【代码审计】yxcms从伪XSS到Getshell

水泡泡 / 2018-02-06 09:29:00 / 浏览数 4873 安全技术 漏洞分析 顶(0) 踩(0)

0x00 前言

整个利用链构造下来是比较有趣的，首发于某个安全圈子，主要是想分享一下思路，发过来先知是为了看看有没有什么建议，讨论。

此次审的是yxcms 1.4.6版本，应该是最后一个版本了吧？

0x01 从任意文件删除漏洞说起

yxcms经过修修补补，前台的一些洞都挖得差不多了，一番挖掘没什么效果，转到后台去。后台的防护是比较松懈的。
找到了个任意文件删除漏洞。

/protected/apps/admin/controller/filesController.php

```
public function del()
   {
      $dirs=in($_GET['fname']);
      $dirs=str_replace(',','/',$dirs);
      $dirs=ROOT_PATH.'upload'.$dirs;
      if(is_dir($dirs)){del_dir($dirs); echo 1;}
      elseif(file_exists($dirs)){
        if(unlink($dirs)) echo 1;
      }else echo '■■■■■';
   }
```

代码很简单，接收文件名，拼接路径，判断文件是否存在，直接删除。没有过滤。

后台大部分请求是有csrf防护的，但有一些是没有，比如这里的文件删除。

那么我们自然想到的是csrf咯，发个链接给管理员，删除install.lock进行重装，然后getshell。

但这样动作太大了，非常容易被管理员发现。

其实我们无非就是希望能够获得管理员的权限，还有没有其他办法？

0x02 更为轻松的办法：session固定漏洞

先简单介绍一下session固定漏洞，session固定漏洞最为核心的其实应该是程序使用session作为认证方式，但又放开了session_id的设置，并且设置session_id在session_s

有这么一个场景，当管理员登陆之后，程序生成一个认证session，而此时的session是没有指定session_id的。如果存在一个接口能够让我们指定session_id，那么我们就可

构造一个请求设置session_id的链接让管理员点击，那么我们就拥有了管理员的权限。（CSRF）

在攻击成功之后，怎么设置我们的session_id呢？

其实就是我们前端经常看到的这个东西。

```
PHPSESSID=fdpmos0quo6o7rq69h6v1u6i50;
```
攻击成功之后，设置PHPSESSID=你自己设置的session_id，然后带着这个cookie请求即可访问后台。

yxcms也是存在session固定漏洞的，看到文件protected\include\lib\common.function.php

```
function session($name='',$value = '') { //session■■
   if(empty($name)){
       return $_SESSION;
   }
   $sessionId = request('request.sessionid');
   if(!empty($sessionId)){ //■■■■■■■session_id
       session_id($sessionId);
   }
   if(!isset($_SESSION)){
       session_starts();
   }
   if($value === ''){
       $session = $_SESSION[$name];
   }else if($value==null){
```

```
        unset($_SESSION[$name]);
    }else{
        $session = $_SESSION[$name] = $value;
    }
    return $session;
}
```

这里接收了一个REQUEST请求，参数名为sessionid的参数，将它设置为session_id。
追溯一下session方法的调用。

用户进行后台相关页面的访问 - >> 先进行登陆和权限检查 --> 调用auth类进行检查

跟进auth类的check方法

先进行session的初始化，然后调用checkLogin方法判断是否有登陆。

```
static public function checkLogin()
    {
        $groupid=session(self::$config['AUTH_SESSION_PREFIX'].'groupid');
        if(!empty($groupid))
        return true;
        else
        return false;
    }
```

而checkLogin里调用了session方法。
那么我们整个调用链就很清晰了。

请求后台任意需要认证的页面都是会调用session()方法，而且sessionid的接收时REQUEST方式，那么我们只要让登陆后台的管理员点击类似这样的链接，就可以拿到后台的

```
http://demo.yxcms.com/index.php?r=admin/index/index&sessionid=123test
```
要让管理员登陆状态下点你的链接，最好的方法是找到个后台的xss啦。

0x03 留言伪xss

随便找了一下，在前台留言的地方发现了一个伪xss，可以插入html标签。

虽然构造不成xss，但是已经足够了。利用img 标签发起一个请求，正好够我们session固定用了。
还有点美中不足的是，在实际场景中，你留了个言，你怎么知道这个管理员什么时候触发呢？

有没有办法能够在第一时间通知我们呢？

其实是有的。
我们可以在我们的公网服务器上，放一个跳转脚本。然后在服务器上写一个脚本去统计访问了这个跳转脚本（脚本名字可以设置的复杂点，以防被扫描器扫到）的服务器，并

0x04 后台getshell

终于到了后台getshell，拿到了权限之后其实就很简单了。
后台有一个编辑模板的地方可以直接getshell。

编辑加入shell代码，访问首页，直接getshell。

0x05 总结

通过前台留言功能，在后台构造了一个伪xss，利用img标签发起csrf
session固定请求，中间利用跳转脚本及时记录下获取到权限的服务器，随之登陆后台利用模板编辑功能进行getshell。

Have Fun !

上一篇：Linux内核调试 下一篇：FreeFloat FTP1.0 ...
1. 4 条回复

xwbk12 2018-02-26 10:18:32

楼主，你的yxcms的版本是多少？

0 回复Ta

xwbk12 2018-02-26 10:29:37

不好意思，写错了

0 回复Ta

水泡泡 2018-02-26 10:30:07

@xwbk12

0 回复Ta

xwbk12 2018-02-26 17:36:37

多谢多谢啊！！

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