UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

Séptimo ciclo

“Control y Auditoría Informática”

Ing. Jorge Bladimir. Rubio Peñaherrera, Mgs.

Tema:

Práctica de Phishing

Nombre:

- Roldan Daquilema Jhonn Alex

Período lectivo:

abril 2025 –agosto 2025

21 de mayo del 2025

Latacunga – Ecuador

PRACTICA DE PHISHING

Para esta actividad se solicita a los estudiantes realizar la siguiente actividad:

ETAPA 1

- **Seleccione un sitio web de su preferencia**

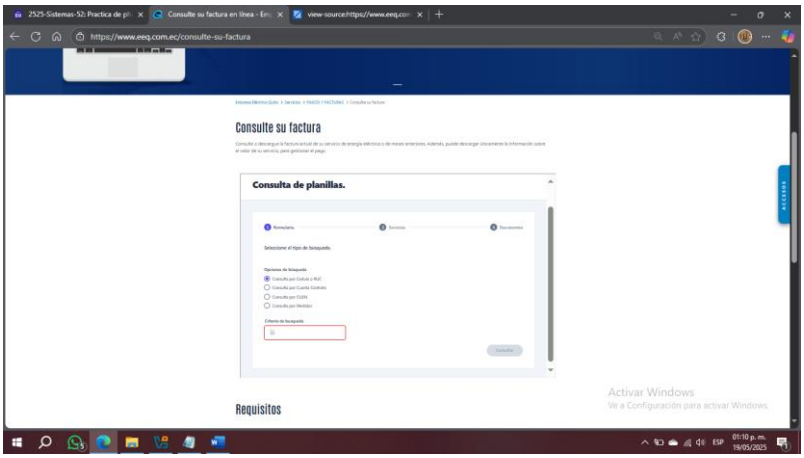

Gráfico 1. Página a clonar

El grafico 1 muestra la página web a clonar, para el ejemplo se ocupó la página de consulta de facturas del servicio básico de Electricidad de la Empresa Eléctrica de Quito (EEQ).

- **Realice la primera practica de phishing utilizando las técnicas de copiar y pegar el código fuente creando el archivo.html**

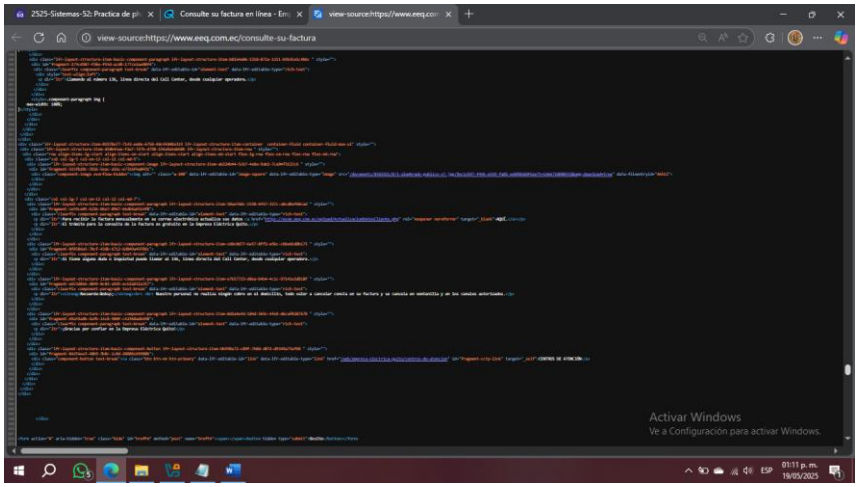

Gráfico 2. Código fuente de la página web

El gráfico 2 muestra el código fuente de la pagina a clonar, cabe recalcar que el código se extiende hasta las cuatro mil líneas de código.

Gráfico 3. Transcripción del código fuente

El gráfico 3 muestra el código transcrito de la pagina web de punta a punta para generar la clonación a través de su código fuente.

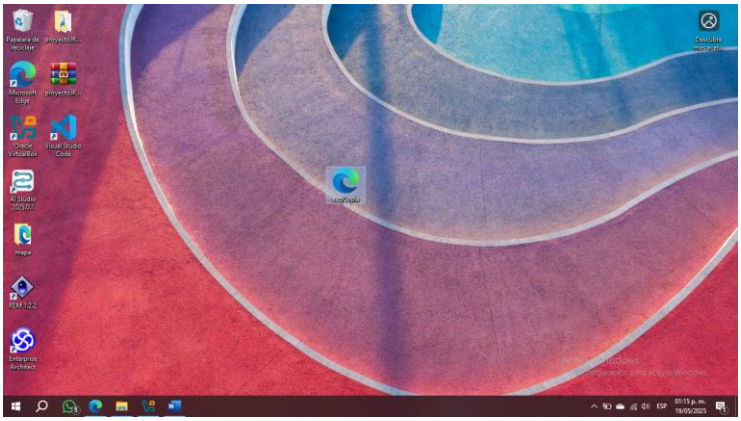

Gráfico 4. Archivo html

El grafico 4 muestra la trascripción del código fuente al formato HTML para que el navegador pueda reconocerlo y ejecutar su contenido.

