Reflected Cross-Site Scripting (XSS) vulnerability was found in “Rail Pass Management System/rpms/admin/search-pass.php” in PHPGurukul Rail Pass Management System Panel in PHP v1.0 allows remote attackers to execute arbitrary code via “searchdata” POST request parameter.

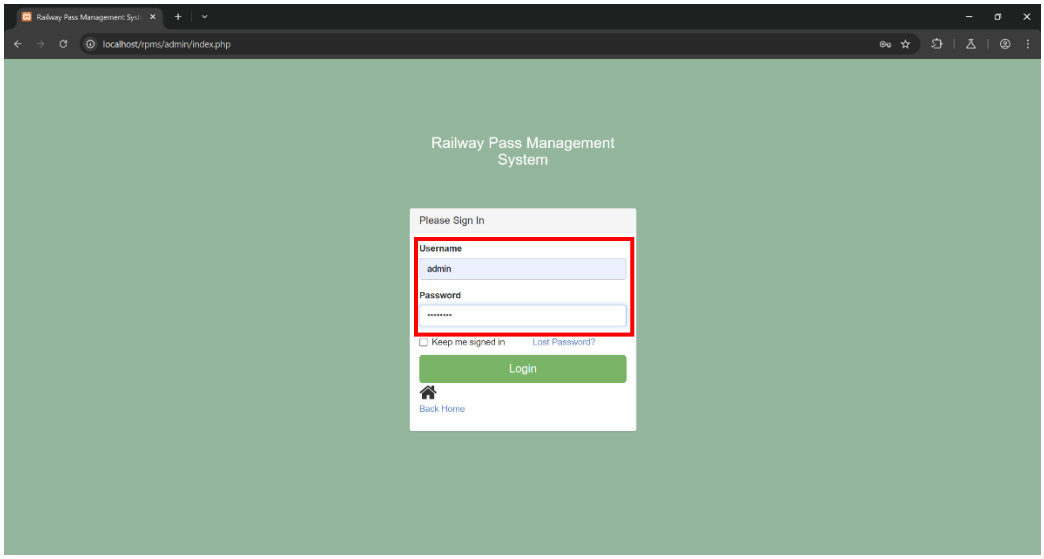
- Official Website URL

  https://phpgurukul.com/rail-pass-management-system-using-php-and-mysql/

- Affected Product Name: Rail Pass Managment System using PHP and MySQL

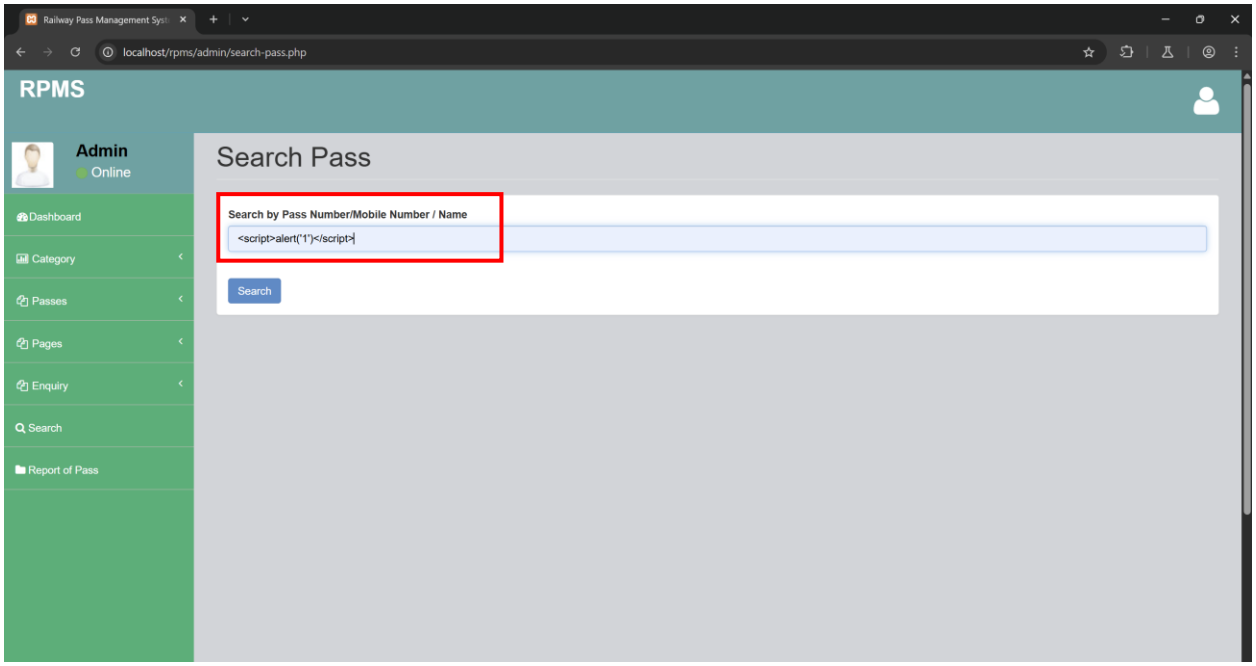
Affected Vendor	Phpgurukul
Affected Code File	Search-pass.php
Affected Parameter	searchdata
Method	POST
Type	Cross-Site Scripting (XSS)
Version	V 1.0

