

HackerDivulgation.com

DOCS

PicoCTF | GET aHEAD

Reto Capture de Flag publicado en el sitio PicoCTF, categoría Web Exploitation. Cambiar el método de petición HTTP es la principal pista para la resolución.

Contenido

- [Problema](#)
- [Requisitos](#)
- [Solución](#)
- [Script en Python](#)
- [Video](#)
- [Referencias](#)

Problema

Find the flag being held on this server to get ahead of the competition

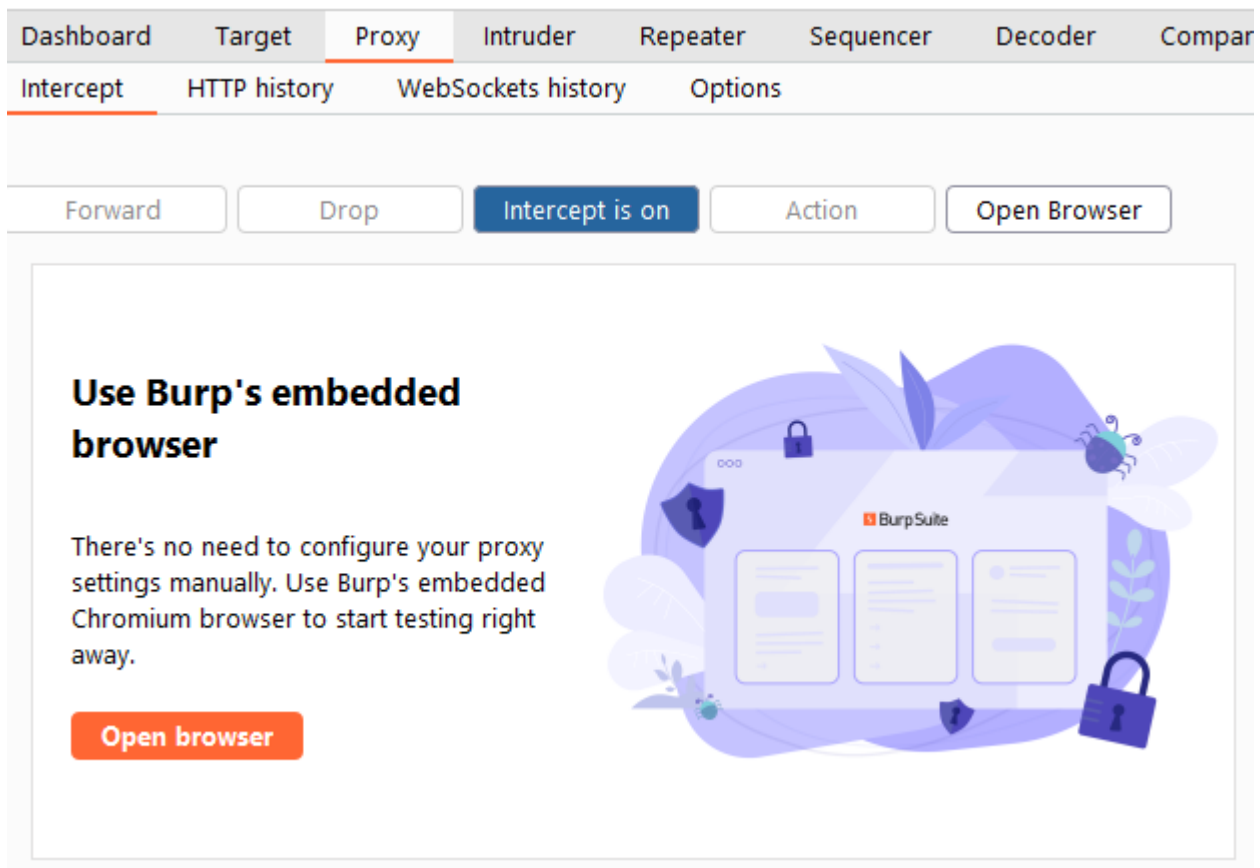
<http://mercury.picoctf.net:45028/>

Requisitos

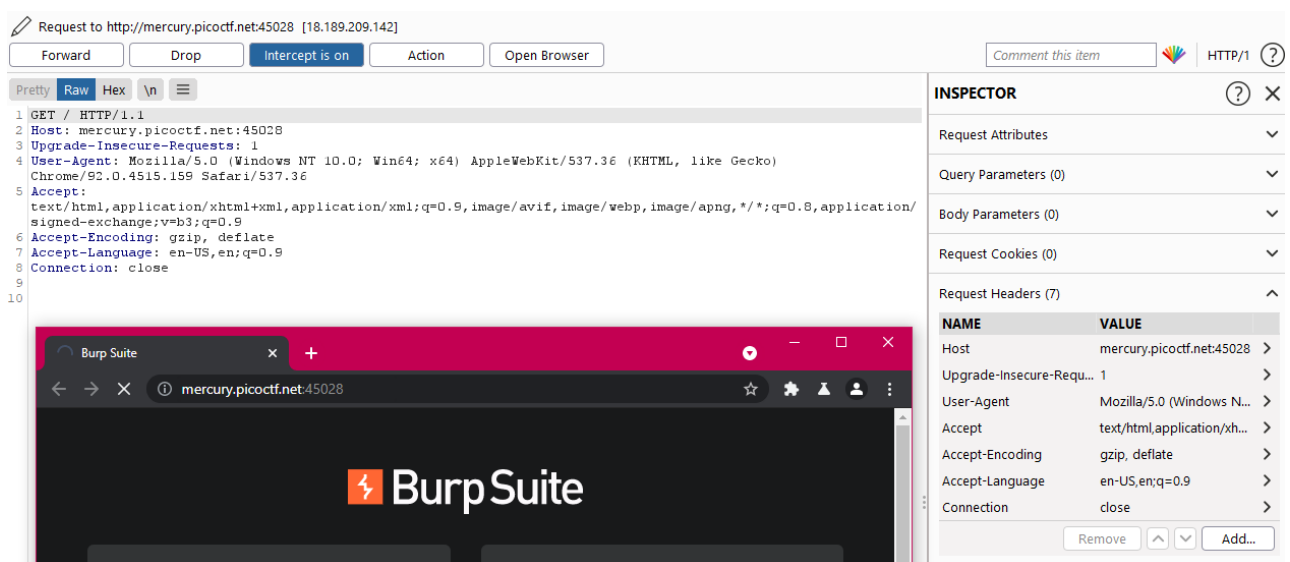
- [Burp Suite Community Edition](#)

Solución

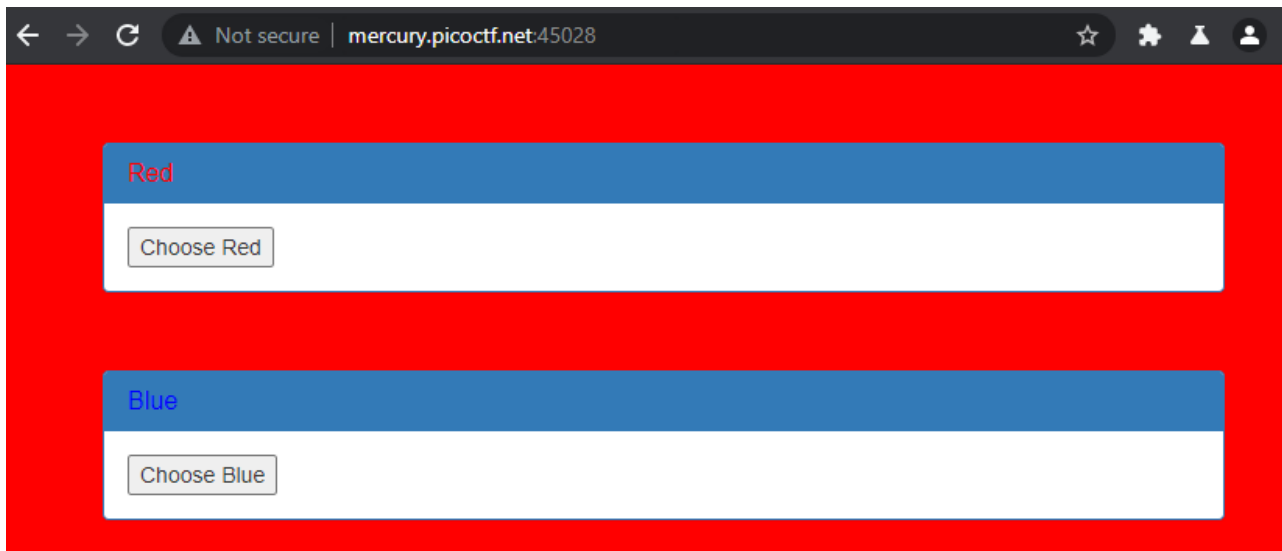
Para resolver este reto se debe interceptar la petición con Burp Suite. Abrir el programa seleccionar Proxy -> Intercept . Habilitar la interceptación de peticiones y dar clic en Open Browser .



