TRABAJO PRÁCTICO N° 3

- **Título del trabajo:** (Panel Django - Captura de Flags y Resolución del Quizz)
- **Nombre y fecha:** Dante Gabriel Balbuena Atar 20/05/2025
- **Profesor:** Lisandro Lezaeta
- **Carrera:** Tecnicatura Universitaria en Ciberseguridad
- **Año:** 2do año
- **Materia:** tratamiento de vulnerabilidades
- **Institución:** UGR

Índice

1. Introducción

2.1 Flag 1

2.2 Flag 2

2.3 Flag 3

2.4 Flag 4

2.5 Flag 5

2.6 Flag 6

2.7 Flag 7

2.8 Flag 8

2.9 Flag 9

2.10 Flag 10

2.11 Flag 11

3. Resultado del Quizz

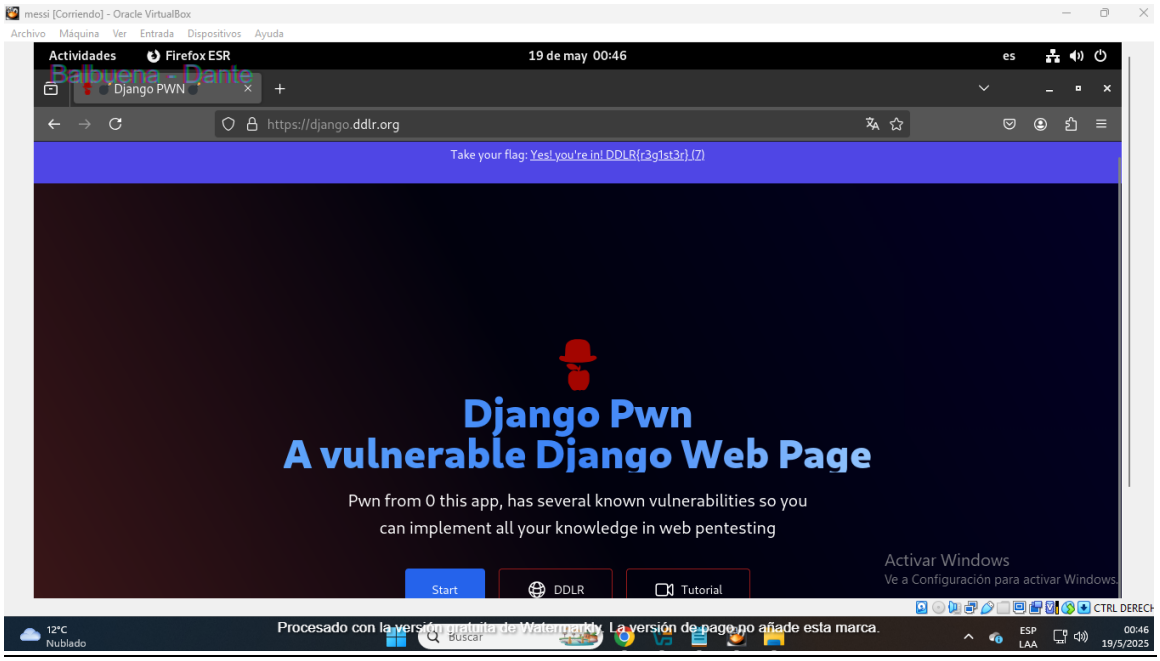
4. Conclusión

1. Introducción

El presente trabajo práctico tiene como objetivo la explotación de vulnerabilidades presentes en un panel web desarrollado con Django. Cada vulnerabilidad, una vez descubierta, revela una flag que representa la correcta ejecución del ataque. El proceso culmina con un quizz de validación, donde se ingresan las flags obtenidas para evaluar el desempeño total. Este ejercicio pone a prueba los conocimientos en seguridad web, incluyendo XSS, SQLi, CSRF, IDOR, manipulación de cookies y otras técnicas.

