Pentest report - 172.67.129.7

Summary

I. Overview

This report presents the results of a vulnerability assessment conducted on **172.67.129.7** 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 12:20

Target : 172.67.129.7

Type: vulnerability scanner

II. DNS Request

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

III. Data about HTTP/HTTPS certificate

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

IV. NMAP scan

Host	Port	Service	Version
172.67.129.7	8080	http-proxy	

V. Nikto scan

Web server : cloudflare

The server supports compression.

Target URL don't use any redirection

Target URL isn't protected by a basic HTTP authentication

The X-XSS-Protection header is not defined.

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

VI. Potential vulnerabilities

Service: http, Version:

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

Service: https, Version:

- CVE-2024-1364
- CVE-2024-4331, CVE-2024-4368
- CVE-2023-7046
- CVE-2024-3832, CVE-2024-3833, CVE-2024-3834, CVE-2024-3837, CVE-2024-3838, CVE-2024-3839, CVE-2024-3840, CVE-2024-3841, CVE-2024-3843, CVE-2024-3844, CVE-2024-3845, CVE-2024-3846, CVE-2024-3847, CVE-2024-3914
- CVE-2024-1521
- CVE-2024-2781
- CVE-2024-2883, CVE-2024-2885, CVE-2024-2886, CVE-2024-2887
- CVE-2024-27894
- CVE-2024-4058, CVE-2024-4059, CVE-2024-4060
- CVE-2024-2120
- CVE-2024-3157, CVE-2024-3515, CVE-2024-3516
- CVE-2024-2121

- CVE-2021-38148

Service: infowave, Version:

Service: gnunet, Version:

- CVE-2012-1182, CVE-2017-7494
- CVE-2006-2413
- 2006-2413

Service: nbx-ser, Version:

Service: http-proxy, Version:

- CVE-2023-38646
- CVE-2024-24784
- CVE-2024-24783
- CVE-2023-45289
- CVE-2023-20198
- CVE-2019-0231, CVE-2019-10172, CVE-2019-13990, CVE-2020-25638, CVE-2020-29508, CVE-2020-35163, CVE-2020-35164, CVE-2020-35166, CVE-2020-35167, CVE-2020-35168, CVE-2020-8908, CVE-2021-23369, CVE-2021-23383, CVE-2021-28861, CVE-2021-36373, CVE-2021-36374, CVE-2021-36770, CVE-2021-37533, CVE-2021-41616, CVE-2021-43113, CVE-2022-1471, CVE-2022-23491, CVE-2022-24329, CVE-2022-24613, CVE-2022-24614, CVE-2022-24839, CVE-2022-25147, CVE-2022-31160, CVE-2022-3171, CVE-2022-34169, CVE-2022-34381, CVE-2022-36033, CVE-2022-40152, CVE-2022-40896, CVE-2022-41704, CVE-2022-41853, CVE-2022-42003, CVE-2022-42004, CVE-2022-42889, CVE-2022-42890, CVE-2022-42920, CVE-2022-44729, CVE-2022-45378, CVE-2022-45688, CVE-2022-46337, CVE-2022-46364, CVE-2022-46751, CVE-2022-48579, CVE-2023-0464, CVE-2023-0465, CVE-2023-0466, CVE-2023-0833, CVE-2023-1108, CVE-2023-1255, CVE-2023-1370, CVE-2023-1436, CVE-2023-20860, CVE-2023-20861, CVE-2023-20862, CVE-2023-20863, CVE-2023-2283, CVE-2023-24021, CVE-2023-24998, CVE-2023-2617, CVE-2023-2618, CVE-2023-2650, CVE-2023-27391, CVE-2023-28708, CVE-2023-28823, CVE-2023-29081, CVE-2023-29499, CVE-2023-2975, CVE-2023-2976, CVE-2023-31122, CVE-2023-3223, CVE-2023-32611, CVE-2023-32636, CVE-2023-32643, CVE-2023-32665, CVE-2023-33201, CVE-2023-33202, CVE-2023-34034, CVE-2023-34035, CVE-2023-34053, CVE-2023-34055, CVE-2023-3446, CVE-2023-34981, CVE-2023-35116, CVE-2023-35141,

