Sri Lanka Institute of Information Technology

WEB SECURITY

(IE2062)

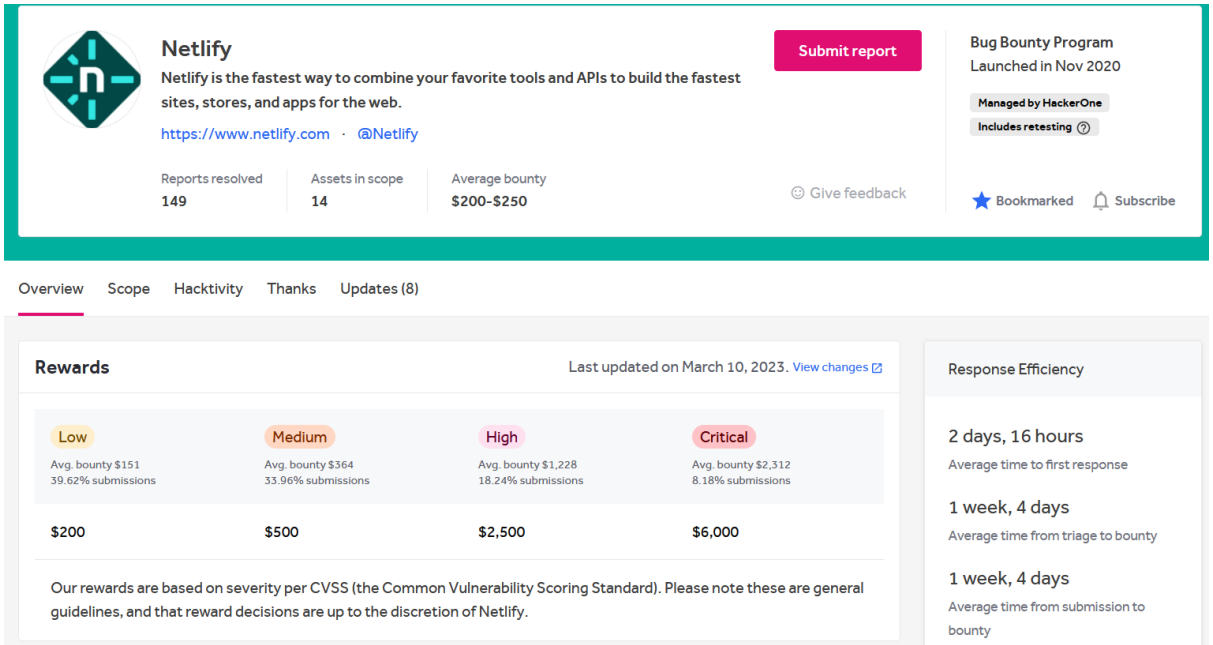
BUG BOUNTY

REPORT 4

Thilakarathna S.T.D- IT22578914

B.Sc. (Hons) in Information Technology Specializing in cyber security

Overview of the website



The flexible web platform Netify.com is revolutionizing how companies maintain their network infrastructure. With its all-inclusive toolkit and services, Netify makes network configuration, monitoring, and optimization easier, enabling businesses to improve security and performance while lowering operational costs. With capabilities like streamlined network setup, traffic pattern analysis, and seamless connectivity across multiple devices and locations, Netify gives organizations the flexibility and intelligence they need to succeed in the modern digital world. With its powerful capabilities and easy-to-use interface, Netify is a dependable partner for businesses looking to maximize the potential of their networks.

Scope

- **InScope**

netlify-cdp-loader.netlify.app Powers this feature: https://docs.netlify.com/site-deploys/deploy-previews/#collaborative-deploy-previews. JavaScript	Domain	In scope	Critical	Eligible	Mar 22, 2023	0 (0%)
***.services-prod.nsvcs.net**	Wildcard	In scope	Critical	Eligible	May 15, 2023	0 (0%)
***.ops.netlify.com**	Wildcard	In scope	Critical	Eligible	May 15, 2023	1 (1%)
***.infra-prod.nsvcs.net**	Wildcard	In scope	Critical	Eligible	May 15, 2023	1 (1%)
***.services.netlify.com**	Wildcard	In scope	Critical	Eligible	May 15, 2023	0 (0%)
internal.netlify.com JavaScript React	Domain	In scope	Critical	Eligible	Mar 22, 2023	6 (4%)
api.netlify.com `netlify api --list` after installing the CLI: https://docs.netlify.com/cli/get-started/. See also https://open-api.netlify.com/. Google Cloud Platform Kubernetes MongoDB Rails Ruby	Domain	In scope	Critical	Eligible	Oct 28, 2022	260 (174%)
app.netlify.com See https://docs.netlify.com/get-started/. Also `netlify init` after installing the CLI: https://docs.netlify.com/cli/get-started/. Google Cloud Platform JavaScript Kubernetes React TypeScript	Domain	In scope	Critical	Eligible	Mar 22, 2023	410 (275%)
***.onegraph.com** As of December 28, 2022 this feature is no longer available for Netlify users who have not yet enabled it. See https://docs.netlify.com/netlify-labs/experimental-features/netlify-graph/get-started/.	Wildcard	In scope	High	Eligible	May 15, 2023	6 (4%)
supportal.netlify.app	Domain	In scope	Medium	Eligible	Mar 22, 2023	0 (0%)
list-v2--netlify-plugins.netlify.app Powers templates offered by app.netlify.com. See: https://www.netlify.com/integrations/templates/.	Domain	In scope	Medium	Eligible	Oct 28, 2022	0 (0%)
internal-docs.netlify.com	Domain	In scope	Medium	Eligible	Oct 28, 2022	0 (0%)
netlify-rum.netlify.app	Domain	In scope	Medium	Eligible	Oct 28, 2022	0 (0%)
screenshot-proxy.netlify.app	Domain	In scope	Medium	Eligible	Oct 28, 2022	0 (0%)

