

VULNERABILITY REPORT

This is a highly concise vulnerability report generated by Python-based modules, offering a comprehensive analysis of the target's security.

Summary

- I. Overview 1
- II. DNS Request1
- III. Data about HTTP/HTTPS certificate1
- IV. NMAP scan2
- V. Nikto scan3
- VI. Potential vulnerabilities3
- VII. Recommendations4

I. Overview

This report presents the results of a vulnerability assessment conducted on **92.51.183.222** 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 03:51

Target : 92.51.183.222

Type: vulnerability scanner

II. DNS Request

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

Metadata

Certificate

-----BEGIN CERTIFICATE----- MIIIGuzCCBaOgAwIBAgIJANka/
r6CSUHamaA0GCSqGSIb3DQEBCwUAMIHGMQswCQYD
VQQGEWJlVUzEQMA4GA1UECBMHQXJpem9uYTETMBEGA1UEBxMKU2NvdHRzZGFsZTEI
MCMGA1UEChMcU3RhcmZpZWxkIFRlY2hub2xvZ2llcywgSW5jLjEzMDEGA1UECxMq
aHR0cDovL2NlcnRzLnN0YXJmaWVsZHRlY2guY29tL3JlcG9zaXRvcnkMTQwMgYD
VQQDEytTdGFyZmllbGQgU2VjdXJlENlcnRpZmljYXRlIEF1dGhvcml0eSAtIEcy
MB4XDTI0MDMxMzExNDAXN1oXDTI1MDQxMjExNDAXN1owGjEYMBYGA1UEAxMPd3d3
LmNoaWVtZ2F1LmRlMlIiBlJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxwbO
YfPEILfwVTqmAlf4d4xox9D0np/8/0G/cTjYxxkulxhdQt8Z/vEJf3YBUZRDQj9B
VGjIOzXFsA2QqSJ20lQTGyTYJ8HtWO5Hgri7T3F8B55YOytPg3U6ko+zrqFjmadm
mEno/tJo1oI023WZWN+wh5RP2J9wxZkQd9H6RPDeoTjJ//l+UMuzMGHUMC/
vVNse m1eRMmJBhiilm6cpl5l0mjTuXnD3rMkfYe1wdB5fam1ajsGhBQLeqIG/
uAtBIWhV