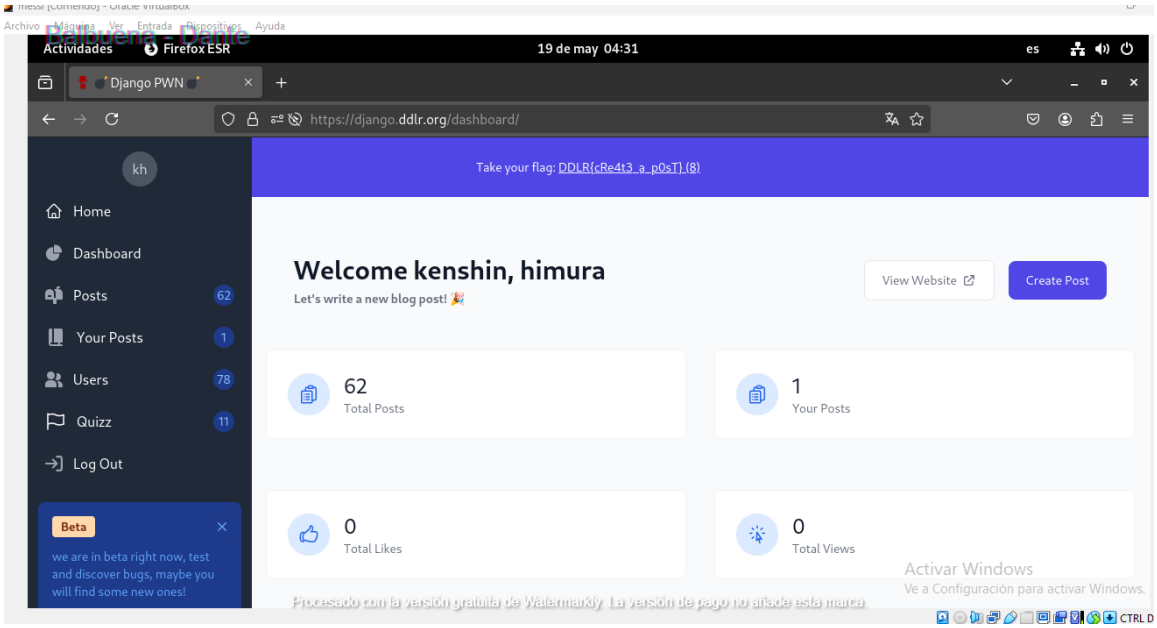
2.1 Flag 1

Flag obtenida: Yes! you're in! DDLR{r3g1st3r} (7)



