VULNERABILITY ASSESSMENT-WEB AUDIT

Sri Lanka Institute of Information Technology

https://www. topcoder.com/

Submitted by:

Student Registration Number	Student Name
IT20643904	MUNASINGHA R.S.I

Purpose

I completed this web audit to finish my Web security module (IE2062) semester end assignment. This report will cover a wide range of topics related to my project. We had to follow the criteria supplied by the experimental website's original web platform, which offered it as a vulnerability testing environment, in order to write a web audit or bug bounty. Rather of using bug bounties to gain money, I opted to utilize this chance to develop my web security abilities by gathering information and reviewing the exploitations that are now being used on real-world active websites all across the internet. I had to learn how to use a variety of technologies to accomplish the same goals as a beginner cyber security student, so I did. This report will cover how I used the hackerone platform to examine five subdomains of a chosen website, as well as any additional tools I employed.

Abstract

Cybercrime, deception, and data breach are all risks that pose significant risks to businesses. A great deal has been lost, and organizations must devise procedures to prevent the hazards from becoming serious and to avert similar catastrophes. This investigation looked into the mechanisms connected with IT security web audits and how they might help firms enhance their IT security. The study assessed IT administrators' and employees' awareness of cybercrime risks, as well as their understanding of IT security audit norms and standards and the impact of IT security audit on the organization's growth. This inquiry used an organization as a backdrop, assessing the company's flow IT security audit state and determining adaptability for the establishment of an IT security audit strategy and system. A quantitative investigation was carried out in order to gather more information on cybercrime and to compile more comprehensive data on the subject. This inquiry definitely shown that an IT security audit is critical for the growth of every organization that uses technology.

Table of Content

Introduction

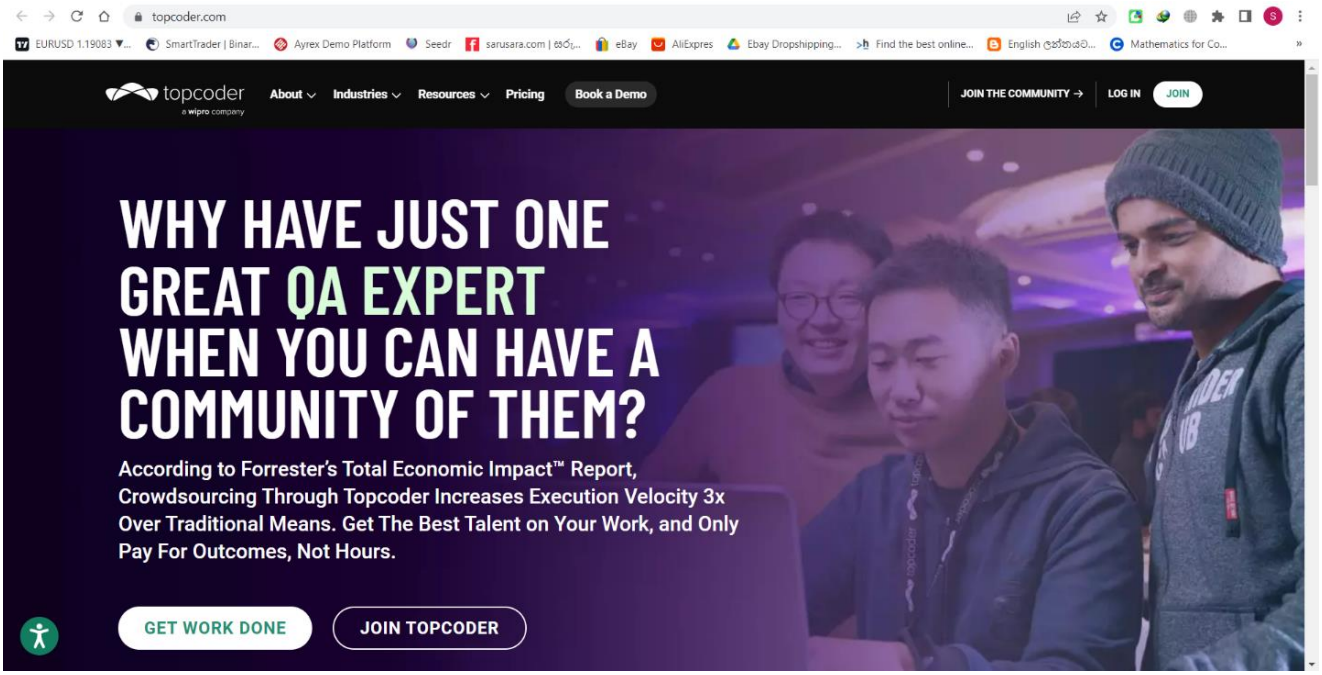
Hackers may exploit all of the weaknesses and security risks revealed by website vulnerability assessments. Online audits encompass all aspects of a web application, such as the infrastructure, extensions, themes, server settings, SSL connection, and so on, to assist you understand how your website may be attacked.

We can utilize this audit to find defects and security problems at that point. We may then move on to web penetration. The threats caused by these weaknesses can now be mitigated by security specialists.

The purpose of a website security audit is to find and correct flaws in the design of your website before they are discovered by malicious hackers.

Scope

My effort was limited to five topcoder.com subdomains, which were part of the hackerone platform's vulnerability disclosure program. These domains, as well as all of their subdomains, are covered by the vulnerability disclosure.



OWASP Top 10 Security Risks and Vulnerabilities

A01:2021-Broken Access Control - https://owasp.org/Top10/A01_2021-Broken_Access_Control/	By giving the attacker the same privileges as the victim, broken authentication attacks aim to obtain control of one or more accounts. When passwords, keys, or session tokens, user account information, and other data are compromised, authentication is "broken."
A02:2021-Cryptographic Failures- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/	Failure of a cryptographic is the same as failure of a cryptographic algorithm. These days many cryptographic techniques are being used to encrypt sensitive information. Passwords, credit card numbers, health recodes, corporate secrets, and other sensitive data are examples.
A03:2021-Injection - https://owasp.org/Top10/A03_2021-Injection/	Using java script, xml, sql, and other programming languages, the attacker injects malicious code into the website. The attacker can acquire access to the web database and site privileges after injecting this code.
A04:2021-Insecure Design - https://owasp.org/Top10/A04_2021-Insecure_Design/	This is a new added vulnerability in the top ten owasp vulnerabilities. This indicates that the web site design has a low level of security. Simply put, this is a developer error. Using unneeded APIs and functions is an example. If developers use these APIs, the website's security is threatened.
A05:2021-Security Misconfiguration - https://owasp.org/Top10/A05_2021-Security_Misconfiguration/	This vulnerability, also known as security misconfiguration, happens when a server or online application fails to enforce or effectively apply all of the security rules.
A06:2021-Vulnerable and Outdated Components - https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/	It likes, online applications, operating systems, data base management systems, APIs, and all runtime environments, all of which are out of date and do not apply security patches. This is a basic example of Vulnerable and Obsolete Components.

A07:2021-Identification and Authentication Failures- https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/	It's critical to check the user's identity, authenticate them, and manage their sessions in order to protect against authentication-related risks. Authentication flaws might be present if the application:
A08:2021-Software and Data Integrity Failures- https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/	"Integrity breaches are not secured by code and infrastructure," according to software and data integrity failures. for example, Some applications allow auto-updating features, when an attacker delivers malicious plugins or extensions to those applications, the attacker can utilize the auto-updating function to steal sensitive data. The system previously trusted apps. The key issue was that the system was unable to identify attackers.
A09:2021-Security Logging and Monitoring Failures- https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/	There is a lack of properly recoding historical information regarding events that occurred within an application. Auditable events, such as logins, unsuccessful logins, and high-value transactions, are not logged by the program. In real time or near real time, the program is unable to identify, escalate, or alert for active attacks. Vulnerability scanning and penetration tests do not raise an alert.
A10:2021-Server-Side Request Forgery- https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/	Server-Side Request Forgery allows an attacker to use a server-side application to send http requests to any domain the attacker wants. A successful SSRF attack might result in unauthorized activity or access to company data, either in the vulnerable application itself or on other back-end systems with which the program interacts. In certain conditions, the SSRF vulnerability could allow an attacker to run arbitrary commands.

Risk Levels

Critical	Exploitation of the vulnerability will very probably result in root-level penetration of a server or infrastructure device. Exploitation is a simple process.
High	The issue is difficult to exploit, but if it is, it may lead to higher privileges. The exploit could result in data loss or unavailability.
Medium	The medium risk level denotes a high amount of risk in conjunction with a specific vulnerability. An attacker can obtain low-level information about the program by exploiting a medium vulnerability. After the high-risk vulnerabilities have been addressed, the medium-risk vulnerabilities should be addressed.
Low	The low-risk level denotes the lowest amount of danger associated with a certain vulnerability. This may lead to the acquisition of information about the web application that would not otherwise be available.

In Scope Domains

In Scope			
Domain	www.topcoder.com	Critical	Ineligible
Domain	api.topcoder.com	Critical	Ineligible
Domain	arena.topcoder.com	Critical	Ineligible
Domain	blockchain.topcoder.com	Critical	Ineligible
Domain	bugzilla.topcoder.com	Critical	Ineligible
Domain	cmap.topcoder.com	Critical	Ineligible
Domain	cognitive.topcoder.com	Critical	Ineligible
Domain	community.topcoder.com	Critical	Ineligible
Domain	community-app.topcoder.com	Critical	Ineligible
Domain	connect.topcoder.com	Critical	Ineligible
Domain	crowdsourcing.topcoder.com	Critical	Ineligible
Domain	dashboards.topcoder.com	Critical	Ineligible
Domain	demo.topcoder.com	Critical	Ineligible
Domain	dev1.topcoder.com	Critical	Ineligible
Domain	dna.topcoder.com	Critical	Ineligible
Domain	enterprise.topcoder.com	Critical	Ineligible
Domain	facedetection.topcoder.com	Critical	Ineligible
Domain	faceid.topcoder.com	Critical	Ineligible
Domain	feeds.topcoder.com	Critical	Ineligible
Domain	forums.topcoder.com	Critical	Ineligible
Domain	hfgeoloc.topcoder.com	Critical	Ineligible
Domain	idolondemand.topcoder.com	Critical	Ineligible
Domain	innovation.topcoder.com	Critical	Ineligible
Domain	ios.topcoder.com	Critical	Ineligible
Domain	lauscher.topcoder.com	Critical	Ineligible

Domain	leaderboards.topcoder.com	Critical	Ineligible
Domain	members.topcoder.com	Critical	Ineligible
Domain	morgoth.topcoder.com	Critical	Ineligible
Domain	namedentity.topcoder.com	Critical	Ineligible
Domain	pam-wind-dash.topcoder.com	Critical	Ineligible
Domain	pins-dash.topcoder.com	Critical	Ineligible
Domain	quantum.topcoder.com	Critical	Ineligible
Domain	radiological.topcoder.com	Critical	Ineligible
Domain	ragnar.topcoder.com	Critical	Ineligible
Domain	scavengerhunt.topcoder.com	Critical	Ineligible
Domain	software.topcoder.com	Critical	Ineligible
Domain	solutions.topcoder.com	Critical	Ineligible
Domain	spacenet.topcoder.com	Critical	Ineligible
Domain	tco18.topcoder.com	Critical	Ineligible
Domain	tco19.topcoder.com	Critical	Ineligible
Domain	textsummarization.topcoder.com	Critical	Ineligible
Domain	veterans.topcoder.com	Critical	Ineligible
Domain	vpn.topcoder.com	Critical	Ineligible
Domain	webhooks.topcoder.com	Critical	Ineligible
Domain	wordpress.topcoder.com	Critical	Ineligible
Domain	wordpress-move.topcoder.com	Critical	Ineligible
Domain	x.topcoder.com	Critical	Ineligible
Domain	zurich.topcoder.com	Critical	Ineligible
Domain	accounts.topcoder.com	Critical	Ineligible
Domain	app.topcoder.com	Critical	Ineligible
Domain	apps.topcoder.com	Critical	Ineligible

Out of Scope Domains

	Out Of Scope Out of Scope:
Other	• admin.topcoder.com • api-work.topcoder.com • dev.arena.topcoder.com • qa.arena.topcoder.com • arenaws.topcoder.com • asteroids.topcoder.com • beta.topcoder.com • beta-community-app.topcoder.com • blitz.topcoder.com • bluehost.topcoder.com • bluehost-test01.topcoder.com • bluehost-test02.topcoder.com • cmap-leaders.topcoder.com • coder.topcoder.com • codeyourwayin.topcoder.com • dtn.topcoder.com • epa.topcoder.com • epa.topcoder.com • hphaven.topcoder.com • ideas.topcoder.com • info.topcoder.com • internal-api.topcoder.com • jp.topcoder.com • lightning.topcoder.com • link.topcoder.com • mediasharedev.topcoder.com • mediasharepoc.topcoder.com • mobile.topcoder.com • predix.topcoder.com • qa.topcoder.com • software.qa.topcoder.com • studio.qa.topcoder.com • site.topcoder.com • smtp.topcoder.com • swift.topcoder.com • talk.topcoder.com • tcdev1.topcoder.com • tcdev3.topcoder.com • topgear.topcoder.com • training.topcoder.com • tunnel1.topcoder.com • vorbote.topcoder.com • wiki.topcoder.com

Out of Scope

Out of scope vulnerabilities

When reporting vulnerabilities, please consider (1) attack scenario / exploitability, and (2) security impact of the bug.

The following issues are considered out of scope:

- Known issues of JBOSS Version
- Known issues JWT Tokens still valid after log out
- Clickjacking on pages with no sensitive actions
- Cross-Site Request Forgery (CSRF) on unauthenticated forms or forms with no sensitive actions
- Attacks requiring MITM or physical access to a user's device.
- Previously known vulnerable libraries without a working Proof of Concept.
- Comma Separated Values (CSV) injection without demonstrating a vulnerability.
- Missing best practices in SSL/TLS configuration.
- Any activity that could lead to the disruption of our service (DoS).
- Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS
- Rate limiting or bruteforce issues on non-authentication endpoints
- Missing best practices in Content Security Policy.
- Missing HttpOnly or Secure flags on cookies
- Missing email best practices (Invalid, incomplete or missing SPF/DKIM/DMARC records, etc.)
- Vulnerabilities only affecting users of outdated or unpatched browsers [Less than 2 stable versions behind the latest released stable version]
- Software version disclosure / Banner identification issues / Descriptive error messages or headers (e.g. stack traces, application or server errors).
- Tabnabbing
- Open redirect - unless an additional security impact can be demonstrated
- Issues that require unlikely user interaction

Information Gathering

- Information collection is an important element of penetration testing since it allows you to learn more about the target. We use tools like zap, burp suite, netsparker, and others to gather data.
- The collection of information phase is used to uncover potential system vulnerabilities, which is then followed by the exploitation phase, in which the vulnerabilities are attempted to be exploited in order to get access to the system.
- There are two types of information gathering.

I. Collecting network data

Such include network hosts, public and private IP blocks, routing tables, TCP and UDP operating services, SSL certificates, open ports, and more.

II. Collecting system-related information

User enumeration, system groups, OS hostnames, OS system type (perhaps via fingerprinting), system banners, and so on are all part of this.

- We can collect data through active and passive scanning. To find possible vulnerabilities, Active scan employs known attacks against the targeted targets. Passive scanning is a vulnerability discovery method that relies on data collected from a target machine's network without requiring direct engagement. For this web audit, I used passive scan.

