

Sri Lanka Institute of Information Technology



**Sri Lanka Institute of
Information Technology**

IE2072 – WEB SECURITY

Year 2, Semester 2

(Assignment – Individual)-2023

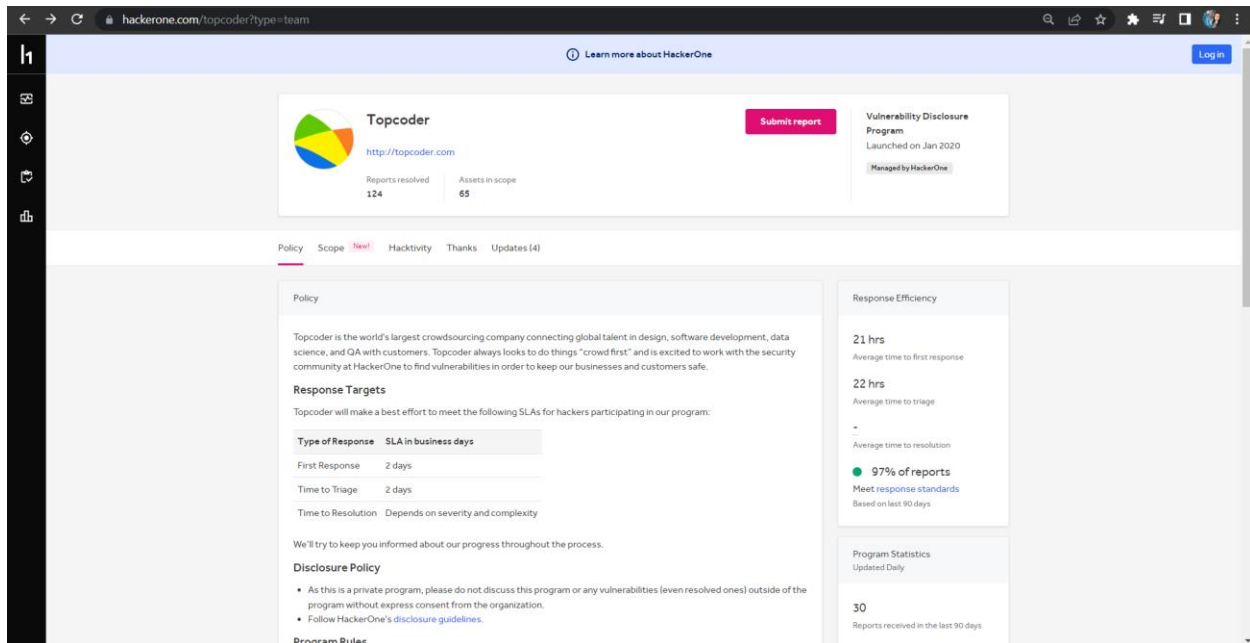
Bug Bounty vulnerability scanning Report 8

Student Register Number	Student Name
IT21167096	DE ZOYSA A.S.

Topcoder

- **Overview**

Topcoder is a crowdsourcing business with a large, open worldwide community of coders, data scientists, and designers. For their efforts on the projects, community members are paid by Topcoder, which also charges corporate, mid-sized, and small-business clients for community services.



Scope of the security audit according <http://topcoder.com/> is as follows,



































- Assessment Scope

In Scope

- ✓ accounts-auth0.topcoder.com
- ✓ accounts.topcoder.com
- ✓ api.topcoder.com
- ✓ app.topcoder.com
- ✓ apps.topcoder.com
- ✓ arena.topcoder.com
- ✓ blockchain.topcoder.com
- ✓ bugzilla.topcoder.com
- ✓ challenges.topcoder.com
- ✓ cmap.topcoder.com
- ✓ cognitive.topcoder.com
- ✓ community-app.topcoder.com
- ✓ community.topcoder.com
- ✓ connect.topcoder.com
- ✓ crowdsourcing.topcoder.com
- ✓ dashboards.topcoder.com
- ✓ demo.topcoder.com
- ✓ dev1.topcoder.com
- ✓ dna.topcoder.com
- ✓ enterprise.topcoder.com
- ✓ facedetection.topcoder.com
- ✓ faceid.topcoder.com
- ✓ feeds.topcoder.com
- ✓ forums.topcoder.com
- ✓ go.topcoder.com
- ✓ hfgeoloc.topcoder.com
- ✓ idolondemand.topcoder.com
- ✓ innovation.topcoder.com
- ✓ ios.topcoder.com
- ✓ lauscher.topcoder.com
- ✓ leaderboards.topcoder.com

