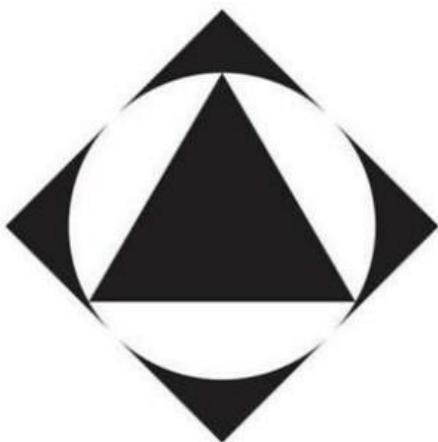


**TUGAS  
KEAMANAN JARINGAN  
SEMESTER GENAP 2025/2026  
PENERATION TESTING USING XRAY**



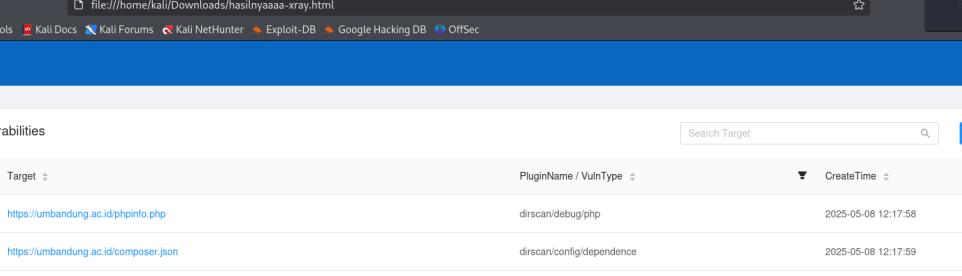
Disusun Oleh:  
Ridayanti Wardani – 152023168

**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 :



The screenshot shows the XRay Report interface with a list of vulnerabilities found on the target website. The vulnerabilities are categorized by plugin name and type, with their creation times listed.

ID	Target	PluginName / VulnType	CreateTime
1	<a href="https://umbandung.ac.id/phpinfo.php">https://umbandung.ac.id/phpinfo.php</a>	dircan/debug/php	2025-05-08 12:17:58
2	<a href="https://umbandung.ac.id/composer.json">https://umbandung.ac.id/composer.json</a>	dircan/config/dependence	2025-05-08 12:17:59
3	<a href="https://umbandung.ac.id/composer.lock">https://umbandung.ac.id/composer.lock</a>	dircan/config/dependence	2025-05-08 12:17:59
4	<a href="https://umbandung.ac.id/.git/index">https://umbandung.ac.id/.git/index</a>	dircan/code/git	2025-05-08 12:18:03
5	<a href="https://umbandung.ac.id/phpmyadmin/index.php">https://umbandung.ac.id/phpmyadmin/index.php</a>	dircan/admin/phpmyadmin	2025-05-08 12:18:04
6	<a href="https://umbandung.ac.id/.git/config">https://umbandung.ac.id/.git/config</a>	dircan/code/git	2025-05-08 12:18:06
7	<a href="https://umbandung.ac.id/.git/HEAD">https://umbandung.ac.id/.git/HEAD</a>	dircan/code/git	2025-05-08 12:18:07
8	<a href="https://umbandung.ac.id/vendor/composer/LICENSE">https://umbandung.ac.id/vendor/composer/LICENSE</a>	dircan/debug/default	2025-05-08 12:18:08

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.

**PHP Version 7.4.33**

<b>System</b>	Linux umb 5.4.0-208-generic #228-Ubuntu SMP Fri Feb 17 19:41:33 UTC 2025 x86_64
<b>Build Date</b>	Aug 2 2024 16:22:28
<b>Server API</b>	Apache 2.0 Handler
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	/etc/php/7.4/apache2
<b>Loaded Configuration File</b>	/etc/php/7.4/apache2/php.ini
<b>Scan this dir for additional .ini files</b>	/etc/php/7.4/apache2/conf.d
<b>Additional .ini files parsed</b>	/etc/php/7.4/apache2/conf.d/10-mysqli.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-dom.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-fm.ini, /etc/php/7.4/apache2/conf.d/20-gd.ini, /etc/php/7.4/apache2/conf.d/20-headers.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mbstring.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-pspell.ini, /etc/php/7.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini, /etc/php/7.4/apache2/conf.d/20-wddx.ini, /etc/php/7.4/apache2/conf.d/20-xmllwriter.ini, /etc/php/7.4/apache2/conf.d/20-xsl.ini, /etc/php/7.4/apache2/conf.d/20-zip.ini
<b>PHP API</b>	20190902
<b>PHP Extension</b>	20190902
<b>Zend Extension</b>	320190902
<b>Zend Extension Build</b>	API320190902.NTS
<b>PHP Extension Build</b>	API20190902.NTS
<b>Debug Build</b>	no
<b>Thread Safety</b>	disabled

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.