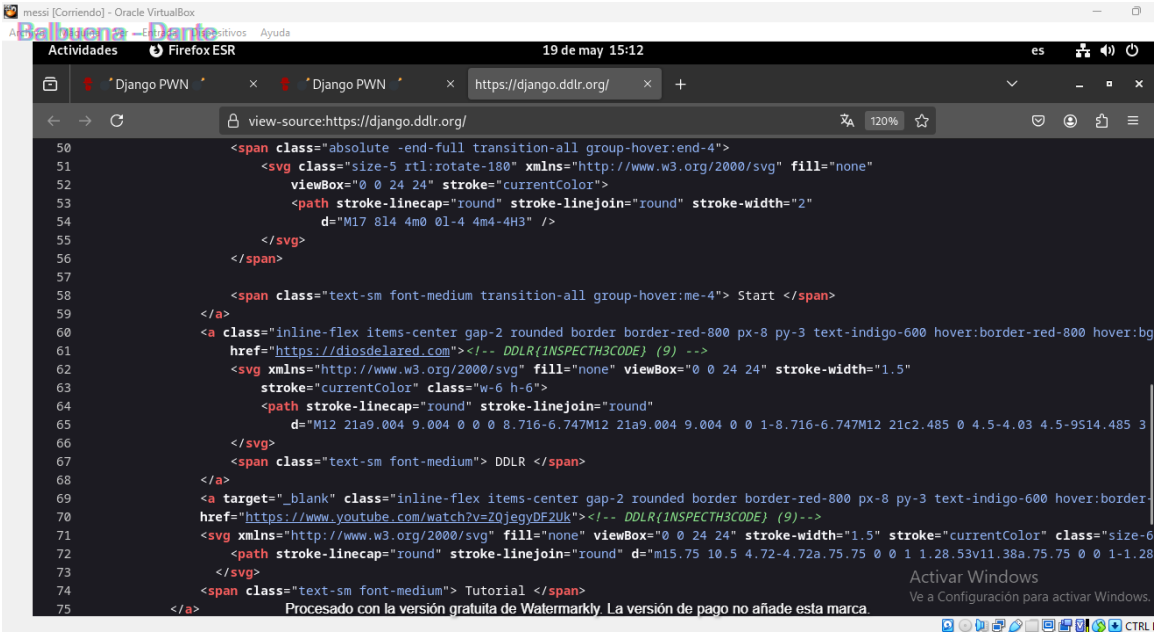
2.2 Flag 2

Flag obtenida: DDLR{cRe4t3 a p0sT} (8)



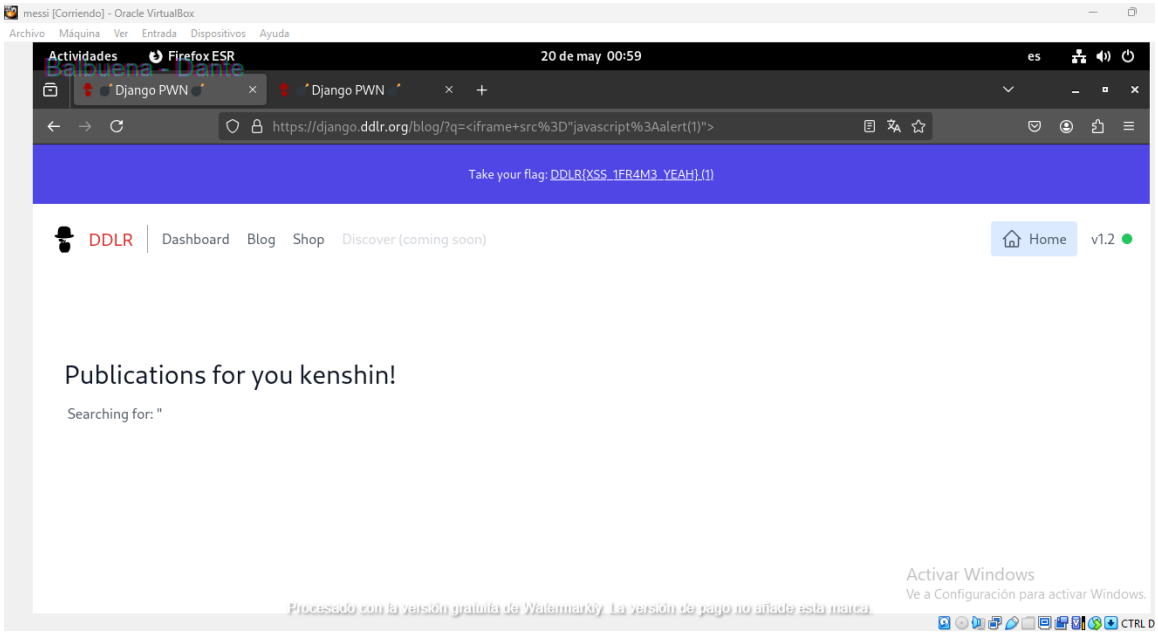
2.3 Flag 3

Flag obtenida: DDLR{1NSPECTH3C0DE} (9)



