

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

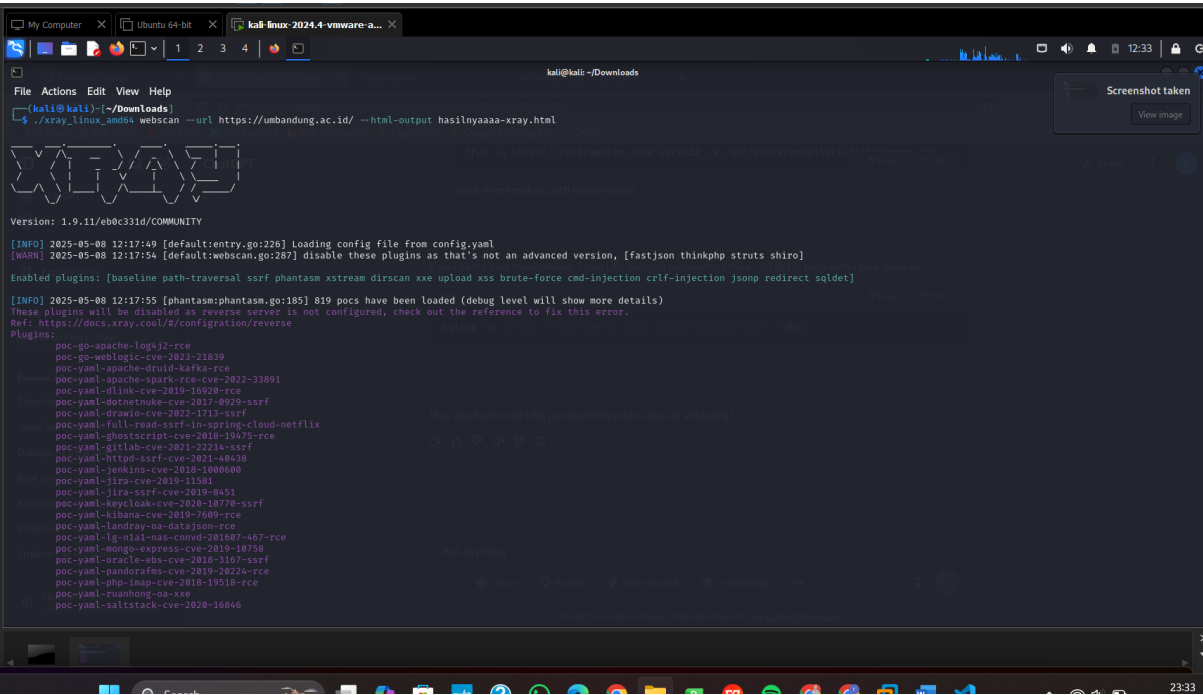


Disusun Oleh:
Ridayanti Wardani – 152023168

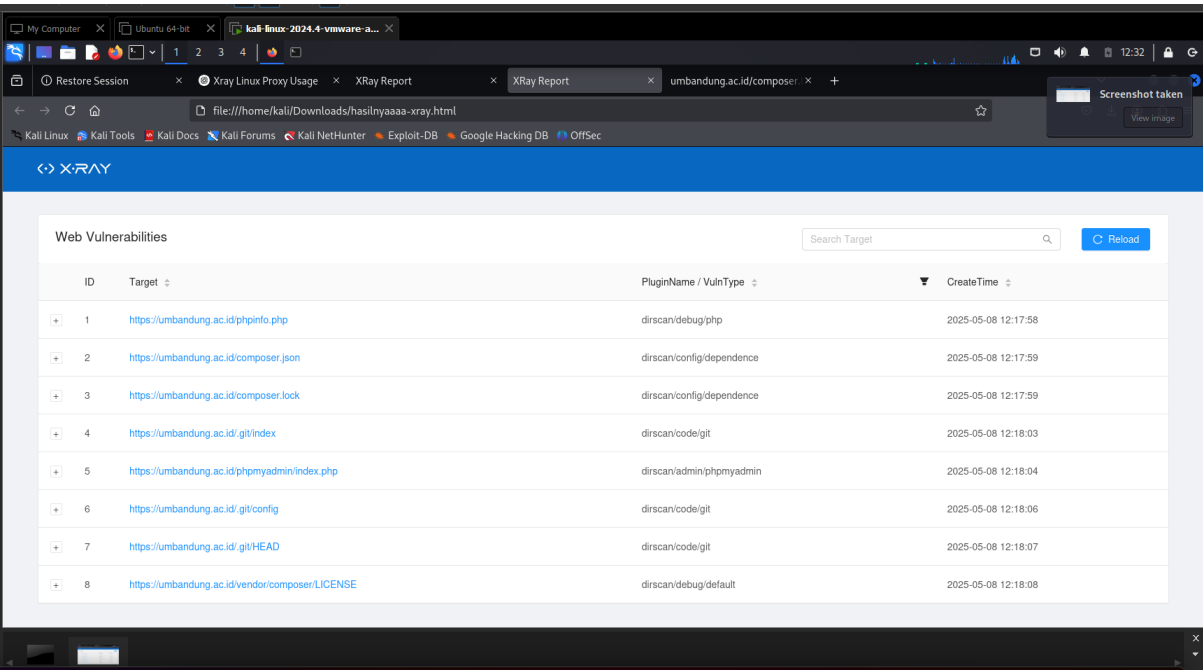
PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL
BANDUNG
2025

1. Penetration testing menggunakan tools xray

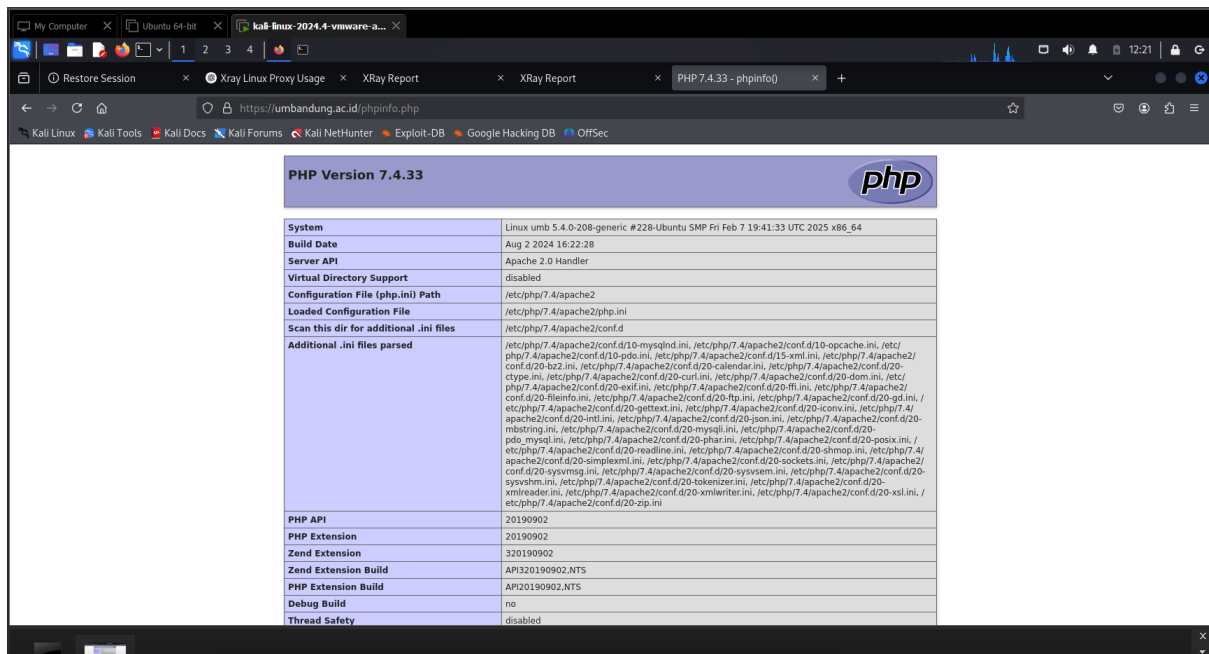
- Lakukan xray test pada URL yang sudah ditentukan
URL Target: <https://umbandung.ac.id>



