Web Audit

www.etsy.com

S.A.D.H. Vishwajith
IT19952376

Web Security - IE2062

B.Sc. (Hons) in Information Technology
Specializing Cyber Security

Content

1. Introduction

Under the module Web Security, we have received an assignment “Web Audit”. It was given to us by Ms. Chethana Liyanapathirana to encourage us and improve our knowledge about web security. For this assignment, I have completed a video and this report.

2. Summary

In reconnaissance of etsy.com I found few High and medium level vulnerabilities and issues.

After scanning I Found these high and medium level vulnerabilities

- ✓ Out-of-date Version (Underscore.js)
- ✓ Weak Ciphers Enabled
- ✓ Out-of-date Version (jQuery)
- ✓ Cookie Not Marked as HttpOnly
- ✓ Cookie Not Marked as Secure
- ✓ Insecure Frame (External)
- ✓ [Possible] Cross-site Request Forgery
- ✓ Missing Content-Type Header
- ✓ X-content-type-option

The details of this are given below report.

3. **OWASP top 10 Security Vulnerabilities**

The Open Web Application Protection Project (OPASP) is an online forum that publishes all documents, methods, documentation, resources, and technology in Web Application Security. Its focuses on the most critical threats. And it can also use to show progress over time toward industry-standard security and compliance. Here are OWASP top 10 security vulnerabilities.

1. **Injection**
   An attacker's attempt to send data to an application in such a way that the interpretation of commands sent to an interpreter is changed is known as injection.

2. **Broken authentication**
   It's a catch-all word for several flaws that attackers use to impersonate legitimate users online.

3. **Unstable data exposure**
   If web applications and APIs not protected, personally attributable information data can be hijacked or modified.

4. **External Entities (XXE)**
   Internal files can be transferred, and it can be used to carry out internal port scanning, remote code execution, and DDoS attacks.

5. **Broken Access Control**
   It usually happens when user access controls aren't strictly followed.

6. **Security Misconfiguration**
   It is essential to securely configure and patch all operating systems, frameworks, and to follow best practices suggested.

7. **Cross-Site Scripting (XSS)**

   XSS attacks are injection attacks in which malicious scripts are injected into otherwise trustworthy and innocuous websites.

8. **Insecure Deserialization**

   These bugs can be used to execute replay, injection, and advantage escalation attacks even if remote code execution does not occur.

9. **Using Components with Known Vulnerabilities**

   Operating systems, database servers, web applications, encryption libraries, and other software modules are examples of components.

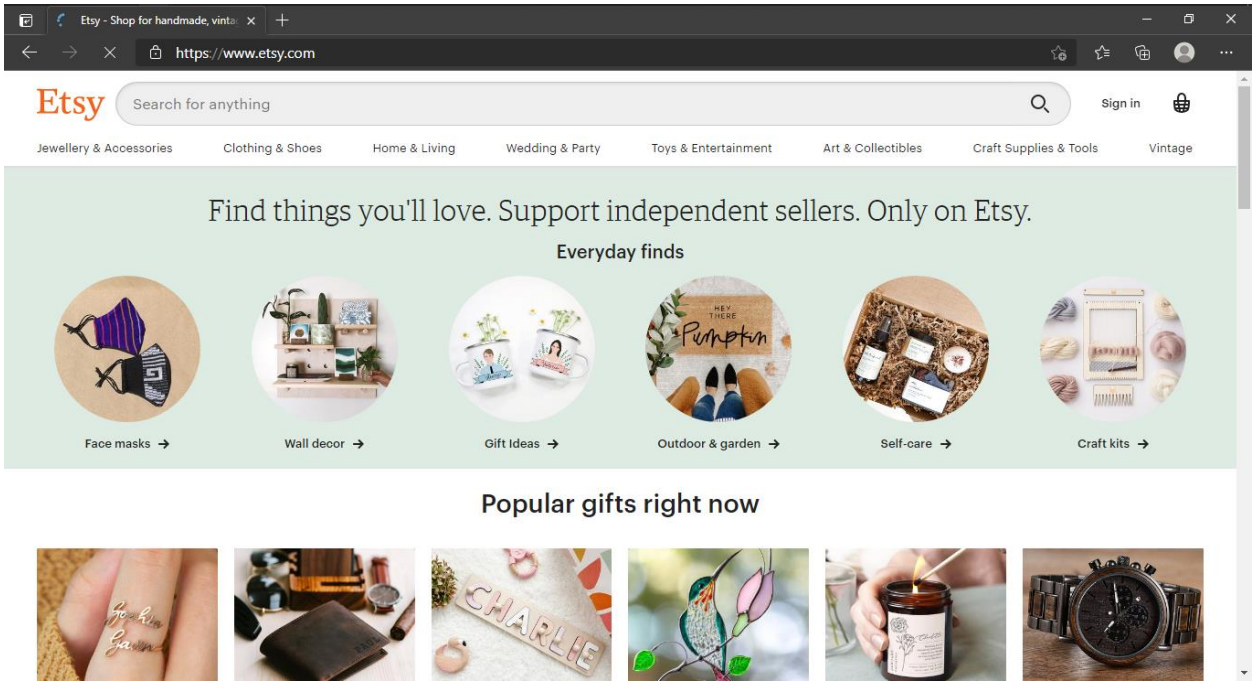
10. **Insufficient Logging and Monitoring**

    Insufficient logging and monitoring may enable attackers to operate undetected within an enterprise, extracting or even destroying critical data.

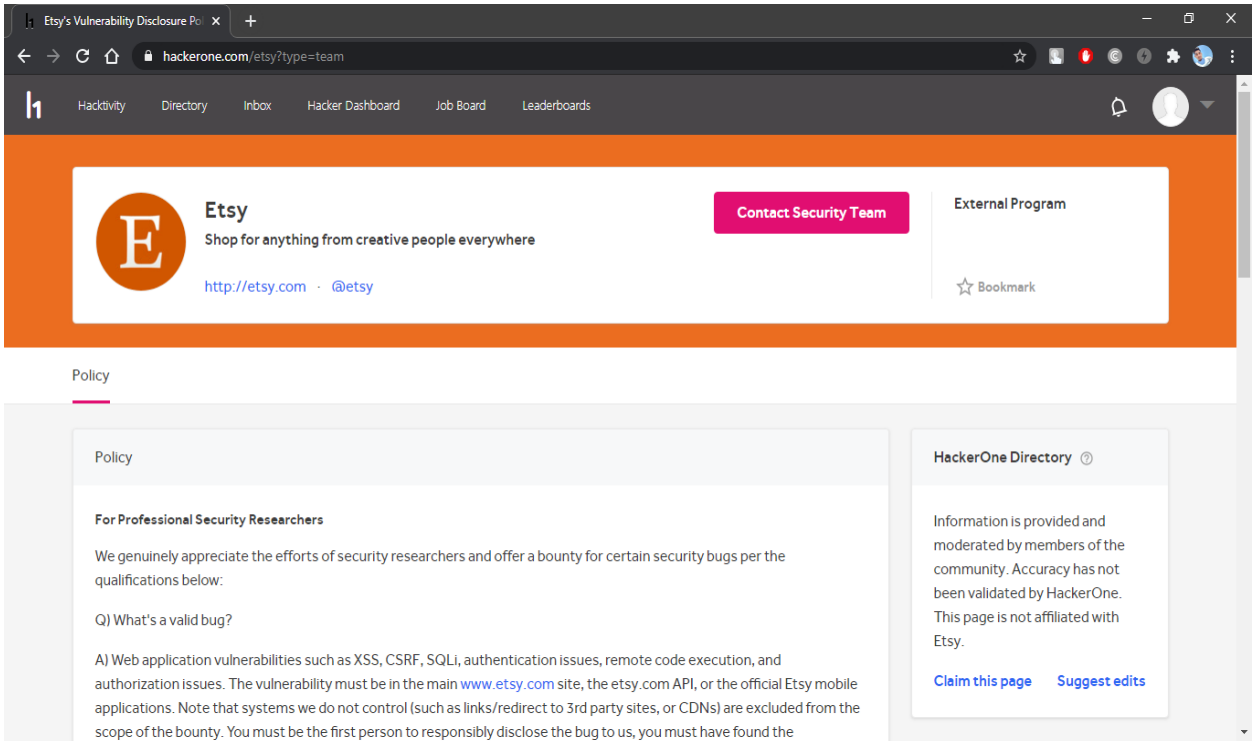
4. Selection of Domain

- **Selected Domain: www.etsy.com**

Most people around the world are interested in buying and selling goods and services online. Etsy is a US e-commerce website devoted to craftsmanship and craftsmanship. Jewelry, bags, clothes, home décor and furniture, toys, paintings, and craft supply and equipment are only a few of the categories in which these pieces can be found. All antique pieces have to be 20 years old or older. Then I proceed to audit the domain for vulnerabilities.



- Check hackerone.com for etsy.com guidelines and policies to get a brief idea about what they expected.



5. Finding Subdomains

Subdomains can contain exploits or bugs that can lead to full website access. However, since the subdomains do not advertise their vulnerabilities, we have no idea what sort of vulnerabilities they have.

There are many subdomain finder tools out there. If you search for a subdomain finder, you will find many tools. Popular tools that are utilized to find subdomains are,

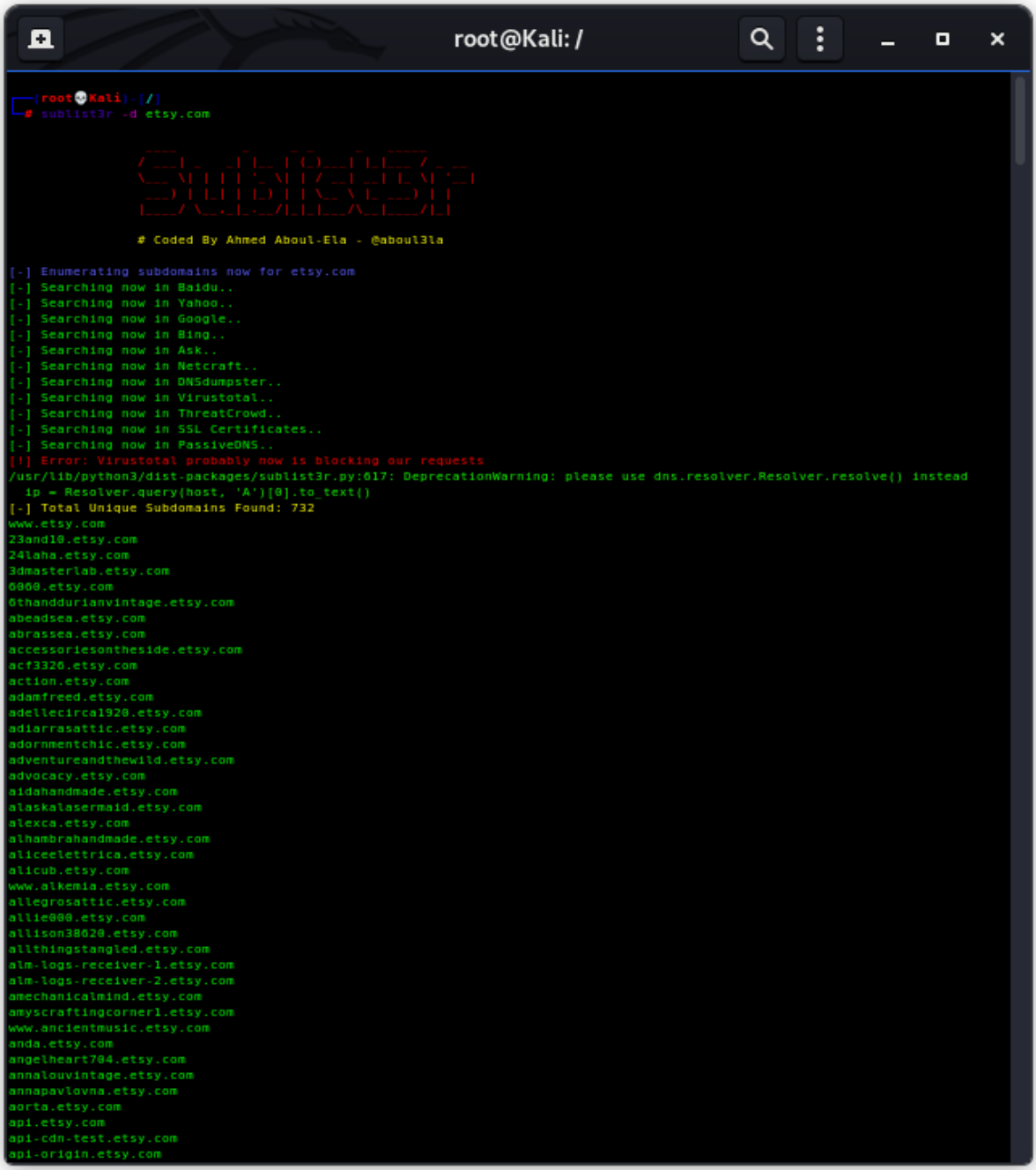
- Sublist3r
- Crt.sh
- Dnscan
- Anubis
- Amass
- Nmap(dns-brute.nse)
- Lepus
- Censys
- Findomain

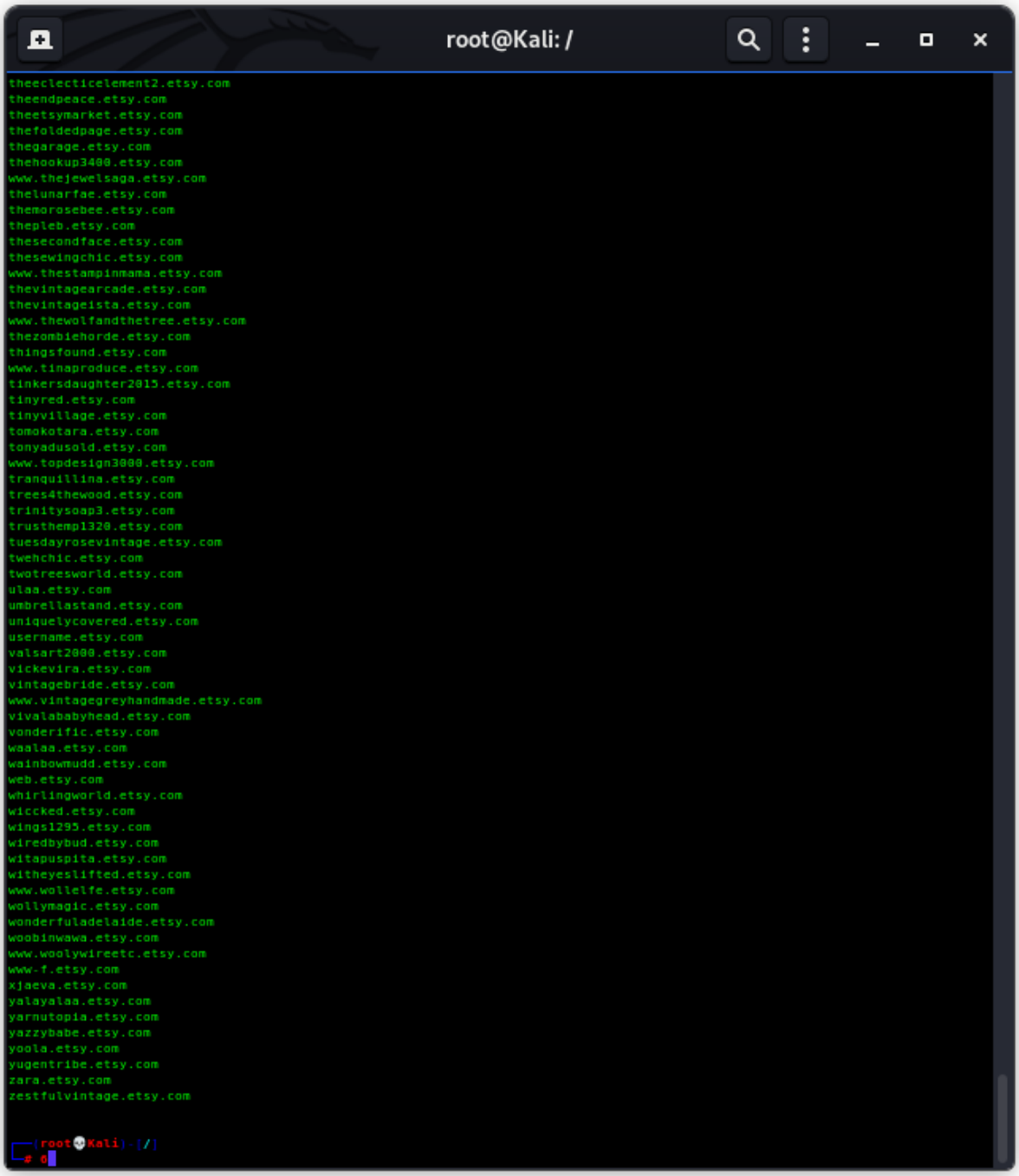
For this project, I used Sublist3r and crt.sh to find subdomains.

5.1. Enumerate Subdomains

5.1.1. Sublist3r

As a result, I found **732 subdomains** for etsy.com using sublist3r tool.




root@Kali: /
theeclecticelement2.etsy.com
theendpeace.etsy.com
theetsymarket.etsy.com
thefoldedpage.etsy.com
thegarage.etsy.com
thehookup3400.etsy.com
www.thejewelsaga.etsy.com
thelunarfae.etsy.com
themorosebee.etsy.com
thepleb.etsy.com
thesecondface.etsy.com
thesewingchic.etsy.com
www.thestampinmama.etsy.com
thevintagearcade.etsy.com
thevintageista.etsy.com
www.thewolfandthetree.etsy.com
thezombiehorde.etsy.com
thingsfound.etsy.com
www.tinaproduce.etsy.com
tinkersdaughter2015.etsy.com
tinyred.etsy.com
tinyvillage.etsy.com
tomokotara.etsy.com
tonyadusold.etsy.com
www.topdesign3000.etsy.com
tranquillina.etsy.com
trees4thewood.etsy.com
trinitysoap3.etsy.com
trusthemp1320.etsy.com
tuesdayrosevintage.etsy.com
twehchic.etsy.com
twotreesworld.etsy.com
ulaa.etsy.com
umbrellastand.etsy.com
uniquelycovered.etsy.com
username.etsy.com
valsart2000.etsy.com
vickevira.etsy.com
vintagebride.etsy.com
www.vintagegreyhandmade.etsy.com
vivalababyhead.etsy.com
vonderific.etsy.com
waalaa.etsy.com
wainbowmudd.etsy.com
web.etsy.com
whirlingworld.etsy.com
wiccked.etsy.com
wings1295.etsy.com
wiredbybud.etsy.com
witapuspita.etsy.com
witheyeslifted.etsy.com
www.wollelfe.etsy.com
wollymagic.etsy.com
wonderfuladelaide.etsy.com
woobinwawa.etsy.com
www.woolywireetc.etsy.com
www-f.etsy.com
xjaeva.etsy.com
yalayalaa.etsy.com
yarnutopia.etsy.com
yazzybabe.etsy.com
yoola.etsy.com
yugentribe.etsy.com
zara.etsy.com
zestfulvintage.etsy.com
root Kali
#

