

1 A10 Server-Side Request Forgery

1.1 Concepto

En un ataque de falsificación de solicitudes del lado del servidor (SSRF), el atacante puede abusar de la funcionalidad del servidor para leer o actualizar recursos internos. El atacante puede proporcionar o modificar una URL a la que el código que se ejecuta en el servidor leerá o enviará datos. Además, al seleccionar cuidadosamente las URL, el atacante puede leer la configuración del servidor, como los metadatos de AWS, conectarse a servicios internos como bases de datos habilitadas para HTTP o realizar solicitudes de publicación hacia servicios internos que no están destinados a ser expuestos.

Objetivos

En los ejercicios de las páginas siguientes, deberá examinar lo que el navegador envía al servidor y ajustar la solicitud para obtener otras cosas del servidor.

Instrucciones de la SSRF

<https://www.hackerone.com/blog-How-To-Server-Side-Request-Forgery-SSRF>



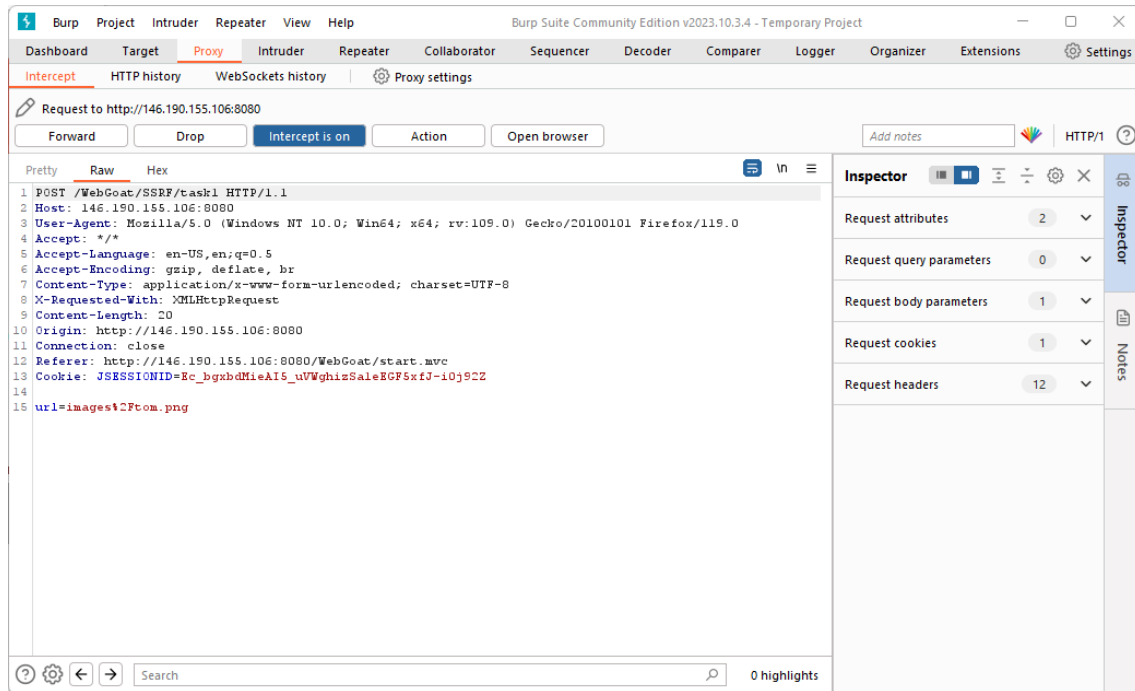
Find and modify the request to display Jerry

Click the button and figure out what happened.