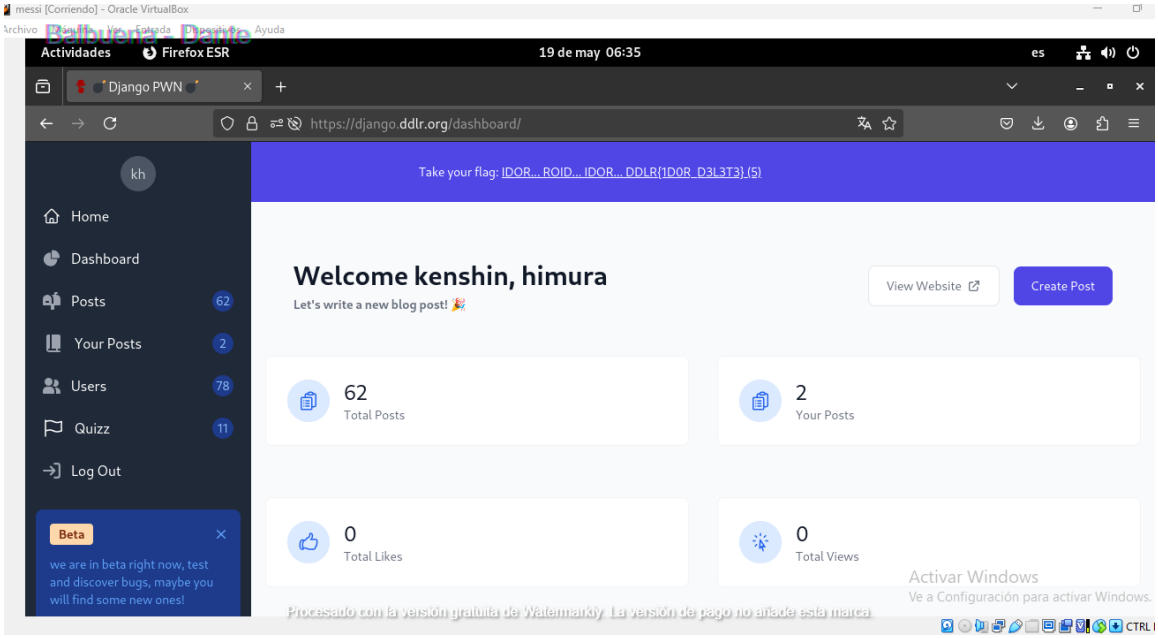
2.4 Flag 4

Flag obtenida: DDLR{XSS 1FR4M3 YEAH}(1)



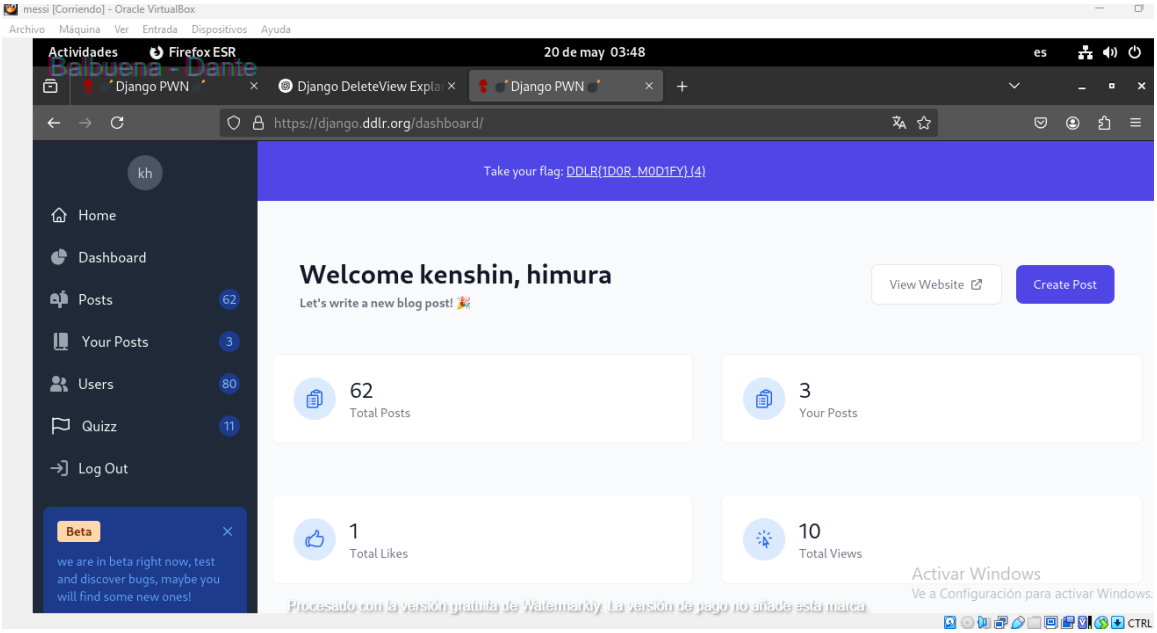
2.5 Flag 5

Flag obtenida: DDLR{1D0R D3L3T3} (5)



