Auto Alpha Advisory

Web Application Deep Scan

Target: brokencrystals.com (public test application)
Date: 2026-07-02

Executive Summary

This Deep Scan of **brokencrystals.com (public test application)** identified **5 confirmed vulnerabilities** (reproduced with proof-of-concept), 3 evidence-backed findings, and 2 leads for manual review.

Tier	Count
Confirmed (with PoC)	5
Evidence-backed	3
Leads (manual review)	2

Confirmed Findings

1. Unauthenticated OS Command Injection (Remote Code Execution) [CRITICAL] [CONFIRMED]

CVSS: 9.8 / 10
URL: https://brokencrystals.com/api/spawn?command=id
Evidence: Response contained: uid=0(root) gid=0(root) groups=0(root) (reproduced; absent in benign-control baseline; echo-token negative control passed)
Proof of concept:

```
curl 'https://brokencrystals.com/api/spawn?command=id'
```

Remediation: Never pass user input to a shell. Remove the command endpoint or replace with a fixed allow-list of parameterised operations; run the service as a non-root user.
Framework references: MITRE ATT&CK: T1190 Exploit Public-Facing Application · NIST CSF: PR.PS-06 · OWASP: A03:2021 Injection · CWE-78 · D3FEND: D3-ITF

2. SQL Injection in authentication parameter [CRITICAL] [CONFIRMED]

CVSS: 9.1 / 10
URL: https://brokencrystals.com/api/auth/login
Evidence: Boolean-differential confirmed: true-condition and false-condition payloads produced distinct, reproducible responses; error-based signature present, absent in baseline.
Proof of concept:

```
curl -X POST 'https://brokencrystals.com/api/auth/login' -d "user=admin'--&password=x"
```

Remediation: Use parameterised queries / prepared statements for every database call. Never concatenate request input into SQL.
Framework references: MITRE ATT&CK: T1190 Exploit Public-Facing Application · NIST CSF: PR.PS-06 · OWASP: A03:2021 Injection · CWE-89 · D3FEND: D3-ITF

3. Server-Side Request Forgery (SSRF) [HIGH] [CONFIRMED]

CVSS: 8.6 / 10
URL: https://brokencrystals.com/api/file?path=

Evidence: Server fetched an operator-controlled URL and returned its response body (reproduced; benign-control baseline did not fetch).
Proof of concept:

```
curl 'https://brokencrystals.com/api/file?path=http://169.254.169.254/latest/meta-data/'
```

Remediation: Validate and allow-list outbound URLs; block internal/link-local ranges (169.254.0.0/16, 127.0.0.0/8, RFC-1918); disable unused URL schemes.
Framework references: MITRE ATT&CK: T1190 Exploit Public-Facing Application · NIST CSF: PR.PS-06 · OWASP: A10:2021 SSRF · CWE-918 · D3FEND: D3-ACH

4. Local File Inclusion / Arbitrary File Read [HIGH] [CONFIRMED]

CVSS: 7.5 / 10
URL: https://brokencrystals.com/api/file?path=../../../../etc/passwd
Evidence: Response contained /etc/passwd content: root:x:0:0:root:/root:/bin/bash (reproduced; non-existent-file negative control returned no signature).
Proof of concept:

```
curl 'https://brokencrystals.com/api/file?path=../../../../etc/passwd'
```

Remediation: Resolve and canonicalise the requested path, then confirm it stays within an allow-listed base directory; reject traversal sequences.
Framework references: MITRE ATT&CK: T1190 Exploit Public-Facing Application · NIST CSF: PR.PS-06 · OWASP: A01:2021 Broken Access Control · CWE-22 · D3FEND: D3-ITF

5. Reflected Cross-Site Scripting (XSS) [HIGH] [CONFIRMED]

CVSS: 6.1 / 10
URL: https://brokencrystals.com/?search=
Evidence: Injected payload reflected unencoded into the HTML response and executed (confirmed by the XSS engine; reproduced).
Proof of concept:

```
curl 'https://brokencrystals.com/?search=<script>alert(1)</script>'
```

Remediation: Context-encode all user input on output; set a strict Content-Security-Policy; prefer framework auto-escaping.
Framework references: MITRE ATT&CK: T1059.007 Command and Scripting Interpreter: JavaScript · NIST CSF: PR.PS-06 · OWASP: A03:2021 Injection · CWE-79 · D3FEND: D3-ITF