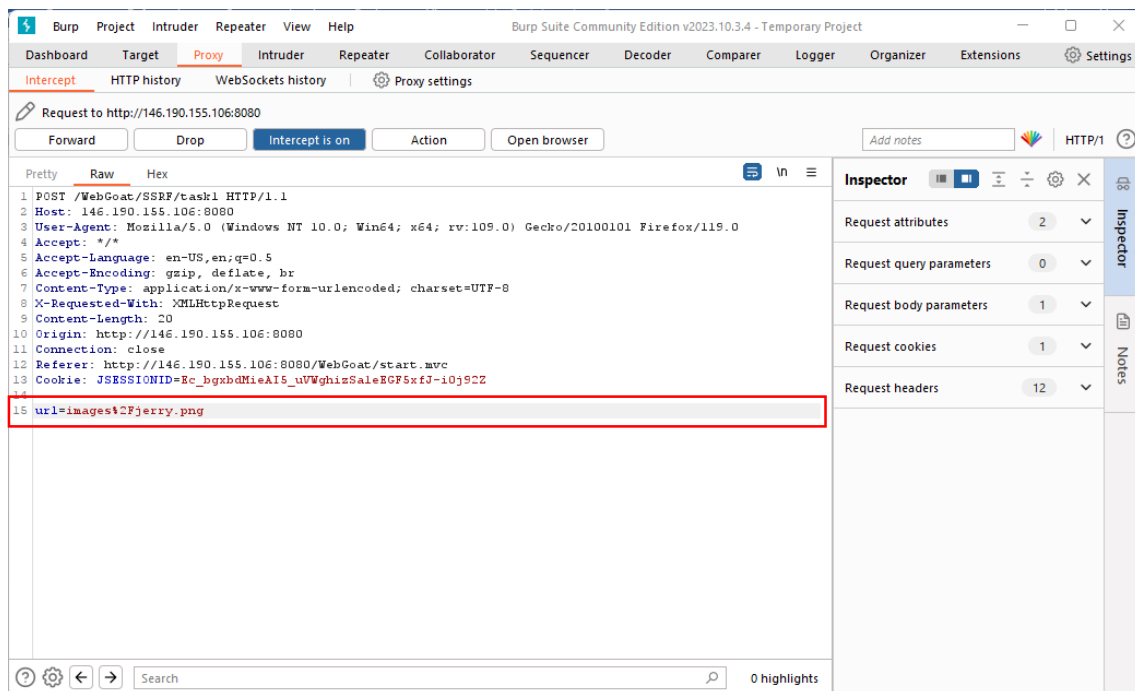
Steal the Cheese

La idea es que se muestre Jerry cuando presionas el botón “Steal the Cheese”

Haz clic en e botón y captura la petición:



Modifica la petición para que se muestre a Jerry



Revisa el browser debe aparecer Jerry

➕ 1 2 3 4 ➖


Find and modify the request to display Jerry

Click the button and figure out what happened.

✓

Steal the Cheese

You rocked the SSRF!



1.2 Cambiando el Request

➕ 1 2 3 4 ➖

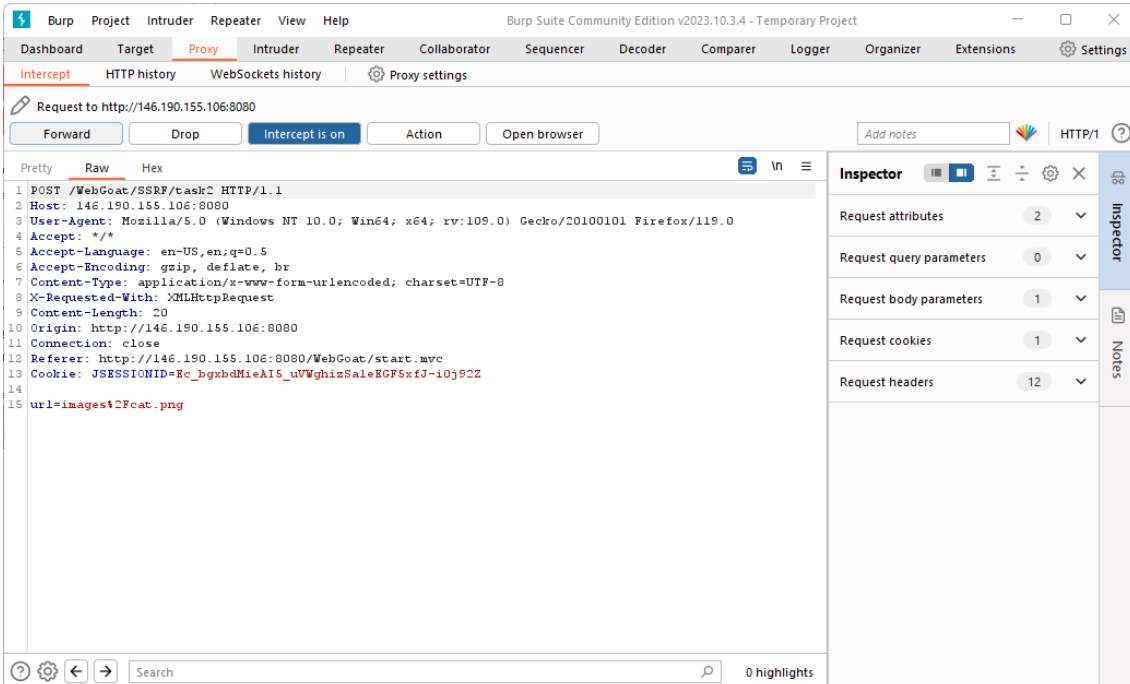
Change the request, so the server gets information from <http://ifconfig.pro>