- ✓ members.topcoder.com
- ✓ morgoth.topcoder.com
- ✓ namedentity.topcoder.com
- ✓ pam-wind-dash.topcoder.com
- ✓ pins-dash.topcoder.com
- ✓ quantum.topcoder.com
- ✓ radiological.topcoder.com
- ✓ ragnar.topcoder.com
- ✓ scavengerhunt.topcoder.com
- ✓ software.topcoder.com
- ✓ solutions.topcoder.com
- ✓ spacenet.topcoder.com
- ✓ spacenet2.topcoder.com
- ✓ status.topcoder.com
- ✓ studio.topcoder.com
- ✓ submission-review-api.topcoder.com
- ✓ submission-review.topcoder.com
- ✓ success.topcoder.com
- ✓ tco12.topcoder.com
- ✓ tco15.topcoder.com
- ✓ tco16.topcoder.com
- ✓ tco17.topcoder.com
- ✓ tco18.topcoder.com
- ✓ tco19.topcoder.com
- ✓ textsummarization.topcoder.com
- ✓ vanilla.topcoder-dev.com
- ✓ veterans.topcoder.com
- ✓ vpn.topcoder.com
- ✓ webhooks.topcoder.com
- ✓ wordpress-move.topcoder.com
- ✓ wordpress.topcoder.com
- ✓ www.topcoder.com
- ✓ x.topcoder.com
- ✓ zurich.topcoder.com

hfgeoloc.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
idolondemand.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
innovation.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
ios.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
lauscher.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
leaderboards.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
members.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
morgoth.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
namedentity.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
pam-wind-dash.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
pins-dash.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
quantum.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
radiological.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
ragnar.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
scavengerhunt.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
software.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
solutions.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible
stargate.topcoder.com	Domain	In scope	<div><div></div></div> Critical	\$ Ineligible

cmap.topcoder.com	Domain	In scope	 Critical	 Ineligible
cognitive.topcoder.com	Domain	In scope	 Critical	 Ineligible
community-app.topcoder.com	Domain	In scope	 Critical	 Ineligible
community.topcoder.com	Domain	In scope	 Critical	 Ineligible
connect.topcoder.com	Domain	In scope	 Critical	 Ineligible
crowdsourcing.topcoder.com	Domain	In scope	 Critical	 Ineligible
dashboards.topcoder.com	Domain	In scope	 Critical	 Ineligible
demo.topcoder.com	Domain	In scope	 Critical	 Ineligible
dev1.topcoder.com	Domain	In scope	 Critical	 Ineligible
dna.topcoder.com	Domain	In scope	 Critical	 Ineligible
enterprise.topcoder.com	Domain	In scope	 Critical	 Ineligible
facedetection.topcoder.com	Domain	In scope	 Critical	 Ineligible
faceid.topcoder.com	Domain	In scope	 Critical	 Ineligible
feeds.topcoder.com	Domain	In scope	 Critical	 Ineligible
forums.topcoder.com	Domain	In scope	 Critical	 Ineligible
go.topcoder.com	Domain	In scope	 Medium	 Ineligible
hfgeoloc.topcoder.com	Domain	In scope	 Critical	 Ineligible

solutions.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
spacenet.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
spacenet2.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
status.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
studio.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
submission-review-api.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
submission-review.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
success.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
tco12.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
tco15.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
tco16.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
tco17.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
tco18.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
tco19.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
textsummarization.topcoder.com	Domain	In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
vanilla.topcoder-dev.com Topcoder is migrating from it's legacy forums to Vanilla forms . This is our development instance. Forums are used as general discussion as well as part of each individual challenge on Topcoder. Please use your hackerone email accounts when you create a topcoder account. Because this is dev, you will need to create a new account. Your account on prod will not work in this environment.				
Domain		In scope	<div><div></div></div> Critical	<div><div></div></div> Ineligible
<div> <div>Amazon AWS WAF</div> <div>Auth0</div> <div>JavaScript</div> <div>PHP</div> </div>				

Out Of Scope

- ✓ 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
- ✓ x-receiver.topcoder.com

Out Of Scope

Out of Scope:

- 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
- x-receiver.topcoder.com



