

Hacking para  
Desarrolladores -  
DevSecOps



 **Bancolombia**

# Objetivo

**Este Capture The Flag (CTF) busca sensibilizar a los devs sobre las principales vulnerabilidades de seguridad en aplicaciones, utilizando la gamificación como herramienta pedagógica.**

**A través de retos prácticos y escenarios simulados, se busca que identifiquen fallas comunes derivadas de malas prácticas de programación, comprendan su impacto en la seguridad de los sistemas, y aprendan cómo desde su rol pueden implementar medidas preventivas para mitigar estos riesgos desde las etapas tempranas del ciclo de desarrollo.**

# Taller

- 20 laboratorios interactivos introductorios a diferentes tipos de vulnerabilidades.
- Completamente solucionable desde el navegador (mayoría) y una consola de comandos (para algunos laboratorios que requieren manipulación de peticiones).
- Plataforma que registra la puntuación de cada persona y permite elegir el top de participantes ganadores.



USERS SCOREBOARD CHALLENGES



ADMIN PANEL



NOTIFICATIONS



PROFILE



SETTINGS



## » WEB

Developer's Best Friend 10	Authentication Logic 10	Client-Side Security 10	Base64 Encoding Detection 10
Secure Admin Panel 10	AI Corporate Assistant 15	SQL Injection 15	Cross-Site Scripting 15
Exposed Backup Files 15	Default Credentials 15	Weak Token Generation 15	Persistence & Rate Limiting 15
The Hidden Truth 15	JWT signature validation by 15	URL Manipulation 20	Directory Traversal 20
Directory Listing 20	JWT Vulnerability 20	JWT Scope Bypass 25	Server-Side Request Forgery 25



USERS SCOREBOARD CHALLENGES



ADMIN PANEL



NOTIFICATIONS



PROFILE

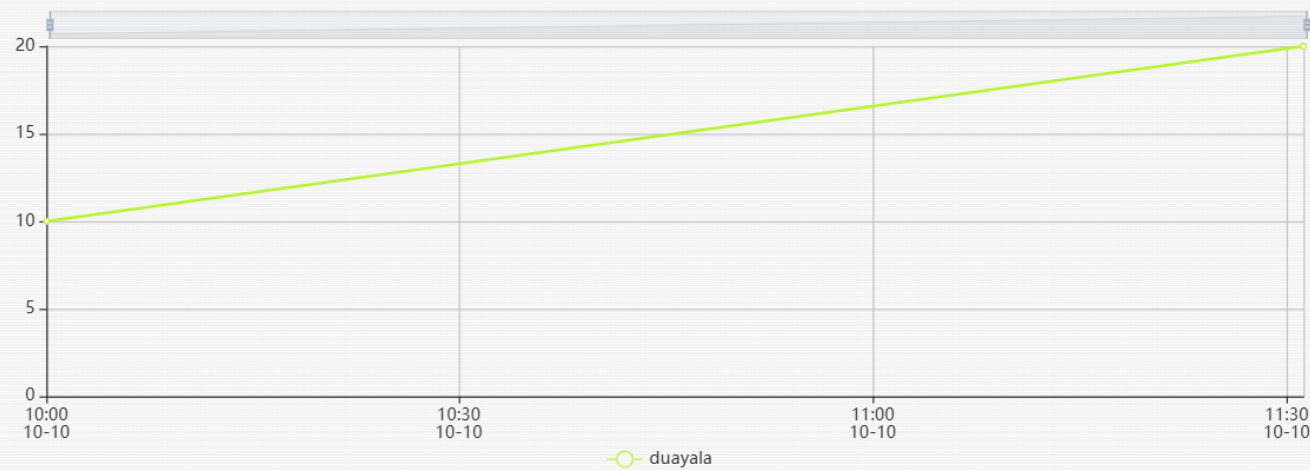


SETTINGS



# Scoreboard

Top 10 Users



Place User

Score

1 duayala

20

# Instrucciones registro

- Plataforma del Taller: <http://ctf.devexp-bancol.com/>
- Abrir taller en incognito y permitir continuar al sitio.
- Registrarse con correo electrónico real, para facilidad de contacto en caso de ser uno de los ganadores
- Código de registro: devsecops-bintec\*2025



# Register

Nombre de usuario

Your username on the site

Correo electrónico

Never shown to the public

Contraseña

Password used to log into your account

Registration Code

Registration code required to create account

Enviar

# Instrucciones taller

- Permite respuestas desde las 3pm 15/10 hasta 2pm 16/10.
- El formato de las respuestas es `flag{xx...xx}`, excepto el laboratorio Cross-Site Scripting.
- Leer atentamente cada laboratorio, estos contienen pistas importantes.
- Dependiendo de la dificultad de cada laboratorio, se otorga mas o menos puntos tras solucionarse.
- Es permitido realizar preguntas de guía.