- **OutScope**

*.netlify.app Except for the in scope subdomains listed as in scope.	Wildcard	Out of scope	None	Ineligible	May 15, 2023	0 (0%)
webpop.com This is an old asset and will be deprecated in the near future.	Domain	Out of scope	None	Ineligible	Nov 2, 2020	0 (0%)
https://github.com/netlify/	URL	Out of scope	None	Ineligible	Jul 13, 2023	0 (0%)
docs.netlify.com	Domain	Out of scope	None	Ineligible	Dec 5, 2022	0 (0%)
answers.netlify.com	Domain	Out of scope	None	Ineligible	Dec 5, 2022	0 (0%)
*.netlify.com Except for the in scope subdomains listed as in scope.	Wildcard	Out of scope	None	Ineligible	May 15, 2023	0 (0%)
*.netlifycms.org	Wildcard	Out of scope	None	Ineligible	Oct 16, 2023	0 (0%)
www.netlify.com This is Netlify's marketing website.	Domain	Out of scope	None	Ineligible	Jul 13, 2023	0 (0%)

Information Gathering

Security researchers and ethical hackers must first gather data through bug bounty programs in order to identify vulnerabilities in a target system or application. This step's objective is to learn as much as you can about the target, including its technologies, architecture, known vulnerabilities, and potential weak points. Open-source intelligence gathering (OSINT), network scanning, fingerprinting, and asset enumeration are typically required to give a complete view of the target's attack surface.

Since it enables ethical hackers to identify potential points of entry and focus their search for system security flaws, efficient information gathering is the cornerstone of a successful bug hunting operation.

Subdomains for Hunting

The process of listing sub-domains for one or more domains is called sub-domain enumeration. This is a critical stage in the reconnaissance process. Finding vulnerabilities is made more likely by sub-domain enumeration, which can identify several domains and sub-domains that are part of a security assessment.

Seen through cryptic, abandoned sub-domains, programs may have dangerous bugs.

The same weaknesses are frequently found throughout numerous domains and applications within a single organization.

- **Sublist3r**

Sublist3r is an open-source program used for efficient subdomain enumeration. Penetration testers, security experts, and ethical hackers utilize Sublist3r to locate subdomains linked to a target website. It accomplishes this by using methods like search engine scraping and DNS requests. Sublist3r only needs to know the target domain to begin searching for relevant subdomains. It then provides useful information that can be utilized for vulnerability discovery and security assessments.

```
┌──(tharusha㉿kali)-[~]
└─$ sublist3r -d netlify.com

                 # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for netlify.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 63
www.netlify.com
answers.netlify.com
answers-staging.netlify.com
bevoiceafrica.netlify.com
canyounot.netlify.com
www.canyounot.netlify.com
colorgrab.netlify.com
communication-test-2.netlify.com
communications.netlify.com
communications-test.netlify.com
community.netlify.com
ctr-lang-docs.netlify.com
fake-site.netlify.com
fake-site-hackerone-866036-javierprovecho.netlify.com
featureflags.netlify.com
graph.netlify.com
hellofrom.netlify.com
mariazobi.netlify.com
ops.netlify.com
consul.ops.netlify.com
grafana.ops.netlify.com
humio-sandbox.ops.netlify.com
humio-sandbox-es.ops.netlify.com
influx.ops.netlify.com
jenkins.ops.netlify.com
jenkins-ec2.ops.netlify.com
kairosdb.ops.netlify.com
```

```
kibana.ops.netlify.com
monitoring.ops.netlify.com
netlify-ghe.ops.netlify.com
assets.netlify-ghe.ops.netlify.com
avatars.netlify-ghe.ops.netlify.com
codeload.netlify-ghe.ops.netlify.com
gist.netlify-ghe.ops.netlify.com
media.netlify-ghe.ops.netlify.com
pages.netlify-ghe.ops.netlify.com
raw.netlify-ghe.ops.netlify.com
render.netlify-ghe.ops.netlify.com
uploads.netlify-ghe.ops.netlify.com
netlify-gitlab.ops.netlify.com
prerender.ops.netlify.com
rethink.ops.netlify.com
spinnaker.ops.netlify.com
spinnaker-api.ops.netlify.com
spinnaker-test.ops.netlify.com
spinnaker-test-api.ops.netlify.com
term.ops.netlify.com
rbl-test.netlify.com
ruhr-wildwest.netlify.com
services.netlify.com
api-create.services.netlify.com
dev-api-create.services.netlify.com
stg-api-create.services.netlify.com
sisponysoeg.netlify.com
slt.netlify.com
authlify.smashingapi.netlify.com
comments.smashingapi.netlify.com
git.smashingapi.netlify.com
gocommerce.smashingapi.netlify.com
staging-community.netlify.com
status.netlify.com
swag.netlify.com
trust.netlify.com
```

