

# Pentest report - [www.pepal.eu](http://www.pepal.eu)

## Summary

- I. Overview
- II. DNS Request
- III. Data about HTTP/HTTPS certificate
- IV. NMAP scan
- V. Nikto scan
- VI. Potential vulnerabilities
- VII. Exploit find
- VIII. Recommendations

## I. Overview

This report presents the results of a vulnerability assessment conducted on **www.pepal.eu** using Python modules. The objective of this assessment is to provide a brief overview of the security posture of the target and identify potential vulnerabilities that could be exploited by attackers.

The main objective of the assessment was to identify vulnerabilities that could be used by attackers to compromise the confidentiality, integrity, or availability of the target. Python modules are used to automate the scanning process and identify potential vulnerabilities in the target.

**Date:** 2024-05-03 09:16

**Target :** [www.pepal.eu](http://www.pepal.eu)

**Type:** vulnerability scanner

## II. DNS Request

Record name		Informations and data
A		[{'address': '51.75.130.27', 'ttl': 28800}]
CNAME		No record found
MX		No record found
NS		No record found
SOA		No record found
TXT		No record found

## III. Data about HTTP/HTTPS certificate

### Metadata

**protocol:** https:

**hostname:** www.pepal.eu

**port:** 443

### Certificate

**protocol:** https:

**hostname:** www.pepal.eu

**port:** 443

**issued\_to:** www.pepal.eu

**issued\_by:** R3

**valid\_from:** 2024-03-23T02:56:19.000Z

**valid\_to:** 2024-06-21T02:56:18.000Z

**alternate\_names:** ['DNS:www.pepal.eu']

**serial\_number:** 036F18A46082EEA96CBB3F1E9A69DD6FF9E9

**fingerprint:** 1E:66:02:01:F4:E6:F8:71:DF:

74:5C:A8:20:F9:57:30:68:C9:57:AA

**raw:**

-----BEGIN CERTIFICATE-----

MIIE5TCCA82gAwIBAgISA28YpGCC7qlsuz8emmndb/

npMA0GCSqGSib3DQEBcwUA

MDIx CzAJBgNVBAYTAIVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQQ

EwJSMzAeFw0yNDAzMjMwMjU2MTIaFw0yNDA2MjEwMjU2MTIaMBcxFTATBgNVBAMT

DHd3dy5wZXBhbC5ldTCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJeA

wHVOtFxCVvUQCqgkqDmt6M5mfZW2sm9Jqk5fcMYQewSY4hGrChB9ZB6PhapYFSe7

IVZftviN2yiKUzOTLhmihyvoFNAJxxjzbzsh3D4rRF1PVUrsIP5svs6C6PKrne68e

TqFPDrXxa3fN+FChSEzRQy49fs61AVViMdP5WX9/

lpetYtk3xa2bAkOhpBX8dtPR m6c/

0NtMrTDpogNhp5pSHGq41RjM8mrBBxfXySMqjU+fMt7H69mrhKWhD1pPg6IB

1tTVroqJbnOCQ0YQHP+slBn52nDBYd3QOB4xi/

gVmrkLGKeZ5jooQgNLafsTVPhS

UzV6O3qQfDhiUjSNEmMCAwEAAaOCAg4wggIKMA4GA1UdDwEB/

wQEAWIFoDAdBgNV

HSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwDAYDVROTAQH/

BAIwADAdBgNVHQ4E

FgQUeS+Ej7LWhoiRXm+UUKZR8EDzh8YwHwYDVR0jBBgwFoAUFC6zF7dYVsuuUAIA

5h+vnYsUwsYwVQYIKwYBBQUHAQEESTBHMCEGCCsGAQUFBzABhhVodHRwOi8vcjMu

by5sZW5jci5vcmcwlgYIKwYBBQUHMAKGFmh0dHA6Ly9yMy5pLmxlbmNyLm9yZy8w