USERS SCOREBOARD CHALLENGES

ADMIN PANEL NOTIFICATIONS PROFILE SETTINGS

CHALLENGE

1 SOLVES

**Developer's Best Friend**

10

Lab: <http://ctf.devexp-bancol.com:3002/>

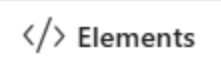
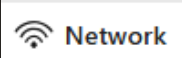
flag{xx...xx}

Submit

WEB

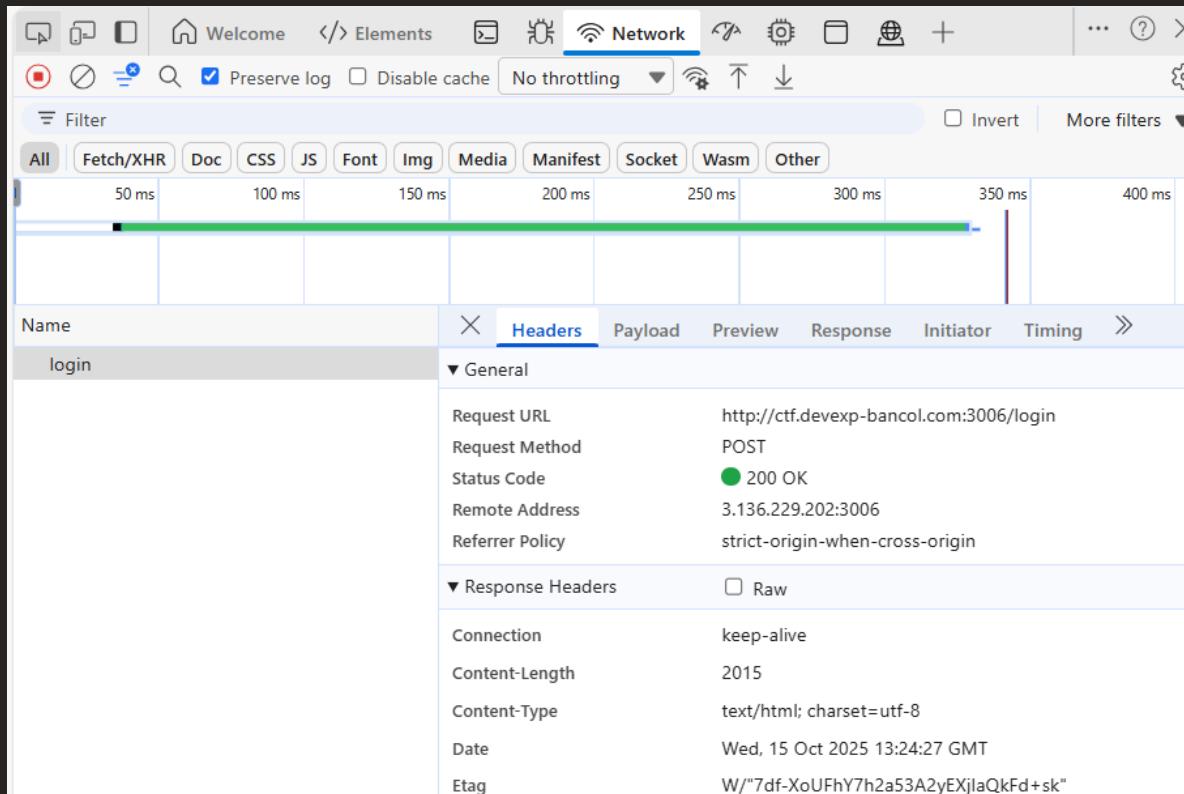
<div>Developer's Best Friend</div> <div>10</div>	<div>Authentication Logic</div> <div>10</div>	<div>Client-Side Security</div> <div>10</div>	<div>Base64 Encoding Detection</div> <div>10</div>
<div>Secure Admin Panel</div> <div>10</div>	<div>AI Corporate Assistant</div> <div>15</div>	<div>SQL Injection</div> <div>15</div>	<div>Cross-Site Scripting</div> <div>15</div>
<div>Exposed Backup Files</div> <div>15</div>	<div>Default Credentials</div> <div>15</div>	<div>Weak Token Generation</div> <div>15</div>	<div>Persistence &amp; Rate Limiting</div> <div>15</div>
<div>The Hidden Truth</div> <div>15</div>	<div>JWT signature validation by</div> <div>15</div>	<div>URL Manipulation</div> <div>20</div>	<div>Directory Traversal</div> <div>20</div>

