VULNERABILITY REPORT

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

I. Overview

This report presents the results of a vulnerability assessment conducted on **extranet.ssq.ca** 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 04:03

Target : extranet.ssq.ca

Type: vulnerability scanner

II. DNS Request

Record name	**Informations and data**
A	[{'address': '45.33.200.80', 'ttl': 3600}]
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: extranet.ssq.ca
port: 443

Certificate

protocol: https:
hostname: extranet.ssq.ca
port: 443
issued_to: extranet.ssq.ca
issued_by: DigiCert Global G2 TLS RSA SHA256 2020 CA1
valid_from: 2024-02-26T00:00:00.000Z
valid_to: 2025-03-19T23:59:59.000Z
alternate_names: ['DNS:extranet.ssq.ca']
serial_number: 0D06A8C79504BF863303ED336280E0D9
fingerprint: 79:9A:65:72:EB:DC:
8C:BD:FA:C4:58:69:72:CC:F7:6C:A0:18:34:3B
raw:
-----BEGIN CERTIFICATE-----

MIIGzzCCBbegAwIBAgIQDQaox5UEv4YzA+0zYoDg2TANBgkqhkiG9w0BAQsFADBZ
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMTMwMQYDVQQ
aWdpQ2VydCBHbG9iYWwgRzIgVExTIFJTQSBTSEEyNTYgMjAyMCBDQTEwHhcNMjQw
MjI2MDAwMDAwWhcNMjUwMzE5MjM1OTU5WjBfMQswCQYDVQQGEwJDQTEQMA4G
CAwHUXXDqWJlYzEPMA0GA1UEBxMGUXVlYmVjMRMwEQYDVQQKEwpCZW5ldmEga
MRgwFgYDVQQDEw9leHRyYW5ldC5zc3EuY2EwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCjLoTMXuD0MZ5exYatsscx1lzI5HsH7wHSvW4n6bpmTI5s69zk
t6L7rLff0oBkNQEfIu917jLlPFJVXguGMYyj3lTKiPjvcvcyVbFPjZau4m7xtmT7
1CqW3b6ZWdFDQ5LUTQsbdGKPp2JeaeU8JptNXkuneuS/
FECCWEorzxT7p3WJH7u7 nTylj+GDJo0HxkQijR/h93E4eA56f9csMAzQ/
8hOLC8KQPxRaFTqMFoQfYNnCWmq
yyIjFhDp7IovdnBEh7y3kqv0wx6pwKWq6/8EyVIqhkurj+uVR/
tz27LLeQ1Uzjn7 FXu5JOgfl/
mGWZlu4O6ucYYomLOkcZR+a+XlAgMBAAGjggOLMIIDhzAfBgNVHSME
GDAWgBR0hYDAZsffN97PvSk3qgMdvu3NFzAdBgNVHQ4EFgQUMyefpT0iBZpzY4h2
qjrYqDZXgxgwGgYDVR0RBBMwEYIPZXh0cmFuZXQuc3NxLmNhMD4GA1UdIAQ3MDU
MwYGZ4EMAQICMCkwJwYIKwYBBQUHAgEWG2h0dHA6Ly93d3cuZGlnaWNlcnQuY29
L0NQUzAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGA
BwMCMIGfBgNVHR8EgZcwgZQwSKBGoESGQmh0dHA6Ly9jcmwzLmRpZ2ljZXJ0LmN
bS9EaWdpQ2VydEdsb2JhbEcyVExTUlNBU0hBMjU2MjAyMENBMS0xLmNybDBIoEag
RIZCaHR0cDovL2NybDQuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xvYmFsRzJUTFNS
U0FTSEEyNTYyMDIwQ0ExLTEuY3JsMIGHBggrBgEFBQcBAQR7MHkwJAYIKwYBBQUH
MAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBRBggrBgEFBQcwAoZFaHR0cDov
L2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0R2xvYmFsRzJUTFNSU0FTSEEy
NTYyMDIwQ0ExLTEuY3J0MAwGA1UdEwEB/
wQCMAAwggF+BgorBgEEAdZ5AgQCBIIB
bgSCAWoBaAB1AE51oydcmhDDOFts1N8/
Uusd8OCOG41pwLH6ZLFimjnfAAABjedP
V28AAAQDAEYwRAIgEU1QY4dKDaPBj5sxd37oXfOPRD9EhbXw5equDjeC6NoCIAQa
QpsXOMFSuw1rpkiQwVnuzQCiW30xzW6PD5bOFlidAHYAfVkeEuF4KnscYWd8Xv34
0IdcFKBOlZ65Ay/ZDowuebgAAAGN509XcgAABAMARzBFAiAj/
b6seLK2chZrrMMO
c9yuK1UqBiz6mHGdl2PDgIMIMQIhAKVZ4OxZn5zWiethST6xiqXF/
3Ggj5vYNCPQ HSKC7hsiAHcA5tIxY0B3jMEQQQbXcbnOwdJA9paEhvu6hzId/
R43jlAAAAGN509X mgAABAMASDBGAiEA9v5c/
QLW4Mlh1aVh0KNZABkOT4Bc8ko+j8lhFThImlkCIQCt
6keWDjCmUXl8NZKLbcLjHXCWwWHoGemGhXWGN99FizANBgkqhkiG9w0BAQsFAAO
AQEAnf+40NFQ9ek6vGdPlZA1FD2/4EzDTZ2nMxNobRfE0/
uLtIDC4qi5lGQ02c64 NuoGQQ/
xyAdVP6+Dc58vuLpy2n+pVlbn1JMJPtPzuVVd+URNCqAdu60ljYHlNCFW
78Lzt8DmjfJ9Z2wvb6SIhd3knUODccocqm4xrCgzsNtnCcuAMpeOesDLBi5tIpDS
L1GN6wB19X4VDuE24XBClxY4ql03Q9goVpy2IUavcy6xvF4ZcidNavz9EpClHQJm
aV9lNLh1ypN7H27Fp9mB+erzgaCPGDETB1aWHpwrh6wfrWe0nWSNp4JDtY7LGbYu
xIZ1o3Cpy4IejCqBAwOJ75Bpzg== -----END CERTIFICATE-----

