Full Scan Report
Demo Company

May 8, 2023

Nextdoorsec BV
Brusselstraat 38
2018 ANTWERPEN

info@nextdoorsec.com
www.nextdoorsec.com

Table of contents

Executive summary

On 08 May, 2023, Demo Company engaged Nextdoorsec BV to perform a security audit on their Web application.

Nextdoorsec BV performed both Security Audit and Reconnaissance.

Observations

During the course of this engagement Nextdoorsec BV was able to discover 6 Subdomains and 116 Vulnerabilities, including informational vulnerabilities and these could pose a significant risk to the security of the application.

The breakdown of the Vulnerabilities Identified in Demo Company by severity are as follows:

- Critical : 0
- High : 0
- Medium : 4
- Low : 4
- Info : 108
- Unknown : 0

Nextdoorsec BV recommends that these issues be addressed in timely manner.

Quick Summary

This section contains quick summary of scan performed on Demo Company

Reconnaissance

Subdomains	Endpoints	Vulnerabilities
6	28	116

Vulnerability Summary

Critical	High	Medium
0	0	4

Low	Info	Unknown
4	108	0

Timeline of the Assessment

Scan started on: May 8, 2023 07:53
Total time taken: Completed in 17 minutes
Report Generated on: May 8, 2023

Interesting Recon Data

Listed below are the 1 interesting subdomains identified on Demo Company

#	Subdomain	Page title	HTTP Status
1	ftp.democompany	403 Forbidden	403

Summary of Vulnerabilities Identified

Listed below are the vulnerabilities identified on Demo Company

#	Vulnerability Name	Times Identified	Severity
1	Weak Cipher Suites Detection	4	Medium
2	Mismatched SSL Certificate	2	Low
3	Untrusted Root Certificate - Detect	2	Low
4	HTTP Missing Security Headers	44	Informational
5	TLS Version - Detect	10	Informational
6	Wappalyzer Technology Detection	5	Informational
7	SSL DNS Names	4	Informational
8	Detect SSL Certificate Issuer	4	Informational
9	Deprecated TLS Detection (TLS 1.1 or SSLv3)	4	Informational
10	CNAME Fingerprint	3	Informational
11	DNS TXT Record Detected	2	Informational
12	WordPress Readme File	2	Informational
13	WAF Detection	2	Informational
14	XSS-Protection Header - Cross-Site Scripting	2	Informational
15	NS Record Detection	2	Informational

16	Wordpress XML-RPC List System Methods	2	Informational
17	Akismet Anti-Spam' Spam Protection Detection	2	Informational
18	WordPress xmlrpc	2	Informational
19	MySQL - Password Vulnerability	2	Informational
20	WordPress Detect	2	Informational
21	CAA Record	2	Informational
22	WordPress Login Panel - Detect	2	Informational
23	CSP Not Enforced	2	Informational
24	MX Record Detection	2	Informational
25	Allowed Options Method	2	Informational
26	MySQL - Detect	2	Informational
27	PHP Detect	1	Informational
28	Metatag CMS Detection	1	Informational

Discovered Assets

Subdomains

During the reconnaissance phase, 6 subdomains were discovered. Out of 6 subdomains, 3 returned HTTP status 200. 1 interesting subdomains were also identified based on the interesting keywords used.

6 subdomains identified on Demo Company

Subdomain	Page title	HTTP Status
democompany.be	Demo Company | Just another WordPress site	200
ftp.democompany	403 Forbidden	403
autoconfig.democompany		200
autodiscover.democompany		200
2a.democompany		0
www.democompany		301

IP Addresses

4 IP Addresses were identified on democompany

IP	Open Ports	Remarks
153.xx.2.19	443/None, 80/None	
2a02:xxxx::d		
2a02:xxxx:8:324:0:1b9a:3ce0:c		
194.5.xxx.97	443/None, 80/None, 7443/None, 3306/None, 21/None, 8443/None	

Reconnaissance Findings

1.	democompany.be	200

Page Title: Demo Company | Just another WordPress site

IP Address:

- 2a02:xxxx:8:324:0:1b9a:3ce0:c
- 194.5.xxx.97
  - Open Ports: 443/None, 80/None, 7443/None, 3306/None, 21/None, 8443/None

