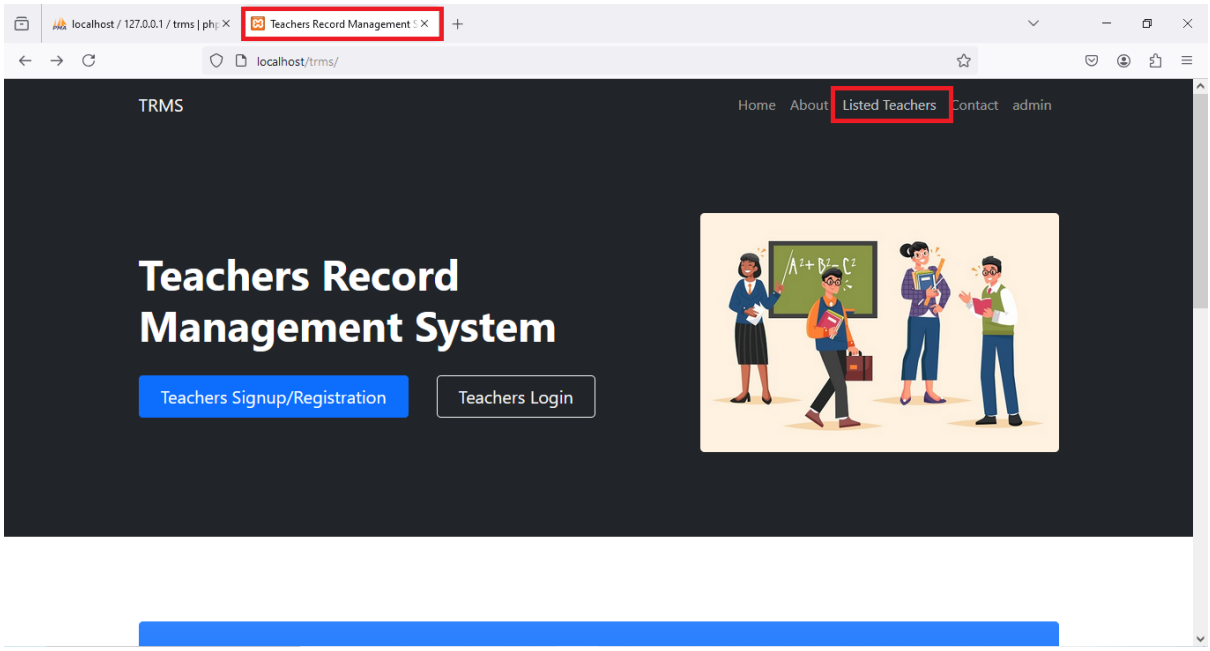
Reflected Cross Site Scripting (XSS) vulnerability was found in "/trms/listed-teachers.php" in Teachers Record Management System v2.1 allows remote attackers to execute arbitrary code via "searchinput" POST request parameter.

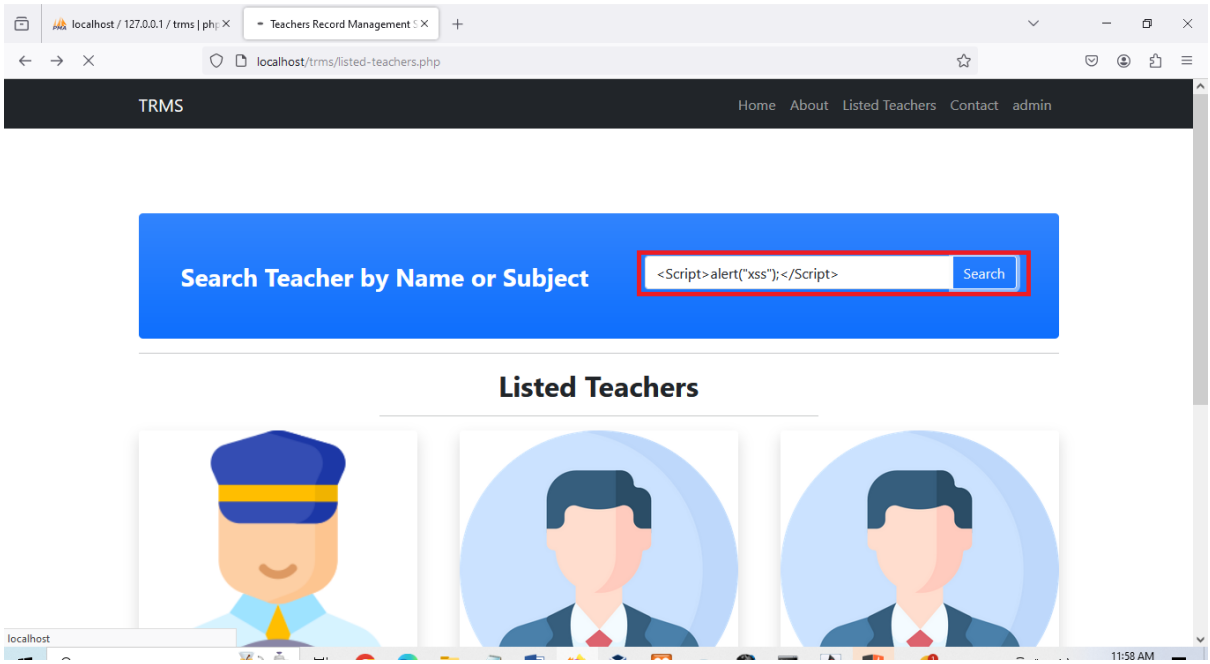
Field	Details
Affected Vendor	PHPGurukul
Affected Product Name	Teachers Record Management System
Product Official Website URL	https://phpgurukul.com/teachers-record-management-system-using-php-and-mysql/
Affected Components	- Version: V 2.1 - Affected Code File: /trms/listed-teachers.php - Affected Parameter: searchinput - Method: POST