- **Amass**

A tool has been developed by the OWASP Amass Project to assist information security professionals in external asset discovery and network mapping of attack surfaces.

```
┌──(tharusha㉿kali)-[~]
└─$ sudo amass enum -passive -d netlify.com
[sudo] password for tharusha:
'https://www.netcraft.com/' netlify.com (FQDN) --> ns_record --> ns02.netlifydns.com (FQDN)
netlify.com (FQDN) --> ns_record --> dns3.p04.nsone.net (FQDN)
netlify.com (FQDN) --> ns_record --> dns2.p04.nsone.net (FQDN)
netlify.com (FQDN) --> ns_record --> ns01.netlifydns.com (FQDN)
netlify.com (FQDN) --> ns_record --> ns03.netlifydns.com (FQDN)
netlify.com (FQDN) --> ns_record --> dns4.p04.nsone.net (FQDN)
netlify.com (FQDN) --> ns_record --> dns1.p04.nsone.net (FQDN)
netlify.com (FQDN) --> ns_record --> ns04.netlifydns.com (FQDN)
netlify.com (FQDN) --> mx_record --> aspmx2.googlemail.com (FQDN)
netlify.com (FQDN) --> mx_record --> aspmx.l.google.com (FQDN)
netlify.com (FQDN) --> mx_record --> alt2.aspmx.l.google.com (FQDN)
netlify.com (FQDN) --> mx_record --> aspmx3.googlemail.com (FQDN)
netlify.com (FQDN) --> mx_record --> alt1.aspmx.l.google.com (FQDN)
ns02.netlifydns.com (FQDN) --> a_record --> 45.54.30.65 (IPAddress)
ns02.netlifydns.com (FQDN) --> aaaa_record --> 2607:f740:e630:4::1 (IPAddress)
digitaldemocracy.netlify.com (FQDN) --> a_record --> 46.137.195.11 (IPAddress)
digitaldemocracy.netlify.com (FQDN) --> a_record --> 13.228.199.255 (IPAddress)
digitaldemocracy.netlify.com (FQDN) --> aaaa_record --> 2406:da18:b3d:e202::64 (IPAddress)
digitaldemocracy.netlify.com (FQDN) --> aaaa_record --> 2406:da18:880:3800::c8 (IPAddress)
048930963719626.netlify.com (FQDN) --> a_record --> 46.137.195.11 (IPAddress)
048930963719626.netlify.com (FQDN) --> a_record --> 13.251.96.10 (IPAddress)
048930963719626.netlify.com (FQDN) --> aaaa_record --> 2406:da18:b3d:e201::64 (IPAddress)
048930963719626.netlify.com (FQDN) --> aaaa_record --> 2406:da18:880:3802::c8 (IPAddress)
ecstatic-mcnulty-1e7f00.netlify.com (FQDN) --> a_record --> 18.139.194.139 (IPAddress)
ecstatic-mcnulty-1e7f00.netlify.com (FQDN) --> a_record --> 13.251.96.10 (IPAddress)
sharp-pike-747d00.netlify.com (FQDN) --> a_record --> 54.161.234.33 (IPAddress)
sharp-pike-747d00.netlify.com (FQDN) --> a_record --> 54.84.236.175 (IPAddress)
sharp-pike-747d00.netlify.com (FQDN) --> aaaa_record --> 2406:da18:880:3802::c8 (IPAddress)
sharp-pike-747d00.netlify.com (FQDN) --> aaaa_record --> 2406:da18:b3d:e201::64 (IPAddress)
seeo.netlify.com (FQDN) --> a_record --> 46.137.195.11 (IPAddress)
seeo.netlify.com (FQDN) --> a_record --> 52.74.166.77 (IPAddress)
seeo.netlify.com (FQDN) --> aaaa_record --> 2600:1f18:2489:8200::c8 (IPAddress)
seeo.netlify.com (FQDN) --> aaaa_record --> 2600:1f18:16e:df00::64 (IPAddress)
promoterleopard-15301.netlify.com (FQDN) --> a_record --> 13.228.199.255 (IPAddress)
promoterleopard-15301.netlify.com (FQDN) --> a_record --> 13.215.144.61 (IPAddress)
ruhr-wildwest.netlify.com (FQDN) --> a_record --> 52.58.254.253 (IPAddress)
ruhr-wildwest.netlify.com (FQDN) --> a_record --> 18.192.94.96 (IPAddress)
ruhr-wildwest.netlify.com (FQDN) --> aaaa_record --> 2a05:d014:58f:6201::64 (IPAddress)
ruhr-wildwest.netlify.com (FQDN) --> aaaa_record --> 2a05:d014:275:cb01::c8 (IPAddress)
nifty-wing-a0ea10.netlify.com (FQDN) --> a_record --> 18.192.231.252 (IPAddress)
nifty-wing-a0ea10.netlify.com (FQDN) --> a_record --> 3.70.101.28 (IPAddress)
nifty-wing-a0ea10.netlify.com (FQDN) --> aaaa_record --> 2406:da18:880:3802::c8 (IPAddress)
nifty-wing-a0ea10.netlify.com (FQDN) --> aaaa_record --> 2406:da18:b3d:e201::64 (IPAddress)
