Michael Vu

CSAW CTF 2016 Quals: Fuzyll

Category: Recon

Points: 200

Solves: 128

Description: All files are lowercase with no spaces. Start here: http://fuzyll.com/files/csaw2016/start

Write Up:

Going to the start you are given this message:

> *CSAW 2016 FUZYLL RECON PART 1 OF ?: People actually liked last year's challenge, so CSAW made me do it again... Same format as last year, new stuff you need to look up. The next part is at /csaw2016 /<the form of colorblindness I have>*

Stalking him on Twitter reveals some tweets that give a hint to what kind of color blindness he had. Of course you could also brute force it.

> *My wife just dropped a bomb on me today: Pistachios are, and have always been, green. MIND. BLOWN.*

The next part to this challenge is here: http://fuzyll.com/files/csaw2016/deuteranomaly

You'll see an image of brownish strawberries; presumably what color blind people see. If you download the image, it'll be downloaded normally as a txt file. If you open the file, you'll see this in the exif:

> *CSAW 2016 FUZYLL RECON PART 2 OF ?: No, strawberries don't look exactly like this, but it's reasonably close. You know what else I can't see well? /csaw2016/<the first defcon finals challenge i ever scored points on*

So after doing some searching, we find that his first DefCon Finals was 19 and that he was on a team called "Hates Irony". By simply brute forcing it, we find that it was tomato.

The next part to this challenge is here: http://fuzyll.com/files/csaw2016/tomato

So after going to the URL you'll find gibberish like this:

> *ÃâÁæ@òðñö@ÆäéèÓÓ@ÙÅÃÖÕ@×ÁÙã@ó@–†@oz@É@„–*
> *•}£@…¥…•@“‰’…@£–”£–…¢Z@Á•¨¦ k@–¤£¢‰„…@–*
> *†@ÃãÆ¢k@É}¥…@,……•@—“¨‰•‡@@†‰™@”–¤•£@–†@æ–™“„@–*
> *†@æ™Ã™†£@–¥…™@£ˆ…@—¢£@¨…™@M•…¥… ™@£ˆ–*
> *¤‡ˆ£@É}„@,…@¢¨‰•‡@£ˆ£@†£…™@Ã£ƒ“¨¢”k@,¤£@ˆ…™…@¦…@*
> *™…]K@ãˆ…@•…§£@—™£@‰¢@£@af¢¦òðñöaL”¨@”‰ •@æ–*
> *æ@fˆ™ƒ£…™}¢@•”…nK*

Initially I believed that it was a character encoding error and from his LinkedIn I assumed that it was a Japanese encoding originally. I was wrong however, and after googling some parts of the string, I was

able to determine that it was actually a Cyrillic encoding, CP933 specifically, and after you convert it you get this:

> *CSAW 2016 FUZYLL RECON PART 3 of ?: I don't even like tomatoes! Anyway, outside of CTFs, I've been playing a fair amount of World of WarCraft over the past year (never thought I'd be saying that after Cataclysm, but here we are). The next part is at /csaw2016/ <my main WoW character's name>.*

Well I knew nothing about WoW so I was looking up stuff on forums and got nowhere. We figured out from his blog that he was a part of a guild called 'Blackfathom Deep Dish' on US-Turalyon. We then used another website to track down the members and based off the join dates he determined that his IGN was elmrik.