- **List of subdomains of Etsy.com**

www.etsy.com
23and10.etsy.com
24laha.etsy.com
3dmasterlab.etsy.com
6060.etsy.com
6thanddurianvintage.etsy.com
abeadsea.etsy.com
abrassea.etsy.com
accessoriesontheside.etsy.com
acf3326.etsy.com
action.etsy.com
adamfreed.etsy.com
adellecirca1920.etsy.com
adiarrasattic.etsy.com
adornmentchic.etsy.com
adventureandthewild.etsy.com
advocacy.etsy.com
aidahandmade.etsy.com
alaskalasermaid.etsy.com
alexca.etsy.com
alhambrahandmade.etsy.com
aliceelettrica.etsy.com
alicub.etsy.com
www.alkemia.etsy.com
allegrosattic.etsy.com
allie000.etsy.com
allison38620.etsy.com
allthingstangled.etsy.com
alm-logs-receiver-1.etsy.com
alm-logs-receiver-2.etsy.com
amechanicalmind.etsy.com
amyscraftingcorner1.etsy.com
www.ancientmusic.etsy.com
anda.etsy.com
angelheart704.etsy.com
annalouvintage.etsy.com
annapavlovna.etsy.com
aorta.etsy.com
api.etsy.com
api-cdn-test.etsy.com
api-origin.etsy.com
aradiya.etsy.com
arnicae.etsy.com
artclub.etsy.com
artfamilia.etsy.com
artificerc.etsy.com

artkissed.etsy.com
artologica.etsy.com
artshapedworld.etsy.com
artsylydia.etsy.com
ashleyarsenic.etsy.com
aubreym3810.etsy.com
aufilde.etsy.com
auth-api.etsy.com
azek2000.etsy.com
babiesandlemonade.etsy.com
www.backtobeyond.etsy.com
backyardbrand.etsy.com
www.baltovintage.etsy.com
bananyastand.etsy.com
bbbellezza.etsy.com
bcn.etsy.com
beachcottagelife.etsy.com
beacon.etsy.com
beadacious1221.etsy.com
beadree.etsy.com
beadworkbyamanda.etsy.com
beamerweb.etsy.com
beautifulera.etsy.com
bebond20.etsy.com
beladonna.etsy.com
www.belladonna10.etsy.com
beneaththerowantree.etsy.com
bespokemadebylaura.etsy.com
beta.etsy.com
betsyandiya.etsy.com
beulahvida.etsy.com
www.bewildandfree.etsy.com
bibliophile1.etsy.com
birdsoflace.etsy.com
bitsyb00.etsy.com
bkinspired.etsy.com
blingbydonna.etsy.com
blog.etsy.com
www.blog.etsy.com
bloomingflowertea.etsy.com
bluenostalgia.etsy.com
bluesky10.etsy.com
blushesandgold.etsy.com
botanic2ceramic.etsy.com
botanicalbird.etsy.com
bronwenhyde.etsy.com
www.bumblebeeboulevard.etsy.com
bunnydee.etsy.com
buttercupmarketplace.etsy.com
butterflylove1.etsy.com

bybrosha.etsy.com
www.bynicola.etsy.com
bysalla.etsy.com
ca.etsy.com
caballera.etsy.com
cannoli.etsy.com
o597.ptr8334.careeralerts.etsy.com
careers.etsy.com
www.careers.etsy.com
catherinebuca.etsy.com
catonalimb.etsy.com
ccsaid10102010.etsy.com
www.ccsaid10102010.etsy.com
cdn-stage.etsy.com
celialuna.etsy.com
chaerea.etsy.com
charlieandella.etsy.com
www.charlieandella.etsy.com
cheldena.etsy.com
chelseapetaja.etsy.com
christinemarieb.etsy.com
chronologievintage.etsy.com
circa810.etsy.com
citizenscholarinc.etsy.com
classicallyromantic.etsy.com
classicbead.etsy.com
www.cobblestonesvintage.etsy.com
cocoshoopla.etsy.com
coin1071.etsy.com
community.etsy.com
community-stage.etsy.com
coolkoala.etsy.com
coralreefer420.etsy.com
www.coralreefer420.etsy.com
jamf.corp.etsy.com
ldap.corp.etsy.com
craigandstasia.etsy.com
crazysocks830.etsy.com
www.creationchama.etsy.com
crozza.etsy.com
cupcake.etsy.com
damesalamode.etsy.com
www.daughtersofbuddha.etsy.com
dcronic.etsy.com
de.etsy.com
deboy2000.etsy.com
www.decadesofvintage.etsy.com
decoylab.etsy.com
deepshade.etsy.com
deerface.etsy.com

deerpathvintage.etsy.com
delftia.etsy.com
demarsvintage.etsy.com
depeapa.etsy.com
designsbysaka.etsy.com
dev-auth-api.etsy.com
devil.etsy.com
devingreen420.etsy.com
diannawolfe.etsy.com
dicopebisuteria.etsy.com
dimatsu100.etsy.com
discord.etsy.com
www.distlefunk2.etsy.com
divinedebrusvintage.etsy.com
dlsarmywife.etsy.com
dns1.etsy.com
dns2.etsy.com
doalittledance.etsy.com
dollb.etsy.com
dollhouseara.etsy.com
dopurcell2012.etsy.com
dragon06.etsy.com
dragonswood.etsy.com
driaa.etsy.com
dsml.etsy.com
www.dsml.etsy.com
dubland.etsy.com
dulcebebe.etsy.com
dummy-api.etsy.com
e.etsy.com
click.e.etsy.com
cloud.e.etsy.com
image.e.etsy.com
mta.e.etsy.com
mta10.e.etsy.com
mta11.e.etsy.com
mta12.e.etsy.com
mta13.e.etsy.com
mta15.e.etsy.com
mta16.e.etsy.com
mta17.e.etsy.com
mta18.e.etsy.com
mta19.e.etsy.com
mta2.e.etsy.com
mta20.e.etsy.com
mta21.e.etsy.com
mta22.e.etsy.com
mta23.e.etsy.com
mta24.e.etsy.com
mta25.e.etsy.com

mta26.e.etsy.com
mta3.e.etsy.com
mta4.e.etsy.com
mta5.e.etsy.com
mta6.e.etsy.com
mta7.e.etsy.com
mta8.e.etsy.com
mta9.e.etsy.com
pages.e.etsy.com
spdmta.e.etsy.com
view.e.etsy.com
www.echoandwild.etsy.com
ecraftic.etsy.com
elisabethspace.etsy.com
shop.ellohpea.etsy.com
else10.etsy.com
ablink.email.etsy.com
o2504.abmail.email.etsy.com
o2505.abmail.email.etsy.com
o2506.abmail.email.etsy.com
o2507.abmail.email.etsy.com
o2508.abmail.email.etsy.com
o2509.abmail.email.etsy.com
o2510.abmail.email.etsy.com
o2511.abmail.email.etsy.com
o2512.abmail.email.etsy.com
o2513.abmail.email.etsy.com
o2514.abmail.email.etsy.com
o2515.abmail.email.etsy.com
o2516.abmail.email.etsy.com
o2517.abmail.email.etsy.com
o2518.abmail.email.etsy.com
o2519.abmail.email.etsy.com
o2520.abmail.email.etsy.com
o2521.abmail.email.etsy.com
o2522.abmail.email.etsy.com
o2523.abmail.email.etsy.com
emcee.etsy.com
emmagerard.etsy.com
emotionalbaggage.etsy.com
engineering.etsy.com
equilibria.etsy.com
erinw440.etsy.com
estateeclectic.etsy.com
etsystatic.etsy.com
etsyu.etsy.com
evarose1900.etsy.com
exploreexplained.etsy.com
external.etsy.com
extfiles.etsy.com

fabrictree.etsy.com
fairepartbedonabebe.etsy.com
fashionfucsia.etsy.com
fawa.etsy.com
featherednest97030.etsy.com
fede.etsy.com
feltcafe.etsy.com
fishpaste.etsy.com
fitacola.etsy.com
freekittensvintage.etsy.com
frostbeard.etsy.com
funbytheyard.etsy.com
fw.etsy.com
fw1.etsy.com
fw2.etsy.com
www.galahad40.etsy.com
galsfly2.etsy.com
gaugenyc.etsy.com
www.gemmy200.etsy.com
georgeandgouma.etsy.com
www.getthepartystarted.etsy.com
giovannini250.etsy.com
giraffeandcustard.etsy.com
glassbead.etsy.com
glitterandbold.etsy.com
gollybard.etsy.com
grandmabarbara.etsy.com
grandmapierce.etsy.com
www.greatstuff2730.etsy.com
greenedenvintage.etsy.com
handofhalcyonnyc.etsy.com
handsintheattic.etsy.com
hayshandcrafted.etsy.com
heartofthemermaid.etsy.com
heavenboundhca.etsy.com
hellocupcakellc.etsy.com
hellomyfriend.etsy.com
help.etsy.com
helvetika.etsy.com
www.hendywood.etsy.com
hiddengarden11.etsy.com
highpointfarm2010.etsy.com
www.hipknits10.etsy.com
historicallybound.etsy.com
www.hochetgaga.etsy.com
holajed.etsy.com
hollyernst430.etsy.com
www.hollyernst430.etsy.com
homegrownvintage.etsy.com
homehooked.etsy.com

honey0550.etsy.com
www.housecatclub.etsy.com
houseofafritude.etsy.com
hummingbirdcraftsllc.etsy.com
idlewylde.etsy.com
idlized.etsy.com
iheartjujubee.etsy.com
image0.etsy.com
image1.etsy.com
image2.etsy.com
image3.etsy.com
img0.etsy.com
img1.etsy.com
img2.etsy.com
img3.etsy.com
inoroutmedia.etsy.com
inspirala.etsy.com
intothewhirled.etsy.com
investors.etsy.com
ireneflorentina.etsy.com
izzysattic.etsy.com
jadecicada.etsy.com
jadehandmade.etsy.com
janeymay79.etsy.com
janicemae.etsy.com
jeandoussetdiamond.etsy.com
jeanknee.etsy.com
www.jellevintage.etsy.com
jems530.etsy.com
www.jems530.etsy.com
jenni20.etsy.com
www.jenni20.etsy.com
jennifermercede.etsy.com
jessgonacha.etsy.com
jewelboxballerina.etsy.com
jewelledfriend.etsy.com
jewelrenee.etsy.com
jewelry1910.etsy.com
jgrant0214.etsy.com
jillrosenwald.etsy.com
jneale3.etsy.com
o596.ptr7485.jobalerts.etsy.com
joinartlife.etsy.com
joolzbylisa.etsy.com
junkstylediva.etsy.com
justaddcocoa.etsy.com
justinegilbuena.etsy.com
jwillowbee.etsy.com
www.jwms00.etsy.com
kaeriefaerie52.etsy.com

kaleidoskopicromance.etsy.com
katlandia.etsy.com
katmariee.etsy.com
kazeseka.etsy.com
kellydesigns4.etsy.com
keoops8.etsy.com
kevinmccain10.etsy.com
kipapee.etsy.com
kitchenculinaria.etsy.com
kivaford.etsy.com
klj8379.etsy.com
kortni10.etsy.com
krissypineda.etsy.com
krityumhandmade.etsy.com
kseniya.etsy.com
kwilson544.etsy.com
labetehandmade.etsy.com
www.lacegrl130.etsy.com
ladetallista.etsy.com
ladybug650.etsy.com
www.larhondashandmade.etsy.com
laughter56.etsy.com
lauraslocumpainted.etsy.com
lbd340.etsy.com
www.lcrknitted.etsy.com
leahjohanna.etsy.com
leajoellehandmade.etsy.com
leopard.etsy.com
lifeiscrafted.etsy.com
lilleypad.etsy.com
www.lilliesdreambyluthea.etsy.com
lillypod.etsy.com
lilu2010.etsy.com
www.lindab142.etsy.com
lindasolovic.etsy.com
www.lindsd620.etsy.com
lisellemade.etsy.com
lisethandmaid.etsy.com
www.littlecritters00.etsy.com
littleplumtree.etsy.com
live610.etsy.com
livenhandmade.etsy.com
livlovelybyolivia.etsy.com
ljctree.etsy.com
loddelina.etsy.com
loellamedina.etsy.com
lorimarsha.etsy.com
loserkid5150.etsy.com
lostandfawned.etsy.com
loveaccented.etsy.com

lovelia.etsy.com
loveofsweetmelissa.etsy.com
lovestamped.etsy.com
lowe40.etsy.com
lucky10.etsy.com
www.lucky10.etsy.com
www.lucky120.etsy.com
luckycharmsusa.etsy.com
luckychelle7.etsy.com
lucyandthelamb.etsy.com
luludee.etsy.com
m.etsy.com
madfish40.etsy.com
mail.etsy.com
o5.ptr4229.mail.etsy.com
o3.ptr6308.mail.etsy.com
o4.ptr6915.mail.etsy.com
mailin.etsy.com
www.mailleetc.etsy.com
mailout.etsy.com
mailout01.etsy.com
mailout02.etsy.com
mailout03.etsy.com
mailout04.etsy.com
mailout05.etsy.com
mailout06.etsy.com
mailout10.etsy.com
mailout11.etsy.com
mailout12.etsy.com
mailout13.etsy.com
mailout14.etsy.com
mailout15.etsy.com
mailout16.etsy.com
mailout17.etsy.com
mailout18.etsy.com
mailout19.etsy.com
mailout20.etsy.com
mailout21.etsy.com
mailout22.etsy.com
mailout23.etsy.com
mailoutaa.etsy.com
mailoutab.etsy.com
mailoutac.etsy.com
mailoutaf.etsy.com
mailoutag.etsy.com
mailoutah.etsy.com
maintenance.etsy.com
makingsofshannatice.etsy.com
malien00.etsy.com
mamachee.etsy.com

management.etsy.com
www.manakahandmade.etsy.com
www.manateebythesea.etsy.com
marge54.etsy.com
maribellecampa.etsy.com
marlasmud.etsy.com
marlenesdesigns2011.etsy.com
marmite.etsy.com
maryfaithpeace.etsy.com
materialised.etsy.com
matty8080.etsy.com
may775.etsy.com
mcp.etsy.com
meadowlion1120.etsy.com
meadowmuffin2010.etsy.com
meganlee.etsy.com
www.meimage.etsy.com
memegalarce.etsy.com
mi.etsy.com
micasita.etsy.com
michaljonca.etsy.com
michelep222.etsy.com
milenska.etsy.com
minnieandmaude.etsy.com
mirror1.etsy.com
misstiger10.etsy.com
mk15048.etsy.com
mochikaka.etsy.com
modelt30.etsy.com
www.moma10.etsy.com
www.monick31.etsy.com
monikaviktoria.etsy.com
mosaicmannyc.etsy.com
motherloadtoad.etsy.com
mouse110.etsy.com
www.mrslaura30.etsy.com
msysmta01.etsy.com
msysmta02.etsy.com
mustard.etsy.com
mx03a.etsy.com
mx04f.etsy.com
www.nadinessra.etsy.com
nafsika.etsy.com
naimacrochethandmade.etsy.com
netwk.etsy.com
brk-vcenter.netwk.etsy.com
neworleanslady85.etsy.com
nikkiana.etsy.com
ninalazina.etsy.com
nisaba.etsy.com

njema.etsy.com
nodtomodvintage.etsy.com
norhymeorreasonat40.etsy.com
nornwood.etsy.com
www.nowthen10.etsy.com
ns1.etsy.com
ns2.etsy.com
ny-dev-fw.etsy.com
ny-dev-fw1.etsy.com
ny-dev-fw2.etsy.com
ny-image0.etsy.com
ny-image1.etsy.com
ny-image2.etsy.com
ny-image3.etsy.com
ny2.etsy.com
ldap.ny2.etsy.com
ny5.etsy.com
ldap.ny5.etsy.com
vm.ny5.etsy.com
adyen-callbacks.vm.ny5.etsy.com
apple-pay-test.vm.ny5.etsy.com
madler.vm.ny5.etsy.com
ny5-border02.etsy.com
nymla.etsy.com
obamalipbalma.etsy.com
omarsamassa.etsy.com
coffeetalk.omarsamassa.etsy.com
onelaneroad.etsy.com
oohvintage.etsy.com
oolawoola.etsy.com
openapi.etsy.com
sandbox.openapi.etsy.com
openapi-f.etsy.com
openapi-origin.etsy.com
organizelife.etsy.com
origin-princess.etsy.com
owlandtoad.etsy.com
owlcreekhandmade.etsy.com
pan2.etsy.com
pan3.etsy.com
paperandfield.etsy.com
paperandlace.etsy.com
parvana.etsy.com
paweljonca.etsy.com
pearliemae.etsy.com
www.pebblesbylanae.etsy.com
peekabua.etsy.com
pemberleypond.etsy.com
persephonevintage.etsy.com
phoenix420.etsy.com

photobird.etsy.com
photobymada.etsy.com
piktorama.etsy.com
pillowhead.etsy.com
pimento.etsy.com
pinderella.etsy.com
pineconemcgee.etsy.com
pinkpaisley1.etsy.com
planetqueenvintage.etsy.com
pmimage.etsy.com
poladora.etsy.com
polyclarific.etsy.com
popwildlife.etsy.com
portmade.etsy.com
pottersfield.etsy.com
potterybyanita.etsy.com
ppq.etsy.com
ppt.etsy.com
priscillamae.etsy.com
o2.ptr5125.etsy.com
o1.ptr9563.etsy.com
puddin450.etsy.com
pudding.etsy.com
puffluna.etsy.com
racjd.etsy.com
ragamuffin2006.etsy.com
raimbowtree.etsy.com
rakshniyavintage.etsy.com
ramona.etsy.com
ramunesceramic.etsy.com
randi100.etsy.com
raven333.etsy.com
ravenshold.etsy.com
reacoustic.etsy.com
www.rebekavintage.etsy.com
rebel1in8.etsy.com
recycledgrace.etsy.com
redmeg8.etsy.com
redthread.etsy.com
redwaistband.etsy.com
refinedrubbishllc.etsy.com
retirementfund.etsy.com
retrograndma.etsy.com
retroreprohandmade.etsy.com
rev2220.etsy.com
www.rev2220.etsy.com
rinconroad.etsy.com
road10.etsy.com
www.road10.etsy.com
rockinlola.etsy.com

roseclearfield.etsy.com
roseinbloom2010.etsy.com
rupydetequila.etsy.com
rusticbeachchic.etsy.com
salondemaria.etsy.com
salvagelife.etsy.com
sararmoniasara.etsy.com
saviahsage.etsy.com
sci2010.etsy.com
www.sci2010.etsy.com
seastar1.etsy.com
secrets.etsy.com
seen1.etsy.com
www.seewhatwemade.etsy.com
ablink.seller.etsy.com
shadowpeople00.etsy.com
shareyourshop.etsy.com
shasam3.etsy.com
shelleywallace.etsy.com
shoppe3130.etsy.com
www.shoppe3130.etsy.com
sigaluna.etsy.com
silvadesignllc.etsy.com
sistersidvintage.etsy.com
skymagenta.etsy.com
smileyme520.etsy.com
smiss00.etsy.com
songbead.etsy.com
spf2000000.etsy.com
www.splendidthread.etsy.com
srambo20.etsy.com
www.srambo20.etsy.com
stageapi.etsy.com
starlight11500.etsy.com
www.starlight11500.etsy.com
statements2000.etsy.com
new.static.etsy.com
new.static2.etsy.com
www.stephenedwardgraphic.etsy.com
www.stephy4030.etsy.com
www.stitchesnstuff10.etsy.com
stitchforward.etsy.com
www.studio120.etsy.com
studio1955.etsy.com
studio550.etsy.com
studiofive10.etsy.com
www.studiolauralee.etsy.com
stuga.etsy.com
www.suesupcyclednvintage.etsy.com
summitengravingltd.etsy.com

