Proof of Concept Evidence
Web Application Security Flaws

Flaw Overview

Flaw Name	Cross-Site Scripting (XSS)
Severity	High
Affected URL	https://example.com/search?q=
Date Discovered	2024-06-04

Description

The affected parameter `q` in the search endpoint does not properly sanitize user input, allowing for reflected XSS attacks. Attackers can inject arbitrary JavaScript code into the application which is then executed in victim browsers.

Proof of Concept

The following payload was injected into the `q` parameter:

```
<script>alert('XSS')</script>
```

Visiting the URL below resulted in a JavaScript alert, proving successful exploitation:

```
https://example.com/search?q=%3Cscript%3Ealert('XSS')%3C/script%3E
```

Impact

Exploitation of this vulnerability could allow an attacker to execute arbitrary code in the context of a user's browser session, leading to potential data theft, session hijacking, or redirection to malicious sites.

Recommendation

- Sanitize and encode user input before rendering in HTML output.
- Use server-side frameworks that automatically escape user-supplied data.
- Implement Content Security Policy (CSP) headers.

Evidence Screenshot

(Insert screenshot here)