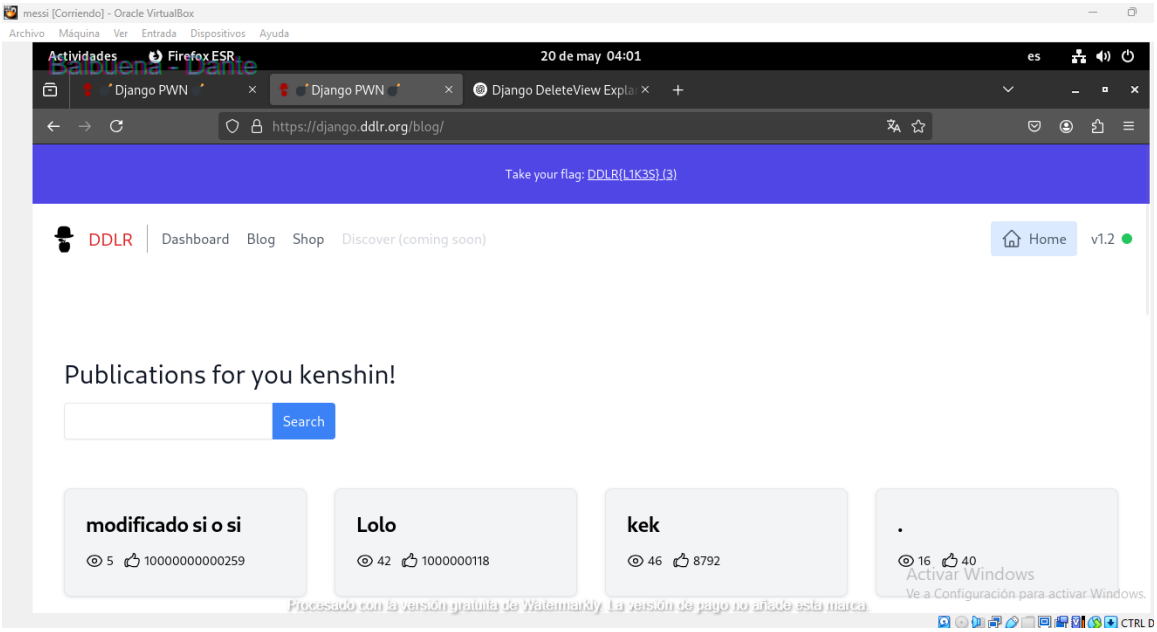
2.6 Flag 6

Flag obtenida: DDLR{1D0R M0D1FY} (4)