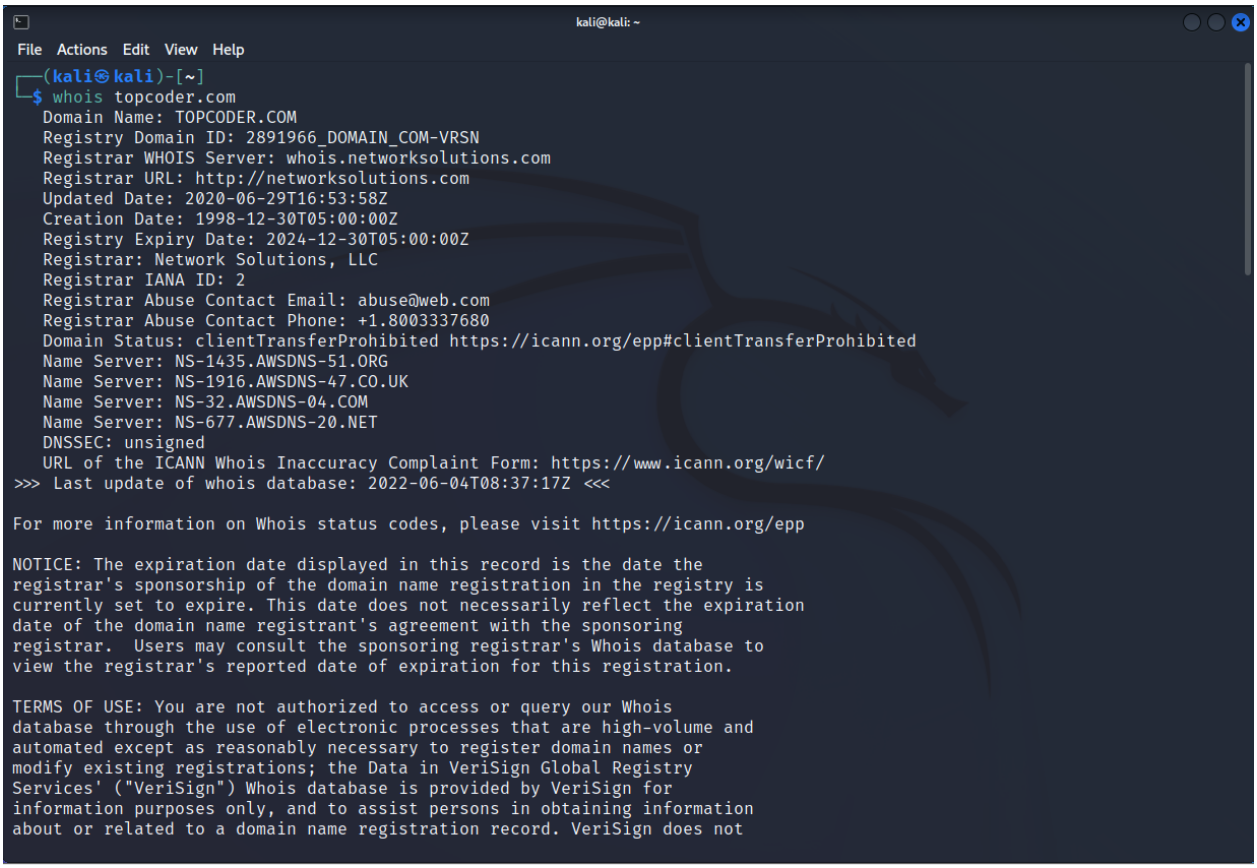
Automated testing

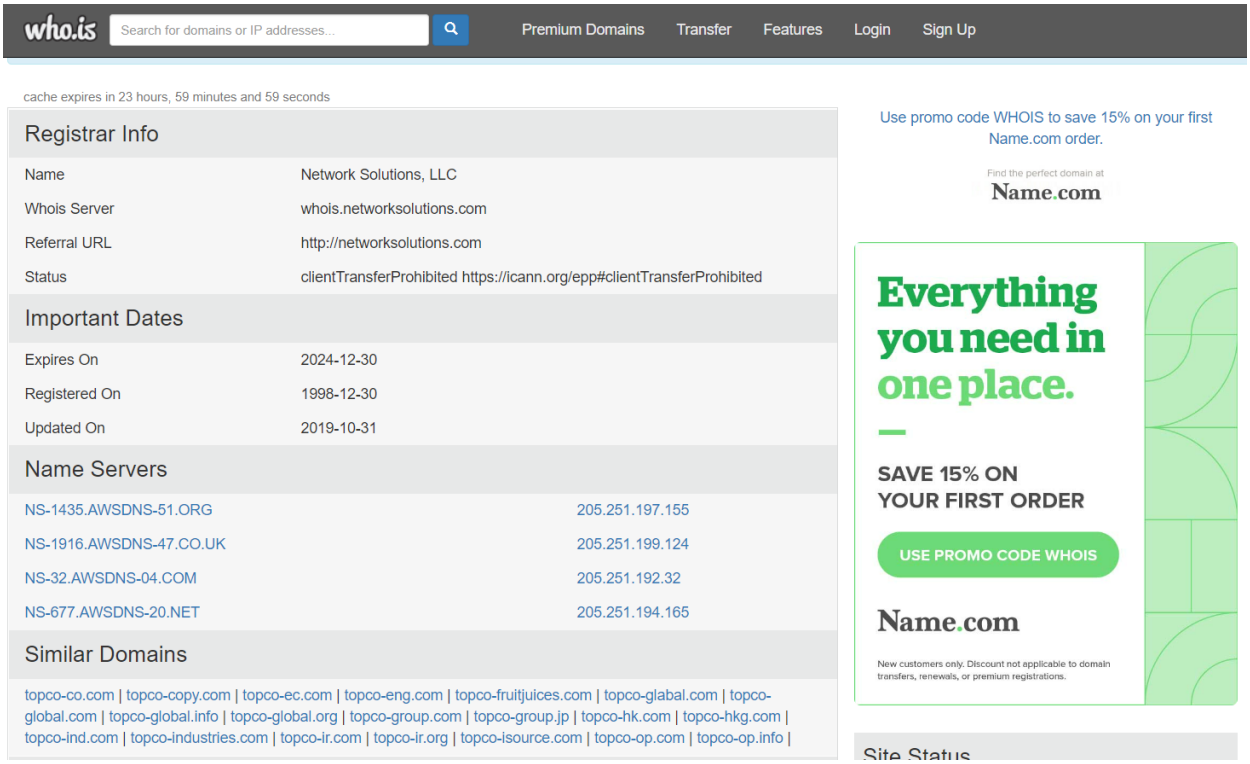
Passive scan

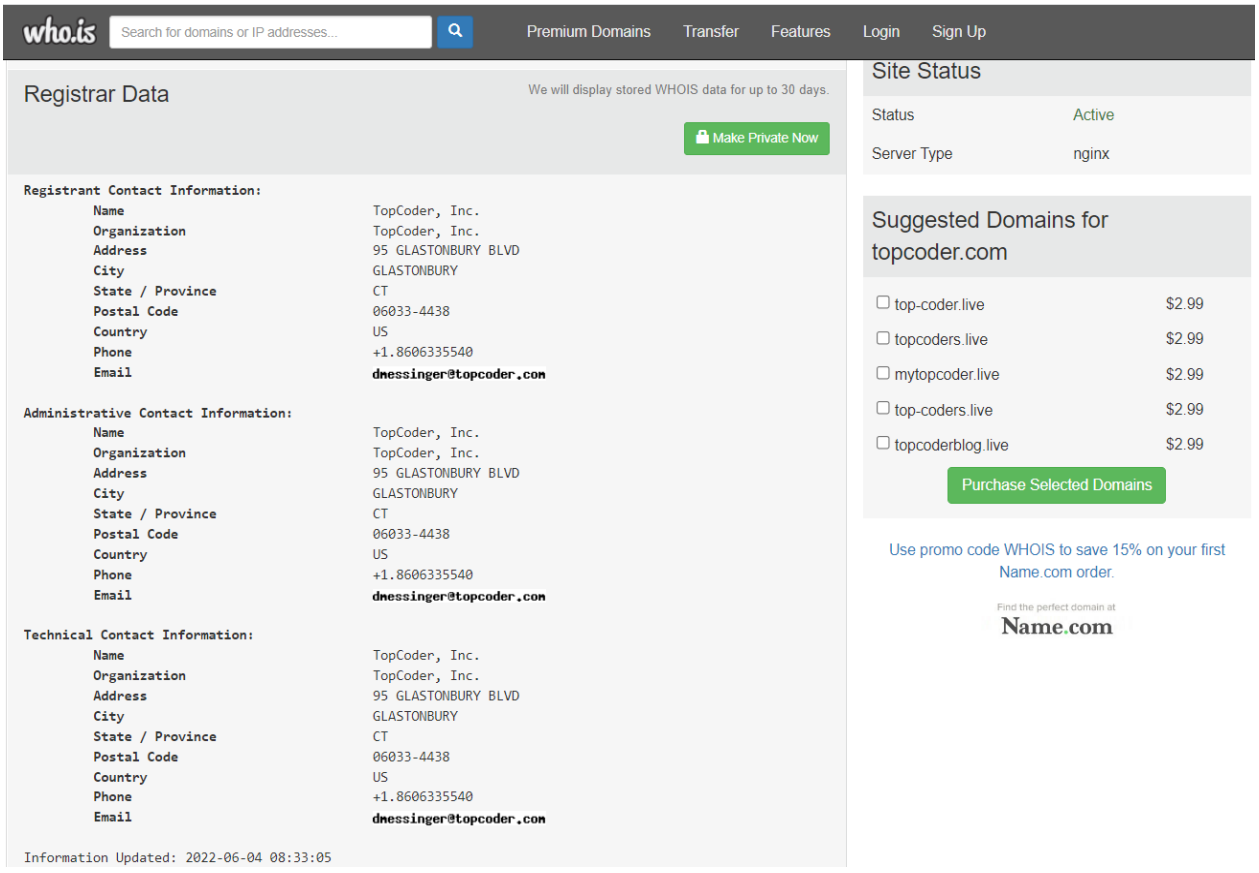
1. Target validation

The hackerone platform provided us with the vulnerability disclosure for topcoder.com in this case, and target validation is the first step in moving forward with the scope provided by the customer. As a result, we may be confident that the website we're looking at is part of the project's scope. We'll use a range of resources to accomplish this.

To learn more about https://www.topcoder.com, I use whois commands and who.is web application. Using this, we can determine whether the targeting domain is valid or not.




who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
cache expires in 23 hours, 59 minutes and 59 seconds
Registrar Info
Name
Network Solutions, LLC
Whois Server
whois.networksolutions.com
Referral URL
http://networksolutions.com
Status
clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Important Dates
Expires On
2024-12-30
Registered On
1998-12-30
Updated On
2019-10-31
Name Servers
NS-1435.AWSDNS-51.ORG
205.251.197.155
NS-1916.AWSDNS-47.CO.UK
205.251.199.124
NS-32.AWSDNS-04.COM
205.251.192.32
NS-677.AWSDNS-20.NET
205.251.194.165
Similar Domains
topco-co.com | topco-copy.com | topco-ec.com | topco-eng.com | topco-fruitjuices.com | topco-glabal.com | topco-global.com | topco-global.info | topco-global.org | topco-group.com | topco-group.jp | topco-hk.com | topco-hkg.com | topco-ind.com | topco-industries.com | topco-ir.com | topco-ir.org | topco-isource.com | topco-op.com | topco-op.info |
Use promo code WHOIS to save 15% on your first Name.com order.
Find the perfect domain at
Name.com
Everything you need in one place.
SAVE 15% ON YOUR FIRST ORDER
USE PROMO CODE WHOIS
Name.com
New customers only. Discount not applicable to domain transfers, renewals, or premium registrations.
Site Status


who.is
Search for domains or IP addresses...
Premium Domains
Transfer
Features
Login
Sign Up
Registrar Data
We will display stored WHOIS data for up to 30 days.
Make Private Now
Registrant Contact Information:
Name TopCoder, Inc.
Organization TopCoder, Inc.
Address 95 GLASTONBURY BLVD
City GLASTONBURY
State / Province CT
Postal Code 06033-4438
Country US
Phone +1.8606335540
Email dmessinger@topcoder.com
Administrative Contact Information:
Name TopCoder, Inc.
Organization TopCoder, Inc.
Address 95 GLASTONBURY BLVD
City GLASTONBURY
State / Province CT
Postal Code 06033-4438
Country US
Phone +1.8606335540
Email dmessinger@topcoder.com
Technical Contact Information:
Name TopCoder, Inc.
Organization TopCoder, Inc.
Address 95 GLASTONBURY BLVD
City GLASTONBURY
State / Province CT
Postal Code 06033-4438
Country US
Phone +1.8606335540
Email dmessinger@topcoder.com
Information Updated: 2022-06-04 08:33:05
Site Status
Status Active
Server Type nginx
Suggested Domains for topcoder.com
top-coder.live $2.99
topcoders.live $2.99
mytopcoder.live $2.99
top-coders.live $2.99
topcoderblog.live $2.99
Purchase Selected Domains
Use promo code WHOIS to save 15% on your first Name.com order.
Find the perfect domain at
Name.com

2.Find subdomains

Identifying subdomains is an element of the collection of information. We can identify the subdomains with the help of several tools.

1. Sublist3r
2. Subfinder
3. Recon –ng Tools
4. SubDomainizer
5. Crt.sh tool

Sublist3r

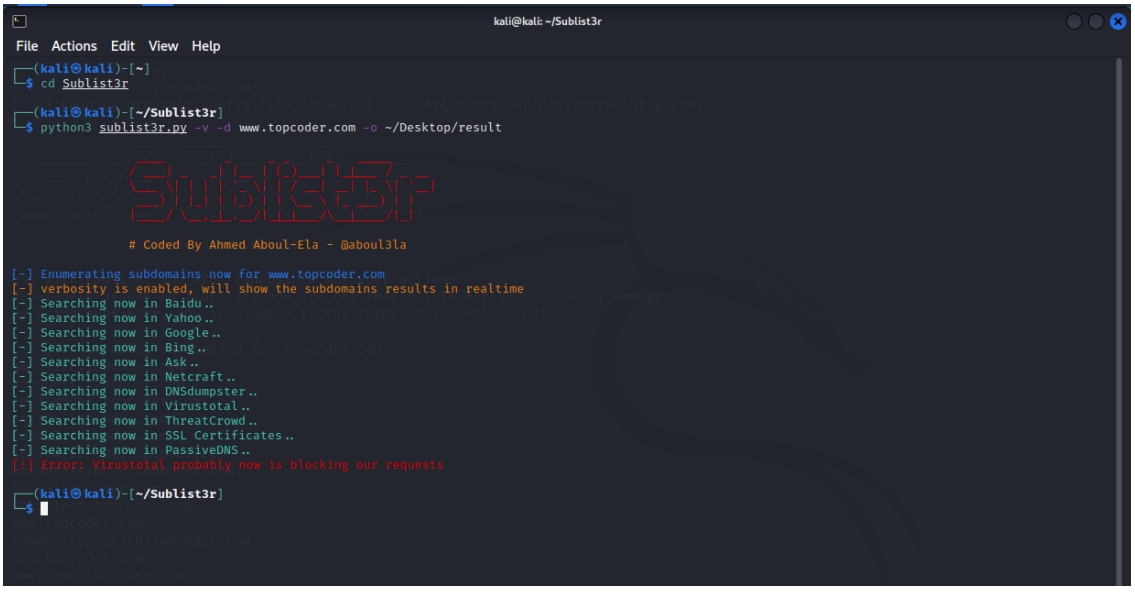
Sublist3r is a python utility that uses OSINT to enumerate website subdomains. It assists penetration testers and bug hunters in gathering and collecting subdomains for the site they are targeting. Sublist3r uses a variety of search engines to find subdomains, including Google, Yahoo, Bing, Baidu, and Ask. Sublist3r also uses Netcraft, Virustotal, ThreatCrowd, DNSdumpster, and ReverseDNS to find subdomains.

- We can Sublist3r install on kali Linux using this command.

  "git clone https://github.com/aboul3la/Sublist3r.git"

- After installing, type this command to scan target domain.

  "python3 sublist3r.py -v -d topcoder.com -o ~/Desktop/result"



We can't use Sublist3r for topecoder.com subdomain scanning. Because Virustotal probably now is blocking our requests

Subfinder

Subfinder is a subdomain discovery tool that uses passive online sources to find acceptable subdomains for websites. It has a simple modular architecture and is optimized for speed. subfinder is built for doing one thing only - passive subdomain enumeration, and it does that very well.

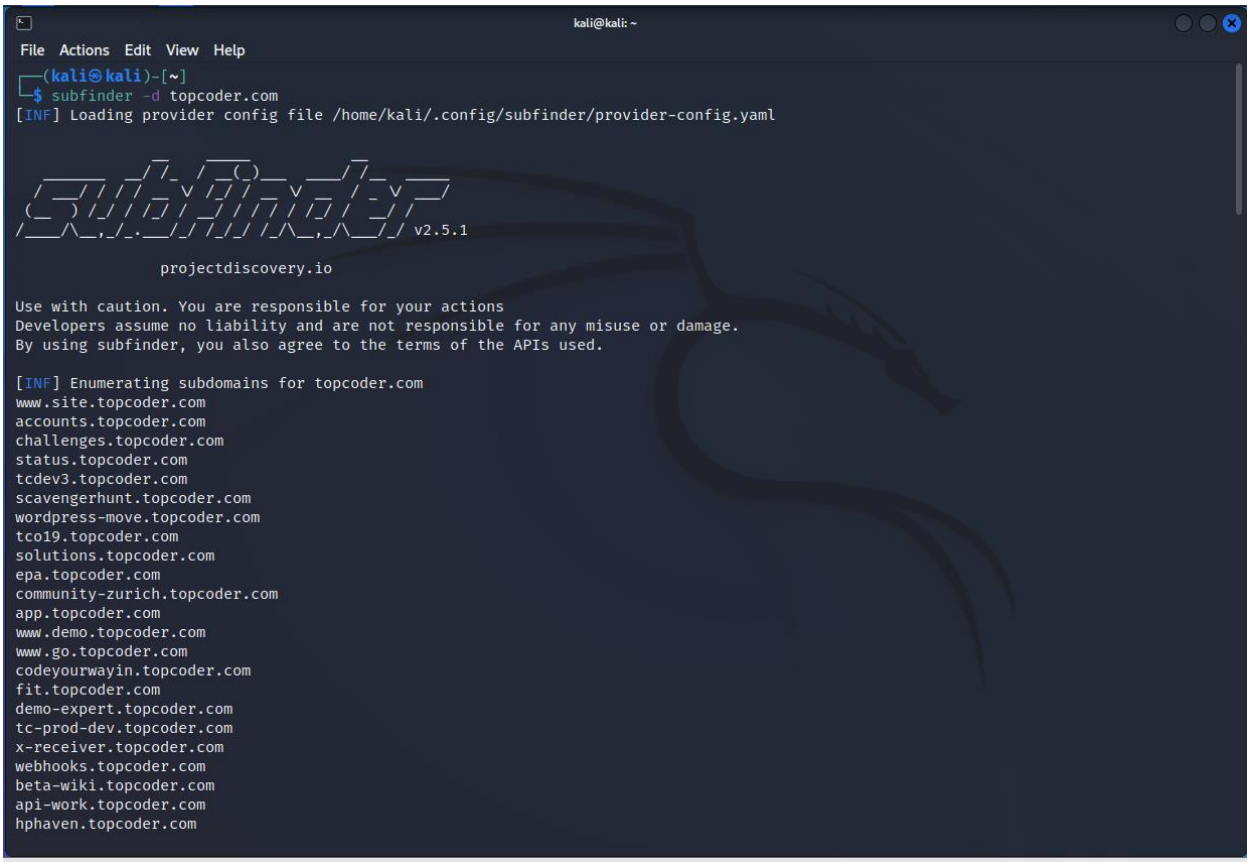
- Installation

  Subfinder requires **go language** to install successfully. Run the following command to install

  "go install -v github.com/projectdiscovery/subfinder/v2/cmd/subfinder@latest"

- After installing, type this command to scan target domain.