The next part to this challenge is here: http://fuzyll.com/files/csaw2016/elmrik

So you were given this piece of code:

```
#!/usr/bin/env ruby

CHARS = ["0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "B", "C", "D",
       "F", "G", "H", "J", "K", "L", "M", "N", "P", "Q", "R", "S", "T",
       "V", "W", "X", "Y", "Z", "b", "c", "d", "f", "g", "h", "j", "k",
       "l", "m", "n", "p", "q", "r", "s", "t", "v", "w", "x", "y", "z"]

def encode(string)
   input = string.bytes.inject {|x, y| (x << 8) + y }
   output = ""
   while input > 0
      output = CHARS[input % 52].to_s + output
      input /= 52
   end
   return output
end

def decode(input)
   # your implementation here
end

message =
"JQSX2NBDykrDZ1ZHjb0BJt5RWFkcjHnsXvCQ4LL9H7zhRrvVZgLbm2gnXZq71Yr6T14tXNZwR1Dld2Y7M0nJsjgv
hWdnhBll5B8w0VP3DFDjd3ZQBlcV4nkcFXBNzdPCSGMXQnQ7FTwcwbkG6RHX7kFHkpvgGDDGJvSDSTx7J6MF
hRmTS2pJxZCtys4yw54RtK7nhyW6tnGmMs1f4pW6HzbCS1rSYNBk3PxzW9R1kJK54R2b7syLXd7x1Mr8GkMsg4
bs3SGmj3rddVqDf4mTYq1G3yX1Rk9gJbj919Jw42zDtT2Jzz4gN0ZBmXPsBY9ktCLPdFrCPZ33NKJy5m37PK0GLXB
xZz9k0cjzyt8x199jMsq7xrvNNgDNvgTbZ0xjZzHhkmrWrCmD7t4q4rWYFSJd4MZBxvnqc0VgGzdkq8jSJjnwcynq9
VfH22WCQSdPKw48NkZL7QKGCT94pSb7ZSl2G6W37vBlW38q0hYDVcXTTDwr0l808nDPF6Ct1fPwKdNGKbRZ3
Q3lHKMCYBC3w8l9VRjcHwMb1s5sMXM0xBvF8WnWn7JVZgPcXcwM2mDdfVkZsFzkrvVQmPfVNNdk9L5WtwD
D8Wp9SDKLZBXY67QkVgW1HQ7PxnbkRdbnQJ4h7KFM2YnGksPvH4PgW2qcvmWcBz62xDT5R6FXJf49LPCKL8
MQJLrxJpQb7jfDw0fTd00dX1KNvZsWmfYSTl1GxPlz1PvPSqMTQ036FxSmGb6k42vrzz2X90610Z"

puts decode(message)
```

The encoding scheme was base 52 and once you broke the code you got this:

> *CSAW 2016 FUZYLL RECON PART 4 OF ?: In addition to WoW raiding, I've also been playing a bunch of Smash Bros. This year, I competed in my first major tournament! I got wrecked in every event I competed in, but I still had fun being in the crowd. This tournament in particular had a number of upsets (including Ally being knocked into losers of my Smash 4 pool). On stream, after one of these big upsets in Smash 4, you can see me in the crowd with a shirt displaying my main character! The next part is at /csaw2016/<the winning player's tag>.*

It was pretty easy to figure out that he was at CEO 2016, and thanks to a fantastic Reddit Community and a bit of brute forcing we find out that the winning player's match of the stream he was on was Jade winning 2-1 over Trela.

https://www.reddit.com/r/smashbros/comments/4pnkud/ceo_2016_smash_4_singles_upsets_day_1/

The next part to this challenge is here: http://fuzyll.com/files/csaw2016/jade

You are given a GNU zip file and once you unzip it, given that you are on Linux, you can determine that the file inside is an image.

The EXIF contains this:

> *CSAW 2016 FUZYLL RECON PART 5 OF 6: I haven't spent the entire year playing video games, though. This past March, I spent time completely away from computers in Peru. This shot is from one of the more memorable stops along my hike to Machu Picchu. To make things easier on you, use only ASCII: /csaw2016/<the name of these ruins>*

After using the reverse Google Images search I found that it was Wiñay Wayna, or Winay Wayna.

The final part to this challenge is here: http://fuzyll.com/files/csaw2016/winaywayna

> *CSAW 2016 FUZYLL RECON PART 6 OF 6: Congratulations! Here's your flag{WH4T_4_L0NG_4ND_STR4NG3_TRIP_IT_H45_B33N}.*

Flag

flag{WH4T_4_L0NG_4ND_STR4NG3_TRIP_IT_H45_B33N}