XSS Injection in was found in “Park-Ticketing-Management-System-Project/ptms/ normal-bwdates-reports-details.php” in PHPGurukul Park Ticketing Management System Project in PHP v2.0 allows remote attackers to execute arbitrary code via “fromdate and todate” POST request parameter.

* Official Website URL

https://phpgurukul.com/park-ticketing-management-system-using-php-and-mysql/

* Affected Product Name:Park Ticketing Management System Using PHP and MySQL

|  |  |
| --- | --- |
| Affected Vendor | Phpgurukul |
| Affected Code File | normal-bwdates-reports-details.php |
| Affected Parameter | fromdate and today |
| Method | POST |
| Type | XSS Injection |
| 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 PTMS Admin section:**

* Navigate to the “Report” section.
* Click the “Normal People Report” section.
* Choose any fromdate to todate input field.

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, **fromdate and todate** parameter by injecting this payload:

(<script>alert(1)</script>)and (<script>alert(2)</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.

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>