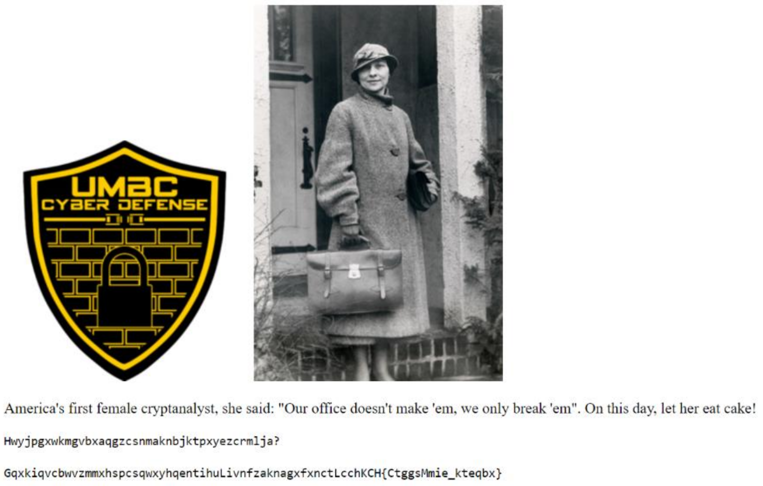
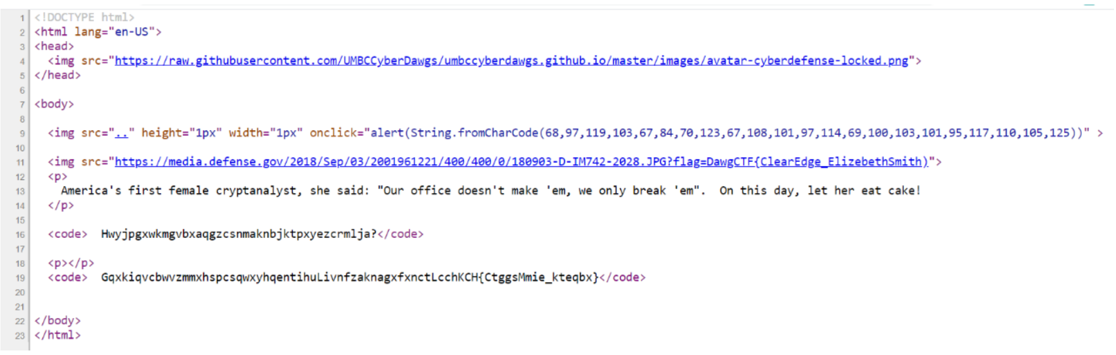
#Chal The Lady is a Smuggler 25



America's first female cryptanalyst, she said: "Our office doesn't make 'em, we only break 'em". On this day, let her eat cake!

```
Hwyjpgxwkmgvbxaqgzcsnmaknbjktpxyezcrmlja?

GqxkiqvcbwvzmmxhspcsqwxyhqentihuLivnfzaknagxfxnctLcchKCH{CtggsMmie_kteqbx}
```

We’re given a URL: https://clearedge.ctf.umbccd.io/, which on opening leads to a webpage with 2 images and 2 lines of text, the lower line of text has curly braces {} which indicates that there might be a flag there. But, since this is a 25 point challenge let’s look at the page source to search for some obvious flags!



```
<!DOCTYPE html>
<html lang="en-US">
<head>
  <img src="https://raw.githubusercontent.com/UMBCCyberDawgs/umbccyberdawgs.github.io/master/images/avatar-cyberdefense-locked.png">
</head>

<body>

  <img src=".." height="1px" width="1px" onclick="alert(String.fromCharCode(68,97,119,103,67,84,70,123,67,108,101,97,114,69,100,103,101,95,117,110,105,125))" >

  <img src="https://media.defense.gov/2018/Sep/03/2001961221/400/400/0/180903-D-IM742-2028.JPG?flag=DawgCTF{ClearEdge_ElizebethSmith)">
  <p>
    America's first female cryptanalyst, she said: "Our office doesn't make 'em, we only break 'em".  On this day, let her eat cake!
  </p>

  <code>  Hwyjpgxwkmgvbxaqgzcsnmaknbjktpxyezcrmlja?</code>

  <p></p>
  <code>  GqxkiqvcbwvzmmxhspcsqwxyhqentihuLivnfzaknagxfxnctLcchKCH{CtggsMmie_kteqbx}</code>


</body>
</html>
```

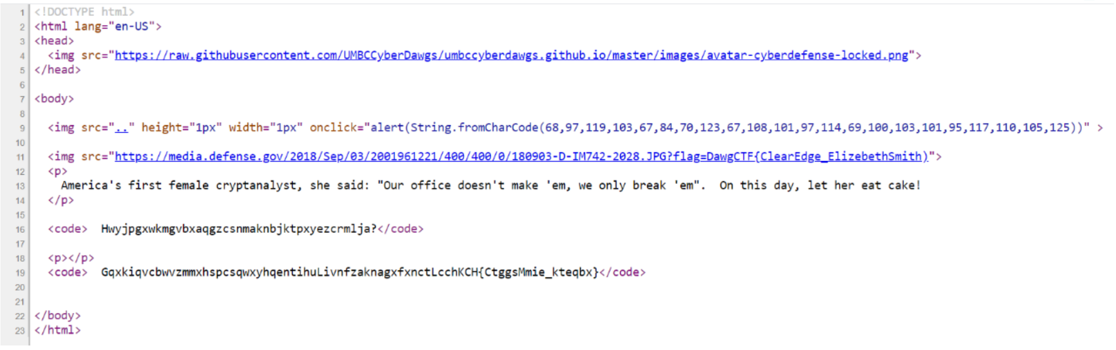
I guess my hunch was right, On opening the source of the page, we see a line in the code: <img src="https://media.defense.gov/2018/Sep/03/2001961221/400/400/0/180903-D-IM742-2028.JPG?flag=DawgCTF{ClearEdge_ElizebethSmith)">

Voila! We found the first flag! :D

Flag: DawgCTF{ClearEdge_ElizebethSmith)

