

Vulnerability Discovery_18

Target

: http://124.60.4.10:10001/write_aciotn.php

Payload

: 글제목 XSS <script>alert(1)</script>

Impact

: 글 내용이 아닌 글 제목 XSS로 게시판 리스트만 접근하는 것으로 XSS 발생, 공격자는 게시판 접근자에게 CSRF 등 추가적인 악성행위 연계 가능성 존재

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/9ac9a734-eb64-44ca-a306-9b0980e6c80d/XSS_script.txt

Welcome! asdf
비밀번호 변경 SIGN OUT

Simple PHP board

검색

Number	Title	Written by	Date	Views
11	스드	yoobi	2023-01-29 13:48:54	2
10	<script>alert(1)</script>	yoobi	2023-01-29 13:46:37	0
9	<script>alert(1)12</script>	yoobi	2023-01-29 13:46:21	0
8	123	yoobi	2023-01-29 13:45:48	5
7	sdfg	gyeom	2023-01-28 18:35:53	2
6	asdf	gyeom	2023-01-28 18:17:27	7
3	1	yoobi	2023-01-23 22:44:27	10
2	tes	yoobi	2023-01-23 22:44:07	2
1	test	yoobi	2023-01-23 22:43:59	1

Write

- Ver.2020.01.05 -
made by yoobi
<https://velog.io/@yoobi/about>