**Sided curl**

Din descrierea la challenge putem observa cateva hinturi importante cum ar fi faptul ca website-ul ia fisere de tip .png , site-ul este creat de un admin asa ca poate exista un admin pannel pe undeva,si ca exista niste restrictii poate un WAF(Web Application Firewall ) existent.Dupa ce intram pe site vedem ca exista un endpoint pentru admini hostat pe portul 8000 iar daca incercam sa folosim http://localhost:8000/admin nu ajuta.Intrebarea este cum facem de la un png sa exfiltram flagul prin endpointul de acolo?


Mai intai ne cere sa introducem fisiere de tip png care contine url de google.com asa ca daca incercam un url ca si: http://google.com/ v-om primi raspuns ca nu exista fisierul prezent.Asa ca am inceput sa ma joc putin cu url ca sa imi dau seama cum as putea da bypass la extensia de .png. Am banuit ca in spatele la backend se afla limbaje de programare precum python sau php asa ca daca trimitem un request cu http://google.com/# cu “#” la final o sa observam ca am dat break putin la website :))


Deci am gasit un bypass pentru extensia de .png acum ce mai trebuie sa facem este sa acessam endpointul controlat local de admin .Dupa putina cautare am observat un writeup (https://bugs.xdavidhu.me/google/2021/12/31/fixing-the-unfixable-story-of-a-google-cloud-ssrf/) care ne poate duce la solve.

Daca incercam un payload de genul : http://google.com@127.0.0.1 :8000/admin# (il trateaza ca si cum am face request direct la localhost si google.com ar fi ignorat) o sa vedem ca primim un response ca avem nevoie sa fim autentificati ca userul “admin” cu parola “admin” si sa acessam un fisier numai admin.php.

```
<!DOCTYPE html>
<html>
<head>
  <title>Admin Login</title>
</head>
<body>
  <form action="admin.php" method="get">
    <label for="username">Username:</label>
    <input type="text" id="username" name="admin" required>

    <label for="password">Password:</label>
    <input type="password" id="password" name="admin" required>
    <br>
    <input type="submit" value="Login">
  </form>
</body>
</html>
```

Pare simplu right?Daca trimitem payloadul final **:http://google.com@127.0.0.1:8000/admin.php? username=admin&password=admin#** Observam ca primim ca response ca url este prea lung.Eh daca scurtezi cu cateva caractere o sa vezi ca suntem asa de aproape asa ca un truc folosit de multi este ca in loc de localhost(127.0.0.1:8000) putem folosi 0:port pe care il va trata la fel.Deci de aici este simplu.Payloadul final:

**http://google.com@0:8000/admin?username=admin&password=admin#**

La acest tip de challenge este important sa incerci foarte mult pana iti da raspunsul.Trial and error is the way to grow happy hacking.

**Flag:**
**CTF{36555d5ff86de7b5a572f4c0…...87d9c043618442d248d940b65}**

**Trolled by masquerade8077**