Vulnerabilities

- MySQL - Detect
- DNS TXT Record Detected
- HTTP Missing Security Headers
- WordPress xmlrpc
- Wordpress XML-RPC List System Methods
- WordPress Detect
- PHP Detect
- Metatag CMS Detection
- Wappalyzer Technology Detection
- WordPress Login Panel - Detect
- CAA Record
- Detect SSL Certificate Issuer
- SSL DNS Names
- HTTP Missing Security Headers
- WordPress Readme File
- Akismet Anti-Spam' Spam Protection Detection
- MySQL - Password Vulnerability
- NS Record Detection
- TLS Version - Detect
- MX Record Detection

2.	ftp.democompany	403

Page Title: 403 Forbidden

IP Address:

- 194.5.xxx.97
  - Open Ports: 443/None, 80/None, 7443/None, 3306/None, 21/None, 8443/None

3.	autoconfig.democompany.be	200

IP Address:

- 2a02:xxxx::d
- 153.xx.2.19
  - Open Ports: 443/None, 80/None

Vulnerabilities

- SSL DNS Names
- CSP Not Enforced
- HTTP Missing Security Headers
- Weak Cipher Suites Detection
- Mismatched SSL Certificate
- Untrusted Root Certificate - Detect
- HTTP Missing Security Headers
- XSS-Protection Header - Cross-Site Scripting
- Wappalyzer Technology Detection
- CNAME Fingerprint
- WAF Detection
- Detect SSL Certificate Issuer
- HTTP Missing Security Headers
- TLS Version - Detect
- Deprecated TLS Detection (TLS 1.1 or SSLv3)
- Allowed Options Method

4.	autodiscover.democompany.be	200

IP Address:

- 2a02:xxxx::d
- 153.xx.2.19
  - Open Ports: 443/None, 80/None

12

Vulnerabilities

- Detect SSL Certificate Issuer
- SSL DNS Names
- CSP Not Enforced
- Weak Cipher Suites Detection
- Mismatched SSL Certificate
- Untrusted Root Certificate - Detect
- XSS-Protection Header - Cross-Site Scripting
- CNAME Fingerprint
- Wappalyzer Technology Detection
- WAF Detection
- HTTP Missing Security Headers
- TLS Version - Detect
- Deprecated TLS Detection (TLS 1.1 or SSLv3)
- Allowed Options Method

5.	2a.democompany.be	N/A

6.	www.democompany.be	301

IP Address:

- 2a02:xxxx:8:324:0:1b9a:3ce0:c
- 194.5.xxx.97
  - Open Ports: 443/None, 80/None, 7443/None, 3306/None, 21/None, 8443/None

13

Vulnerabilities

- MySQL - Detect
- WordPress Readme File
- Wordpress XML-RPC List System Methods
- WordPress Detect
- WordPress xmlrpc
- Wappalyzer Technology Detection
- CNAME Fingerprint
- WordPress Login Panel - Detect
- CAA Record
- Detect SSL Certificate Issuer
- SSL DNS Names
- DNS TXT Record Detected
- Akismet Anti-Spam' Spam Protection Detection
- MySQL - Password Vulnerability
- NS Record Detection
- TLS Version - Detect
- MX Record Detection

Vulnerabilities Discovered

This section reports the security issues found during the audit.
A Total of 116 were discovered in democompany.be, 0 of them were Critical, 0 of them were High Severity, 4 of them were Medium severity, 4 of them were Low severity, and 108 of them were Informational. 0 of them were Unknown Severity.

Vulnerability Breakdown by Severity

Critical	High	Medium
0	0	4

Low	Info	Unknown
4	108	0

Weak Cipher Suites Detection — MEDIUM

Description
A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken.

Vulnerable URL(s)

- autoconfig.democompany.be:443
  Result/Findings
  [tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA] [tls10 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]
- autodiscover.democompany.be:443
  Result/Findings
  [tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA] [tls10 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]

References

- https://www.acunetix.com/vulnerabilities/web/tls-ssl-weak-cipher-suites/
- http://ciphersuite.info

Untrusted Root Certificate - Detect LOW

Description
A root certificate is a digital certificate issued by a trusted certificate authority that acts as a basis for other digital certificates. An untrusted root certificate is a certificate that is issued by an authority that is not trusted by the computer, and therefore cannot be used to authenticate websites or other digital certificates.