Other

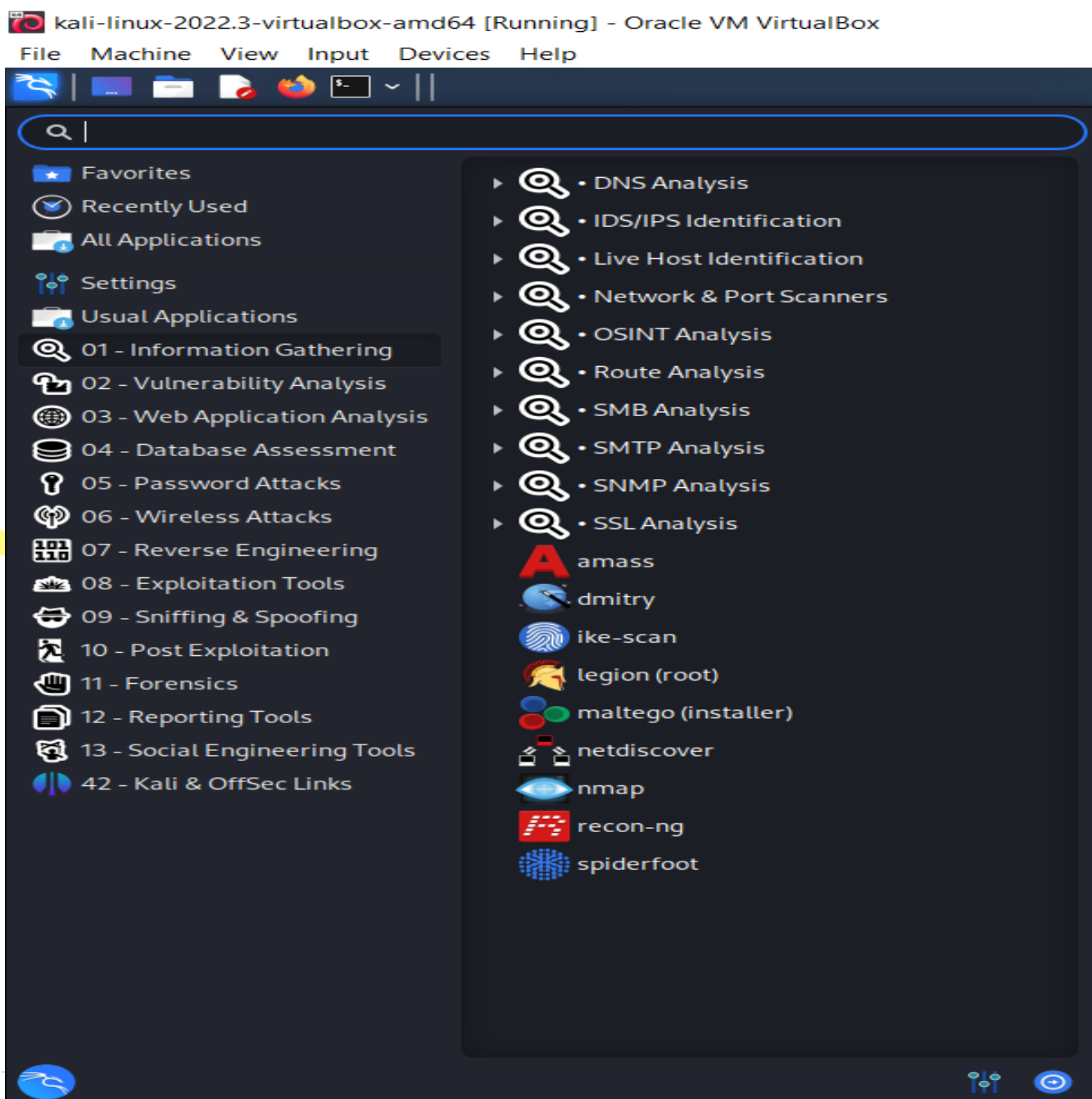
Out of scope

None

Ineligible

- Information gathering

It is the process of collecting data from many sources for a range of purposes. Learning to create efficient information-gathering techniques will benefit studying in a variety of ways. Effective information collecting involves making better use of time, fostering critical thinking through the use of shifting/sorting strategies, and enlarging one's perspective and topic knowledge through the investigation of new sources. Additionally, obtaining knowledge may be useful for a number of purposes, but the major advantage in terms of academic studies is that one will become aware of more varied sources, viewpoints, and techniques that can improve one's academic work.



- Subdomains for Hunting

Sub-domain enumeration is the process of listing sub-domains for one or more domains. In the process of reconnaissance, it's a crucial phase. Sub-domain enumeration can reveal several domains and sub-domains that are included in a security assessment, which increases the chance of finding vulnerabilities.

Finding applications using cryptic, abandoned sub-domains may reveal serious bugs.

Within a single company, the same vulnerabilities are routinely discovered across many domains and applications.

What is Knockpy?

With only a few lines of code, knockpy's python version of the knockoffs framework makes it simple to use knockoff-based inference. The modular design of Knockpy makes it simple for researchers and analysts to add features on top of it.

- searching subdomain by knockpy,

Knockpy is a portable and flexible Python3 utility that uses passive reconnaissance and dictionary scanning to swiftly enumerate subdomains on a specified domain.

