

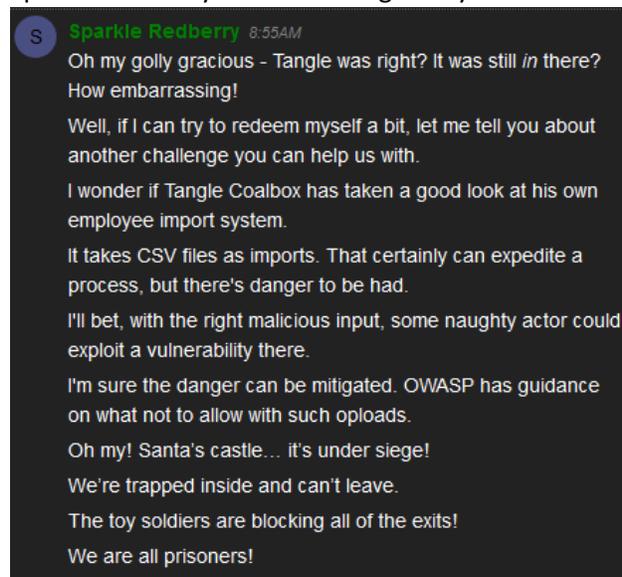
Objective--HR Incident Response (Part 1)

What you can learn from this

Major spreadsheet applications, like Excel, accept files in the comma separated values (CSV) format. Major spreadsheet applications also allow their users to call other applications through their spreadsheets via formulas. Attackers have exploited this combination in several major attacks by exfiltrating data or even opening reverse shells to the victim computer. Attackers are still pursuing CSV Injection attacks now, so this is something IT security professionals should be aware of.

Hints

Sparkle Redberry has something to say about CSV Injection, after her Dev Ops Fail terminal is solved.



Additionally, she added two hints to our badge.



First, listen to Brian Hostetler's talk, [CSV Formula Injections: Pwn Web Apps Like a Ninja](#).

Second, read the [OWASP CSV Injection Page](#) that Sparkle talks about. A link from the OWASP page to an article entitled [Comma Separated Vulnerabilities](#) is also worth your time. Note that their solution to prevent CSV Injection is to edit the CSV files to disable formulas before opening them. I don't know of many organizations that do this for their users, although their Intrusion Prevention Systems (IPS) may block the injections. That assumes the attacker's traffic is not encrypted, or the IPS is decrypting incoming traffic, however.

CSV Injection is still a useful attack today.

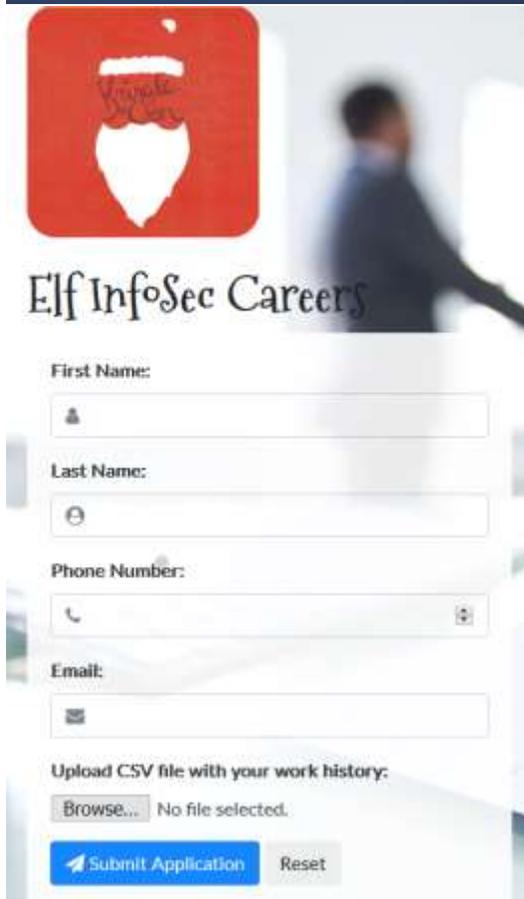
Getting Started

The web site we are interested in is <https://careers.kringlecastle.com/>. As you can see, it asks that applicants upload a CSV file with their work history.

7) HR Incident Response

Difficulty: ●●●● 🌲

Santa uses an Elf Resources website to look for talented information security professionals. Gain access to the website and fetch the document C:\candidate_evaluation.docx. Which terrorist organization is secretly supported by the job applicant whose name begins with "K." For hints on achieving this objective, please visit Sparkle Redberry and help her with the Dev Ops Fail Cranberry Pi terminal challenge.



Elf InfoSec Careers

First Name:

Last Name:

Phone Number:

Email:

Upload CSV file with your work history:

Browse... No file selected.

Submit Application Reset

Important Note

The talk and articles are very helpful, but most of their examples involve PowerShell. I believe the site is blocking attempts to run PowerShell through CSV Injection and is not allowing reverse shells. Please attend Tim Medin's talk, [Hacking Dumberly not Harder](#). His philosophy will be very useful here. You may want to probe the site a little, especially looking for interesting error messages.

Also note that the server will refuse injections that have a space in the first six or so characters, even though that will work if you test it on your local system. It appears to be a bug.

It is important that you create this file in a text editor and not in a spreadsheet. If you use a spreadsheet, the application will mangle your injection text.

Hand In

- 1) What is the text of an error message that may help you? After reading it, what do you think your attack should try to do?
- 2) What is the content of your successful CSV Injection file?
- 3) Which terrorist organization is secretly supported by the applicant whose name begins with 'K'?