#Chal Tracking 100

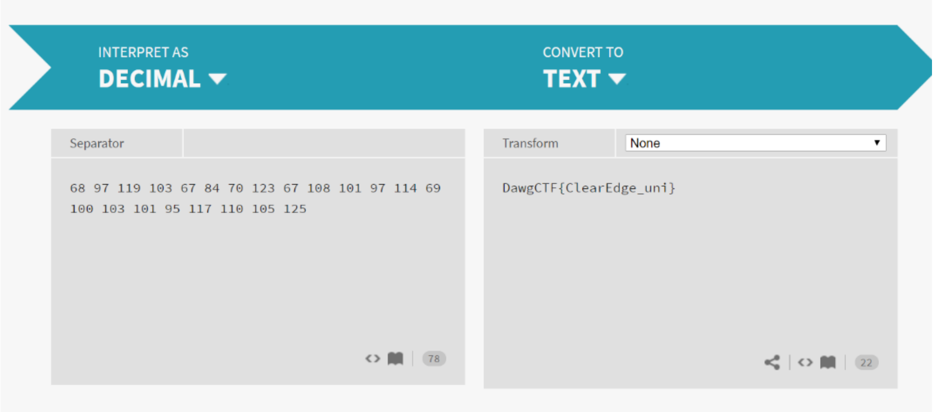
We’re again given the same URL: https://clearedge.ctf.umbccd.io/. Which we saw in the Lady Smuggler challenge before! Let’s once again look at the source of the page for some interesting quirks/hints!



```
<!DOCTYPE html>
<html lang="en-US">
<head>
  <img src="https://raw.githubusercontent.com/UMBCCyberDawgs/umbccyberdawgs.github.io/master/images/avatar-cyberdefense-locked.png">
</head>

<body>

  <img src=".." height="1px" width="1px" onclick="alert(String.fromCharCode(68,97,119,103,67,84,70,123,67,108,101,97,114,69,100,103,101,95,117,110,105,125))" >

  <img src="https://media.defense.gov/2018/Sep/03/2001961221/400/400/0/180903-D-IM742-2028.JPG?flag=DawgCTF{ClearEdge_ElizebethSmith}">
  <p>
    America's first female cryptanalyst, she said: "Our office doesn't make 'em, we only break 'em".  On this day, let her eat cake!
  </p>

  <code>  Hwyjpgxwkmgvbxaqgzcsnmaknbjktpxyezcrmlja?</code>

  <p></p>
  <code>  GqxkiqvcbwvzmmxhspcsqwxyhqentihuLivnfzaknagxfxnctLcchKCH{CtggsMmie_kteqbx}</code>


</body>
</html>
```

I guess my hunch was right once again, On opening the source of the page, we see a line in the code: <img src=".." height="1px" width="1px" onclick="alert(String.fromCharCode(68,97,119,103,67,84,70,123,67,108,101,97,114,69,100,103,101,95,117,110,105,125))" >

The alert function is passing a very interesting ASCII code to Letter conversion as a parameter. Let’s copy the ASCII codes and convert them to text to see what it says:



Transform: None

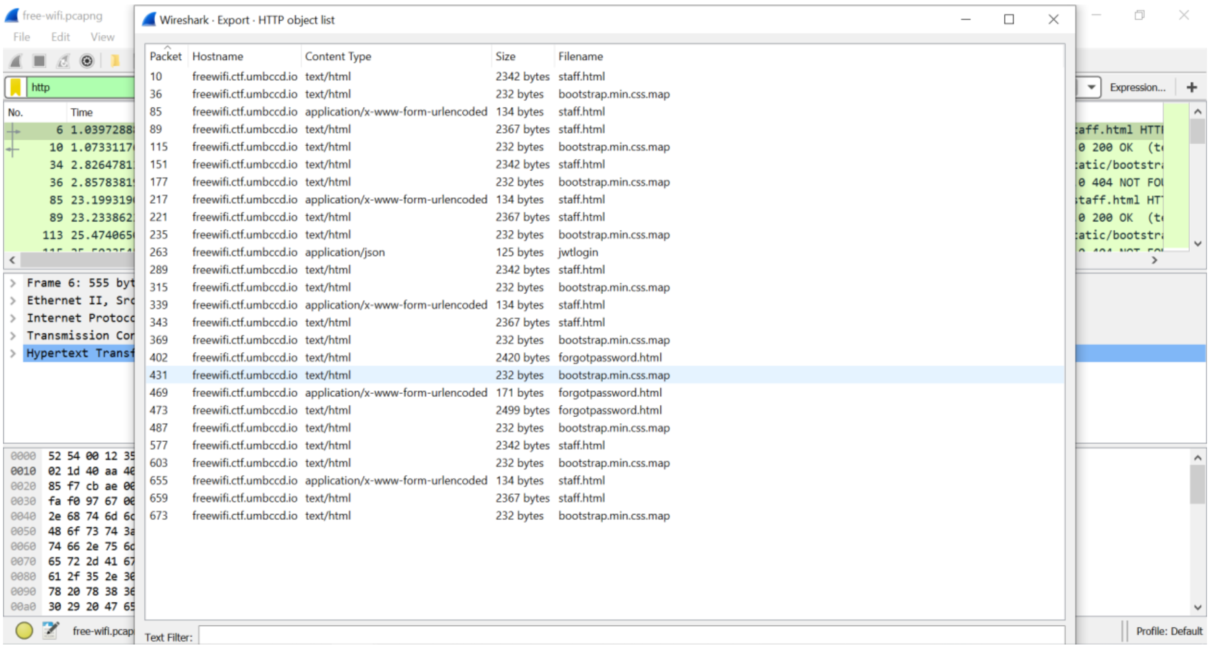
```
68 97 119 103 67 84 70 123 67 108 101 97 114 69
100 103 101 95 117 110 105 125
```

```
DawgCTF{ClearEdge_uni}
```

Voila! We found another flag: DawgCTF{ClearEdge_uni}

#Chal Free Wi-Fi Part 1 50

In this challenge, we're given a URL: http://freewifi.ctf.umbccd.io/, and we're told that it hasn't been implemented as of yet. We're also given a .pcapng file. Let's open wireshark and see what hints we can find! Since our objective is to find data about a URL, let's use the http protocol filter. We find a string of HTTP packets. I used the export http objects to get a list of web pages being referred and opened.