FwYDVR0RBBAwDoIMd3d3LnBlcGFsLmV1MBMGA1UdIAQMMAowCAYGZ4EMAQIBMIIB

BAYKKwYBBAHWeQIEAgSB9QSB8gDwAHYA7s3QZNxbGs7FXLedtM0TojKHRny87N7D

UUhZRnEftZsAAAGOaXPIYAAABAMARzBFAiEAvTFE0ycH1nEKn3AG4a+7APx9WLry

NS1hDGkSxJlz7TICID7hQzPlng7R09/

gWtZ40PrARvEB+ejxmMfn2VgMLq8tAHYA

PxdLT9ciR1iUHWUchL4NEu2QN38fhWrrwb8ohez4ZG4AAAGOaXPQJAAABAMARzBF

AiAd4/eX97jIBJ1UCPU4+J+kAKJTyIPUGAM50r0dXmIWsglhAOCrR7zYx/

80I90J

QN0D1R59m5OS9a+0TC0pfCfnL3yTMA0GCSqGSib3DQEBcwUAA4IBAQB4Hb1sms8C

IPEVGw1ymvleaSj1PljM7ZRhJ8YIVkl0A4zhBuKmzlkNFhBMd8AtkvCv2yxaV6zM

nsYk2fQjBX0XxsD6ZZ8TYgi8K5PThfLpz66JMWVxldCqoXLrwg3Eenfjppq0dHn+h

C9gph8HdLFgQnMrDrZdQyDYhtlFGfPSyGNRo7yno/03/bi5KvEtHdW+J/

f11Lopg

cMSEXrAJXFDXt+HXvWVU0R9pkk5BhcKzfh8cYgOIHX3CsK23HWJYBW7131xTnKP

7En4UFnnT38xTE993JIM1GwrG063TLNRcr4WdNGla4mo+j73wtCtsO5xuq6T3lik

eYiKHKigdBv2 -----END CERTIFICATE-----

## IV. NMAP scan

```
[['51.75.130.27', 21, 'ftp', ''], ['51.75.130.27', 22, 'ssh', ''],  
['51.75.130.27', 25, 'ssh', ''], ['51.75.130.27', 80, 'http', ''],  
['51.75.130.27', 443, 'ssl', '']]
```

## V. Nikto scan

Web server : Apache

The server supports compression.

Target URL don't use any redirection

Target URL isn't protected by a basic HTTP authentication

The anti-clickjacking X-Frame-Options header is not present.

## VI. Potential vulnerabilities

### CVE associated with ftp

### Service: ftp, Version:

CVE-2023-33850, CVE-2024-20918, CVE-2024-20919,  
CVE-2024-20921, CVE-2024-20926, CVE-2024-20945,  
CVE-2024-20952  
CVE-2023-22067, CVE-2023-22081, CVE-2023-5676  
CVE-2024-0737  
CVE-2024-1016  
CVE-2024-29733  
CVE-2024-20918, CVE-2024-20921, CVE-2024-20926,  
CVE-2024-20932, CVE-2024-20945, CVE-2024-20952,  
CVE-2024-22361  
CVE-2024-0731  
CVE-2024-0547  
CVE-2024-0548  
CVE-2024-0693  
CVE-2024-0732  
CVE-2024-0736  
CVE-2024-0889

CVE-2019-19368  
CVE-2024-1017  
CVE-2020-27735  
CVE-2021-4432

## VII. Exploit find

Exploit find result goes here

## VIII. Recommendations

Keep your systems up-to-date with the latest security patches and updates for all software and services running on your domain or IP address. Vulnerabilities are often discovered and patched by vendors, so it's important to stay current with updates to minimize risk.

We also recommend reviewing the list of links provided in this report, which point to known exploits and vulnerabilities affecting various services. These links can provide additional information and guidance on how to mitigate these specific security risks for your domain or IP address.

By following these recommendations and staying vigilant against emerging security threats, you can help protect your systems and data from unauthorized access and exploitation.