挖洞经验丨有上传文件的文件名处发现的时间延迟注入漏洞

转载

普通网友 于 2019-07-25 17:15:27 发布 1869 收藏 2
分类专栏： mysql


mysql 专栏收录该内容
35 篇文章 0 订阅
订阅专栏

***本文中涉及到的相关漏洞已报送厂商并得到修复，本文仅限技术研究与讨论，严禁用于非法用途，否则产生的一切后果自行承担。**

该Writeup是作者在邀请测试项目中发现的，在上传文件的文件名处（filename）的一个时间延迟盲注漏洞，这种姿势相对少见，分享在此希望能对大家起到借鉴学习作用。以下是作者的发现过程。

本月初，我受邀参与了HackerOne平台某厂商的一个私密众测项目，由于此前我有些朋友也做过该厂商的众测，所以我就向他们征询该厂商相关系统应用的大概情况，以便提前了解其中存在的难点和会遇到的坑。

从注册页面入手发现上传功能

在和朋友@reefbr聊过之后，他发给了我目标厂商某重要域名下的一个会员注册页面，刚好该注册页面在本次测试范围之内。现在要做的就是，实际注册测试一下吧。整个注册过程都很正常，一会之后，我留的注册邮箱就收到了一封包含访问Web应用凭据的邮件。

以会员身份登录目标Web应用之后，我发现其中存在一个文件上传功能。于是，我通过随机文件上传进行测试看看其中的安全限制，发现：

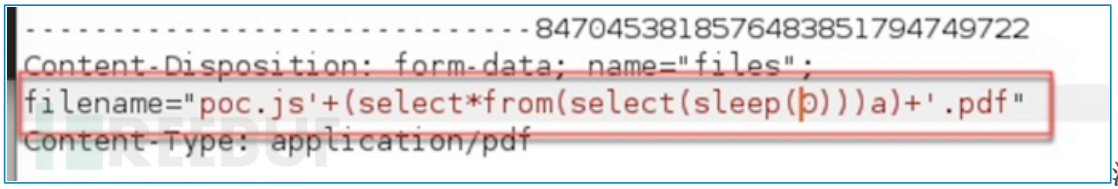
> 上传只接受PDF格式文档
>
> Web应用后端部署有杀毒软件AV

经过一番分析之后，我觉得该上传点只接收类似”filename.pdf”的PDF格式文档，我曾尝试绕过这种文件格式限制措施，虽然某些条件下可以成功上传其它格式文件，但上传文件却不能在服务端有效执行，所以，我转向了其它功能点的测试。

记得以前在做渗透测试时，我曾遇到过一个把文件名都包含存储到数据库中的Web应用，那次，我通过构造其文件名参数，成功发现了其基于时间差盲注(Time-Based Blind SQL)的漏洞。那么，这个Web应用是否存在该漏洞呢？试试看。