  "subfinder -d topcoder.com"



After scanning this domain, we can able to find 184 subdomains.

www.site.topcoder.com	beta.topcoder.com
accounts.topcoder.com	tco10.topcoder.com
challenges.topcoder.com	apiservices.topcoder.com
status.topcoder.com	tco17.topcoder.com
tcdev3.topcoder.com	connect.topcoder.com
scavengerhunt.topcoder.com	tco20.topcoder.com
wordpress-move.topcoder.com	training.topcoder.com
tco19.topcoder.com	iot.topcoder.com
solutions.topcoder.com	enterprise.topcoder.com
epa.topcoder.com	site.topcoder.com
community-zurich.topcoder.com	comcast.topcoder.com
app.topcoder.com	wordpress.topcoder.com
www.demo.topcoder.com	lp.topcoder.com
www.go.topcoder.com	taascalc.topcoder.com
codeyourwayin.topcoder.com	pins-dash.topcoder.com
fit.topcoder.com	morgoth.topcoder.com
demo-expert.topcoder.com	tco04.topcoder.com
tc-prod-dev.topcoder.com	smtp01.qa.topcoder.com
x-receiver.topcoder.com	studio.topcoder.com
webhooks.topcoder.com	dashboards.topcoder.com
beta-wiki.topcoder.com	dna.topcoder.com
api-work.topcoder.com	bluehost-test02.topcoder.com
hphaven.topcoder.com	hello.topcoder.com
cshelp.topcoder.com	tco02.topcoder.com
asteroids.topcoder.com	beta-community-app.topcoder.com
mediasharepoc.topcoder.com	lightning.topcoder.com
tco15.topcoder.com	analytics.topcoder.com
mediasharedev.topcoder.com	staging-community-app.topcoder.com
hfgeoloc.topcoder.com	forums.topcoder.com
blitz.topcoder.com	arenaws.topcoder.com
internal-api.topcoder.com	qa.topcoder.com
submission-review-api.topcoder.com	idolondemand.topcoder.com
submission-review.topcoder.com	help.topcoder.com
rdm-leaderboard.topcoder.com	ideas.topcoder.com
connect-auth0.topcoder.com	vorbote.topcoder.com
mailer.topcoder.com	community.topcoder.com
cognitive.topcoder.com	tco03.topcoder.com
blockchain.topcoder.com	tccindia15.topcoder.com
leaderboards.topcoder.com	payment.topcoder.com
dev.topcoder.com	tco11.topcoder.com
lauscher.topcoder.com	prod-hub02.corp.topcoder.com
mm.topcoder.com	innovation.topcoder.com
dtn.topcoder.com	dpeak-dash.topcoder.com
tco12.topcoder.com	qa.arena.topcoder.com
techapp.topcoder.com	fs.topcoder.com
cs.topcoder.com	link.topcoder.com

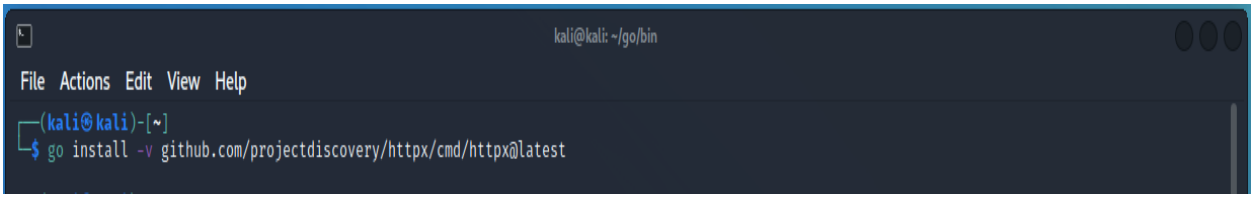
spacenet2.topcoder.com	ios.topcoder.com
cat.topcoder.com	tcwiki.topcoder.com
admin.topcoder.com	auth.topcoder.com
bluehost-test01.topcoder.com	www.bluehost-test02.topcoder.com
cmap-leaders.topcoder.com	www.topcoder.com
nist.topcoder.com	iarpa3dchallenge.topcoder.com
spacenet.topcoder.com	jp.topcoder.com
talk.topcoder.com	tco16.topcoder.com
smtp.topcoder.com	software.qa.topcoder.com
tunnel1.topcoder.com	namedentity.topcoder.com
coder.topcoder.com	mm111.topcoder.com
ragnar.topcoder.com	topcoder.com
demo.topcoder.com	tco09.topcoder.com
feeds.topcoder.com	platform.topcoder.com
smtp01.topcoder.com	vpn.topcoder.com
tco21.topcoder.com	facedetection.topcoder.com
marketing2.topcoder.com	autodiscover.topcoder.com
apimail.topcoder.com	quantum.topcoder.com
community-app-cdn.topcoder.com	www.bluehost.topcoder.com
arena.topcoder.com	topgear.topcoder.com
www.bluehost-test01.topcoder.com	apps.topcoder.com
www.help.topcoder.com	gateway.poseidon.topcoder.com
marketing3.topcoder.com	cmap.topcoder.com
wipro.topcoder.com	accounts-auth0.topcoder.com
discussions.topcoder.com	dev1.topcoder.com
internal-mm-leaderboard.topcoder.com	success.topcoder.com
mail.topcoder.com	checkmarx.topcoder.com
bluehost.topcoder.com	connectv2.topcoder.com
faceid.topcoder.com	tco14.topcoder.com
challenge-comparison.topcoder.com	tco07.topcoder.com
connectv1.topcoder.com	x.topcoder.com
tco22.topcoder.com	crowdsourcing.topcoder.com
swift.topcoder.com	tco13.topcoder.com
api.topcoder.com	tco08.topcoder.com
bugzilla.topcoder.com	studio.qa.topcoder.com
wiki.topcoder.com	spacenet7.topcoder.com
tco05.topcoder.com	robots.topcoder.com
mailccr.corp.topcoder.com	zurich.topcoder.com
veterans.topcoder.com	tcdev1.topcoder.com
community-app.topcoder.com	info.topcoder.com
go.topcoder.com	pam-wind-dash.topcoder.com
textsummarization.topcoder.com	software.topcoder.com
tc-public-static-files.topcoder.com	members.topcoder.com
mobile.topcoder.com	predix.topcoder.com
tco18.topcoder.com	solarsystems.topcoder.com
radiological.topcoder.com	tunnel2.topcoder.com

Before select subdomains we need to verify these subdomains are alive subdomains. Then we select tool for find alive subdomain. Tool name is **httpx**

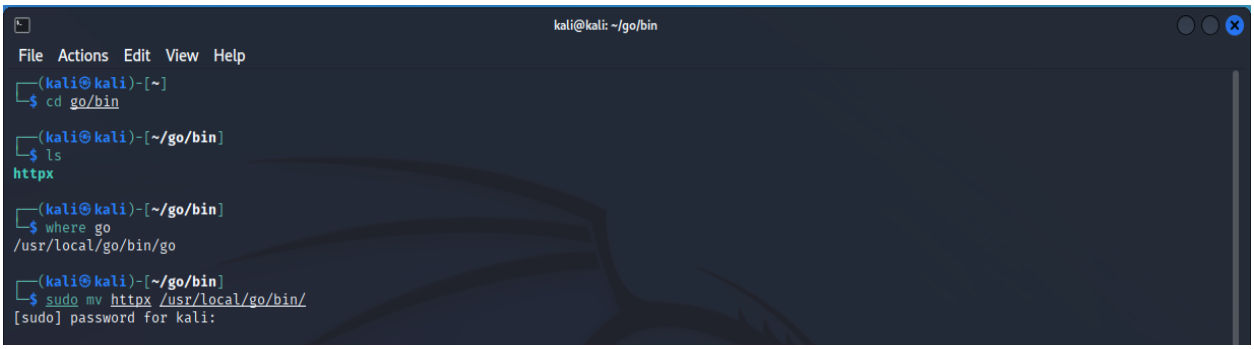
httpx

- Run the following command to install httpx

  "go install -v github.com/projectdiscovery/httpx/cmd/httpx@latest"

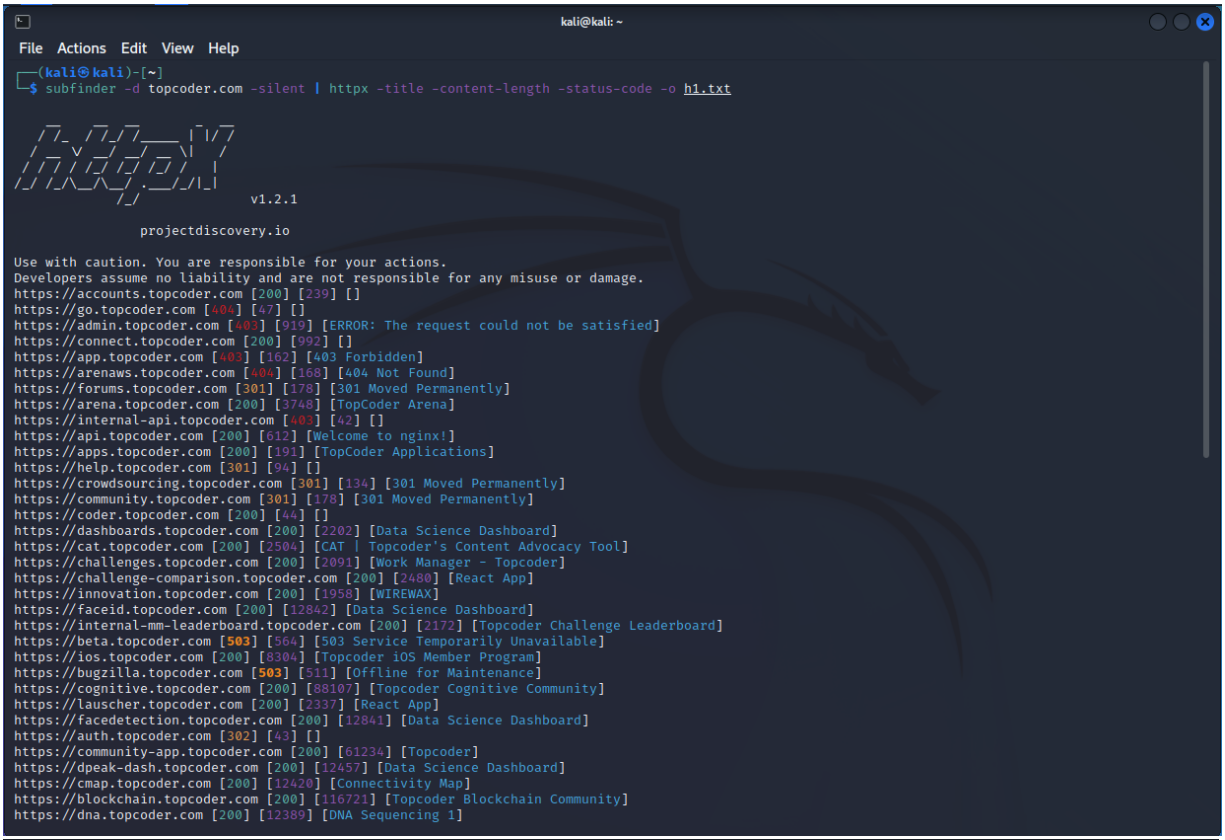


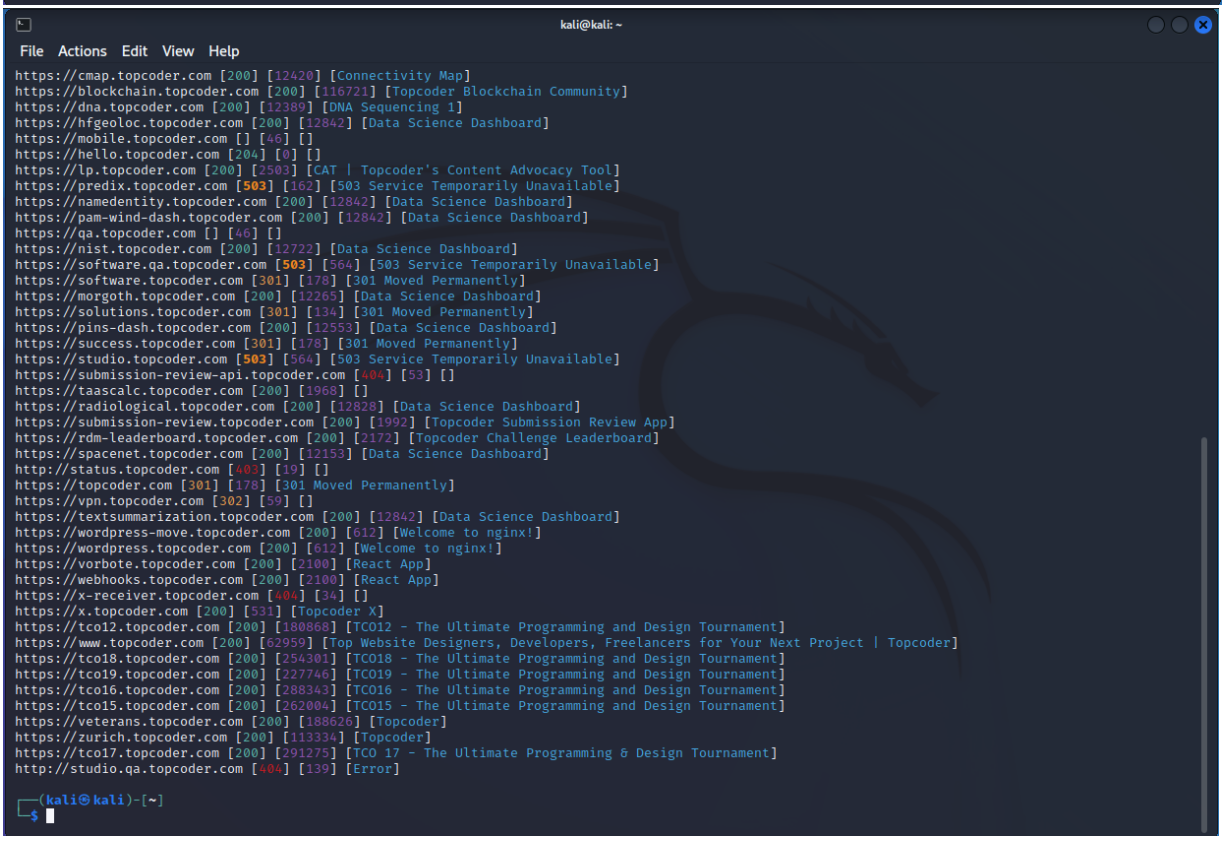
- then change the path httpx tool. That was usefull to run this tool anywhere



- then run httpx tool with using Subfinder output.

  "subfinder -d topcoder.com -silent | httpx -title -content-length -status-code -o h1.txt"


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ subfinder -d topcoder.com -silent | httpx -title -content-length -status-code -o h1.txt
v1.2.1
projectdiscovery.io
Use with caution. You are responsible for your actions.
Developers assume no liability and are not responsible for any misuse or damage.
https://accounts.topcoder.com [200] [239] []
https://go.topcoder.com [404] [47] []
https://admin.topcoder.com [403] [919] [ERROR: The request could not be satisfied]
https://connect.topcoder.com [200] [992] []
https://app.topcoder.com [403] [162] [403 Forbidden]
https://arenaws.topcoder.com [404] [168] [404 Not Found]
https://forums.topcoder.com [301] [178] [301 Moved Permanently]
https://arena.topcoder.com [200] [3748] [TopCoder Arena]
https://internal-api.topcoder.com [403] [42] []
https://api.topcoder.com [200] [612] [Welcome to nginx!]
https://apps.topcoder.com [200] [191] [TopCoder Applications]
https://help.topcoder.com [301] [94] []
https://crowdsourcing.topcoder.com [301] [134] [301 Moved Permanently]
https://community.topcoder.com [301] [178] [301 Moved Permanently]
https://coder.topcoder.com [200] [44] []
https://dashboards.topcoder.com [200] [2202] [Data Science Dashboard]
https://cat.topcoder.com [200] [2504] [CAT | Topcoder's Content Advocacy Tool]
https://challenges.topcoder.com [200] [2091] [Work Manager - Topcoder]
https://challenge-comparison.topcoder.com [200] [2480] [React App]
https://innovation.topcoder.com [200] [1958] [WIREWAX]
https://faceid.topcoder.com [200] [12842] [Data Science Dashboard]
https://internal-mm-leaderboard.topcoder.com [200] [2172] [Topcoder Challenge Leaderboard]
https://beta.topcoder.com [503] [564] [503 Service Temporarily Unavailable]
https://ios.topcoder.com [200] [8304] [Topcoder iOS Member Program]
https://bugzilla.topcoder.com [503] [511] [Offline for Maintenance]
https://cognitive.topcoder.com [200] [88107] [Topcoder Cognitive Community]
https://lauscher.topcoder.com [200] [2337] [React App]
https://facedetection.topcoder.com [200] [12841] [Data Science Dashboard]
https://auth.topcoder.com [302] [43] []
https://community-app.topcoder.com [200] [61234] [Topcoder]
https://dpeak-dash.topcoder.com [200] [12457] [Data Science Dashboard]
https://cmap.topcoder.com [200] [12420] [Connectivity Map]
https://blockchain.topcoder.com [200] [116721] [Topcoder Blockchain Community]
https://dna.topcoder.com [200] [12389] [DNA Sequencing 1]