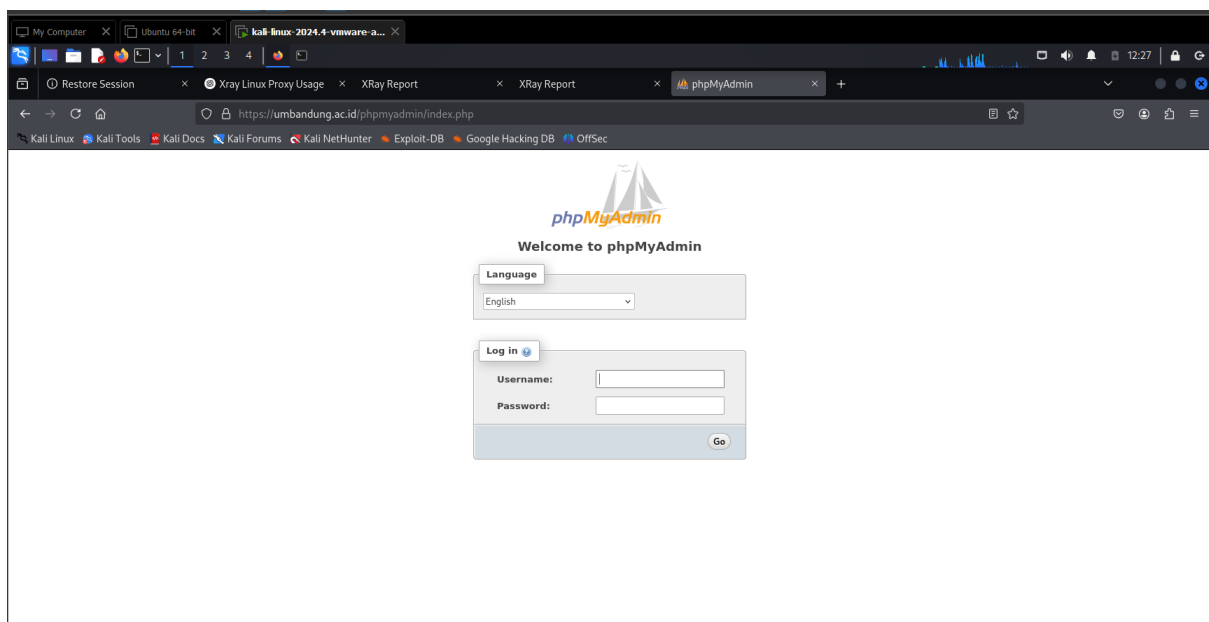
Hasil :



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.