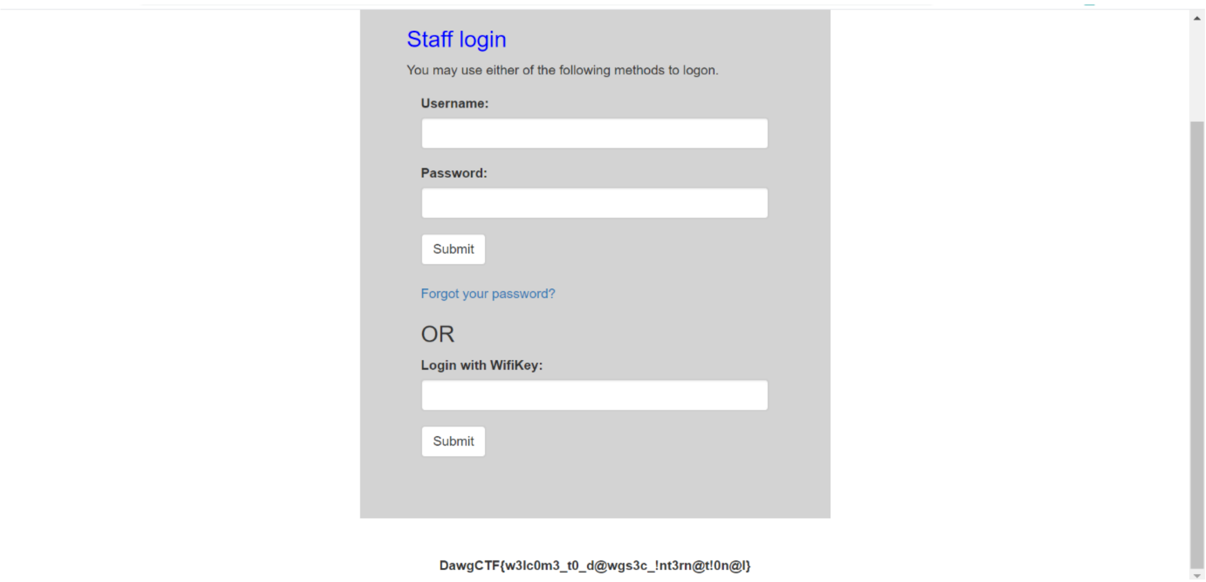


Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
10	freewifi.ctf.umbccd.io	text/html	2342 bytes	staff.html
36	freewifi.ctf.umbccd.io	text/html	232 bytes	bootstrap.min.css.map
85	freewifi.ctf.umbccd.io	application/x-www-form-urlencoded	134 bytes	staff.html
89	freewifi.ctf.umbccd.io	text/html	2367 bytes	staff.html
115	freewifi.ctf.umbccd.io	text/html	232 bytes	bootstrap.min.css.map
151	freewifi.ctf.umbccd.io	text/html	2342 bytes	staff.html
177	freewifi.ctf.umbccd.io	text/html	232 bytes	bootstrap.min.css.map
217	freewifi.ctf.umbccd.io	application/x-www-form-urlencoded	134 bytes	staff.html
221	freewifi.ctf.umbccd.io	text/html	2367 bytes	staff.html
235	freewifi.ctf.umbccd.io	text/html	232 bytes	bootstrap.min.css.map
263	freewifi.ctf.umbccd.io	application/json	125 bytes	jwtlogin
289	freewifi.ctf.umbccd.io	text/html	2342 bytes	staff.html
315	freewifi.ctf.umbccd.io	text/html	232 bytes	bootstrap.min.css.map
339	freewifi.ctf.umbccd.io	application/x-www-form-urlencoded	134 bytes	staff.html
343	freewifi.ctf.umbccd.io	text/html	2367 bytes	staff.html
369	freewifi.ctf.umbccd.io	text/html	232 bytes	bootstrap.min.css.map
402	freewifi.ctf.umbccd.io	text/html	2420 bytes	forgotpassword.html
431	freewifi.ctf.umbccd.io	text/html	232 bytes	bootstrap.min.css.map
469	freewifi.ctf.umbccd.io	application/x-www-form-urlencoded	171 bytes	forgotpassword.html
473	freewifi.ctf.umbccd.io	text/html	2499 bytes	forgotpassword.html
487	freewifi.ctf.umbccd.io	text/html	232 bytes	bootstrap.min.css.map
577	freewifi.ctf.umbccd.io	text/html	2342 bytes	staff.html
603	freewifi.ctf.umbccd.io	text/html	232 bytes	bootstrap.min.css.map
655	freewifi.ctf.umbccd.io	application/x-www-form-urlencoded	134 bytes	staff.html
659	freewifi.ctf.umbccd.io	text/html	2367 bytes	staff.html
673	freewifi.ctf.umbccd.io	text/html	232 bytes	bootstrap.min.css.map

Text Filter:

Through this we can clearly see staff.html is being visited quite often, let's navigate to that URL.



Staff login

You may use either of the following methods to logon.

Username:

Password:

Submit

Forgot your password?

OR

Login with WifiKey:

Submit

DawgCTF{w3lc0m3_t0_d@wgs3c_!nt3rn@t!0n@l}

And Voila! We get the flag, easy peezy lemon squeezy.

Flag: DawgCTF{w3lc0m3_t0_d@wgs3c_!nt3rn@t!0n@l}

#Chal Take It Back Now, Y'all 25

Seems like a pretty easy challenge as the challenge description says, “Sanity check. crypto.ctf.umbccd.io 13370”. It also gives us a python file to: client0.py. On opening the python file we see that the server has 2 methods, and that the flg method will print the flag.

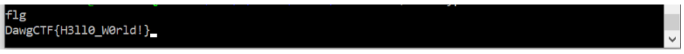
Welcome to my sanity check. You'll find this to be fairly easy.

The oracle is found at umbccd.io:13370, and your methods are:

flg - returns the flag

tst - returns the message after the : in "tst:..."

Now all we need to do is netcat to crypto.ctf.umbccd.io 13370 & type in ‘flg’ to get our flag!



```
flg
DawgCTF{H3ll0_W0rld!}
```

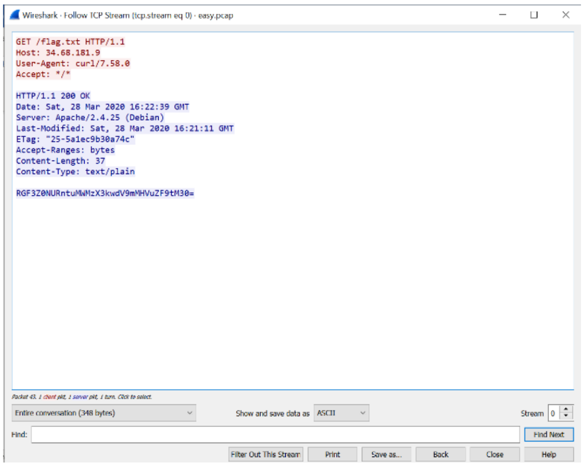
There you go!

Flag: DawgCTF{H3ll0_W0rld!}

#Chal My First Pcap 50

We’re told to “Find the flag in the network traffic” & given a .pcap network traffic capture file. Let’s open wireshark to see what we get, on opening wireshark we find out there are multiple UDP, TCP & HTTP Packets.

Let’s apply the first hack in the forensics wireshark playbook. Follow the TCP Stream (Select a TCP Packet and press Ctrl+ Alt + Shift + T). On following the TCP Stream we get this:



```
GET /flag.txt HTTP/1.1
Host: 34.68.181.9
User-Agent: curl/7.58.0
Accept: */*

HTTP/1.1 200 OK
Date: Sat, 28 Mar 2020 16:22:39 GMT
Server: Apache/2.4.25 (Debian)
Last-Modified: Sat, 28 Mar 2020 16:21:11 GMT
ETag: "25-5a1ec9b30a74c"
Accept-Ranges: bytes
Content-Length: 37
Content-Type: text/plain

RGF3Z0NURntuMWMzX3kwdV9mMHVuZF9tM30=
```

Packet 43. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (348 bytes)

