Bug Report
Information Systems Security Analysis - CPSC 601.29

ATutor Multiple Cross-Site Scripting Vulnerabilities

Vulnerable Systems
ATutor Learning Management Tools 2.0.2

Summary
ATutor is a web-based application for developing online courses. The application is affected by multiple cross-site scripting vulnerabilities.

Successful exploits may allow attackers to execute scripts in a victim's browser in the context of the affected application; access or modify data in the underlying database; or carry other attacks.

Technical Description
ATutor is a web-based Learning Management System (LMS) application written in PHP, and is used to develop and deliver online courses.

The vulnerabilities exist due to the lack of input validation in the affected scripts when using (PHP_SELF, REQUEST_URI, SCRIPT_URL [or URI]) before returning to user.

[Details Omitted]

Attack Scenario
Cross Site Scripting

1. An attacker locates a site running the affected application.
2. The attacker crafts a URI that includes malicious script code (usually Javascript) designed to leverage the issue.
3. The attacker entices unsuspecting users to follow the link. This may be done by email, hosting on a webpage, IM or other means.
4. When the attacker follows the link, the malicious code is executed in the victim's browser in the context of the affected application.

A successful exploit may allow an attacker to steal cookie-based authentication credentials or launch other attacks

Exploitability
The following Proof-of-concepts have been tested:

[Details Omitted]

Mitigating Strategies

Restrict access to affected applications at network boundaries if external access is not required.

Remove affected files if not required by the application.

Deploy web filtering technologies or IPS to detect script injection and monitor network traffic for malicious activity.

Solution

No fixes are currently available to address these issues.

Credit

These vulnerabilities were discovered by Patrick Jungles.

References

Learning Management Tools
http://atutor.ca/