monk-bear-77310.netlify.com (FQDN) --> a_record --> 54.84.236.175 (IPAddress)
monk-bear-77310.netlify.com (FQDN) --> a_record --> 44.219.53.183 (IPAddress)
dealer-horse-30010.netlify.com (FQDN) --> a_record --> 35.169.59.174 (IPAddress)
dealer-horse-30010.netlify.com (FQDN) --> a_record --> 54.84.236.175 (IPAddress)
```

```
dealer-horse-30010.netlify.com (FQDN) ⟶ a_record ⟶ 54.84.236.175 (IPAddress)
dealer-horse-30010.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2406:da18:880:3802::c8 (IPAddress)
dealer-horse-30010.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2406:da18:b3d:e201::64 (IPAddress)
yihui.netlify.com (FQDN) ⟶ a_record ⟶ 13.215.144.61 (IPAddress)
yihui.netlify.com (FQDN) ⟶ a_record ⟶ 13.251.96.10 (IPAddress)
yihui.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2406:da18:b3d:e201::64 (IPAddress)
yihui.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2406:da18:b3d:e202::64 (IPAddress)
chairmanflorence-60521.netlify.com (FQDN) ⟶ a_record ⟶ 3.70.101.28 (IPAddress)
chairmanflorence-60521.netlify.com (FQDN) ⟶ a_record ⟶ 18.192.231.252 (IPAddress)
chairmanflorence-60521.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2406:da18:b3d:e200::64 (IPAddress)
chairmanflorence-60521.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2406:da18:b3d:e202::64 (IPAddress)
18--elegant-visvesvaraya-7ec74b.netlify.com (FQDN) ⟶ a_record ⟶ 44.217.161.11 (IPAddress)
18--elegant-visvesvaraya-7ec74b.netlify.com (FQDN) ⟶ a_record ⟶ 54.84.236.175 (IPAddress)
18--elegant-visvesvaraya-7ec74b.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2600:1f18:16e:df00::64 (IPAddress)
18--elegant-visvesvaraya-7ec74b.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2600:1f18:2489:8202::c8 (IPAddress)
architectchicken-74778.netlify.com (FQDN) ⟶ a_record ⟶ 13.251.96.10 (IPAddress)
architectchicken-74778.netlify.com (FQDN) ⟶ a_record ⟶ 18.139.194.139 (IPAddress)
architectchicken-74778.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2a05:d014:275:cb00::c8 (IPAddress)
architectchicken-74778.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2a05:d014:58f:6201::64 (IPAddress)
gardenertape-28187.netlify.com (FQDN) ⟶ a_record ⟶ 13.215.144.61 (IPAddress)
gardenertape-28187.netlify.com (FQDN) ⟶ a_record ⟶ 18.139.194.139 (IPAddress)
gardenertape-28187.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2600:1f18:2489:8202::c8 (IPAddress)
gardenertape-28187.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2600:1f18:16e:df02::64 (IPAddress)
accountant-bob-42510.netlify.com (FQDN) ⟶ a_record ⟶ 18.139.194.139 (IPAddress)
accountant-bob-42510.netlify.com (FQDN) ⟶ a_record ⟶ 46.137.195.11 (IPAddress)
accountant-bob-42510.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2a05:d014:58f:6200::64 (IPAddress)
accountant-bob-42510.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2a05:d014:58f:6202::64 (IPAddress)
confident-noyce-526310.netlify.com (FQDN) ⟶ a_record ⟶ 3.72.140.173 (IPAddress)
confident-noyce-526310.netlify.com (FQDN) ⟶ a_record ⟶ 35.156.224.161 (IPAddress)
confident-noyce-526310.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2a05:d014:58f:6201::64 (IPAddress)
confident-noyce-526310.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2a05:d014:275:cb00::c8 (IPAddress)
cartoonistdent-67427.netlify.com (FQDN) ⟶ a_record ⟶ 44.217.161.11 (IPAddress)
cartoonistdent-67427.netlify.com (FQDN) ⟶ a_record ⟶ 54.161.234.33 (IPAddress)
cartoonistdent-67427.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2600:1f18:2489:8202::c8 (IPAddress)
cartoonistdent-67427.netlify.com (FQDN) ⟶ aaaa_record ⟶ 2600:1f18:16e:df00::64 (IPAddress)
```