How to Find Subdomain in Knockpy: `knockpy <Domain Name>`

```

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ knockpy topcoder.com

Knockpy v6.1.0

local: 10757 | remote: 167

Wordlist: 10924 | Target: topcoder.com | Ip: 44.199.67.13

06:28:09

Ip address      Code Subdomain      Server      Real hostname
-----
52.84.251.77    200 academy.topcoder.com    AmazonS3
13.224.249.97   200 accounts-auth0.topcoder.com AmazonS3
13.33.88.69     403 admin.topcoder.com      CloudFront
34.224.235.88   200 accounts.topcoder.com     AmazonS3
13.33.33.7      200 arena.topcoder.com        CloudFront
52.21.102.148   200 api.topcoder.com          nginx
34.224.235.88   200 apps.topcoder.com          nginx
54.84.134.104   400 arenaws.topcoder.com
34.224.235.88   403 app.topcoder.com         nginx
44.199.67.13    503 beta.topcoder.com        awselb/2.0    topcoder.com
52.21.102.148   404 analytics.topcoder.com
  
```

File	Actions	Edit	View	Help
44.199.67.13	503	beta.topcoder.com	awselb/2.0	topcoder.com
52.21.102.148	404	analytics.topcoder.com		
54.91.6.89	503	bugzilla.topcoder.com	Cowboy	rigid-honeysuckle-fdzd0s5z0bq8c2q1438u1y5u.herokuapp.com
18.232.192.139	200	blockchain.topcoder.com		
104.18.102.2	200	auth.topcoder.com	nginx	topcoder-cd-khkhjjudojdapubd.edge.tenants.auth0.com
54.221.251.148	200	challenge-comparison.topcoder.com	nginx	infinite-passionflower-02ty105bmij5tmc5jzgm6maz.herokuapp.com
52.84.251.68	200	challenges.topcoder.com		
44.214.68.32	404	certificate.topcoder.com		d-y8czowe2t3.execute-api.us-east-1.amazonaws.com
104.16.82.103	200	auth-prod.topcoder.com	nginx	tc-prod-cd-s8jjfxxrr5vidaca.edge.tenants.us.auth0.com
104.16.83.103	200	auth-dev.topcoder.com	nginx	tc-dev-cd-ff3ulxocaopmcl5j.edge.tenants.us.auth0.com
104.16.82.103	200	auth-qa.topcoder.com	nginx	tc-qa-cd-cxctwmvhtj7muip.edge.tenants.us.auth0.com
54.221.251.148	200	cmap.topcoder.com	Apache	lit-brushlands-ley0jqnnokopclycarl270u.herokuapp.com
34.224.235.88	200	cognitive.topcoder.com		
18.232.192.139	200	comcast.topcoder.com		
34.224.235.88	200	community-app.topcoder.com		
13.33.88.21	404	community-app-cdn.topcoder.com	CloudFront	dlxczxtayxv6.cloudfront.net
13.33.33.49	200	connect.topcoder.com	AmazonS3	do9e0l7aspc2o.cloudfront.net
52.21.102.148	200	community.topcoder.com	nginx	
104.16.53.111	409	csheip.topcoder.com	cloudflare	topcoder.zendesk.com
40.99.10.72	200	autodiscover.topcoder.com		autod.ms-acdc-autod.office.com
44.199.67.13	200	crowdsourcing.topcoder.com	nginx	www.topcoder.com
54.91.6.89	200	dashboards.topcoder.com	Apache	descriptive-pandsy-7jwdfqcnkqai7c88cjo25ow.herokuapp.com
52.21.102.148		coder.topcoder.com		
54.157.58.70	200	dna.topcoder.com	Apache	morning-loquat-7rkf8rhkk3wmpy78zq0i8y3x.herokuapp.com
3.232.242.170	200	dpeak-dash.topcoder.com	Apache	philosophical-tern-g3w98hv54rsdzbvb4h6vgppv.herokuapp.com
52.21.102.148	200	discussions.topcoder.com	Apache/2.4.29 (Ubuntu)	
54.173.154.8		dev1.topcoder.com		
54.192.150.103		internal-api.topcoder.com		d1jn0zr6nijn2.cloudfront.net
54.91.59.199	200	internal-mm-leaderboard.topcoder.com	Cowboy	pointy-rabbit-g7pd8qfj98ztetj2xotp3rs2.herokuapp.com
52.21.102.148	200	ios.topcoder.com	nginx	
54.196.16.164	200	innovation.topcoder.com	Cowboy	innovation.topcoder.com.herokuapp.com
54.157.4.65	200	lauscher.topcoder.com	Cowboy	lauscher.topcoder.com.herokuapp.com

```

File Actions Edit View Help
54.157.4.65 200 lauscher.topcoder.com Cowboy lauscher.topcoder.com.herokudns.com
34.224.235.88 404 link.topcoder.com nginx
18.235.133.129 200 marketing3.topcoder.com nginx/1.14.0 (Ubuntu)
54.157.4.65 200 morgoth.topcoder.com Apache gentle-crane-jj5pvf1jaqjbbjpfax2wi6d6.herokudns.com
52.84.251.36 mm.topcoder.com gf5gcxgfwc.execute-api.us-east-1.amazonaws.com
18.232.192.139 500 mobile.topcoder.com
54.85.218.55 members.topcoder.com
3.220.57.224 200 namedentity.topcoder.com Apache graceful-moth-wjmjstbnc3r5tryxt92t5v.herokudns.com
34.201.80.84 200 nist.topcoder.com Apache shrouded-stegosaurus-uyj10gj3bmfk6q9tlb38wq73.herokudns.com
52.20.78.240 200 pam-wind-dash.topcoder.com Apache flat-chamber-ez6y4b88v8dh7z2m2blx243w.herokudns.com
18.232.192.139 platform.topcoder.com
52.21.102.148 platform-ui.topcoder.com
3.232.242.170 pins-dash.topcoder.com cubed-marsupial-o2n7cdxl6pp8rfmw0ulibdxu.herokudns.com
52.21.102.148 payment.topcoder.com
54.161.241.46 200 spacenet.topcoder.com Apache cryptic-triceratops-rg8zfwy700mq2p9xzac6v2.herokudns.com
34.204.219.77 smtp.topcoder.com
52.215.192.133 200 status.topcoder.com 27w69fm2z8mn.stspg-customer.com
34.224.235.88 503 studio.topcoder.com awselb/2.0
52.21.102.148 200 staging-community-app.topcoder.com
18.232.192.139 404 submission-review-api.topcoder.com
54.162.128.250 200 taascalc.topcoder.com Cowboy clear-vulture-plobu2fk5y4i7cz4aqsnsejx.herokudns.com
54.192.150.59 403 tc-public-static-files.topcoder.com AmazonS3
13.224.249.37 403 tca.topcoder.com AmazonS3
52.21.102.148 200 software.topcoder.com AmazonS3
44.199.67.13 200 solutions.topcoder.com nginx www.topcoder.com
44.199.67.13 200 success.topcoder.com nginx www.topcoder.com
34.224.235.88 200 submission-review.topcoder.com
52.21.102.148 200 tco08.topcoder.com
52.21.102.148 200 tco10.topcoder.com
52.21.102.148 200 tco11.topcoder.com
18.232.192.139 200 tco19.topcoder.com
52.21.102.148 200 tco23.topcoder.com

