Report - By Ly Ngoc Vu

First bug: moodle-auth-XSS

Vulnerability type: XSS

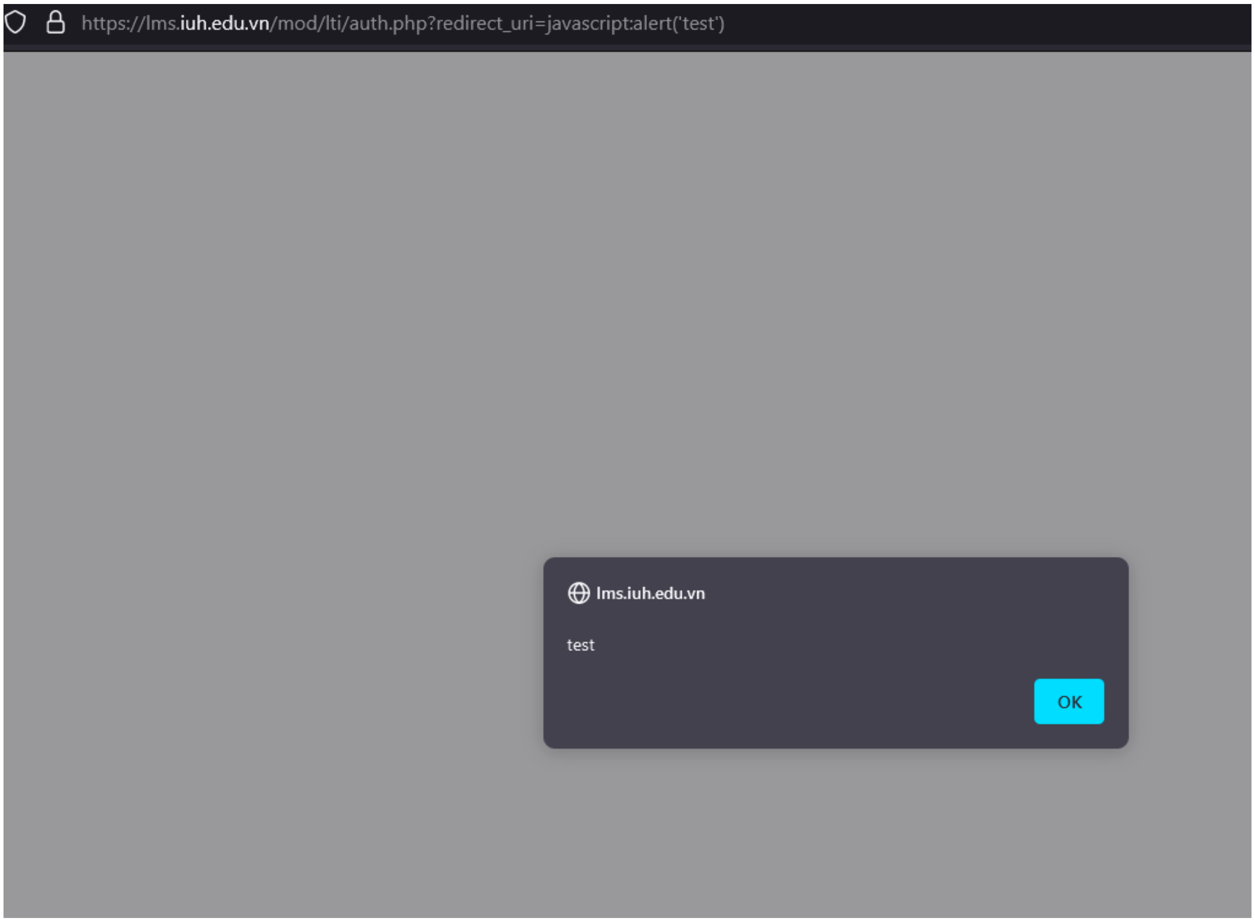
Domain: https://lms.iuh.edu.vn

How: Reflected XSS in "/mod/lti/auth.php" via `redirect_uri` parameter.

Description:

- What: Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise users' interactions with a vulnerable application. It allows an attacker to circumvent the same origin policy, designed to segregate different websites from each other. Cross-site scripting vulnerabilities typically allow an attacker to masquerade as a victim user, carry out any actions the user can perform, and access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain complete control over all of the application's functionality and data.
- Why: Cross-site scripting works by manipulating a vulnerable website so that it returns malicious JavaScript to users. When the malicious code executes inside a victim's browser, the attacker can fully compromise their interaction with the application.

Payload: https://lms.iuh.edu.vn/mod/lti/auth.php?redirect_uri=javascript:alert('test')



https://lms.iuh.edu.vn/mod/lti/auth.php?redirect_uri=javascript:alert('test')

lms.iuh.edu.vn

test

Second bug: git-file-leak

Vulnerability type: Git leaks

Domain: http://lms.faa.iuh.edu.vn

How: Git leaks in "/.git/HEAD" and "/.git/config".

Description:

- Can dump all source code of the website.

Third bug: WordPress-directory-listing

Vulnerability type: Sensitive file leaks

Domain: https://fme.iuh.edu.vn

ptchc.iuh.edu.vn

How: leaks directory in /wp-includes/ directory

Description: Can leak the structure of the website.

Fourth bug: JetBrains-idea-exposed

Vulnerability type: Sensitive file leaks

Domain:

http://doantn.iuh.edu.vn/.idea/workspace.xml

http://doantn.iuh.edu.vn/.idea/modules.xml

https://smia.iuh.edu.vn/.idea/modules.xml

How: Can leak the structure of the website.