- **Netcraft**

Based in Bath, Somerset, England, Netcraft provides internet services. A variety of industries are served by the company's cybercrime disruption services. I learned useful knowledge from this website. Like backdrop, IP delegation, SSL/TLS, Network, and Transparency of Certificates.

netcraft

LEARN MORE | REPORT FRAUD

Background

Site title	Scale & Ship Faster with a Composable Web Architecture | Netlify	**Date first seen**	December 2014
Site rank	12087	**Primary language**	English
Description	Realize the speed, agility and performance of a scalable, composable web architecture with Netlify. Explore the composable web platform now!		

Network

Site	https://www.netlify.com	**Domain**	netlify.com
Netblock Owner	Amazon Data Services Ireland Limited	**Nameserver**	dns1.p04.nsone.net
Hosting company	Amazon - EU West (Ireland) datacenter	**Domain registrar**	name.com
Hosting country	ie	**Nameserver organisation**	whois.corporatedomains.com
IPv4 address	34.249.214.183 (VirusTotal)	**Organisation**	Netlify, Non-Public Data, Non-Public Data, 00000, United States
IPv4 autonomous systems	AS16509	**DNS admin**	hostmaster@nsone.net
IPv6 address	2a05:d018:1d0c:7400:0:0:0:1f4	**Top Level Domain**	Commercial entities (.com)
IPv6 autonomous systems	AS16509	**DNS Security Extensions**	Unknown
Reverse DNS	ec2-34-249-214-183.eu-west-1.compute.amazonaws.com		

IP delegation

IPv4 address (34.249.214.183)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 34.0.0.0-34.255.255.255	United States	NET34	American Registry for Internet Numbers
↳ 34.192.0.0-34.255.255.255	United States	AT-88-Z	Amazon Technologies Inc.
↳ 34.248.0.0-34.255.255.255	Ireland	AMAZON-DUB	Amazon Data Services Ireland Limited
↳ 34.249.214.183	Ireland	AMAZON-DUB	Amazon Data Services Ireland Limited

IPv6 address (2a05:d018:1d0c:7400:0:0:0:1f4)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
↳ 2a00::/11	European Union	EU-ZZ-2A00	RIPE NCC
↳ 2a00::/12	Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre
↳ 2a05:d000::/25	Ireland	IE-AMAZON-20150219	Amazon Data Services Ireland Ltd
↳ 2a05:d010::/28	European Union	EC2-Aggregate	
↳ 2a05:d018:1d0c:7400:0:0:0:1f4	European Union	EC2-Aggregate	

SSL/TLS

Assurance	Organisation validation	**Perfect Forward Secrecy**	Yes
Common name	*.netlify.com	**Supported TLS Extensions**	RFC8446 supported versions, RFC8446 key share, RFC7301 application-layer protocol negotiation
Organisation	Netlify, Inc	**Application-Layer Protocol Negotiation**	h2
State	California	**Next Protocol Negotiation**	Not Present
Country	US	**Issuing organisation**	DigiCert Inc
Organisational unit	Not Present	**Issuer common name**	DigiCert TLS Hybrid ECC SHA384 2020 CA1
Subject Alternative Name	*.netlify.com, netlify.com	**Issuer unit**	Not Present
Validity period	From Jul 14 2023 to Aug 13 2024 (12 months, 4 weeks, 2 days)	**Issuer location**	Not Present
Matches hostname	Yes	**Issuer country**	US
Server	Netlify	**Issuer state**	Not Present
Public key algorithm	id-ecPublicKey	**Certificate Revocation Lists**	http://crl3.digicert.com/DigiCertTLSHybridECCSHA3842020CA1-1.crl http://crl4.digicert.com/DigiCertTLSHybridECCSHA3842020CA1-1.crl
Protocol version	TLSv1.3	**Certificate Hash**	u/bxK0mS5gPXLWXEeTfuxQCZ0NI
Public key length	256	**Public Key Hash**	90059138b605b47ebc1e33a966f8c787f5c31a3b5e8207602e850fa6aba68bb1
Certificate check	ok	**OCSP servers**	http://ocsp.digicert.com
Signature algorithm	ecdsa-with-SHA384	**OCSP stapling response**	No response received
Serial number	0x0f8e0be5aa6915709a2d0ebae8b16		

