TUGAS
KEAMANAN JARINGAN
SEMESTER GENAP 2025/2026
PENERATION TESTING USING XRAY

Disusun Oleh:

Ridayanti Wardani – 152023168

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

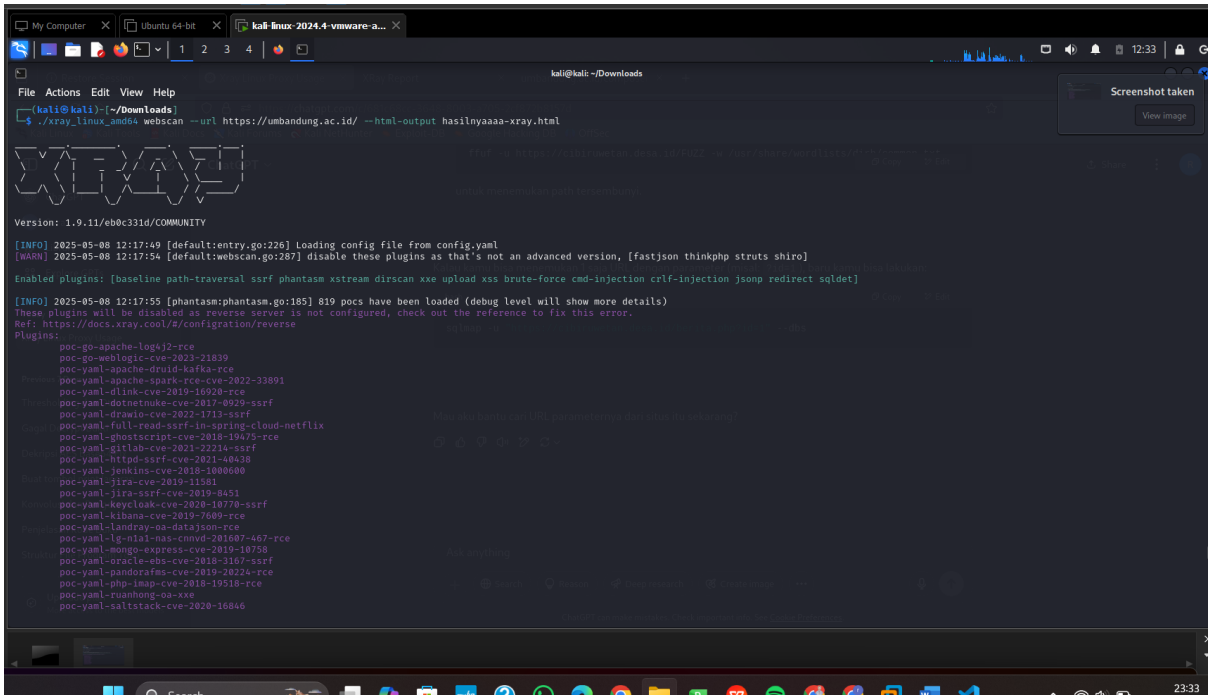
INSTITUT TEKNOLOGI NASIONAL

