

Writeup

Team Herald

Hack Today 2020
9 AGUSTUS 2020

Contents

Web - BabyPHP.....	1
Forensic - Nothosaurus.....	2
Forensic - Harta-Karun.....	3
Forensics - Kataware - Doki.....	4
Forensics - Stegosaurus	6
Misc - Sanity Check	7
Misc - O-seen.....	8
Misc - Insanity Check.....	9
Misc - O-seen 2.....	10
Misc - Hard Rock Casino	11
Misc - Ulti-Insanity Check.....	13

Web - BabyPHP

1. Diberikan link yaitu <http://chall.codepwnda.id:15011/>
2. Ketika dibuka, keluar kode dalam php, flag di encode dengan menggunakan sha1 sehingga kita harus mendecodenya dengan fungsi berikut

```

Set as interpreter
1  #!/usr/bin/env python
2
3  import hashlib
4
5  i=0
6  while (True):
7      plaintext = "0e%d" % i
8      hasher = hashlib.sha1()
9      hasher.update(plaintext.encode('utf-8'))
10     h = hasher.hexdigest()
11
12     if h.startswith('0e'):
13         if h[2:].isdigit():
14             print(plaintext, h)
15             break
16     i+=1
17

```

3. Kemudian, setelah menunggu beberapa saat akan mendapatkan output berupa kode yaitu

```

PS C:\Users\graci> & python "c:/Users/graci/Dropbox/My PC (LAPTOP-EHIQPF20)/Documents/CTF/hacktoday/penyisihan/babyPHP.py"
0e1290633704 0e19985187802402577070739524195726831799
PS C:\Users\graci> & python "c:/Users/graci/Dropbox/My PC (LAPTOP-EHIQPF20)/Documents/CTF/hacktoday/penyisihan/babyPHP.py"
Traceback (most recent call last):
  File "c:/Users/graci/Dropbox/My PC (LAPTOP-EHIQPF20)/Documents/CTF/hacktoday/penyisihan/babyPHP.py", line 20, in <module>
    print(b64encode(flag)[1:])

```

4. Dengan menggunakan curl "http://chall.codepwnda.id:15011/?baby=0e1290633704" diperoleh output
`print(b64encode(flag)[1:])`

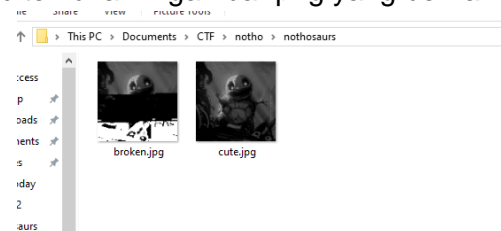
GFJa3RvZGF5e3NlbGFtYXRfZGF0YW5nX2RpX3NvYWxfZD2VifQ==

Enjoy ur Flag !

5. Kemudian decode dengan base64 hanya keluar 'X^^[[X]][W[X]', maka dicoba menghilangkan char satu per satu dari depan hingga didapat 'a3RvZGF5e3NlbGFtYXRfZGF0YW5nX2RpX3NvYWxfZD2VifQ==' yang apabila di decode dengan base64 menghasilkan kode 'ktoday{selamat_datang_di_soal_web}' dan karena format flag dalam bentuk ^hacktoday{w+}\$ maka didapat flag yaitu **hacktoday{selamat_datang_di_soal_web}**

Forensic - Nothosaurus

1. Pada nothosaurus diberi 5 file dengan okay, ill, be, today, again.
2. Ketika dilihat dengan edit notepad dapat dilihat bahwa file okay adalah file header dari tipe file zip dan file again adalah file footer/akhir dari file zip itu. Maka dapat diasumsikan bahwa kelima file ini adalah 1 file zip yang dipisah-pisah sehingga perlu digabungkan lagi.
3. Kami menggunakan fungsi concatenate dari hxd hex editor untuk menggabungkan kelima file. Karena urutan 3 file sisa tidak diketahui, maka dicoba2 saja karena total kemungkinan kombinasi hanya 6.
4. Lalu didapat dengan urutan okay-today-ill-be -again dan disave sebagai file zip. Di dalam file zip ini akan ditemukan 2 gambar png yang bernama broken dan cute.