kali@kali: ~
File Actions Edit View Help
https://cmap.topcoder.com [200] [12420] [Connectivity Map]
https://blockchain.topcoder.com [200] [116721] [Topcoder Blockchain Community]
https://dna.topcoder.com [200] [12389] [DNA Sequencing 1]
https://hfgeoloc.topcoder.com [200] [12842] [Data Science Dashboard]
https://mobile.topcoder.com [] [46] []
https://hello.topcoder.com [204] [0] []
https://lp.topcoder.com [200] [2503] [CAT | Topcoder's Content Advocacy Tool]
https://predix.topcoder.com [503] [162] [503 Service Temporarily Unavailable]
https://namedentity.topcoder.com [200] [12842] [Data Science Dashboard]
https://pam-wind-dash.topcoder.com [200] [12842] [Data Science Dashboard]
https://qa.topcoder.com [] [46] []
https://nist.topcoder.com [200] [12722] [Data Science Dashboard]
https://software.qa.topcoder.com [503] [564] [503 Service Temporarily Unavailable]
https://software.topcoder.com [301] [178] [301 Moved Permanently]
https://morgoth.topcoder.com [200] [12265] [Data Science Dashboard]
https://solutions.topcoder.com [301] [134] [301 Moved Permanently]
https://pins-dash.topcoder.com [200] [12553] [Data Science Dashboard]
https://success.topcoder.com [301] [178] [301 Moved Permanently]
https://studio.topcoder.com [503] [564] [503 Service Temporarily Unavailable]
https://submission-review-api.topcoder.com [404] [53] []
https://taascalc.topcoder.com [200] [1968] []
https://radiological.topcoder.com [200] [12828] [Data Science Dashboard]
https://submission-review.topcoder.com [200] [1992] [Topcoder Submission Review App]
https://rdm-leaderboard.topcoder.com [200] [2172] [Topcoder Challenge Leaderboard]
https://spacenet.topcoder.com [200] [12153] [Data Science Dashboard]
http://status.topcoder.com [403] [19] []
https://topcoder.com [301] [178] [301 Moved Permanently]
https://vpn.topcoder.com [302] [59] []
https://textsummarization.topcoder.com [200] [12842] [Data Science Dashboard]
https://wordpress-move.topcoder.com [200] [612] [Welcome to nginx!]
https://wordpress.topcoder.com [200] [612] [Welcome to nginx!]
https://vorbote.topcoder.com [200] [2100] [React App]
https://webhooks.topcoder.com [200] [2100] [React App]
https://x-receiver.topcoder.com [404] [34] []
https://x.topcoder.com [200] [531] [Topcoder X]
https://tco12.topcoder.com [200] [180868] [TCO12 - The Ultimate Programming and Design Tournament]
https://www.topcoder.com [200] [62959] [Top Website Designers, Developers, Freelancers for Your Next Project | Topcoder]
https://tco18.topcoder.com [200] [254301] [TCO18 - The Ultimate Programming and Design Tournament]
https://tco19.topcoder.com [200] [227746] [TCO19 - The Ultimate Programming and Design Tournament]
https://tco16.topcoder.com [200] [288343] [TCO16 - The Ultimate Programming and Design Tournament]
https://tco15.topcoder.com [200] [262004] [TCO15 - The Ultimate Programming and Design Tournament]
https://veterans.topcoder.com [200] [188626] [Topcoder]
https://zurich.topcoder.com [200] [113334] [Topcoder]
https://tco17.topcoder.com [200] [291275] [TCO 17 - The Ultimate Programming & Design Tournament]
http://studio.qa.topcoder.com [404] [139] [Error]
(kali㉿kali)-[~]
$

https://accounts.topcoder.com [200] [239] []

https://go.topcoder.com [404] [47] []

https://admin.topcoder.com [403] [919] [ERROR: The request could not be satisfied]

https://connect.topcoder.com [200] [992] []

https://app.topcoder.com [403] [162] [403 Forbidden]

https://arenaws.topcoder.com [404] [168] [404 Not Found]

https://forums.topcoder.com [301] [178] [301 Moved Permanently]

https://arena.topcoder.com [200] [3748] [TopCoder Arena]

https://internal-api.topcoder.com [403] [42] []

https://api.topcoder.com [200] [612] [Welcome to nginx!]

https://apps.topcoder.com [200] [191] [TopCoder Applications]

https://help.topcoder.com [301] [94] []

https://crowdsourcing.topcoder.com [301] [134] [301 Moved Permanently]

https://community.topcoder.com [301] [178] [301 Moved Permanently]

https://coder.topcoder.com [200] [44] []

https://dashboards.topcoder.com [200] [2202] [Data Science Dashboard]

https://cat.topcoder.com [200] [2504] [CAT | Topcoder's Content Advocacy Tool]

https://challenges.topcoder.com [200] [2091] [Work Manager - Topcoder]

https://challenge-comparison.topcoder.com [200] [2480] [React App]

https://innovation.topcoder.com [200] [1958] [WIREWAX]

https://faceid.topcoder.com [200] [12842] [Data Science Dashboard]

https://internal-mm-leaderboard.topcoder.com [200] [2172] [Topcoder Challenge Leaderboard]

https://beta.topcoder.com [503] [564] [503 Service Temporarily Unavailable]

https://ios.topcoder.com [200] [8304] [Topcoder iOS Member Program]

https://bugzilla.topcoder.com [503] [511] [Offline for Maintenance]

https://cognitive.topcoder.com [200] [88107] [Topcoder Cognitive Community]

https://lauscher.topcoder.com [200] [2337] [React App]

https://facedetection.topcoder.com [200] [12841] [Data Science Dashboard]

https://auth.topcoder.com [302] [43] []

https://community-app.topcoder.com [200] [61234] [Topcoder]

https://dpeak-dash.topcoder.com [200] [12457] [Data Science Dashboard]

https://cmap.topcoder.com [200] [12420] [Connectivity Map]

https://blockchain.topcoder.com [200] [116721] [Topcoder Blockchain Community]

https://dna.topcoder.com [200] [12389] [DNA Sequencing 1]

https://hfgeoloc.topcoder.com [200] [12842] [Data Science Dashboard]

https://mobile.topcoder.com [] [46] []

https://hello.topcoder.com [204] [0] []

https://lp.topcoder.com [200] [2503] [CAT | Topcoder's Content Advocacy Tool]

https://predix.topcoder.com [503] [162] [503 Service Temporarily Unavailable]

https://namedentity.topcoder.com [200] [12842] [Data Science Dashboard]

https://pam-wind-dash.topcoder.com [200] [12842] [Data Science Dashboard]

https://qa.topcoder.com [] [46] []

https://nist.topcoder.com [200] [12722] [Data Science Dashboard]

https://software.qa.topcoder.com [503] [564] [503 Service Temporarily Unavailable]

https://software.topcoder.com [301] [178] [301 Moved Permanently]

https://morgoth.topcoder.com [200] [12265] [Data Science Dashboard]

https://solutions.topcoder.com [301] [134] [301 Moved Permanently]

https://pins-dash.topcoder.com [200] [12553] [Data Science Dashboard]

https://success.topcoder.com [301] [178] [301 Moved Permanently]

https://studio.topcoder.com [503] [564] [503 Service Temporarily Unavailable]

https://submission-review-api.topcoder.com [404] [53] []

https://taascalc.topcoder.com [200] [1968] []

https://radiological.topcoder.com [200] [12828] [Data Science Dashboard]

https://submission-review.topcoder.com [200] [1992] [Topcoder Submission Review App]

https://rdm-leaderboard.topcoder.com [200] [2172] [Topcoder Challenge Leaderboard]

https://spacenet.topcoder.com [200] [12153] [Data Science Dashboard]

http://status.topcoder.com [403] [19] []

https://topcoder.com [301] [178] [301 Moved Permanently]

https://vpn.topcoder.com [302] [59] []

https://textsummarization.topcoder.com [200] [12842] [Data Science Dashboard]

https://wordpress-move.topcoder.com [200] [612] [Welcome to nginx!]

https://wordpress.topcoder.com [200] [612] [Welcome to nginx!]

https://vorbote.topcoder.com [200] [2100] [React App]

https://webhooks.topcoder.com [200] [2100] [React App]

https://x-receiver.topcoder.com [404] [34] []

https://x.topcoder.com [200] [531] [Topcoder X]

https://tco12.topcoder.com [200] [180868] [TCO12 - The Ultimate Programming and Design Tournament]

https://www.topcoder.com [200] [62959] [Top Website Designers, Developers, Freelancers for Your Next Project | Topcoder]

https://tco18.topcoder.com [200] [254301] [TCO18 - The Ultimate Programming and Design Tournament]

https://tco19.topcoder.com [200] [227746] [TCO19 - The Ultimate Programming and Design Tournament]

https://tco16.topcoder.com [200] [288343] [TCO16 - The Ultimate Programming and Design Tournament]

https://tco15.topcoder.com [200] [262004] [TCO15 - The Ultimate Programming and Design Tournament]

https://veterans.topcoder.com [200] [188626] [Topcoder]

https://zurich.topcoder.com [200] [113334] [Topcoder]

https://tco17.topcoder.com [200] [291275] [TCO 17 - The Ultimate Programming & Design Tournament]

http://studio.qa.topcoder.com [404] [139] [Error]

Selected Subdomains

www.topcoder.com

www.blockchain.topcoder.com

www.community-app.topcoder.com

www.faceid.topcoder.com

www.morgoth.topcoder.com

Vulnerability scanning

- Vulnerability scanning is the process of finding security vulnerabilities and faults in the systems and software that run on them when it comes to systems and software.
- We can identify the vulnerabilities with the help of several technologies. A vulnerability scanner is a software that identifies all systems connected to a network and creates an inventory of them. It is employed in the detection and prevention of cyber-attacks. In addition, it attempts to establish which operating system is presently running and what software is installed on each device it discovers, as well as other features such as open ports and user accounts.

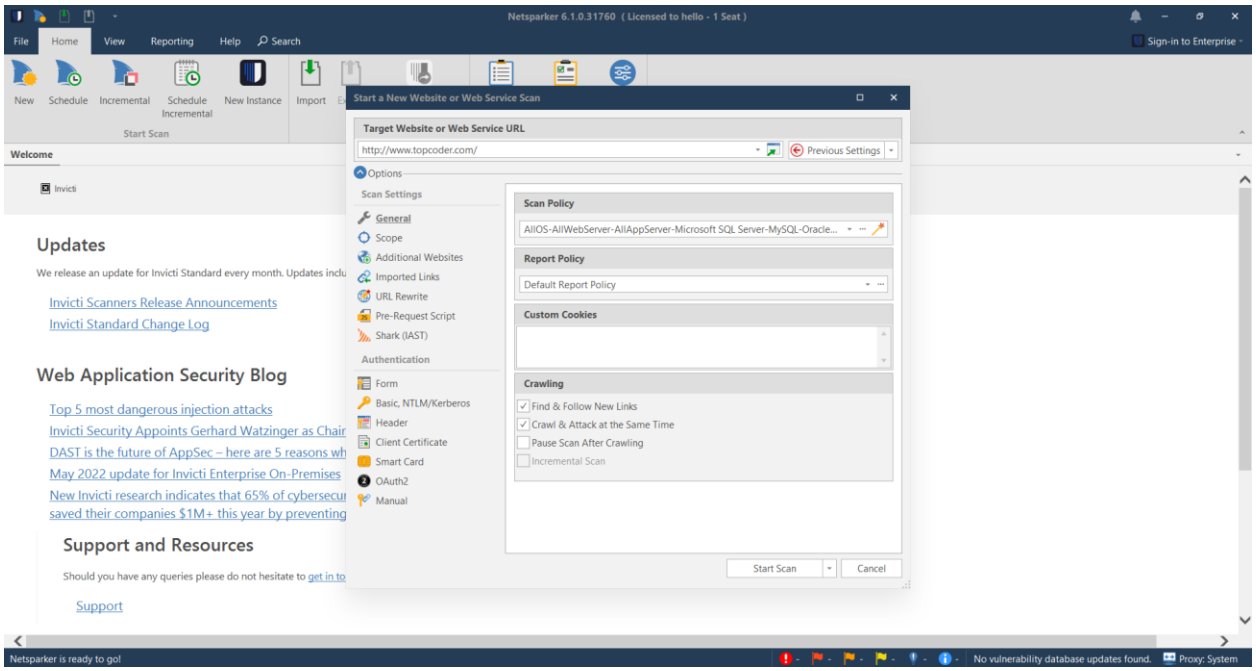
- Tools of scan vulnerabilities.
    1. Netsparker
    2. Nikto
    3. Nmap
    4. owaspZap
    5. Nessus
    6. Legion

Netsparker

- Netsparker is a web application vulnerability scanner that is totally automated. Regardless of platform or programming language, Netsparker can scan any type of online application. It allows you to scan websites, online applications, and web services for security flaws.

How to start scan

Open Netsparker >> go to Home tab >> click New >> paste target domain url >> start scan



www.topcoder.com

http://www.topcoder.com/

Scan Time	6/4/2022 4:16:52 AM (UTC+05:30)
Scan Duration	00:00:51:14
Total Requests	: 32,062
Average Speed	: 10.4r/s

Risk Level:
MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2017 classification.
There are 96 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

80 IDENTIFIED	35 CONFIRMED	0 CRITICAL
0 HIGH	7 MEDIUM	44 LOW
	0 BEST PRACTICE	29 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	7
Low	44
Best Practice	0
Information	29
TOTAL	**80**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	26
Best Practice	0
Information	8
TOTAL	**35**

VULNERABILITY SUMMARY

A3 - SENSITIVE DATA EXPOSURE

	Weak Ciphers Enabled	GET	https://www.topcoder.com/	MEDIUM
	Cookie Not Marked as Secure	GET	https://www.topcoder.com/api/cdn/public/contentful/EDU/master/published/entries?content_type=article&fields.type=Article&limit=4&order=-fields.creationDate&skip=0	LOW
	Cookie Not Marked as Secure	GET	https://www.topcoder.com/api/blog/?category=Community%20Stories&limit=4	LOW
	Cookie Not Marked as Secure	GET	https://www.topcoder.com/api/cdn/public/contentful/default/master/published/entries?content_type=viewport&sys.id=6sjlJHboX3aG3mFS5FnZND	LOW
	Cookie Not Marked as Secure	GET	https://www.topcoder.com/api/recruit/taasjobs?isApplicationPageActive=true&perPage=5&sortBy=createdAt&sortOrder=desc&status=sourcing	LOW
	Cookie Not Marked as Secure	GET	https://www.topcoder.com/api/cdn/public/contentful/default/master/published/entries/5HmoppBlc79RfxOwb8JAls	LOW
	Cookie Not Marked as Secure	GET	https://www.topcoder.com/api/cdn/public/forums/discussions?categoryID=1441	LOW
	Cookie Not Marked as Secure	POST	https://www.topcoder.com/community-app-assets/api/logger	LOW
	Cookie Not Marked as Secure	GET	https://www.topcoder.com/api/recruit/jobs?job_status=1	LOW
	Cookie Not Marked as Secure	GET	https://www.topcoder.com/api/cdn/public/contentful/EDU/master/published/entries/15caxocitaxyK65K9oSd91	LOW
	Cookie Not Marked as Secure	GET	https://www.topcoder.com/api/cdn/public/contentful/EDU/master/published/entries/fExfNMgkaAN9f6RE1II5W	LOW
	Cookie Not Marked as Secure	GET	https://www.topcoder.com/api/cdn/public/contentful/EDU/master/published/entries/2A1VVaGZsR6isWXGwx6j8S	LOW

A6 - SECURITY MISCONFIGURATION

	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://www.topcoder.com/	MEDIUM
	Cookie Not Marked as HttpOnly	GET	https://www.topcoder.com/?s=3	LOW

	Cookie Not Marked as HttpOnly	GET	https://www.topcoder.com/how-it-works/	LOW
	Cookie Not Marked as HttpOnly	GET	https://www.topcoder.com/security/	LOW
	Cookie Not Marked as HttpOnly	GET	https://www.topcoder.com/the-talent/?ref=nav	LOW
	Cookie Not Marked as HttpOnly	GET	https://www.topcoder.com/data-science/	LOW
	Cookie Not Marked as HttpOnly	GET	https://www.topcoder.com/api/cdn/public/contentful/EDU/master/published/entries?content_type=article&fields.type=Article&limit=4&order=-fields.creationDate&skip=0	LOW
	Cookie Not Marked as HttpOnly	GET	https://www.topcoder.com/api/blog/?category=Community%20Stories&limit=4	LOW
	Cookie Not Marked as HttpOnly	GET	https://www.topcoder.com/api/cdn/public/contentful/default/master/published/entries?content_type=viewport&sys.id=6sjlJHboX3aG3mFS5FnZND	LOW
	Cookie Not Marked as HttpOnly	GET	https://www.topcoder.com/api/recruit/taasjobs?isApplicationPageActive=true&perPage=5&sortBy=createdAt&sortOrder=desc&status=sourcing	LOW
	Cookie Not Marked as HttpOnly	GET	https://www.topcoder.com/api/cdn/public/contentful/default/master/published/entries/5HmoppBlc79RfxOwb8JAls	LOW
	Cookie Not Marked as HttpOnly	GET	https://www.topcoder.com/api/cdn/public/forums/discussions?categoryID=1441	LOW

	Insecure Frame (External)	GET	https://www.topcoder.com/?s=3	LOW
	Insecure Frame (External)	GET	https://www.topcoder.com/security/	LOW
	Insecure Frame (External)	GET	https://www.topcoder.com/the-talent/?ref=nav	LOW
	Insecure Frame (External)	GET	https://www.topcoder.com/data-science/	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.topcoder.com/.svn/wc.db	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.topcoder.com/	LOW

	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.topcoder.com/(268409241-40268	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.topcoder.com/.well-known/?nsextt=%0d%0ans%3anetsparker056650%3dvuln	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.topcoder.com/.well-known/(268409241-79828	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.topcoder.com/etc/passwd	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.topcoder.com/.well-known/etc/passwd	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.topcoder.com/etc/passwd	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.topcoder.com/.well-known/apple-app-site-association?hTTp://r87.com/n	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.topcoder.com/.well-known/etc/passwd	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.topcoder.com/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd	LOW
	Misconfigured Access-Control-Allow-Origin Header	GET	https://www.topcoder.com/wp-json/	LOW
	Misconfigured Access-Control-Allow-Origin Header	GET	https://www.topcoder.com/wp-json/wp/	LOW
	Misconfigured Access-Control-Allow-Origin Header	GET	https://www.topcoder.com/wp-json/wp/v2/	LOW
	Misconfigured Access-Control-Allow-Origin Header	GET	https://www.topcoder.com/wp-json/wp/v2/pages/	LOW
	Misconfigured Access-Control-Allow-Origin Header	GET	https://www.topcoder.com/wp-json/wp/v2/pages/46320	LOW
	Misconfigured Access-Control-Allow-Origin Header	GET	https://www.topcoder.com/wp-json/oembed/1.0/	LOW

www.blockchain.topcoder.com

http://blockchain.topcoder.com/

Scan Time	6/4/2022 1:23:12 PM (UTC+05:30)
Scan Duration	00:00:04:47
Total Requests	: 4,155
Average Speed	: 14.5r/s