BurpSuite抓包分析

用Burp Proxy代理抓包分析HTTP请求，点击上传按钮后，把其中的文件名filename值更改为以下红框内的值：

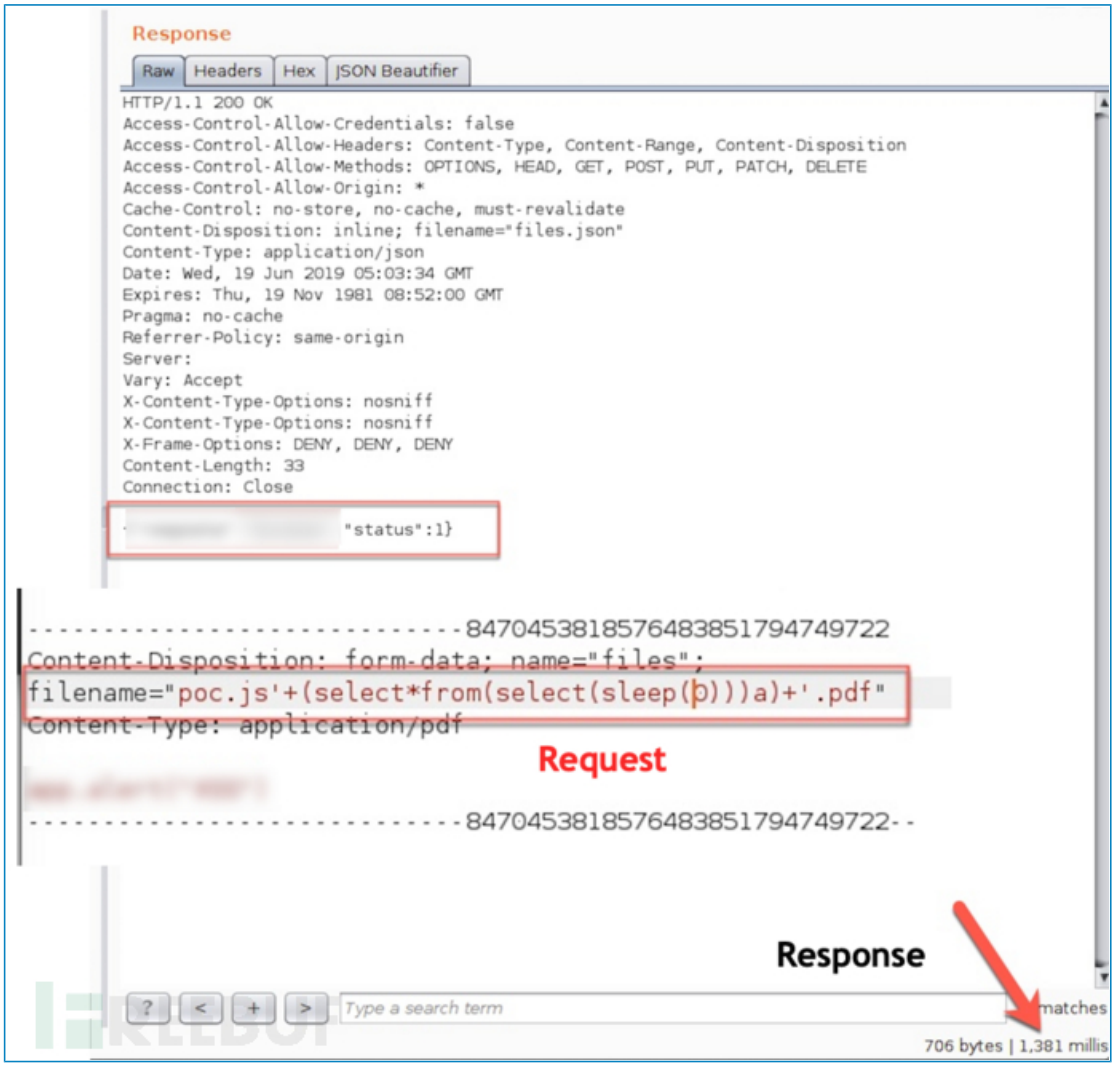


注意：以上filename值情况下，当我不加最后的.pdf后缀名发送请求时，目标Web应用是拒绝接收的。探测发现，目标Web应用之后部署有Cloudflare WAF，所以我的好多测试都被这个WAF给阻挡了，返回的都是”Access Denied” 消息。

我突然想到朋友@reefbr说过他在该厂商之间的测试项目中，曾上报过一个Cloudflare的绕过漏洞，这是一个由配置问题导致的问题，所以，我刚好可以拿来试试看，这一试，我就发现了一个SQL盲注漏洞了。什么都不说了，直接上POC吧。

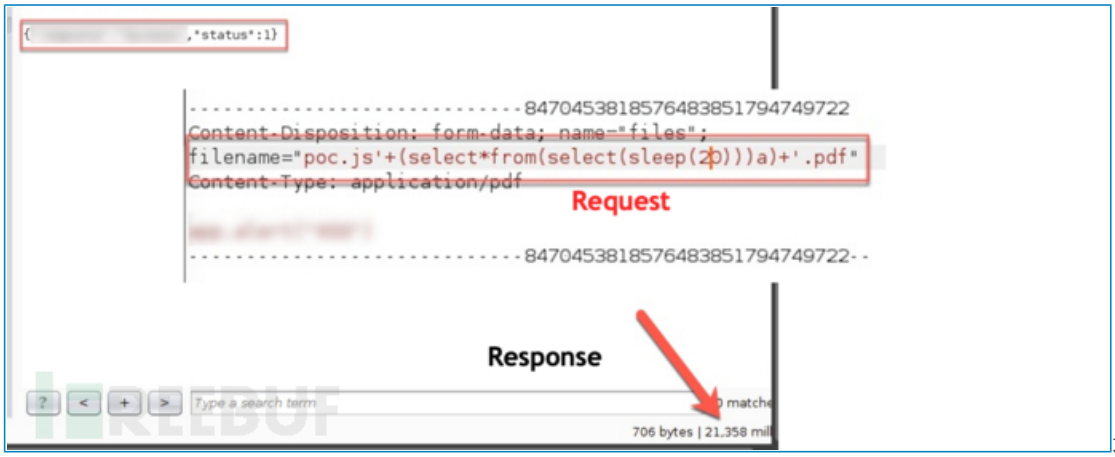
POC

利用上述的文件名构造方式，结合Cloudflare绕过问题，我发起了以下请求，注意看其中的时间延迟sleep：



以上是sleep(0)无延迟的情况，请求需要1380毫秒。现在换成sleep(10)延迟10秒，即10000毫秒，看看：

增加10000毫秒后，确实变成11350毫秒了。现在，再增加成20秒，即20000毫秒：



最后时间确实在之前基础上增加了20000毫秒，变成了21358毫秒了。厂商团队应该清楚问题实质了吧，我们再增加一点延迟时间看看：

那么，这里明显存在一个盲注漏洞。由于目标系统负责处理大量的个人身份信息（PII），所以，如果攻击者利用这种盲注漏洞对系统中的数据进行提取，将会导致大量的敏感信息泄露，也是因为此种原因，我才采用了破坏力稍低的时间延迟注入方法来说明漏洞问题。

上报进程

> 漏洞初报
>
> 漏洞分类
>
> 漏洞修复
>
> 赏金奖励

***参考来源：jspin，clouds编译，转载请注明来自FreeBuf.COM**