6. Missing / weak HTTP security headers [MEDIUM] [EVIDENCE-BACKED]

CVSS: 4.3 / 10
URL: https://brokencrystals.com/
Evidence: Response missing Content-Security-Policy, Strict-Transport-Security, and X-Content-Type-Options headers.
Remediation: Add CSP, HSTS (with a long max-age + preload once validated), X-Content-Type-Options: nosniff, and a Referrer-Policy.
Framework references: MITRE ATT&CK: T1190 Exploit Public-Facing Application · NIST CSF: PR.PS-01 · OWASP: A05:2021 Security Misconfiguration · CWE-693 · D3FEND: D3-ACH

7. Deprecated TLS protocol supported [MEDIUM] [EVIDENCE-BACKED]

CVSS: 5.9 / 10
URL: https://brokencrystals.com/
Evidence: Endpoint negotiated a deprecated TLS version (TLS 1.0/1.1) during the handshake probe.
Remediation: Disable TLS 1.0/1.1; require TLS 1.2+ (prefer 1.3) with modern cipher suites.
Framework references: MITRE ATT&CK: T1557 Adversary-in-the-Middle · NIST CSF: PR.DS-02 · OWASP: A02:2021 Cryptographic Failures · CWE-327 · D3FEND: D3-MENCR

8. Vulnerable client-side JavaScript library [MEDIUM] [EVIDENCE-BACKED]

CVSS: 6.1 / 10
URL: https://brokencrystals.com/
Evidence: Page loads jQuery 1.8.3, which has known published XSS vulnerabilities.
Remediation: Upgrade the library to a current, patched release; add it to a dependency-monitoring process.
Framework references: MITRE ATT&CK: T1190 Exploit Public-Facing Application · NIST CSF: PR.PS-02 · OWASP: A06:2021 Vulnerable & Outdated Components · CWE-1104

Appendix A — Leads for Manual Review

The following findings carry no automated proof and require manual verification. They are NOT confirmed vulnerabilities.

#	Title	Severity	URL
1	Sensitive path exposed (directory listing)	LOW	https://brokencrystals.com/.git/
2	Possible open redirect	LOW	https://brokencrystals.com/redirect?url=

Appendix B — Scope & Authorization

This report was generated by FatTool for authorized security testing only. All testing was conducted within the defined scope.

Scope & Limitations

What this Deep Scan covers (externally visible / black-box detectable surface):
• Confirmed injection vulnerabilities: SQL injection (SQLi) and Cross-Site Scripting (XSS), reproduced with proof-of-concept requests.
• In-band Server-Side Request Forgery (SSRF) — where the server fetches an attacker-controlled URL and the response is observable.
• Security-header and TLS posture: missing or weak HTTP response headers (CSP, HSTS, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, cookie flags) and deprecated TLS protocols or certificate issues.
• Vulnerable client-side libraries detected in page HTML and linked JavaScript bundles.
• Exposed files and secrets in client-accessible code (API keys, tokens, credentials in page source or JS bundles).
• Unauthenticated backend / Row-Level Security exposure: when the backend service is client-attested in scope, the scan confirms whether data is readable without authentication.

What this Deep Scan does not cover — these classes require source / repository access or authenticated multi-identity testing (a separate engagement):
• **Server-side hardcoded secrets:** credentials stored in environment variables, configuration files, or server memory are not visible to a black-box scanner.
• **Supply-chain / vulnerable-dependency analysis:** identifying outdated or malicious packages in the server-side dependency tree requires access to the project's package manifest and lock file (SAST/SCA mode).
• **Business-logic flaws:** flaws arising from incorrect application-specific rules (e.g. price manipulation, workflow bypass) cannot be detected without understanding the intended logic — they require source review or informed manual testing.
• **Authorisation / IDOR / BOLA testing:** confirming that one authenticated user cannot access another's resources requires two or more provisioned test identities. This scan is unauthenticated by default; multi-identity authorisation testing is available as a separate engagement.

Findings outside the above surface should be investigated via source-code review, software composition analysis, or an authenticated engagement. Auto Alpha Advisory is available to scope and conduct those assessments.