Risk Level:
MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2017 classification.
There are 79 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

43 IDENTIFIED	34 CONFIRMED	0 CRITICAL
0 HIGH	3 MEDIUM	33 LOW
	0 BEST PRACTICE	7 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	3
Low	33
Best Practice	0
Information	7
TOTAL	**43**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	27
Best Practice	0
Information	6
TOTAL	**34**

VULNERABILITY SUMMARY

A3 - SENSITIVE DATA EXPOSURE

	Weak Ciphers Enabled	GET	https://blockchain.topcoder.com/	MEDIUM
	Insecure HTTP Usage	GET	http://blockchain.topcoder.com/	MEDIUM
	Cookie Not Marked as Secure	GET	https://blockchain.topcoder.com/challenges/sw.js	LOW
	Cookie Not Marked as Secure	POST	https://blockchain.topcoder.com/community-app-assets/api/logger	LOW
	Cookie Not Marked as Secure	GET	https://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/entries?content_type=viewport&fields.name=Blockchain%20Community%20-%20Home	LOW
	Cookie Not Marked as Secure	GET	https://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/entries/6GxdEbhe0MkKkcgUi6eWsW	LOW
	Cookie Not Marked as Secure	GET	https://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/entries/XdBwv6Hsg8euE62E8i8kK	LOW
	Cookie Not Marked as Secure	GET	https://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/assets/2jtDbwm02EAMYk0A0qCOum	LOW
	Cookie Not Marked as Secure	GET	https://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/assets/1pJ51Scg0A8OsoyyeMcisg	LOW
	Cookie Not Marked as Secure	GET	https://blockchain.topcoder.com/challenges/	LOW
	Cookie Not Marked as Secure	GET	https://blockchain.topcoder.com/community-app-assets/api/logger	LOW
	Cookie Not Marked as Secure	GET	https://blockchain.topcoder.com/	LOW
	Cookie Not Marked as Secure	GET	https://blockchain.topcoder.com/challenges	LOW

A6 - SECURITY MISCONFIGURATION

	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://blockchain.topcoder.com/	MEDIUM
	Cookie Not Marked as HttpOnly	POST	http://blockchain.topcoder.com/community-app-assets/api/logger	LOW

	Cookie Not Marked as HttpOnly	GET	http://blockchain.topcoder.com/	LOW
	Cookie Not Marked as HttpOnly	GET	http://blockchain.topcoder.com/challenges/sw.js	LOW
	Cookie Not Marked as HttpOnly	GET	http://blockchain.topcoder.com/community-app-assets/api/logger	LOW
	Cookie Not Marked as HttpOnly	GET	http://blockchain.topcoder.com/community-app-assets/themes/blockchain/	LOW
	Cookie Not Marked as HttpOnly	GET	http://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/entries?content_type=viewport&fields.name=Blockchain%20Community%20-%20Home	LOW
	Cookie Not Marked as HttpOnly	GET	http://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/entries/6GxdEbhe0MkKkcgUi6eWsW	LOW
	Cookie Not Marked as HttpOnly	GET	http://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/entries/XdBwv6Hsg8euE62E8i8kK	LOW
	Cookie Not Marked as HttpOnly	GET	http://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/assets/2jtDbwm02EAMYk0A0qCOum	LOW
	Cookie Not Marked as HttpOnly	GET	http://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/assets/1pJ51Scg0A8OsoyyeMcisg	LOW
	Cookie Not Marked as HttpOnly	GET	http://blockchain.topcoder.com/challenges/	LOW
	Insecure Frame (External)	GET	http://blockchain.topcoder.com/	LOW
	Insecure Frame (External)	GET	http://blockchain.topcoder.com/challenges/	LOW
	Insecure Frame (External)	GET	http://blockchain.topcoder.com/learn	LOW
	Insecure Frame (External)	GET	http://blockchain.topcoder.com/challenges	LOW
	Insecure Frame (External)	GET	http://blockchain.topcoder.com/bsic-incubator	LOW
	Misconfigured Access-Control-Allow-Origin Header	GET	http://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/assets/1pJ51Scg0A8OsoyyeMcisg	LOW

	Misconfigured Access-Control-Allow-Origin Header	GET	http://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/entries/	LOW
	Misconfigured Access-Control-Allow-Origin Header	GET	http://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/entries/XdBwv6Hsg8euE62E8i8kK	LOW
	Misconfigured Access-Control-Allow-Origin Header	GET	http://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/assets/2jtDbwm02EAMYk0A0qCOum	LOW
	Misconfigured Access-Control-Allow-Origin Header	GET	http://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/entries/6GxdEbhe0MkKkcgUi6eWsW	LOW
	Misconfigured Access-Control-Allow-Origin Header	GET	http://blockchain.topcoder.com/api/cdn/public/contentful/default/master/published/entries?content_type=viewport&fields.name=Blockchain%20Community%20-%20Home	LOW

www.community-app.topcoder.com

http://community-app.topcoder.com/

Scan Time	6/4/2022 6:23:37 PM (UTC+05:30)
Scan Duration	00:00:12:30
Total Requests	: 10,263
Average Speed	: 13.7r/s

Risk Level:
MEDIUM

Explanation

This report is generated based on OWASP Top Ten 2017 classification.
There are 98 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

54 IDENTIFIED	40 CONFIRMED	0 CRITICAL
0 HIGH	3 MEDIUM	39 LOW
	0 BEST PRACTICE	12 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	3
Low	39
Best Practice	0
Information	12
TOTAL	**54**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	28
Best Practice	0
Information	11
TOTAL	**40**

VULNERABILITY SUMMARY

A3 - SENSITIVE DATA EXPOSURE

	Weak Ciphers Enabled	GET	https://community-app.topcoder.com/	MEDIUM
	Insecure HTTP Usage	GET	http://community-app.topcoder.com/	MEDIUM
	Cookie Not Marked as Secure	OPTIONS	https://community-app.topcoder.com/community-app-assets/api/tc-communities	LOW
	Cookie Not Marked as Secure	GET	https://community-app.topcoder.com/community-app-assets/api/tc-communities	LOW
	Cookie Not Marked as Secure	OPTIONS	https://community-app.topcoder.com/community-app-assets/api/tc-communities/undefined/meta	LOW
	Cookie Not Marked as Secure	GET	https://community-app.topcoder.com/community-app-assets/api/tc-communities/undefined/meta	LOW
	Cookie Not Marked as Secure	GET	https://community-app.topcoder.com/api/cdn/public/contentful/default/master/published/entries?content_type=route&sys.id=2z6DvIzyhKQ0YusYGsaQc6	LOW
	Cookie Not Marked as Secure	POST	https://community-app.topcoder.com/community-app-assets/api/logger	LOW

A6 - SECURITY MISCONFIGURATION

	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://community-app.topcoder.com/	MEDIUM
	Cookie Not Marked as HttpOnly	GET	http://community-app.topcoder.com/api/cdn/public/contentful/default/master/published/entries?content_type=route&sys.id=2z6DvIzyhKQ0YusYGsaQc6	LOW
	Cookie Not Marked as HttpOnly	GET	http://community-app.topcoder.com/	LOW
	Cookie Not Marked as HttpOnly	GET	http://community-app.topcoder.com/challenges/sw.js	LOW
	Cookie Not Marked as HttpOnly	GET	http://community-app.topcoder.com/analytics.min.js	LOW
	Cookie Not Marked as HttpOnly	OPTIONS	https://community-app.topcoder.com/community-app-assets/api/tc-communities	LOW

	Cookie Not Marked as HttpOnly	POST	http://community-app.topcoder.com/community-app-assets/api/logger	LOW
	Cookie Not Marked as HttpOnly	GET	https://community-app.topcoder.com/community-app-assets/api/tc-communities	LOW
	Cookie Not Marked as HttpOnly	GET	http://community-app.topcoder.com/challenges/	LOW
	Cookie Not Marked as HttpOnly	GET	http://community-app.topcoder.com/challenges/30058473	LOW
	Cookie Not Marked as HttpOnly	GET	http://community-app.topcoder.com/challenges/30058637	LOW
	Cookie Not Marked as HttpOnly	GET	http://community-app.topcoder.com/api/recruit/jobs?job_status=1	LOW
	Insecure Frame (External)	GET	http://community-app.topcoder.com/	LOW
	Insecure Frame (External)	GET	http://community-app.topcoder.com/challenges/	LOW
	Insecure Frame (External)	GET	http://community-app.topcoder.com/challenges/30058473	LOW
	Insecure Frame (External)	GET	http://community-app.topcoder.com/challenges/30058637	LOW
	Insecure Frame (External)	GET	http://community-app.topcoder.com/challenges/30049552	LOW
	Insecure Frame (External)	GET	http://community-app.topcoder.com/challenges/30050696	LOW
	Insecure Frame (External)	GET	http://community-app.topcoder.com/challenges/30058529	LOW
	Insecure Frame (External)	GET	http://community-app.topcoder.com/challenges	LOW
	Insecure Frame (External)	GET	http://community-app.topcoder.com/home	LOW
	Insecure Frame (External)	GET	http://community-app.topcoder.com/challenges/30050680	LOW
	Insecure Frame (External)	GET	http://community-app.topcoder.com/members/TonyJ	LOW

	[Possible] Phishing by Navigating Browser Tabs	GET	http://community-app.topcoder.com/analytics.min.js	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	http://community-app.topcoder.com/(268409241-8093)	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	http://community-app.topcoder.com/challenges/(268409241-2168)	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	http://community-app.topcoder.com/challenges/?nsextt=%0d%0ans%3anetsparker056650%3dvuln	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	http://community-app.topcoder.com/etc/passwd	LOW
	[Possible] Phishing by Navigating Browser Tabs	POST	http://community-app.topcoder.com/challenges/	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	http://community-app.topcoder.com/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp?fileName=/etc/passwd	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	http://community-app.topcoder.com/challenges/etc/passwd	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	http://community-app.topcoder.com/cdn.segment.com/?nsextt=%0d%0ans%3anetsparker056650%3dvuln	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	http://community-app.topcoder.com/cdn.segment.com/(268409241-84438)	LOW
	[Possible] Phishing by Navigating Browser Tabs	GET	http://community-app.topcoder.com/cdn.segment.com/etc/passwd	LOW

www.faceid.topcoder.com

http://faceid.topcoder.com/

Scan Time	6/4/2022 6:38:30 PM (UTC+05:30)
Scan Duration	00:00:04:49
Total Requests	: 4,004
Average Speed	: 13.8r/s

Risk Level:
HIGH

Explanation

This report is generated based on OWASP Top Ten 2017 classification.
There are 33 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

28 IDENTIFIED	4 CONFIRMED
0 CRITICAL	4 HIGH
4 MEDIUM	7 LOW
7 BEST PRACTICE	6 INFORMATION

Identified Vulnerabilities

Critical	0
High	4
Medium	4
Low	7
Best Practice	7
Information	6
TOTAL	**28**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	0
Low	0
Best Practice	0
Information	4
TOTAL	**4**

VULNERABILITY SUMMARY

A3 - SENSITIVE DATA EXPOSURE

HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://faceid.topcoder.com/	MEDIUM

A6 - SECURITY MISCONFIGURATION

Missing X-Frame-Options Header	GET	http://faceid.topcoder.com/	LOW
Missing X-Frame-Options Header	GET	http://faceid.topcoder.com/css/	LOW
Missing X-Frame-Options Header	GET	http://faceid.topcoder.com/data/challenge-posts.json	LOW
Missing X-Frame-Options Header	GET	http://faceid.topcoder.com/js/	LOW
Missing X-Frame-Options Header	GET	http://faceid.topcoder.com/data/	LOW
Missing X-Frame-Options Header	GET	http://faceid.topcoder.com/i/	LOW

A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES

Out-of-date Version (Highcharts)	GET	http://faceid.topcoder.com/	HIGH
Out-of-date Version (Highcharts)	GET	http://faceid.topcoder.com/js/highcharts.js	HIGH
Out-of-date Version (Moment.js)	GET	http://faceid.topcoder.com/	HIGH
Out-of-date Version (Moment.js)	GET	http://faceid.topcoder.com/js/moment.min.js	HIGH
Out-of-date Version (Bootstrap)	GET	http://faceid.topcoder.com/js/bootstrap.min.js	MEDIUM
Out-of-date Version (jQuery)	GET	http://faceid.topcoder.com/	MEDIUM
Out-of-date Version (jQuery)	GET	http://faceid.topcoder.com/js/jquery.min.js	MEDIUM

www.morgoth.topcoder.com

http://morgoth.topcoder.com/

Scan Time	6/4/2022 6:45:29 PM (UTC+05:30)
Scan Duration	00:00:03:59
Total Requests	: 3,165
Average Speed	: 13.2r/s

Risk Level:
HIGH

Explanation

This report is generated based on OWASP Top Ten 2017 classification.
There are 37 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

36 IDENTIFIED	4 CONFIRMED	0 CRITICAL
4 HIGH	4 MEDIUM	11 LOW
	11 BEST PRACTICE	6 INFORMATION

Identified Vulnerabilities

Critical	0
High	4
Medium	4
Low	11
Best Practice	11
Information	6
TOTAL	**36**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	0
Low	0
Best Practice	0
Information	4
TOTAL	**4**

VULNERABILITY SUMMARY

A3 - SENSITIVE DATA EXPOSURE

	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://morgoth.topcoder.com/	MEDIUM

A6 - SECURITY MISCONFIGURATION

	Missing X-Frame-Options Header	GET	http://morgoth.topcoder.com/	LOW
	Missing X-Frame-Options Header	GET	http://morgoth.topcoder.com/js/	LOW
	Missing X-Frame-Options Header	GET	http://morgoth.topcoder.com/i/	LOW
	Missing X-Frame-Options Header	GET	http://morgoth.topcoder.com/css/	LOW
	Missing X-Frame-Options Header	GET	http://morgoth.topcoder.com/.svn/wc.db	LOW
	Missing X-Frame-Options Header	GET	http://morgoth.topcoder.com/data/	LOW
	Missing X-Frame-Options Header	GET	http://morgoth.topcoder.com/i/.svn/wc.db	LOW
	Missing X-Frame-Options Header	GET	http://morgoth.topcoder.com/css/.svn/wc.db	LOW
	Missing X-Frame-Options Header	GET	http://morgoth.topcoder.com/data/.svn/wc.db	LOW
	Missing X-Frame-Options Header	GET	http://morgoth.topcoder.com/js/.svn/wc.db	LOW
	Missing X-Frame-Options Header	GET	http://morgoth.topcoder.com/.well-known/c:/boot.ini	LOW

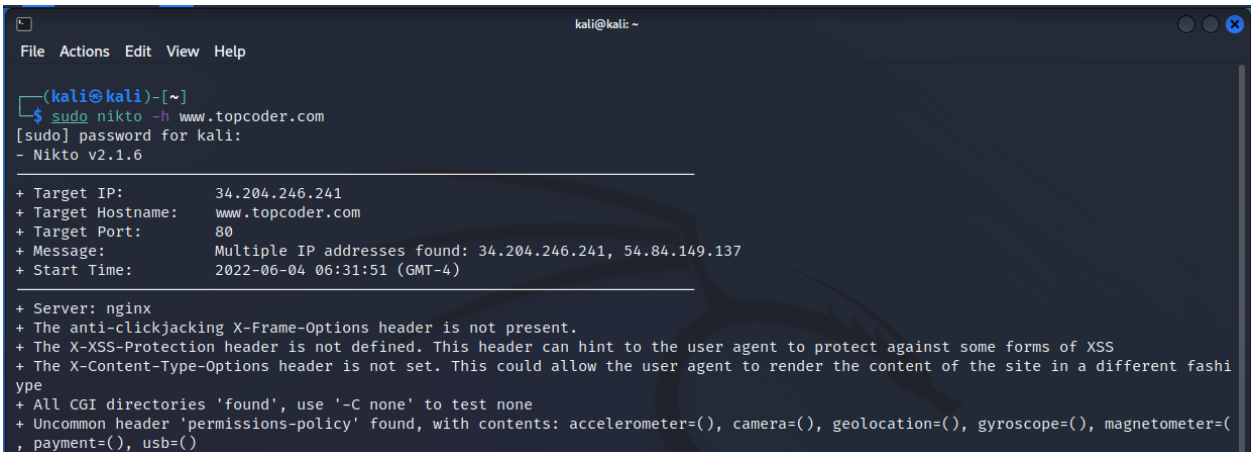
A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES

	Out-of-date Version (Highcharts)	GET	http://morgoth.topcoder.com/	HIGH
	Out-of-date Version (Highcharts)	GET	http://morgoth.topcoder.com/js/highcharts.js	HIGH
	Out-of-date Version (Moment.js)	GET	http://morgoth.topcoder.com/	HIGH
	Out-of-date Version (Moment.js)	GET	http://morgoth.topcoder.com/js/moment.min.js	HIGH
	Out-of-date Version (Bootstrap)	GET	http://morgoth.topcoder.com/js/bootstrap.min.js	MEDIUM
	Out-of-date Version (jQuery)	GET	http://morgoth.topcoder.com/	MEDIUM
	Out-of-date Version (jQuery)	GET	http://morgoth.topcoder.com/js/jquery.min.js	MEDIUM

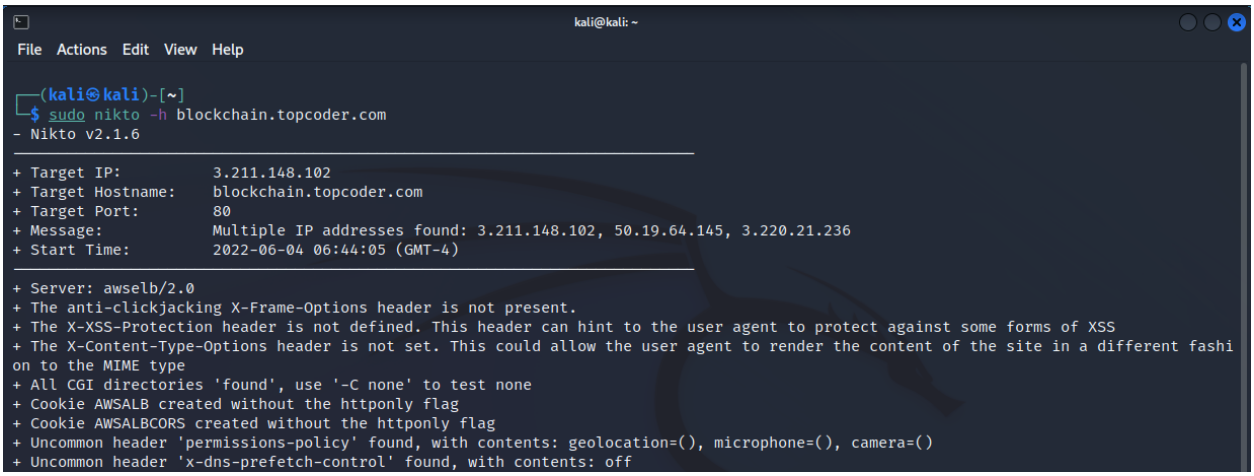
Nikto

- Nikto isn't designed to be a stealthy tool. It will swiftly test a web server, and the results will be displayed in log files or to an IPS/IDS. If you want to try out LibWhisker's anti-IDS tactics, you're welcome to (or test your IDS system). Although not every check poses a security concern, the most majority do. Some items are "info only" tests that seek for objects on the server that may or may not have a security concern, but that the webmaster or security engineer is unaware of. In most cases, these items are accurately designated in the textual content. There are also some tests for unidentified items found in log files that have been searched for.

