picoCTF 2019

Aufschrieb

Contents

General Skills

Warm Up

Man übersetzt Hex zu Ascii mit dem befehl xxd. In diesem Fall `echo "0x70" | xxd -r`.

Lösung: picoCTF{p}

Warmed Up

What is 0x3D (base 16) in decimal (base 10).

Die Umrechnung kann man mit Python erreichen. In der Python Shell dann `0x3D` eingeben. Das Ergebnis ist die Lösung.

Lösung: picoCTF{61}

2Warm

Can you convert the number 42 (base 10) to binary (base 2)?

Lösung: picoCTF{101010}

Bases

What does this bDNhcm5fdGgzX3IwcDM1 mean? I think it has something to do with bases.

Ist base64: `echo "bDNhcm5fdGgzX3IwcDM1" | base64 -d`

Lösung: picoCTF{l3arn_th3_r0p35}

First Grep

Can you find the flag in file? This would be really tedious to look through manually, something tells me there is a better way. You can also find the file in /problems/first-grep_2_04dbf496b78e6c37c0097cdfef734d88 on the shell server.

Datei enthält nur Müll: `cat file | grep pico`

Lösung: picoCTF{grep_is_good_to_find_things_bf6aec61}

Resources

Auf der Seite ist die Lösung

Lösung: picoCTF{r3source_pag3_f1ag}

strings it

Can you find the flag in file without running it? You can also find the file in /problems/strings-it_2_865eec66d190ef75386fb14e15972126 on the shell server.

```
strings strings | grep pico
```

Lösung: picoCTF{5tRIng5_1T_d5b86184}

what's net cat?

Using netcat (nc) is going to be pretty important. Can you connect to 2019shell1.picoctf.com at port 21865 to get the flag?

```
ncat 2019shell1.picoctf.com 21865
```

Lösung: picoCTF{nEtCat_Mast3ry_4fefb685}

Based

To get truly 1337, you must understand different data encodings, such as hexadecimal or binary. Can you get the flag from this program to prove you are on the way to becoming 1337? Connect with nc 2019shell1.picoctf.com 20836.

Lösung mit Skripten im Ordner Skripte.

Lösung: picoCTF{learning_about_converting_values_6cdcad0d}

First Grep: Part II

Can you find the flag in /problems/first-grep–part-ii_2_1c866f894e7ef69b77a69a224b0c3f60/files on the shell server? Remember to use grep.

```
cat ./*/* | grep pico
```

Lösung: picoCTF{grep_r_to_find_this_ee829ae6}

plumbing

Sometimes you need to handle process data outside of a file. Can you find a way to keep the output from this program and search for the flag? Connect to 2019shell1.picoctf.com 18944.

```
ncat 2019shell1.picoctf.com 18944 >> ncatoutput.txt
```

Lösung: picoCTF{digital_plumb3r_1d5b7de7}

whats-the-difference

Can you spot the difference? kitters cattos. They are also available at /problems/whats-the-difference_0_00862749a2aeb45993f36cc9cf98a47a on the shell server.

Forensics

Glory of the garden

This garden contains more than it seems. You can also find the file in /problems/glory-of-the-garden_3_346e50df4a37bcc4aa5f6e5831604e2a on the shell server.

`strings file.jpg`

Lösung: picoCTF{more_than_m33ts_the_3y35a97d3bB}

unzip

Can you unzip this file and get the flag?

Einfach unzippen.

Lösung: picoCTF{unz1pp1ng_1s_3a5y}

##What lies within Theres something in the building. Can you retrieve the flag?

Glaube nicht, dass es so "versteckt" war, aber es hat mit dem stego-toolkit geklappt.
`zsteg -a buildings.png | grep pico`

Lösung: picoCTF{h1d1ng_1n_th3_b1t5}

extensions

This is a really weird text file TXT? Can you find the flag?

`file flag.txt` ist eine PNG Datei. `mv flag.txt flag.png` und anschaun.

Lösung: picoCTF{now_you_know_about_extensions}

Shark on wire 1

We found this packet capture. Recover the flag. You can also find the file in /problems/shark-on-wire-1_0_13d709ec13952807e477ba1b5404e620.

Einfach immer wiede rden Streams gefolgt und weg gefiltert.

Lösung: picoCTF{StaT31355_636f6e6e}

Whitepages

I stopped using YellowPages and moved onto WhitePages… but the page they gave me is all blank!

##c0rrupt We found this file. Recover the flag. You can also find the file in /problems/c0rrupt_0_1fcad1344c25a122a00721e4af86de13.

Hint: Try fixing the file header

Cryptography

The numbers

The numbers… what do they mean?

Einfach die Zahlen als Stellen im Alphabet nehmen.

Lösung: PICOCTF{THENUMBERSMASON}

13

Cryptography can be easy, do you know what ROT13 is? cvpbPGS{abg_gbb_onq_bs_n_ceboyrz}

Mit dem eigenen Skript dekodieren.

Lösung: picoCTF{not_too_bad_of_a_problem}

Easy1

The one time pad can be cryptographically secure, but not when you know the key. Can you solve this? We've given you the encrypted flag, key, and a table to help UFJKXQZQUNB with the key of SOLVECRYPTO. Can you use this table to solve it?.

Mit eigenem Skript.

Lösung: picoCTF{CRYPTOISFUN}

caesar

Decrypt this message. You can find the ciphertext in /problems/caesar_4_33e5994add902b2321c8c38c8b962eff on the shell server.

Mit eigenem Skript.

Lösung: picoCTF{crossingtherubiconljmawiae}

Flags

What do the flags mean?

Mr-Worldwide

A musician left us a message. What's it mean?

Sind Koordinaten. Anfangsbuchstaben der Städte ergeben die Lösung.

Lösung: picoCTF{KODIAK_ALASKA}

Tapping

Theres tapping coming in from the wires. What's it saying nc 2019shell1.picoctf.com 12285.

Ist Morsecode.

Lösung: PICOCTF{M0RS3C0D31SFUN1137903549}

la cifra de

rsa-pop-quiz

Class, take your seats! It's PRIME-time for a quiz… nc 2019shell1.picoctf.com 53028

Lösungen sind wie folgt:

$N = p \cdot q$

$tantient(n) =? \Rightarrow$ Rechner im Netz

$p^e < N \rightarrow p^e = c$

Webexploitation

Insp3ct0r

Kishor Balan tipped us off that the following code may need inspection: https://2019shell1.picoctf.com/problem/52962/ (link) or http://2019shell1.picoctf.com:52962

Einfach den Inspect Element!!

Lösung: picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?39dd9e36}

Binary Exploitation