Show and save data as: ASCII

Stream: 0

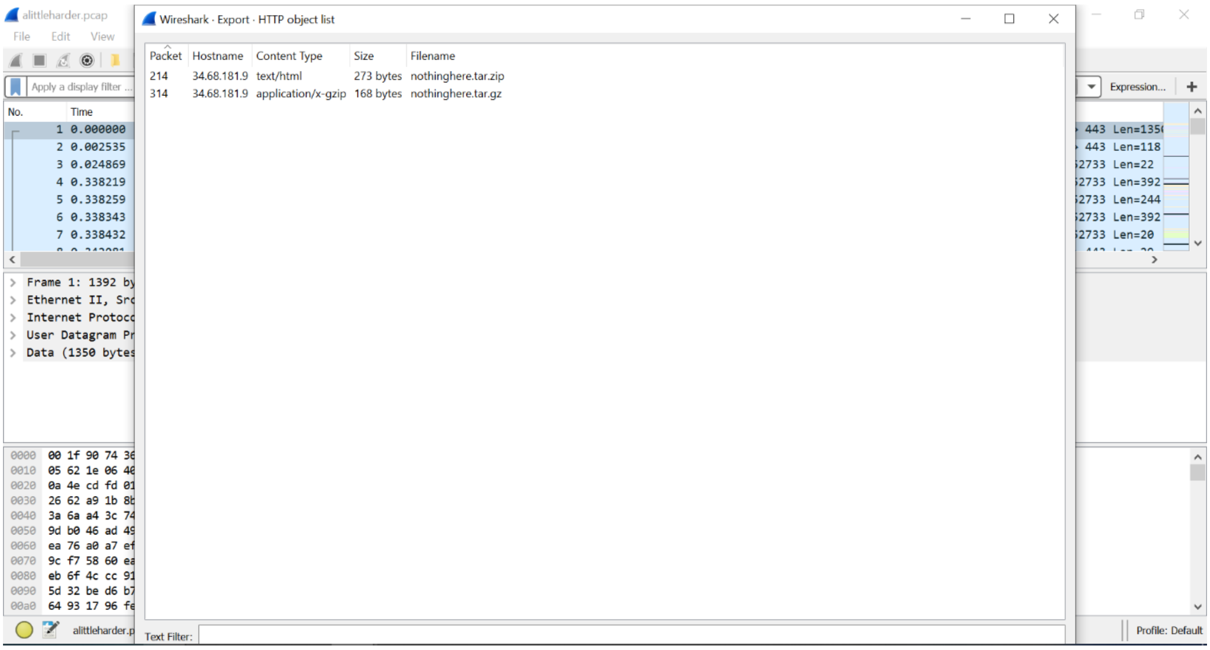
Find:

It is a get request being made for the file flag.txt, at the end of the request we can see a base 64 encoded text that looks like our flag: RGF3Z0NURntuMWMzX3kwdV9mMHVuZF9tM30=

Let’s decrypt it: DawgCTF{n1c3_y0u_f0und_m3}. We got our flag!

#Chal Another Pcap 100

The flag must be somewhere around here... is what we're told and we're given another .pcap file, let's fire up wireshark once again! On exporting the HTTP objects list, we get 2 zip files:

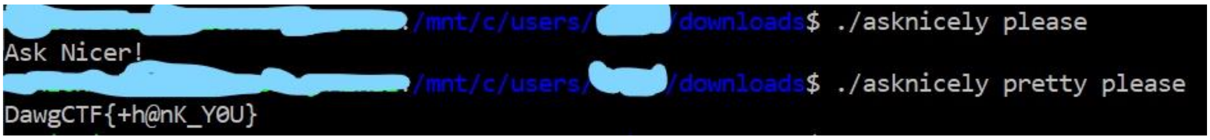


Packet	Hostname	Content Type	Size	Filename
214	34.68.181.9	text/html	273 bytes	nothinghere.tar.zip
314	34.68.181.9	application/x-gzip	168 bytes	nothinghere.tar.gz

On extracting the nothinghere.tar.gz, we get a flag.txt which contains base64 encoded text: RGF3Z0NURnszeHRyNGN0MW5nX2YxbDM1XzFzX2Z1bn0=, which on decoding gives us the flag: DawgCTF{3xtr4ct1ng_f1l35_1s_fun}

#Chal Ask Nicely 50

This is a reversing challenge and the only hint we get is ask nicely! So let's run the binary file, on running it we get an output ask nicely, let's try to use some parameters now:



```
[redacted]/mnt/c/users/[redacted]/downloads$ ./asknicely please
Ask Nicer!
[redacted]/mnt/c/users/[redacted]/downloads$ ./asknicely pretty please
DawgCTF{+h@nK_Y0U}
```

First we try please, and then pretty please: which gives us the flag :D

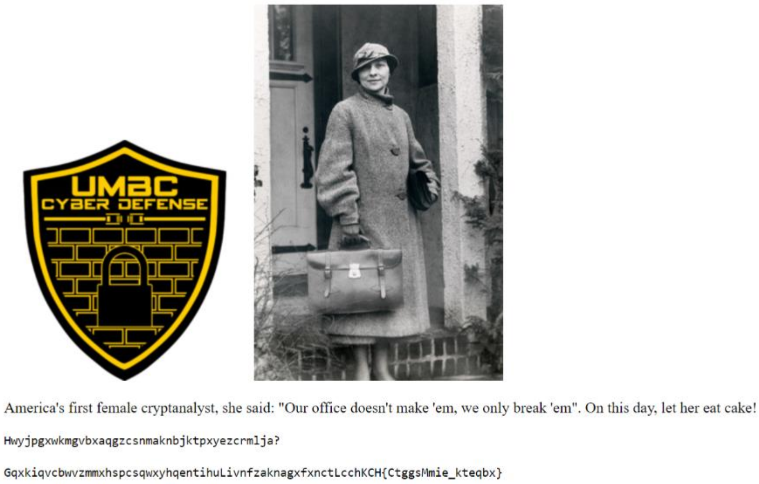
Flag: DawgCTF{+h@nK_YOU}

#Chal UMBC Cyber Defense - can it be breached? 150

Is the shield for keeping things in or keeping things out?

https://clearedge.ctf.umbccd.io/

Once again we get a challenge with the same URL, there is a hint in the text which tell us that the shield plays a key role, let's do some steganography extracting on the shield image.

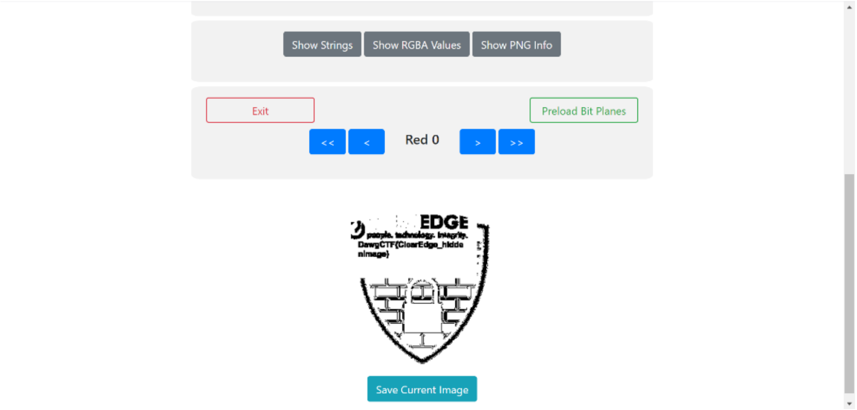


America's first female cryptanalyst, she said: "Our office doesn't make 'em, we only break 'em". On this day, let her eat cake!

Hwyjpgxwkmgvbxaqgzcsnmaknbjktpxyezcrmlja?

