awd 线下攻防java防护_2017强网杯线下AWD攻防总结（适合新手）

原创

浩浩耗 于 2021-02-26 22:18:34 发布 380 收藏 1
文章标签： awd 线下攻防java防护

本文链接：https://blog.csdn.net/weixin_29184371/article/details/114757185

这篇文章首发于个人博客https://iewoaix8736.github.io/

鉴于刚建立博客，比较少人看，所以在t00ls分享给大家，欢迎来交流

前言：

本菜为高校组，这篇文章适合新手学习参考(dalao飘过，不喜勿喷)

AWD攻击

这次线下攻防用的是一个Finecms，版本是5.0.9的

之前对这个cms并不了解

现在复现一下，

从哪里跌倒，就从哪里爬起来。

朋友给我看了他审计的一片文章

http://www.cnblogs.com/post/readauth?url=/test404/p/7351144.html(密码：panghuf)

其实百度也很多，

5.0.9这个版本存在头像上传getshell漏洞

比赛的源码是修改了的，先来看看

```
/**
* 上传头像处理
* 传入头像压缩包，解压到指定文件夹后删除非图片文件
*/
public function upload() {
// 创建图片存储文件夹
$dir = SYS_UPLOAD_PATH.'/member/'.$this->uid.'/';
@dr_dir_delete($dir);
!is_dir($dir) && dr_mkdirs($dir);
if ($_POST['tx']) {
$file = str_replace(' ', '+', $_POST['tx']);
if (preg_match('/^(data:\s*image\/(\w+);base64,)/', $file, $result)){
$bad_ext=array('php','php3','php4','php5');
if(in_array($result[2],$bad_ext)){
exit('hack');
}
$new_file = $dir.'0x0.'.$result[2];
if (!@file_put_contents($new_file, base64_decode(str_replace($result[1], '', $file)))) {
exit(dr_json(0, '目录权限不足或磁盘已满'));
} else {
$this->load->library('image_lib');
$config['create_thumb'] = TRUE;
$config['thumb_marker'] = '';
$config['maintain_ratio'] = FALSE;
$config['source_image'] = $new_file;
```

```
foreach (array(30, 45, 90, 180) as $a) {
$config['width'] = $config['height'] = $a;
$config['new_image'] = $dir.$a.'x'.$a.'.'.$result[2];
$this->image_lib->initialize($config);
if (!$this->image_lib->resize()) {
exit(dr_json(0, '上传错误：'.$this->image_lib->display_errors()));
break;
}
}
list($width, $height, $type, $attr) = getimagesize($dir.'45x45.'.$result[2]);
!$type && exit(dr_json(0, '图片字符串不规范'));
}
} else {
exit(dr_json(0, '图片字符串不规范'));
}
} else {
exit(dr_json(0, '图片不存在'));
}
// 上传图片到服务器
if (defined('UCSSO_API')) {
$rt = ucsso_avatar($this->uid, file_get_contents($dir.'90x90.jpg'));
!$rt['code'] && $this->_json(0, fc_lang('通信失败：%s', $rt['msg']));
}
exit('1');
}
}
```

