SQl Injection in was found in “/DMS/dms/admin/edit-directory.php” in PHPGurukul Directory Management System Project in PHP v2.0 allows remote attackers to execute arbitrary code via “email” 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 | edit-directory.php |
| Affected Parameter | email |
| Method | POST |
| Type | Time-based blind |
| 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 “Directory by Status” section.
* Click the “Private” section.
* Click the Edit button to modify the Record.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Move to the Add Directory Section**

* Locate the input field on the edit-directory page, find the Directory by Status section.

Inject SQL payload in one of the editable fields (such as email), enter the following HTML payload: '%2b(select\*from(select(sleep(20)))a)%2b'

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.

A screenshot of a computer program

AI-generated content may be incorrect.

1. **Send the Modified Request:**

* Forward the modified request in the Burp Suite Repeater.
* Observe the delay in the response time.
* The server will delay its response by 20 seconds, confirming the successful execution of the SLEEP () function, indicating a time-based SQL injection vulnerability.

A screenshot of a computer

AI-generated content may be incorrect.

**Impact:**

* Data Theft: Hackers can steal sensitive user or system data.
* Data Tampering: Attackers may change or delete data, affecting their integrity.
* Reconnaissance: Hackers can explore the database structure to find more vulnerabilities.

**Mitigation:**

* Use proper input validation and output encoding.
* Set a strong Content Security Policy (CSP) to block malicious scripts.

**Reafference**

[SQL Injection Prevention - OWASP Cheat Sheet Series](https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)