Best salon management system project in php project - XSS Vulnerability

Exploit Title: Best Salon Management System 1.0 - Persistent XSS

Date: 27.08.2025

Exploit Author: Abdulhalik Enes Ağcahan

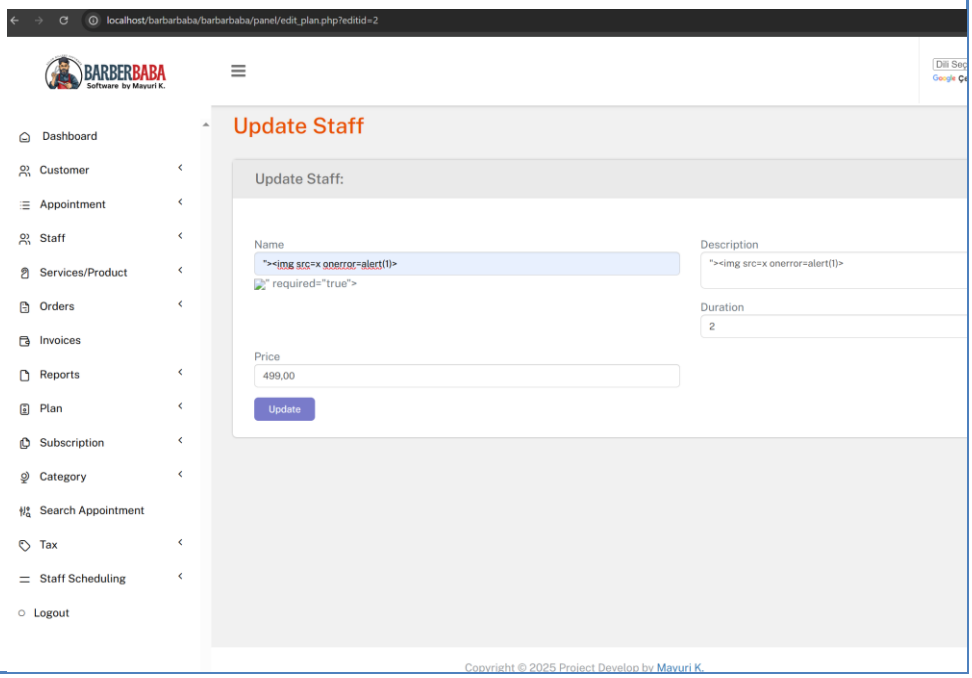
Vendor Homepage: https://www.sourcecodester.com/php/18171/best-salon-management-system-project-php.html

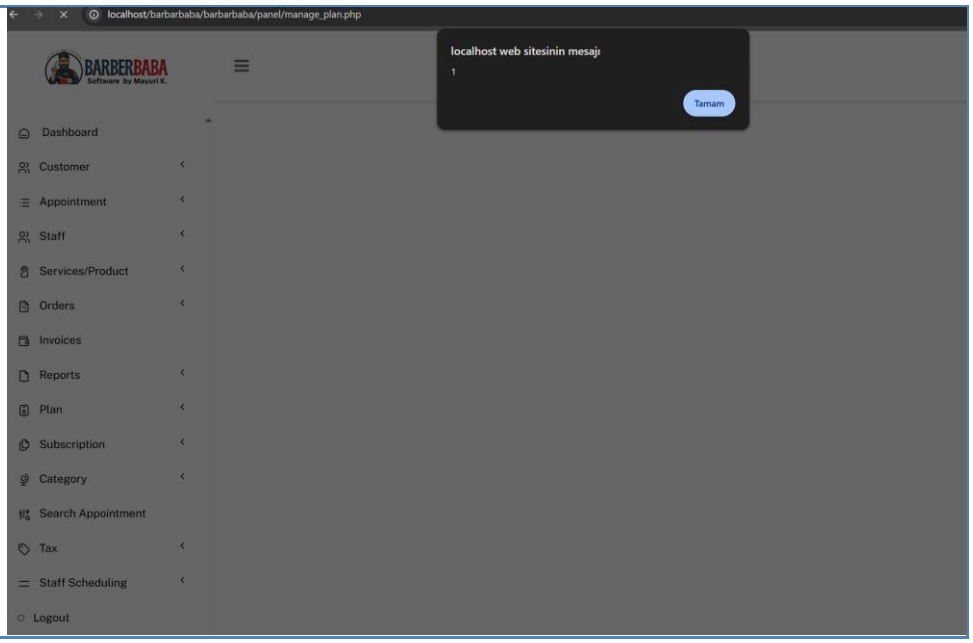
Software Link: https://www.sourcecodester.com/download-code?nid=18171&title=Best+salon+management+system+project+in+php

Version: 1.0

Tested on: Windows

Finding Title	**Persistent Cross-Site Scripting (XSS) Vulnerability**
Severity	High
Description	A persistent (stored) Cross-Site Scripting (XSS) vulnerability was identified in the target application. This occurs when user input is stored on the server (e.g., in a database) and then displayed to other users without proper sanitization or encoding. Attackers can inject malicious scripts that execute in the browsers of other users, potentially leading to session hijacking, data theft, or further attacks. The page where the finding was detected is in the update personnel section of the edit_plan.php page. Screenshots are available.
Evidence	- Vulnerable parameter: 'Name' field in the blog post update staff form. - Payload used: "><img src=x onerror=alert(1)> - The payload was stored in the database and executed whenever any user viewed the affected blog post.
Impact	Successful exploitation allows attackers to run arbitrary JavaScript in the victim's browser. This can result in theft of session cookies, redirection to malicious sites, credential harvesting, or full account compromise of affected users.
Recommendation	- Implement proper output encoding (e.g., HTML entity encoding) before displaying user-supplied input. - Apply input validation to block malicious scripts. - Utilize Content Security Policy (CSP) headers to mitigate XSS attacks.

	- Regularly test web applications for XSS vulnerabilities during development and production.
Screenshots	



References

• OWASP XSS Prevention Cheat Sheet - https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

• Mozilla Developer Network (MDN) - https://developer.mozilla.org/en-US/docs/Glossary/Cross-site_scripting