FeaturesBusinessExplorePricing

This repositorySearch

Sign in or Sign up


USCGA / writeups

Watch3Star6Fork2


<> Code0Issues0Pull requests0Projects0PulseGraphs

Branch: masterwriteups / online\_ctfs / bitstcf\_2017 / banana\_princess /

Create new fileFind fileHistory

 JohnHammond Added writeups for Labour and Banana PrincessLatest commit 69494ee on 7 Feb

..		
 <a href="#">.-000.ppm</a>	Added writeups for Labour and Banana Princess	2 months ago
 <a href="#">.-001.ppm</a>	Added writeups for Labour and Banana Princess	2 months ago
 <a href="#">MinionQuest.pdf</a>	Added writeups for Labour and Banana Princess	2 months ago
 <a href="#">README.md</a>	Added writeups for Labour and Banana Princess	2 months ago
 <a href="#">new-1_1.jpg</a>	Added writeups for Labour and Banana Princess	2 months ago
 <a href="#">new.pdf</a>	Added writeups for Labour and Banana Princess	2 months ago
 <a href="#">pdf.png</a>	Added writeups for Labour and Banana Princess	2 months ago

 README.md

# Banana Princess

John Hammond | Monday, February 6th, 2017

The princess has been kidnapped! It is up to you to rescue her now, with the help of the minions. They have provided you with a letter (which may or may not have touched the kidnappers hands on its way to you).

Authors - Speeddy, Blaze

This was the first crypto challenge, worth 20 points.

We were given a [PDF](#) file [to download](#); but the thing was broken, we couldn't load it into a viewer or really read anything out of it.

I ran `file` on the file for some simple and easy recon, but there was really nothing interesting there.

```
$ file MinionQuest.pdf
MinionQuest.pdf: data
```

Next I opened up in [hexedit](#) (again to get a better idea of what is really up with this file) and everything looked like gibberish. Some of the text looked like [base64](#), so I tried to decode it but nothing worth while.

Eventually, after staring at it for way too long, I took a look at the very top of the file.

I saw that the file started with bytes representing:

```
%CQS-1.5.
```

And this looked super weird, [because it should be](#) `PDF` , but it looked similar to it. On a hunch and gut feeling, I started to check the difference between those letters.

```
>>> ord('P') - ord('C')
13
>>> ord('D') - ord('Q')
-13
```

```
>>> ord('F') - ord('S')  
-13
```

Aha. Thirteen. That encourages my hunch. I grabbed a random string and tested it:

```
$ strings MinionQuest.pdf | head  
%CQS-1.5  
4 0 bow  
<</Yvarnevmrq 1/Y 430190/B 6/R 404343/A 1/G 429991/U [ 576 155]>>  
raqbow  
  
kers  
4 14  
0000000016 00000 a  
0000000731 00000 a  
0000000791 00000 a
```

I wanted to see if it was simply ROT13'd...

```
$ echo "Yvarnevmrq" | rot13  
Linearized
```

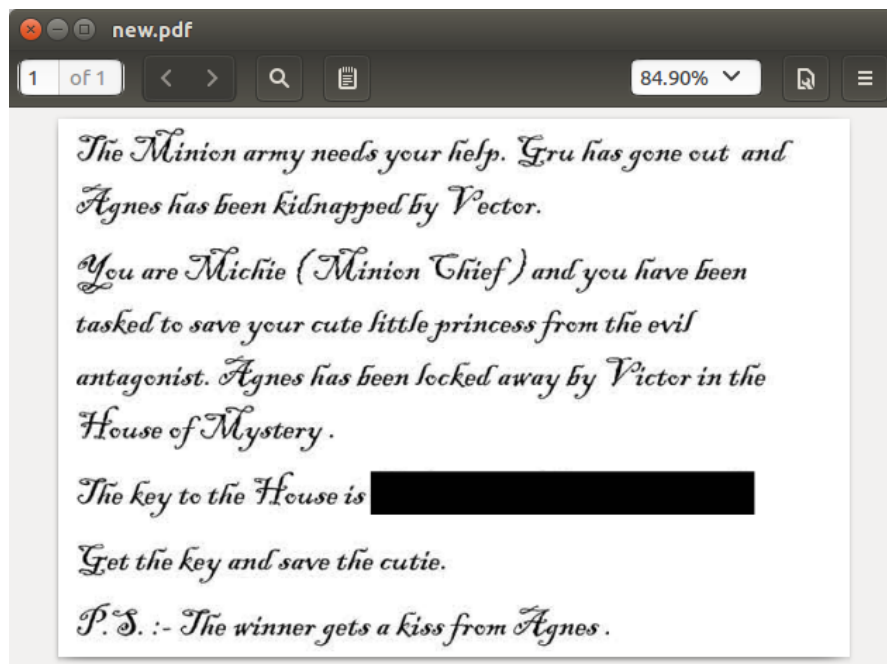
Yup, that's totally a valid PDF element tag.

**The whole PDF file must have been ROT13'd!**

Now to correct it:

```
$ cat MinionQuest.pdf | rot13 > new.pdf  
new.pdf: PDF document, version 1.5
```

Got it. Now let's check it out.



Of course, they censored the flag.

I tried to pull anything out of the PDF with `pdftotext`. I was able to pull out the original picture and see the flag!

*The Minion army needs your help. Gru has gone out and Agnes has been kidnapped by Vector.*

*You are Michie (Minion Chief) and you have been tasked to save your cute little princess from the evil antagonist. Agnes has been locked away by Victor in the House of Mystery.*

*The key to the House is `BITSCTF{save_the_kid}`*

*Get the key and save the cutie.*

*P.S. :- The winner gets a kiss from Agnes.*

The flag was: `BITSCTF{save_the_kid}`

