Pentest report - your-server.de

Summary

I. Overview

This report presents the results of a vulnerability assessment conducted on **your-server.de** 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: 2024-05-06 08:02

Target : your-server.de

Type: vulnerability scanner

II. DNS Request

Record name	**Informations and data**
A	[{'address': '85.10.215.232', 'ttl': 7200}]
CNAME	No record found
MX	[{'exchange': 'dediextern.your-server.de', 'priority': 10}]
NS	[{'nameserver': 'ns3.second-ns.de'}, {'nameserver': 'ns.second-ns.com'}, {'nameserver': 'ns1.your-server.de'}]
SOA	[{'nameserver': 'ns1.your-server.de', 'hostmaster': 'postmaster.your-server.de'}]
TXT	['v=spf1 mx ~all']

III. Data about HTTP/HTTPS certificate

Metadata

protocol: https:

hostname: your-server.de
port: 443

Certificate

protocol: https:
hostname: your-server.de
port: 443
issued_to: your-server.de
issued_by: Encryption Everywhere DV TLS CA - G2
valid_from: 2024-04-12T00:00:00.000Z
valid_to: 2025-04-12T23:59:59.000Z
alternate_names: ['DNS:your-server.de', 'DNS:www.your-server.de']
serial_number: 0DE8F4A4813B1ED6D06DA156FD5AA0E0
fingerprint: 49:AD:2D:67:14:7D:CF:
42:63:46:5E:D2:E4:2B:DC:C2:99:EF:00:7A
raw:
-----BEGIN CERTIFICATE-----
MIIGBzCCBO+gAwIBAgIQDej0pIE7HtbQbaFW/
Vqg4DANBgkqhkiG9w0BAQsFADBu
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQ
d3cuZGlnaWNlcnQuY29tMS0wKwYDVQQDEyRFbmNyeXB0aW9uIEV2ZXJ5d2hlcmUg
RFYgVExTIENBIC0gRzIwHhcNMjQwNDEyMDAwMDAwWhcNMjUwNDEyMjM1OTU
MRcwFQYDVQQDEw55b3VyLXNlcnZlci5kZTCCASIwDQYJKoZIhvcNAQEBBQADggE
ADCCAQoCggEBALVJqhmJRcF00teC1cbAdG0EwQJL3gWgxiQK/
QdaUnAenz8Zr5KV
khMEclkW3OSAQLJfIcQtdtOMDUAFejA0G7JcKSIhnWFRn6Vwa1Bhmd0sf3sH3nlZ
NwN7K9wO3WFfi6rR7n8zzGMiFK0iniBeVTtRihZTKsx3DUEssfS+cT8MHIRUXka/
DOIkhgnaUNgihOV6xCg8yqXF14IQ1EX11dXmwXkLuda9FKWCIHwXt0ufpK638mNb
kmyJUNH8XbOhgoLxtuzgFKUxRQLqn9302/
D2QCDyy5N+WbiHjitAgCoaDwBehsM
L789jE9KhhpIbqM1YW71ezut91Gw7YlF7f0CAwEAAaOCAvQwggLwMB8GA1UdIwQY
MBaAFHjfkZBf7t6s9sV169VMVVPvJEq2MB0GA1UdDgQWBBQnKlH0wKW/
kq4pG5CX
FL4FgfzKazAtBgNVHREEJjAkgg55b3VyLXNlcnZlci5kZYISd3d3LnlvdXItc2Vy
dmVyLmRlMD4GA1UdIAQ3MDUwMwYGZ4EMAQIBMCkwJwYIKwYBBQUHAgEWG2
Ly93d3cuZGlnaWNlcnQuY29tL0NQUzAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBY
FAYIKwYBBQUHAwEGCCsGAQUFBwMCMIGABggrBgEFBQcBAQR0MHIwJAYIKwYB
MAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBKBggrBgEFBQcwAoY+aHR0cD
L2NhY2VydHMuZGlnaWNlcnQuY29tL0VuY3J5cHRpb25FdmVyeXdoZXJlRFZUTFND
QS1HMi5jcnQwDAYDVR0TAQH/
BAIwADCCAX0GCisGAQQB1nkCBAIEggFtBIIBaQFn
AHYATnWjJ1yaEMM4W2zU3z9S6x3w4I4bjWnAsfpksWKaOd8AAAGOz+HZHgAABAM
RzBFAiEAqwdPClsTsgrpu8K5prr1oKO52NbsplOOR93Tv3PM/
UYCIHT7Bw7BW1zb dTTPFlNZLa/
NF7DbVth4vru5p2gHAlGWAHYA5tIxY0B3jMEQQQbXcbnOwdJA9paE
hvu6hzId/
R43jlAAAAGOz+HZaAAABAMARzBFAiAxuVzeBcmyPKlx6Cms+uSambB5
ksayKLSBL6PT+N19NAIhAITcUKVl/dfJcXKC6AI3m+FjuMc4hWUg2/
GQQA12nBlJ AHUAzxFW7tUufK/

zh1vZaS6b6RpxZ0qwF+ysAdJbd87MOwgAAAGOz+HZVQAABAMA
RjBEAiBwqqRdqYA05XMwZ8qwQ7f8sLGanN38vNlcYSaLkw0+IAIgRA3uhm6srbD/
7yILEYqzZjLZhjVXtb4ehtHUfzo7F0AwDQYJKoZIhvcNAQELBQADggEBAGZDKG8D
WBtJtotcbs2vbxCRU5ac7D9QZrTJH78cS/O6KAIEh0ZrGfAHk430Xm/
5BC5idtxi xY4bHmZoyBPB5bHi/
7TtYOhrbj228XSaj7IAQsfaZqqcYUCIxpKVbXZWf3UcEsDE
h0sJSGiwl11okj021WasB4dB11/97fenbWJgUaZ8LVgm7BUFfqKSEoWugxfnLQFf
bCzknplSzY8/9/
jcmEBv8k6wj2YguRFAil63uTWkWjDNNY36wzC5Ih7mc6oSTjoB
k4tstrvv+DupP+AolpEo6VdIIQE89cYvIiuTS6n+NPUz12TNPBthFbmP5t03SdPG
DXPSBj/3KNF8NPw= -----END CERTIFICATE-----

IV. NMAP scan

Host	Port	Service	Version
85.10.215.232	443	http	

V. Nikto scan

Web server : Apache

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.

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

VI. Potential vulnerabilities

None

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.