REwALCnk87zorB0qywUXJPEM5KaF1inWNGbgVgyRHPQiWKQ+UuTtXQQggrN63SPX
X9UJg2m62MI/L+D8bwIDAQABo4IDVTCCA1EwDAYDVR0TAQH/
BAIwADAdBgNVHSUE FjAUBggrBgEFBQcDAQYIKwYBBQUHAWIwDgYDVR0PAQH/
BAQDAgWgMD0GA1UdHwQ2
MDQwMqAwoC6GLGh0dHA6Ly9jcmwuc3RhcmZpZWxkdGVjaC5jb20vc2ZpZzJzMS02
ODYuY3JsMGMGA1UdIARcMFowTgYLYIZIAYb9bgEHFwEwPzA9BggrBgEFBQcCARYx
aHR0cDovL2NlcnRpZmljYXRlcy5zdGFyZmllbGR0ZWNoLmNvbS9yZXBvc2l0b3J5
LzAlBgZngQwBAgEwgYIGCCsGAQUFBwEBBHYwdDAqBggrBgEFBQcwAYYeaHR0cDov
L29jc3Auc3RhcmZpZWxkdGVjaC5jb20vMEYGCCsGAQUFBzACHjpodHRwOi8vY2Vy
dGlmaWNhdGVzLnN0YXJmaWVsZHRlY2guY29tL3JlcG9zaXRvcnkvc2ZpZzluY3J0
MB8GA1UdIwQYMBaAFcVfGWhQJjg9Oy0svs1q2bY9s2ZjMCCGA1UdEQQgMB6CD3d3
dy5jaGllbWdhds5kZYILY2hpZW1nYXUuZGUwHQYDVR0OBBYEFjiqrOxyMuSIHtmN
HiCPZOiDLF3DMIIBfgYKKwYBBAHWeQIEAgSCAW4EggFqAWgAdgBOdaMnXJoQwzhb
bNTfP1LrHfDgjhuNacCx+mSxYpo53wAAAY43nPuDAAAEAwBHMEUCIHuibyaMDQFI
PY+9MuFBQoVY0aDd4SIxzyXoavUu2CsAiEAlXpEXM8ke1vIRIZM8LwRDMLKlzY3
hgjKOIQXukRZiSwAdwB9WR4S4XgqexxhZ3xe/fjQh1wUoE6VnrkDL9kOjC55uAAA
AY43nPwuAAAEAwBIMEYCIQCvoe886AuKFPKMDp09PHUvmvT8js3A6nOPHs2ohzXS
HAIhAj9+MNNKh5IfQRu/
WH8BxC2lwosyxdUbYDsMQDI9rGwoAHUAzPsPaoVxCWX+
IZtTzumyfCLphVwNI422qX5UwP5MDbAAAAGON5z8sAAABAMARjBEAiAYpInkN7s2
6vwlORDEIMTRrRXzBMyNDvG+5NJWqyrTAIgYHCFitGsXYcBVxKq7ofP7qkcpPfx
cV4SQ6tP935+f/
EwDQYJKoZIhvcNAQELBQADggEBAFnmb04eXvKZJ5jyQyVGs73B
yMzvs6ZSp5Elo6zkuBqeHHXSfOkzRQDajc3qhwp82NmqaUTAM3Rit4o8nmk38Gkp /
FTvak1gWHlo7MUcmOhktb/6r/GBsO5KfRRO/4qekqMUaFc5Nak20fMlw+mxYD8K
Zb9hUL2ijCEPgfMeQU5YTvqsJ2TR+C0XqD10f+gQBfKZRjXNpyF3wvuS+ARTHfxI
lFrntR1aaCoyQvjO1a2z6BF3g09s8qaZff28d6CtXPg3Kbz+z75FOrYuy2CsRe8I
YI6M5DFNZ8vx4Xc55a262OfTBCvnIfLT3KItXHQMtHsL02xEMrQuRNMzulEGxXE=
-----END CERTIFICATE-----

IV. NMAP scan

```
[['92.51.183.222', 21, 'ftp', '2.0.8'], ['92.51.183.222', 22, 'ssh', ''],  
['92.51.183.222', 25, 'ssh', ''], ['92.51.183.222', 80, 'http', '2.4.41'],  
['92.51.183.222', 443, 'http', '2.4.41']]
```

V. Nikto scan

Web server : Apache/2.4.41 (Ubuntu)

The server supports compression.

Version of software might be found in the following header Server : 2.4.41

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.

The X-Content-Type-Options header is not set.

VI. Potential vulnerabilities

Service: ftp, Version: 2.0.8

+-----+-----+ | | CVE associated with ftp 2.0.8 |
+=====+=====+
| CVE-2011-4088 | CVE-2012-1106 | +-----+-----+ |
CVE-2020-8169 | CVE-2020-8284 | +-----+-----+ |
CVE-2012-5660 | CVE-2012-5659 | +-----+-----+ |
CVE-2012-5659 | CVE-2012-5660 | +-----+-----+ |
CVE-2018-17189 | CVE-2019-0196 | +-----+-----+ |
CVE-2001-1112 | | +-----+-----+

Service: ssh, Version:

+-----+ | CVE associated with ssh |
+=====+ | CVE-2023-48795 |
+-----+ | CVE-2013-4436 | +-----+ |
CVE-2024-29950 | +-----+ | CVE-2020-16846 |
+-----+ | CVE-2021-43565 | +-----+ |
CVE-2017-3204 | +-----+ | CVE-2018-16837 |
+-----+ | CVE-2008-5161 | +-----+ |
CVE-2021-3148 | +-----+ | CVE-2021-45099 |
+-----+ | CVE-2019-17069 | +-----+ |
CVE-2024-29960 | +-----+