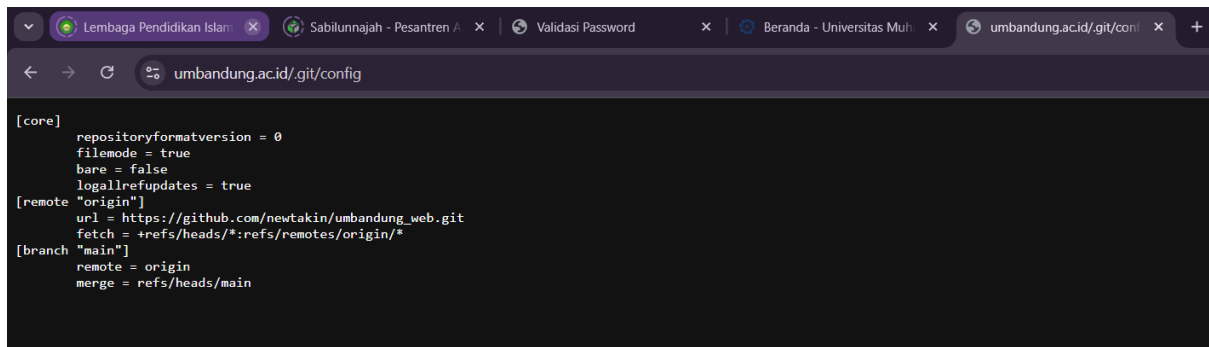


URL <https://umbandung.ac.id/phpmyadmin/> dapat diakses publik tanpa pembatasan. Hal ini sangat berisiko karena membuka akses ke manajemen database secara langsung.

```
{
  "readme": [
    "This file locks the dependencies of your project to a known state",
    "Read more about it at https://getcomposer.org/doc/01-basic-usage.md#installing-dependencies",
    "This file is @generated automatically"
  ],
  "content-hash": "afe98fde3d30635ba3e7666e41893cc",
  "packages": [
    {
      "name": "greenlion/php-sql-parser",
      "version": "v4.6.0",
      "source": {
        "type": "git",
        "url": "https://github.com/greenlion/PHP-SQL-Parser.git",
        "reference": "f0e4d9eb1612f0a295e3d35bd4c7740a8c366"
      },
      "dist": {
        "type": "zip",
        "url": "https://api.github.com/repos/greenlion/PHP-SQL-Parser/zipball/f0e4d9eb1612f0a295e3d35bd4c7740a8c366",
        "reference": "f0e4d9eb1612f0a295e3d35bd4c7740a8c366",
        "shasum": ""
      },
      "require": {
        "php": ">=5.3.2"
      },
      "require-dev": {
        "analog/analog": "~1.0.6",
        "phpunit/phpunit": "~9.5.13",
        "squizlabs/php_codesniffer": "~1.5.1"
      },
      "type": "library",
      "autoload": {
        "psr-0": {
          "PHPSQLParser\\": "src/"
        }
      },
      "notification-url": "https://packagist.org/downloads/",
      "license": [
        "BSD-3-Clause"
      ],
      "authors": [
        {
          "name": "Justin Swanhart",
          "email": "greenlion@gmail.com",
          "homepage": "http://code.google.com/u/greenlion@gmail.com/"
        }
      ]
    }
  ]
}
```

```
{
  "description": "The CodeIgniter framework",
  "name": "codeigniter/framework",
  "type": "project",
  "homepage": "https://codeigniter.com",
  "license": "MIT",
  "support": {
    "forum": "http://forum.codeigniter.com",
    "wiki": "https://github.com/bcit-ci/CodeIgniter/wiki",
    "slack": "https://codeigniterchat.slack.com",
    "source": "https://github.com/bcit-ci/CodeIgniter"
  },
  "require": {
    "php": ">=5.3.7",
    "myk373/vfsstream": "~1.6.*",
    "phpunit/phpunit": "4.* || 5.* || 9.*"
  },
  "require-dev": {
    "paragonie/random_compat": "Provides better randomness in PHP 5.x"
  },
  "scripts": {
    "test-coverage": [
      "phpunit --color=always --coverage-text --configuration tests/travis/sqlite.phpunit.xml"
    ],
    "post-install-cmd": [
      "sed -i s/name[0]/ vendor\\/mikey173\\/vfsstream\\/src\\/mass\\/php\\/org\\/bovigo\\/vfs\\/vfsStream\\.php/"
    ],
    "post-update-cmd": [
      "sed -i s/name[0]/ vendor\\/mikey173\\/vfsstream\\/src\\/mass\\/php\\/org\\/bovigo\\/vfs\\/vfsStream\\.php/"
    ]
  }
}
```

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 ($\geq 5.3.2$), 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.



```
[core]
  repositoryformatversion = 0
  filemode = true
  bare = false
  logallrefupdates = true
[remote "origin"]
  url = https://github.com/newtakin/umbandung_web.git
  fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
  remote = origin
  merge = refs/heads/main
```

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.