可以看到这一段代码

```
$bad_ext=array('php','php3','php4','php5');
```

这里把基本把php后缀的文件都给屏蔽了

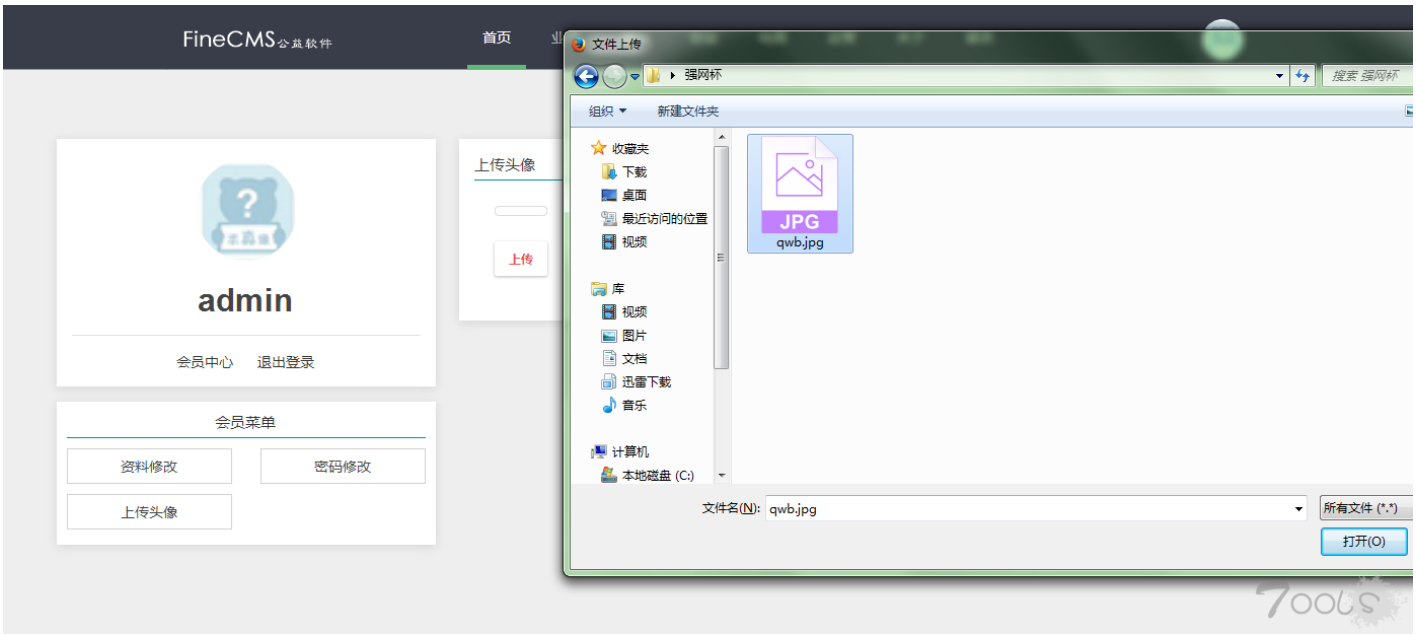
但是忘了我们还有phtml

PHTML(有时叫做PHP)网页是一种包含PHP(一种和JavaScript或Microsoft VBScript类似的语言)脚本的网页和ASP一样，PHP脚本镶嵌在网页的HTML代码之中。

