A DISTURBING LACK OF TASTE

Writeups   **About**

A DISTURBING LACK OF TASTE

☰

2014-01-15

Hack you 2014 CTF - Writeup Net100-Web100-Crypto100-Rev100

Easy peasy tasks:

Web100:

just set in the URL
id=0x3120616e6420313d3220756e696f6e2073656c65637420666c61672066726f6d20466

so we bypass is_numeric() check and then in 2nd and 3rd query we can inject basically what we want as a normal injection.

Net100:

http://pastebin.com/n7m6ZpaP

digest access authentication method applied here. Just a bit of bruteforce for the password and then break it.

Crypto100:

http://pastebin.com/5VPPvU05

Just recover the key + some bruteforce on chars range (0x1-0xff) to break encryption algorithm without reversing it.

Rev100:

dotPeek decompiler do the job. just read the challenge binary and with some xor/mod stuff recover the flag with known "key":

http://pastebin.com/mvtAtA8i

Razor4x