Confidential assessment report

Target: `https://example.com`
Prepared 2026-09-20 14:51 UTC

Executive summary

Assessment of http://localhost. Confirmed SQL injection lets an unauthenticated visitor influence backend queries (error-based on Cylinders and orderby; UNION extraction proven on Cylinders). That is a path to reading application data — not an assumption, a reproduced result. ELMAH error logs are reachable. Those pages often contain exception detail and, in some deployments, session cookies — treat this as a high-confidence exposure. Claims such as session theft are only stated where a cookie flag or ELMAH exposure makes that path plausible — they are not assumed from missing headers alone.

How the findings connect

• ELMAH exposure can turn application errors into an intelligence source — stack traces, request data, and sometimes authentication cookies.

Top attack paths

Attack path	Chain	Why it applies
Database compromise	SQLi → UNION extraction → sensitive records	Confirmed injection on catalog/sort parameters. UNION proved data can surface in the page.
Admin / session compromise	ELMAH exposure → leaked cookies/errors → account takeover	ELMAH is reachable. Error logs are a known source of exception detail and, in some setups, auth cookies.

Attack scenes

The catalog query that talks too much

It is late. An attacker opens https://x/CarsByCylinders the way a customer would, then changes one value — a cylinder count, a sort column — and adds a single quote. The page stops being a car listing and becomes a database confession: syntax error, table names, sometimes a UNION column of data sitting in the HTML. From there the attacker does not need malware. They walk the same URL the site already trusts and ask the database for accounts instead of supercars.

Critical

[CRITICAL / confirmed] SQL injection on /CarsByCylinders [Cylinders]
`Cylinders on CarsByCylinders`

• `https://x/CarsByCylinders`

Fix: Use parameterized queries.

[CRITICAL / firm] Exposed ELMAH error logs
`elmah.axd`

• `https://x/elmah`

Recon notes (not vulnerabilities)

[INFO / firm] [nuclei] DNS WAF Detection
`waf`

Residual risk

Authenticated / multi-role testing requires two auth headers. Blind SSRF requires the out-of-band listener.

Coverage

Scanners used: ffuf-builtin
Skipped: none