Welcome to phpMyAdmin

Language: English

Log in

Username:

Password:

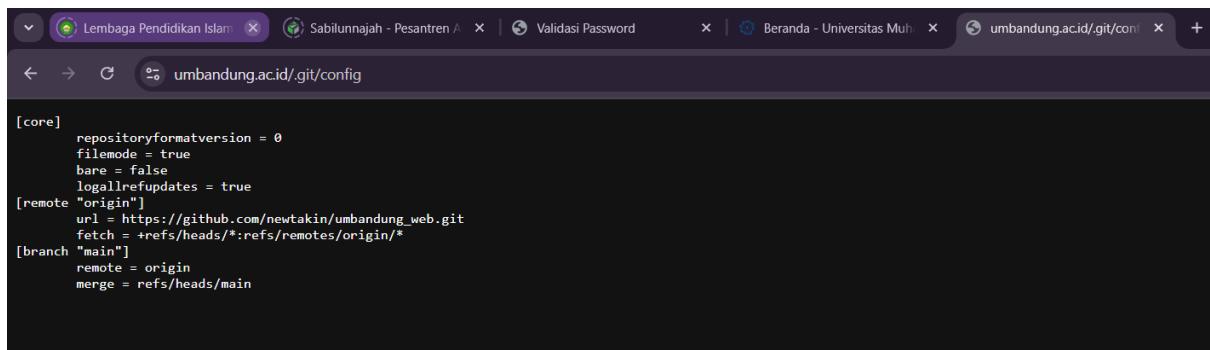
Go

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": "afe980fde3d0635ba3e7666e41893cc",
  "packages": [
    {
      "name": "greenlion/php-sql-parser",
      "version": "4.6.0",
      "source": {
        "type": "git",
        "url": "https://github.com/greenlion/PHP-SQL-Parser.git",
        "reference": "f0e4645eb1612f0a295e3d35bda4c7740ae8c366"
      },
      "dist": {
        "type": "zip",
        "url": "https://api.github.com/repos/greenlion/PHP-SQL_Parser/zipball/f0e4645eb1612f0a295e3d35bda4c7740ae8c366",
        "reference": "f0e4645eb1612f0a295e3d35bda4c7740ae8c366",
        "shasum": ""
      },
      "require": {
        "php": ">=5.3.2"
      },
      "require-dev": [
        "analog/analog": "1.0.6",
        "phpunit/phpunit": "9.5.13",
        "squizlabs/php_codesniffer": "1.5.1"
      ],
      "types": "library",
      "autoload": {
        "psr-0": {
          "PHPSQLParser": "src/"
        }
      },
      "notification-url": "https://packagist.org/downloads/",
      "license": [
        "BSD-3-Clause"
      ],
      "authors": [
        {
          "name": "Justin Seward",
          "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",
    "netkoding/codeigniter-databases": "1.0"
  },
  "suggest": {
    "paragonie/random_compat": "Provides better randomness in PHP 5.x"
  },
  "scripts": {
    "test:coverage": [
      {
        "command": "\$env{XDEBUG_MODE}=coverage",
        "script": [
          "phpunit --color=always --coverage-text --configuration tests/travis/sqlite.phpunit.xml"
        ]
      }
    ],
    "post-install-cmd": [
      {
        "command": "sed -i s/name@*/name@*/ vendor/mikey179/vfsstream/src/main/php/org/bovigo/vfs/vfsStream.php"
      }
    ],
    "post-update-cmd": [
      {
        "command": "sed -i s/name@*/name@*/ vendor/mikey179/vfsstream/src/main/php/org/bovigo/vfs/vfsStream.php"
      }
    ]
  },
  "require-dev": {
    "mikey179/vfsstream": "1.6.*",
    "phpunit/phpunit": "4.* || 5.* || 9.*"
  }
}
```

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 eksplorasi 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.