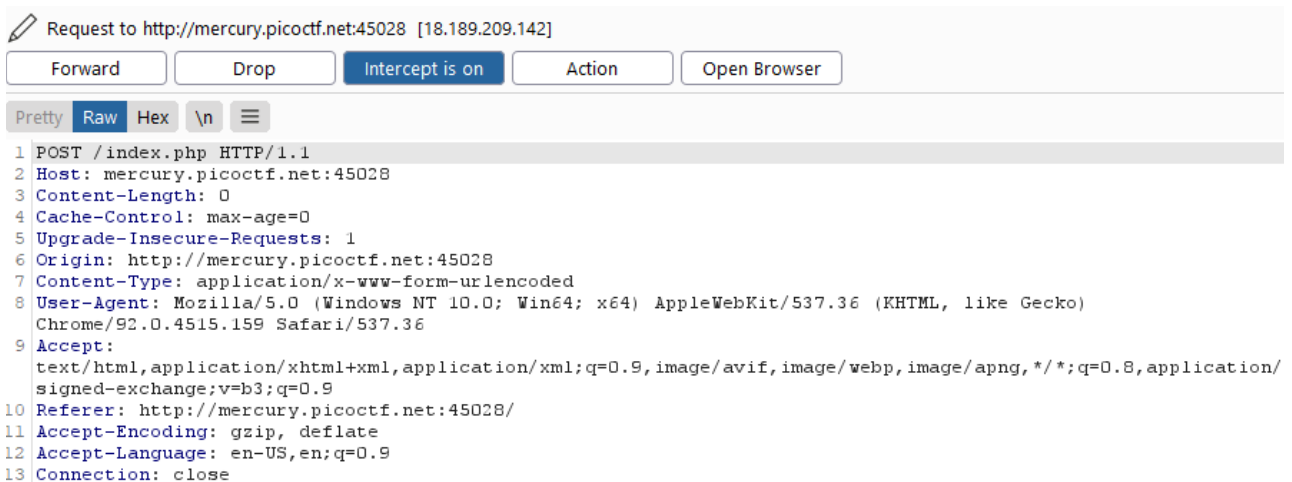
Colocar la URL del reto en la ventana del navegador y Enter . Interceptará la primera petición GET al servidor. Clic en Forward .



Se mostrará el sitio del reto, clic en botón Choose Blue .



Se muestra la petición que se realizará en este caso POST, cambiar el método por HEAD y clic en Forward .



