

main

...

CVE-report / OFRS.md



As4ki Update OFRS.md

History

2 contributors



22 lines (11 sloc) | 533 Bytes

...

Online Fire Reporting System v1.0 has XSS injection vulnerability

Login account: admin/admin123

vendor : <https://www.sourcecodester.com/php/15346/online-fire-reporting-system-phpoop-free-source-code.html>

Vulnerability file: /ofrs/report.php

The screenshot shows a web browser window with the address bar displaying 'phpcove.com/?p=report'. The website has a red header with the text 'OFRS - PHP' and navigation links: 'Home', 'Report', 'View Status', 'About', and 'Contact Us'. A 'Login' link is on the right. Below the header is a red banner with the text 'Fire Reporting'. The main content area contains a form with the following fields:

- Fullname ***: A text input field.
- Contac # ***: A text input field.
- Message ***: A large text area.
- Location ***: A text input field.

At the bottom of the form are two buttons: 'Submit' (blue) and 'Cancel' (grey).

Vulnerability location: /index.php/?p=report

[+]Payload:

When the report sent by the user is mixed with malicious code, as follows

This screenshot shows the same 'Fire Reporting' form, but with data entered in the fields. The 'Contac #' field is highlighted with a red border and contains the malicious payload: `<script>alert("1")</script>`. The other fields contain the text 'dsad'.

- Fullname ***: dsad
- Contac # ***: `<script>alert("1")</script>`
- Message ***: dsad
- Location ***: dsad

The 'Submit' and 'Cancel' buttons are still present at the bottom.

At this time, when the administrator checks the daily report, he will receive XSS attack