5. Karena didapat 2 buah gambar yang mirip, maka dilakukan pengecekan perbedaan dari kedua file menggunakan 'diff' pada terminal

```

null@Null: ~/Desktop/Bad boy
null@Null:~/Desktop/Bad boy$ diff broken.jpg cute.jpg
Binary files broken.jpg and cute.jpg differ
null@Null:~/Desktop/Bad boy$
  
```

6. Setelah diketahui ada perbedaan, perbedaan yang ada dapat dipisah dan dilihat menggunakan cmp broken.png dan cute.png dan untuk merapihkan hasil, digunakan awk dan tr sehingga didapat flag yaitu **hacktoday{broken_image}**

```

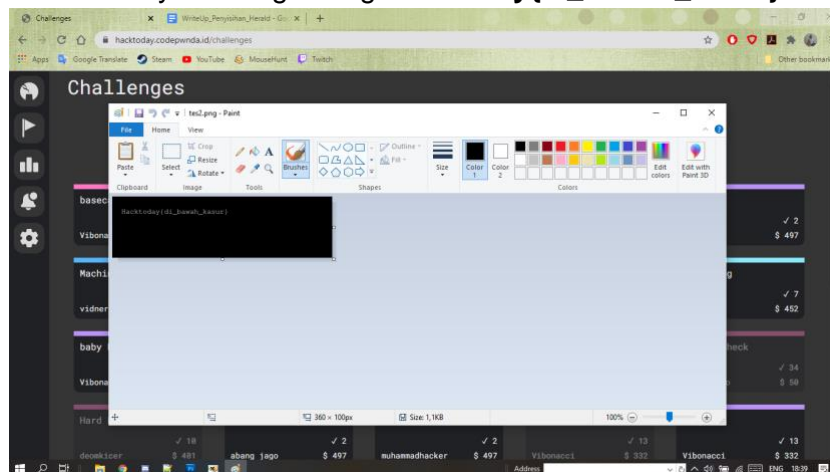
null@Null: ~/Desktop/Bad boy
null@Null:~/Desktop/Bad boy$ cmp -bl broken.jpg cute.jpg | awk '{print $3}' | tr
-d '\n'
hacktoday{broken_image}null@Null:~/Desktop/Bad boy$
  
```

Forensic - Harta-Karun

1. Pada soal ini diberikan sebuah gambar png.
2. Jika dilihat dengan notepad, maka dapat dilihat bahwa setelah footer file png masih terdapat lanjutannya yang juga merupakan file signature zip sehingga dapat disimpulkan bahwa ada file zip yang disembunyikan di dalam file png itu.

The screenshot shows a Notepad++ window with a file named 'C:\Users\Gavin\Downloads\peta.png'. The text content is a mix of ASCII and non-ASCII characters, including the PNG signature 'PNG' and a ZIP signature 'PK' at the end, indicating a hidden ZIP file.

3. Setelah file zip itu dikeluarkan, maka didapat 4 file yaitu ke, lo, sy, en.
4. Jika file ini dilihat dengan notepad, maka diketahui bahwa lo memiliki header png, dan en memiliki footer png sehingga dapat disimpulkan bahwa keempat file ini adalah suatu file png yang dipisahkan.
5. Keempat file digabungkan. Ada 2 kemungkinan urutan yaitu lo-ke-sy-en dan lo-sy-ke-en. Keduanya dapat menghasilkan gambar namun yang memiliki flag adalah file dengan urutan lo-ke-sy-en dengan flag **hacktoday{di_bawah_kasur}**



Forensics - Kataware - Doki

1. Pada soal ini diberikan suatu wav file yang merupakan suara yang digunakan dalam SSTV.
2. Maka digunakan suatu aplikasi yang dapat menerjemahkan suara SSTV ini menjadi suatu gambar. Kelompok kami menggunakan aplikasi RX - SSTV.
3. Untuk membuat kualitas gambar baik, digunakan aplikasi virtual cable agar output suara tidak keluar melalui speaker namun langsung dicerna PC.
4. Aplikasi dijalankan bersama wav file. Didapatkan gambar QR code seperti ini.