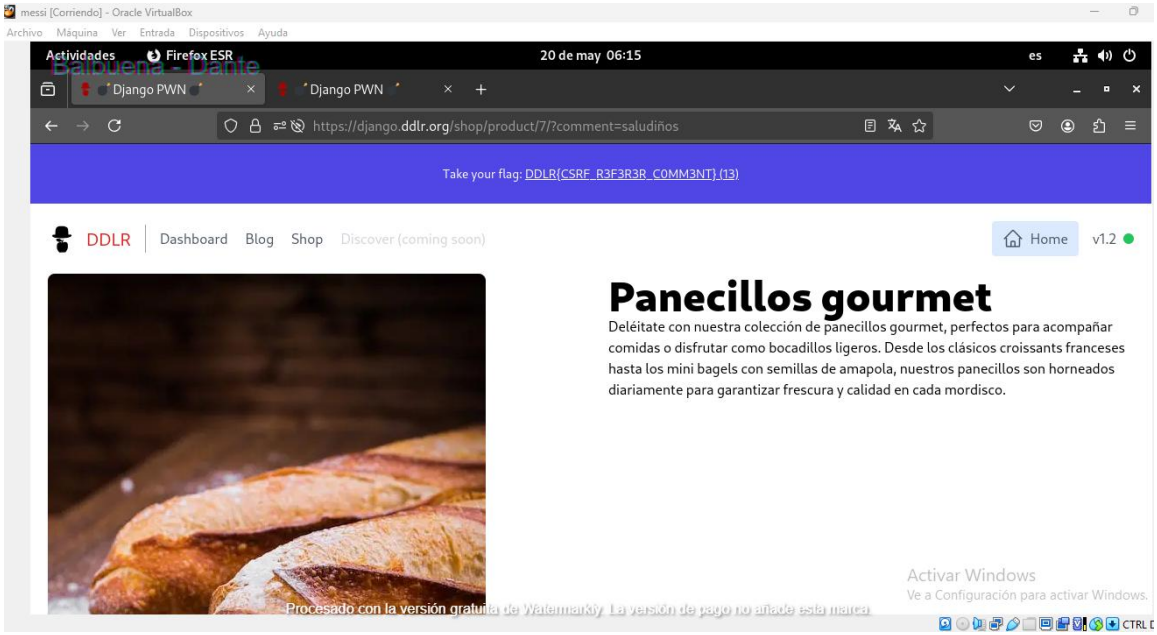
2.7 Flag 7

Flag obtenida: DDLR{L1K3S} (3)



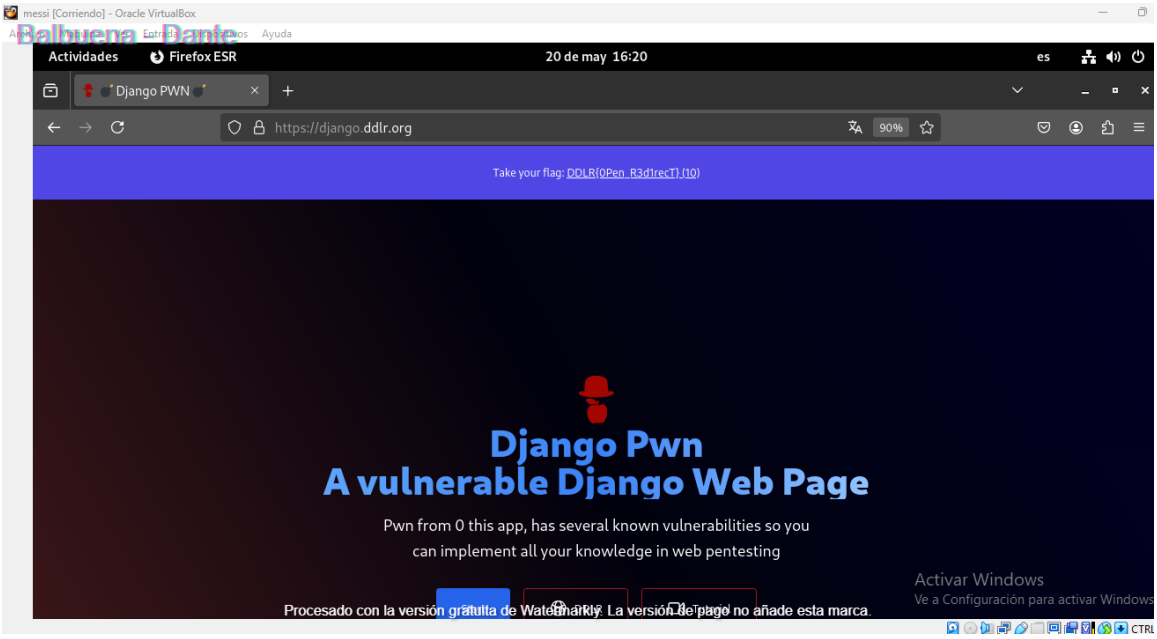
2.8 Flag 8

Flag obtenida: DDLR{CSRF R3F3R3R C0MM3NT} (13)