BANDUNG

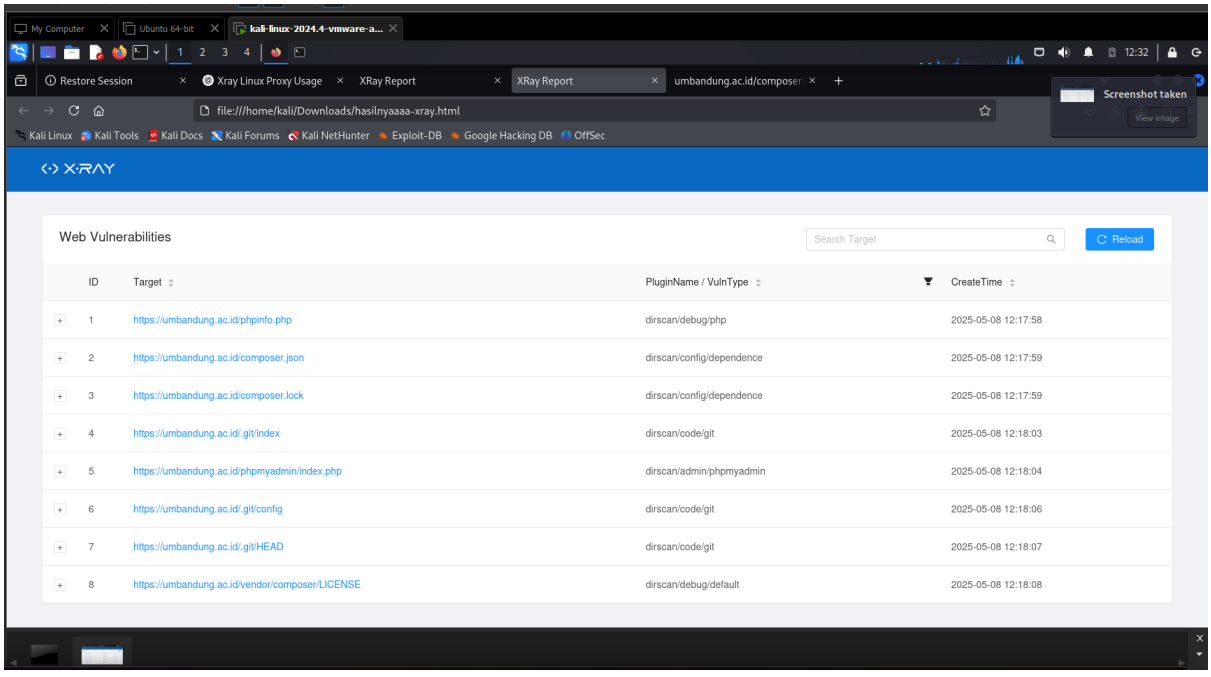
2025

1. Penetration testing menggunakan tools xray

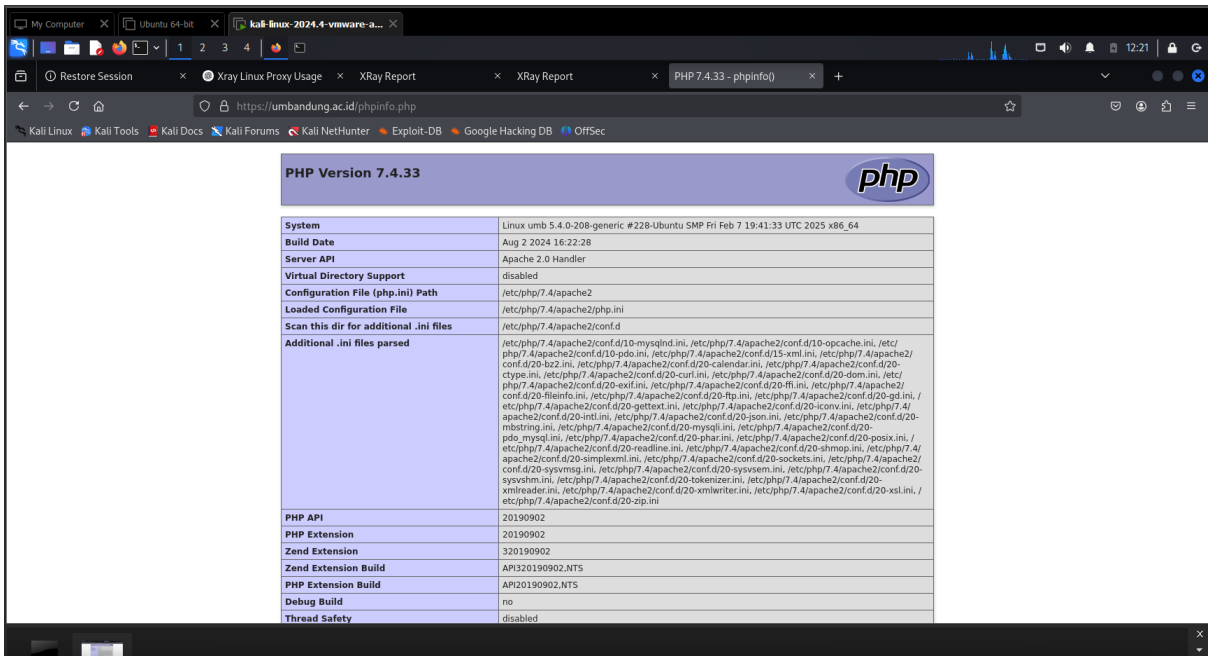
- Lakukan xray test pada URL yang sudah ditentukan
  URL Target: https://umbandung.ac.id