5. Ketika QR code dibersihkan dan diterjemahkan menggunakan tools yang disediakan oleh <https://zxing.org/w/decode>, bisa juga menggunakan smartphone, didapat kalimat `shit3ru_you}`.



Decode Succeeded	
Raw text	shit3ru_you}
Raw bytes	40 c7 36 86 97 43 37 27 55 f7 96 f7 57 d0 ec 11 ec 11 ec
Barcode format	QR_CODE
Parsed Result Type	TEXT
Parsed Result	shit3ru_you}

6. Karena flag ini tidak lengkap, maka tentunya ada sesuatu yang masih disembunyikan di file. Diketahui nama soal dan gambar dibalik QR code adalah dari film Kimi no Na wa dan ceritanya ada 2 orang yang terpisah begitu dan banyak sekali promo artinya yang seperti gambar pertama namun ada 2 orang di kanan dan kiri. Maka kami pun terpikir untuk menerjemahkan suara SSTVnya dari audio kanan dan audio kiri.
7. Ketika menggunakan audio kiri, didapatkan gambar yang sama dengan gambar pertama. Namun, ketika menggunakan audio kanan, didapatkan gambar yang berbeda.



8. Setelah QR code dibersihkan dan diterjemahkan didapatkan kalimat `hacktoday{I_`



Decode Succeeded	
Raw text	hacktoday{I_
Raw bytes	40 c6 86 16 36 b7 46 f6 46 17 97 b4 95 f0 ec 11 ec 11 ec
Barcode format	QR_CODE
Parsed Result Type	TEXT
Parsed Result	hacktoday{I_

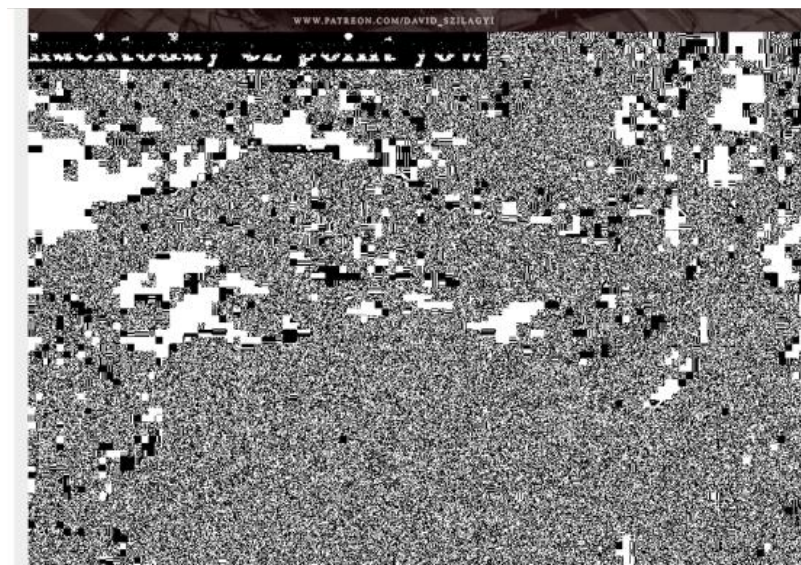
9. Maka kalimatnya digabungkan dan dapat flag **`hacktoday{I_shit3ru_you}`**

Forensics - Stegosaurus

1. Diberi suatu file bendera.txt yang berisi suatu text dari wikipedia tentang stegosaurus dan dibawahnya ada banyak spasi dan tab
2. Spasi dan tab ini adalah suatu steganography yaitu SNOW. Digunakan SNOW untuk mendecode steganography ini. Program yang digunakan didapat dari https://sbmlabs.com/notes/snow_whitespace_steganography_tool/
3. Pada cmd dimasukkan line 'SNOW.EXE -C bendera.txt'

```
C:\Users\          \Desktop>SNOW.EXE -C bendera.txt
https://drive.google.com/file/d/17abT2zPLrVUZJLQ-PbW3qU9L__pihQtJ/view?usp=sharing
```