IV. NMAP scan

[['45.33.200.80', 80, 'http', ''], ['45.33.200.80', 443, 'https', '']]

V. Nikto scan

Web server : nginx

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.

VI. Potential vulnerabilities

Service: http, Version:

+----------------------------+ | CVE associated with http | +============================+ | CVE-2021-3007 | +----------------------------+ | CVE-2023-34062 | +----------------------------+ | CVE-2016-4423 | +----------------------------+ | CVE-2013-4407 | +----------------------------+ | CVE-2023-44487 | +----------------------------+ | CVE-2007-6423 | +----------------------------+ | CVE-2007-6420 | +----------------------------+ | CVE-2015-2308 | +----------------------------+ | CVE-2024-2653 | +----------------------------+ | CVE-2018-19790 | +----------------------------+ | CVE-2023-45288 | +----------------------------+ | CVE-2021-31618 | +----------------------------+

Service: https, Version:

+----------------------------+ | CVE associated with https | +============================+ | CVE-2024-1364 | +----------------------------+ | CVE-2024-2121 | +----------------------------+ | CVE-2024-2781 | +----------------------------+ | CVE-2024-3157 | +----------------------------+ | CVE-2024-1521 | +----------------------------+ | CVE-2010-4340 | +----------------------------+ | CVE-2021-38148 | +----------------------------+ | CVE-2024-3832 | +----------------------------+ | CVE-2023-7046 | +----------------------------+ | CVE-2024-4331 | +----------------------------+ | CVE-2024-4058 | +----------------------------+ | CVE-2024-2120 | +----------------------------+ | CVE-2024-27894 | +----------------------------+

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.