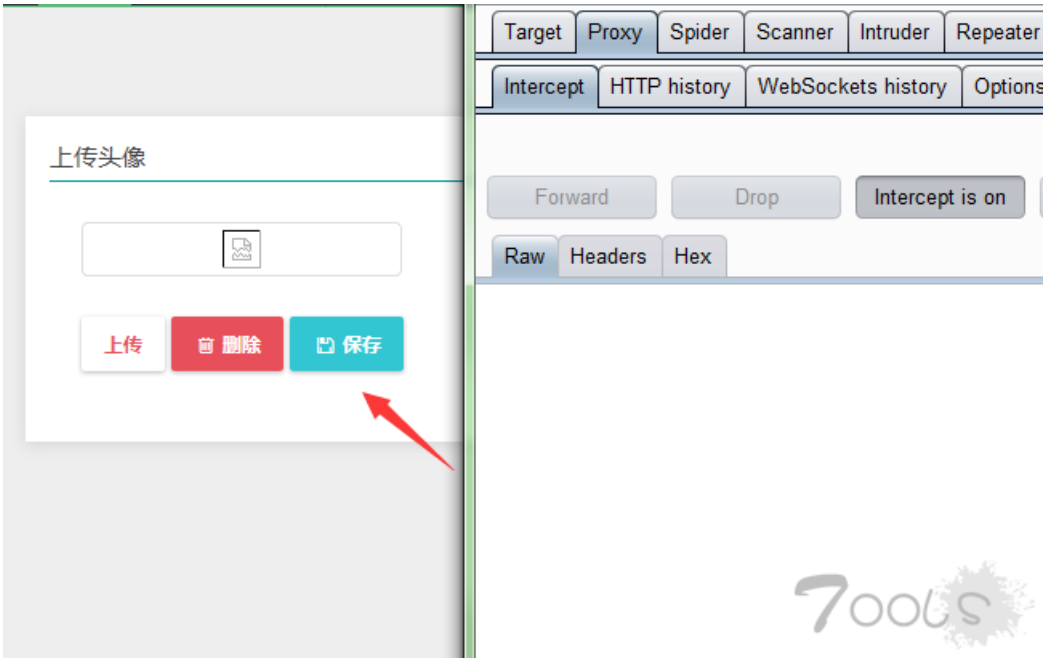
其实比赛中应该要想到了，之前CTF就有遇到过，我想我可能被打懵了吧。。。

这里先上传一个jpg的一句话

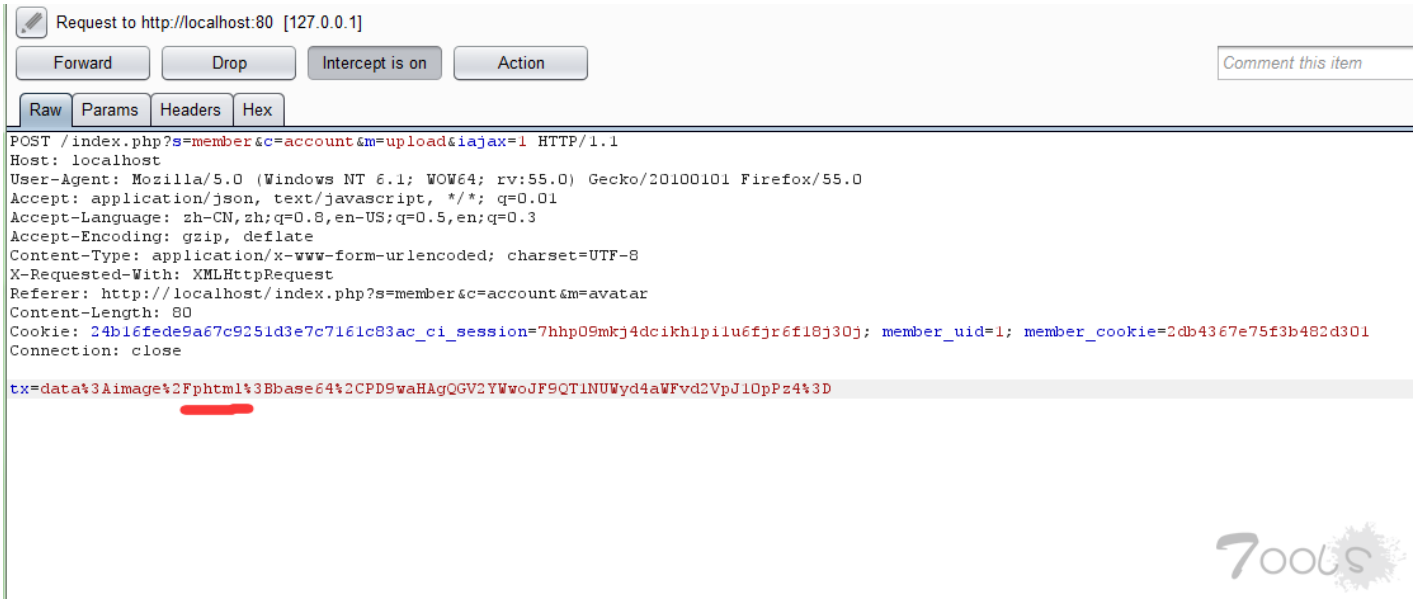
PS:因为直接上传的话phtml可能不行，他会判断是不是图片.