4. Dari ini didapatkan link menuju suatu google drive yaitu https://drive.google.com/file/d/17abT2zPLrVUZJLQ-PbW3qU9L__pihQtJ/view?usp=sharing
5. Link ini berisi file pokeslow.png
6. Dapat dilihat bahwa bagian pojok kiri atas dari gambar ada sesuatu yang berbeda dari sisa gambarnya dan jika dimainkan kontras gambarnya akan semakin terlihat kejanggalannya. Dari ini dapat diasumsikan ada sesuatu yang disembunyikan di gambar ini melalui steganography
7. Dengan link <https://osric.com/chris/steganography/decode.html>, didapatkan hasil seperti ini.



8. Dapat dilihat ada tulisan di pojok kiri atas gambar yaitu flag **hacktoday{ez_point_yow}**

Misc - Sanity Check

Diberikan link yaitu ipb.link/hacktoday2020-sanity-check yang berisi flag dalam file google docs namun dapat di edit. Sehingga hanya perlu copy paste flag sebelum flag dihapus oleh pemain lain. Flag tersebut adalah
hacktoday{welcome_to_hacktoday_2020_broda__s8jm}

Misc - O-seen

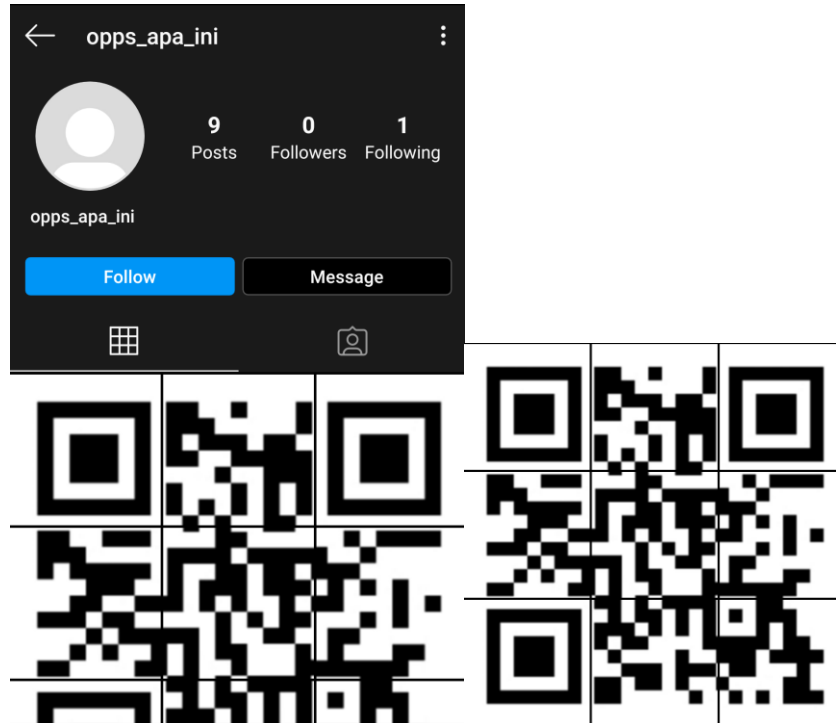
Diberikan attachment gambar berupa salah satu post di instagram hacktoday. Pada post tersebut terdapat komen dari akun instagram hacktoday_fake_flag yang memiliki flag asli di bio instagramnya yaitu **hacktoday{__searching_4_flag__}**

Misc - Insanity Check

Diberikan hint berupa kak friska. Ketika ingin tag @friska di discord, maka akan keluar role yang berupa flag yaitu **hacktoday{ciee_ketawan_ngepoin_friska}**

Misc - O-seen 2

1. Diberikan hint 'no "Follow", no flag. I have flag, so i follow it today.'
2. Maka dilakukan pengecekan follower pada akun instagram @ittoday_ipb
3. Ditemukan akun mencurigakan tanpa foto profil dan username aneh yaitu @opps_apa_ini.
4. Pada feed @opps_apa_ini terdapat 9 post yang masing-masing post merupakan bagian dari sebuah QR code.