Vulnerable URL(s)

- autodiscover.democompany.be: 443
- Result/Findings

References

- https://www.sslmarket.com/ssl/trusted-and-untrusted-certificate
- https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/ssl-untrusted-root-certificate/

Mismatched SSL Certificate LOW

Vulnerable URL(s)

- autoconfig.democompany.be: 443
  Result/Findings CN: *.mail.hostinger.com

References

- https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/ssl-certificate-name-hostname-mismatch/

Untrusted Root Certificate - Detect LOW

Description
A root certificate is a digital certificate issued by a trusted certificate authority that acts as a basis for other digital certificates. An untrusted root certificate is a certificate that is issued by an authority that is not trusted by the computer, and therefore cannot be used to authenticate websites or other digital certificates.

Vulnerable URL(s)

- autoconfig.democompany.be:443
  Result/Findings

References

- https://www.sslmarket.com/ssl/trusted-and-untrusted-certificate
- https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/ssl-untrusted-root-certificate/

Mismatched SSL Certificate LOW

Vulnerable URL(s)

- autodiscover.democompany.be: 443
- Result/Findings
  CN: *.mail.hostinger.com

References

- https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/ssl-certificate-name-hostname-mismatch/

WordPress xmlrpc INFO

Vulnerable URL(s)

- https://democompany.be/xmlrpc.php
  Result/Findings

Wordpress XML-RPC List System Methods INFO

Vulnerable URL(s)

- https://democompany.be/xmlrpc.php
  Result/Findings
- https://www.democompany.be/xmlrpc.php
  Result/Findings

WordPress Detect INFO

Vulnerable URL(s)

- https://democompany.be
  Result/Findings
- https://democompany.be
  Result/Findings

CSP Not Enforced INFO

Description
Checks if there is a CSP header

Vulnerable URL(s)

- https://autodiscover.democompany.be
  Result/Findings
- https://autoconfig.democompany.be
  Result/Findings

HTTP Missing Security Headers INFO

Description
This template searches for missing HTTP security headers. The impact of these missing headers can vary.

Vulnerable URL(s)

- https://autoconfig.democompany.be
  Result/Findings
  content-security-policy

WordPress xmlrpc INFO

Vulnerable URL(s)

- https://www.democompany.be/xmlrpc.php
- Result/Findings

HTTP Missing Security Headers — INFO

Description
This template searches for missing HTTP security headers. The impact of these missing headers can vary.

Vulnerable URL(s)

- https://autoconfig.democompany.be
  Result/Findings
  clear-site-data

XSS-Protection Header - Cross-Site Scripting — INFO

Description
Setting the XSS-Protection header is deprecated. Setting the header to anything other than `0` can actually introduce an XSS vulnerability.

CVSS Metrics
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Vulnerable URL(s)

- https://autodiscover.democompany.be
  Result/Findings
  1; mode=block
- https://autoconfig.democompany.be
  Result/Findings
  1; mode=block

References

- https://developer.mozilla.org/en-us/docs/web/http/headers/x-xss-protection
- https://owasp.org/www-project-secure-headers/#x-xss-protection

PHP Detect INFO

Vulnerable URL(s)

- https://democompany.be
  Result/Findings 5.3.29

Wappalyzer Technology Detection INFO

Vulnerable URL(s)

- https://www.democompany.be
  Result/Findings
  php
- https://autoconfig.democompany.be
  Result/Findings
  nginx

CNAME Fingerprint INFO

Description
A CNAME DNS record was discovered.

CWE IDs

cwe-200

Vulnerable URL(s)

- www.democompany.be
  Result/Findings
  democompany.be.
- autoconfig.democompany.be
  Result/Findings
  autoconfig.mail.hostinger.com.

References

- https://www.theregister.com/2021/02/24/dns_cname_tracking/
- https://www.ionos.com/digitalguide/hosting/technical-matters/cname-record/

Metatag CMS Detection INFO

Description
Generic CMS Detection using html meta generator tag

Vulnerable URL(s)

- https://democompany.be
  Result/Findings
  WordPress 3.7.1

References

- https://www.w3schools.com/tags/att_meta_name.asp

CNAME Fingerprint INFO

Description
A CNAME DNS record was discovered.

CWE IDs
cwe-200

Vulnerable URL(s)

- autodiscover.democompany.be
  Result/Findings
  autodiscover.mail.hostinger.com.

References

- https://www.theregister.com/2021/02/24/dns_cname_tracking/
- https://www.ionos.com/digitalguide/hosting/technical-matters/cname-record/

Wappalyzer Technology Detection INFO

Vulnerable URL(s)

- https://autodiscover.democompany.be
  Result/Findings
  nginx
- https://democompany.be
  Result/Findings
  google-font-api • php

WordPress Login Panel - Detect INFO

Description
WordPress login panel was detected.