- **DNSrecon**

For DNS enumeration and reconnaissance, an open-source tool named DNSRecon is utilized. The purpose of gathering information is to assist with penetration testing and security evaluations by providing details on DNS servers, domains, subdomains, and DNS records.

```
┌──(tharusha㉿kali)-[~]
└─$ dnsrecon -d netlify.com
[*] std: Performing General Enumeration against: netlify.com...
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 52.74.166.77
[!] It is resolving to 13.215.144.61
[!] All queries will resolve to this list of addresses!!
[-] DNSSEC is not configured for netlify.com
[*]      SOA dns1.p04.nsone.net 198.51.44.4
[*]      SOA dns1.p04.nsone.net 2620:4d:4000:6259:7:4:0:1
[*]      NS dns2.p04.nsone.net 198.51.45.4
[*]      Bind Version for 198.51.45.4 "a0bd971e3"
[*]      NS dns2.p04.nsone.net 2a00:edc0:6259:7:4::2
[*]      NS ns01.netlifydns.com 45.54.30.1
[*]      Bind Version for 45.54.30.1 "a0bd971e3"
[*]      NS ns01.netlifydns.com 2607:f740:e630::1
[*]      NS dns4.p04.nsone.net 198.51.45.68
[*]      Bind Version for 198.51.45.68 "a0bd971e3"
[*]      NS dns4.p04.nsone.net 2a00:edc0:6259:7:4::4
[*]      NS ns04.netlifydns.com 45.54.30.193
[*]      Bind Version for 45.54.30.193 "a0bd971e3"
[*]      NS ns04.netlifydns.com 2607:f740:e630:c::1
[*]      NS ns02.netlifydns.com 45.54.30.65
[*]      Bind Version for 45.54.30.65 "a0bd971e3"
[*]      NS ns02.netlifydns.com 2607:f740:e630:4::1
[*]      NS ns03.netlifydns.com 45.54.30.129
[*]      Bind Version for 45.54.30.129 "a0bd971e3"
[*]      NS ns03.netlifydns.com 2607:f740:e630:8::1
[*]      NS dns3.p04.nsone.net 198.51.44.68
[*]      Bind Version for 198.51.44.68 "a0bd971e3"
[*]      NS dns3.p04.nsone.net 2620:4d:4000:6259:7:4:0:3
[*]      NS dns1.p04.nsone.net 198.51.44.4
[*]      Bind Version for 198.51.44.4 "a0bd971e3"
[*]      NS dns1.p04.nsone.net 2620:4d:4000:6259:7:4:0:1
[*]      MX alt2.aspmx.l.google.com 142.250.141.26
[*]      MX aspmx.l.google.com 172.217.194.27
[*]      MX aspmx2.googlemail.com 173.194.202.27
[*]      MX aspmx3.googlemail.com 142.250.141.27
[*]      MX alt1.aspmx.l.google.com 173.194.202.27
[*]      MX alt2.aspmx.l.google.com 2607:f8b0:4023:c0b::1a
[*]      MX aspmx.l.google.com 2404:6800:4003:c04::1a
[*]      MX aspmx2.googlemail.com 2607:f8b0:400e:c00::1b
[*]      MX aspmx3.googlemail.com 2607:f8b0:4023:c0b::1b
[*]      MX alt1.aspmx.l.google.com 2607:f8b0:400e:c00::1a
[*]      A netlify.com 65.2.47.247
[*]      A netlify.com 13.127.237.255
[*]      AAAA netlify.com 2406:da1a:103:e602::1f4
[*]      AAAA netlify.com 2406:da1a:103:e601::1f4
[*]      TXT _dmarc.netlify.com v=DMARC1; p=reject; rua=mailto:fexahwip@ag.dmarcian.com; ruf=mailto:fexahwip@fr.dmarcian.com; fo=1
[*] Enumerating SRV Records
[-] No SRV Records Found for netlify.com
```

- **Whatweb**

A web application's technology stack can be discovered with this open-source research tool. It analyzes HTTP answers from a target web server to collect further information about the web server, web framework, programming language, content management system (CMS), JavaScript libraries, and other technologies that the target site may be utilizing.

```
┌──(tharusha㉿kali)-[~]
└─$ whatweb netlify.com
http://netlify.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Netlify], IP[13.127.237.255], RedirectLocation[https://netlify.com/], UncommonHeaders[x-nf-request-id]
https://netlify.com/ [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Netlify], IP[3.7.135.175], RedirectLocation[https://www.netlify.com/], Strict-Transport-Security[max-age=31536000; i
nHeaders[x-nf-request-id]
https://www.netlify.com/ [200 OK] Country[UNITED STATES][US], Email[fraud@netlify.com], Frame, HTML5, HTTPServer[Netlify], IP[65.2.47.247], MetaGenerator[Astro v4.4.11], Open-Graph-Protocol[website],
ict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[Scale &amp; Ship Faster with a Composable Web Architecture | Netlify], UncommonHeaders[cache-status,permissions-policy,serve
```

- **Wafw00f**

An open-source program called Wafw00f is used to identify and fingerprint Web application firewalls (WAFs). Web application firewalls (WAFs), security solutions, defend against SQL injection, cross-site scripting (XSS), and other attacks.

```
┌──(tharusha㉿kali)-[~]
└─$ wafw00f netlify.com

                    ____
                   /    \
                  (  Woof! )
                   \  ___/
                  ,,
             .-. _
            ()``; |==|_______)
           / ('        /|\
      (  /  )         / | \
       \(_)_))       /  |  \

                  ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://netlify.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

- **Using nmap, open port enumeration**

Open port enumeration is a method for locating and classifying the open network ports on a target machine or network using the Nmap (Network Mapper) program. Nmap is an effective open-source tool for network scanning and host discovery that provides extensive information on the services and statuses that are running on various ports. This process involves sending specially made packets to a target system and analyzing the responses in order to determine which ports are open and what services are using them.

Nmap is a popular tool for network administrators and security specialists to assess system security, identify potential security flaws, and enhance network configurations due to its abundance of features and versatility. It's a helpful tool for enhancing security and computer network administration in general.