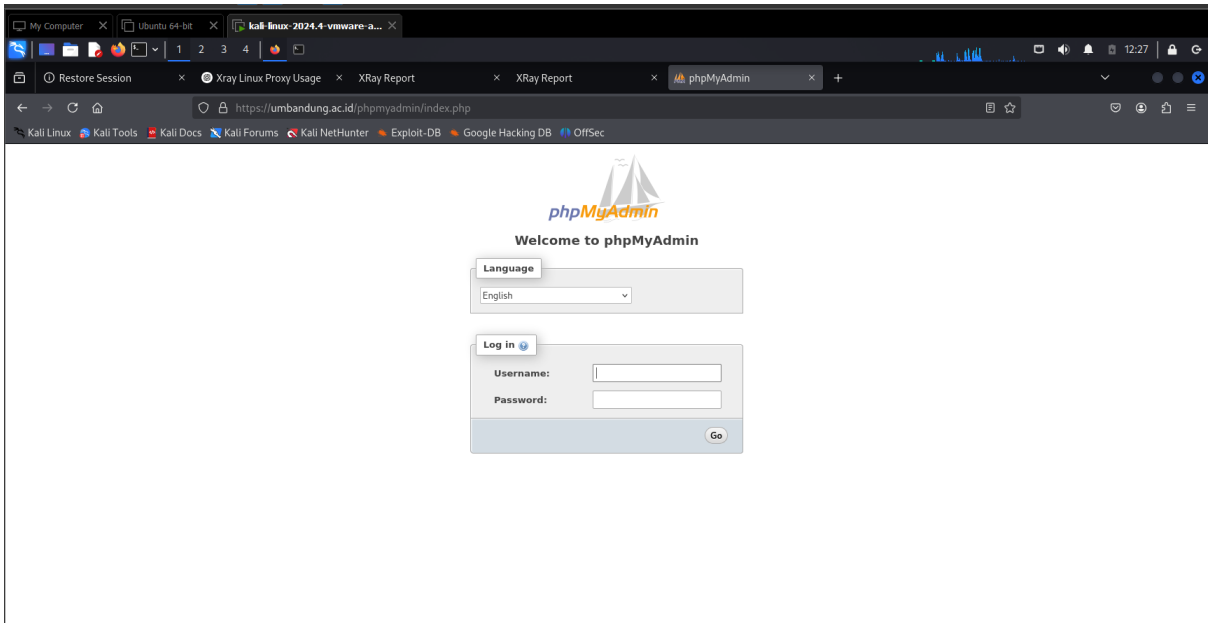
Hasil :



