README.md

31C3 CTF 2014: sso

Category: crypto Points: 30 Solves: 72 Description:

> In a world, where everybody and their mom rolls out their own crypto implemented PHP, Joe plays it safe with Standard Crypto. http://188.40.18.87:5144/

Write-up

By HoLyVieR

The encryption used was done character by character, and we could decrypt any token of our choice with the `info.php` page. With this in mind, we could bruteforce each character individually until we get the character of our choice once decrypted. This would then let us craft a token with the value of our choice. Here's an example of a decrypted token that worked:

```
{"User":"admin","Admin":1}
```

Code:

```
import httplib

target = '{"User":"admin","Admin":1}'
conn = httplib.HTTPConnection('188.40.18.87:5144')

def getvalue(token):
        conn.request('GET', 'http://188.40.18.87:5144/info.php?token=%s' % (token), '')
        return conn.getresponse().read()

# We get this part of the token by simply using a token generated for any user
token = '69222e97316b9dd8f7'

for j in range(len(token) / 2, len(target)):
        for i in range(256):
                h = hex(i)[2:]
                if len(h) == 1:
                        h = '0' + h

                r = getvalue(token + h)

                if r == target[:len(r)]:
                        token += h
                        break

        print(token)
```

Then we had to visit `http://188.40.18.87:5144/admin.php?token=INSERT_TOKEN_HERE` .

Other write-ups and resources

- http://www.crimsonagents.com/2015/01/31c3ctf-crypto-sso.html