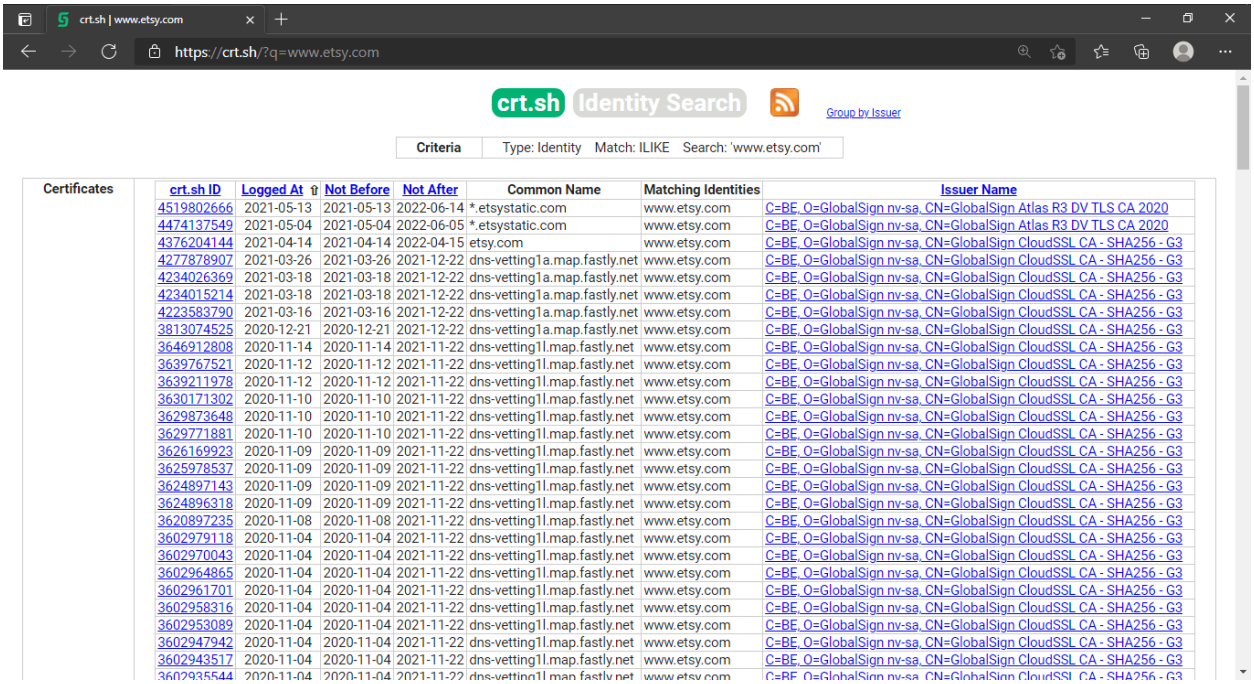
supayana.etsy.com
superteams.etsy.com
susie730.etsy.com
sweetandstitched.etsy.com
sweetpeashoppe10.etsy.com
tamara30.etsy.com
tanjasova.etsy.com
tantehilde.etsy.com
tarahandmade.etsy.com
teameja.etsy.com
technochic.etsy.com
tentandtiara.etsy.com
terrikasuba.etsy.com
textilegeisha.etsy.com
the1650.etsy.com
theartofsuicide.etsy.com
www.thebeadedbead.etsy.com
www.thecharmedwife.etsy.com
thechocolatelab.etsy.com
thechurchofvintage.etsy.com
thecuddlycephalopod.etsy.com
theeclecticelement2.etsy.com
theendpeace.etsy.com
theetsymarket.etsy.com
thefoldedpage.etsy.com
thegarage.etsy.com
thehookup3400.etsy.com
www.thejewelsaga.etsy.com
thelunarfae.etsy.com
themorosebee.etsy.com
thepleb.etsy.com
thesecondface.etsy.com
thesewingchic.etsy.com
www.thestampinmama.etsy.com
thevintagearcade.etsy.com
thevintageista.etsy.com
www.thewolfandthetree.etsy.com
thezombiehorde.etsy.com
thingsfound.etsy.com
www.tinaproduce.etsy.com
tinkersdaughter2015.etsy.com
tinyred.etsy.com
tinyvillage.etsy.com
tomokotara.etsy.com
tonyadusold.etsy.com
www.topdesign3000.etsy.com
tranquillina.etsy.com
trees4thewood.etsy.com
trinitysoap3.etsy.com
trusthemp1320.etsy.com

tuesdayrosevintage.etsy.com
twehchic.etsy.com
twotreesworld.etsy.com
ulaa.etsy.com
umbrellastand.etsy.com
uniquelycovered.etsy.com
username.etsy.com
valsart2000.etsy.com
vickevira.etsy.com
vintagebride.etsy.com
www.vintagegreyhandmade.etsy.com
vivalababyhead.etsy.com
vonderific.etsy.com
waalaa.etsy.com
wainbowmudd.etsy.com
web.etsy.com
whirlingworld.etsy.com
wiccked.etsy.com
wings1295.etsy.com
wiredbybud.etsy.com
witapuspita.etsy.com
witheyeslifted.etsy.com
www.wollelfe.etsy.com
wollymagic.etsy.com
wonderfuladelaide.etsy.com
woobinwawa.etsy.com
www.woolywireetc.etsy.com
www-f.etsy.com
xjaeva.etsy.com
yalayalaa.etsy.com
yarnutopia.etsy.com
yazzybabe.etsy.com
yoola.etsy.com
yugentribe.etsy.com
zara.etsy.com
zestfulvintage.etsy.com

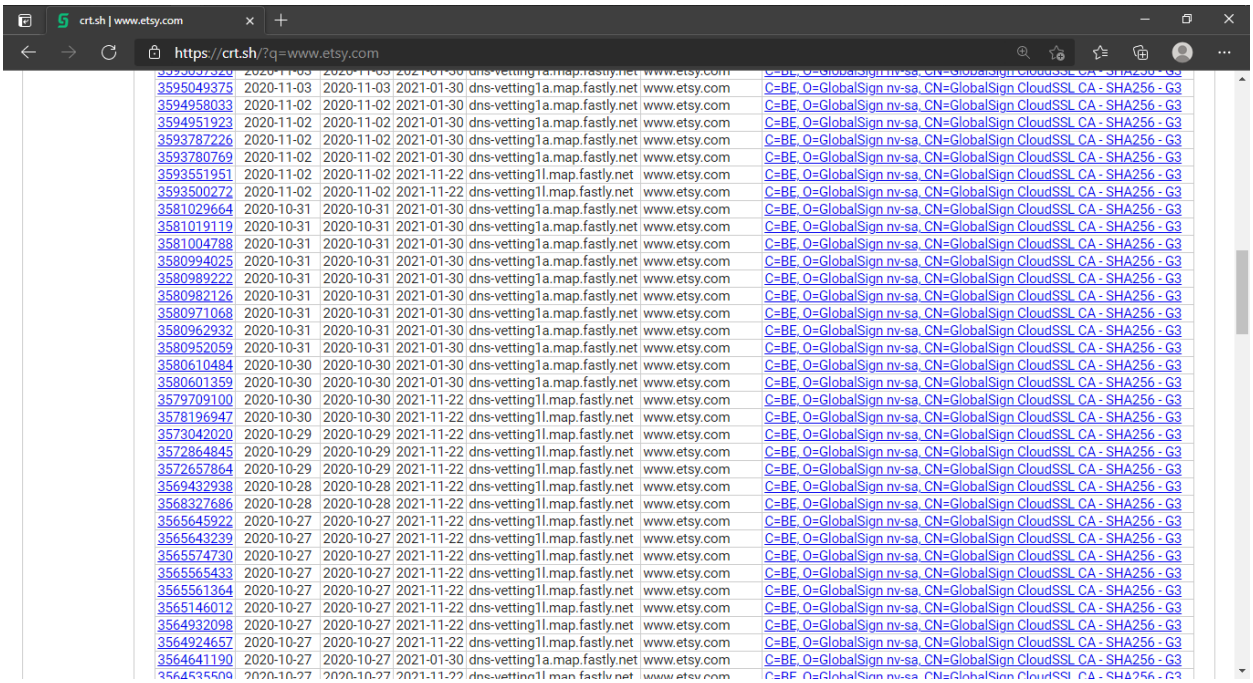
5.1.2. crt.sh

In **crt.sh** I found many subdomains.

- Link: https://crt.sh/?q=%25.etsy.com

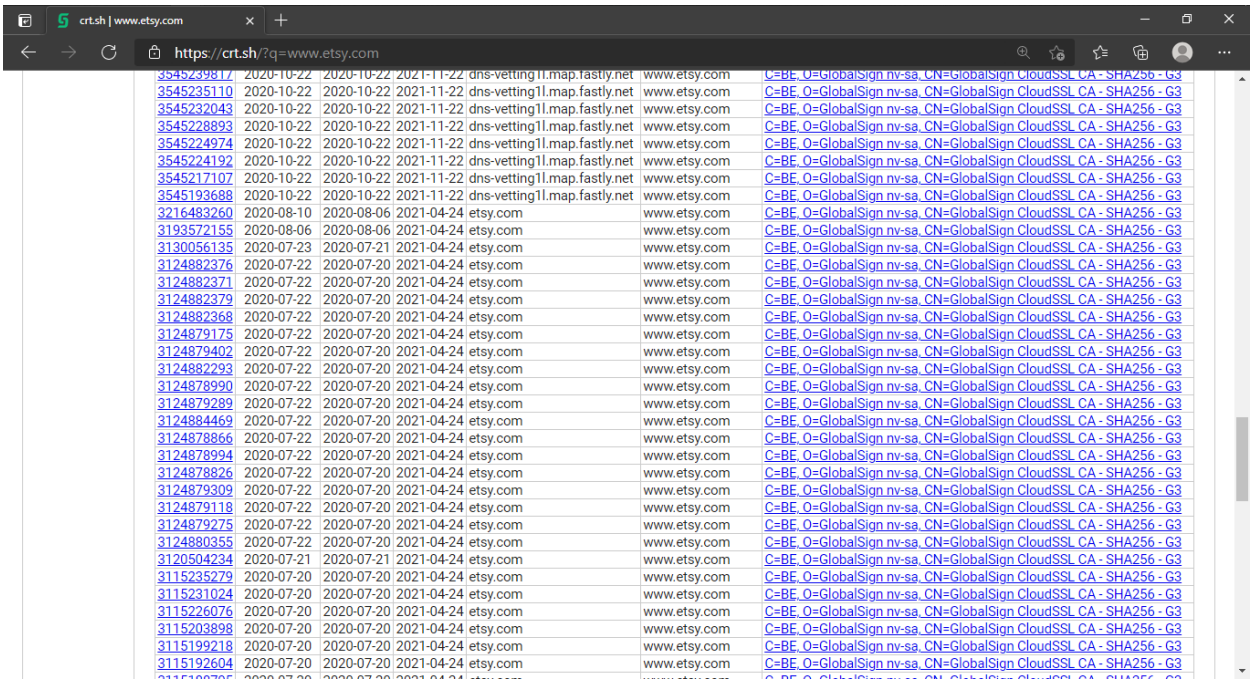


crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
4519802666	2021-05-13	2021-05-13	2022-06-14	*.etsystatic.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlas R3 DV TLS CA 2020
4474137549	2021-05-04	2021-05-04	2022-06-05	*.etsystatic.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign Atlas R3 DV TLS CA 2020
4376204144	2021-04-14	2021-04-14	2022-04-15	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
4277878907	2021-03-26	2021-03-26	2021-12-22	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
4234026369	2021-03-18	2021-03-18	2021-12-22	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
4234015214	2021-03-18	2021-03-18	2021-12-22	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
4223583790	2021-03-16	2021-03-16	2021-12-22	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3813074525	2020-12-21	2020-12-21	2021-12-22	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3646912808	2020-11-14	2020-11-14	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3639767521	2020-11-12	2020-11-12	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3639211978	2020-11-12	2020-11-12	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3630171302	2020-11-10	2020-11-10	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3629873648	2020-11-10	2020-11-10	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3629771881	2020-11-10	2020-11-10	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3626169923	2020-11-09	2020-11-09	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3625978537	2020-11-09	2020-11-09	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3624897143	2020-11-09	2020-11-09	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3624896318	2020-11-09	2020-11-09	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3620897235	2020-11-08	2020-11-08	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602979118	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602970043	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602964865	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602961701	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602958316	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602953089	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602947942	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602943517	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602935544	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602926084	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602923335	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602917267	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602881406	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602873625	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602867520	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602861062	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602851746	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602848728	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602841692	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602838896	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602832724	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602769976	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602759950	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602753515	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602749395	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602728480	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602670346	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602665926	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602659983	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602655356	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3602445037	2020-11-04	2020-11-04	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3598543073	2020-11-03	2020-11-03	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3598539560	2020-11-03	2020-11-03	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3598537111	2020-11-03	2020-11-03	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3598507900	2020-11-03	2020-11-03	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3595150606	2020-11-03	2020-11-03	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3595108217	2020-11-03	2020-11-03	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3595100575	2020-11-03	2020-11-03	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3595095156	2020-11-03	2020-11-03	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3595079998	2020-11-03	2020-11-03	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3595070961	2020-11-03	2020-11-03	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3595064495	2020-11-03	2020-11-03	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3595057326	2020-11-03	2020-11-03	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3



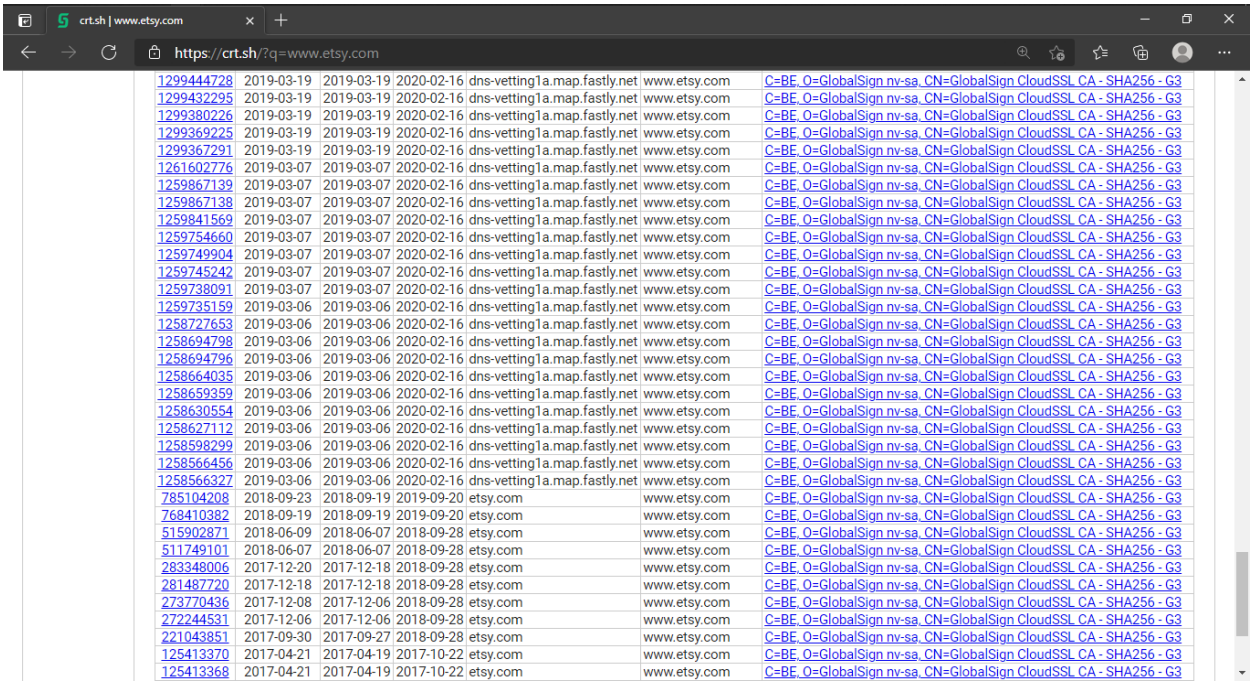
3595049375	2020-11-03	2020-11-03	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3594958033	2020-11-02	2020-11-02	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3594951923	2020-11-02	2020-11-02	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3593787226	2020-11-02	2020-11-02	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3593780769	2020-11-02	2020-11-02	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3593551951	2020-11-02	2020-11-02	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3593500272	2020-11-02	2020-11-02	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3581029664	2020-10-31	2020-10-31	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3581019119	2020-10-31	2020-10-31	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3581004788	2020-10-31	2020-10-31	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3580994025	2020-10-31	2020-10-31	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3580989222	2020-10-31	2020-10-31	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3580982126	2020-10-31	2020-10-31	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3580971068	2020-10-31	2020-10-31	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3580962932	2020-10-31	2020-10-31	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3580952059	2020-10-31	2020-10-31	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3580610484	2020-10-30	2020-10-30	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3580601359	2020-10-30	2020-10-30	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3579709100	2020-10-30	2020-10-30	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3578196947	2020-10-30	2020-10-30	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3573042020	2020-10-29	2020-10-29	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3572864845	2020-10-29	2020-10-29	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3572657864	2020-10-29	2020-10-29	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3569432938	2020-10-28	2020-10-28	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3568327686	2020-10-28	2020-10-28	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3565645922	2020-10-27	2020-10-27	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3565643239	2020-10-27	2020-10-27	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3565574730	2020-10-27	2020-10-27	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3565565433	2020-10-27	2020-10-27	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3565561364	2020-10-27	2020-10-27	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3565146012	2020-10-27	2020-10-27	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3564932098	2020-10-27	2020-10-27	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3564924657	2020-10-27	2020-10-27	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3564641190	2020-10-27	2020-10-27	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3564535509	2020-10-27	2020-10-27	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3

3564535509	2020-10-27	2020-10-27	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3564524798	2020-10-27	2020-10-27	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3564427411	2020-10-27	2020-10-27	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3564416560	2020-10-27	2020-10-27	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3564348606	2020-10-27	2020-10-27	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3561372641	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3561364979	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3561358096	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3561052982	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3560775252	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3560767678	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3560568589	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3560556949	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3560526619	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3560523209	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3560494889	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3560409816	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3560383263	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3560381278	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3560352038	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3560349433	2020-10-26	2020-10-26	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3556650589	2020-10-25	2020-10-25	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3556646421	2020-10-25	2020-10-25	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3556641489	2020-10-25	2020-10-25	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3556631763	2020-10-25	2020-10-25	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3556626578	2020-10-25	2020-10-25	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3556620135	2020-10-25	2020-10-25	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3549131876	2020-10-23	2020-10-23	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3548904256	2020-10-23	2020-10-23	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3548645138	2020-10-23	2020-10-23	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3548631743	2020-10-23	2020-10-23	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3548626463	2020-10-23	2020-10-23	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3548612575	2020-10-23	2020-10-23	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3548595972	2020-10-23	2020-10-23	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3548591051	2020-10-23	2020-10-23	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3



3545239817	2020-10-22	2020-10-22	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3545235110	2020-10-22	2020-10-22	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3545232043	2020-10-22	2020-10-22	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3545228893	2020-10-22	2020-10-22	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3545224974	2020-10-22	2020-10-22	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3545224192	2020-10-22	2020-10-22	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3545217107	2020-10-22	2020-10-22	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3545193688	2020-10-22	2020-10-22	2021-11-22	dns-vetting1l.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3216483260	2020-08-10	2020-08-06	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3193572155	2020-08-06	2020-08-06	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3130056135	2020-07-23	2020-07-21	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124882376	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124882371	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124882379	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124882368	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124879175	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124879402	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124882293	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124878990	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124879289	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124884469	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124878866	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124878994	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124878826	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124879309	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124879118	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124879275	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3124880355	2020-07-22	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3120504234	2020-07-21	2020-07-21	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115235279	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115231024	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115226076	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115203898	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115199218	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115192604	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3

3115192604	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115188795	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115173243	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115106185	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115103309	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115100495	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115094860	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115085555	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115082825	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115079250	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115071790	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
3115067936	2020-07-20	2020-07-20	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
2731946433	2020-04-25	2020-04-23	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
2724473301	2020-04-23	2020-04-23	2021-04-24	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
2393714823	2020-01-30	2020-01-30	2021-01-30	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
2393710676	2020-01-30	2020-01-30	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
2386513109	2020-01-28	2006-04-26	2008-06-25	www.etsy.com	www.etsy.com	C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness CA-1
1797786903	2019-08-22	2019-08-20	2020-08-20	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1790920427	2019-08-20	2019-08-20	2020-08-20	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1569812057	2019-06-12	2019-06-10	2019-09-20	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1562843965	2019-06-10	2019-06-10	2019-09-20	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1299444910	2019-03-19	2019-03-19	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1299444728	2019-03-19	2019-03-19	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1299432295	2019-03-19	2019-03-19	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1299380226	2019-03-19	2019-03-19	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1299369225	2019-03-19	2019-03-19	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1299367291	2019-03-19	2019-03-19	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1261602776	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259867139	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259867138	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259841569	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259754660	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259749904	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259745242	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259738091	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3



1299444728	2019-03-19	2019-03-19	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1299432295	2019-03-19	2019-03-19	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1299380226	2019-03-19	2019-03-19	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1299369225	2019-03-19	2019-03-19	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1299367291	2019-03-19	2019-03-19	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1261602776	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259867139	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259867138	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259841569	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259754660	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259749904	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259745242	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259738091	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259735159	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258727653	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258694798	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258694796	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258664035	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258659359	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258630554	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258627112	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258598299	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258566456	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258566327	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
785104208	2018-09-23	2018-09-19	2019-09-20	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
768410382	2018-09-19	2018-09-19	2019-09-20	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
515902871	2018-06-09	2018-06-07	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
511749101	2018-06-07	2018-06-07	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
283348006	2017-12-20	2017-12-18	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
281487720	2017-12-18	2017-12-18	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
273770436	2017-12-08	2017-12-06	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
272244531	2017-12-06	2017-12-06	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
221043851	2017-09-30	2017-09-27	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
125413370	2017-04-21	2017-04-19	2017-10-22	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
125413368	2017-04-21	2017-04-19	2017-10-22	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3

1259738091	2019-03-07	2019-03-07	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1259735159	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258727653	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258694798	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258694796	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258664035	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258659359	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258630554	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258627112	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258598299	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258566456	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
1258566327	2019-03-06	2019-03-06	2020-02-16	dns-vetting1a.map.fastly.net	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
785104208	2018-09-23	2018-09-19	2019-09-20	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
768410382	2018-09-19	2018-09-19	2019-09-20	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
515902871	2018-06-09	2018-06-07	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
511749101	2018-06-07	2018-06-07	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
283348006	2017-12-20	2017-12-18	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
281487720	2017-12-18	2017-12-18	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
273770436	2017-12-08	2017-12-06	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
272244531	2017-12-06	2017-12-06	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
221043851	2017-09-30	2017-09-27	2018-09-28	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
125413370	2017-04-21	2017-04-19	2017-10-22	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
125413368	2017-04-21	2017-04-19	2017-10-22	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
125413352	2017-04-21	2017-04-19	2017-10-22	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
89096422	2017-02-10	2017-02-08	2017-10-22	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
89096416	2017-02-10	2017-02-08	2017-10-22	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3
51738771	2016-11-13	2016-11-08	2017-10-22	etsy.com	www.etsy.com	C=BE, O=GlobalSign nv-sa, CN=GlobalSign CloudSSL CA - SHA256 - G3

© Sectigo Limited 2015-2021. All rights reserved.