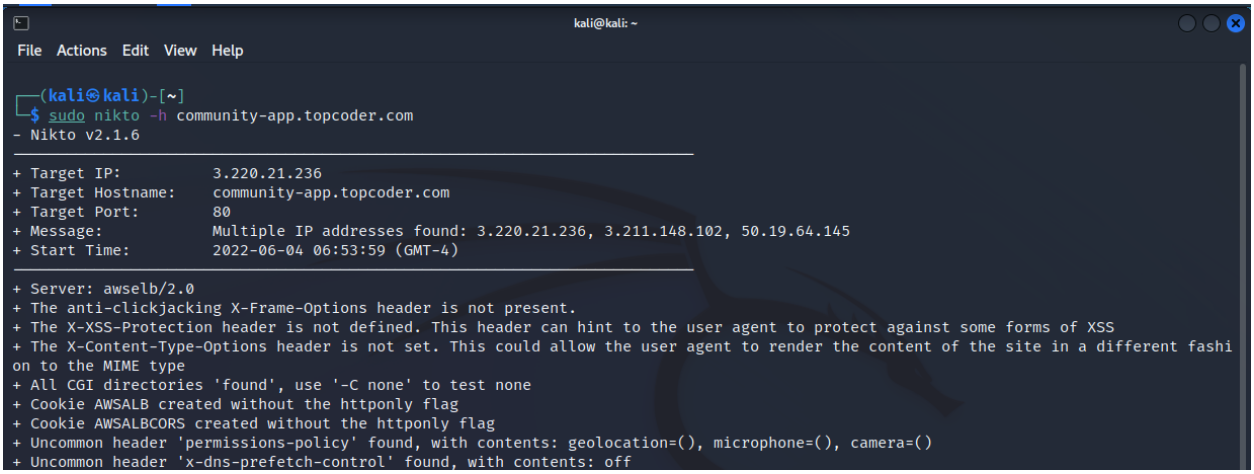
www.topcoder.com



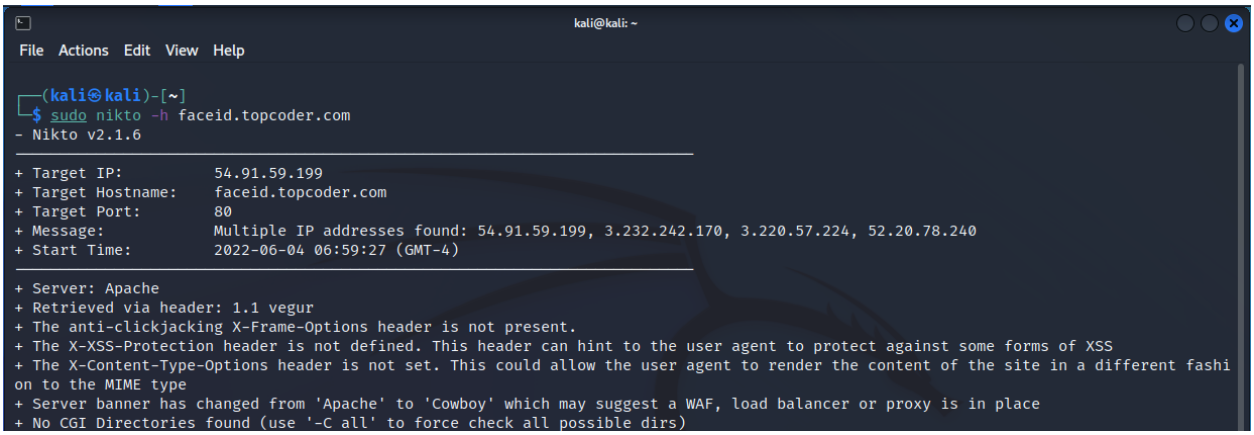
blockchain.topcoder.com



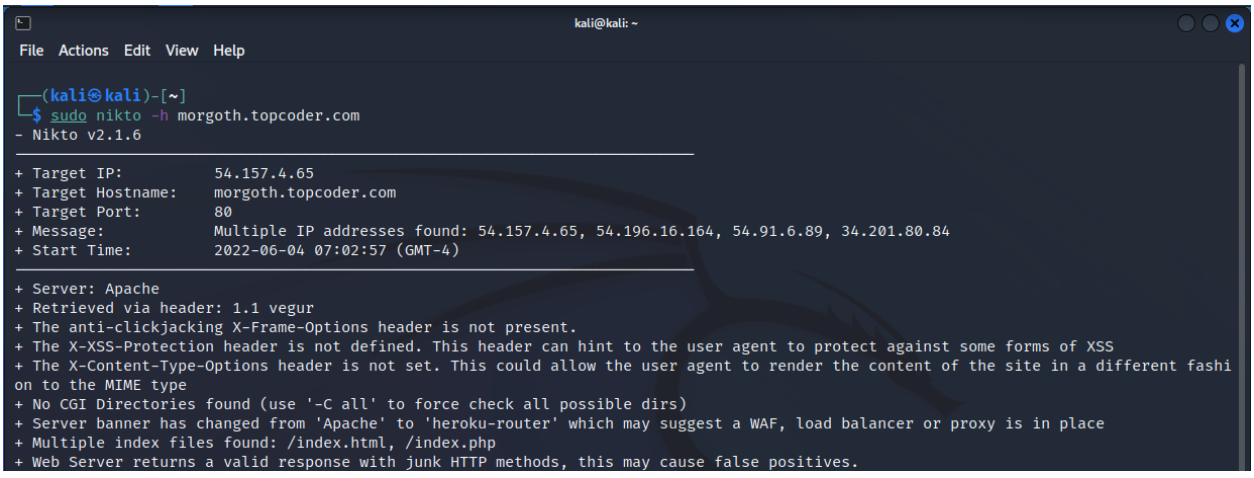
www.community-app.topcoder.com



www.faceid.topcoder.com



www.morgoth.topcoder.com

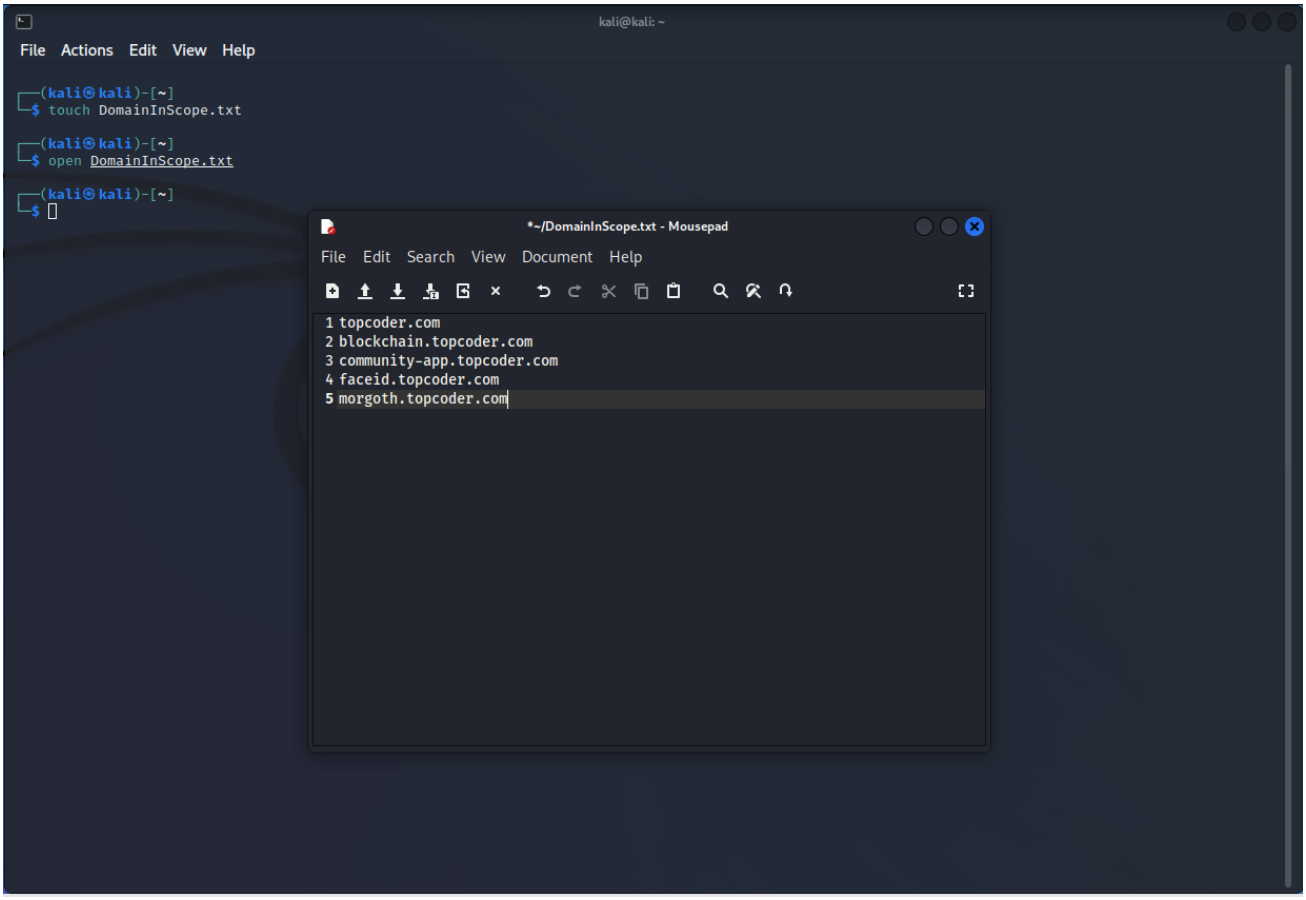


Find target has open ports

- **Nmap tool**

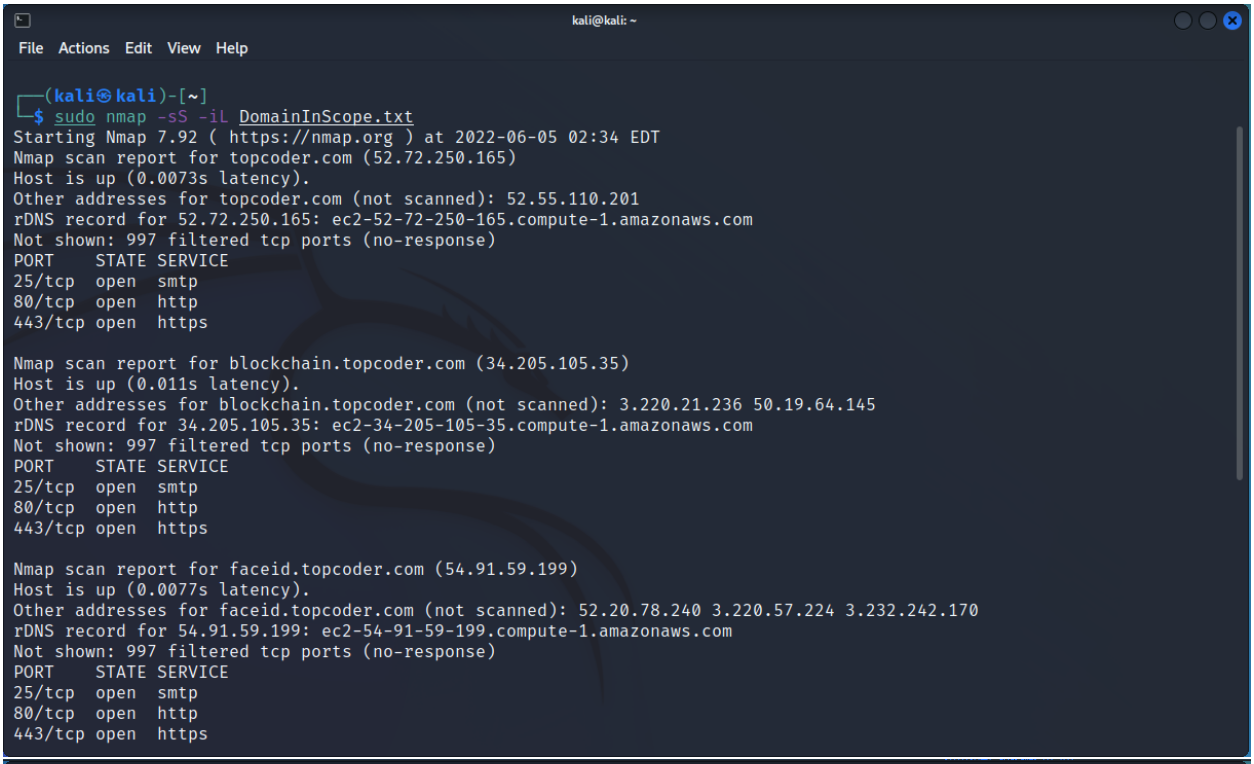
  Nmap is a network scanner that is free and open source. It's used for network security audits and detection. Nmap was designed to swiftly scan large networks, although it also works well on single hosts. According to some system and network managers, it's also useful for regulating service upgrade timelines. Official binary versions for Linux, Windows, and Mac OS X are available. Nmap is compatible with all major computer operating systems.

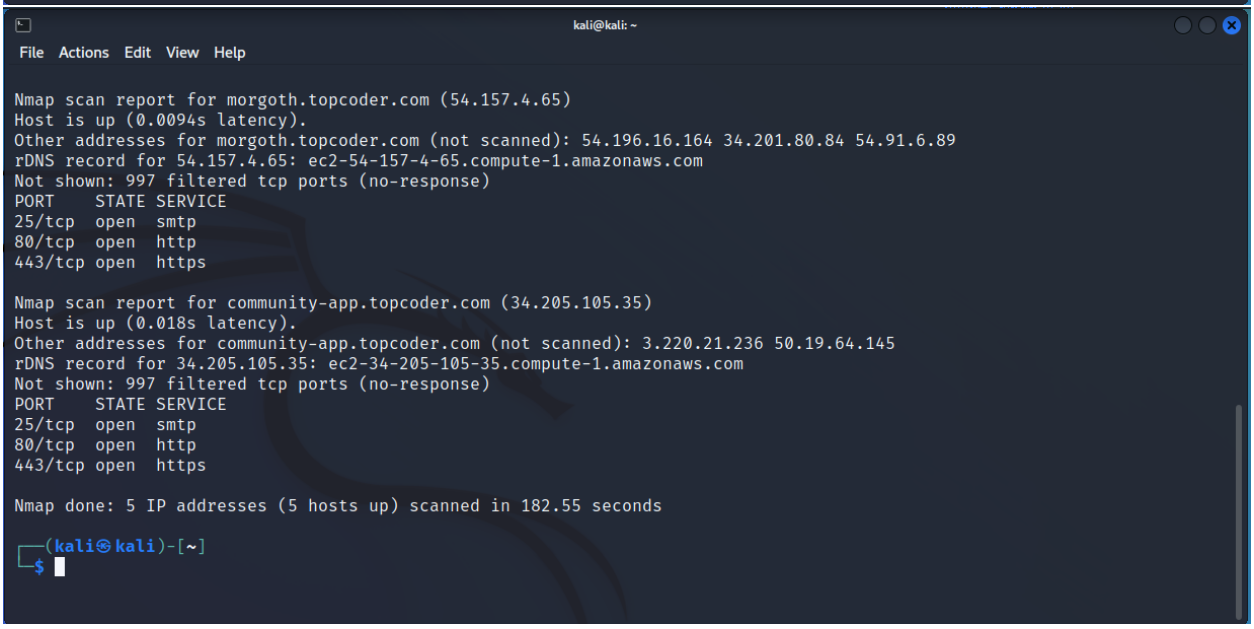
Create a new txt file and put our five selected sub domain, then save it.



Now run this command for scan open port

“sudo nmap -sS -iL DomainInScope.txt”





Vulnerability Analytics

In this section, I'll talk about some of the vulnerabilities we discovered throughout our scans. Their level of risk, as well as other information.

Feather We're concentrating on the amount of vulnerabilities, their sorts, and so forth.

Netspaker Scan Analytics

Hear I scan 5 domains, and I found High level, medium level and low-level vulnerabilities.