```



```

kali@kali: ~
File Actions Edit View Help
52.21.102.148 200 tco08.topcoder.com
52.21.102.148 200 tco10.topcoder.com
52.21.102.148 200 tco11.topcoder.com
18.232.192.139 200 tco19.topcoder.com
52.21.102.148 200 tco23.topcoder.com
52.21.102.148 200 tco21.topcoder.com
3.220.57.224 200 textsummarization.topcoder.com Apache primal-cassava-hp8k12lrzjz7vhrtrtq7y7max.herokudns.com
54.86.140.82 studio.qa.topcoder.com
52.21.102.148 200 tco17.topcoder.com
34.224.235.88 200 tco15.topcoder.com
18.232.192.139 200 tco14.topcoder.com
34.224.235.88 200 tco20.topcoder.com
52.21.102.148 200 tco22.topcoder.com
34.224.235.88 200 test-wp.topcoder.com nginx/1.14.0 (Ubuntu)
18.232.192.139 200 tco12.topcoder.com
34.224.235.88 200 tco13.topcoder.com
34.224.235.88 200 tco01.topcoder.com
34.234.203.85 200 tunnel1.topcoder.com nginx
18.232.192.139 200 tco18.topcoder.com
18.232.192.139 200 tco16.topcoder.com
52.84.251.68 403 uni-nav.topcoder.com AmazonS3
18.232.192.139 200 uninav.topcoder.com nginx/1.14.0 (Ubuntu)
18.232.192.139 200 topgear.topcoder.com nginx
34.201.80.84 503 vorbote.topcoder.com Cowboy vorbote.topcoder.com.herokudns.com
34.224.235.88 200 veterans.topcoder.com
54.91.6.89 503 webhooks.topcoder.com Cowboy webhooks.topcoder.com.herokudns.com
52.84.251.20 200 work.topcoder.com AmazonS3
44.199.67.13 200 www.topcoder.com nginx
52.21.102.148 404 x-receiver.topcoder.com
54.227.217.39 200 wordpress-move.topcoder.com nginx
54.227.217.39 200 wordpress.topcoder.com nginx
34.224.235.88 200 zurich.topcoder.com nginx

```

```
52.21.102.148 404 x-receiver.topcoder.com
54.227.217.39 200 wordpress-move.topcoder.com      nginx
54.227.217.39 200 wordpress.topcoder.com          nginx
34.224.235.88 200 zurich.topcoder.com              nginx
52.21.65.101  vpn.topcoder.com
18.232.192.139 200 x.topcoder.com
```

06:36:37

Ip address: 93 | Subdomain: 101 | elapsed time: 00:08:27

```
(kaliⓈkali)-[~]
$
```


- Open Ports Enumeration

A port that is open is one that is actively receiving TCP or UDP packets. A port is in use and can't be utilized for anything else if a service demands it. If the services using open ports are misconfigured, unpatched, or insecure, then there is a security risk.