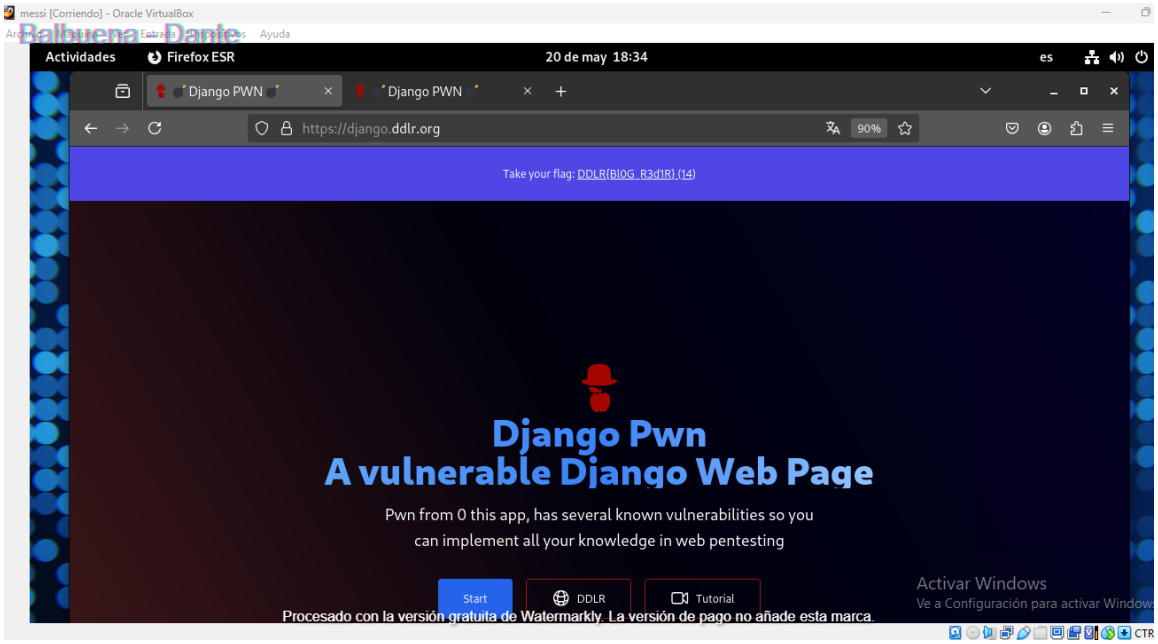
2.9 Flag 9

Flag obtenida: DDLR{0Pen R3d1recT} (10)