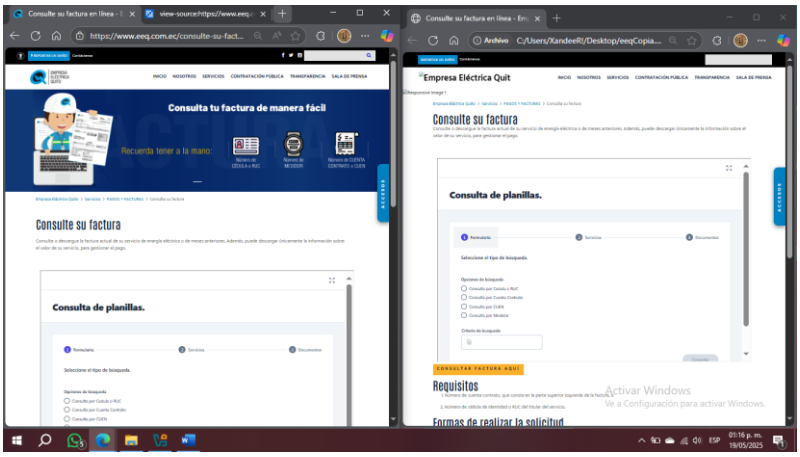

Gráfico 5. Resultado final

El grafico 5 muestra el resultado final de la clonación a partir del código fuente de la página web, a la izquierda tenemos la página web original, y a la derecha tenemos la página web clonada.

- **Audite (analice) el sistema e indique si el sitio es seguro o no.**

  La clonación del sitio mediante copia de código fuente fue exitosa, replicando casi por completo su apariencia y funcionalidad. Esto evidencia que el sitio original carece de protecciones básicas contra phishing, como ofuscación de código, validaciones de backend o CAPTCHA. El impacto de este fallo es significativo, ya que un atacante podría engañar fácilmente a los usuarios y robar información sensible sin necesidad de herramientas avanzadas. Por lo tanto, el sitio no es seguro frente a este tipo de ataques. Se recomienda aplicar medidas técnicas (ej.: ofuscación, CSP) y educar a los usuarios para mitigar el riesgo.

ETAPA 2

- **Del sitio seleccionado analice la página de dónde se puede extraer información (robo de credenciales)**

  En el sitio web clonado, el dato más crítico expuesto es la cédula de identidad, utilizada por los usuarios para consultar sus facturas de consumo eléctrico. Este documento es altamente sensible, ya que permite acceder a información personal, servicios e inclusos cuentas bancarias asociados a número de cédula.. El formulario clonado replica el campo

de ingreso de la cédula, facilitando su robo si los usuarios no identifican que están en una página falsa.

- **Luego realice el respectivo phishing utilizando la herramienta Setoolkit de Kali Linux para verificar si es posible o no el robo de credenciales.**

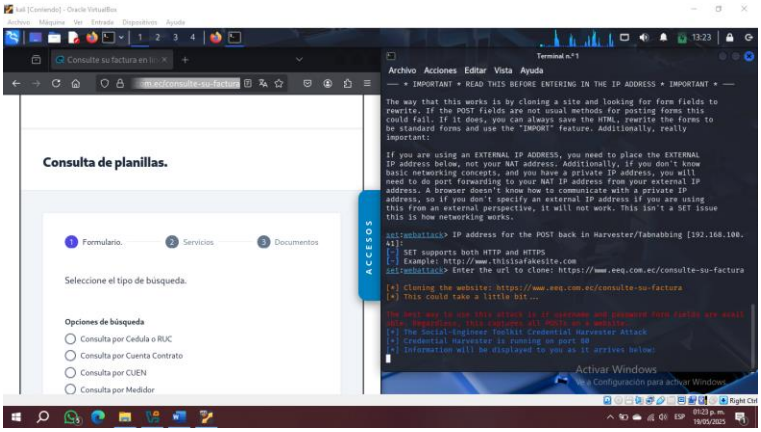

Gráfico 6. Clonación de la página a través de SEToolKit

El gráfico 6 muestra la clonación de la página web a través de la herramienta SEToolKits, a través de la URL de la pagina web, la herramienta está generando la clonación en la dirección IP 192.196.100.41