Steps to Reproduce:

1. **Log in to the Admin Panel:**
   - Open the admin login page.
   - Enter your credentials and sign
   - 

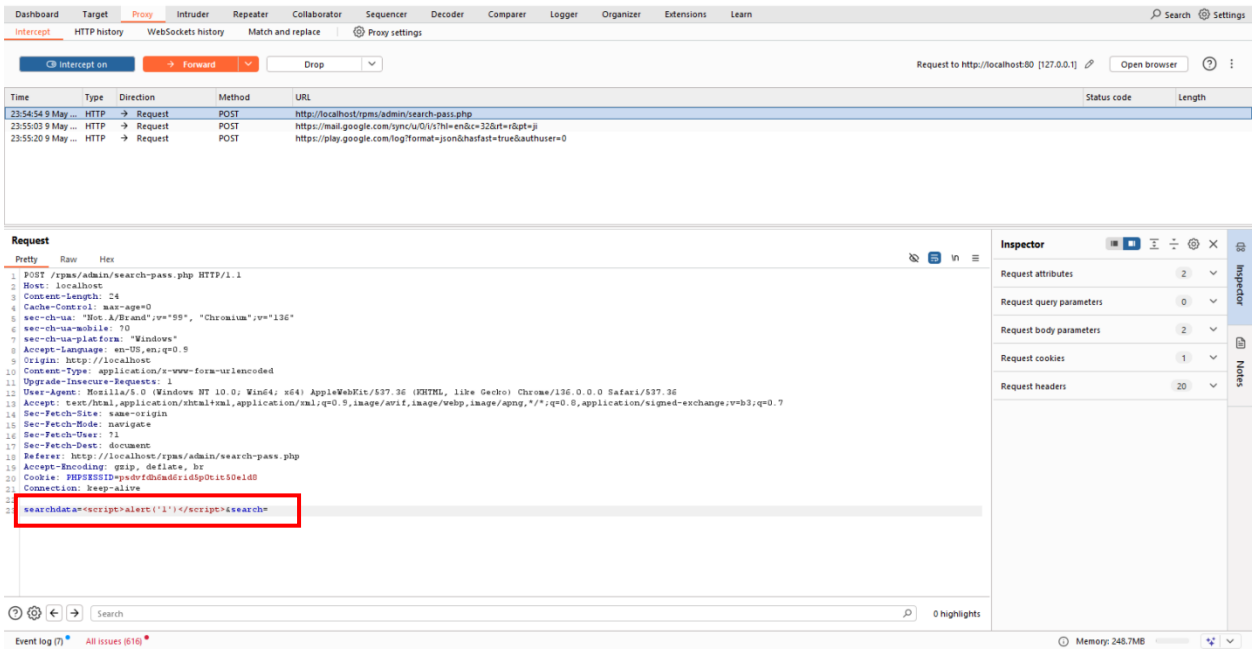
2. **Go to Manage profile:**

- Navigate to the “search” section.