Service: ssh, Version:

+-----+ | CVE associated with ssh |
+=====+ | CVE-2023-48795 |
+-----+ | CVE-2013-4436 | +-----+ |
CVE-2024-29950 | +-----+ | CVE-2020-16846 |
+-----+ | CVE-2021-43565 | +-----+ |
CVE-2017-3204 | +-----+ | CVE-2018-16837 |
+-----+ | CVE-2008-5161 | +-----+ |
CVE-2021-3148 | +-----+ | CVE-2021-45099 |
+-----+ | CVE-2019-17069 | +-----+ |
CVE-2024-29960 | +-----+

Service: http, Version: 2.4.41

+-----+-----+-----+-----+ ||| CVE
associated with http 2.4.41 |

```
+=====+=====+=====+=====+=====+=====+=====+=====+=====+=====+
| CVE-2023-31122 | CVE-2023-43622 | CVE-2023-44487 | CVE-2023-45802 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
CVE-2019-0196 | CVE-2020-1927 | CVE-2020-1934 | | +-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
CVE-2020-13950 ||| +-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| CVE-2019-0220 | CVE-2019-10092 |
CVE-2019-10098 | CVE-2020-1927 | +-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| CVE-2019-10092 | CVE-2019-10098 |
CVE-2020-1927 | CVE-2020-1934 | +-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| CVE-2023-38709 | CVE-2024-24795 |
CVE-2024-27316 || +-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| CVE-2024-28056 ||| +-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| CVE-2020-1927 ||| +-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| CVE-2019-13057 |
CVE-2019-13565 | CVE-2020-12243 || +-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| CVE-2019-10092 | CVE-2019-10097 |
CVE-2019-10098 || +-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| CVE-2020-12243 ||| +-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| CVE-2023-23752 ||| +-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| CVE-2020-1927 |
CVE-2020-1934 ||| +-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
```

Service: http, Version: 2.4.41

```
+-----+-----+-----+-----+ ||| CVE
associated with http 2.4.41 |
```

```
+=====+=====+=====+=====+=====+=====+=====+=====+=====+=====+
| CVE-2023-31122 | CVE-2023-43622 | CVE-2023-44487 | CVE-2023-45802 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
CVE-2019-0196 | CVE-2020-1927 | CVE-2020-1934 | | +-----+
+-----+-----+-----+-----+-----+-----+ CVE-2020-1934 | | |
+-----+-----+-----+-----+-----+-----+
```

CVE-2020-13950 ||| +-----+-----+-----
+-----+ | CVE-2019-0220 | CVE-2019-10092 |
CVE-2019-10098 | CVE-2020-1927 | +-----+-----+-----
+-----+ | CVE-2019-10092 | CVE-2019-10098 |
CVE-2020-1927 | CVE-2020-1934 | +-----+-----+-----
+-----+ | CVE-2023-38709 | CVE-2024-24795 |
CVE-2024-27316 || +-----+-----+-----
+-----+ | CVE-2024-28056 ||| +-----+-----
+-----+-----+ | CVE-2020-1927 ||| +-----
+-----+-----+-----+ | CVE-2019-13057 |
CVE-2019-13565 | CVE-2020-12243 || +-----+-----+-----
+-----+ | CVE-2019-10092 | CVE-2019-10097 |
CVE-2019-10098 || +-----+-----+-----
+-----+ | CVE-2020-12243 ||| +-----+-----
+-----+-----+ | CVE-2023-23752 ||| +-----
+-----+-----+-----+ | CVE-2020-1927 |
CVE-2020-1934 ||| +-----+-----+-----
+-----+

VII. 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.
