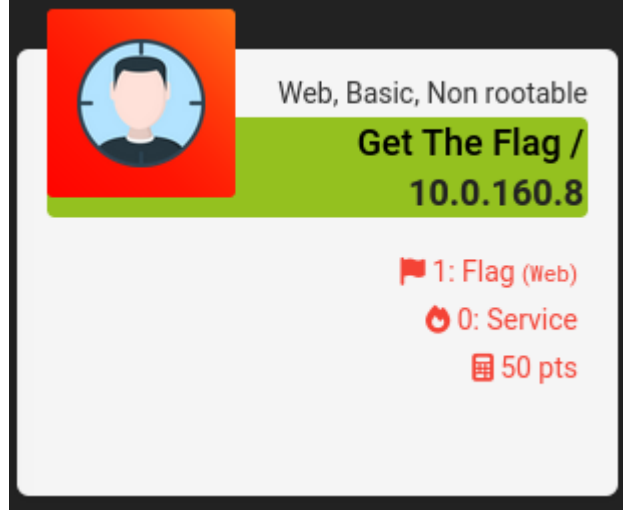


GET THE FLAG WRITEUP



Bayrağın yoluna gitsemde alamıyorum bir el atarmısın ?

- 1) Öncelikle ağ arayüzünde hiç gürültü çıkarmamak adına ve gereksiz zaman kayıplarının önüne geçmek adına makinamızın ipv4 adresini şöyle bir güzel tarayıcıya atalım bakalım. Bunu yapmamdaki sebep eğer ki web uygulamalarıyla uğraşıyorsak ağ taramasıyla vaktimizi harcayacağımız süreyi doğrudan directory enumeration ile harcamayı tercih ediyorum.



Welcome to the HOC

Do you want another flag ???

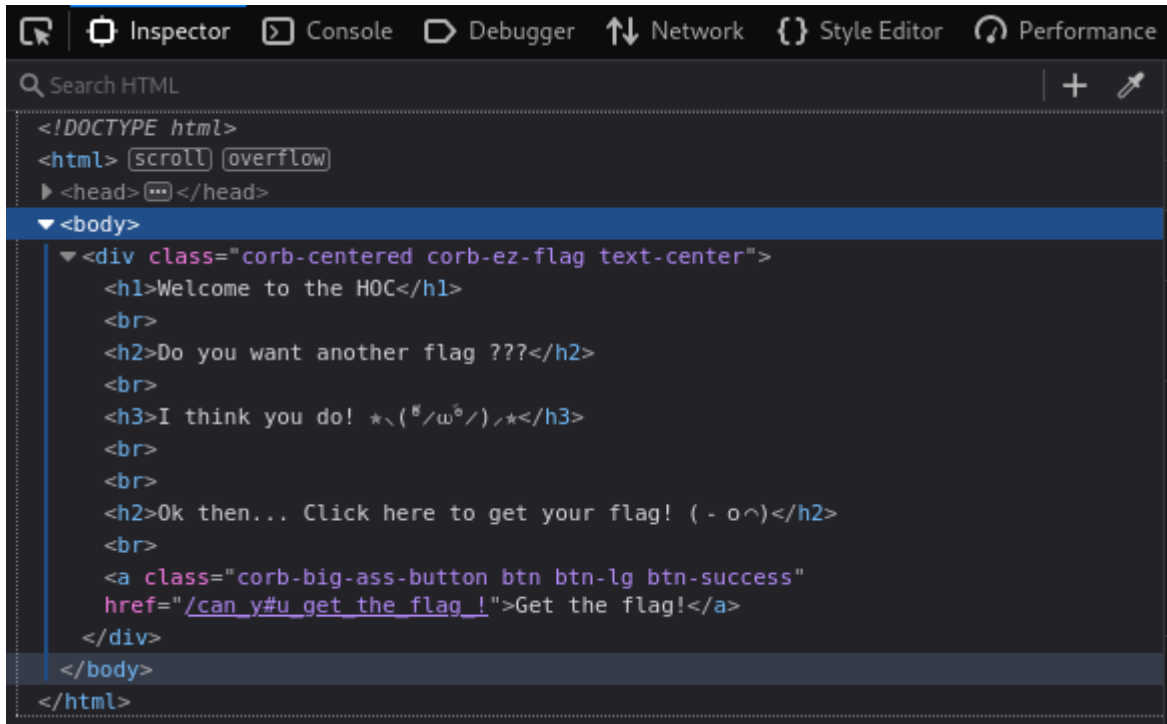
I think you do! ☆_(ツ)_☆

Ok then... Click here to get your flag! (- o ^)

