Año 2025

Desarrollo Seguro de Aplicaciones
Práctica 1 - Introducción y criptografía

Términos relacionados:

- OWASP top 10 (**2021**): **A02 (Cryptographic Failures)**

Fecha de entrega: 17/04/2025 a las 17:59

CTF

Un integrante del equipo deberá registrarse en el CTF ingresando a https://ctf.dsa.linti.unlp.edu.ar y crear el equipo "team" para participar de la competencia, el resto del equipo deberán registrarse y unirse al team.

Para el resto de los ejercicios de esta práctica, **deberás comprobar que los resolviste correctamente ingresando la respuesta en el CTF**.

Nota: la bandera (flag) a encontrar posee el formato **flag{[a-z_]*}**

Ejercicios - Encoding

2) Develar el mensaje que se intentó ocultar utilizando un sistema de codificación:

a) 102 108 97 103 123 101 109 112 101 122 97 110 100 111 95 97 95 101 110 99 111 100 101 97 114 125
b) ZmxhZ3szbmMwZGVhcl9uMF8zc19lbmNyMXB0NHJ9
c) 6-12-1-7{2-9-5-14-22-5-14-9-4-15-19-1-4-19-1}
d) 66 6c 61 67 7b 68 33 78 63 6f 64 33 34 6e 64 30 5f 74 30 64 30 7d
e) `..-. .-.. .- --. { .... --- .-.. .. ... }`

Ejercicios - Hashing

3) Utilizando alguna página que permita la búsqueda inversa de hashes, busca el texto plano de los siguientes:

a) bef58f652fddb1c20ecbfdb7cf31d932
b) c8074675a6310657d3ddf7f35a61bf393af41141
c) 111fca2d52def4c33f4d8f1be7e74d14b65d365e5ddb91610c3c0dbecc192073b0b0df28213e3828cc0321f6286baf94449a4f8803203be3293595f4d67ff7e2

4) Hashing - MD5 hacker: Encontrá la clave correcta https://clientside.dsa.linti.unlp.edu.ar/md5/.

Ejercicio - Criptografía

5) Criptografía Básica - AES: Para encontrar la flag en este reto vas a tener que desencriptar la variable “flagEncrypted” con la password “myPassword”: https://clientside.dsa.linti.unlp.edu.ar/decrypt

---

Ejercicios - Introducción a HTTP/HTML/JS

6) Estos ejercicios sirven para aprender conceptos básicos de HTML, HTTP y JS. Todos se pueden resolver en el cliente (tu navegador). Para resolverlos vas a necesitar:

- Ver el código fuente de la página (HTML y JS)
- Ver las peticiones HTTP de respuesta
- Debuggear JS para manipular el valor de una variable
- Utilizar las herramientas de programador del navegador

A. Mirá los source: Encontrá la bandera: https://clientside.dsa.linti.unlp.edu.ar/comentario/

B. Cabeceras: Sabes ver los requerimientos HTTP de respuesta?: https://cabeceras.dsa.linti.unlp.edu.ar/

C. Login?: Encontrá las credenciales correctas para obtener la flag: https://clientside.dsa.linti.unlp.edu.ar/login

D. Debugging JS: Utilizá tu capacidad de debugger JS. Para encontrar la flag utiliza breakpoints y cambiá de valor la variable “getFlag”: https://clientside.dsa.linti.unlp.edu.ar/breakpoint/

E. Manipulando requests nivel 1: ¿Podés mandar variables por POST sin tener un formulario? https://manipulandorequests.dsa.linti.unlp.edu.ar/

Ejercicio - PGP

1) La finalidad de este ejercicio es trabajar los conceptos de **Pretty Good Privacy (PGP)** vistos en clase, para ello cada alumno/a deberá formar grupo de hasta tres personas y comunicarlo a la cátedra de la siguiente manera:
    - El correo debe contener apellido, nombre, nro. de alumno y usuario de github, usuario y grupo del CTF de todos sus miembros
    - El correo debe estar **firmado con PGP**
    - Adjuntar las claves PGP de los/as integrantes del grupo.
    - Enviar el correo **cifrado con PGP** tanto como para sus compañeros como para:

- einar@info.unlp.edu.ar
- mcarbone@linti.unlp.edu.ar
- sandrazilla@gmail.com
- nmacia@info.unlp.edu.ar