Vulnerability Name	Reflected Cross-site Scripting
Affected Vendor, Version	OpenKM 6.3
Affected Endpoint	http://localhost:8080/OpenKM/frontend/index.jsp
Product Official Website URL	https://www.openkm.com/
Affected Component:	Affected parameter: Search

Description: - Reflected Cross-Site Scripting (XSS) is a web application vulnerability in which an attacker injects malicious script code into a request that is immediately returned by the server in the response and executed in the victim's browser. Unlike Stored XSS, the payload is not saved on the server. Instead, it is reflected through dynamic content such as search results, error messages, or URL parameters when user input is included in the response without proper validation or encoding.

Root Cause: - The root cause of Reflected XSS is insufficient input validation and lack of proper output encoding. The application trusts and reflects user-controlled input directly into the response page, allowing malicious scripts to execute in the browser.

Impact: - Reflected XSS can lead to the theft of sensitive information such as session tokens, login credentials, or personal data. It may also allow attackers to perform unauthorized actions on behalf of the victim user. Additionally, attackers can use Reflected XSS to deliver phishing content, distribute malware, or manipulate page content, which can result in reputational and security risks for the organization.

Mitigation: -Apply strict input validation to filter unexpected or dangerous characters and patterns. Sanitize all user input and implement proper context-aware output encoding before displaying user-controlled data in the browser. Enforce Content Security Policy (CSP) headers to restrict script execution and reduce the impact of injected payloads.

Remediation: -Developers should implement secure coding practices, including robust input validation, context-aware output encoding, and a properly configured Content Security Policy (CSP). Conduct regular security audits and penetration testing to identify XSS issues early. Deploying a Web Application Firewall (WAF) can also help detect and block malicious requests targeting XSS vulnerabilities.

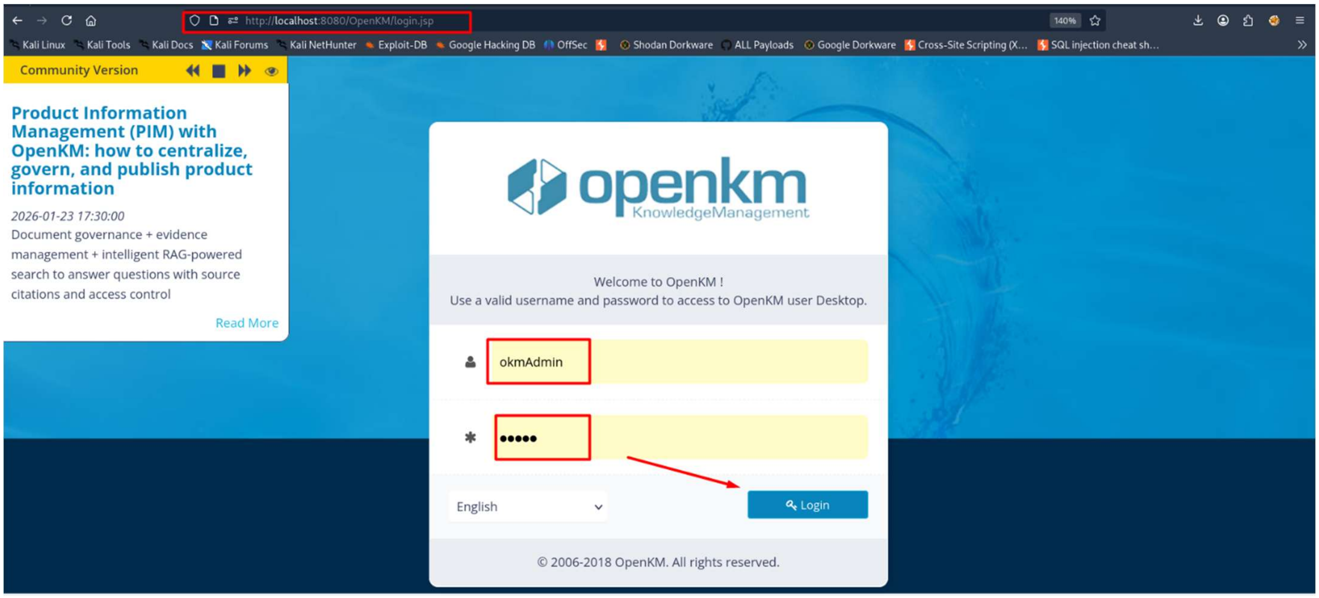
Severity Score

CVSS v3.1 Base Score: 6.1 (Medium)

Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Proof of Concept

Step 1: - First navigate to http://localhost:8080/OpenKM/login.jsp and login with username and Password.



http://localhost:8080/OpenKM/login.jsp

Community Version

Product Information Management (PIM) with OpenKM: how to centralize, govern, and publish product information

2026-01-23 17:30:00

Document governance + evidence management + intelligent RAG-powered search to answer questions with source citations and access control

Read More

Welcome to OpenKM !
Use a valid username and password to access to OpenKM user Desktop.

okmAdmin

•••••

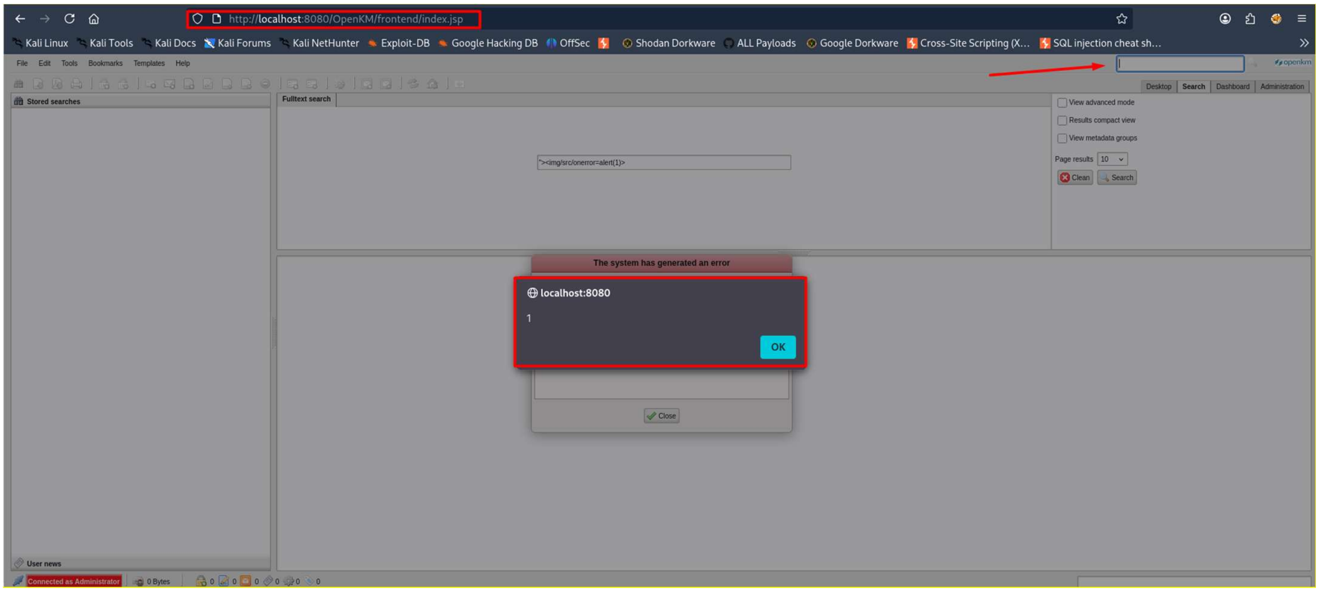
English

Login

© 2006-2018 OpenKM. All rights reserved.

Step 2: - The vulnerability can be reproduced by injecting a crafted payload into the search parameter, for example:

"><img/src/onerror=alert(1)>



http://localhost:8080/OpenKM/frontend/index.jsp

"><img/src/onerror=alert(1)>

The system has generated an error

localhost:8080

1

OK

Connected as Administrator

References

1. OWASP — Cross-Site Scripting (XSS)
   https://owasp.org/www-community/attacks/xss/
2. OWASP — XSS Prevention Cheat Sheet
   https://owasp.org/www-community/xss-prevention

Thankyou