Domain Name	High Risks	Medium Risks	Low Risks	Total
topcoder.com		7	44	**51**
blockchain.topcoder.com		3	33	**36**
Community-app.topcoder.com		3	39	**42**
faceid.topcoder.com	4	4	7	**15**
morgoth.topcoder.com	4	4	11	**19**
Total	**8**	**21**	**134**	**163**

Nmap Scan Analytics

Domain Name	Open Ports
1. www.topcoder.com 2. blockchain.topcoder.com 3. community-app.topcoder.com 4. faceid.topcoder.com 5. morgoth.topcoder.com	**25/tcp open smtp** **80/tcp open http** **443/tcp open https**

HIGH AND MEDIUM LEVEL VULNERABILITY SUMMARY

Vulnerability	www.topcoder.com	blockchain.topcoder.com	community-app.topcoder.com	faceid.topcoder.com	morgoth.topcoder.com
Weak Ciphers Enabled	✓	✓	✓		
HTTP Strict Transport Security (HSTS)	✓	✓	✓	✓	✓
Insecure HTTP Usage		✓	✓		
Out-of-date Version (Bootstrap)				✓	✓
Out-of-date Version (jQuery)	✓			✓	✓
Out-of-date Version (Highcharts)				✓	✓
Out-of-date Version (Moment.js)				✓	✓

Vulnerability Assessment and Evaluation

Vulnerability assessment is the process of defining, detecting, categorizing, and prioritizing vulnerabilities in computer systems, applications, and network infrastructures. Organizations can use vulnerability assessments to get the information, awareness, and risk background they need to recognize and respond to threats to their environment.

Importance of vulnerability assessments

A vulnerability assessment identifies any security issues in a company's environment. It also teaches how to assess the risks associated with specific defects. This approach provides the organization with a better understanding of its assets, security weaknesses, and overall risk, lessening the likelihood of a cybercriminal breaking into its systems and catching it off guard.

Identify Vulnerabilities in **https://www.topcoder.com**

Weak Ciphers Enabled

- Netsparker discovered that weak ciphers are enabled during a secure connection (SSL). Only strong ciphers should be allowed on your web server to ensure secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

3.1. https://www.topcoder.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)

Request

```
[SSL Connection]
```

Response

Response Time (ms) : 1 Total Bytes Received : 16 Body Length : 0 Is Compressed : No

```
[SSL Connection]
```

How to fix vulnerabilities

- Use strong ciphers.

Identify Vulnerabilities in https://blockchain.topcoder.com

HTTP Strict Transport Security (HSTS)

- Hsts is a type of security header. When we type the domain http protocol, the security header changes it to the https protocol. This security header contributes to the prevention of man-in-the-middle attacks, protocol downgrade attacks, and cookie hijacking.

Impact

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

Vulnerabilities

1.1. https://blockchain.topcoder.com/

Error	Resolution
preload directive not present	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

Certainty

Request

```
GET / HTTP/1.1
Host: blockchain.topcoder.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 1198.2896 Total Bytes Received : 117723 Body Length : 116748 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: AWSALB=pGdqPGxNqAdEz3YC6Jc6bTTLxQSUFgc8k9qJ8XX0vMJy30eGZ9+QSdIW+VmfxcaAkY3mAjjUsVo/3j3WP
HyHVGw5AFLrSIWpa78f65v8gxkjOJGk1vTfVQBhsJze; Expires=Sat, 11 Jun 2022 07:53:41 GMT; Path=/
Set-Cookie: AWSALBCORS=pGdqPGxNqAdEz3YC6Jc6bTTLxQSUFgc8k9qJ8XX0vMJy30eGZ9+QSdIW+VmfxcaAkY3mAjjUsVo/3
j3WPHyHVGw5AFLrSIWpa78f65v8gxkjOJGk1vTfVQBhsJze; Expires=Sat, 11 Jun 2022 07:53:41 GMT; Path=/; Same
Site=None; Secure
Content-Encoding:
X-Content-Type-Options: nosniff
Connection: keep-alive
X-Download-Options: noopen
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-DNS-Prefetch-Control: off
Strict-Transport-Security: max-age=15552000; includeSubDomains
Referrer-Policy: strict-origin-when-cross-origin
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Permissions-Policy: geolocation=(), microphone=(), camera=()
Date: Sat, 04 Jun 2022 07:53:42 GMT
ETag: W/"1c80c-XslROfUAg1HtFgZN5B6g+8sAYJM"
Vary: Accept-Encoding
```

```
<!DOCTYPE html>
<html>
<head>
<title data-react-helmet="true">Topcoder Blockchain Community</title>
<meta data-react-helmet="true" name="theme-color" content="#FFFFFF"/><meta data-react-helmet="true"
name="description" content="Learn about and build the next great decentralized application (DApp) on
Ethereum platform"/><meta data-react-helmet="true" name="twitter:card" content="summary_large_image"
/><meta data-react-helmet="true" name="twitter:title" content="Topcoder Blockchain Community"/><meta
data-react-helmet="true" name="twitter:description" content="Learn about and build the next great de
centralized application (DApp) on Ethereum platform"/><meta data-react-helmet="true" name="twitter:i
mage" content="http://blockchain.topcoder.com/community-app-assets/images/5e0e9556ff05f1e94cca9ecaa2
02ee6b.jpg"/><meta data-react-helmet="true" name="twitter:site" content="@Topcoder Blockchain Commun
ity"/><meta data-react-helmet="true" property="og:title" content="Topcoder Blockc
…
```

How to fix vulnerabilities

This domain must be added to the hsts preload list. This will ensure that the browser automatically connects to the website via https.

The max-age must be at least 31536000 seconds (1year)

The includeSubdomains directive must be specified

Identify Vulnerabilities in **https://community-app.topcoder.com**

Insecure HTTP Usage

- Netsparker discovered that the target website permits web browsers to access it through HTTP but does not redirect them to HTTPS.
- Although HSTS is enabled on the target website, HTTP queries are not forwarded to HTTPS. This severely reduces the value of HSTS implementation.
- Visitors who have not previously visited the HTTPS version of the website, for example, will be unable to benefit from HSTS.

Impact

Users will not be able to take advantage of HSTS which almost renders the HSTS implementation useless. Not having HSTS will make MITM attacks easier for attackers.
If there is a client side redirect to HTTPS version of the website (via JavaScript or Meta tags) then you can ignore this vulnerability.

Vulnerabilities

1.1. http://community-app.topcoder.com/

Certainty

Request

```
GET / HTTP/1.1
Host: community-app.topcoder.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 1158.6154 Total Bytes Received : 62256 Body Length : 61290 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: AWSALB=qhLT/t4yW1Fv8UyISHRq2AaPcS8xAkhL4YFwqpe+bIslHRQtlTp7B7MWjuBhxHAIZ2NYsue+M0Y1JAFuK
49/PhWhucvqZzPpjX0i+j+3uN91KekuJiEf0RtG1EQz; Expires=Sat, 11 Jun 2022 12:54:06 GMT; Path=/
Set-Cookie: AWSALBCORS=qhLT/t4yW1Fv8UyISHRq2AaPcS8xAkhL4YFwqpe+bIslHRQtlTp7B7MWjuBhxHAIZ2NYsue+M0Y1J
AFuK49/PhWhucvqZzPpjX0i+j+3uN91KekuJiEf0RtG1EQz; Expires=Sat, 11 Jun 2022 12:54:06 GMT; Path=/; Same
Site=None
Content-Encoding:
X-Content-Type-Options: nosniff
Connection: keep-alive
X-Download-Options: noopen
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
X-DNS-Prefetch-Control: off
Strict-Transport-Security: max-age=15552000; includeSubDomains
Referrer-Policy: strict-origin-when-cross-origin
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Permissions-Policy: geolocation=(), microphone=(), camera=()
Date: Sat, 04 Jun 2022 12:54:06 GMT
ETag: W/"ef6a-EiFc3sgzdP23DnI6bl+E3WUyPr0"
Vary: Accept-Encoding
```

```
<!DOCTYPE html>
<html>
<head>
<title data-react-helmet="true">Topcoder</title>
<meta data-react-helmet="true" name="theme-color" content="#FFFFFF"/><meta data-react-helmet="true"
name="description" content="Topcoder is a crowdsourcing marketplace that connects businesses with ha
rd-to-find expertise. The Topcoder Community includes more than one million of the world's top desig
ners, developers, data scientists, and algorithmists. Global enterprises and startups alike use Topc
oder to accelerate innovation, solve challenging problems, and tap into specialized skills on deman
d."/><meta data-react-helmet="true" name="twitter:card" content="summary_large_image"/><meta data-re
act-helmet="true" name="twitter:title" content="Topcoder"/><meta data-react-helmet="true" name="twit
ter:description" content="Topcoder is a crowdsourcing marketplace that connects businesses with hard
-to-find expertise. The Topcoder Community includes more than one million of the world's top designe
rs, developers
…
```

How to fix vulnerabilities

Configure webserver to redirect HTTP requests to HTTPS.

Identify Vulnerabilities in **https://faceid.topcoder.com**

Out-of-date Version (Bootstrap)

- Netsparker discovered that the target website uses Bootstrap and that it is out of date.
- Since this is an old version of the software, it may be vulnerable to attacks.

Vulnerabilities

3.1. http://faceid.topcoder.com/js/bootstrap.min.js

Identified Version

- 3.3.5

Latest Version

- 3.4.1 (in this branch)

Overall Latest Version

- 5.1.3

Vulnerability Database

- Result is based on 06/03/2022 20:30:00 vulnerability database content.

Certainty

Request

```
GET /js/bootstrap.min.js HTTP/1.1
Host: faceid.topcoder.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://faceid.topcoder.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 921.6875 Total Bytes Received : 37178 Body Length : 36816 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Connection: keep-alive
Via: 1.1 vegur
Content-Length: 36816
Last-Modified: Mon, 29 Apr 2019 15:52:44 GMT
Accept-Ranges: bytes
Pragma: no-cache
Content-Type: application/javascript
Date: Sat, 04 Jun 2022 13:09:30 GMT
Cache-Control: max-age=0, no-cache, no-store,
…
15:52:44 GMT
Accept-Ranges: bytes
Pragma: no-cache
Content-Type: application/javascript
Date: Sat, 04 Jun 2022 13:09:30 GMT
Cache-Control: max-age=0, no-cache, no-store, must-revalidate

/*!
* Bootstrap v3.3.5(http://getbootstrap.com)
* Copyright 2011-2015 Twitter, Inc.
* Licensed under the MIT license
*/
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(
…
```

How to fix vulnerabilities

- upgrade Bootstrap to the latest stable version.

Out-of-date Version (jQuery)

- Netsparker discovered that the target website is utilizing jQuery and that it is out of date.
- jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Vulnerabilities

5.1. http://faceid.topcoder.com/

Identified Version

- 2.1.4

Latest Version

- 2.2.4 (in this branch)

Overall Latest Version

- 3.6.0

Vulnerability Database

- Result is based on 06/03/2022 20:30:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: faceid.topcoder.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 947.596 Total Bytes Received : 13022 Body Length : 12842 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache
Connection: keep-alive
Via: 1.1 vegur
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Sat, 04 Jun 2022 13:08:29 GMT

<!doctype html Cache-Control:no-cache; >
<html>
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<title id="brwsrTitle">Data Science Dashboard</title>

<!-- CSS Files -->
<link rel="stylesheet" href="./css/bootstrap.min.css">
<link rel="stylesheet" href="./css/daterangepicker.css" />
<link rel="stylesheet" href="./css/style.css">
</head>

<body>
<header>
<div class="container-fluid">
<h1> </h1>
<h1 id="pageTitle"></h1>
<!--
<div class="row brands ">
<div class="col-md-2 vertical-center col-md-offset-2"><img src="./i/NNSA-logo.png" class="img-respon
sive img-center" alt="" /></div>
<div class="col-md-2 vertical-center"><img src="./i/LANL-logo.png" class="img-responsive img-center
 vertical-center" alt="" /></div>
<div class="col-md-2"><img src="./i/ORNL-twoline-green.png" class="img-responsive img-center vertica
l-center" alt="" /></div>
<div class="col-md-2 vertical-center"><img src="./i/BerkeleyLab_Masterbrand_logo.png" class="img-res
ponsive img-center" alt="" /></div>
</div>


</div>
<div class="row brands ">
<div class="col-md-2 col-md-offset-3"><img src="./i/lish_logo2.png" class="img-responsive img-cente
r" alt="" /></div>
<div class="col-md-2 vertical-center"><img src="./i/Nasa_Tournament_Lab_Logo.png" class="img-respons
ive img-center" alt="" /></div>
<div class="col-md-2"><a href="http://crowdsourcing.topcoder.com/" target="_blank"><img src="./i/tc-
full-clipped.png" class="img-responsive img-center" alt="" /></a>

</div>
```

```
-->

</div>

<nav>
<ul>
<li><a href="./index.html" class="results active">Results</a></li>
<li><a href="./geography.html" class="geography">Geography</a></li>
<li><a href="https://www.to
…
```

5.2. http://faceid.topcoder.com/js/jquery.min.js

Identified Version

- 2.1.4

Latest Version

- 2.2.4 (in this branch)

Overall Latest Version

- 3.6.0

Vulnerability Database

- Result is based on 06/03/2022 20:30:00 vulnerability database content.

Certainty

Request

```
GET /js/jquery.min.js HTTP/1.1
Host: faceid.topcoder.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://faceid.topcoder.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 1053.8575 Total Bytes Received : 84742 Body Length : 84380 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Connection: keep-alive
Via: 1.1 vegur
Content-Length: 84380
Last-Modified: Mon, 29 Apr 2019 15:52:44 GMT
Accept-Ranges: bytes
Pragma: no-cache
Content-Type: application/javascript
Date: Sat, 04 Jun 2022 13:09:33 GMT
Cache-Control: max-age=0, no-cache, no-store,
…
2019 15:52:44 GMT
Accept-Ranges: bytes
Pragma: no-cache
Content-Type: application/javascript
Date: Sat, 04 Jun 2022 13:09:33 GMT
Cache-Control: max-age=0, no-cache, no-store, must-revalidate

/*! jQuery v2.1.4| (c) 2005, 2015 jQuery Foundation, Inc. | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b
(a,!0):function(a){if(!a.document)t
…
```

How to fix vulnerabilities

- upgrade jQuery to the latest stable version

Identify Vulnerabilities in **https://morgoth.topcoder.com**

Out-of-date Version (Highcharts)

Netsparker discovered that the target website is using Highcharts and that it is out of date.

Since this is an old version of the software, it may be vulnerable to attacks.

Highcharts JS is a JavaScript charting library based on SVG. In Highcharts versions 8 and earlier, the chart options structure was not systematically filtered for XSS vectors. The potential impact was that content from untrusted sources could execute code in the end user's browser. The vulnerability is patched in version 9. As a workaround, implementers who are not able to upgrade may apply DOMPurify recursively to the options structure to filter out malicious markup.

Vulnerabilities

1.1. http://morgoth.topcoder.com/

Identified Version

- 4.1.9

Latest Version

- 10.1.0

Vulnerability Database

- Result is based on 06/03/2022 20:30:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: morgoth.topcoder.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 796.5852 Total Bytes Received : 12445 Body Length : 12265 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache
Connection: keep-alive
Via: 1.1 vegur
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Sat, 04 Jun 2022 13:15:28 GMT

<!doctype html>
<html>
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<title id="brwsrTitle">Data Science Dashboard</title>

<!-- CSS Files -->
<link rel="stylesheet" href="./css/bootstrap.min.css">
<link rel="stylesheet" href="./css/daterangepicker.css" />
<link rel="stylesheet" href="./css/style.css">
</head>

<body>
<header>
<div class="container-fluid">
<h1> </h1>
<h1 id="pageTitle"></h1>

<div class="row brands">
<div class="col-md-2 col-md-offset-3"><img src="./i/iarpa-logo_for_on_white.png" class="img-responsi
ve img-center" alt="" /></div>
<div class="col-md-2 "><img src="./i/morgoth.png" class="img-responsive img-center" alt="" /></div>
<div class="col-md-2"><a href="http://crowdsourcing.topcoder.com/" target="_blank"><img src="./i/hig
h_topcoder_vertical_fullcolor.png" class="img-responsive img-center" alt="" /></a></div>

</div>

<nav>
<ul>
<li><a href="./index.html" class="results active">Results</a></li>
<li><a href="./geography.html" class="geography">Geography</a></li>
<li><a href="https://community.topcoder.com/longcontest/?module=ViewProblemStatement&rd=16937&pm=146
38" target="_blank" class="results">Overview</a></li>
</ul>
</nav>


</div><!-- / .container-fluid -->
</header>
<!-- / header -->
```

```
<main>
<div class="filters">
<div class="container-fluid">
<div class="row">
<div class="col-md-2">
<p class="form-control-static text-right">View:</p>
</div>
<div class="col-md-2">
<div class="btn-group">
<button type="button" class="btn btn-default dropdown-toggle" aria-haspopup="true" aria-expanded="fa
lse">
<span id="score-text">Provisional Score
…
```

1.2. http://morgoth.topcoder.com/js/highcharts.js

Identified Version

- 4.1.9

Latest Version

- 10.1.0

Vulnerability Database

- Result is based on 06/03/2022 20:30:00 vulnerability database content.