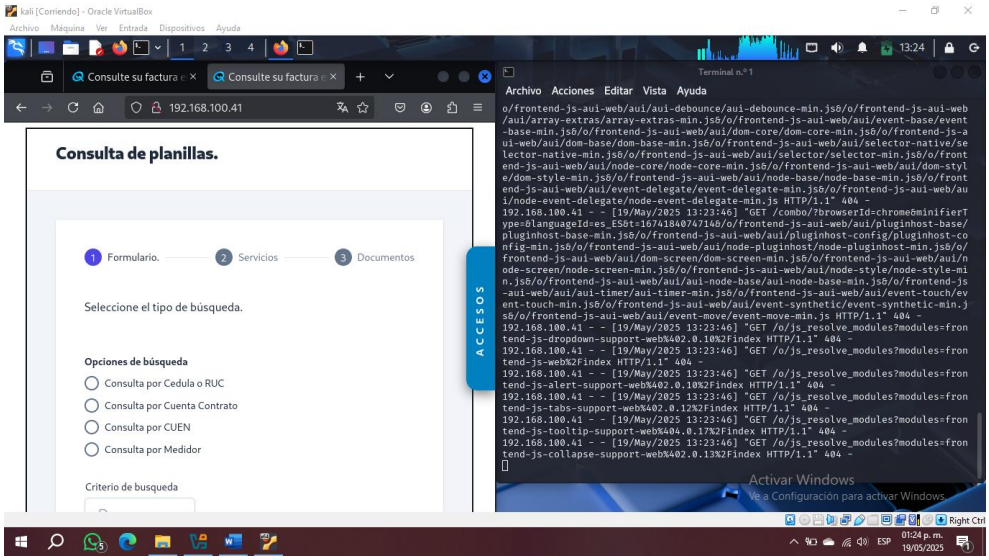

Gráfico 7. Ingreso a la página clonada

El grafico 7 muestra el ingreso la página clonada (IP 192.196.100.41) el terminal de Kali Linux muestra todas las peticiones y respuestas que esta haciendo la página clonada, cabe destacar que la clonación de la pagina fue perfecta, no hay ninguna diferencia entre la pagina original y la página clonada a diferencia de la clonación a través de su código fuente.

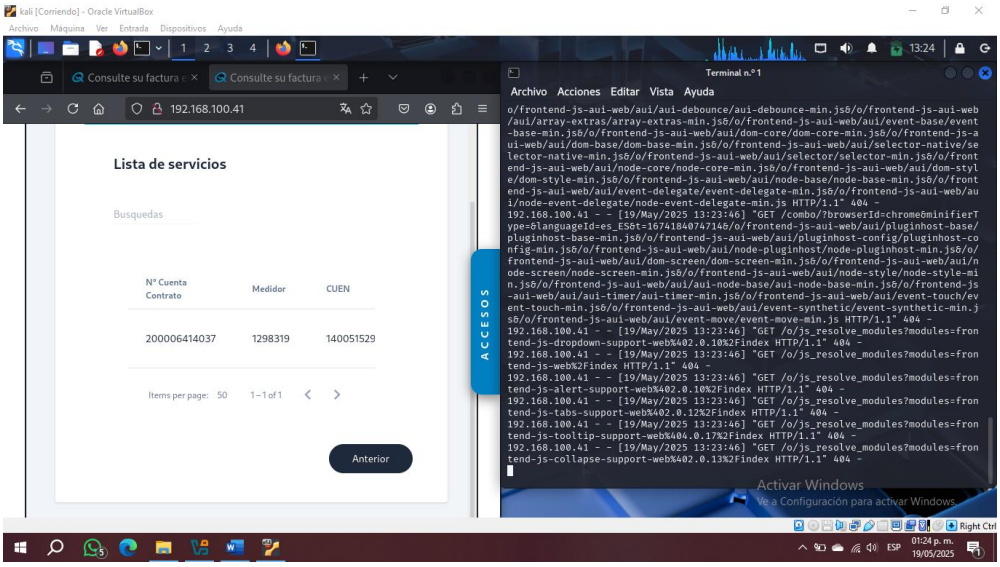

Gráfico 8. Resultado final

El grafico 8 muestra el resultado del ingreso de los datos en el formulario y el resultado de las capturas de credenciales en el terminal de Kali Linux.

- **Audite (analice) el sistema e indique si el sitio es seguro o no.**

  La clonación mediante SEToolKit replicó perfectamente el sitio web objetivo, demostrando su vulnerabilidad a ataques de phishing. Sin embargo, la herramienta no logró capturar las cédulas ingresadas, lo que sugiere que el sitio original tiene validaciones backend o cifrado que mitigaron parcialmente el robo de datos. Sin embargo, la clonación exitosa revela el riesgo latente de un atacante con mejores recursos, el cual podría eludir estas protecciones. Por tanto, el sitio no es seguro ante phishing avanzado.

CONCLUSIÓN:

La práctica de phishing realizada confirmó que el sitio analizado es vulnerable a clonaciones maliciosas, tanto por métodos manuales (código fuente) como automatizados (SEToolKit). Si bien no se extrajeron datos sensibles en esta prueba, la réplica perfecta del sitio lo hacen susceptible a ataques reales. Se concluye que el sistema no es seguro ante phishing avanzado. Esta actividad subraya la importancia de auditar sistemas propios para identificar riesgos antes de que sean explotados por actores maliciosos.