# Herramientas

- **DevTools (Edge):** Para abrir la herramienta damos clic derecho inspeccionar sobre la pagina o directamente con F12.
- Para el laboratorio tenemos dos pestañas muy útiles que serán  **Elements** primera para mirar el código fuente de la pagina (también se puede obtener por medio de la combinación de teclas “Ctrl + U”) y la segunda para conocer las peticiones que salen hacia el servidor.  **Network**

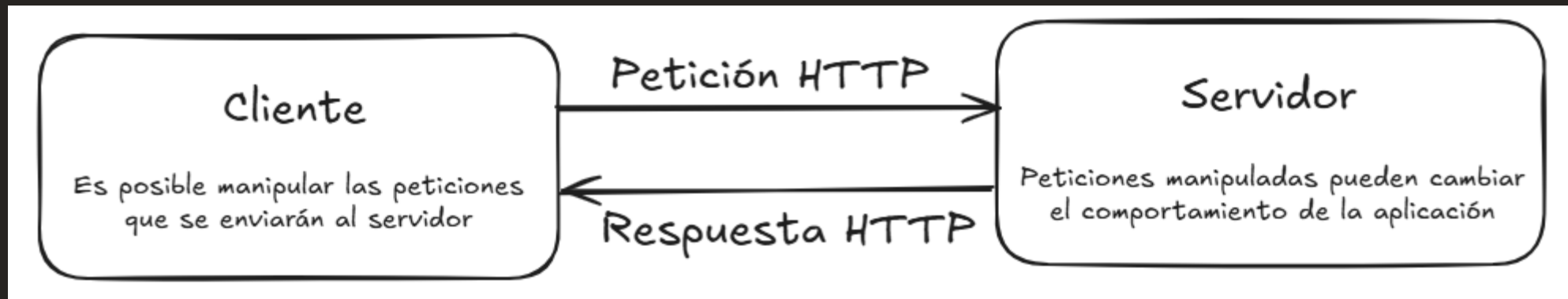
# DevTools - Network

Así se ven las peticiones cuando van al servidor.



Situándonos en la petición de nuestro interés podemos conocer todas sus cabeceras, cuerpo, obtener la petición completa, tiempo de respuesta, response, etc. Para posteriormente, porque no... **Modificar esta petición según nuestras necesidades.**