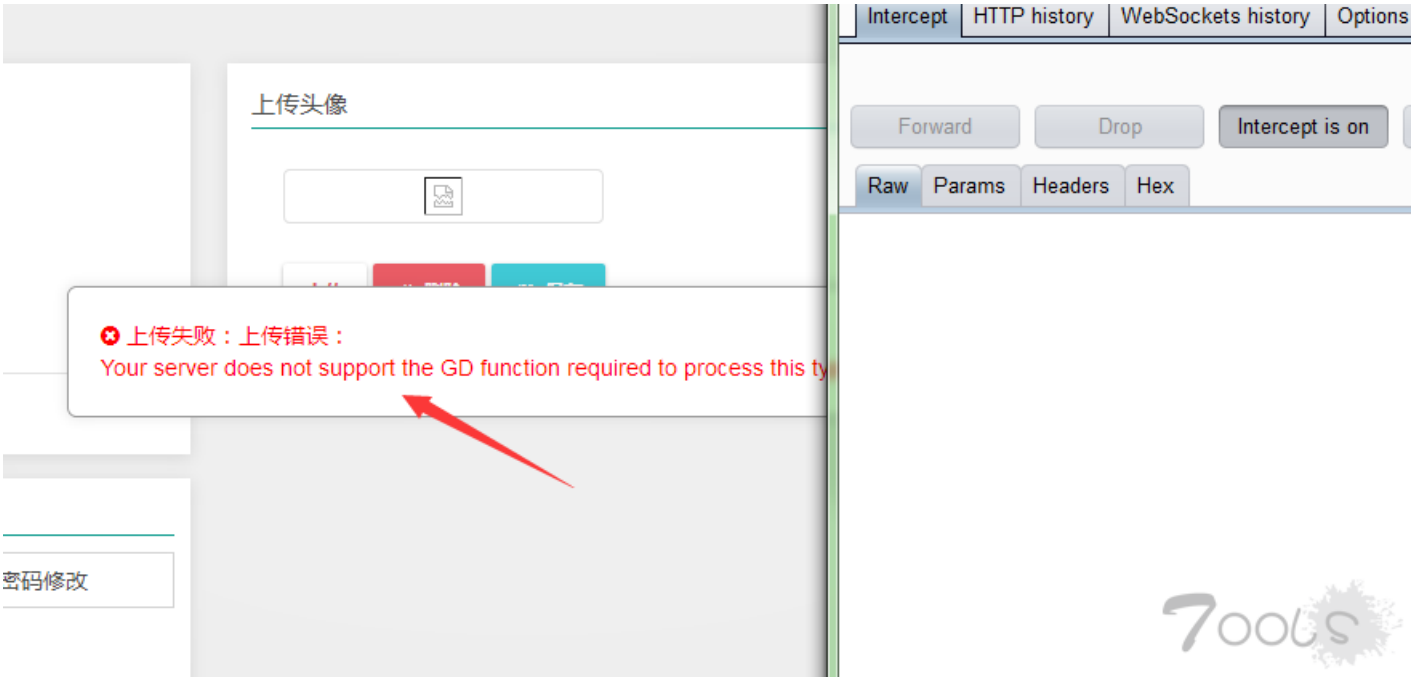
然后再点击保存抓包



然后将这里jpeg改成phtml



然后Forward，他会报错



但是我们看源码，并没有这一句英文的错误，不管他，进目录看看

```
                }
                list($width, $height, $type, $attr) = getimagesize($dir.'45x45.'.$result[2]);
                !$type && exit(dr_json(0, '图片字符串不规范'));
            }
        } else {

            exit(dr_json(0, '图片字符串不规范'));
        }
    } else {
        exit(dr_json(0, '图片不存在'));
    }
```

