CVE Reporting Lenna.ai

Vulnerability Summary

1. **HTTP PARAMETER POLLUTION LEAD TO CROSS SITE SCRIPTING XSS LEAD TO STEALING COOKIE - MEDIUM**

Vulnerability Findings

1. **Finding 2: HTTP PARAMETER POLLUTION LEAD TO CROSS SITE SCRIPTING XSS– MEDIUM**

DESCRIPTION

I found a reflected cross-site scripting XSS vulnerability at the search feature in the v3.lenna.ai website. There is an input that allows users to search any information on the website, but it is vulnerable to html and JavaScript injection.

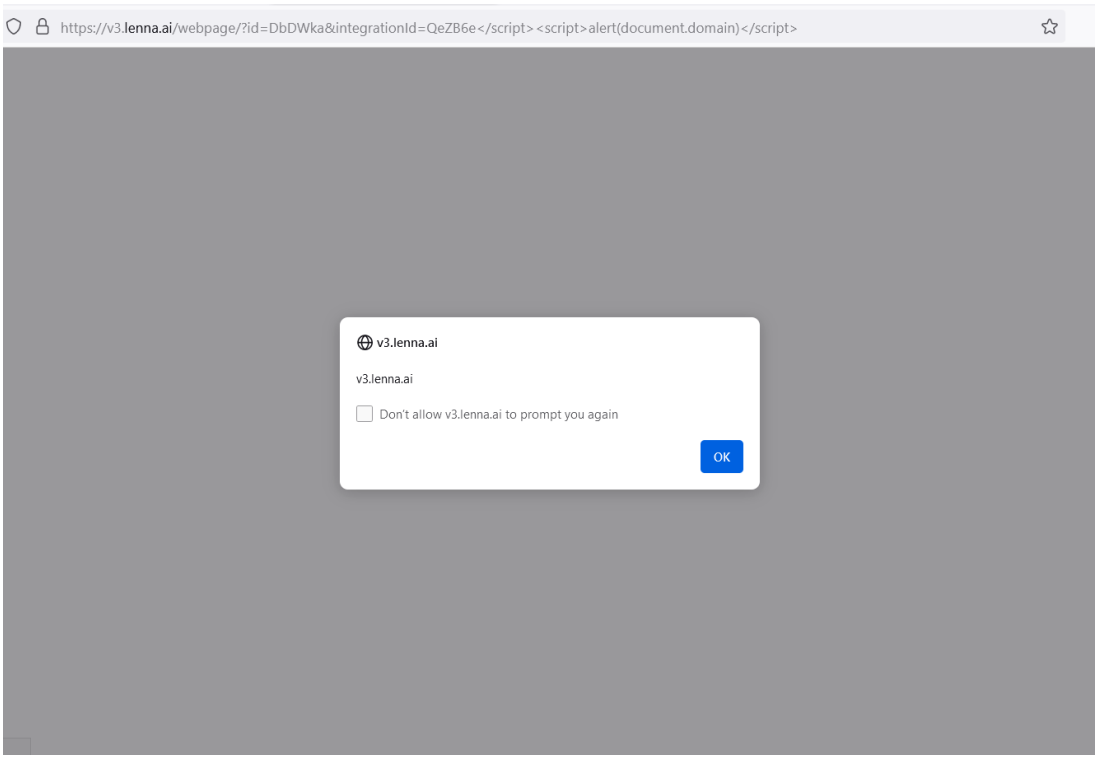
SCOPE

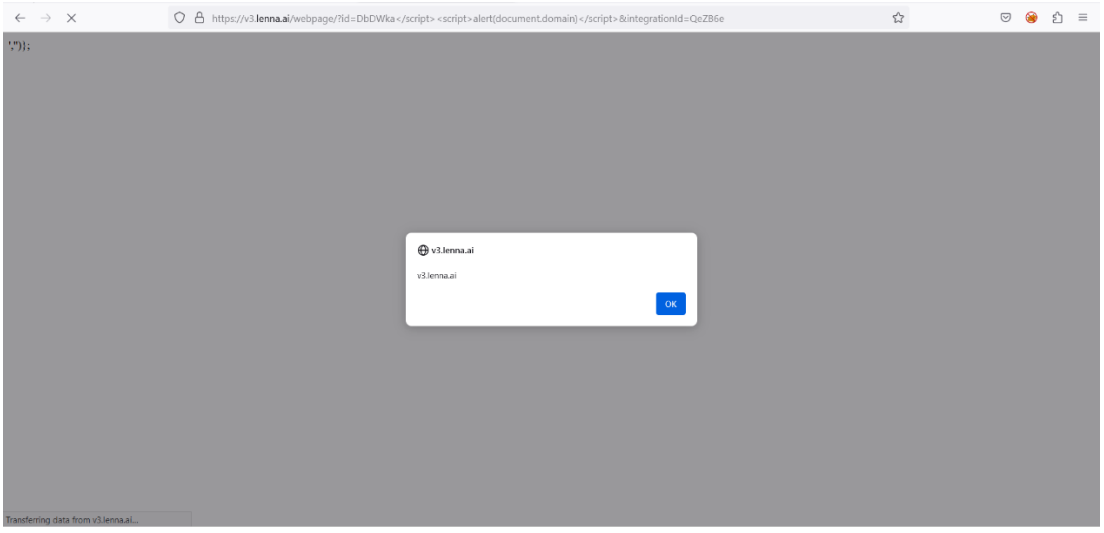
- https://v3.lenna.ai/webpage/?id=DbDWka&integrationId=QeZB6e

STEP TO REPRODUCE

1. Visit https://v3.lenna.ai/webpage/?id=DbDWka&integrationId=QeZB6e
2. Go to search parameter.
3. Input any XSS payload at the integrationId or Id, for example: </script><script>alert(document.location)</script>
4. And the alert will appear.

SCREENSHOTS





SECURITY RISK

Attackers could take advantage the XSS vulnerable to target the user apps with the malicious client-side script. Attackers possibly could steal the user session or even defacing the web apps.

RECOMMENDATION

Perform input validation on the above parameters from the backend side to not allow inputs containing the following characters: single quotes ('), double quotes ("), greater than (>), less than (<). Perform html encoding before displaying parameters on a web page. Additionally, use strip_tags() for sanitizing the client's side input.

REFERENCE

- https://owasp.org/Top10/A03_2021-Injection/
- https://security.snyk.io/vuln/SNYK-JAVA-STRUTS-472636
- https://owasp.org/www-community/attacks/xss/