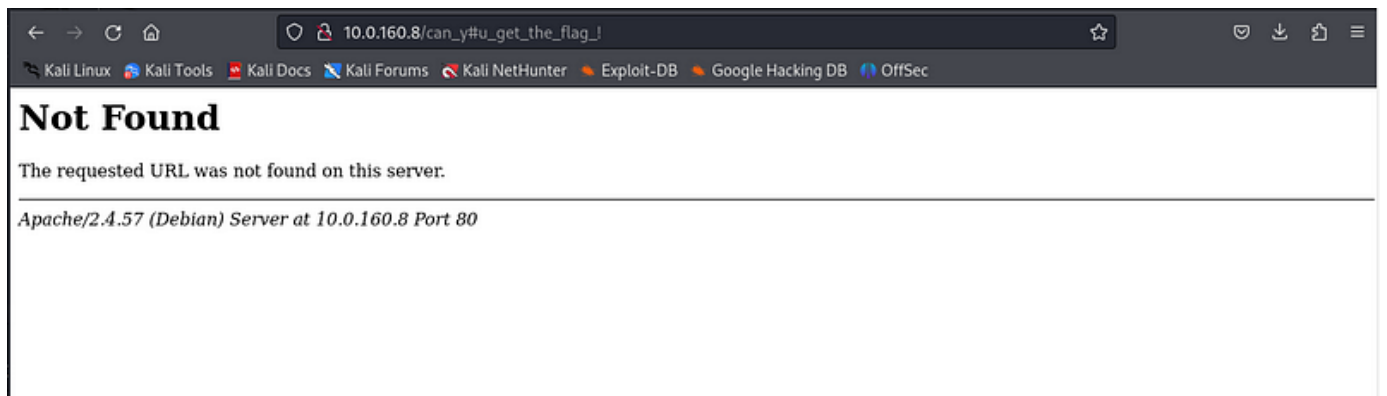
Get the flag!

Evet her zaman web uygulaması çalışacak diye bir şey yok. Deneme-yanılma üzerinden bir web uygulaması karşımıza çıkageldi. Her zaman bu yöntem işe yaramayacağı için baktık hiçbir şey elimize geçmedi doğrudan nmap üzerinden http veya https portlarını aramak veya bunlarla ilişkilendirebileceğimiz Apache servislerini aramak çok daha mantıklı tabiki.

- 2) Merak ettim ve butona basarsam tutu ve beni bir path'e yönlendirdi. Ben butona basmadan önce şöyle bir yaklaşımda da bulundum belki de bir "href" html uzantısı bizi bilinmedik yerlere yönlendirir diye.



```
<!DOCTYPE html>
<html> scroll overflow
<head> ... </head>
<body>
  <div class="corb-centered corb-ez-flag text-center">
    <h1>Welcome to the HOC</h1>
    <br>
    <h2>Do you want another flag ???</h2>
    <br>
    <h3>I think you do! *\(%/w^/)*</h3>
    <br>
    <br>
    <h2>Ok then... Click here to get your flag! (- o^)</h2>
    <br>
    <a class="corb-big-ass-button btn btn-lg btn-success"
      href="/can_y#u_get_the_flag_!">Get the flag!</a>
  </div>
</body>
</html>
```



