

This repository | Search

Pull requests Issues Gist



ctfs / write-ups-2014

Watch

219

Star

1,279

Fork

457

<> Code

Issues 15

Pull requests 0

Projects 0

Pulse

Graphs

Branch: master

write-ups-2014 / plaid-ctf-2014 / parlor /

Create new file

Upload files

Find file

History

abpolym New writeup for phdays-quals freeBDSM! Latest commit f9138e4 on Feb 1 2015

README.md

New writeup for phdays-quals freeBDSM!

2 years ago

README.md

Plaid CTF 2014: parlor

Category: Crypto Points: 250 Description:

The Plague is running a betting service to build up funds for his massive empire. Can you figure out a way to beat the house?

The service is running at 54.197.195.247:4321.

Write-up

```
$ nc 54.197.195.247 4321
```

```
/-----\
| Welcome to the betting parlor!
|
| We implement State of the Art cryptography to give you the fairest and most
| exciting betting experience!
|
| Here's how it works: we both pick a nonce, you tell us odds, and you give us
| some money.
| If md5(our number + your number) % odds == 0, you win bet amount*odds.
| UPDATE: IF YOU DIDN'T REALIZE IT, WE DO INCLUDE A NEWLINE AT THE END OF YOUR
| NUMBER. SORRY FOR THE INCONVENIENCE. THANK YOU FOR USING PARLOR
| Otherwise, we get your money! We're even so nice, we gave you $1000 to start.
|
| If you don't trust us, we will generate a new nonce, and reveal the old nonce
| to you, so you can verify all of our results!
|
| (Oh, and if you win a billion dollars, we'll give you a flag.)
\-----/
```

```
=====
1) set your odds
2) set your bet
3) play a round
4) get balance
5) reveal nonce
6) quit
=====
```

(TODO)

Other write-ups and resources

- <http://blog.mheistermann.de/2014/04/14/plaidctf-2014-parlor-crypto-250-writeup/>
- <http://mslc.ctf.su/wp/plaidctf-2014-parlor-writeup/>
- <https://fail0verflow.com/blog/2014/plaidctf2014-crypto250-parlor.html>
- Source code for this challenge, released after the CTF

- <http://blog.ztrix.me/blog/2014/04/14/plaidctf-2014-parlor-writeup/>