到目录上看看，果然上传上去了

然后菜刀连接直接可以在根目录上看到flag了

这里就不演示了

防御：

这里说下防御方法

一般都会给你ssh的账号密码，

登录上去down下源码，然后自己修改代码

1.修改代码

$bad_ext=array('php','php3','php4','php5');可以看到这段代码，没过滤phtml，这里可以添加上去，

也可以添加其他后缀的文件，免得dalao们各种奇淫技巧突破，

比赛后还听到有dalao说上传asp的增加权限，

这里我就不清楚了,不过也可以添加上去过滤掉。

2.修改登录密码

比赛中很多后台登录都是弱口令的

admin密码其实可以在数据库中找到

比赛中我是直接弱口令admin上去的

然后手速要快，修改之后一般人就无法用你账号进入后台了

3.修改注册代码

```php
// 会员配置
$MEMBER = $this->get_cache('MEMBER');


// 判断是否开启注册
if (!$MEMBER['setting']['register']) {
    $this->member_msg(fc_lang('站点已经关闭了会员注册'));
}

if (IS_POST) {
    $data = $this->input->post('data', TRUE);
    $back_url = $_POST['back'] ? urldecode($this->input->post('back')) : '';
    $back_url = $back_url && strpos($back_url, 'register') === FALSE ? $back_url : dr_member_url('home/index');
    if ($MEMBER['setting']['regcode'] && !$this->check_captcha('code')) {
        $error = array('name' => 'code', 'msg' => fc_lang('验证码不正确'));
    } elseif ($result = $this->is_username($data['username'])) {
        $error = array('name' => 'username', 'msg' => $result);
    } elseif (!$data['password']) {
        $error = array('name' => 'password', 'msg' => fc_lang('密码不能为空'));
    } elseif ($data['password'] !== $data['password2']) {
        $error = array('name' => 'password2', 'msg' => fc_lang('两次密码输入不一致'));
    } elseif ($result = $this->is_email($data['email'])) {
        $error = array('name' => 'email', 'msg' => $result);
    } else {
        $id = $this->member_model->register($data, 0);
        if ($id > 0) {
            // 注册成功
            $data['uid'] = $id;
            $this->hooks->call_hook('member_register_after', $data); // 注册之后挂钩点
            // 注册后的登录
            $code = $this->member_model->login($id, $data['password'], $data['auto'] ? 8640000 : $MEMBER['setting']['loginexpire'], 0
                , 1);

        } elseif ($id == -1) {
            $error = array('name' => 'username', 'msg' => fc_lang('该会员【%s】已经被注册', $data['username']));
        } elseif ($id == -2) {
```

这里是注册的代码

你可以修改成不管怎么输入最后都注册不了，

改完admin密码，改完注册代码后基本上可以防御绝大多数进攻了

这样可以不用删除这个注册页面，删除的话会判断down机，扣分

4.挂waf

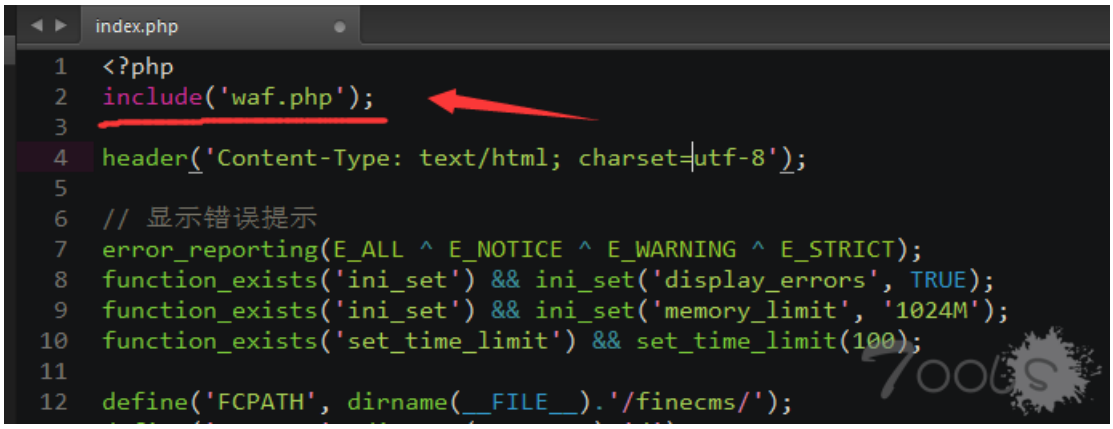
比赛后跟dalao交谈，说除了头像上传外还有一处命令执行漏洞，

这个时候就要用到waf了，

因为比赛中一般是user普通用户，没有权限重启服务

所以只能采用包含waf脚本了

可以直接包含在index里面，注意waf所在目录



你可以添加过滤各种函数，符号，base64编码等等

这样可以有效抵御一般的命令执行了(dalao路过)

当然，如果会修改那个漏洞更好。

后续:

好了，到这里就全部结束了，本辣鸡只能吹到这里，

欢迎各位dalao来指点一二，

有喜欢打比赛的也可以交流交流，

有dalao不嫌弃的话可以收了我，哈哈哈哈

再.....后续:

比赛不是唯一，能学到东西就好。

能交到很多朋友，我很高兴。

每经历一次比赛就成长一次，

多总结，提升自己。

最后，最后，

感谢支持我的朋友.

TCV期望值：0.01