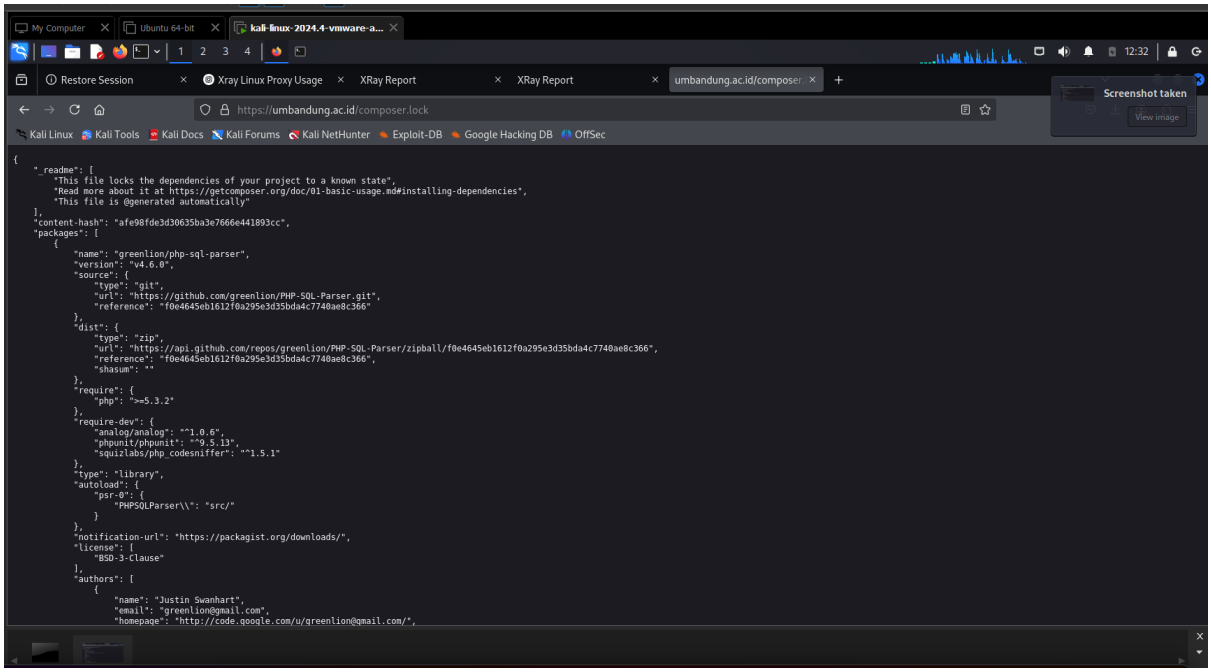
Dari hasil pemindaian dengan xray, ditemukan sejumlah file dan direktori yang dapat mengungkapkan informasi sensitive pada server. Beberapa file tersebut berpotensi meningkatkan risiko serangan siber.