Steps to Reproduce:

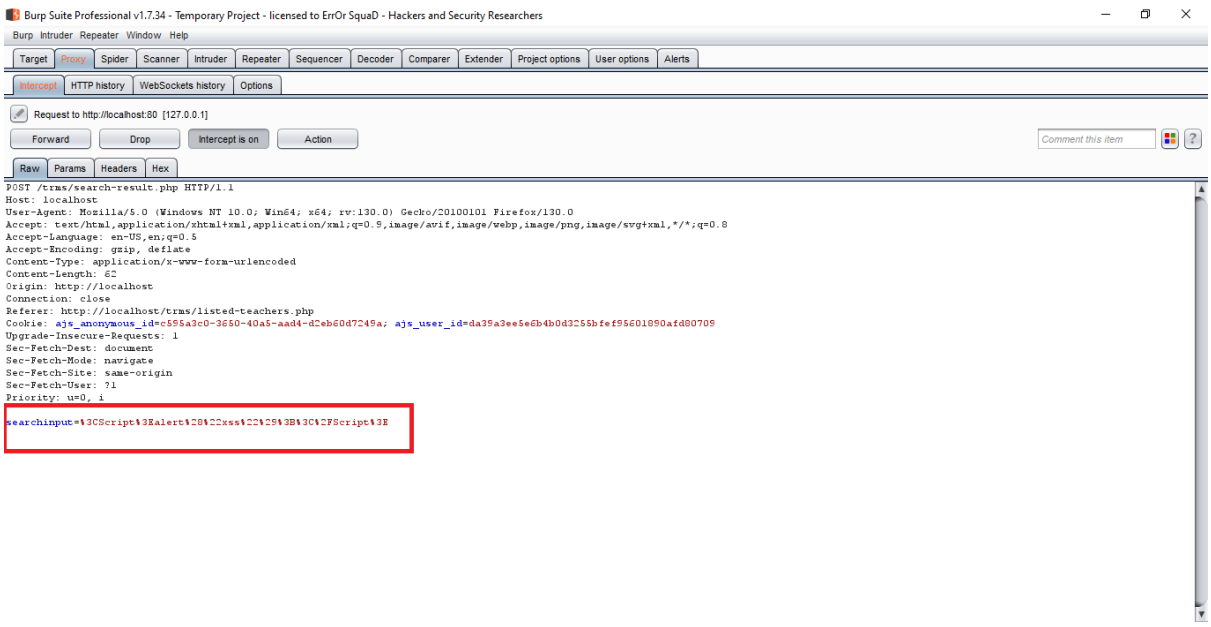
Step 1: Click on Check Listed Teachers



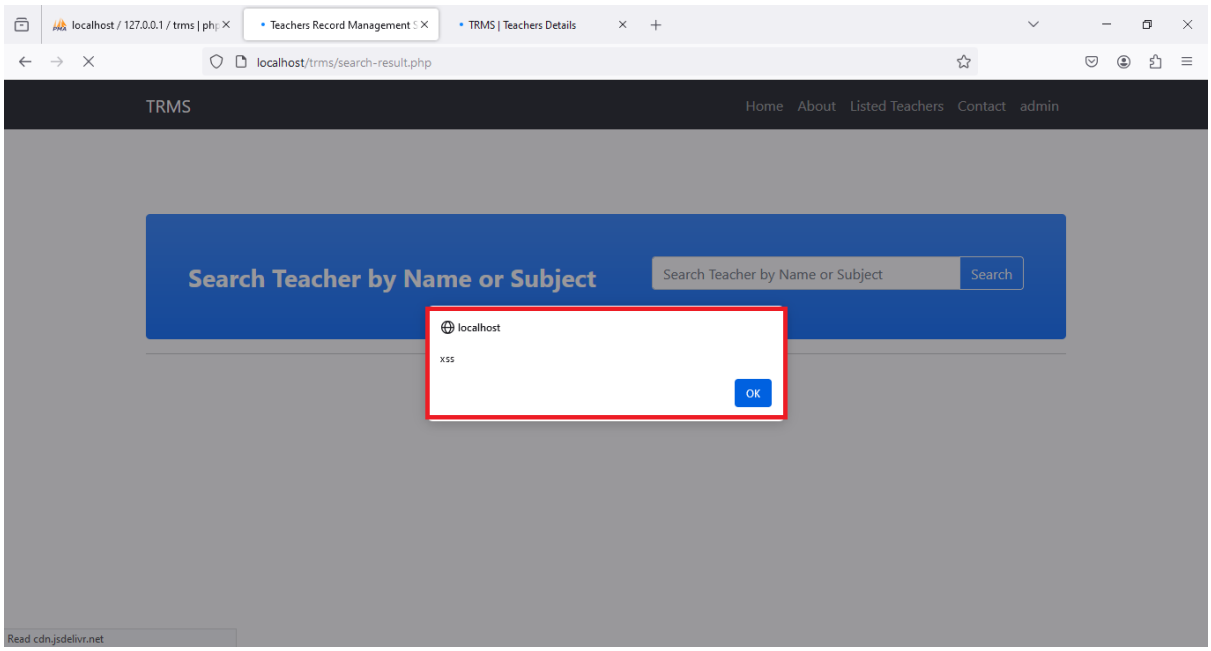
Step 2: In search bar, provide values `<Script>alert("xss");</Script>` and enable burpsuite to confirm the parameter.



Step 3: Observe that the payload is the `searchinput` parameter. Now proceed to forward the request.



Step 4: After forwarding the request, observe in the browser that the payload is executed, resulting in a popup.



Mitigation/recommendations

- https://portswigger.net/web-security/cross-site-scripting
- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html