```
┌──(tharusha㉿kali)-[~]
└─$ sudo nmap -sS netlify.com
[sudo] password for tharusha:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-09 19:16 EDT
Nmap scan report for netlify.com (13.127.237.255)
Host is up (0.013s latency).
Other addresses for netlify.com (not scanned): 65.2.47.247 2406:da1a:103:e602::1f4 2406:da1a:103:e600::1f4
rDNS record for 13.127.237.255: ec2-13-127-237-255.ap-south-1.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.46 seconds
┌──(tharusha㉿kali)-[~]
└─$ sudo nmap --script vuln netlify.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-09 19:18 EDT
Nmap scan report for netlify.com (3.7.135.175)
Host is up (0.012s latency).
Other addresses for netlify.com (not scanned): 13.127.237.255 2406:da1a:103:e600::1f4 2406:da1a:103:e601::1f4
rDNS record for 3.7.135.175: ec2-3-7-135-175.ap-south-1.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
443/tcp open  https
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

Nmap done: 1 IP address (1 host up) scanned in 198.12 seconds
```

- **Using Nikto to scan for vulnerabilities**

One method to check for vulnerabilities in Kali Linux is to use the powerful open-source tool Nikto web scanner, which is part of the popular operating system for penetration testing and ethical hacking. Nikto is specifically designed to identify and assess server and web application vulnerabilities.

When checking target web servers for known vulnerabilities, common security issues, and misconfigurations, Nikto can be used from the Kali Linux command line. Nikto searches for issues including outdated software, possibly unsafe scripts, security headers, and other online vulnerabilities. It helps ethical hackers and security professionals understand and reduce such threats by providing comprehensive information on the vulnerabilities discovered.

```
┌──(tharusha㉿kali)-[~]
└─$ sudo nikto -h netlify.com
[sudo] password for tharusha:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 13.127.237.255, 65.2.47.247, 2406:da1a:103:e602::1f4, 2406:da1a:103:e600::1f4
+ Target IP:          13.127.237.255
+ Target Hostname:    netlify.com
+ Target Port:        80
+ Start Time:         2024-05-09 19:17:16 (GMT-4)
---------------------------------------------------------------------------
+ Server: Netlify
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Netlify was identified by the x-nf-request-id header. See: https://www.netlify.com/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the
sing-content-type-header/
+ Root page / redirects to: https://netlify.com/
^C

┌──(tharusha㉿kali)-[~]
└─$ sudo nikto -h 13.127.237.255
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          13.127.237.255
+ Target Hostname:    13.127.237.255
+ Target Port:        80
+ Start Time:         2024-05-09 19:17:42 (GMT-4)
---------------------------------------------------------------------------
+ Server: Netlify
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Netlify was identified by the x-nf-request-id header. See: https://www.netlify.com/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the
sing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Exploitation

I employed PWNXSS and SQLMAP tools to identify cross-site and SQL injection vulnerabilities in the target web application for the exploitations.

- **PwnXSS**

PwnXSS is a free and open-source application that may be found on GitHub. This program especially detects cross-site scripting. I execute several payloads in numerous web application directories while testing my target domain for XSS vulnerabilities. After the test, I discovered that indrive.com had no XSS vulnerabilities.

```
┌──(tharusha㉿kali)-[~/PwnXSS]
└─$ python3 pwnxss.py -u https://www.netlify.com/contact/?attr=homepage

PWNXSS  {v0.5 Final}
        https://github.com/pwn0sec/PwnXSS

<<<<<<< STARTING >>>>>>>

[19:33:33] [INFO] Starting PwnXSS...
***************
[19:33:33] [INFO] Checking connection to: https://www.netlify.com/contact/?attr=homepage
[19:33:34] [INFO] Connection estabilished 200
[19:33:34] [WARNING] Target have form with POST method: https://www.netlify.com/contact/?attr=homepage
[19:33:34] [INFO] Collecting form input key.....
[19:33:34] [INFO] Form key name: firstname value: <script>alert(6000/3000)</script>
[19:33:34] [INFO] Form key name: lastname value: <script>alert(6000/3000)</script>
[19:33:34] [INFO] Form key name: email value: <script>alert(6000/3000)</script>
[19:33:34] [INFO] Form key name: company value: <script>alert(6000/3000)</script>
[19:33:34] [INFO] Internal error: 'type'
[19:33:34] [INFO] Form key name: utm_campaign value: <script>alert(6000/3000)</script>
[19:33:34] [INFO] Form key name: utm_content value: <script>alert(6000/3000)</script>
[19:33:34] [INFO] Form key name: utm_medium value: <script>alert(6000/3000)</script>
[19:33:34] [INFO] Form key name: utm_source value: <script>alert(6000/3000)</script>
[19:33:34] [INFO] Form key name: utm_term value: <script>alert(6000/3000)</script>
[19:33:34] [INFO] Form key name: attr value: <script>alert(6000/3000)</script>
[19:33:34] [INFO] Form key name: hubspotformid value: <script>alert(6000/3000)</script>
[19:33:34] [INFO] Form key name: hubspotutk value: <script>alert(6000/3000)</script>
[19:33:34] [INFO] Internal error: 'type'
[19:33:34] [INFO] Internal error: 'name'
[19:33:34] [INFO] Sending payload (POST) method...
[19:33:34] [INFO] Parameter page using (POST) payloads but not 100% yet...
[19:33:34] [WARNING] Found link with query: attr=homepage Maybe a vuln XSS point
[19:33:34] [INFO] Query (GET) : https://www.netlify.com/contact/?attr=<script>alert(6000/3000)</script>#main
[19:33:34] [INFO] Query (GET) : https://www.netlify.com/contact/?attr=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E#main
[19:33:34] [INFO] Parameter page using (GET) payloads but not 100% yet...
[19:33:34] [WARNING] Found link with query: subject=Abuse%20report&body=Please%20include%20the%20site%20URL%20and%20reason%20for%20your%20report%2C%20and%20we%20will%20reply%20promptly. Maybe a vuln XSS point
[19:33:34] [INFO] Query (GET) : mailto:fraud@netlify.com?subject=<script>alert(6000/3000)</script>
[19:33:34] [INFO] Query (GET) : mailto:fraud@netlify.com?subject=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&body=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[19:33:34] [INFO] URL is not an HTTP url, ignoring
***************
```

- **SQLmap**

An open-source penetration testing tool called SQL Map automatically locates and takes advantage of SQL injection vulnerabilities to take over databases.