APPLYING NMAP

```
(kali㉿kali)-[~]  
$ sudo nmap -sS topcoder.com  
[sudo] password for kali:  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-28 03:43 EDT  
Nmap scan report for topcoder.com (44.199.67.13)  
Host is up (0.030s latency).  
rDNS record for 44.199.67.13: ec2-44-199-67-13.compute-1.amazonaws.com  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp   open  https  
5003/tcp  open  filemaker  
  
Nmap done: 1 IP address (1 host up) scanned in 21.17 seconds
```

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https
5003/tcp	open	filemaker

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https
5003/tcp	open	filemaker

A port that is open is one that is actively receiving TCP or UDP packets. A port is in use and cannot be used for anything else if a service uses it. Open ports offer a security risk if the services operating on them are improperly configured, unsecure, or unpatched.

Using Nmap to List Open Ports

The most popular port security network scanner in the world is called Nmap. You may assess the efficacy of your firewall and security settings with the help of the Nmap hosted security tool.

Checking for Vulnerabilities using NIKTO

A security program called the Nikto web server scanner scans a website for thousands of possible security holes. This includes malicious files, services that have been set up improperly, vulnerable scripts, and other issues. It was created using plugins and is open source to allow for feature expansion. New security checks are frequently added to these plugins through regular updates. Many penetration testers and security analysts maintain the famous Nikto Web Vulnerability Scanner in their toolkit. It typically unearths valuable data about a web server or website that may be used for subsequent exploitation or vulnerability analysis.

```
(kali@kali)-[~]
$ sudo nikto -h topcoder.com
- Nikto v2.5.0

+ Target IP:      44.199.67.13
+ Target Hostname: topcoder.com
+ Target Port:    80
+ Start Time:     2023-05-28 03:47:47 (GMT-4)

+ Server: nginx
+ Root page / redirects to: https://topcoder.com/
+ : Server banner changed from 'nginx' to 'awselb/2.0'.
+ /kwrL5Ksd.log: 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 MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7963 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:      2023-05-28 04:30:21 (GMT-4) (2554 seconds)

+ 1 host(s) tested
```

```
(kali㉿kali)-[~]  
$ sudo nikto -h 44.199.67.13  
[sudo] password for kali:  
- Nikto v2.5.0  
  
+ Target IP: 44.199.67.13  
+ Target Hostname: 44.199.67.13  
+ Target Port: 80  
+ Start Time: 2023-05-28 04:43:49 (GMT-4)  
  
+ Server: awselb/2.0  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: 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 MIME type.  
See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ 8102 requests: 0 error(s) and 2 item(s) reported on remote host  
+ End Time: 2023-05-28 05:26:05 (GMT-4) (2536 seconds)  
  
+ 1 host(s) tested
```

Scanned Vulnerabilities Using Netsparker

1) Out-of-date version(jQuery)

The screenshot displays the Netsparker 5.8.1.28119 interface. The main window shows a vulnerability report for 'Out-of-date Version (jQuery)' on the URL <https://www.topcoder.com/>. The risk level is categorized as 'MEDIUM'. The report details the identified version (3.3.1) and the latest version (3.7.0). It also provides a classification of the vulnerability based on various standards like PCI DSS 3.2, OWASP 2013, and OWASP 2017. The impact states that since this is an old version of the software, it may be vulnerable to attacks. The remedy suggests upgrading the installation of jQuery to the latest stable version. A link to 'Downloading jQuery' is provided under the 'Remedy References' section. The left sidebar shows a list of other detected issues, and the right sidebar shows a knowledge base with various categories like AJAX / XML HTTP Requests, Comments, Cookies, etc.

Risk type : Medium

URL : <https://www.topcoder.com/>

Identified Version : 3.3.1

Latest Version : 3.7.0 (in this branch)

Vulnerability Database : Result is based on 05/23/2023 20:30:00 vulnerability database content.

• Vulnerability Details

Netsparker identified the target web site is using jQuery and detected that it is out of date

- **Impact**

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

- **Remedy**

Please upgrade your installation of jQuery to the latest stable version.