CVE-2023-35887, CVE-2023-3635, CVE-2023-36478,
CVE-2023-36479, CVE-2023-36632, CVE-2023-37536,
CVE-2023-38039, CVE-2023-3817, CVE-2023-38325,
CVE-2023-38545, CVE-2023-38546, CVE-2023-39151,
CVE-2023-39975, CVE-2023-4016, CVE-2023-40167,
CVE-2023-40217, CVE-2023-4043, CVE-2023-41056,
CVE-2023-41074, CVE-2023-41080, CVE-2023-41105,
CVE-2023-41900, CVE-2023-41993, CVE-2023-42282,
CVE-2023-42503, CVE-2023-42917, CVE-2023-43494,
CVE-2023-43495, CVE-2023-43496, CVE-2023-43497,
CVE-2023-43498, CVE-2023-43622, CVE-2023-43804,
CVE-2023-44271, CVE-2023-44483, CVE-2023-44487,
CVE-2023-44981, CVE-2023-45142, CVE-2023-4527,
CVE-2023-45802, CVE-2023-45803, CVE-2023-46218,
CVE-2023-46219, CVE-2023-46308, CVE-2023-4641,
CVE-2023-46589, CVE-2023-46604, CVE-2023-46809,
CVE-2023-47038, CVE-2023-47039, CVE-2023-47100,
CVE-2023-4806, CVE-2023-4807, CVE-2023-4863,
CVE-2023-48795, CVE-2023-49083, CVE-2023-4911,
CVE-2023-50298, CVE-2023-50386, CVE-2023-5072,
CVE-2023-50782, CVE-2023-51074, CVE-2023-51257,
CVE-2023-5156, CVE-2023-51775, CVE-2023-52428,
CVE-2023-5341, CVE-2023-5363, CVE-2023-5379, CVE-2023-5678,
CVE-2023-5752, CVE-2023-6004, CVE-2023-6129, CVE-2023-6246,
CVE-2023-6378, CVE-2023-6481, CVE-2023-6507, CVE-2023-6779,
CVE-2023-6780, CVE-2023-6918, CVE-2024-0727, CVE-2024-0853,
CVE-2024-1459, CVE-2024-1597, CVE-2024-1635,
CVE-2024-20918, CVE-2024-20919, CVE-2024-20921,
CVE-2024-20922, CVE-2024-20923, CVE-2024-20925,
CVE-2024-20926, CVE-2024-20932, CVE-2024-20945,
CVE-2024-20952, CVE-2024-20954, CVE-2024-20989,
CVE-2024-20990, CVE-2024-20991, CVE-2024-20992,
CVE-2024-20993, CVE-2024-20994, CVE-2024-20995,
CVE-2024-20997, CVE-2024-20998, CVE-2024-20999,
CVE-2024-21000, CVE-2024-21001, CVE-2024-21002,
CVE-2024-21003, CVE-2024-21004, CVE-2024-21005,
CVE-2024-21006, CVE-2024-21007, CVE-2024-21008,
CVE-2024-21009, CVE-2024-21010, CVE-2024-21011,
CVE-2024-21012, CVE-2024-21013, CVE-2024-21014,
CVE-2024-21015, CVE-2024-21016, CVE-2024-21017,
CVE-2024-21018, CVE-2024-21019, CVE-2024-21020,
CVE-2024-21021, CVE-2024-21022, CVE-2024-21023,
CVE-2024-21024, CVE-2024-21025, CVE-2024-21026,
CVE-2024-21027, CVE-2024-21028, CVE-2024-21029,
CVE-2024-21030, CVE-2024-21031, CVE-2024-21032,
CVE-2024-21033, CVE-2024-21034, CVE-2024-21035,
CVE-2024-21036, CVE-2024-21037, CVE-2024-21038,
CVE-2024-21039, CVE-2024-21040, CVE-2024-21041,
CVE-2024-21042, CVE-2024-21043, CVE-2024-21044,
CVE-2024-21045, CVE-2024-21046, CVE-2024-21047,
CVE-2024-21048, CVE-2024-21049, CVE-2024-21050,
CVE-2024-21051, CVE-2024-21052, CVE-2024-21053,

CVE-2024-21054, CVE-2024-21055, CVE-2024-21056, CVE-2024-21057, CVE-2024-21058, CVE-2024-21059, CVE-2024-21060, CVE-2024-21061, CVE-2024-21062, CVE-2024-21063, CVE-2024-21064, CVE-2024-21065, CVE-2024-21066, CVE-2024-21067, CVE-2024-21068, CVE-2024-21069, CVE-2024-21070, CVE-2024-21071, CVE-2024-21072, CVE-2024-21073, CVE-2024-21074, CVE-2024-21075, CVE-2024-21076, CVE-2024-21077, CVE-2024-21078, CVE-2024-21079, CVE-2024-21080, CVE-2024-21081, CVE-2024-21082, CVE-2024-21083, CVE-2024-21084, CVE-2024-21085, CVE-2024-21086, CVE-2024-21087, CVE-2024-21088, CVE-2024-21089, CVE-2024-21090, CVE-2024-21091, CVE-2024-21092, CVE-2024-21093, CVE-2024-21094, CVE-2024-21095, CVE-2024-21096, CVE-2024-21097, CVE-2024-21098, CVE-2024-21099, CVE-2024-21100, CVE-2024-21101, CVE-2024-21102, CVE-2024-21103, CVE-2024-21104, CVE-2024-21105, CVE-2024-21106, CVE-2024-21107, CVE-2024-21108, CVE-2024-21109, CVE-2024-21110, CVE-2024-21111, CVE-2024-21112, CVE-2024-21113, CVE-2024-21114, CVE-2024-21115, CVE-2024-21116, CVE-2024-21117, CVE-2024-21118, CVE-2024-21119, CVE-2024-21120, CVE-2024-21121, CVE-2024-21626, CVE-2024-21634, CVE-2024-21892, CVE-2024-22019, CVE-2024-22195, CVE-2024-22201, CVE-2024-22233, CVE-2024-22243, CVE-2024-22257, CVE-2024-22259, CVE-2024-23635, CVE-2024-23672, CVE-2024-24549, CVE-2024-24815, CVE-2024-24816, CVE-2024-25062, CVE-2024-25710, CVE-2024-26130, CVE-2024-26308
- CVE-2023-44487
- CVE-2024-24785
- CVE-2023-26159
- CVE-2023-45288

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.