In an attempt to locate any web application injection points, I experimented with various payloads and parameters. I tested this application and discovered that it is not injectable.

```
┌──(tharusha㉿kali)-[~]
└─$ sqlmap -u 'https://app.netlify.com/login/email'
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state
esponsible for any misuse or damage caused by this program

[*] starting @ 19:26:06 /2024-05-09/

[19:26:06] [WARNING] you've provided target URL without any GET parameters (e.g. 'http://www.site.com/article.php?id=1') and without providing any POST parameters through op
do you want to try URI injections in the target URL itself? [Y/n/q] y
[19:26:09] [INFO] testing connection to the target URL
[19:26:09] [INFO] checking if the target is protected by some kind of WAF/IPS
[19:26:10] [INFO] testing if the target URL content is stable
[19:26:10] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parame
 manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] y
[19:26:12] [INFO] searching for dynamic content
[19:26:12] [INFO] dynamic content marked for removal (25 regions)
[19:26:12] [INFO] testing if URI parameter '#1*' is dynamic
[19:26:13] [WARNING] URI parameter '#1*' does not appear to be dynamic
[19:26:14] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[19:26:14] [INFO] testing for SQL injection on URI parameter '#1*'
[19:26:14] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:26:21] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:26:22] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[19:26:24] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[19:26:26] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[19:26:28] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[19:26:30] [INFO] testing 'Generic inline queries'
[19:26:31] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[19:26:33] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[19:26:35] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[19:26:37] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[19:26:39] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[19:26:41] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[19:26:43] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[19:27:25] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[19:27:30] [WARNING] URI parameter '#1*' does not seem to be injectable
[19:27:30] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. You can
has a low percentage of textual content (~0.84% of page content is text). If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could
nd/or switch '--random-agent'

[*] ending @ 19:27:30 /2024-05-09/
```

Vulnerabilities detect when Scanning

In order to process and find problems and vulnerabilities that are based on the OWASP top 10, I used tool like OWASP ZAP.

OWASP ZAP is a testing tool that may be used to identify potential security gaps in internet applications. OWASP ZAP can be used to find common vulnerabilities such as SQL injection and cross-site scripting (XSS).

1. Vulnerability Title

Edit Alert

Hash Disclosure - Mac OSX salted SHA-1	
URL:	https://www.netlify.com/v3/img/blog/screen-shot-2021-06-22-at-10.31.49-pm.jpg
Risk:	High
Confidence:	Medium
Parameter:	
Attack:	
Evidence:	9797979797979797979797979797979797979797979797
CWE ID:	200
WASC ID:	13

Vulnerability Description

A hash was disclosed by the web server. - Mac OSX salted SHA-1

How to mitigate

Ensure that hashes that are used to protect credentials or other resources are not leaked by the web server or database. There is typically no requirement for password hashes to be accessible to the web browser.

2. Vulnerability Title

Edit Alert

PII Disclosure	
URL:	https://www.netlify.com/blog/modular-web-design-architecture/
Risk:	High
Confidence:	High
Parameter:	
Attack:	
Evidence:	5068792632343
CWE ID:	359
WASC ID:	13

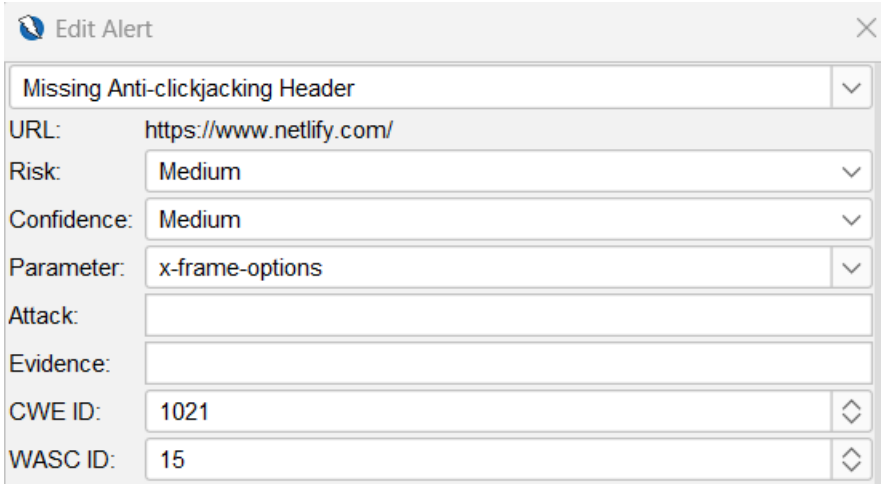
Vulnerability Description

The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

How to mitigate

Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

3. Vulnerability Title



Vulnerability Description

The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

How to mitigate

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.