HTML Injection in was found in “Park-Ticketing-Management-System-Project/ptms/edit-ticket.php” in PHPGurukul Timetable Generator System Project in PHP v2.0 allows remote attackers to execute arbitrary code via “tickettype and tprice” 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 | edit-ticket.php |
| Affected Parameter | tickettype and tprice |
| Method | POST |
| Type | HTML 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 Admin Dashboard section:**

* Navigate to the “Manage Type Ticket” section.
* Click the “Edit” button.

A screenshot of a computer

AI-generated content may be incorrect.

* Make any changes if needed for Update Ticket.
* 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, tickettype and tprice parameter by injecting this payload:

(<h1>Hello</h1)

A screenshot of a computer

AI-generated content may be incorrect.

1. **Send and Observe:**

The injected HTML is rendered on this page

A screenshot of a computer

AI-generated content may be incorrect.

**Recommended Mitigations:**

**Mitigation:** Implement proper input validation, output encoding, and Content Security Policy (CSP) to prevent malicious HTML injection.