CVSS Metrics
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

CWE IDs
cwe-200

Vulnerable URL(s)

- https://democompany.be/wp-login.php
  Result/Findings
- https://www.democompany.be/wp-login.php
  Result/Findings

WAF Detection INFO

Description
A web application firewall was detected.

CWE IDs
cwe-200

Vulnerable URL(s)

- https://autodiscover.democompany.be/
  Result/Findings nginxgeneric
  https://autoconfig.democompany.be/
- Result/Findings nginxgeneric

References

- https://github.com/ekultek/whatwaf

CAA Record INFO

Description
A CAA record was discovered. A CAA record is used to specify which certificate authorities (CAs) are allowed to issue certificates for a domain.

CWE IDs
cwe-200

Vulnerable URL(s)

- www.democompany.be
  Result/Findings
  comodoca.com • globalsign.com • sectigo.com • digicert.com • letsencrypt.org
- democompany.be
  Result/Findings
  letsencrypt.org • digicert.com • comodoca.com • sectigo.com • globalsign.com

References

- https://support.dnsimple.com/articles/caa-record/#whats-a-caa-record

Detect SSL Certificate Issuer INFO

Vulnerable URL(s)

- www.democompany.be:443
  Result/Findings Let's Encrypt

SSL DNS Names INFO

Vulnerable URL(s)

- www.democompany.be:443

Result/Findings
democompany.be
• www.democompany.be

Detect SSL Certificate Issuer INFO

Vulnerable URL(s)

- democompany.be:443
  Result/Findings Let's Encrypt

SSL DNS Names INFO

Vulnerable URL(s)

- democompany.be:443
  Result/Findings
  democompany.be • www.democompany.be

Detect SSL Certificate Issuer INFO

Vulnerable URL(s)

- autoconfig.democompany.be:443
  Result/Findings DigiCert, Inc.

HTTP Missing Security Headers — INFO

Description
This template searches for missing HTTP security headers. The impact of these missing headers can vary.

Vulnerable URL(s)

- https://autoconfig.democompany.be
  Result/Findings
  access-control-allow-credentials • access-control-allow-methods • permissions-policy • referrer-policy • cross-origin-embedder-policy • access-control-expose-headers • access-control-max-age • x-permitted-cross-domain-policies • cross-origin-opener-policy • cross-origin-resource-policy • access-control-allow-origin • access-control-allow-headers
- https://autodiscover.democompany.be
  Result/Findings
  cross-origin-opener-policy • cross-origin-resource-policy • access-control-allow-origin • access-control-allow-credentials • access-control-expose-headers • clear-site-data • referrer-policy • access-control-allow-methods • permissions-policy • access-control-max-age • x-permitted-cross-domain-policies • cross-origin-embedder-policy • access-control-allow-headers • content-security-policy
- https://democompany.be
  Result/Findings
  access-control-allow-credentials • access-control-expose-headers • access-control-max-age • x-frame-options

DNS TXT Record Detected — INFO

Description
A DNS TXT record was detected. The TXT record lets a domain admin leave notes on a DNS server.

CWE IDs
cwe-200

Vulnerable URL(s)

- www.democompany.be
  Result/Findings
  "v=spf1 include:_spf.mail.hostinger.com ~all"

References

- https://www.netspi.com/blog/technical/network-penetration-testing/analyzing-dns-txt-records-to-fingerprint-service-providers/

HTTP Missing Security Headers — INFO

Description
This template searches for missing HTTP security headers. The impact of these missing headers can vary.

Vulnerable URL(s)

- https://democompany.be
  Result/Findings
  access-control-allow-origin • access-control-allow-methods • permissions-policy • x-content-type-options • referrer-policy • strict-transport-security • clear-site-data • cross-origin-embedder-policy • cross-origin-opener-policy • access-control-allow-headers • x-permitted-cross-domain-policies

WordPress Readme File — INFO

Vulnerable URL(s)

- https://democompany.be/readme.html
  Result/Findings

Akismet Anti-Spam' Spam Protection Detection INFO

Vulnerable URL(s)

- https://www.democompany.be/wp-content/plugins/akismet/readme.txt
  Result/Findings
  outdated_version 2.5.9
- https://democompany.be/wp-content/plugins/akismet/readme.txt
  Result/Findings
  outdated_version 2.5.9

References

- https://wordpress.org/plugins/akismet/

MySQL - Password Vulnerability INFO

Description
MySQL database queries with enabled native password support are susceptible to password brute-force attacks.