5. Dilakukan scan pada qr code dan didapatkan flag **hacktoday{oppsiee_ketemu_deh}**

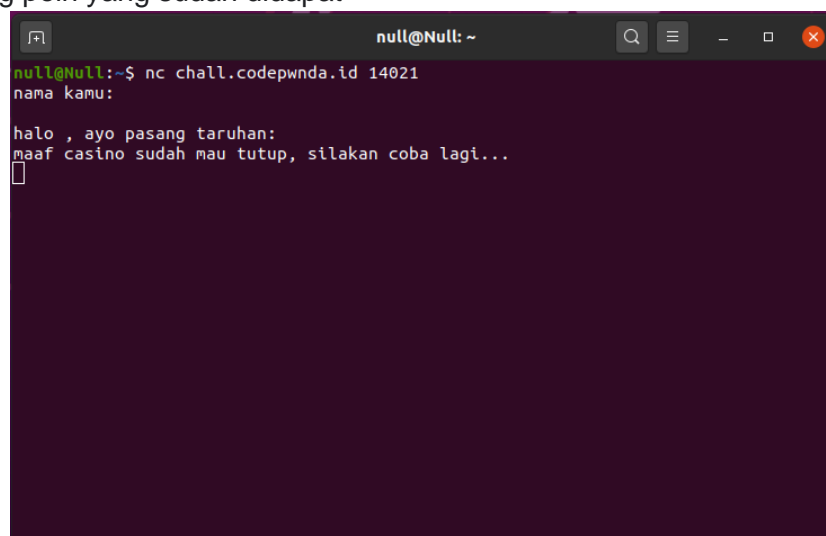
Misc - Hard Rock Casino

1. Diberikan 'nc chall.codepwnda.id 14021' maka dibuka pada terminal dan terdapat sebuah game taruhan, dimana kalau berhasil maka didapatkan poin sebesar yang dipertaruhkan. Dan apabila kalah maka kehilangan poin sebesar yang dipertaruhkan. Poin yang maksimal yang dapat dipertaruhkan adalah jumlah poin yang dimiliki sekarang.



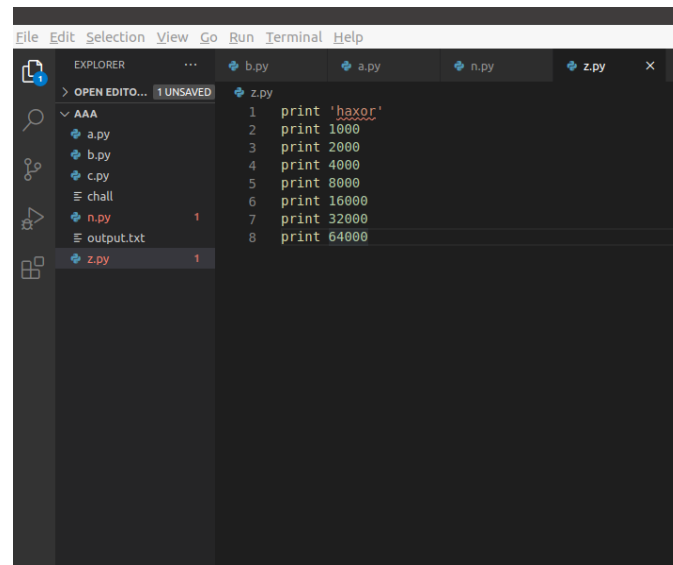
```
nc chall.codepwnda.id 14021
nama kamu:
halo , ayo pasang taruhan:
```

2. Setelah agak lama, didapat bahwa ada batasan waktu untuk bermain dan harus mengulang poin yang sudah didapat

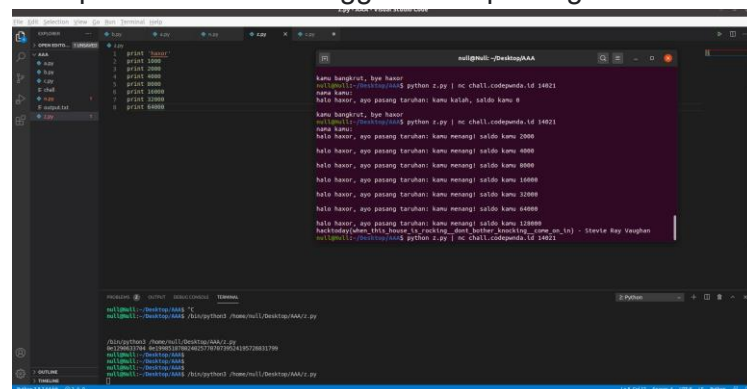


```
nc chall.codepwnda.id 14021
nama kamu:
halo , ayo pasang taruhan:
maaf casino sudah mau tutup, silakan coba lagi...
```