6. Vulnerability Scanning

Vulnerability scanning is an examination of a computer's or network's possible points of exploitation in order to find security flaws. A vulnerability scan identifies and classifies device flaws in devices, networks, and communications equipment, as well as predicting how successful countermeasures would be.

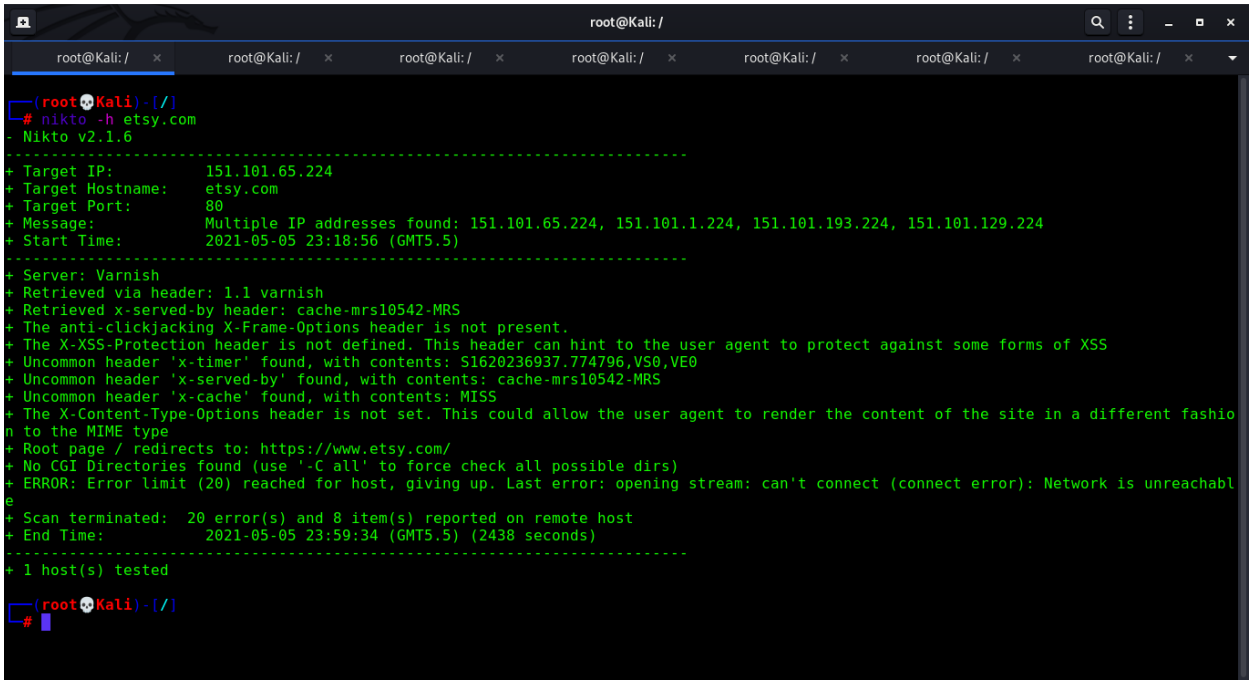
There are many vulnerability scanning tools out there. If you search for a vulnerability scanner, you will find many tools. Popular tools that are utilized to scan vulnerability are,

- Nikto
- Burp Suite
- SQL Map
- ZenMAP
- Nmap

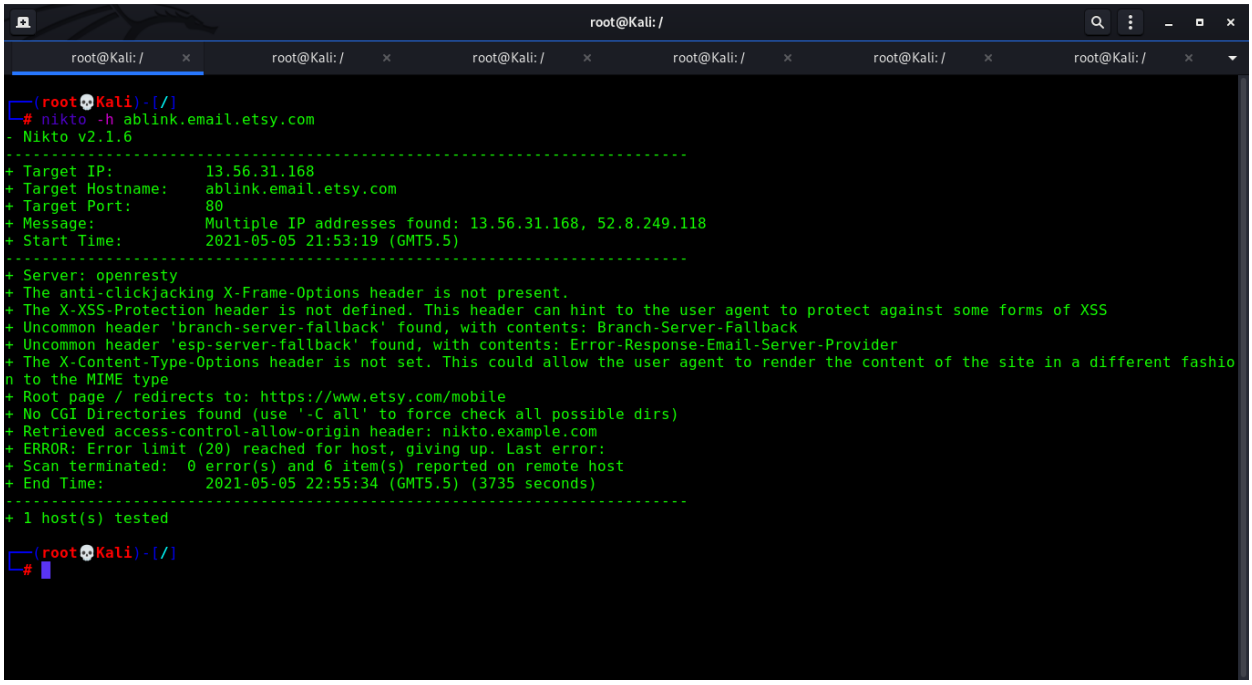
For this report, I used Nikto tool for scanning vulnerabilities.

