

TerraMeow 50

by a.krontab / 2amResearch

Tags: [miscellaneous](#) [misc](#)

Rating: 5.0

This was a pretty simple challenge if you have some knowledge of terraform. We are given the `tf` files for the challenge and see that there is a variable named `FLAG`. We also see in the challenge script that if the flag is in the output then we get a monkey as the output an no flag. So we need a terraform function that modified the variable value in some way.

After checking the Terraform console function docs we see there is a function called `strrev` which reverses the value it's given. Why you would even need this in an IaC tool is beyond me, but a flag is a flag, so let's give it a try.

```
(kali@kali:)[~/Desktop/terraform]
└─$ nc 172.190.120.133 50002

[+] Welcome challenger to the epic IAC Madness
Enter terraform console commands (Enter an empty line to
strrev(flag))

")3t4T_0rDnA_3t4Ts_fT(hg4uLx0"

(kali@kali:)[~/Desktop/terraform]
└─$ echo ")3t4T_0rDnA_3t4Ts_fT(hg4uLx0" | rev
0xk4ugh{f_sT4t3_AnDr0_T4t3}
```

Flag: 0xL4ugh{Tf_sT4t3_AnDr0_T4t3}

GitMeow 50

by a.krontab / 2amResearch

Tags: [misc](#) [miscellaneous](#)

Rating: 5.0

We are given a prompt to enter git commands. After some trial and error we can see that the `git grep` command is allowed. Knowing the flag format is `0x14ugh[something]` we can use `grep` and that should find all files that have the string `ugh` and should print out the flag.

```

kali@kali:~/Desktop/git]$ nc 172.190.120.133 50001

  _ _ _ _ _
 | _ ( ) | | \ |
 | | \ | | | . | _ _ _ _ _
 | | _ | | | | / _ \ \ \ \ /
 | | \ | | | | | _ ( ) \ \ \ /
  _ _ _ _ _ | _ _ _ _ _ \ \ \
                _ _ _ _ _

[+] Welcome challenger to the epic GIT Madness, can you read /flag.txt?
Enter git commands (Enter an empty line to end):

grep ugh

flag.txt:0xL4ugh[GiT_D0c3_F0r_Th3_Win}

```

Flag: 0xL4ugh{GiT_D0c3_F0r_Th3_WiN}

Library 50

by [a.kronlab](#) / [2amResearch](#)

Tags: [misc](#) [miscellaneous](#)

Rating:

This was a fun challenge that gave us a prompt in a custom library management software. Two interesting options are `7.Save Book` and `8.Check File Presence`. After reviewing the source code we see that with option 8 there might be possibility for some command injection. Some testing showed that only the `ls` command could be executed so if we gave it the `-l` flag, maybe we could see something interesting in the filesystem.

```
(kali㉿kali)-[~/Desktop/Library]
└─$ nc 172.190.120.133 50003

Library Management System
1. Add Member
2. Add Book
3. Display Books
4. Search Book
5. Check Out Book
6. Return Book
7. Save Book
8. Check File Presence
0. Exit
Enter your choice (0-8): 7

Book Manager:
1. Save Existing
2. Create new book
Enter your choice (1-2): 2
Enter book title: -l
Enter book author: a
Enter book ISBN: a
Enter number of copies: 1
Book saved successfully
```

```
Book Manager:
1. Save Existing
2. Create new book
Enter your choice (1-2): 2
Enter book title: -l
Enter book author: a
Enter book ISBN: a
Enter number of copies: 1
Book saved successfully

Library Management System
1. Add Member
2. Add Book
3. Display Books
4. Search Book
5. Check Out Book
6. Return Book
7. Save Book
8. Check File Presence
0. Exit
Enter your choice (0-8): 8
Enter the name of the book (file) to check: -l
total 44
-rw-r--r--  1 challeng challeng      9 Feb  9 22:33 -l
-rw-r--r--  1 challeng challeng      9 Feb  9 19:37 0xL4ugh{TrU5t_M3_L1F3_I5_H4rD3r!}
-rw-r--r--  1 challeng challeng      9 Feb  9 17:18 ;id;
-rw-r--r--  1 challeng challeng      9 Feb  9 17:27 a
-rw-r--r--  1 challeng challeng      9 Feb  9 19:11 alo
-rw-rw-r--  1 root    root          8975 Jan 31 22:43 challenge.py
-rw-rw-r--  1 root    root          103 Jan 31 22:19 exec.sh
-rw-r--r--  1 challeng challeng      9 Feb  9 18:07 thetales of test
-rw-r--r--  1 challeng challeng     11 Feb  9 20:53 {library}
The book is not found in the current directory.
```

Looks like there was a file named with the flag format and if we try it that seems to work. My guess is that the file needed to be created with the `{FLAG}` variable as the name and then we could read the file system to get the flag. Cheers to who ever figured it out and got the file created with the flag name!

Flag: `0xL4ugh{TrU5t_M3_L1F3_I5_H4rD3r!}`

Lost In History 50

by [a.krontab](#) / [2amResearch](#)

Tags: [osint](#)

Rating: 3.0

Description

MM0X and xElessaway were in a mission to find someone but seems they had a stalker and got us this picture of them both. can you identify the place they were?

Flag Format: 0xL4ugh{The Name of the place with spaces}

Solution

There's no Exif info on the photo so that lead is a dead end.

We can google the username xElessaway and find his instagram. There's a photo with a place that has similar walls and floors which is the [National Museum Of Egyptian Civilization](#). So we plug that into the flag and get:

Flag: 0xL4ugh{National Museum Of Egyptian Civilization}