Click the button and figure out what happened.

try this

Haz clic en el botón “try this”

Captura la petición y cambia a url



Burp Suite Community Edition v2023.10.3.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Settings

Intercept HTTP history WebSockets history Proxy settings

Request to http://146.190.155.106:8080

Forward Drop Intercept is on Action Open browser

Add notes HTTP/1 ?

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 1

Request cookies 1

Request headers 12

Notes

1 POST /WebGoat/SSRF/task2 HTTP/1.1

2 Host: 146.190.155.106:8080

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0

4 Accept: */*

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8

8 X-Requested-With: XMLHttpRequest

9 Content-Length: 20

10 Origin: http://146.190.155.106:8080

11 Connection: close

12 Referer: http://146.190.155.106:8080/WebGoat/start.mvc

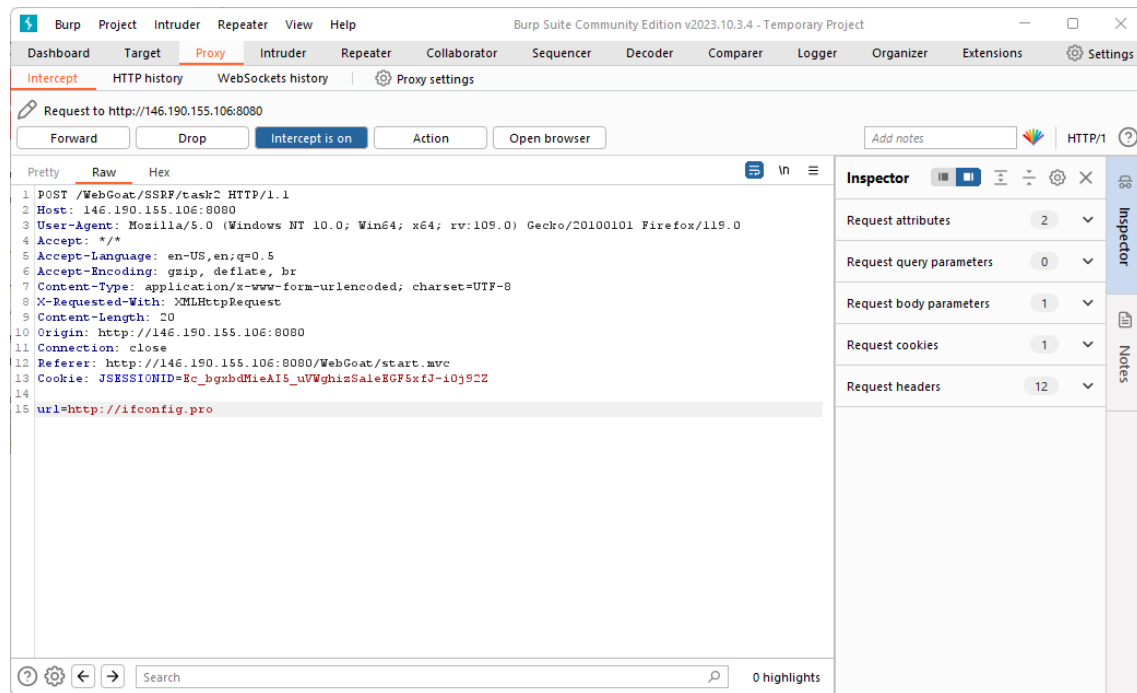
13 Cookie: JSESSIONID=Ec_bgxhdMieAIS_uVWghizSale8GF5xfJ-i0j92Z

14

15 url=images12Fcat.png

0 highlights

Cambia el valor del parámetro url



Envía la petición y observa la respuesta en el browser.