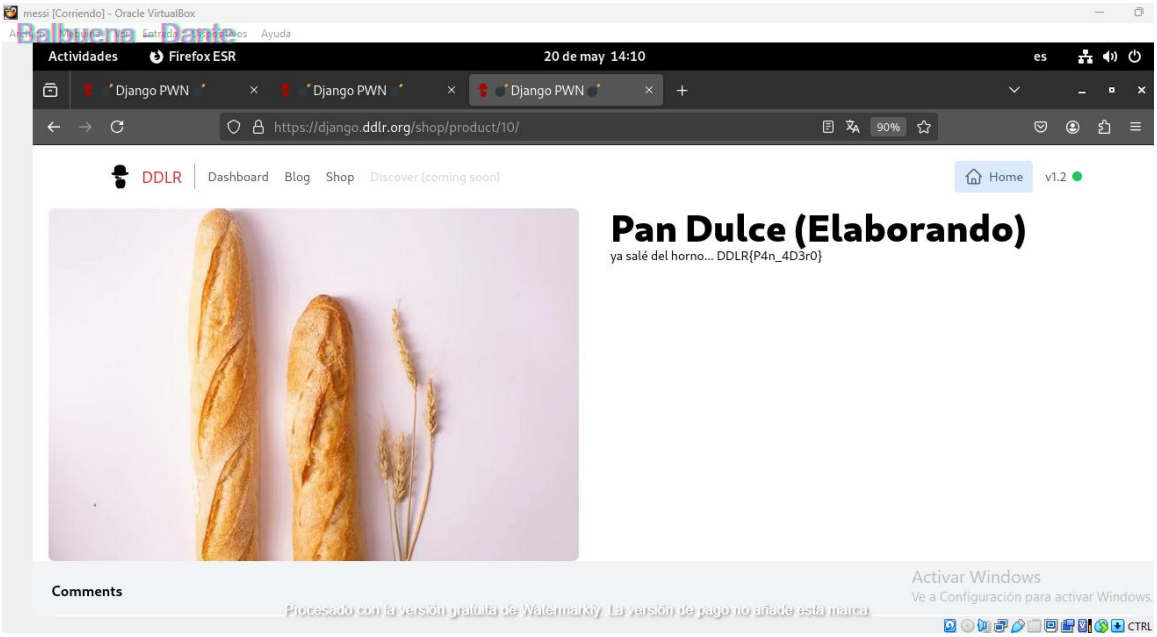
2.10 Flag 10

Flag obtenida: DDLR{Bl0G R3d1R} (14)

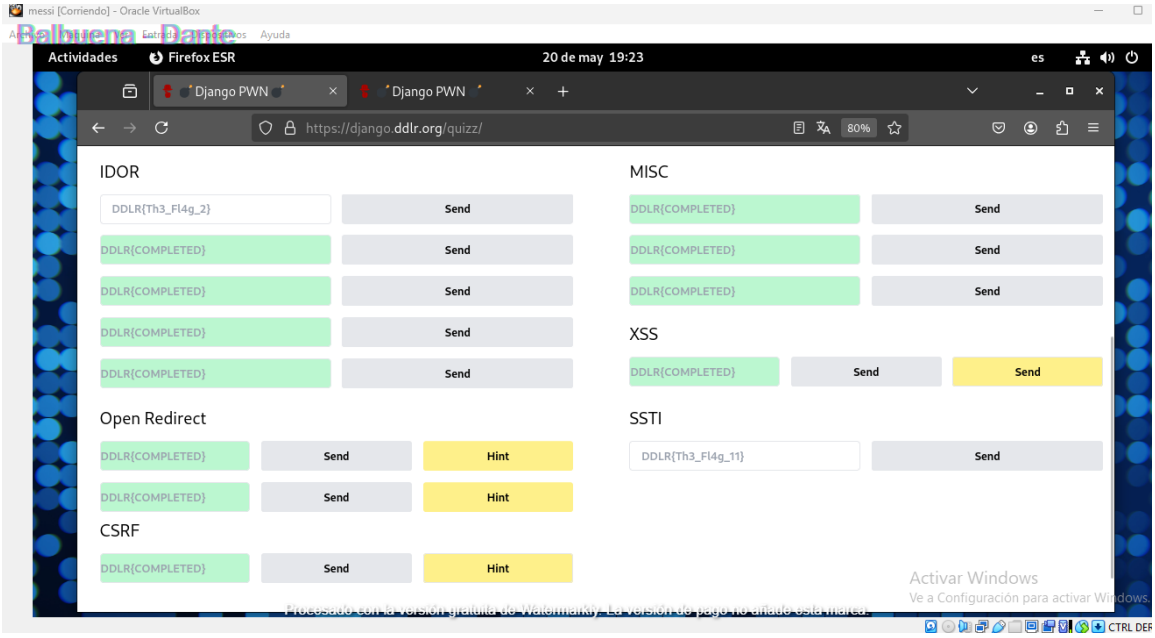


2.11 Flag 11

Flag obtenida: DDLR{P4n_4D3r0}



3. Resultado del Quizz



4. Conclusión

El trabajo permitió afianzar los conocimientos adquiridos en la materia, abordando vulnerabilidades reales en entornos controlados. La obtención de las 11 flags demuestra un dominio sólido de las técnicas de explotación y de la metodología de análisis de seguridad ofensiva. Si bien falto explotar dos vulnerabilidades mas debido a inconvenientes personales que afectaron el tiempo disponible que poseo y no fue posible documentarlo pero eso no quita el hecho de que lo voy a resolver si o si pronto en algun momento dado.