3. Maka dibuatlah sebuah program python untuk menyelesaikan permasalahan ini dengan cara print secara cepat. Karena poin awal 1000 dan target adalah 100000 dan poin menjadi 2 kali lipat apabila selalu mempertaruhkan semua poin maka dibuat program python untuk print nama, 1000, 2000, 4000, 8000, 16000, 32000, 64000.



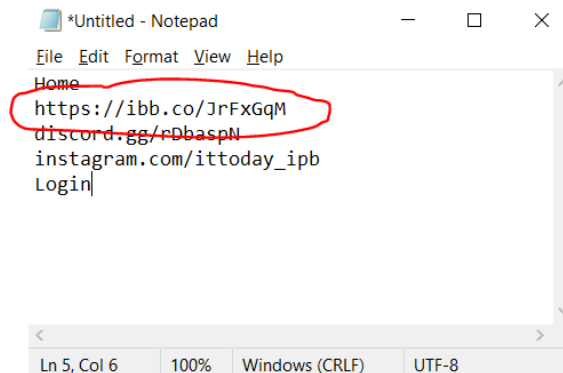
4. Karena untuk mendapatkan poin secara berturut turut memiliki peluang yang kecil, maka file python dijalankan beberapa kali hingga didapat flag. Dijalankan 'python z.py | nc chall.codepwnda.id 14021' hingga mendapat flag.



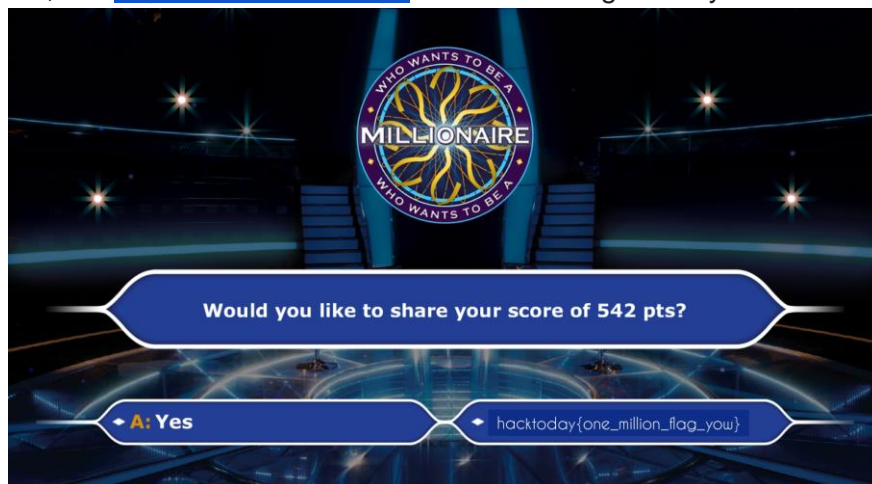
5. Didapat flag
hacktoday{when_this_house_is_rocking__dont_bother_knocking__come_on_i_n}

Misc - Ulti-Insanity Check

1. Diberikan hint bahwa ada sesuatu di website challenges dan disembunyikan.
2. Maka dengan mencoba ctrl+a dan paste di masing-masing page di website lalu di paste di notepad, didapatkan sebuah link yang disembunyikan pada alt attribute dari gambar HackToday pada home. Link ini juga dapat dilihat dari inspect element pada gambar.



3. Saat dibuka, link <https://ibb.co/JrFxGqM> berisi sebuah gambar yaitu



4. Maka didapatkan flag yaitu **hacktoday{one_million_flag_yow}**