Diferencia entre POST y HEAD:

- POST se utiliza para enviar una entidad a un recurso en específico. Ejemplo: enviar datos o credenciales en un formulario.
- HEAD pide una respuesta idéntica a la de una petición GET, pero sin el cuerpo de la respuesta.

```
Request to http://mercury.picoctf.net:45028 [18.189.209.142]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex \n
1 HEAD /index.php HTTP/1.1
2 Host: mercury.picoctf.net:45028
3 Content-Length: 0
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://mercury.picoctf.net:45028
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/92.0.4515.159 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
  signed-exchange;v=b3;q=0.9
10 Referer: http://mercury.picoctf.net:45028/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
```

Ir hacia la pestaña de HTTP history, seleccionar la petición y revisar la respuesta del servidor. En las cabeceras de respuesta aparece una key llamada flag con el valor de respuesta al reto.

Intercept	HTTP history	WebSockets history	Options									
Filter: Hiding CSS, image and general binary content												?
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	
1	http://mercury.picoctf.net:45028	GET	/			200	1123	HTML		Red		
3	http://mercury.picoctf.net:45028	GET	/favicon.ico			404	80	text	ico			
4	http://mercury.picoctf.net:45028	POST	/index.php		✓	200	103	HTML	php			
5	http://mercury.picoctf.net:45028	POST	/index.php		✓	200	103	HTML	php			
6	http://mercury.picoctf.net:45028	GET	/			200	1123	HTML		Red		
7	http://mercury.picoctf.net:45028	GET	/favicon.ico			404	80	text	ico			
8	http://mercury.picoctf.net:45028	POST	/index.php		✓	200	103	HTML	php			

Original request

Pretty Raw Hex \n

1 POST /index.php HTTP/1.1
2 Host: mercury.picoctf.net:45028
3 Content-Length: 0
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://mercury.picoctf.net:45028
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://mercury.picoctf.net:45028/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14

Response

Pretty Raw Hex Render \n

1 HTTP/1.1 200 OK
2 flag: picoCTF{r3j3ct_th3_du4l1ty_775f2530}
3 Content-type: text/html; charset=UTF-8
4
5

INSPECTOR

Request Attributes

Protocol HTTP/1 HTTP/2

ATTRIBUTE	VALUE
Method	POST
Path	/index.php

Request Headers (12)

Response Headers (2)

NAME	VALUE
flag	picoCTF{r3j3ct_th3_du4l...
Content-type	text/html; charset=UTF-8

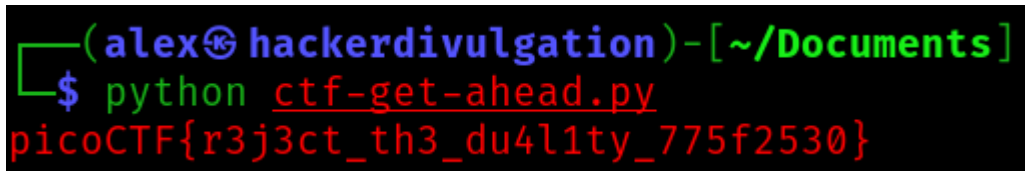
picoCTF{r3j3ct_th3_du4l1ty_775f2530}

Script en Python

El siguiente código permite automatizar todo el análisis anteriormente explicado. Se usa la librería [Requests de Python](#) para automatizar las peticiones.

```
import requests
```

```
headers = {  
    'user-agent': 'Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko  
    'content-type': 'application/x-www-form-urlencoded'  
}  
  
req = requests.head("http://mercury.picoctf.net:45028/index.php", headers=headers)  
  
print(req.headers['flag'])
```



A terminal window with a black background and colorful text. The prompt is `(alex@hackerdivulgation) - [~/Documents]`. The user enters `$ python ctf-get-ahead.py`. The output is `picoCTF{r3j3ct_th3_du4l1ty_775f2530}` in red text.

[Download Script Code](#)

Video

Video en YouTube mostrando como realizar el reto.

[Video: PicoCTF Get aHead](#) | [Blog](#)

Referencias

1. Sitio oficial de PicoCTF. <https://www.picoctf.org/>
2. Métodos de petición HTTP. <https://developer.mozilla.org/es/docs/Web/HTTP/Methods>
3. Documentación de librería Requests de Python. <https://docs.python-requests.org/en/latest/>



Esta obra está bajo una [licencia de Creative Commons Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional](#).