- 3) Bu bilgilerle bir yere ulaşacağımı düşünmediğim için önce bir Gobuster taraması atayım dedim. Buradan büyük bir wordlist kullanmama rağmen yine bir sonuç alamadım.

```
└─# gobuster dir -u http://10.0.160.8/ -w /usr/share/dirb/wordlists/big.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.0.160.8/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

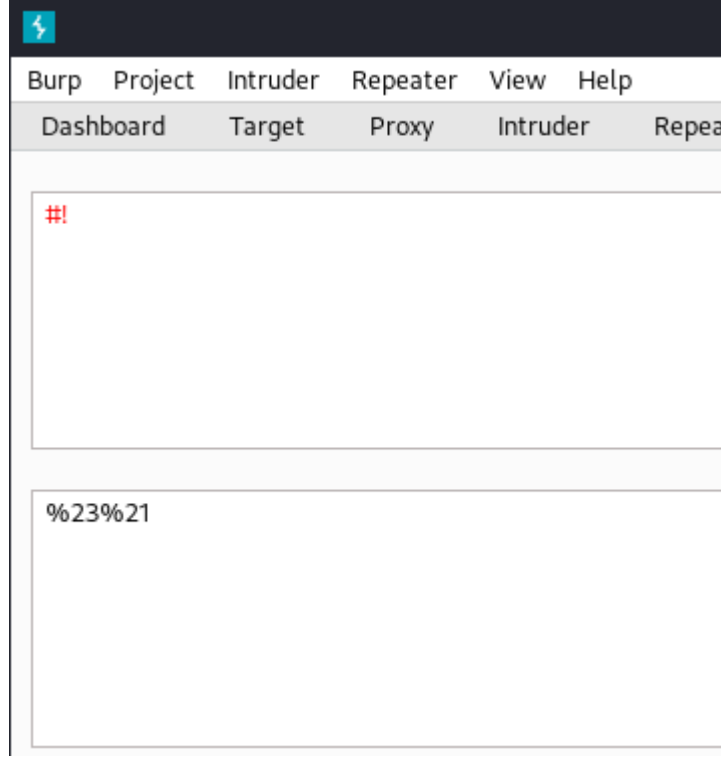
/.htaccess (Status: 403) [Size: 275]
/.htpasswd (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 20469 / 20470 (100.00%)

Finished
```

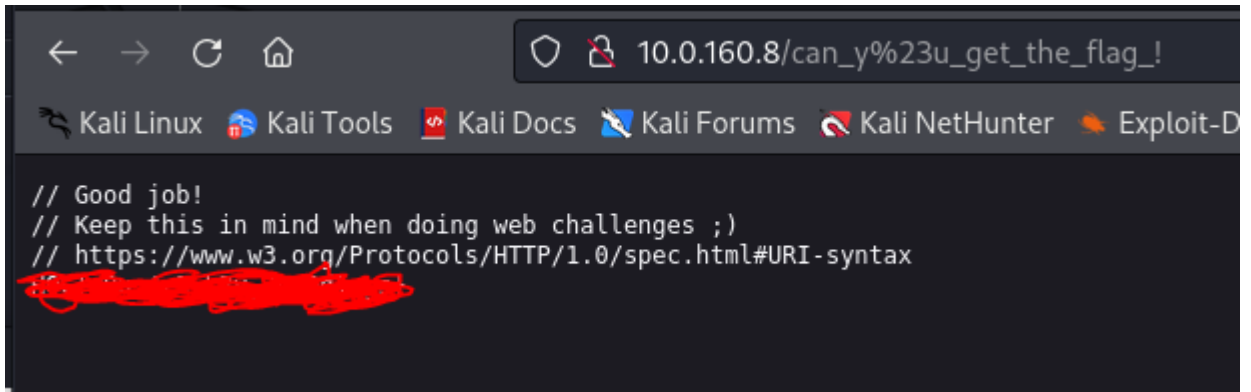
Aynı anda gerçekleştirdiğim nmap tarama sonucu:

```
SYN Stealth Scan Timing: About 99.99% done; ETC: 15:38 (0:00:00 remaining)
Nmap scan report for 10.0.160.8
Host is up (0.11s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: EASY FLAG HOC
```

- 4) Uzun süre düşündükten sonra bi encryption/decryption veya hashing algoritması olup olmayacağından şüphelendim. Baktım ki sonuç yok belki de mesaj şifrelenmek yerine formatı değiştirilmek istenmiştir diye düşündüm. Çünkü baktığımızda URLin yönlendirdiği mesaj ın sonu ve başı ! ve # işaretleri içeriyor. Bunlar hemen aklımda URL veya HTML encoding ve decodingı getirdi. Ben de bu işaretleri ayrı ayrı Burpsuite içerisinde encoding yaptım.



- 5) Ardından tüm stringi çevirerek URLe yapıştırdım ama bir sonuç elde edemedim. Bu sefer sadece ünlem ve hash işaretini değiştirerek encode haliyle atmayı denedim yani şu şekilde:



Arkadařlar bu makina korkun derecede zor deęil ama tek bir noktası can alıcı ve bunu grmesi ok zor. Emin olun 3-4 saatimi burda ne olabilir kısmına harcadım nk attığım nmap taramasından da bir bulgu elde edemedim. Ardından aklımda kalan tek weaponizing yani silahlanma řekli bu oldu. Kriptografik bir yaklaşım bekledim ama decode edilmiş URL'i encode ederek bu işi halletmiş oldum.