➢ Nikto

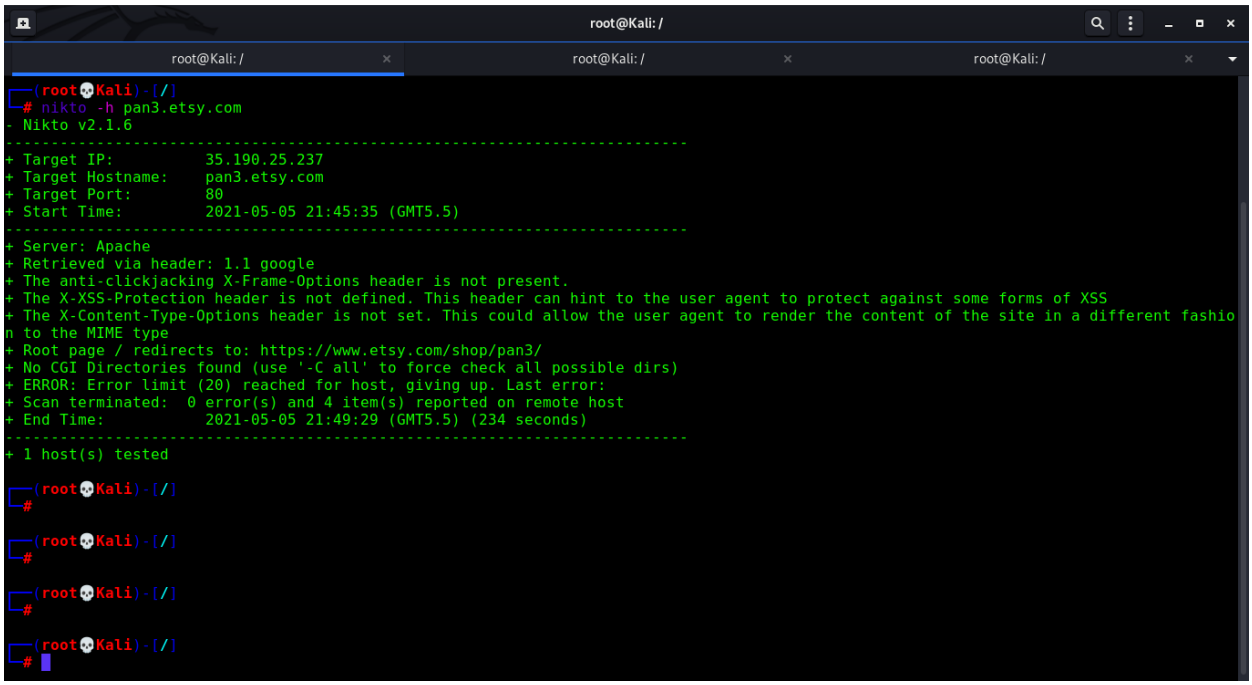
➢ www.etsy.com



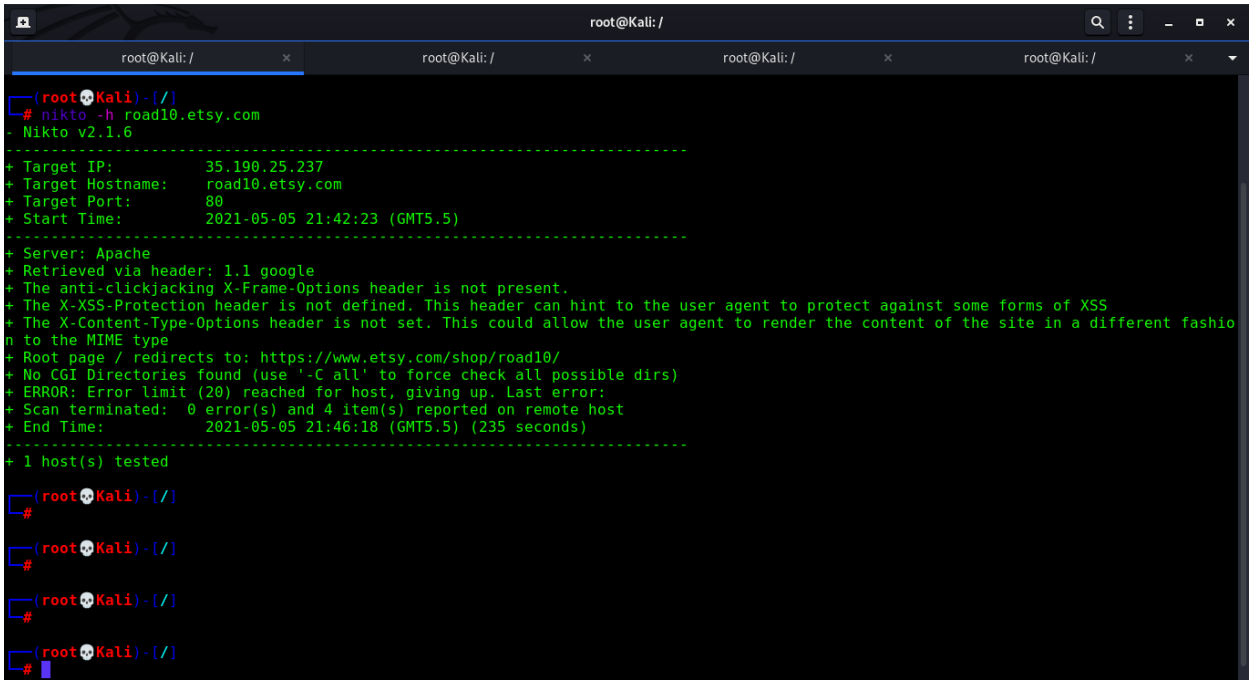
- **ablink.email.etsy.com**



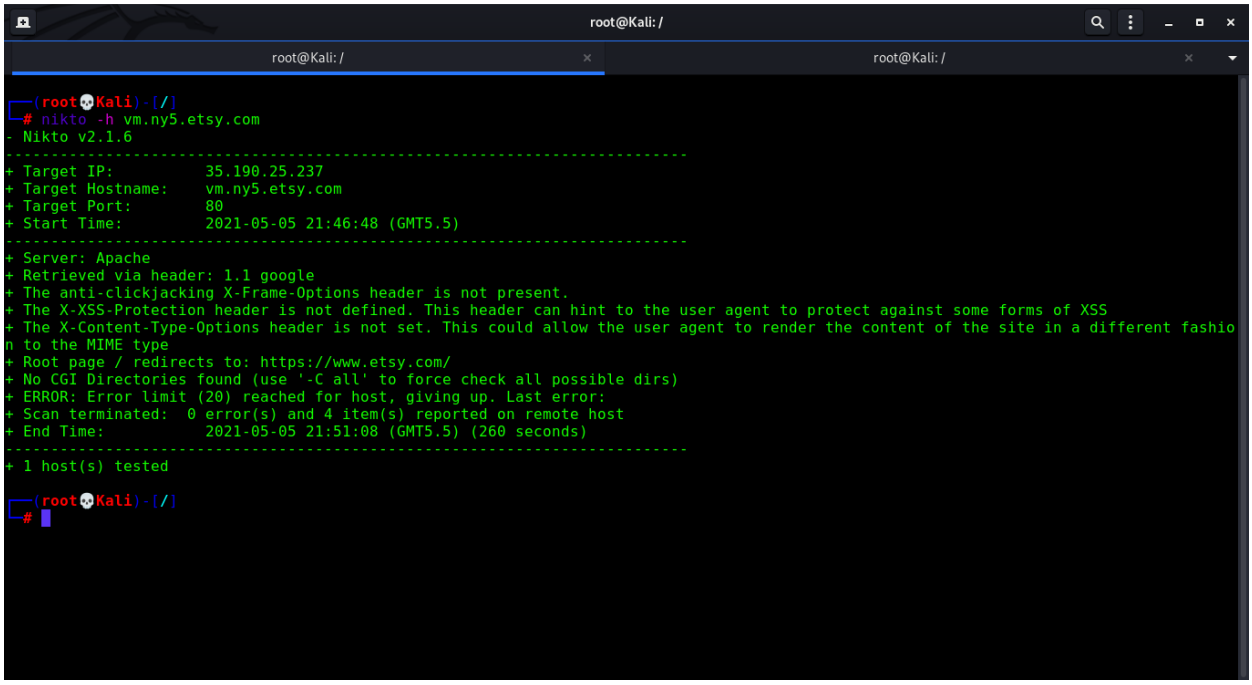
- **pan3.etsy.com**



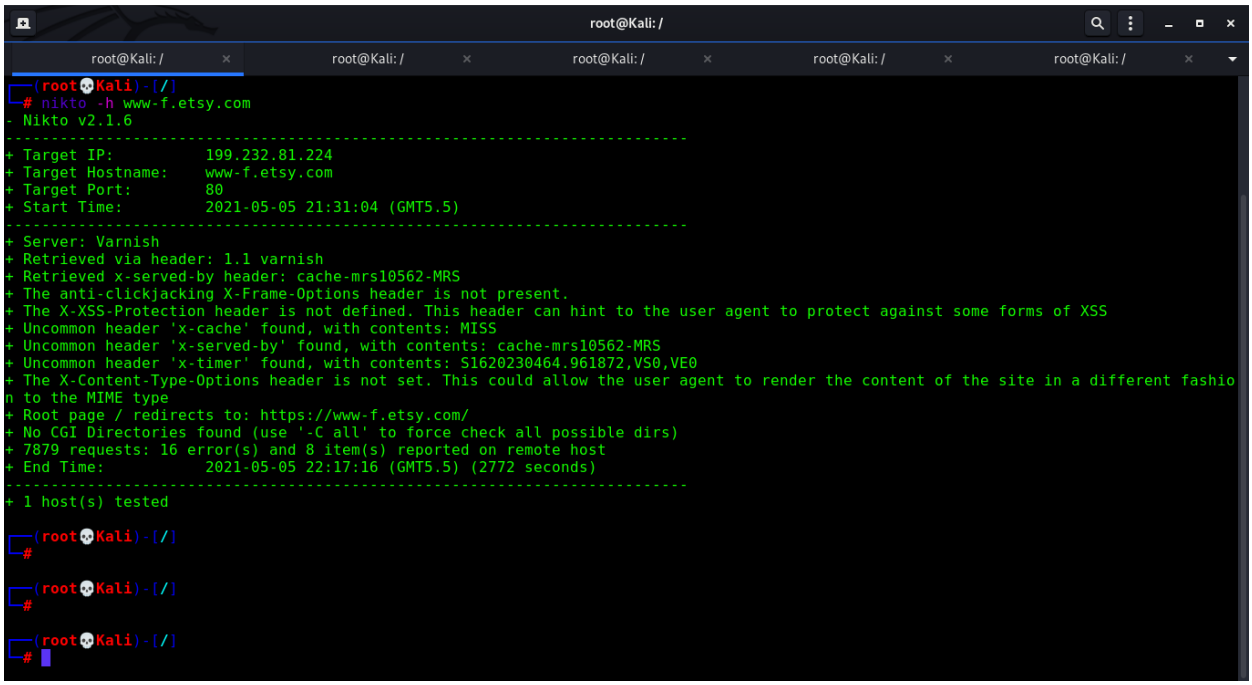
- **road10.etsy.com**



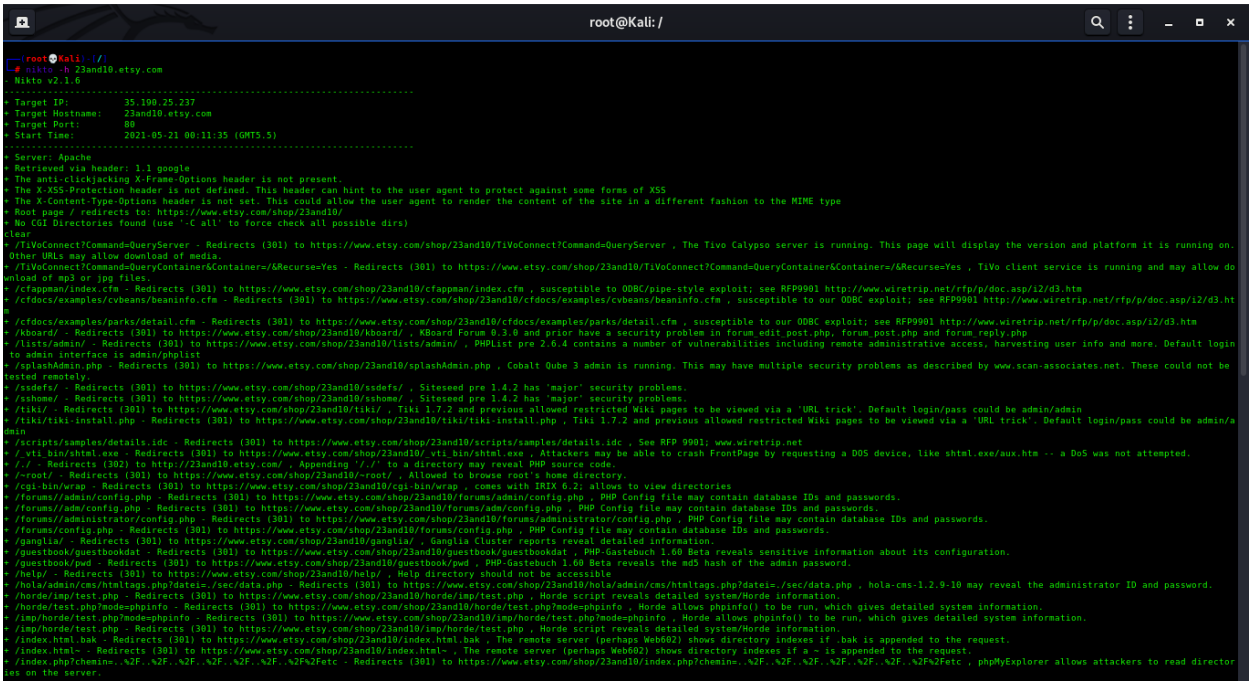
- **vm.ny5.etsy.com**

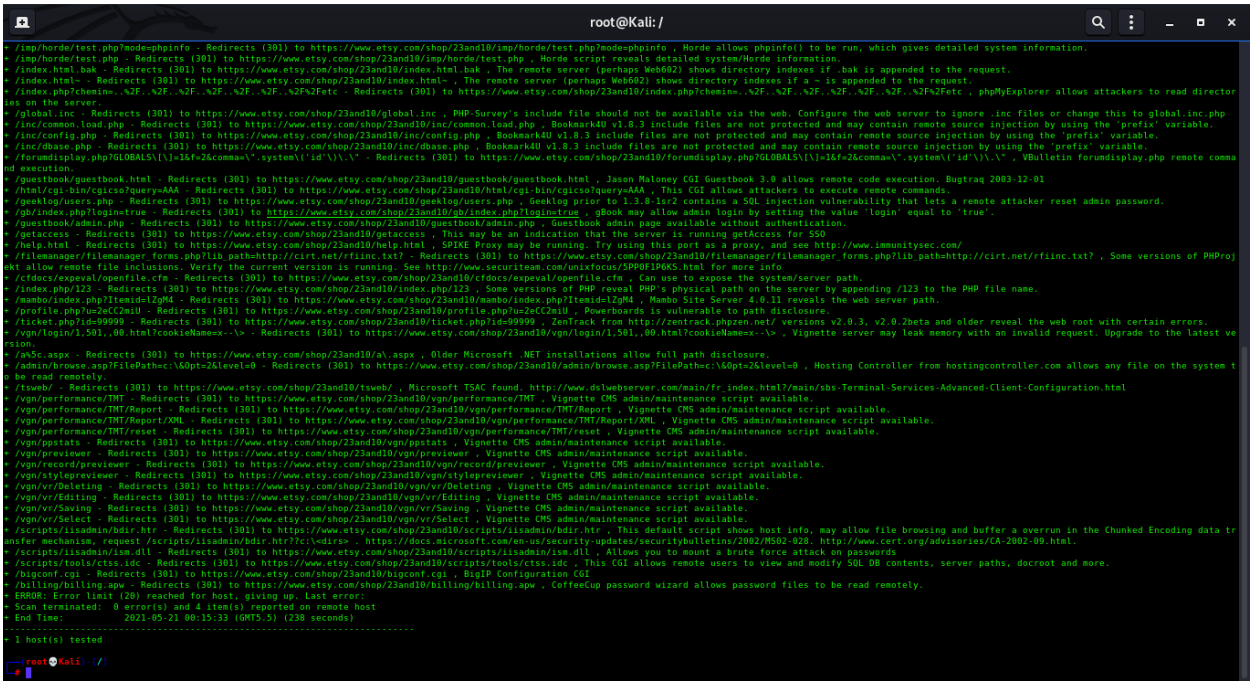


- **www-f.etsy.com**

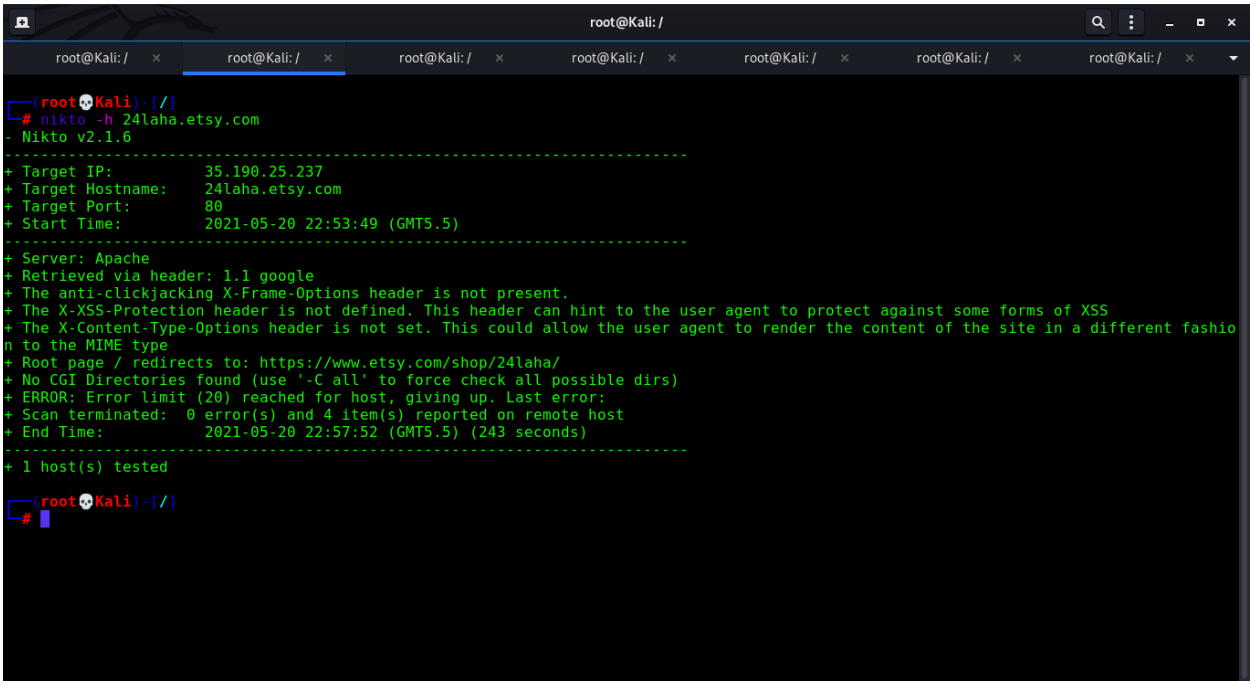


➢ 23and10.etsy.com

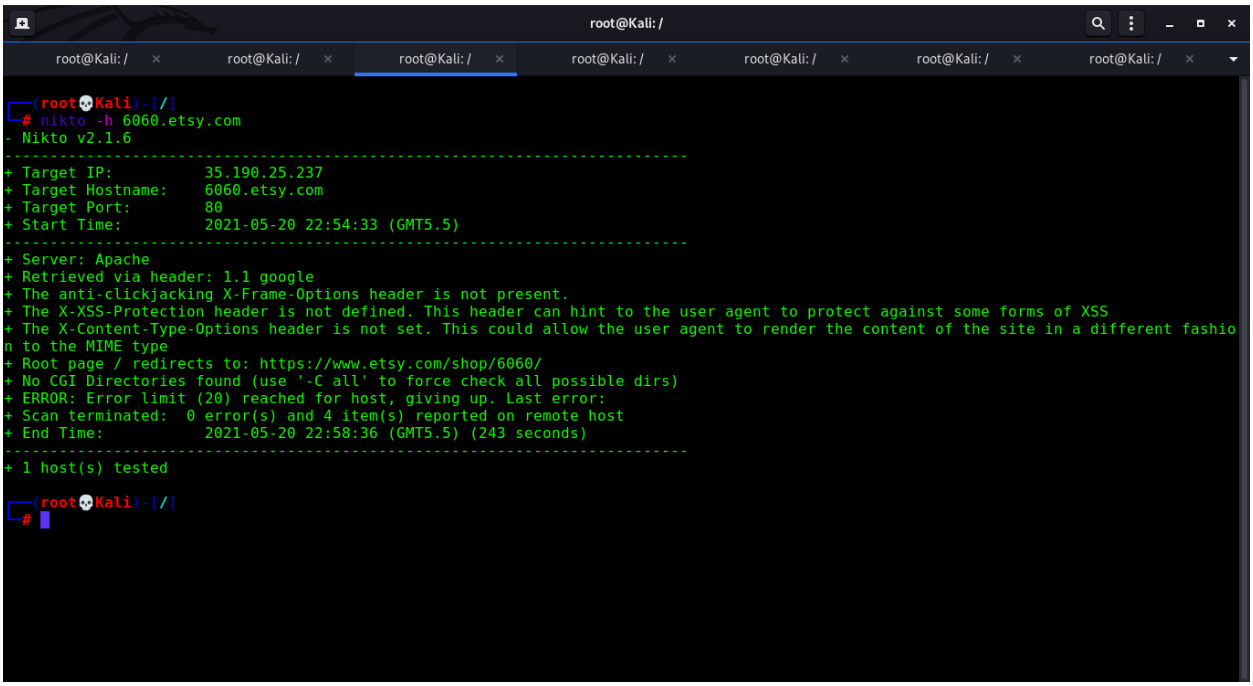




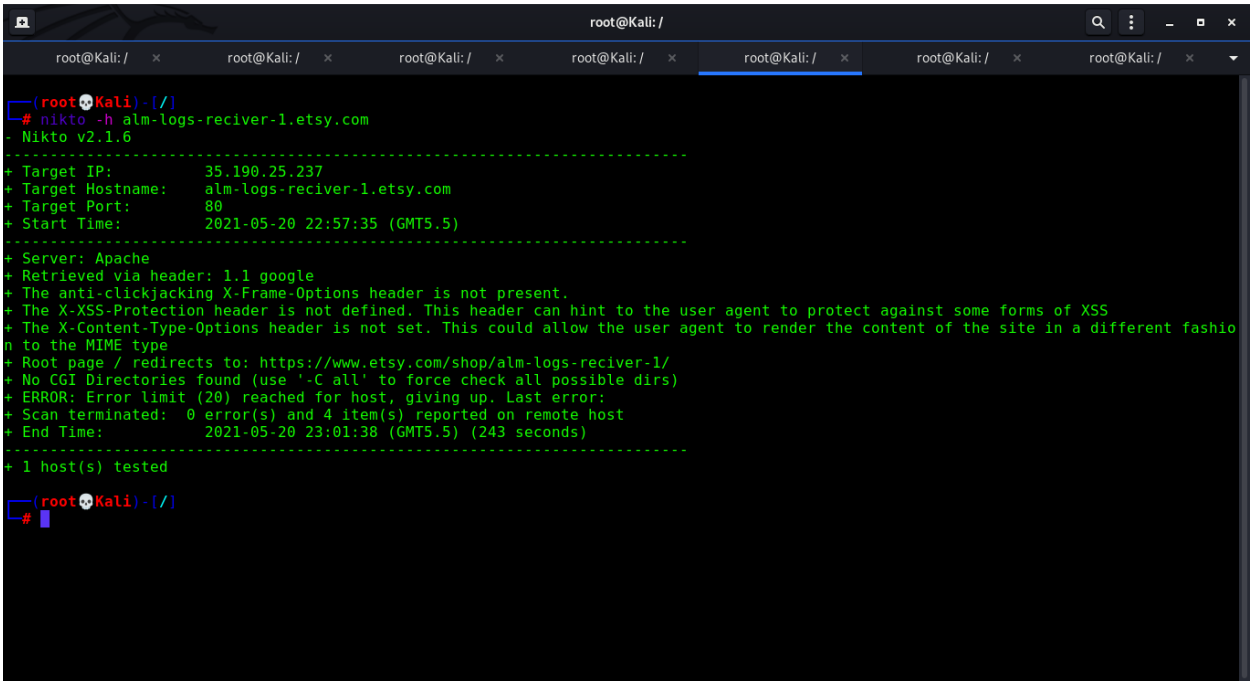
- **24laha.etsy.com**



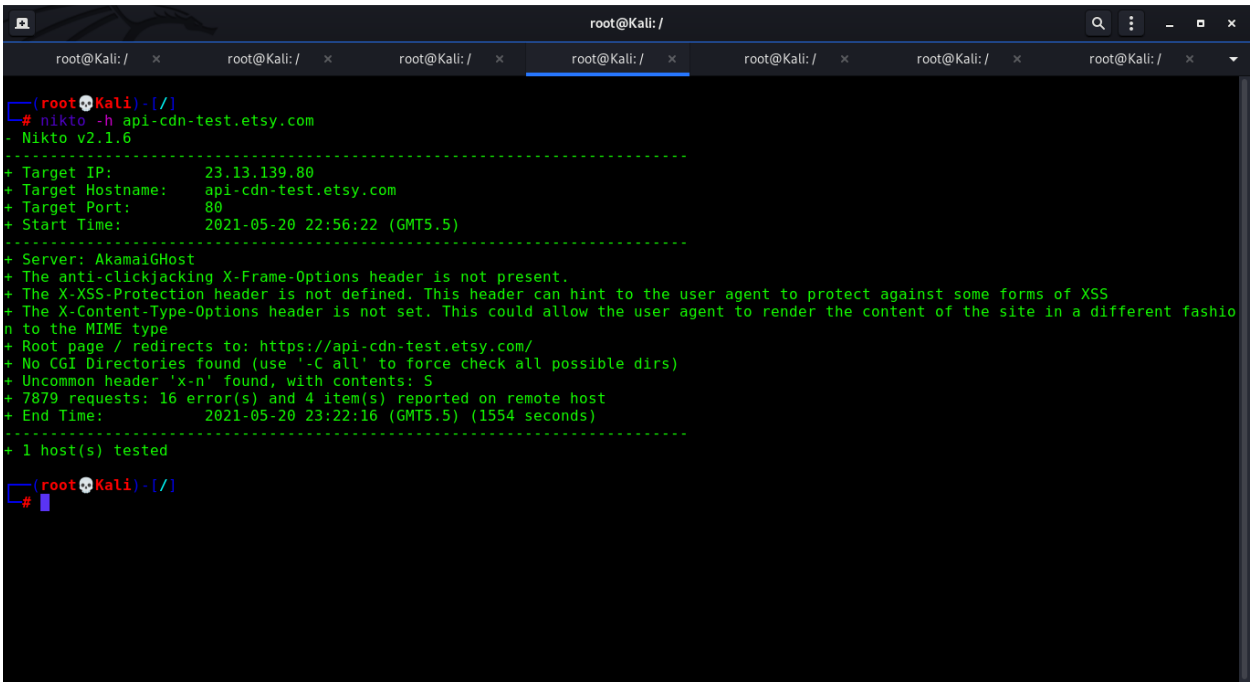
- **6060.etsy.com**



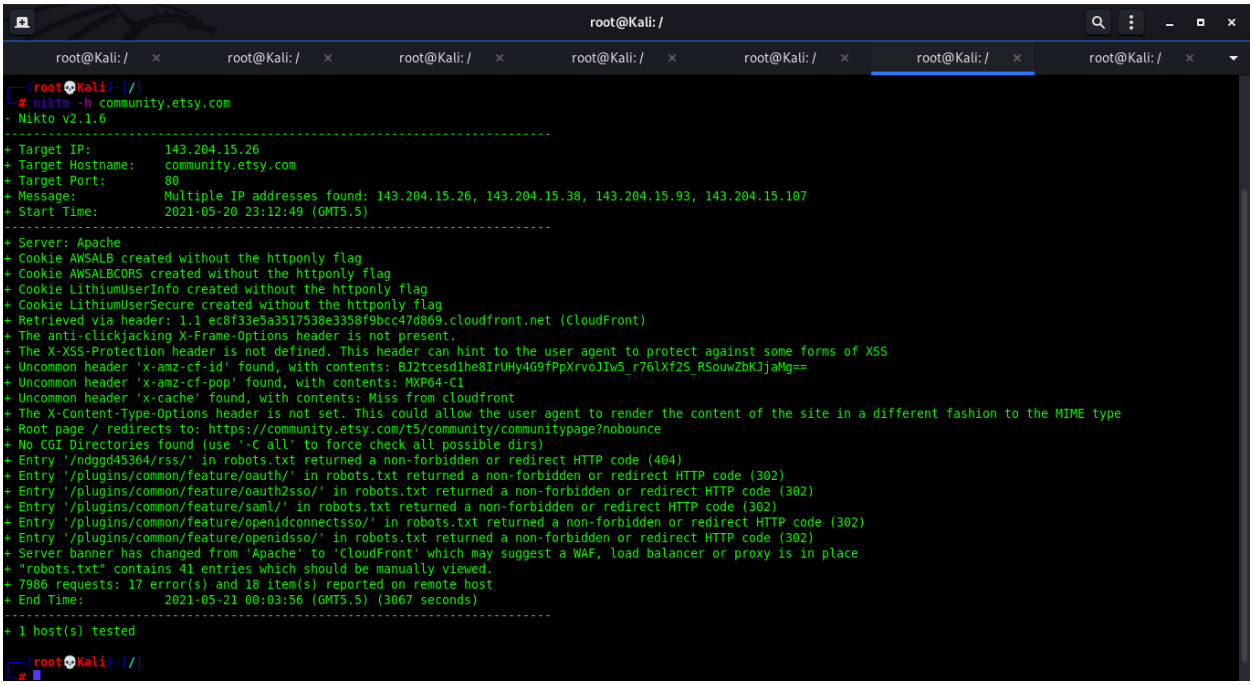
- **Alm-logs-reciver-1.etsy.com**



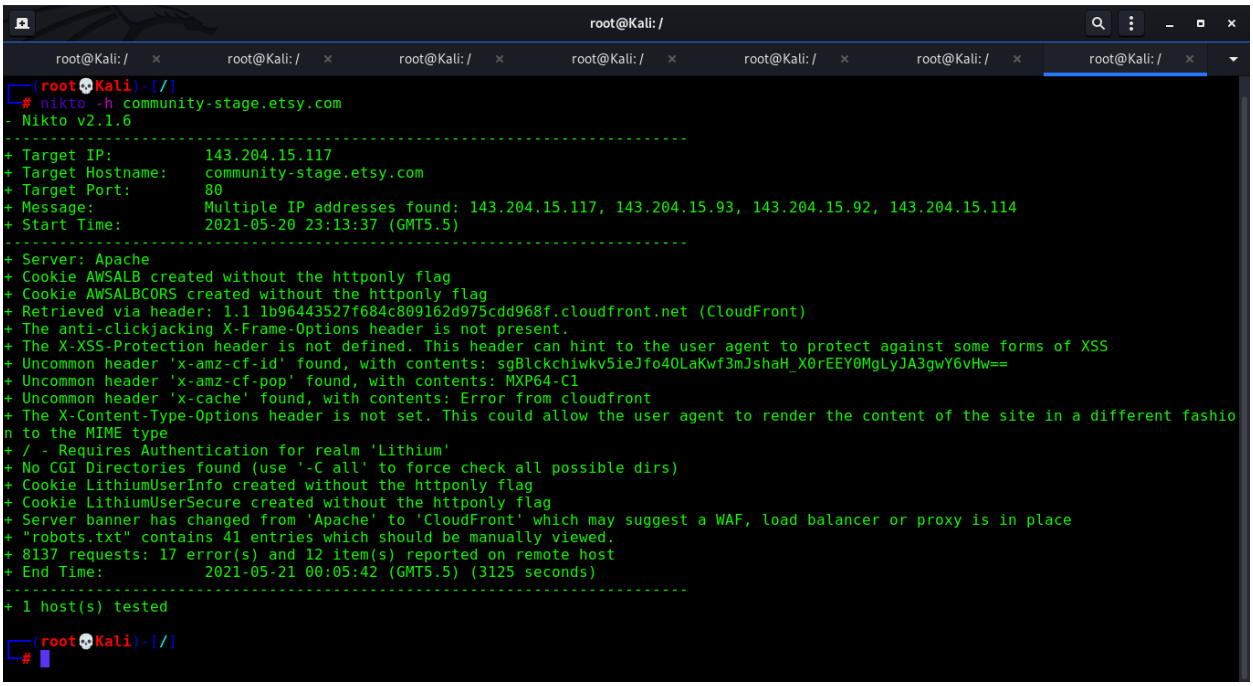
- **Api-cdn-test.etsy.com**



- **Community.etsy.com**



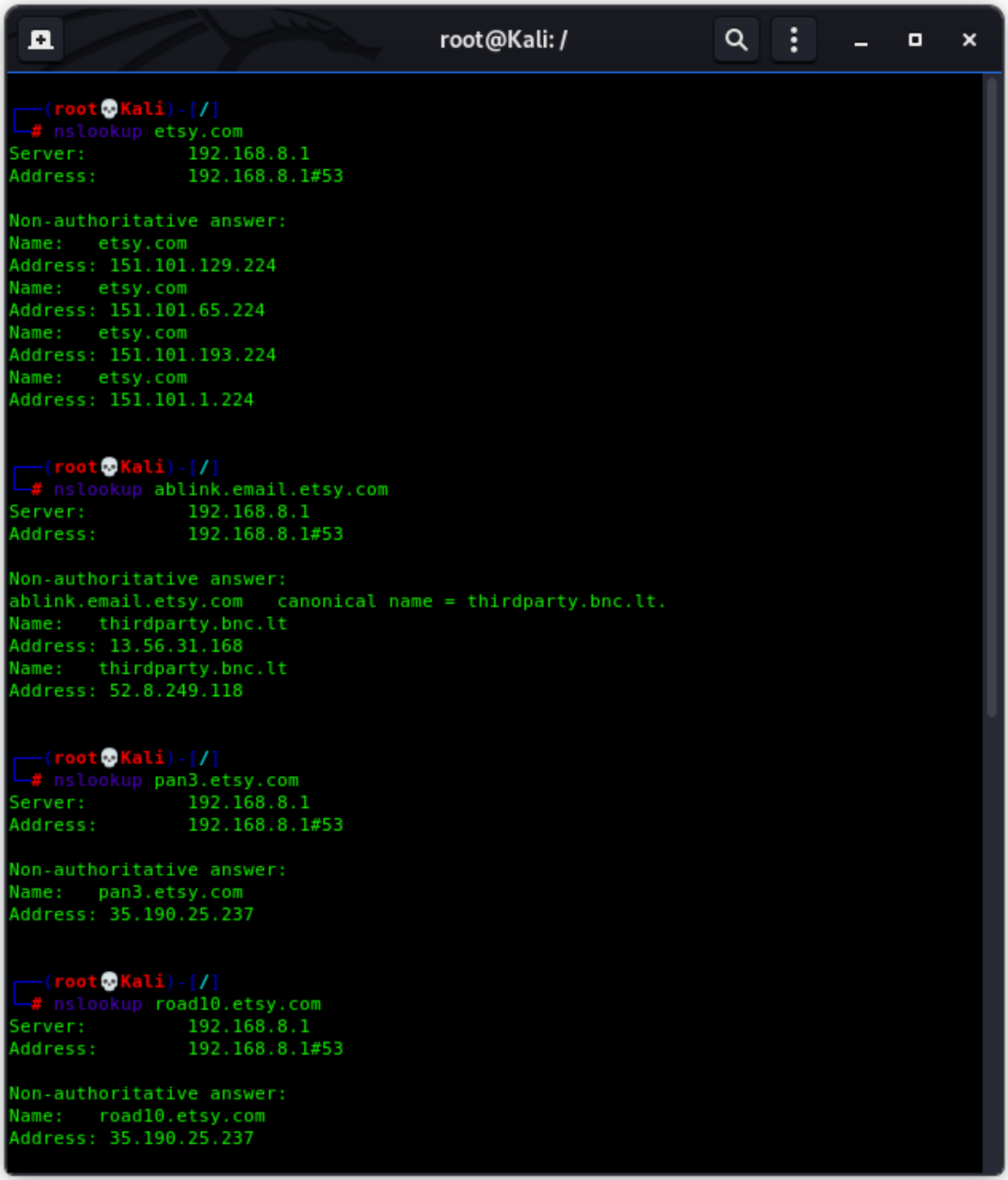
- **Community-stage.etsy.com**

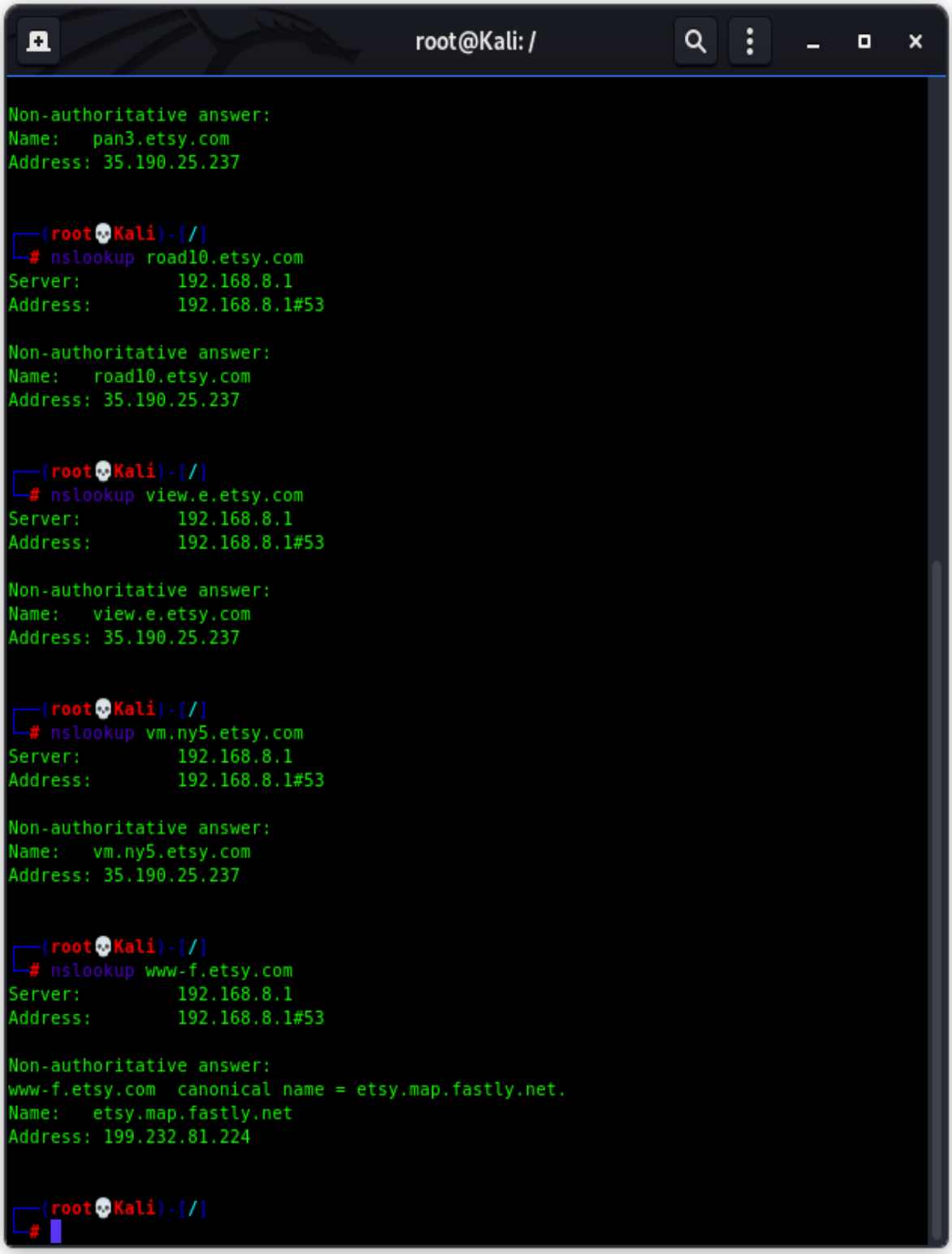


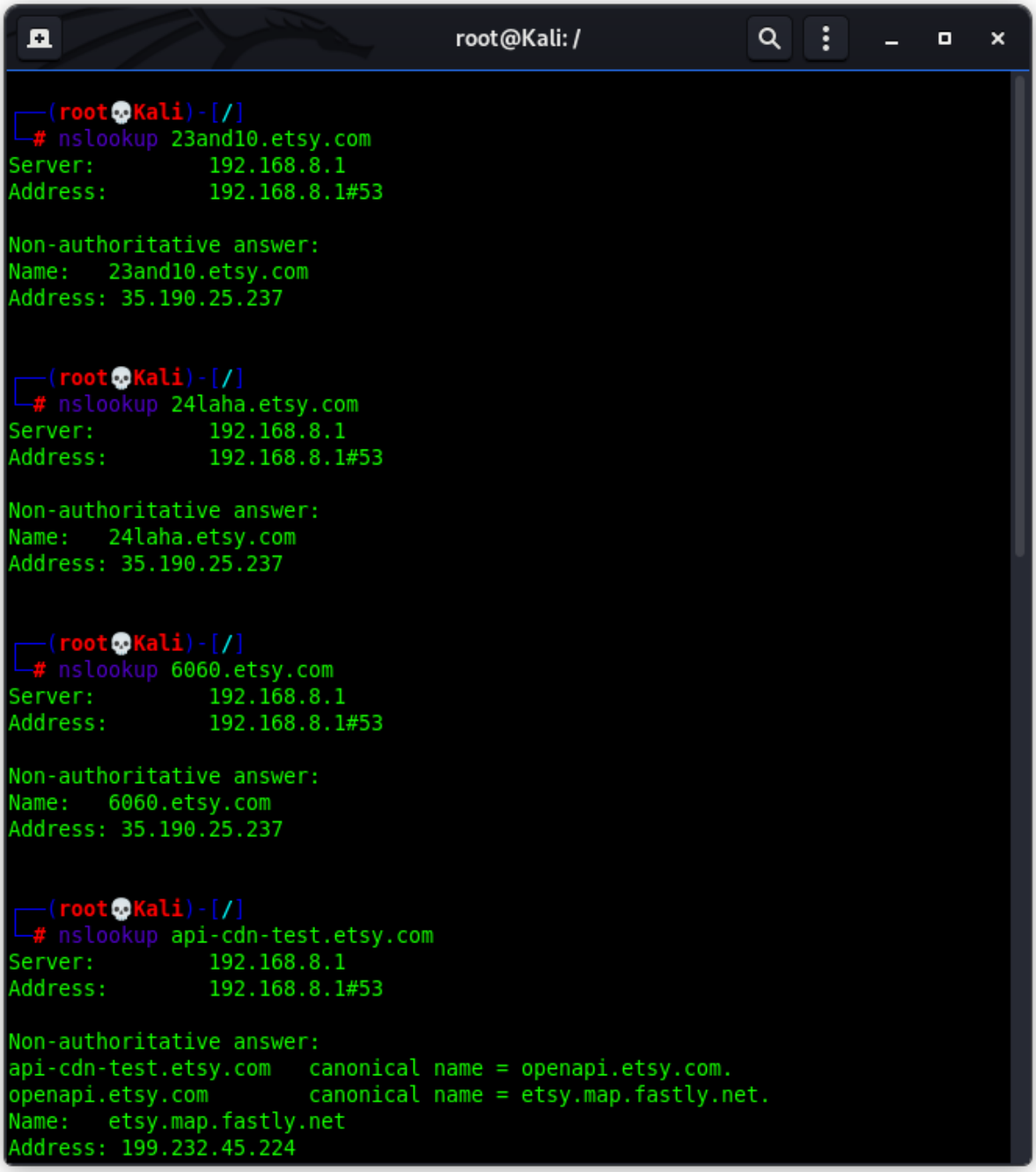
7. Discover host and Ip Addresses

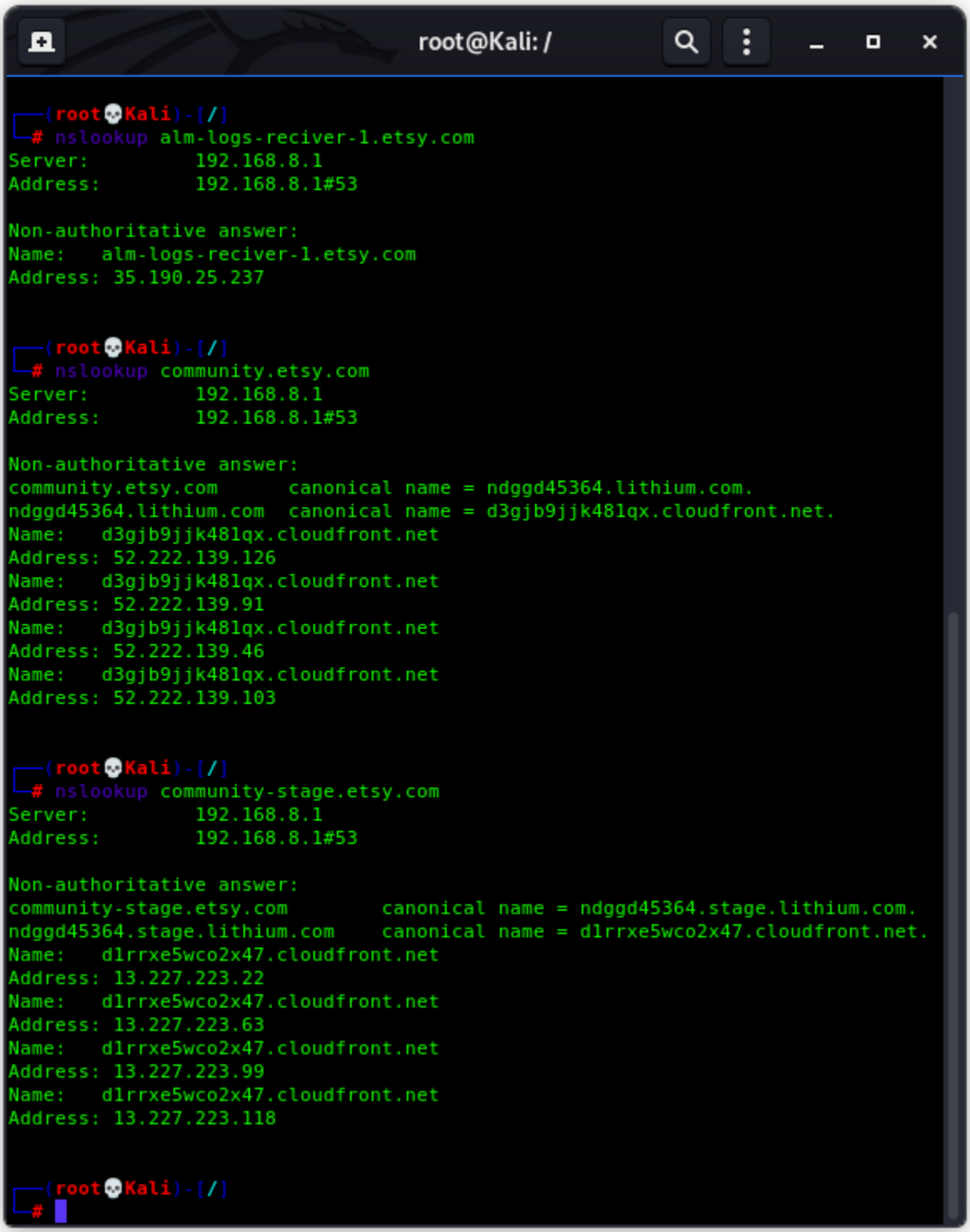
7.1 Nslookup

I used nslookup to get ip address in domain and subdomains.




root@Kali: /
Non-authoritative answer:
Name: pan3.etsy.com
Address: 35.190.25.237
┌──(root💀Kali)-[/]
└─# nslookup road10.etsy.com
Server: 192.168.8.1
Address: 192.168.8.1#53
Non-authoritative answer:
Name: road10.etsy.com
Address: 35.190.25.237
┌──(root💀Kali)-[/]
└─# nslookup view.e.etsy.com
Server: 192.168.8.1
Address: 192.168.8.1#53
Non-authoritative answer:
Name: view.e.etsy.com
Address: 35.190.25.237
┌──(root💀Kali)-[/]
└─# nslookup vm.ny5.etsy.com
Server: 192.168.8.1
Address: 192.168.8.1#53
Non-authoritative answer:
Name: vm.ny5.etsy.com
Address: 35.190.25.237
┌──(root💀Kali)-[/]
└─# nslookup www-f.etsy.com
Server: 192.168.8.1
Address: 192.168.8.1#53
Non-authoritative answer:
www-f.etsy.com canonical name = etsy.map.fastly.net.
Name: etsy.map.fastly.net
Address: 199.232.81.224
┌──(root💀Kali)-[/]
└─#


root@Kali: /
┌──(root💀Kali)-[/]
