Pentest report - kinezo.com

Summary

I. Overview

This report presents the results of a vulnerability assessment conducted on **kinezo.com** 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 09:27

Target : kinezo.com

Type: vulnerability scanner

II. DNS Request

Record name	**Informations and data**
A	[{'address': '51.161.122.78', 'ttl': 1799}]
CNAME	No record found
MX	[{'exchange': 'aspmx.l.google.com', 'priority': 1}, {'exchange': 'alt2.aspmx.l.google.com', 'priority': 5}, {'exchange': 'alt1.aspmx.l.google.com', 'priority': 5}, {'exchange': 'aspmx2.googlemail.com', 'priority': 10}, {'exchange': 'aspmx3.googlemail.com', 'priority': 10}]
NS	[{'nameserver': 'dns1.registrar-servers.com'}, {'nameserver': 'dns2.registrar-servers.com'}]
SOA	[{'nameserver': 'dns1.registrar-servers.com', 'hostmaster': 'hostmaster.registrar-servers.com'}]
TXT	No record found

III. Data about HTTP/HTTPS certificate

Metadata

protocol: https:
hostname: kinezo.com
port: 443

Certificate

protocol: https:
hostname: kinezo.com
port: 443
issued_to: www.kinezo.com
issued_by: R3
valid_from: 2024-04-29T23:02:34.000Z
valid_to: 2024-07-28T23:02:33.000Z
alternate_names: ['DNS:kinezo.com', 'DNS:razor.ca', 'DNS:resolveaudio.com', 'DNS:thehoneybeecharcuterie.ca', 'DNS:www.kinezo.com', 'DNS:www.resolveaudio.com']
serial_number: 03E4833B8BFBF836214661947BBB8BADFC27
fingerprint: 2A:C4:E4:5D:A2:CD:BD:8E:71:1C:84:FB:C2:17:9E:62:FF:26:91:9C
raw:
-----BEGIN CERTIFICATE-----
MIIFQjCCBCqgAwIBAgISA+SDO4v7+DYhRmGUe7uLrfwnMA0GCSqGSIb3DQEBCw
MDIxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYD
EwJSMzAeFw0yNDA0MjkyMzAyMzRaFw0yNDA3MjgyMzAyMzNaMBkxFzAVBgNVBA
Dnd3dy5raW5lem8uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
tIC9axo6dNDzquu+N4gnqMqoyFF/
vgg2niPzJA3B1kZVAbEAi+tiVeQ8hdlUXF5d
H2G6jeaJwueDvqimkmK6ohi9XXdGro0EU/
wwg2gtbWnA6JRXDkZdRi9J1OEMpRVb mqoXe4pJ7KMIkFL9snR/
ttXgCJbWMwatU4fWnXVk8ZXav3veXFJ0o1Ek0s1N/ykf
baXimIXHL3RDM7xW2JnOKPMCe+uuPsRY3qHFp/
15H63HGTW7Q1+3bWVzt5TnJcQB 7URTeA/
JmuRTJrKYyXRGQAbOt33Fi7m0PrB+OsofvXeCSB3SNZHVkDrP/
385e2vr
uWjaYuZccyFmC1YhuoeGuQIDAQABo4ICaTCCAmUwDgYDVR0PAQH/
BAQDAgWgMB0G
A1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAMBgNVHRMBAf8EAjAAMB0
DgQWBBQJbBrke4GF8Sxy48i4N0qcdPDfdTAfBgNVHSMEGDAWgBQULrMXt1hWy65
CUDmH6+dixTCxjBVBggrBgEFBQcBAQRJMEcwIQYIKwYBBQUHMAGGFWh0dHA6L
My5vLmxlbmNyLm9yZzAiBggrBgEFBQcwAoYWaHR0cDovL3IzLmkubGVuY3Iub3Jn
LzByBgNVHREEazBpggpraW5lem8uY29tgghyYXpvci5jYYIQcmVzb2x2ZWF1ZGlv
LmNvbYIZdGhlaG9uZXliZWVjaGFyY3V0ZXJpZS5jYYIOd3d3LmtpbmV6by5jb22C
FHd3dy5yZXNvbHZlYXVkaW8uY29tMBMGA1UdIAQMMAowCAYGZ4EMAQIBMIIBB
KwYBBAHWeQIEAgSB9QSB8gDwAHYASLDja9qmRzQP5WoC+p0w6xxSActW3SyB2b
qznYhHMAAAGPLE9wlAAABAMARzBFAiBrFMjL+S5gTlo2Wls/
146OWG7TGy6GdEuj

Hr24RsoSWQIhAMuoUhqW936Qpvyd1eIL719zkyiPLoXKIj/
Xz49JSl70AHYA3+FW 66oFr7WcD4ZxjajAMk6uVtlup/
WlagHRwTu+UlwAAAGPLE9xZQAABAMARzBFAiEA
rBqfl89yHepgSiyO5R70Nd5Xa1860MrB0YPxNf4Zm2YCIGSQDCzNEZOvCYK3qlDA
kPTrone687ln0Pi7ywuRZHQlMA0GCSqGSIb3DQEBCwUAA4IBAQBw/
OigAE8Dapk8
eKHgSNEfgyCzQEAm5g1ItLZIa5Z3e+5ktk25HyTVFidkUmyLxO/
7R+jDXde+Cp8a 0hScd00ZylSBXz+4kXEA0/gKjBpJZEmwy/
6aSPyLy1etuE5lPU3R8qpc2rKfFcob SgOzYHhoM/
1OMU3haQC8WlmyEUtTxrhssDF6W557PdQfIHM/I+Z465+tzVWMkzVh
BR/xNZdZlsQUACge+NsMERG/pGdC+EGkOog2DqHhdmJhjs9w9Sz/
QQVDS4r37oq2
yxK6E1mkS8mk4AOOklcT73YygbOk9Rzx4+OtyLZFcUAQLvI7DDu/
ctjpMnwjE5k/ ZWMStSib -----END CERTIFICATE-----

IV. NMAP scan

Host	Port	Service Version
80	http	
143	tcpwrapped	
443	http	
5900	tcpwrapped	
8888	tcpwrapped	

V. Nikto scan

Web server : Apache

The server supports 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.