GqxkiqvcbwvzmmxhspcsqwxyhqentihuLivnfzaknagxfxnctLcchKCH{CtggsMmie_kteqbx}

Using the stegonline tool by geormnet, we uncover the png 'Red 0' bit panes for the image and voila we got our flag! :D



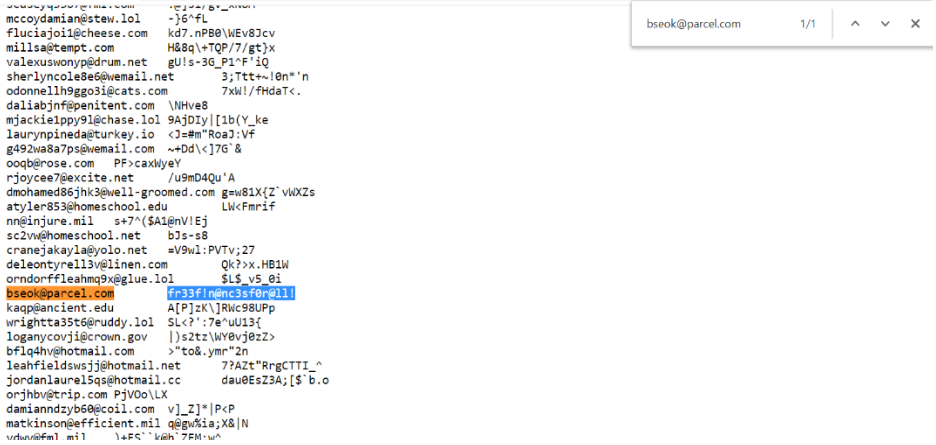
Flag: DawgCTF{ClearEdge_hiddenimage}

#Chal Impossible Pen Test Part 1

This is the hint we're given: Welcome! We're trying to hack into Burke Defense Solutions & Management, and we need your help. Can you help us find the password of an affiliate's CEO somewhere on the internet and use it to log in to the corporate site? https://theinternet.ctf.umbccd.io/

When we navigate to: https://theinternet.ctf.umbccd.io/burkedefensesolutions.html, we find a list of affiliate CEO's.

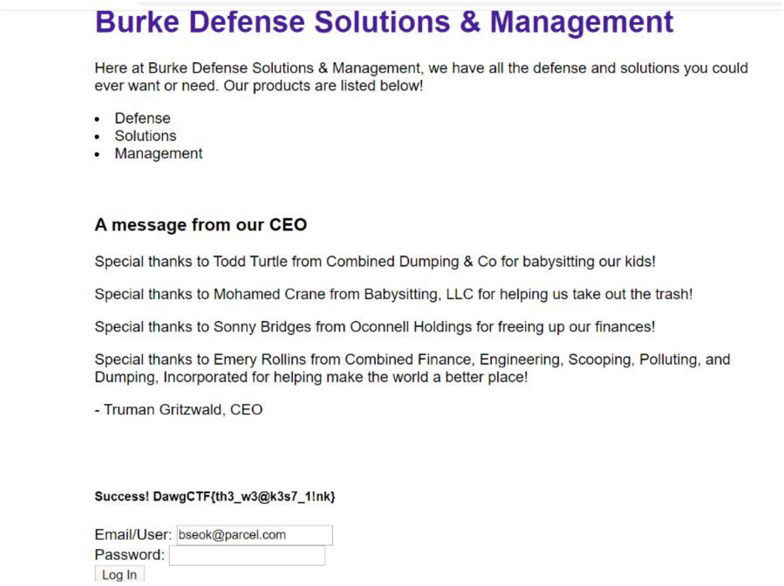
We're told that one of them has faced a data breach. On going through the facespace page for emery rollins one of the CEO’s we find out that charoletteinternational has had a leak! By searching for the email id’s of all the other CEO’s in the breach document we find out that it was Sonny Bridges!



bseok@parcel.com 1/1

```
mccoydamian@stew.lol    -}6^fL
fluciajoi1@cheese.com   kd7.nPB0\WEv8Jcv
millsa@tempt.com        H&8q\+TQP/7/gt}x
valexuswonyp@drum.net   gU!s-3G_P1^F'iQ
sherlyncole8e6@wemail.net       3;Ttt+~!0n*'n
odonnellh9ggo3i@cats.com        7xW!/fHdaT<.
daliabjnf@penitent.com  \NHve8
mjackie1ppy91@chase.lol 9AjDIy|[1b(Y_ke
laurynpineda@turkey.io  <J=#m"RoaJ:Vf
g492wa8a7ps@wemail.com  ~+Dd\<]7G`&
ooqb@rose.com   PF>caxWyeY
rjoycee7@excite.net     /u9mD4Qu'A
dmohamed86jhk3@well-groomed.com g=w81X{Z`vWXZs
atyler853@homeschool.edu        LW<Fmrif
nn@injure.mil   s+7^($A1@nV!Ej
sc2vw@homeschool.net    bJs-s8
cranejakayla@yolo.net   =V9wl:PVTv;27
deleontyrell3v@linen.com        Qk?>x.HB1W
orndorffleahmq9x@glue.lol       $L$_v5_0i
bseok@parcel.com        fr33f!n@nc3sf0r@ll!
kaqp@ancient.edu        A[P]zK\]RWc98UPp
wrightta35t6@ruddy.lol  SL<?':7e^uU13{
loganycovji@crown.gov   |)s2tz\WY0vj0zZ>
bflq4hv@hotmail.com     >"to&.ymr"2n
leahfieldswsjj@hotmail.net      7?AZt"RrgCTTI_^
jordanlaurel5qs@hotmail.cc      dau0EsZ3A;[$`b.o
orjhbv@trip.com PjVOo\LX
damianndzyb60@coil.com  v]_Z]*|P<P
matkinson@efficient.mil q@gw%ia;X&|N
vdwv@fml.mil    )+ES``k@h`ZEM:w^
```

On logging in with his password on the main page we get the flag!



Burke Defense Solutions & Management

Here at Burke Defense Solutions & Management, we have all the defense and solutions you could ever want or need. Our products are listed below!

- Defense
- Solutions
- Management

A message from our CEO

Special thanks to Todd Turtle from Combined Dumping & Co for babysitting our kids!

Special thanks to Mohamed Crane from Babysitting, LLC for helping us take out the trash!

Special thanks to Sonny Bridges from Oconnell Holdings for freeing up our finances!

Special thanks to Emery Rollins from Combined Finance, Engineering, Scooping, Polluting, and Dumping, Incorporated for helping make the world a better place!

- Truman Gritzwald, CEO

Success! DawgCTF{th3_w3@k3s7_1!nk}

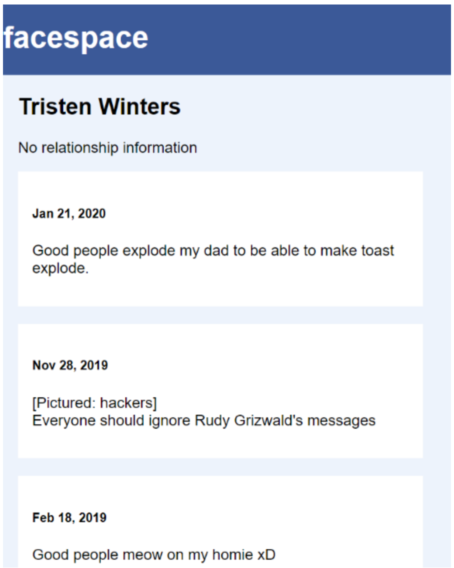
Email/User: bseok@parcel.com
Password:

#chal Impossible Pen Test Part 2

Welcome! We're trying to hack into Burke Defense Solutions & Management, and we need your help. Can you help us find a disgruntled former employee somewhere on the internet (their URL will be the flag)?

https://theinternet.ctf.umbccd.io/

On reading the description we know we have to find out about a rogue employee, by going through the Truman Gritzwald CEO’s facespace page we find out that he is about to fire his CFO, then we find out about his CISO Madalyn Burke, through her facespace page we find out about facespace CTO Royce joyce, through his page we find out about the entire team, after a lot of searching: On Tristen Winter’s page we learn about a employee who’s messages we should ignore.



facespace

Tristen Winters

No relationship information

Jan 21, 2020

Good people explode my dad to be able to make toast explode.

