Express:

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

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

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

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

Fix & Simulation: Remediation: Add Referrer-Policy: strict-origin-when-cross-origin header.

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

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

Code Fix: For Node.js/Express:

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

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

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

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

Fix & Simulation: Remediation: Add the Permissions-Policy header to restrict browser features.

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

How to simulate:

curl -I https://juice-shop-vsqli.onrender.com | grep -i "permissions-policy"

Code Fix (Node.js/Express):

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

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

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

Endpoint	Proof / Evidence
https://juice-shop-vsqli.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 with curl -I https://juice-shop-vsqli.onrender.com .

How to simulate: curl -I -H "Cross-Origin-Embedder-Policy: require-corp" https://juice-shop-vsqli.onrender.com .

Code Fix: For Node.js/Express:

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

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

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

Endpoint	Proof / Evidence
https://juice-shop-vsqli.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-vsqli.onrender.com .

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

Code Fix (Node.js/Express):

```
app.use((req, res, next) => {
  res.setHeader("cross-origin-opener-policy", "same-origin");
  next();
});
```

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

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

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

Fix & Simulation: Remediation: Add Cross-Origin-Resource-Policy header to server responses.

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

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

Code Fix (Node.js/Express):

```
app.use((req, res, next) => {
  res.setHeader('Cross-Origin-Resource-Policy', 'same-site');
  next();
});
```

17. 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-vsqli.onrender.com	Header "x-permitted-cross-domain-policies" not present in response

Fix & Simulation: Remediation: Add the x-permitted-cross-domain-policies header to restrict cross-domain access.

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

How to simulate: curl -I https://juice-shop-vsqli.onrender.com

Code Fix: For Node.js/Express:

```
app.use((req, res, next) => {
  res.setHeader('X-Permitted-Cross-Domain-Policies', 'none');
  next();
});
```

18. 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-vsqli.onrender.com/login	Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/cookiecons...
https://juice-shop-vsqli.onrender.com/.git/HEAD	Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/cookiecons...
https://juice-shop-vsqli.onrender.com/swagger.json	Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/cookiecons...

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 source code of the endpoint and found the script tag without SRI.

How to simulate:

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

Code Fix (JS):

```
// Update the script tag in your HTML or JS file
const 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);
```

19. 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-vsqli.onrender.com/login	Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2...
https://juice-shop-vsqli.onrender.com/.git/HEAD	Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2...
https://juice-shop-vsqli.onrender.com/swagger.json	Insecure tag: <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2...

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-KJ3o2DKtIkVYIK3UENzmM7KcKr/rE9/Qpg6aAZGJwFDMVNA/GpGFF93hXpG5KkN" crossorigin="anonymous"></script>

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

How to simulate:

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

Code Fix:

```
// Before
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>

// After
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js" integrity="sha384-KJ3o2DKtIkVYIK3UENzmM7KcKr/rE9/Qpg6aAZGJwFDMVNA/GpGFF93hXpG5KkN" crossorigin="anonymous"></script>
```

20. 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-vsqli.onrender.com/login	<link href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cook...
https://juice-shop-vsqli.onrender.com/.git/HEAD	<link href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cook...
https://juice-shop-vsqli.onrender.com/swagger.json	<link href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cook...

Fix & Simulation: Remediation: Add SRI to the CSS file in the HTML.

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

How to simulate:

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

Code Fix:

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

21. Logging Failure [Low]

Description: Potential log file accessible at /logs

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

Fix & Simulation: Remediation: Implement proper logging configuration to ensure all relevant security events are logged.

How it was confirmed: Accessing the logs endpoint returned a large amount of data without any visible filtering or security event logging.

How to simulate:

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

Code Fix (Node.js/Express):

```
// Configure winston logger with security event filtering
const winston = require('winston');
const logger = winston.createLogger({
  level: 'info',
  format: winston.format.combine(
    winston.format.timestamp(),
    winston.format.json()
  ),
  transports: [
    new winston.transports.File({ filename: 'security.log', level: 'info' })
  ]
});
```

```
]
});
```

22. Logging Failure (Rate Limiting) [Low]

Description: No rate limiting detected on rapid requests

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

Fix & Simulation: Remediation: Implement rate limiting middleware to restrict requests to 5 per minute.

How it was confirmed: `curl -i -X GET https://juice-shop-vsqli.onrender.com -H "Host: juice-shop-vsqli.onrender.com" -H "Connection: keep-alive"` executed 5 times in rapid succession returned non-429 responses.

How to simulate: `for i in {1..6}; do curl -s -o /dev/null -w "%{http_code}" https://juice-shop-vsqli.onrender.com; done`

Code Fix (Express.js):

```
const rateLimit = require('express-rate-limit');
app.use(rateLimit({
  windowMs: 60 * 1000, // 1 minute
  max: 5 // limit each IP to 5 requests per windowMs
}));
```

Key Recommendations

- 7 high-severity issues should be resolved before deployment.
- Add all recommended security headers (CSP, HSTS, X-Frame-Options, etc.).

Generated by VulnSight-AI — Agentic Security Auditor