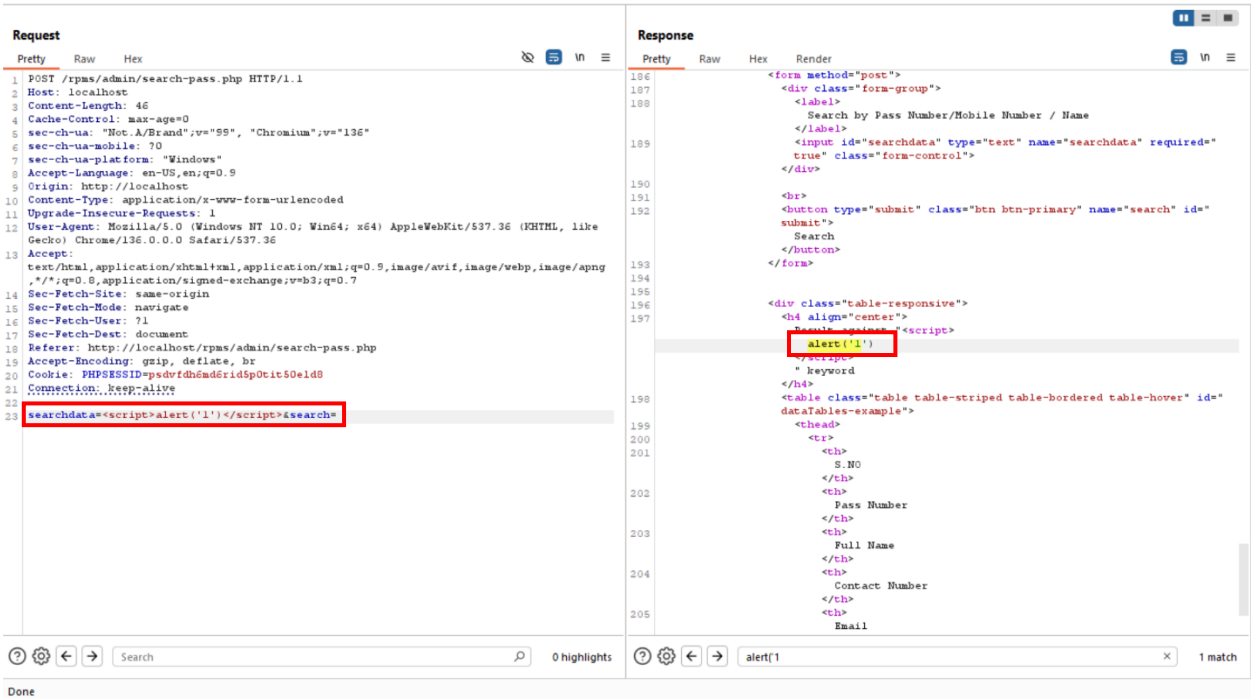
3. **Intercept the Request:**

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



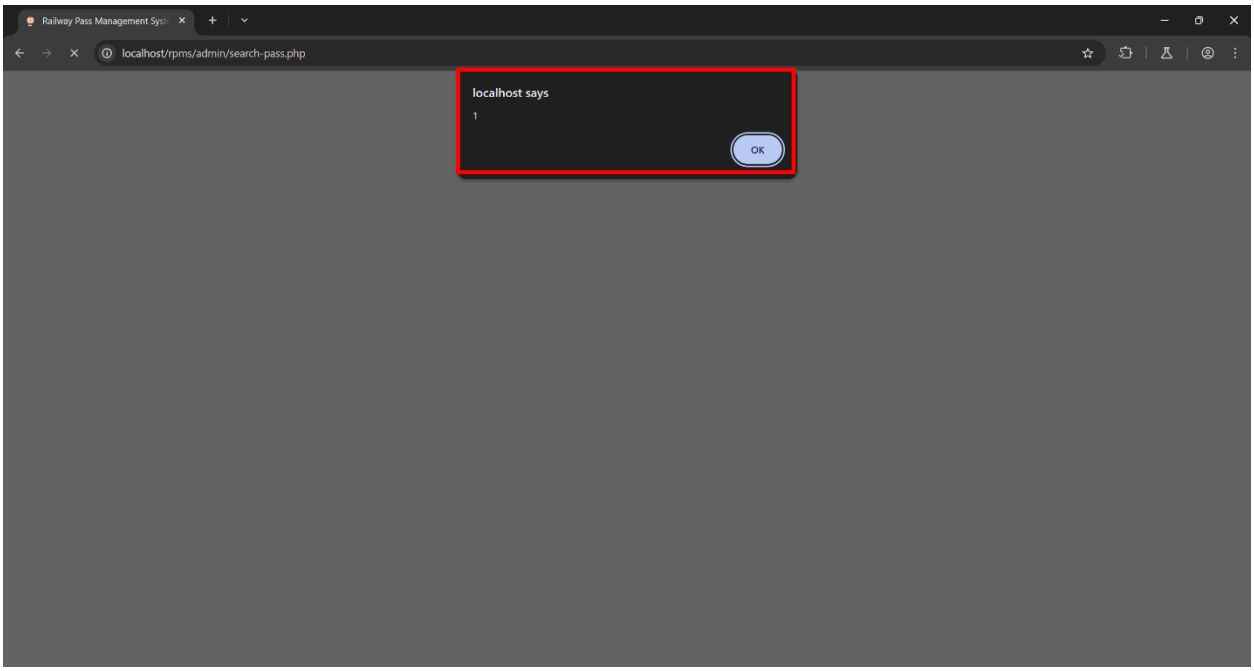
4. Modify the Request:

- Capture the request when updating user details.
- Send it to the Burp Suite Repeater.
- Modify the searchdata parameter by injecting this payload: (<script>alert(1)</script>)



5. Send and Observe:

The injected XSS is rendered on this page



Recommended Mitigations:

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