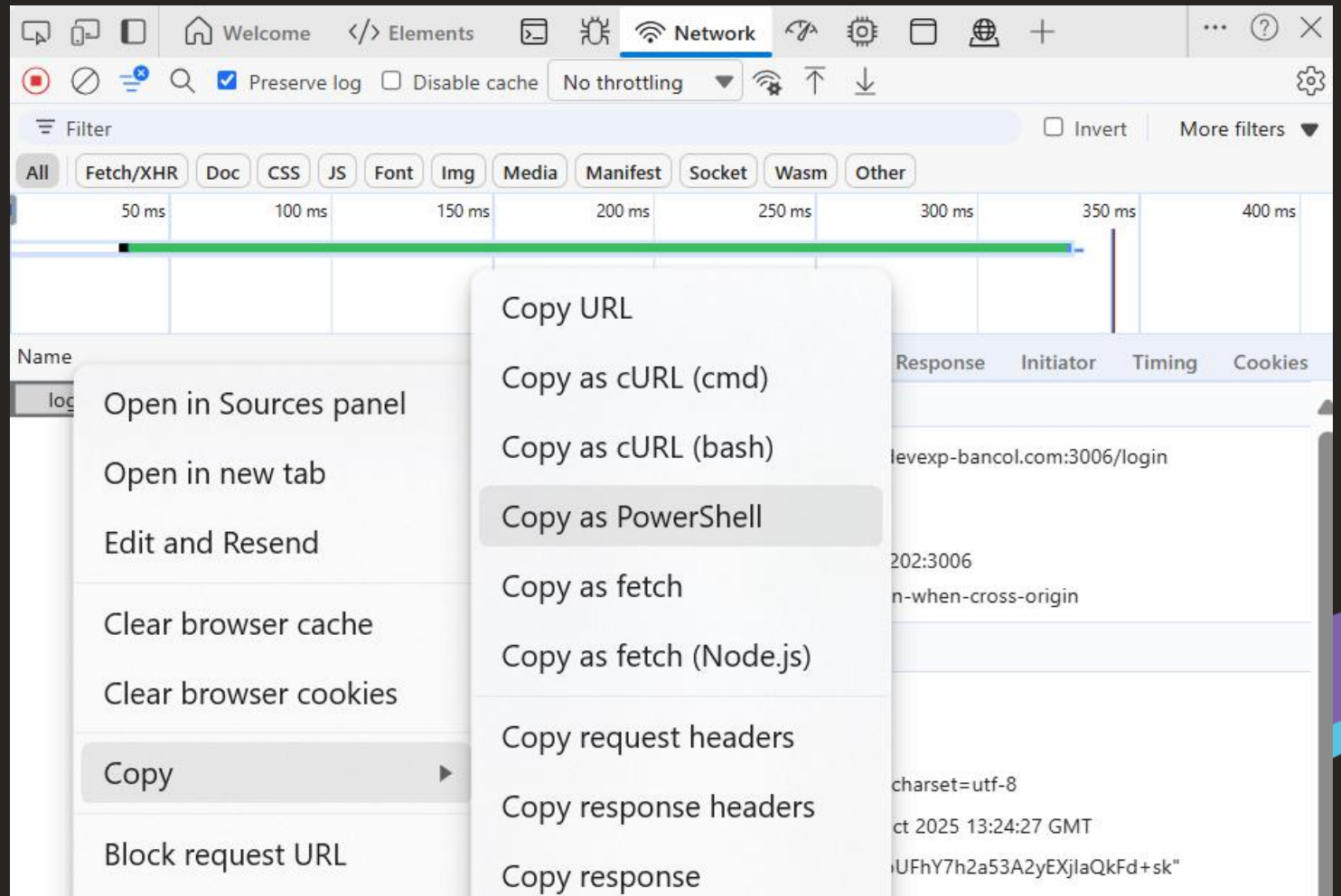
# Manipulación de peticiones



# DevTools – Network

## Manipulación de peticiones.

Con clic derecho sobre la petición podemos copiar la petición de diferentes formas, por ejemplo, por medio de powershell y posteriormente enviarla directamente desde nuestra CLI.





# Powershell

## Manipulación de peticiones.

Dado el caso de que la respuesta de la petición no se muestre completa, podemos guardar el response en una variable y posteriormente acceder a su contenido como se ve en la imagen.

```
PS C:\Users\ocvelez>
PS C:\Users\ocvelez> $response = Invoke-WebRequest -UseBasicParsing -Uri "http://ctf.devexp-bancol.com:3006/login" `
>> -Method "POST" `
>> -WebSession $session `
>> -Headers @{
>>     "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=0.7"
>>     "Accept-Encoding"="gzip, deflate"
>>     "Accept-Language"="es,es-ES;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6,es-CO;q=0.5"
>>     "Cache-Control"="max-age=0"
>>     "Referer"="http://ctf.devexp-bancol.com:3006/"
>>     "Upgrade-Insecure-Requests"="1"
>> } `
>> -ContentType "application/x-www-form-urlencoded" `
>> -Body "user=admin&pass=12345"
PS C:\Users\ocvelez> $response.RawContent
HTTP/1.1 200 OK
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 2015
Content-Type: text/html; charset=utf-8
Date: Wed, 15 Oct 2025 13:43:14 GMT
ETag: W/"7df-XoUFhY7h2a53A2yEXjIaQkFd+sk"
X-Powered-By: Express

<!DOCTYPE html>
<html>
<head>
<title>Access Denied - DevSecOps CTF Bintec</title>
<style>
  body {
    font-family: Arial, sans-serif;
```