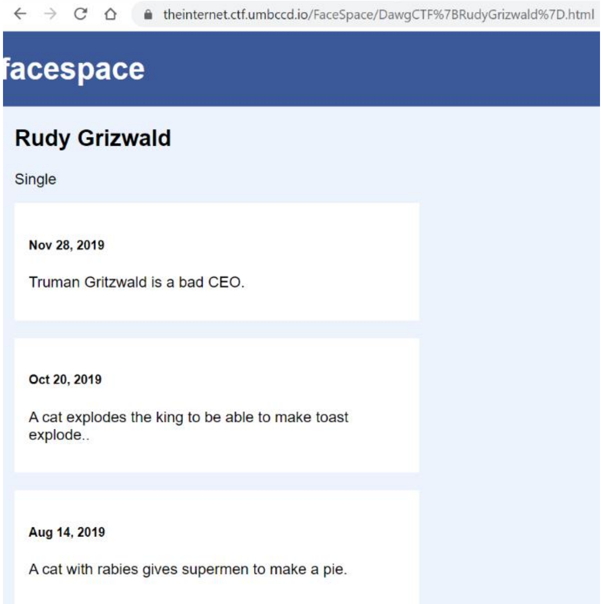
Nov 28, 2019

[Pictured: hackers]
Everyone should ignore Rudy Grizwald's messages

Feb 18, 2019

Good people meow on my homie xD

On Rudy Grizwald’s page, the flag is in the URL.



theinternet.ctf.umbccd.io/FaceSpace/DawgCTF%7BRudyGrizwald%7D.html

facespace

Rudy Grizwald

Single

Nov 28, 2019

Truman Gritzwald is a bad CEO.

Oct 20, 2019

A cat explodes the king to be able to make toast explode..

Aug 14, 2019

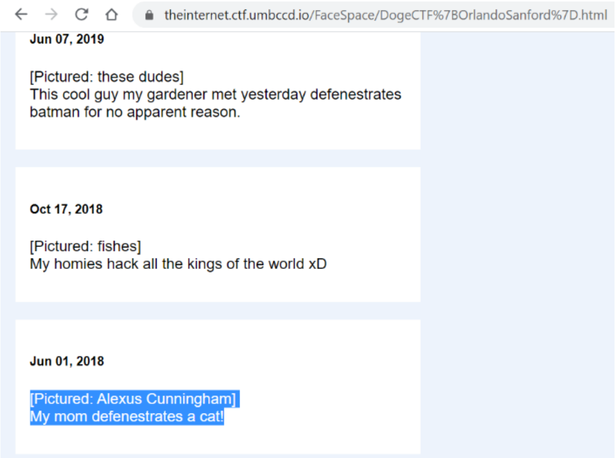
A cat with rabies gives supermen to make a pie.

#chal Impossible Pen Test Part 3

Welcome! We're trying to hack into Burke Defense Solutions & Management, and we need your help. Can you help us find the mother of the help desk employee's name with their maiden name somewhere on the internet (the mother's URL will be the flag)?

https://theinternet.ctf.umbccd.io/

Since we had already found out the team in Royce joyce’s page, read chal2 writeup for deets. We go through their pages one by one: we find out that Orlando Sanford is the help desk employee, on his facespace page, we find out his mother’s name!



theinternet.ctf.umbccd.io/FaceSpace/DogeCTF%7BOrlandoSanford%7D.html

Jun 07, 2019

[Pictured: these dudes]
This cool guy my gardener met yesterday defenestrates batman for no apparent reason.

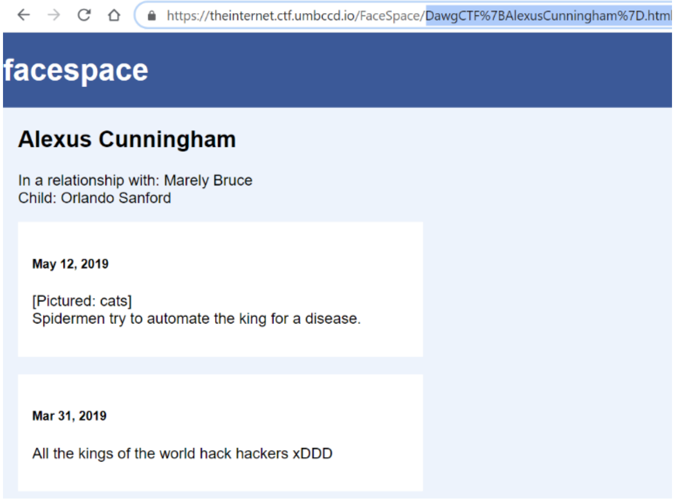
Oct 17, 2018

[Pictured: fishes]
My homies hack all the kings of the world xD

Jun 01, 2018

[Pictured: Alexus Cunningham]
My mom defenestrates a cat!

And on her facespace page in the URL we get the flag!



https://theinternet.ctf.umbccd.io/FaceSpace/DawgCTF%7BAlexusCunningham%7D.htm

Alexus Cunningham

In a relationship with: Marely Bruce
Child: Orlando Sanford

May 12, 2019

[Pictured: cats]
Spidermen try to automate the king for a disease.

Mar 31, 2019

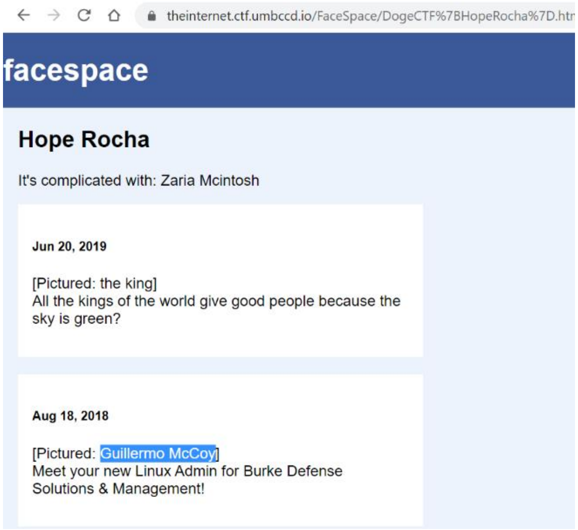
All the kings of the world hack hackers xDDD

#chal Impossible Pen Test Part 4

Welcome! We're trying to hack into Burke Defense Solutions & Management, and we need your help. Can you help us find the syncedin page of the linux admin somewhere on the internet (their URL will be the flag)?

https://theinternet.ctf.umbccd.io/

Since we had already found out the team in Royce joyce's page, read chal2 writeup for deets. We go through their pages one by one: on Hope Rocha's page we find out that Guillermo McCoy is the new Linux Admin!



