# Day52　代码审计–PHP项目类 RCE及文件包含下载删除

```
漏洞关键字
SQL注入：
 select insert update mysql_query mysqli等
文件上传：
 $FILES,type="file"，上传，move_upload_file()等
 XSS跨站：
 print print_r echo sprintf die var_dump var_export等
文件包含：
 Include include_once require require_once等
代码执行：
 eval assert preg replace call user func call user func array等
命令执行：
 system exec shell_exec `` passthru pcntl_exec popen proc_open
变量覆盖：
 extract() parse_str() importrequestvariables() $$等
反序列化：
 serialize() unserialize() _construct _destruct等
通用关键字：
 $GET $POST $REQUEST $FILES $SEVER
```

## 52.1 通用关键字

```
---$_GET,$_POST,$_REQUEST,$_FILES,$_SERVER 等

---功能点或关键字分析可能存在漏洞

---抓包或搜索关键字找到代码出处及对应文件

---追踪过滤或接受的数据函数，寻找触发此函数或代码的地方进行触发测试

http://192.168.0.102:91/?r=../../index.txt%00

http://192.168.0.102:94/admin/save.php?act=delfile
path=/upload/../install/install.lock
```

## 52.2 案例思路

### 52.2.1 xhcms-无框架-文件包含跨站-搜索或应用-include

```
整体思路
通用应用及url地址等分析可能存在xss及包含安全漏洞
抓包找到xss无过滤代码块及文件包含有后缀需绕过代码块
（具体分析过程查看链接
https://www.bilibili.com/read/cv15169189?spm_id_from=333.999.0.0
```

## 52.2.2 earmusic-无框架-文件下载-搜索或应用功能-down 等

```
整体思路
---通过应用分析或搜索判断可能存在文件下载操作
---抓包分析下载地址找到对应代码块，文件下载地址由$file 控制
---$file 从数据库查询语句得知，追踪那里可更新或更改此类数据
---尝试修改发现过滤，追踪过滤机制分析绕过，采用全路径地址绕过
```

```
分析思路
进入靶场，观察功能
---这里从会员中心的功能可能存在的漏洞：
        音乐下载存在文件下载漏洞；
        头像和音乐上传存在文件上传漏洞；
        个人信息修改可能存在SQL注入漏洞；
        日志，页脚可能存在XSS漏洞；
        查看调用的api可能存在一些其他漏洞；
        查看数据包传输格式等等
---根据网站的功能，取猜测可能存在的漏洞：
        偏向社交，注入、XSS多一点；音乐下载，文件下载、上传漏洞多；
---这里文件下载漏洞挖掘的两种思路：
        （1）根据文件下载的功能测试
        （2）搜索文件下载的相关函数和关键字然后抓包分析
        （3）追踪过滤或接受的数据函数，寻找触发此函数或代码的地方进行触发测试
```

## 52.2.3 zzzcms-无框架-文件删除 RCE-搜索或应用-unlink,eval

```
整体思路
---文件删除搜索关键字 unlink,对应函数 del_file，查看调用此的地方
---后台 delfile 函数调用，如何处罚 delfile 函数，受参数控制，进行测试
---代码执行搜索关键字 eval,对应配置模版解析文件，查看调用此的地方
---判断后台可修改模版文件，前台触发模版文件，构造 payload 进行测试
```

```
分析步骤：
---文件删除一般用于白盒审计，可以删除install.lock文件
（具体步骤见链接：https://www.bilibili.com/read/cv15169189?spm_id_from=333.999.0.0）
```