Pentest report - 20.7.1.11

Summary

I. Overview

This report presents the results of a vulnerability assessment conducted on **20.7.1.11** 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 11:56

Target : 20.7.1.11

Type: vulnerability scanner

II. DNS Request

Check your domain name or the API website (https://networkcalc.com/api/)

III. Data about HTTP/HTTPS certificate

Metadata

protocol: https:
hostname: 20.7.1.11
port: 443

Certificate

protocol: https:
hostname: 20.7.1.11
port: 443
issued_to: TRAEFIK DEFAULT CERT
issued_by: TRAEFIK DEFAULT CERT
valid_from: 2024-05-03T11:45:25.000Z
valid_to: 2025-05-03T11:45:25.000Z
alternate_names: ['DNS:e3f0864ee1a623ea179f4a050e00323b.685c5275a8e815078d86fc5b3658dd2f.traefik.default']
serial_number: 15D4831C3BB8690A30C5D17992EE61DB
fingerprint: F0:9F:52:7F:BA:53:4D:7F:45:A0:66:48:87:EC:4B:68:03:07:34:2B
raw:

-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAgIQFdSDHDu4aQowxdF5ku5h2zANBgkqhkiG9w0BAQsFADAf
MR0wGwYDVQQDExRUUkFFRklLIERFRkFVTFQgQ0VSVDAeFw0yNDA1MDMxMTQ
Fw0yNTA1MDMxMTQ1MjVaMB8xHTAbBgNVBAMTFFRSQUVGSUsgREVGQVVMVC
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuX+/
WLvIUYfz2SK/yUBZ
GwhX2G3z3oLT9dN4cHiInJQHOVASiWmx+HjcqVZ1Xjuk9xKyzFlqEhhqAuQ2Xp4z
+Bb58V0roz+Ml+n7rDpcDFKAWYulCEofMBV3HTzrssqlR4F4emoMyYCHPtnCWaww
EZ5pZbXSljvZj7bfjV4UkPBNRv/
XerTtax7DiMBCZI8idUid9BfVcN21j013lvLo
nKSbgrw3iX3W5aI0z4576GS/F/zrF3T1Q4EmQnWaa1/
BGru3VdNgttKjKJV5myaZ JteKOycL6x/Li54qcjkqG8EgsNn/
XXGe4Bf2mkVi3CDWEuuKfIgRC7nZCej9tfXF
KQIDAQABo4GUMIGRMA4GA1UdDwEB/
wQEAwIDuDATBgNVHSUEDDAKBggrBgEFBQcD
ATAMBgNVHRMBAf8EAjAAMFwGA1UdEQRVMFOCUWUzZjA4NjRlZTFhNjIzZWExN
NGEwNTBlMDAzMjNiLjY4NWM1Mjc1YThlODE1MDc4ZDg2ZmM1YjM2NThkZDJmL
YWVmaWsuZGVmYXVsdDANBgkqhkiG9w0BAQsFAAOCAQEAqLrsoIr/
IUgl7aGJaPwi dLt2GFCiXsEaIg/
1ZM5M1gYA8l0rBA+V+rFZD4NJ6zmXd7DFldwEY1YKudHbO5am
D0BlevgF4gDFX5h4Ow7yWbYX8nZD4j8kGVpEFeV2/
jwsi1s+ZnKGvfPcspKWuJnj OLiagtP/
qNsSocfmwFvpMw7nI7M6Bw6LwLGdDk9n78VDajrNfEkxAN3W6jx/
Esgt
xkDlCalgj99y6YR0mPWFVn4sQEuM9KYeall5fsEkuV5jGC6gkMkmKUNxlG89lkeo
8WtyYkVyCTGgxvSpNtLgioaoaybvuzi3gkhnMdtumbJJw8SNpmSD789FdnwWafix
bw== -----END CERTIFICATE-----

IV. NMAP scan

Host	Port	Service	Version
20.7.1.11	80	http	
20.7.1.11	443	http	

V. Nikto scan

The server doesn't support 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.

The X-XSS-Protection header is not defined.

VI. Potential vulnerabilities

Service: http, Version:

- CVE-2021-3007
- CVE-2013-4407
- CVE-2007-6420
- CVE-2023-45288
- CVE-2024-2653
- CVE-2015-2308
- CVE-2016-4423
- CVE-2023-44487
- CVE-2018-19790
- CVE-2021-31618
- CVE-2003-1307
- CVE-2023-34062

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.