Remedy References : Downloading jQuery

- **Known Vulnerabilities in this Version**

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions : 1.9.0 to 3.4.1

External References : CVE-2020-11023

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions : 1.9.0 to 3.4.1

External References : CVE-2020-11022

jQuery Prototype Pollution Vulnerability

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Affected Versions : 1.0 to 3.3.1

External References : CVE-2019-11358

2) HTTP Strict Transport Security(HSTS)Errors and Warnings

The screenshot shows the Netsparker 5.8.1.28119 interface. The main window displays the title 'HTTP Strict Transport Security (HSTS) Errors and Warnings' with a 'MEDIUM' risk level. Below the title, it shows the 'Certainty' as 'High' and the 'URL' as 'https://www.topcoder.com/'. A table lists the classification of the error, including OWASP 2013, OWASP 2017, CWE, WASC, and ISO27001. The 'Error' and 'Resolution' table shows the error 'preload directive not present' and the resolution 'Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS)'. The 'Vulnerability Details' section states 'Netsparker detected errors during parsing of Strict-Transport-Security header.' and the 'Impact' section states 'The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.'

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

Classification	Score
OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ISO27001	A.14.1.2

Vulnerability Details
Netsparker detected errors during parsing of Strict-Transport-Security header.

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

Risk type : Medium

URL : https://www.topcoder.com/

Error : preload directive not present

Resolution : Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

• Vulnerability Details

Netsparker detected errors during parsing of Strict-Transport-Security header.

- **Impact**

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

- **Remedy**

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

- Serve a valid certificate

If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:

In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists

- Serve an HSTS header on the base domain for HTTPS requests:

- ✚ The max-age must be at least 31536000 seconds (1 year)
- ✚ The includeSubDomains directive must be specified
- ✚ The preload directive must be specified
- ✚ If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

3) Weak Ciphers Enabled

Weak Ciphers Enabled

CONFIRMED MEDIUM

URL : <https://www.topcoder.com/>

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)

Vulnerability Details

Netsparker detected that weak ciphers are enabled during secure communication (SSL). You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

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

Actions to Take

For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

CLASSIFICATION

PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

Risk type : Medium

URL : <https://www.topcoder.com/>

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)

- **Vulnerability Details**

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

- **Impact**

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

- **Actions to Take**

For Apache, you should modify the SSLCipherSuite directive in the httpd.conf. SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4Lighttpd: ssl.honor-cipher-order = "enable"

ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM" For Microsoft IIS, you should make some changes to the system registry. Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.

a. Click Start, click Run, type regedit32 or type regedit, and then click OK.

b. In Registry Editor, locate the following registry key:

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

c. Set "Enabled" DWORD to "0x0" for the following registry keys:

SCHANNEL\Ciphers\DES 56/56 SCHANNEL\Ciphers\RC4
64/128 SCHANNEL\Ciphers\RC4 40/128 SCHANNEL\Ciphers\RC2
56/128 SCHANNEL\Ciphers\RC2 40/128 SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5Remedy

Configure your web server to disallow using weak ciphers.

4) Misconfigured Access-Control-Allow-Origin Header

The screenshot displays the Netsparker web application security scanner interface. The main window shows a vulnerability report for the 'Misconfigured Access-Control-Allow-Origin Header' on the URL `https://www.topcoder.com/wp-json/`. The severity is classified as 'LOW'. The report details the 'Access-Control-Allow-Origin' header value as `http://r87.com` and includes a note explaining that `Access-Control-Allow-Credentials` is set to true, which allows cross-domain requests and responses to be read. The 'Vulnerability Details' section describes Cross-Origin Resource Sharing (CORS) and its security implications. The 'Impact' section states that this is generally inappropriate when using the same-origin security policy. The 'Remedy' section provides guidance on when this configuration might be appropriate. The left sidebar shows a list of other detected issues, and the right sidebar lists various site analysis metrics.

Misconfigured Access-Control-Allow-Origin Header
LOW

Certainty : [REDACTED]
URL : <https://www.topcoder.com/wp-json/>
Access-Control-Allow-Origin : <http://r87.com>
Note : Access-Control-Allow-Credentials is set to true which means credentials are sent via cross-domain requests and response can be read. If this is not intended, you can send this header for only trusted third parties.

Vulnerability Details

Netsparker detected a possibly misconfigured Access-Control-Allow-Origin header in resource's HTTP response.

Cross-origin resource sharing (CORS) is a mechanism that allows resources on a web page to be requested outside the domain through XMLHttpRequest.

Unless this HTTP header is present, such "cross-domain" requests are forbidden by web browsers, per the same-origin security policy.

Impact

This is generally not appropriate when using the same-origin security policy. The only case where this is appropriate when using the same-origin policy is when a page or API response is considered completely public content and it is intended to be accessible to everyone.

Remedy

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ISO27001	A.14.12

Risk type : Low

URL : <https://www.topcoder.com/wp-json/>

Access-Control-Allow-Origin : <http://r87.com>

Note : Access-Control-Allow-Credentials is set to true which means credentials are sent via cross-domain requests and response can be read. If this is not intended, you can send this header for only trusted third parties.