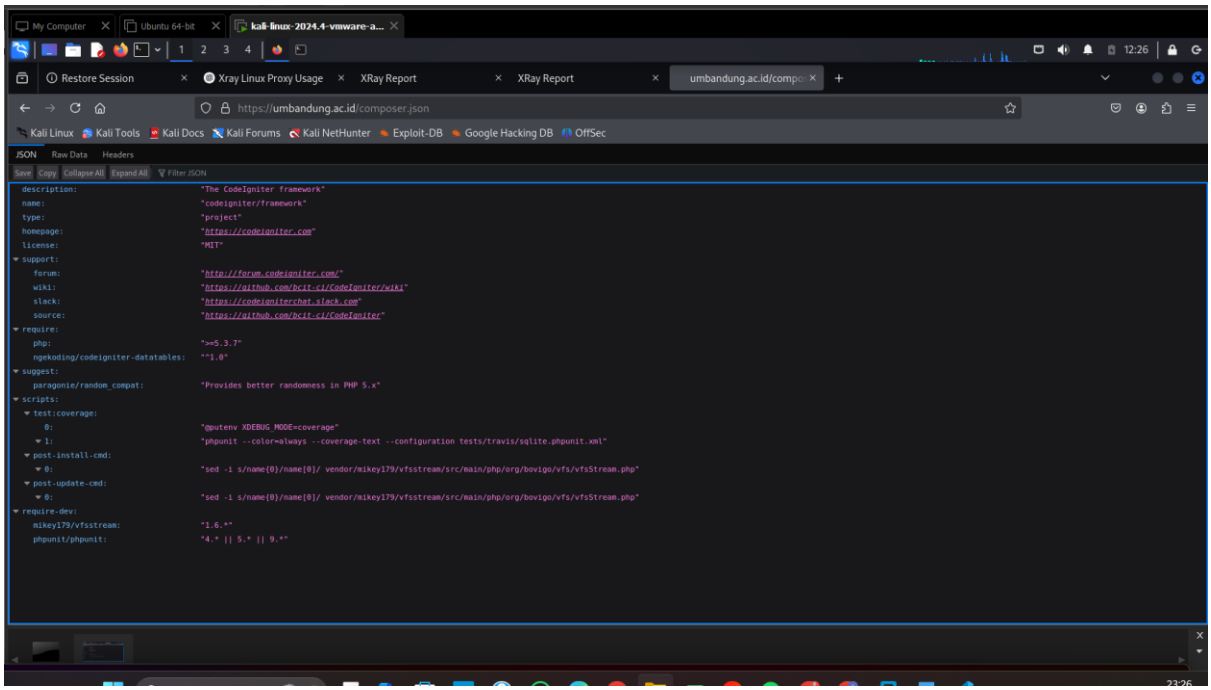


Situs umbandung.ac.id terdeteksi memiliki file phpinfo.php yang dapat diakses publik. Halaman ini berpotensi menjadi **informasi awal untuk fingerprinting** oleh penyerang, karena memberikan informasi lengkap mengenai konfigurasi server.

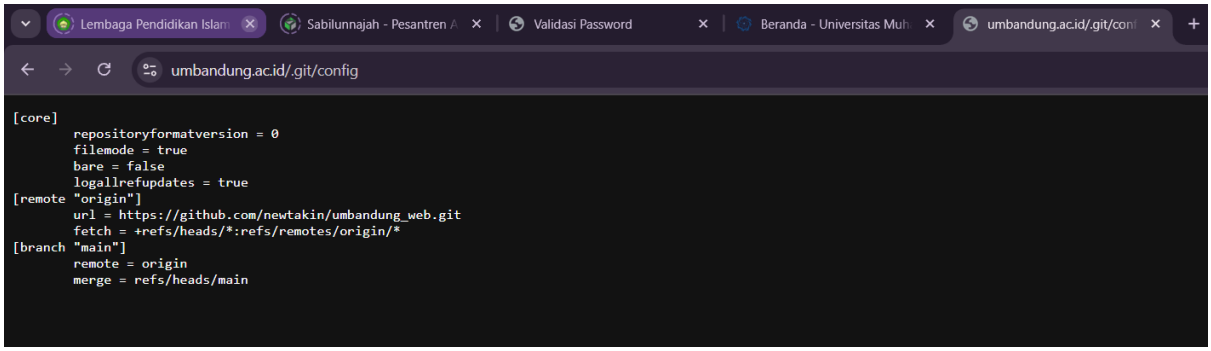


URL https://umbandung.ac.id/phpmyadmin/ dapat diakses publik tanpa pembatasan. Hal ini sangat berisiko karena membuka akses ke manajemen database secara langsung.





Berdasarkan hasil analisis terhadap file composer.json dan composer.lock pada situs *umbandung.ac.id*, ditemukan bahwa situs ini menggunakan framework CodeIgniter versi 3.5.7 serta beberapa library pihak ketiga seperti greenlion/PHP-SQL-Parser. File konfigurasi tersebut seharusnya bersifat internal, namun dapat diakses publik, sehingga menimbulkan potensi risiko keamanan. Informasi ini mengungkap versi PHP minimum yang digunakan (≥5.3.2), dependensi library, dan informasi pengembang, yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk menyusun eksploitasi berdasarkan kerentanan versi atau library yang digunakan. Selain itu, akses ke halaman login phpMyAdmin juga terdeteksi.



Terbukanya akses ke file .git/config menunjukkan adanya celah keamanan serius, karena dapat memberikan informasi sensitif terkait struktur proyek dan lokasi repositori Git publik atau privat.