└─# nslookup 23and10.etsy.com
Server: 192.168.8.1
Address: 192.168.8.1#53
Non-authoritative answer:
Name: 23and10.etsy.com
Address: 35.190.25.237
┌──(root💀Kali)-[/]
└─# nslookup 24laha.etsy.com
Server: 192.168.8.1
Address: 192.168.8.1#53
Non-authoritative answer:
Name: 24laha.etsy.com
Address: 35.190.25.237
┌──(root💀Kali)-[/]
└─# nslookup 6060.etsy.com
Server: 192.168.8.1
Address: 192.168.8.1#53
Non-authoritative answer:
Name: 6060.etsy.com
Address: 35.190.25.237
┌──(root💀Kali)-[/]
└─# nslookup api-cdn-test.etsy.com
Server: 192.168.8.1
Address: 192.168.8.1#53
Non-authoritative answer:
api-cdn-test.etsy.com canonical name = openapi.etsy.com.
openapi.etsy.com canonical name = etsy.map.fastly.net.
Name: etsy.map.fastly.net
Address: 199.232.45.224


root@Kali: /
┌──(root💀Kali)-[/]
└─# nslookup alm-logs-reciver-1.etsy.com
Server: 192.168.8.1
Address: 192.168.8.1#53
Non-authoritative answer:
Name: alm-logs-reciver-1.etsy.com
Address: 35.190.25.237
┌──(root💀Kali)-[/]
└─# nslookup community.etsy.com
Server: 192.168.8.1
Address: 192.168.8.1#53
Non-authoritative answer:
community.etsy.com canonical name = ndggd45364.lithium.com.
ndggd45364.lithium.com canonical name = d3gjb9jjk481qx.cloudfront.net.
Name: d3gjb9jjk481qx.cloudfront.net
Address: 52.222.139.126
Name: d3gjb9jjk481qx.cloudfront.net
Address: 52.222.139.91
Name: d3gjb9jjk481qx.cloudfront.net
Address: 52.222.139.46
Name: d3gjb9jjk481qx.cloudfront.net
Address: 52.222.139.103
┌──(root💀Kali)-[/]
└─# nslookup community-stage.etsy.com
Server: 192.168.8.1
Address: 192.168.8.1#53
Non-authoritative answer:
community-stage.etsy.com canonical name = ndggd45364.stage.lithium.com.
ndggd45364.stage.lithium.com canonical name = d1rrxe5wco2x47.cloudfront.net.
Name: d1rrxe5wco2x47.cloudfront.net
Address: 13.227.223.22
Name: d1rrxe5wco2x47.cloudfront.net
Address: 13.227.223.63
Name: d1rrxe5wco2x47.cloudfront.net
Address: 13.227.223.99
Name: d1rrxe5wco2x47.cloudfront.net
Address: 13.227.223.118
┌──(root💀Kali)-[/]
└─#

