SUSlo.PAS CTF Team blog. Write-ups, news, etc

March 16, 2014

RuCTF: Crypto 100 (MD5)

We have a remote service and a part of its source code:

```
------------------------------
    buf = c.recv(4096)
    digest, msg = buf.split(" ", 1)
    if (digest == md5(password+msg).hexdigest()):
        #here I send a secret
    else:
        c.send("Wrong signature\n")
------------------------------
```

Obviously, it is just a hash length extension attack that can be easily used with hash_extender.
Hash_extender cmdline is:
hash_extender.exe -f md5 -d='do test connection' -s b34c39b9e83f0e965cf392831b3d71b8 -a azaza --secret-min=1 --secret-max=16 --out-data-format=cstr
Now we just manually bruteforce all the lengths, 15 gives us the flag:
Final cmdline:
echo -ne 'ed766f6b30cc8315cede90553d7eeec1
do\x20test\x20connection\x80\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x08\x01\x00\x00\x00\x00\x00\x00azaza' | nc python27.quals.ructf.org 12337
Answer is:
Message accepted! The answer is RUCTF_CryptoIsFunAndEasy

Автор: Роман Лебедев на 3/16/2014 07:41:00 AM

No comments:

Post a Comment

Enter your comment...

Comment as: Select profile...

Publish Preview

Newer Post Home Older Post