theinternet.ctf.umbccd.io/FaceSpace/DogeCTF%7BHopeRocha%7D.htr

facespace

Hope Rocha

It's complicated with: Zaria Mcintosh

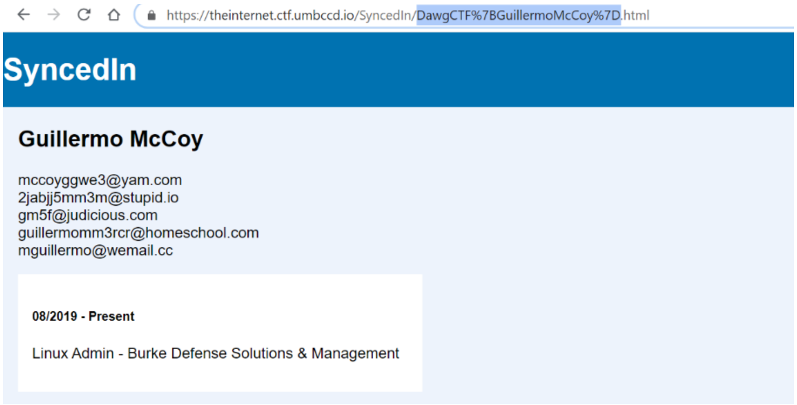
Jun 20, 2019

[Pictured: the king]
All the kings of the world give good people because the sky is green?

Aug 18, 2018

[Pictured: Guillermo McCoy]
Meet your new Linux Admin for Burke Defense Solutions & Management!

On his page we get the flag in the URL:



https://theinternet.ctf.umbccd.io/SyncedIn/DawgCTF%7BGuillermoMcCoy%7D.html

SyncedIn

Guillermo McCoy

mccoyggwe3@yam.com
2jabjj5mm3m@stupid.io
gm5f@judicious.com
guillermomm3rcr@homeschool.com
mguillermo@wemail.cc

08/2019 - Present

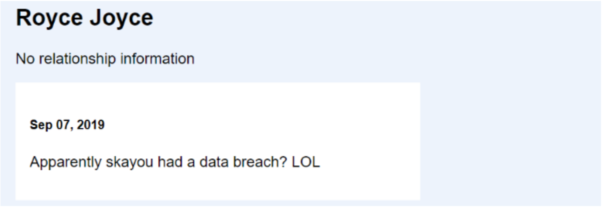
Linux Admin - Burke Defense Solutions & Management

#chal Impossible Pen Test Part 5

Welcome! We're trying to hack into Burke Defense Solutions & Management, and we need your help. Can you help us find the CTO's password somewhere on the internet and use it to log in to the corporate site?

https://theinternet.ctf.umbccd.io/

Since we had already found out that the CTO is Royce Joyce, read chal2 writeup for deets. We go through his page for deets. Isabela Baker is another CTO but she is a red herring.



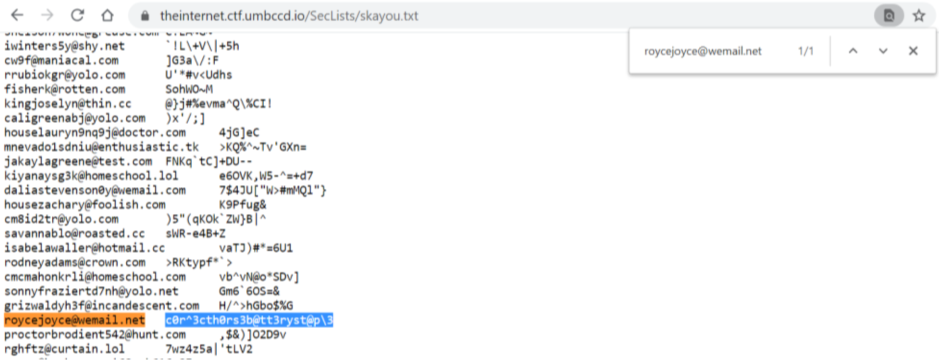
Royce Joyce

No relationship information

Sep 07, 2019

Apparently skayou had a data breach? LOL

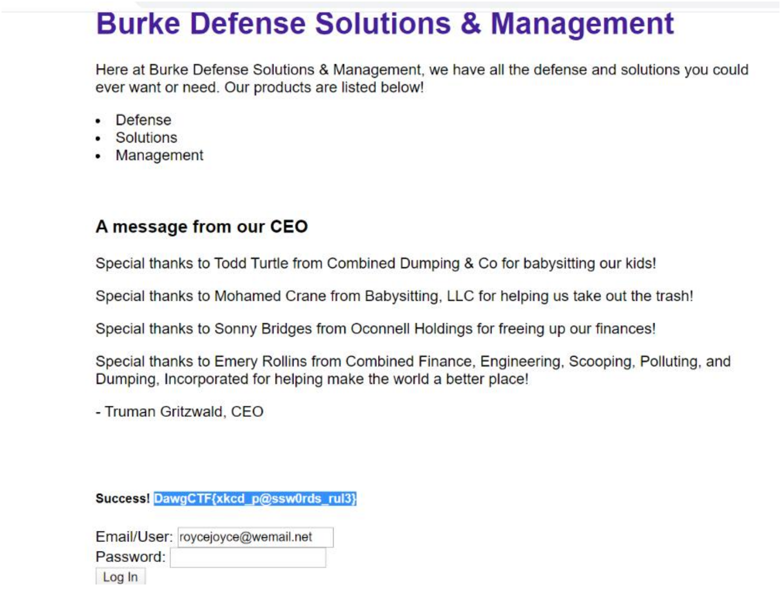
On his page we find out skayou is great and if you scroll down on his page his first post was “I love skayou” so definitely his password leak in the breach, let’s find out using the databreach option on the home page of this challenge:



theinternet.ctf.umbccd.io/SecLists/skayou.txt

```
iwinters5y@shy.net      `!L\+V\|+5h
cw9f@maniacal.com       ]G3a\/:F
rrubiokgr@yolo.com      U'*#v<Udhs
fisherk@rotten.com      SohWO~M
kingjoselyn@thin.cc     @}j#%evma^Q\%CI!
caligreenabj@yolo.com   )x'/;]
houselauryn9nq9j@doctor.com     4jG]eC
mnevado1sdniu@enthusiastic.tk   >KQ%^~Tv'GXn=
jakaylagreene@test.com  FNKq`tC]+DU--
kiyanaysg3k@homeschool.lol      e6OVK,W5-^=+d7
daliastevenson0y@wemail.com     7$4JU["W>#mMQl"}
housezachary@foolish.com        K9Pfug&
cm8id2tr@yolo.com       )5"(qKOk`ZW}B|^
savannablo@roasted.cc   sWR-e4B+Z
isabelawaller@hotmail.cc        vaTJ)#*=6U1
rodneyadams@crown.com   >RKtypf*`>
cmcmahonkrli@homeschool.com     vb^vN@o*SDv]
sonnyfraziertd7nh@yolo.net      Gm6`6OS=&
grizwaldyh3f@incandescent.com   H/^>hGbo$%G
roycejoyce@wemail.net   c0r^3cth0rs3b@tt3ryst@p\3
proctorbrodient542@hunt.com     ,$&)]O2D9v
rghftz@curtain.lol      7wz4z5a|'tLV2
```

As expected we got his credentials in the skayou breach, now we just need to login on the corporate's website, On logging in we get the flag!