- **As result I found below ip address in domain and subdomains.**

- **nslookup etsy.com**

  - Server: 192.168.8.1
  - Address: 192.168.8.1#53

  - Non-authoritative answer:
  - Name: etsy.com
  - Address: 151.101.1.224
  - Name: etsy.com
  - Address: 151.101.193.224
  - Name: etsy.com
  - Address: 151.101.65.224
  - Name: etsy.com
  - Address: 151.101.129.224

- **nslookup ablink.email.etsy.com**

  - Server: 192.168.8.1
  - Address: 192.168.8.1#53
  -
  - Non-authoritative answer:
  - ablink.email.etsy.com canonical name = thirdparty.bnc.lt.
  - Name: thirdparty.bnc.lt
  - Address: 13.56.31.168
  - Name: thirdparty.bnc.lt
  - Address: 52.8.249.118

- **nslookup pan3.etsy.com**
  - Server: 192.168.8.1
  - Address: 192.168.8.1#53

  - Non-authoritative answer:
  - Name: pan3.etsy.com
  - Address: 35.190.25.237

- **nslookup road10.etsy.com**
  - Server: 192.168.8.1
  - Address: 192.168.8.1#53

  - Non-authoritative answer:
  - Name: road10.etsy.com
  - Address: 35.190.25.237

- **nslookup vm.ny5.etsy.com**
  - Server: 192.168.8.1
  - Address: 192.168.8.1#53

  - Non-authoritative answer:
  - Name: vm.ny5.etsy.com
  - Address: 35.190.25.237

- **nslookup www-f.etsy.com**
  - Server: 192.168.8.1
  - Address: 192.168.8.1#53

  - Non-authoritative answer:
  - www-f.etsy.com canonical name = etsy.map.fastly.net.
  - Name: etsy.map.fastly.net
  - Address: 199.232.45.224

- **nslookup 23and10.etsy.com**
  - Server: 192.168.8.1
  - Address: 192.168.8.1#53

  - Non-authoritative answer:
  - Name: 23and10.etsy.com
  - Address: 35.190.25.237

- **nslookup 24laha.etsy.com**
  - Server: 192.168.8.1
  - Address: 192.168.8.1#53

  - Non-authoritative answer:
  - Name: 24laha.etsy.com
  - Address: 35.190.25.237

- **nslookup 6060.etsy.com**
  - Server: 192.168.8.1
  - Address: 192.168.8.1#53

  - Non-authoritative answer:
  - Name: 6060.etsy.com
  - Address: 35.190.25.237

- **nslookup api-cdn-test.etsy.com**
  - Server: 192.168.8.1
  - Address: 192.168.8.1#53

  - Non-authoritative answer:
  - api-cdn-test.etsy.com canonical name = openapi.etsy.com.
  - openapi.etsy.com canonical name = etsy.map.fastly.net.
  - Name: etsy.map.fastly.net
  - Address: 199.232.45.224

- **nslookup alm-logs-reciver-1.etsy.com**
  - Server: 192.168.8.1
  - Address: 192.168.8.1#53

  - Non-authoritative answer:
  - Name: alm-logs-reciver-1.etsy.com
  - Address: 35.190.25.237

- **nslookup community.etsy.com**
  - Server: 192.168.8.1
  - Address: 192.168.8.1#53

  - Non-authoritative answer:
  - community.etsy.com canonical name = ndggd45364.lithium.com.
  - ndggd45364.lithium.com canonical name = d3gjb9jjk481qx.cloudfront.net.
  - Name: d3gjb9jjk481qx.cloudfront.net
  - Address: 52.222.139.126
  - Name: d3gjb9jjk481qx.cloudfront.net
  - Address: 52.222.139.91
  - Name: d3gjb9jjk481qx.cloudfront.net
  - Address: 52.222.139.46
  - Name: d3gjb9jjk481qx.cloudfront.net
  - Address: 52.222.139.103

- **nslookup community-stage.etsy.com**
  - Server: 192.168.8.1
  - Address: 192.168.8.1#53

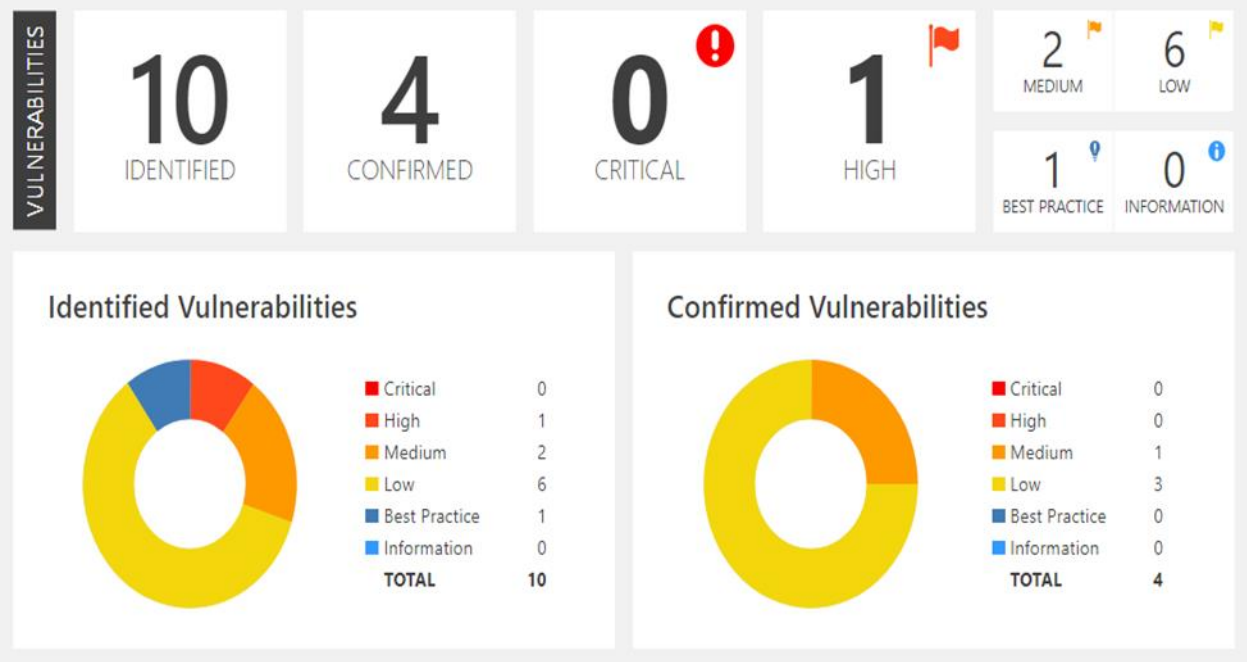
  - Non-authoritative answer:
  - community-stage.etsy.com canonical name = ndggd45364.stage.lithium.com.
  - ndggd45364.stage.lithium.com canonical name = d1rrxe5wco2x47.cloudfront.net.
  - Name: d1rrxe5wco2x47.cloudfront.net
  - Address: 13.227.223.22
  - Name: d1rrxe5wco2x47.cloudfront.net
  - Address: 13.227.223.63

- Name: d1rrxe5wco2x47.cloudfront.net
- Address: 13.227.223.99
- Name: d1rrxe5wco2x47.cloudfront.net
- Address: 13.227.223.118

8. Vulnerability Analyzing Phase and Recommendation

I used Netsparker Professional version to Vulnerability Analyzing Phase and Recommendation. We can generate a Details report, summary report, and OWASP Top 10 Security risk report for our scope. I scanned below domains categorized under OWASP top 10.

8.1 Target Domain - https://www.etsy.com



USING COMPONENTS WITH KNOWN VULNERABILITIES

A. Out-of-date Version (Underscore.js)

Method: GET
Severity: HIGH

Netsparker identified that the target web site is using Underscore.js and detected that it is out of date.

Impact

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

Underscore.js Improper Control of Generation of Code ('Code Injection') Vulnerability

The package underscore from 1.13.0-0 and before 1.13.0-2, from 1.3.2 and before 1.12.1 are vulnerable to Arbitrary Code Injection via the template function, particularly when a variable property is passed as an argument as it is not sanitized.

B. Weak Ciphers Enabled

Method: GET

Severity: MEDIUM

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

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

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. 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 `regedt32`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\MD5
```

Proof of Concept

A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES

	Out-of-date Version (Underscore.js)	GET	https://www.etsy.com/	HIGH
	Out-of-date Version (jQuery)	GET	https://www.etsy.com/	MEDIUM

SENSITIVE DATA EXPOSURE

A. Weak Cipher Enabled

Method: GET
Severity: MIDIUM

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.

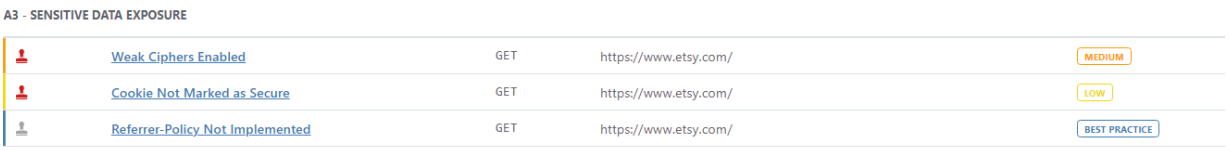
Impact

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

Remedy

Configure your web server to disallow using weak ciphers.

Proof of Concept



Actions to Take

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

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

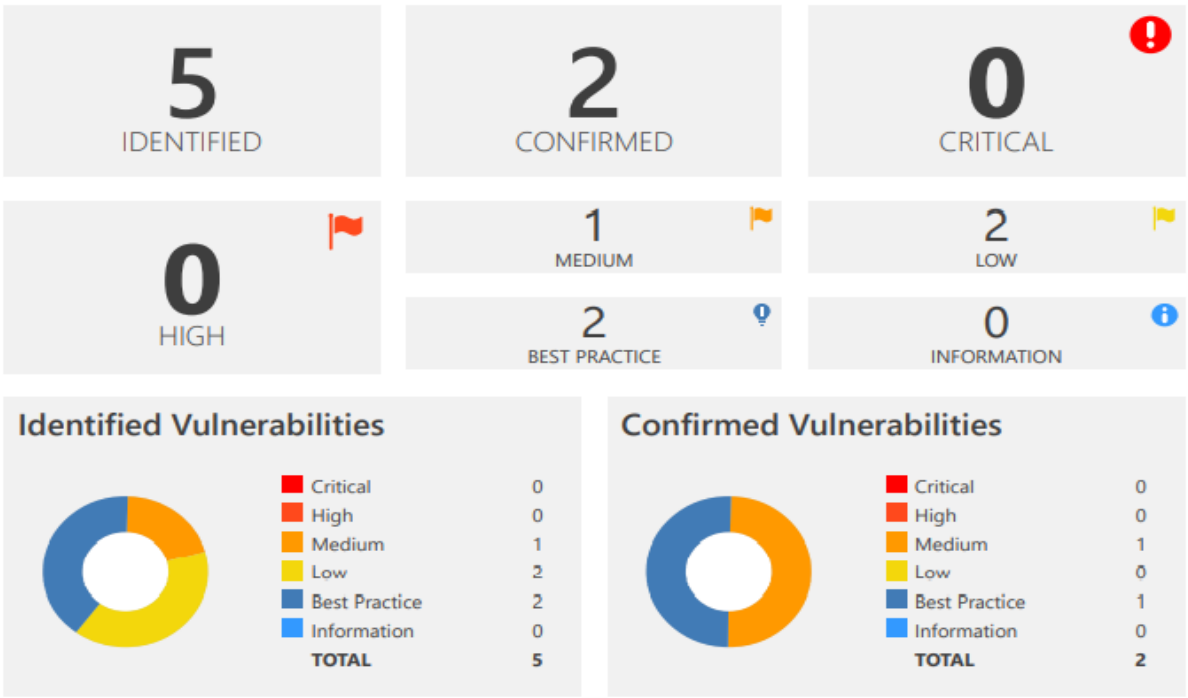
```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. 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 `regedt32`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\MD5
```

8.2 Target Domain - https://ablink.email.etsy.com



SENSITIVE DATA EXPOSURE

A. Weak Ciphers Enabled

Method: GET
Severity: MIDIUM

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.

List of Supported Weak Ciphers

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)**Request**
[NETSPARKER] SSL Connection

Response
Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No [NETSPARKER] SSL Connection

Remedy

Configure your web server to disallow using weak ciphers.

Actions to Take

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

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. 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 `regedt32`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:

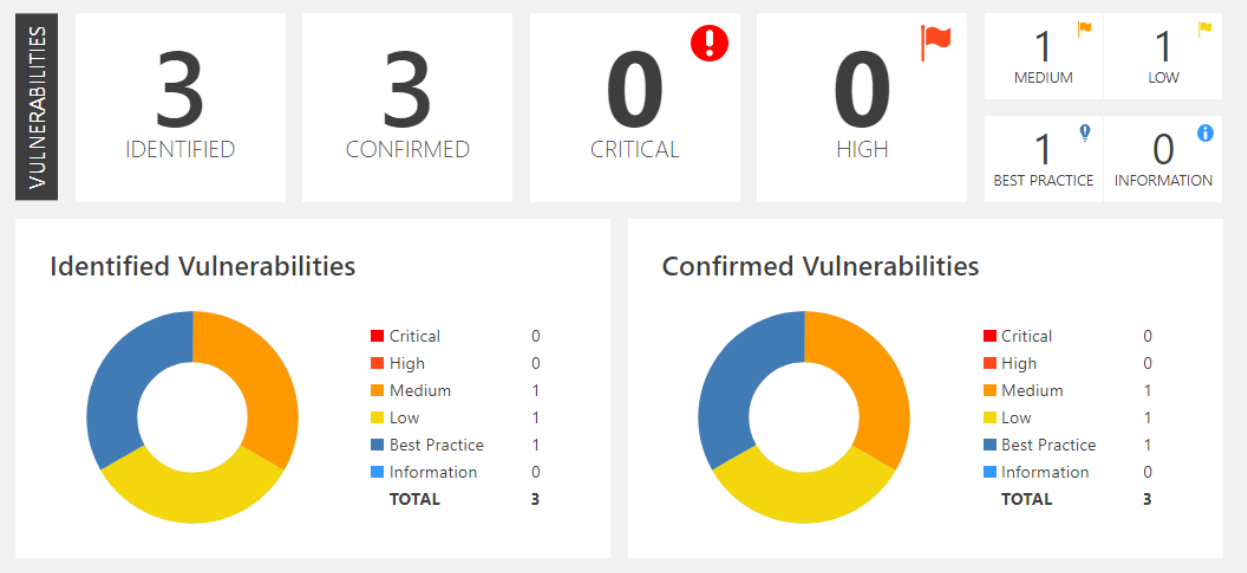
```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Proof of Concept

A3 - SENSITIVE DATA EXPOSURE

	Weak Ciphers Enabled	GET	https://ablink.email.etsy.com/	MEDIUM
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://ablink.email.etsy.com/	BEST PRACTICE
	Referrer-Policy Not Implemented	GET	https://ablink.email.etsy.com/	BEST PRACTICE

8.3 Target Domain - https://pan3.etsy.com



SENSITIVE DATA EXPOSURE

A. Weak Ciphers Enabled

Method: GET
Severity: MEDIUM

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

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

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

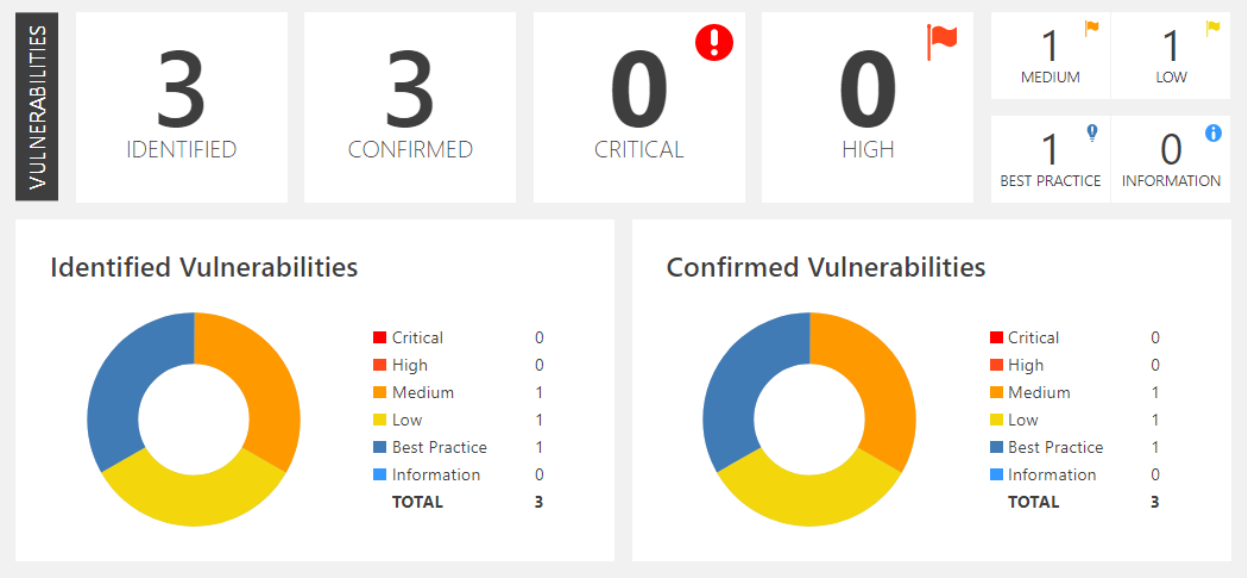
```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. 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 `regedt32`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\MD5
```

8.4 Target Domain - https://road10.etsy.com



SENSITIVE DATA EXPOSURE

A. Weak Ciphers Enabled

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

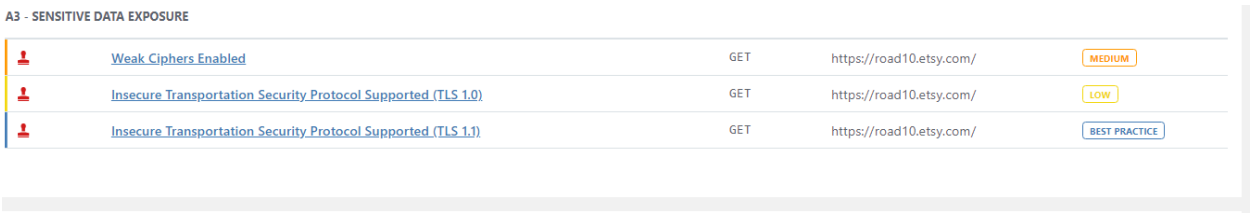
List of Supported Weak Ciphers

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)

Remedy

Configure your web server to disallow using weak ciphers.

