Xiunobbs Upload

31 Jul 2019

一.漏洞摘要

漏洞名称

xiunobbs 4.0.4版本，前台文件上传导致XSS

日期

2019-07-31

发现者

陈瑞琦，陈辉亮

产品首页

http://bbs.xiuno.com

获取连接

https://bbs.xiuno.com/down/xiunobbs_4.0.4.zip

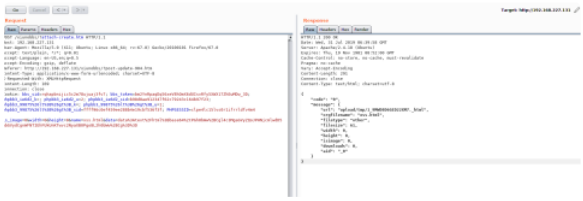
影响版本

4.0.4 及之前版本

二.漏洞描述

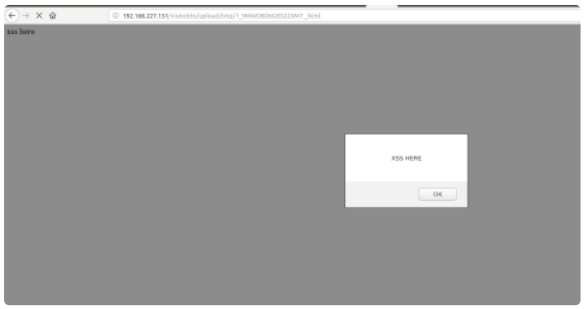
在普通用户发帖功能处，上传附件功能 可以上传html文件，后台会将文件存储，并且修改后缀名为 .__html

如下图所示



但是上传有恶意js代码的html文件，服务器（apache）仍然会解析.__html格式内的js代码

效果如下图所示



三.漏洞POC

xss.html

```
<html>
        XSS HERE
        <script>alert('XSS HERE')</script>
</html>
```

Related Posts

XSS in Blogtext version 3.7.6 [CVE-2016-9418] 06 Feb 2017

XSS in Blogtext version 3.7.6 [CVE-2016-9418] 06 Feb 2017

XSS in wordpress version 4.7.2 [CVE-2016-9418] 06 Feb 2017