- **Vulnerability Details**

Netsparker detected a possibly misconfigured Access-Control-Allow-Origin header in resource's HTTP response.

Cross-origin resource sharing (CORS) is a mechanism that allows resources on a web page to be requested outside the domain through XMLHttpRequest.

Unless this HTTP header is present, such "cross-domain" requests are forbidden by web browsers, per the same-origin security policy.

- **Impact**

This is generally not appropriate when using the same-origin security policy. The only case where this is appropriate when using the same-origin policy is when a page or API response is considered completely public content and it is intended to be accessible to everyone.

- **Remedy**

If this page is intended to be accessible to everyone, you don't need to take any action. Otherwise please follow the guidelines for different architectures below in order to set this header and permit outside domain.

Apache

Add the following line inside either the <directory>, <location>, <files> or <virtualhost> sections of your server config (usually located in httpd.conf or apache.conf), or within a .htaccess file. Header set Access-Control-Allow-Origin "domain"

IIS6

Open Internet Information Service (IIS) Manager

Right click the site you want to enable CORS for and go to Properties

Change to the HTTP Headers tab

In the Custom HTTP headers section, click Add

Enter Access-Control-Allow-Origin as the header name

Enter domain as the header value

IIS7

Merge the following xml into the web.config file at the root of your application or site:<?xml version="1.0" encoding="utf-8" ?>

```
<configuration>
  <system.webserver>
    <httpprotocol>
      <customheaders>
        <add name="Access-Control-Allow-Origin" value="domain" />
      </customheaders>
    </httpprotocol>
  </system.webserver>
</configuration>
```

ASP.NET

If you don't have access to configure IIS, you can still add the header through ASP.NET by adding the following line to your source pages:Response.AppendHeader("Access-Control-Allow-Origin", "domain");

5) Cookie Not Marked as HttpOnly

The screenshot displays the Netsparker web application security scanner interface. The main window shows a vulnerability report titled "Cookie Not Marked as HttpOnly" for the target URL "https://www.topcoder.com/". The report is marked as "CONFIRMED" and "LOW" severity. The identified cookies are "_conv_v", "_conv_s", "_gd_visitor", and "_gd_session", all sourced from JavaScript. The vulnerability details explain that HTTPOnly cookies cannot be read by client-side scripts, and not marking them as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks. The impact states that during a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session. The actions to take suggest marking all cookies as HTTPOnly. The interface also shows a left sidebar with a site map and a right sidebar with a knowledge base.

Risk type : Low

URL : <https://www.topcoder.com/>

Identified Cookie(s) : _conv_v
_conv_s
_gd_visitor
_gd_session

Cookie Source : JavaScript

• Vulnerability Details

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

• Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

- **Actions to Take**

See the remedy for solution.

Consider marking all of the cookies used by the application as HTTPOnly. (After these changes javascript code will not be able to read cookies.)

- **Remedy**

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnel to bypass HTTP Only protection

6) Cookie Not Marked as Secure

The screenshot displays the Netsparker 5.8.1.28119 interface. The main window shows a vulnerability report titled "Cookie Not Marked as Secure" with a classification of "CONFIRMED" and "LOW". The URL is <https://www.topcoder.com/>. The identified cookie(s) are `_conv_v` and `_conv_s`. The cookie source is JavaScript. The vulnerability details state: "Netsparker identified a cookie not marked as secure, and transmitted over HTTPS. This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack." The impact is: "This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (such as a session cookie), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie." The actions to take are: "See the remedy for solution. Mark all cookies used within the application as secure. If the cookie is not related". The classification table lists: PCI DSS 3.2 (6.5.10), OWASP 2013 (A6), OWASP 2017 (A3), CWE (6.14), CAPEC (102), WASC (15), and ISO27001 (A.14.1.2). The CVSS 3.0 SCORE is: Base (2 (Low)), Temporal (2 (Low)), and Environmental (2 (Low)). The CVSS Vector String is: CVSS3.0(AV:P/AC:H/PR:N/UI:N/SU:CL/IN:). The status bar at the bottom shows "Auto save finished successfully - 5/28/2023 02:15:34 PM" and "Crawling & Attacking (2/3) 5%".

URL : <https://www.topcoder.com/>

Identified Cookie(s) : `_conv_v`

`_conv_s`

Cookie Source : JavaScript

• Vulnerability Details

Netsparker identified a cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.

- **Impact**

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (such as a session cookie), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

- **Actions to Take**

See the remedy for solution.

Mark all cookies used within the application as secure. (If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)

- **Remedy**

Mark all cookies used within the application as secure.

- **Required Skills for Successful Exploitation**

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to be understand layer 2, have physical access to systems either as waypoints for the traffic, or have locally gained access to to a system between the victim and the web server.