Reflected Cross-Site Scripting (XSS) vulnerability was found in “Time-Table-Generator-System/ttg/admin/profile.php” in PHPGurukul Timetable Generator System panel Project in PHP v1.0 allows remote attackers to execute arbitrary code via “adminname” POST request parameter.

* Official Website URL

[https://phpgurukul.com/time-table-generator-system-using-php-and-mysql/](https://phpgurukul.com/time-table-generator-system-using-php-and-mysql/%20)

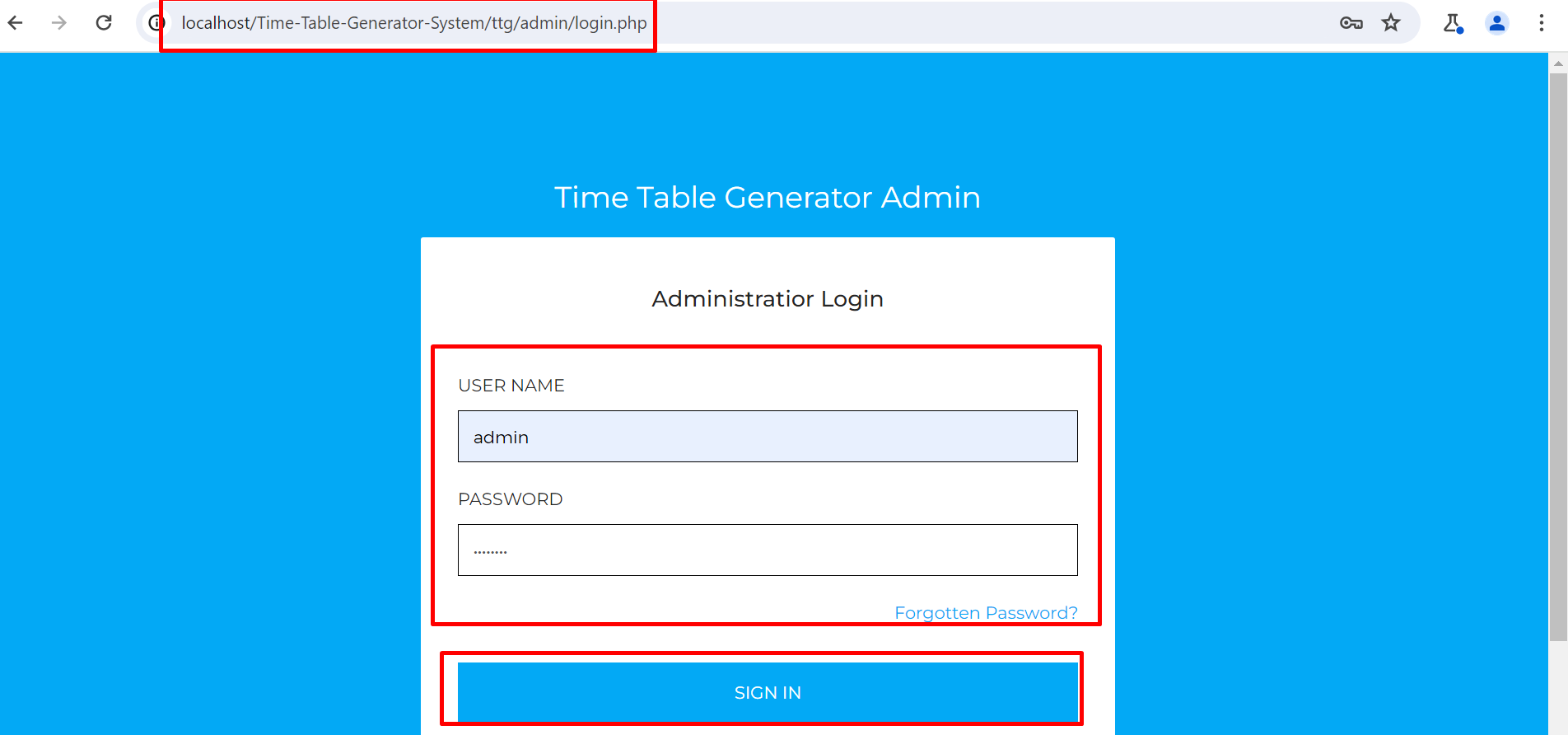
* Affected Product Name:Timetable Generator System using PHP and MySQL

|  |  |
| --- | --- |
| Affected Vendor | Phpgurukul |
| Affected Code File | edit-profile.php |
| Affected Parameter | adminname |
| Method | POST |
| Type | Cross-Site Scripting (XSS) |
| Version | V 1.0 |

**Steps to Reproduce:**

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

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



1. **Go to Manage profile:**

* Navigate to the “superadmin” section.
* Click the “Profile” button.

A screenshot of a computer

AI-generated content may be incorrect.

* Make any changes if needed.
* Click “Update”.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Intercept the Request:**

* Launch Burp Suite and configure your browser to route traffic through it.
* Enable Burp Suite Interceptor to capture requests.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Modify the Request:**

* Capture the request when updating user details.
* Send it to the Burp Suite Repeater.
* Modify the adminname 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 on this page

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>