CVSS Metrics
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

CWE IDs
cwe-200

Vulnerable URL(s)

- democompany.be:3306
  Result/Findings
- www.democompany.be:3306
  Result/Findings

References

- https://github.com/tinram/mysql-brute

NS Record Detection INFO

Description
An NS record was detected. An NS record delegates a subdomain to a set of name servers.

CWE IDs
cwe-200

Vulnerable URL(s)

- www.democompany.be
  Result/Findings
  ns2.dns-parking.com. • ns1.dns-parking.com.
- democompany.be
  Result/Findings
  ns2.dns-parking.com. • ns1.dns-parking.com.

TLS Version - Detect INFO

Description
TLS version detection is a security process used to determine the version of the Transport Layer Security (TLS) protocol used by a computer or server. It is important to detect the TLS version in order to ensure secure communication between two computers or servers.

Vulnerable URL(s)

- autodiscover.democompany.be:443
  Result/Findings
  tls10
- autoconfig.democompany.be:443

Result/Findings
tls10
- democompany.be:443
Result/Findings
tls12
- www.democompany.be:443
Result/Findings
tls12 tls13
- autoconfig.democompany.be:443
Result/Findings
tls11
- democompany.be:443
Result/Findings
tls13
- autodiscover.democompany.be:443
Result/Findings
tls11
- autoconfig.democompany.be:443
Result/Findings
tls12
- autodiscover.democompany.be:443
Result/Findings
tls12

Deprecated TLS Detection (TLS 1.1 or SSLv3) INFO

Description
Both TLS 1.1 and SSLv3 are deprecated in favor of stronger encryption.

Vulnerable URL(s)

- autoconfig.democompany.be:443
Result/Findings
tls10
- autodiscover.democompany.be:443
Result/Findings
tls10 tls11
- autoconfig.democompany.be:443
Result/Findings
tls11

References

- https://ssl-config.mozilla.org/#config=intermediate

Allowed Options Method INFO

Vulnerable URL(s)

- https://autoconfig.democompany.be
  Result/Findings
  GET, HEAD, OPTIONS https://autodiscover.democompany.be
- Result/Findings
  GET, HEAD, OPTIONS

MX Record Detection INFO

Description
An MX record was detected. MX records direct emails to a mail exchange server.

CWE IDs
cwe-200

Vulnerable URL(s)

- democompany.be
  Result/Findings
  5 mx1.hostinger.com. • 10 mx2.hostinger.com.

References

- https://www.cloudflare.com/learning/dns/dns-records/dns-mx-record/

- https://mxtoolbox.com/

SSL DNS Names INFO

Vulnerable URL(s)

- autoconfig.democompany.be:443
  Result/Findings
  *.mail.hostinger.com

MX Record Detection INFO

Description
An MX record was detected. MX records direct emails to a mail exchange server.

CWE IDs
cwe-200

Vulnerable URL(s)

- www.democompany.be
  Result/Findings
  10 mx2.hostinger.com. • 5 mx1.hostinger.com.

References

- https://www.cloudflare.com/learning/dns/dns-records/dns-mx-record/
- https://mxtoolbox.com/

Detect SSL Certificate Issuer — INFO

Vulnerable URL(s)

- autodiscover.democompany.be:443
  Result/Findings
  DigiCert, Inc.

SSL DNS Names — INFO

Vulnerable URL(s)

- autodiscover.democompany.be:443
  Result/Findings
  *.mail.hostinger.com

MySQL - Detect — INFO

Description
MySQL instance was detected.

CVSS Metrics
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

CWE IDs
cwe-200

Vulnerable URL(s)

- democompany.be:3306
  Result/Findings
- www.democompany.be:3306

Result/Findings

DNS TXT Record Detected INFO

Description
A DNS TXT record was detected. The TXT record lets a domain admin leave notes on a DNS server.

CWE IDs
cwe-200

Vulnerable URL(s)

- democompany.be
  Result/Findings
  "v=spf1 include:_spf.mail.hostinger.com ~all"

References

- https://www.netspi.com/blog/technical/network-penetration-testing/analyzing-dns-txt-records-to-fingerprint-service-providers/

WordPress Readme File INFO

Vulnerable URL(s)

- https://www.democompany.be/
  readme.html Result/Findings

HTTP Missing Security Headers INFO

Description

This template searches for missing HTTP security headers. The impact of these missing headers can vary.

Vulnerable URL(s)

- https://democompany.be

Result/Findings

cross-origin-resource-policy

END OF REPORT