Certainty

Request

```
GET /js/highcharts.js HTTP/1.1
Host: morgoth.topcoder.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://morgoth.topcoder.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 1163.3547 Total Bytes Received : 165308 Body Length : 165037 Is Compressed : No

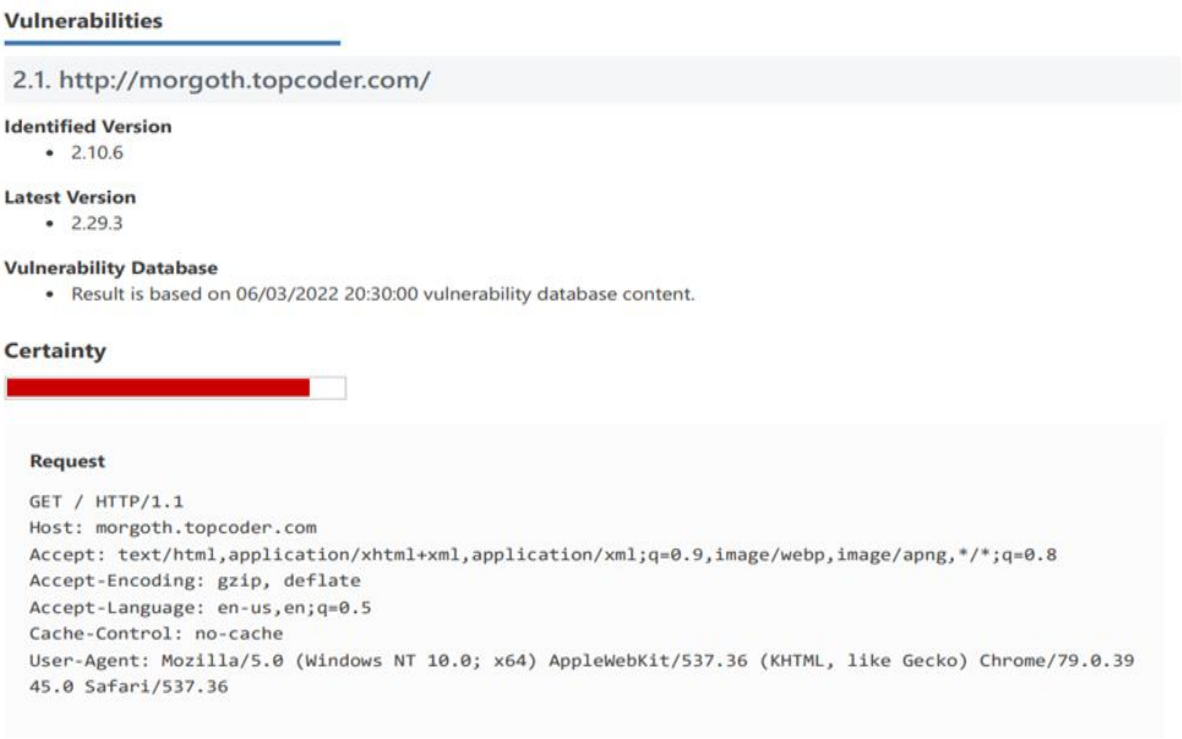
```
HTTP/1.1 200 OK
Server: Apache
Connection: keep-alive
Via: 1.1 vegur
Content-Length: 165037
Last-Modified: Wed, 24 Mar 2021 16:53:24 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Sat, 04 Jun 2022 13:16:33 GMT
Etag: "284ad
…
ntent-Length: 165037
Last-Modified: Wed, 24 Mar 2021 16:53:24 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Sat, 04 Jun 2022 13:16:33 GMT
Etag: "284ad-5be4b2315a900"

/*
Highcharts JS v4.1.9(2015-10-07)

(c) 2009-2014 Torstein Honsi

License: www.highcharts.com/license
*/
(function(){function D(){var a,b=arguments,c,d={},e=function(a,b){var c,d;typeof a!=="object"&&(a=
{});for(d in b)b
…
```

How to fix vulnerabilities

- upgrade Highcharts to the latest stable version.

Out-of-date Version (Moment.js)

- Netsparker discovered that the target website uses Moment.js and that it is out of date.
- Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability impacts npm (server) users of Moment.js between versions 1.0.1 and 2.29.1, especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the patch can be applied to all affected versions. As a workaround, sanitize the user-provided locale name before passing it to Moment.js.



Vulnerabilities

2.1. http://morgoth.topcoder.com/

Identified Version
- 2.10.6

Latest Version
- 2.29.3

Vulnerability Database
- Result is based on 06/03/2022 20:30:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: morgoth.topcoder.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 796.5852 Total Bytes Received : 12445 Body Length : 12265 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache
Connection: keep-alive
Via: 1.1 vegur
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Sat, 04 Jun 2022 13:15:28 GMT

<!doctype html>
<html>
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<title id="brwsrTitle">Data Science Dashboard</title>

<!-- CSS Files -->
<link rel="stylesheet" href="./css/bootstrap.min.css">
<link rel="stylesheet" href="./css/daterangepicker.css" />
<link rel="stylesheet" href="./css/style.css">
</head>

<body>
```

```
<header>
<div class="container-fluid">
<h1> </h1>
<h1 id="pageTitle"></h1>

<div class="row brands">
<div class="col-md-2 col-md-offset-3"><img src="./i/iarpa-logo_for_on_white.png" class="img-responsi
ve img-center" alt="" /></div>
<div class="col-md-2 "><img src="./i/morgoth.png" class="img-responsive img-center" alt="" /></div>
<div class="col-md-2"><a href="http://crowdsourcing.topcoder.com/" target="_blank"><img src="./i/hig
h_topcoder_vertical_fullcolor.png" class="img-responsive img-center" alt="" /></a></div>

</div>

<nav>
<ul>
<li><a href="./index.html" class="results active">Results</a></li>
<li><a href="./geography.html" class="geography">Geography</a></li>
<li><a href="https://community.topcoder.com/longcontest/?module=ViewProblemStatement&rd=16937&pm=146
38" target="_blank" class="results">Overview</a></li>
</ul>
</nav>


</div><!-- / .container-fluid -->
</header>
<!-- / header -->
```

```
<main>
<div class="filters">
<div class="container-fluid">
<div class="row">
<div class="col-md-2">
<p class="form-control-static text-right">View:</p>
</div>
<div class="col-md-2">
<div class="btn-group">
<button type="button" class="btn btn-default dropdown-toggle" aria-haspopup="true" aria-expanded="fa
lse">
<span id="score-text">Provisional Score
…
```

2.2. http://morgoth.topcoder.com/js/moment.min.js

Identified Version

- 2.10.6

Latest Version

- 2.29.3

Vulnerability Database

- Result is based on 06/03/2022 20:30:00 vulnerability database content.

Certainty

Request

```
GET /js/moment.min.js HTTP/1.1
Host: morgoth.topcoder.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://morgoth.topcoder.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.39
45.0 Safari/537.36
```

Response

Response Time (ms) : 268.6664 Total Bytes Received : 35684 Body Length : 35415 Is Compressed : No

```
HTTP/1.1 200 OK
Server: Apache
Connection: keep-alive
Via: 1.1 vegur
Content-Length: 35415
Last-Modified: Wed, 24 Mar 2021 16:53:24 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Sat, 04 Jun 2022 13:16:33 GMT
Etag: "8a57
…
ur
Content-Length: 35415
Last-Modified: Wed, 24 Mar 2021 16:53:24 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Sat, 04 Jun 2022 13:16:33 GMT
Etag: "8a57-5be4b2315a900"

//! moment.js
//! version : 2.10.6
//! authors : Tim Wood, Iskren Chernev, Moment.js contributors
//! license : MIT
//! momentjs.com
!function(a,b){"object"==typeof exports&&"undefined"!=typeof module?module.exports=b():"function"==t
y
…
```

How to fix vulnerabilities

- upgrade Moment.js to the latest stable version.

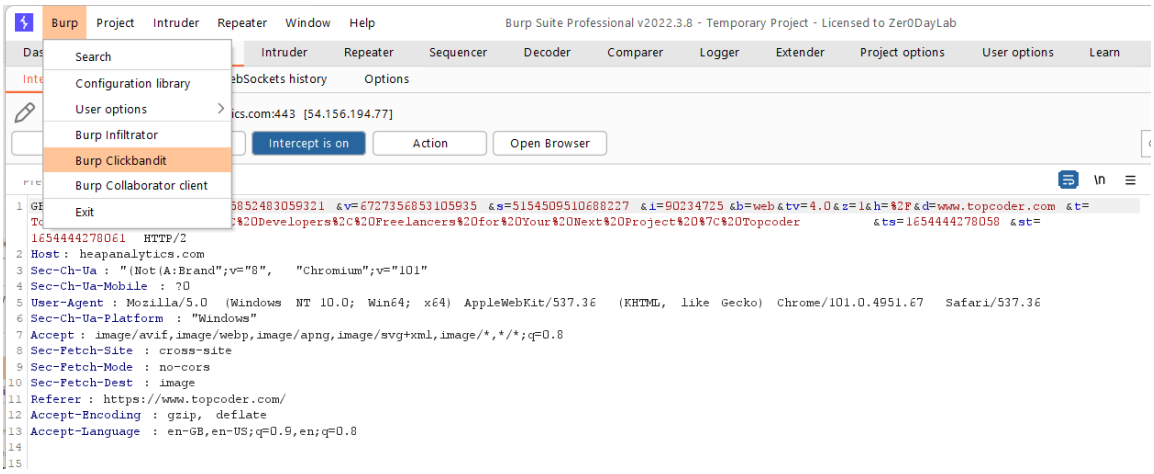
Manual testing

I use this domain-“ https://www.topcoder.com **“for manual testing.** I try do **click jacking** attack.

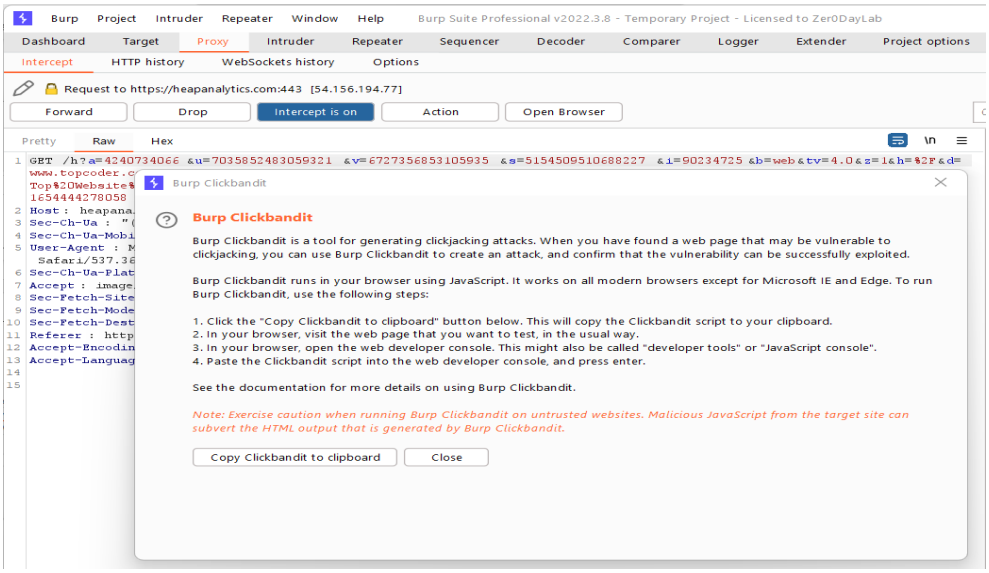
Using burp suite tool

- A clickjacking assault occurs when a user is fooled into clicking a hidden or disguised website element. As a result, users may unintentionally download malware, visit risky websites, provide passwords or personal information, transmit money, or make online purchases.

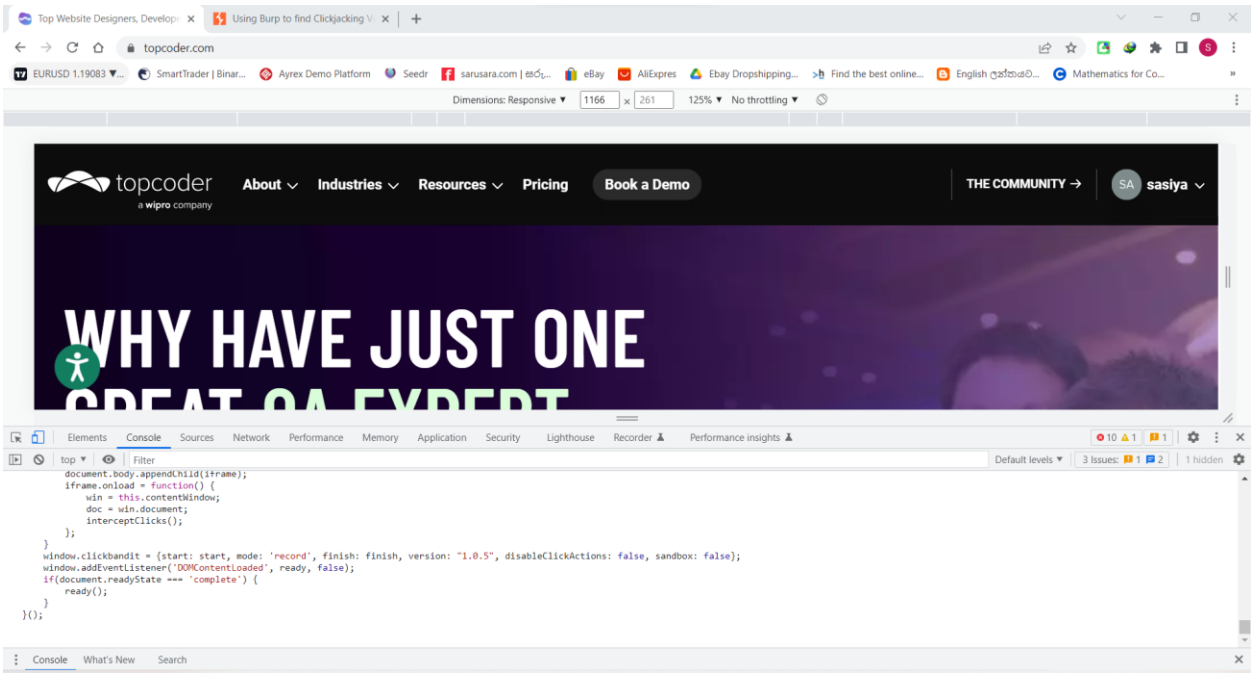
First we need to go **Burp** option and click the **Burp Clickbandit** option.



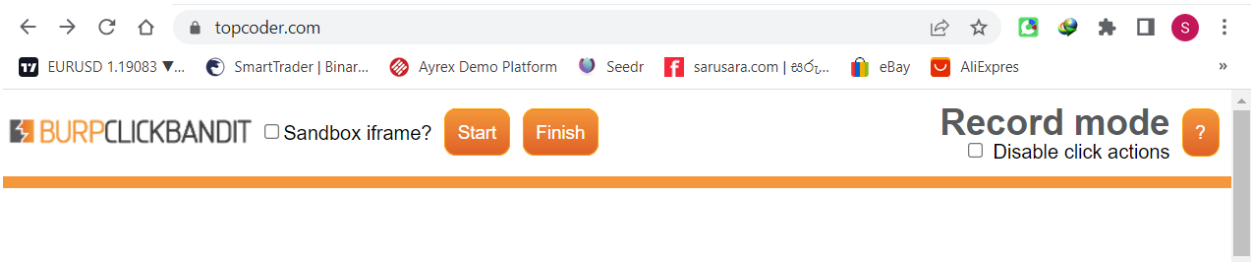
Then click **Copy Clickbandit to Clipboard.**



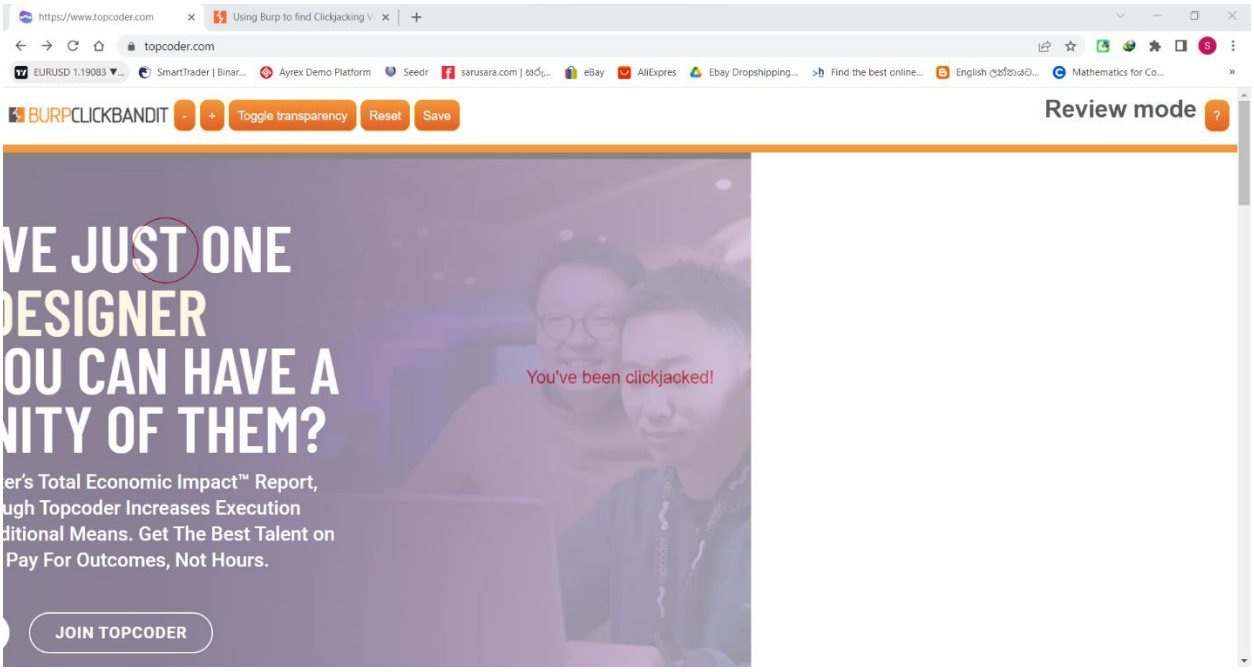
After copying clickbandit. Go to the topcoder.com and go to the console and paste it. now hit Enter.



Then click **start**



Now we can see this result. This website is not secure site for click jacking.



Conclusion

I choose Topcoder.com web domain from HackerOne platform. First, I gather some information about topcoder, and I used tools like Nikto, Who.is, etc. after I analyzed that information. I scan Topcoder domain with using Netspaker, Nikto, and Nmap. Overall, they have good security defenses.