Burke Defense Solutions & Management

Here at Burke Defense Solutions & Management, we have all the defense and solutions you could ever want or need. Our products are listed below!

- Defense
- Solutions
- Management

A message from our CEO

Special thanks to Todd Turtle from Combined Dumping & Co for babysitting our kids!

Special thanks to Mohamed Crane from Babysitting, LLC for helping us take out the trash!

Special thanks to Sonny Bridges from Oconnell Holdings for freeing up our finances!

Special thanks to Emery Rollins from Combined Finance, Engineering, Scooping, Polluting, and Dumping, Incorporated for helping make the world a better place!

- Truman Gritzwald, CEO

Success! DawgCTF{xkcd_p@ssw0rds_rul3}

Email/User: roycejoyce@wemail.net
Password:

That was the last writeup for the pentest challenges, hope you had fun reading them! 😊

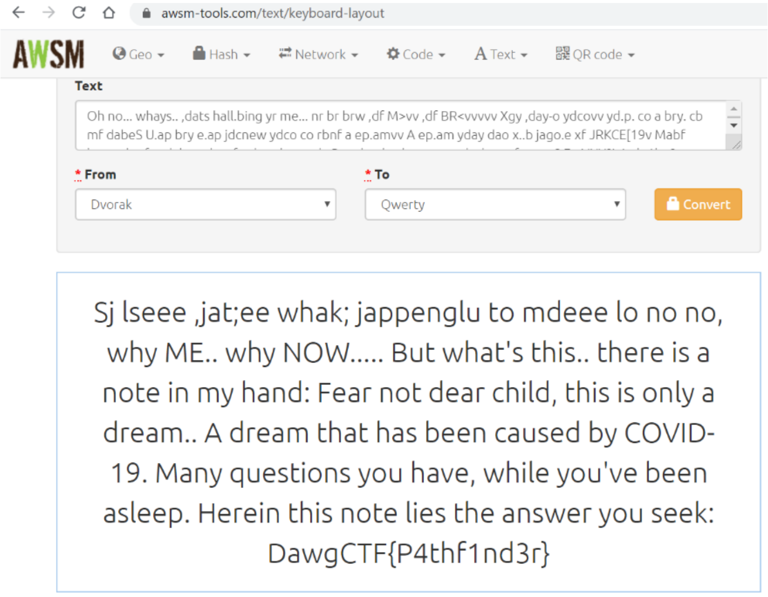
#Chal Qwerky Qwerty 50

We’re given this text: Looks like a shifted/encoded/ciphertext.

Oh no... whays.. ,dats hall.bing yr me... nr br brw ,df M>vv ,df BR<vvvvv Xgy ,day-o ydcovv yd.p. co a bry. cb mf dabeS U.ap bry e.ap jdcnew ydco co rbnf a ep.amvv A ep.am yday dao x..b jago.e xf JRKCE[19v Mabf 'g.oycrbo frg dak.w ,dcn. frg-k. x..b aon..lv D.p.cb ydco bry. nc.o yd. abo,.p frg o..tS Ea,iJYU?L4ydu1be3p+

Let’s do some OSINT, shall we? Let’s google for qwerty encodings/qwerty cipher?

Here’s an awsmtool (pun intended) I found that converts keyboard layouts, after trying all p&c’s I found out that the answer is DVORAK to QWERTY:



Text

Oh no... whays.. ,dats hall.bing yr me... nr br brw ,df M>vv ,df BR<vvvvv Xgy ,day-o ydcovv yd.p. co a bry. cb mf dabeS U.ap bry e.ap jdcnew ydco co rbnf a ep.amvv A ep.am yday dao x..b jago.e xf JRKCE[19v Mabf

From: Dvorak

To: Qwerty

Sj lseee ,jat;ee whak; jappenglu to mdeee lo no no, why ME.. why NOW..... But what's this.. there is a note in my hand: Fear not dear child, this is only a dream.. A dream that has been caused by COVID-19. Many questions you have, while you've been asleep. Herein this note lies the answer you seek: DawgCTF{P4thf1nd3r}

Flag: DawgCTF{P4thf1nd3r}

#Chal Let her eat cake! 75

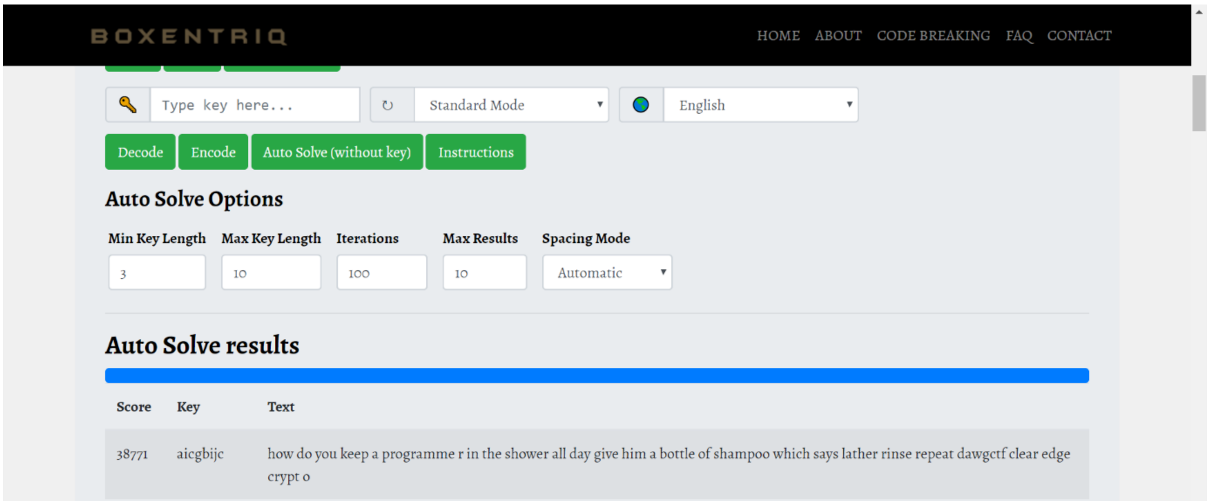
Yet again, we begin on a journey to conquer: She's hungry! https://clearedge.ctf.umbccd.io/. Our only hint, she's hungry!

This time since we've already gotten three flags out of this page, let's try to decrypt the ciphertext on the main page:

Hwyjpgxwkmgvbxaqgzcsnmaknbjktpxyezcrmlja?

GqxkiqvcbwvzmmxhspcsqwxyhqentihuLivnfzaknagxfxnctLcchKCH{CtggsMmie_kteqbx}

By using a vignere cipher auto solver we found out:



Auto Solve Options

Min Key Length	Max Key Length	Iterations	Max Results	Spacing Mode
3	10	100	10	Automatic

Auto Solve results

Score	Key	Text
38771	aicgbijc	how do you keep a programme r in the shower all day give him a bottle of shampoo which says lather rinse repeat dawgctf clear edge crypt o

The flag is DawgCTF{clearedge_crypto}. I must admit the non-flag text was kinda funny too, they should have t-shirts with that slogan! XD