Stored Cross-site scripting (XSS) in was found in “/DMS/dms/admin/ search-directory.php” in PHPGurukul Directory Management System Project in PHP v2.0 allows remote attackers to execute arbitrary code via “searchdata” POST request parameter.

* Official Website URL

<https://phpgurukul.com/directory-management-system-using-php-and-mysql/>

* Affected Product Name:Directory Management System Using PHP and MySQL

|  |  |
| --- | --- |
| Affected Vendor | Phpgurukul |
| Affected Code File | search-directory.php |
| Affected Parameter | searchdata |
| Method | POST |
| Type | Stored Cross-site scripting (XSS) |
| Version | V 2.0 |

**Steps to Reproduce:**

1. **Log in to the Admin Panel:**

* Open the admin login page.
* Enter your credentials and sign

A screenshot of a computer

AI-generated content may be incorrect.

1. **Go to DMS Admin Dashboard section:**

* Navigate to the “Search Directory” section.
* Click the input field to Search the Record.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Intercept the Request:**

* Open Burp Suite and set your browser to use its proxy (127.0.0.1:8080).
* Go to the **Proxy** tab and turn on **the Interceptor**.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Modify the Request:**

* Capture the request when updating directory details.
* Send it to the Burp Suite Repeater.
* Modify the, **searchdata** parameter by injecting this payload:

(<script>alert(1)</script>)

A screenshot of a computer

AI-generated content may be incorrect.

1. **Send and Observe:**

The injected xss is rendered here.

A screenshot of a computer

AI-generated content may be incorrect.

**Recommended Mitigations:**

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