Proof of Concept



Actions to Take

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

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

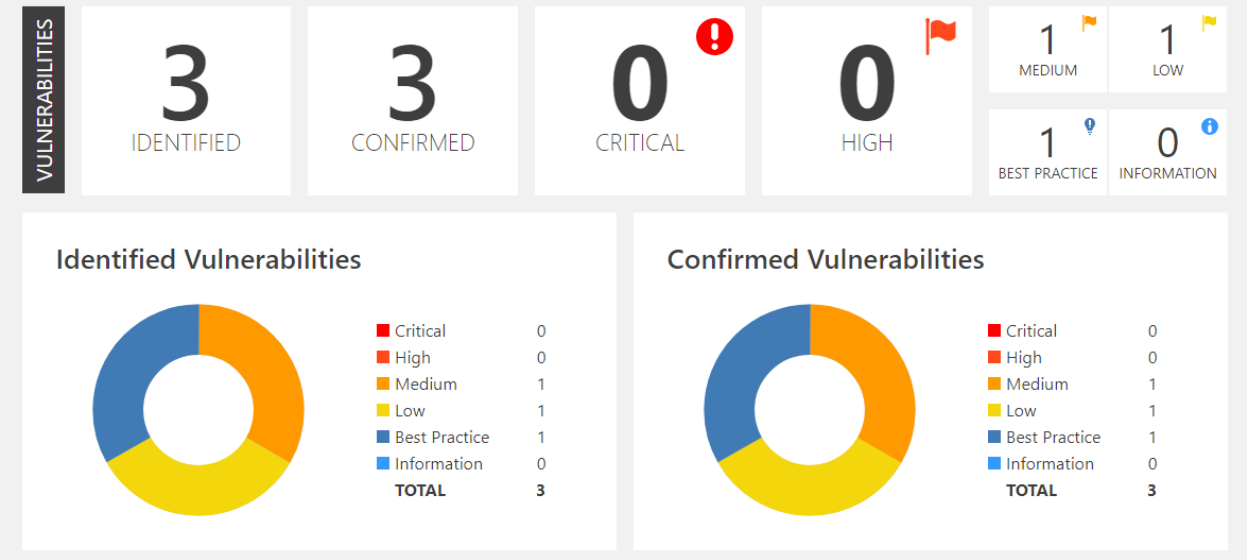
```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. 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 `regedt32`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\MD5
```

8.5 Target Domain - https://vm.ny5.etsy.com



SENSITIVE DATA EXPOSURE

A. Weak Ciphers Enabled

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.

List of Supported Weak Ciphers

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)

Actions to Take

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

   SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4

2. Lighttpd:

   ssl.honor-cipher-order = "enable"
   ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"

3. 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 regedt32or 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:

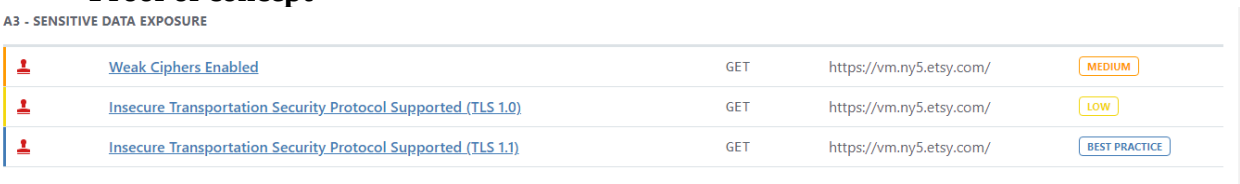
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128

SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5

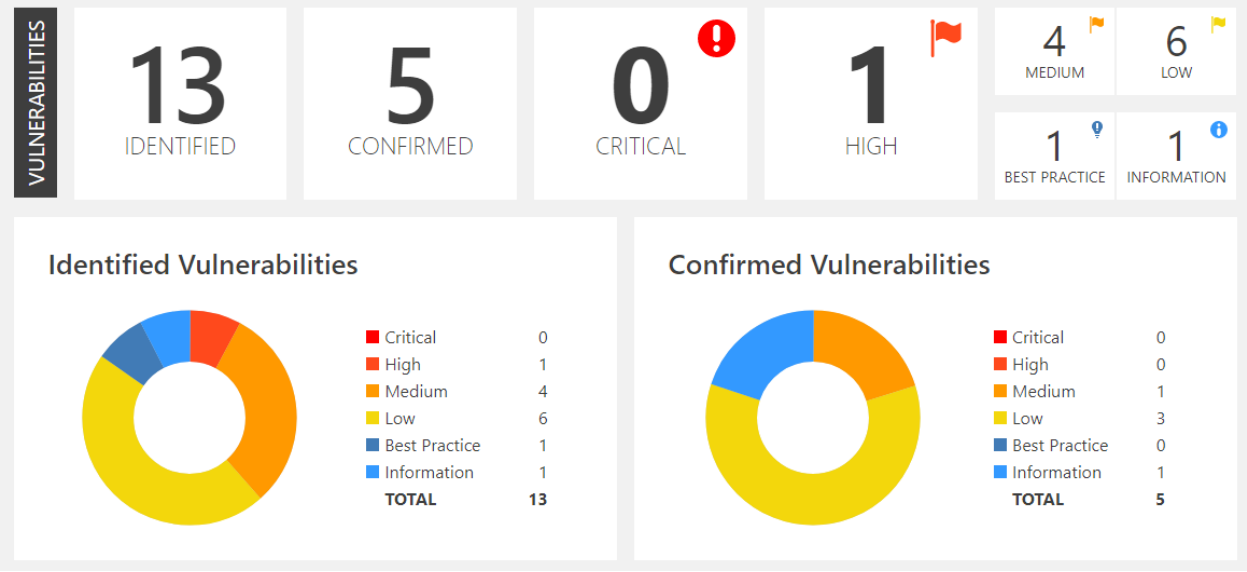
Remedy

Configure your web server to disallow using weak ciphers.

Proof of concept



8.6 Target Domain - https://www-f.etsy.com



USING COMPONENTS WITH KNOWN VULNERABILITIES

A. Out-of-date version (Underscore.js)

Netsparker identified that the target web site is using Underscore.js and detected that it is out of date.

Impact

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

Underscore.js Improper Control of Generation of Code ('Code Injection') Vulnerability

The package underscore from 1.13.0-0 and before 1.13.0-2, from 1.3.2 and before 1.12.1 are vulnerable to Arbitrary Code Injection via the template function, particularly when a variable property is passed as an argument as it is not sanitized.

Remedy

Please upgrade your installation of Underscore.js to the latest stable version.

B. [Possible] BREACH Attack Detected

Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website. Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.

Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

Impact

Even if you use an SSL/TLS protected connection, an attacker can still view the victim’s encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

- Inject partial plaintext they have uncovered into a victim's requests.
- Measure the size of encrypted traffic.

Remedy

Netsparker reported a Possible BREACH Attack issue because the target web page meets the following conditions that facilitate it:

- Served from a server that uses HTTP-level compression (ie. gzip)
- Reflects user-input in the HTTP response bodies
- Contains sensitive information (such as a CSRF token) in HTTP response bodies

To mitigate the issue, we recommend the following solutions:

1. If possible, disable HTTP level compression
2. Separate sensitive information from user input
3. Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
4. Hide the length of the traffic by adding a random number of bytes to the responses.
5. Add in a rate limit, so that the page maximum is reached five times per minute.

C. Out-of-date Version (jQuery)

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.

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

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.

Affected Versions

1.8.0 to 2.2.4

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

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

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

Remedy

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

Proof of Concept

A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES

Out-of-date Version (Underscore.js)	GET	https://www-f.etsy.com/	HIGH
[Possible] BREACH Attack Detected	GET	https://www-f.etsy.com/signin?from_page=https%3A%2F%2Fwww.etsy.com%2F&workflow=c3Vic2NyaWJlX3RvX2VtYWlsX2xpc3Q6bmV3X2F0X2V0c3k6MTYyMjEwOTQ4NjozYThkZWMzZTkyNzVkYTBiYWE4MjA0NjJmYjk0Y2RmZA==	MEDIUM
Out-of-date Version (jQuery)	GET	https://www-f.etsy.com/	MEDIUM

SECURITY MISCONFIGURATION

A. HTTP Strict Transport Security (HSTS) Errors and Warnings

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

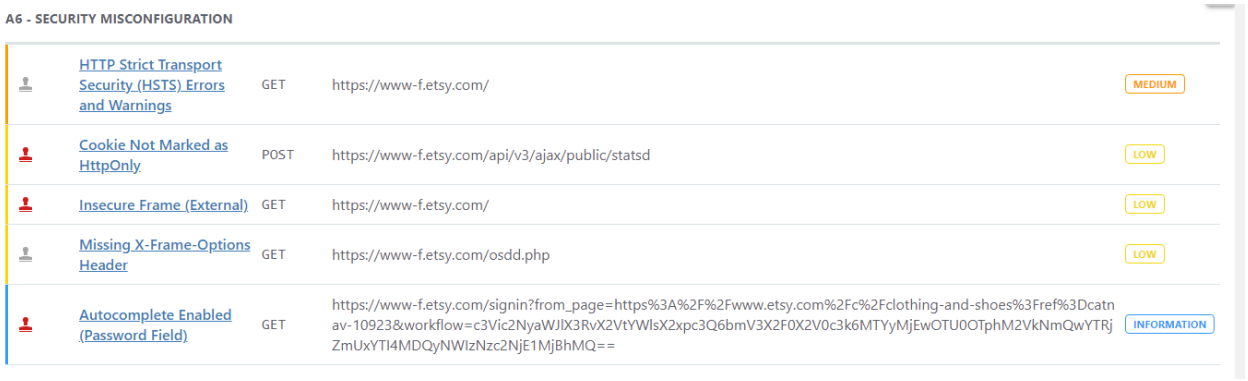
Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, 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-agemust be at least 31536000 seconds (1 year)
    - The includeSubDomainsdirective must be specified
    - The preloaddirective 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)

Proof of Concept



SENSITIVE DATA EXPOSURE

A. Weak Ciphers Enabled

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

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

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

3. ssl.honor-cipher-order = "enable"

```
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

4. 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.**

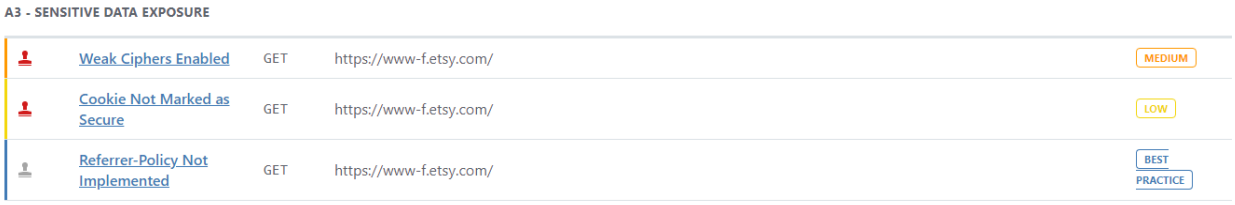
   a.Click Start, click Run, type regedt32or type regedit, and then click OK.
   b.In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
   c.Set "Enabled" DWORD to "0x0" for the following registry keys:

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\MD5

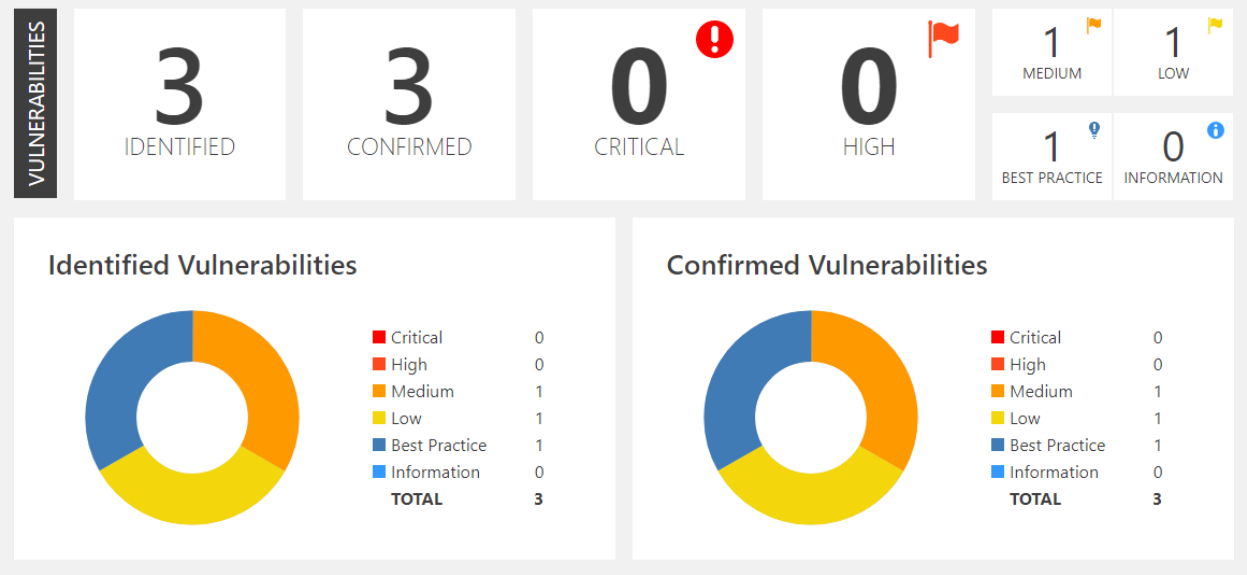
Remedy

Configure your web server to disallow using weak ciphers.

Proof of Concept



8.7 Target Domain - https://23and10.etsy.com



SENSITIVE DATA EXPOSURE

A. Weak Ciphers Enabled

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

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

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
3. ssl.honor-cipher-order = "enable"

ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

4. 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 regedt32or 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\MD5
```

Remedy

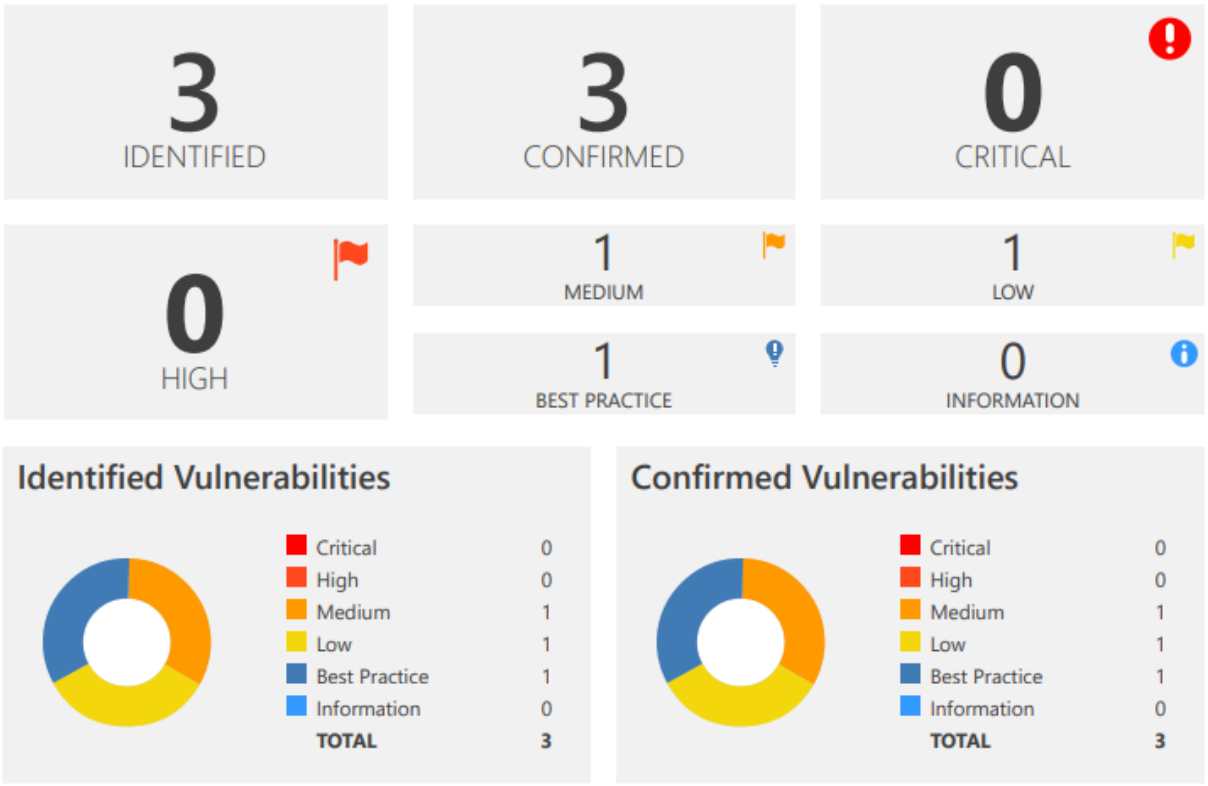
Configure your web server to disallow using weak ciphers.

Proof of Concept

A3 - SENSITIVE DATA EXPOSURE

	Weak Ciphers Enabled	GET	https://23and10.etsy.com/	MEDIUM
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://23and10.etsy.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://23and10.etsy.com/	BEST PRACTICE

8.8 Target Domain - https://24laha.etsy.com



SENSITIVE DATA EXPOSURE

A. Weak Ciphers Enabled

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.

List of Supported Weak Ciphers

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)

Request

[NETSPARKER] SSL Connection

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

[NETSPARKER] SSL Connection

Actions to Take

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

SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4

2. Lighttpd:

ssl.honor-cipher-order = "enable"

ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"

3. 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.

- Click Start, click Run, type regedt32or type regedit, and then click OK.
- In Registry Editor, locate the following registry key:
- HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

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

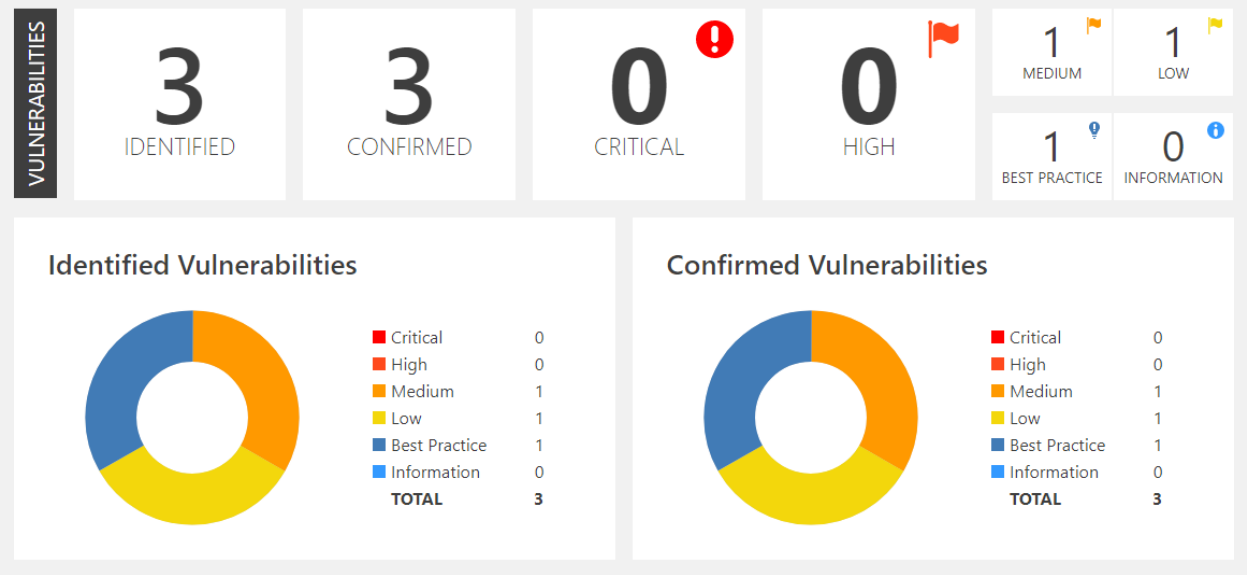
SCHANNEL\Hashes\MD5

Remedy

Configure your web server to disallow using weak ciphers.

Proof of concept

8.9 Target Domain - https://6060.etsy.com



SENSITIVE DATA EXPOSURE

A. Weak Ciphers Enabled

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

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

   SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4

2. Lighttpd:

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.**

1. Click Start, click Run, type regedt32or type regedit, and then click OK.
2. In Registry Editor, locate the following registry

3. key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

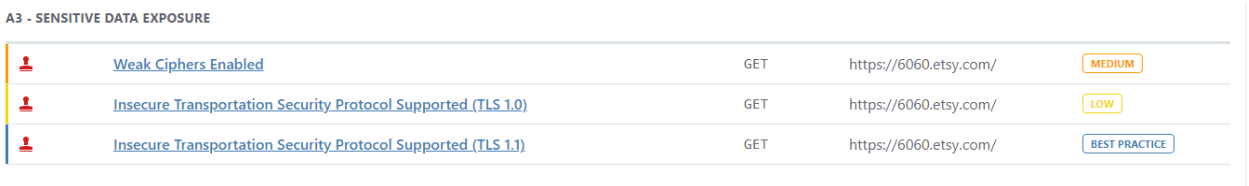
Set "Enabled" DWORD to "0x0" for the following registry keys:

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\MD5

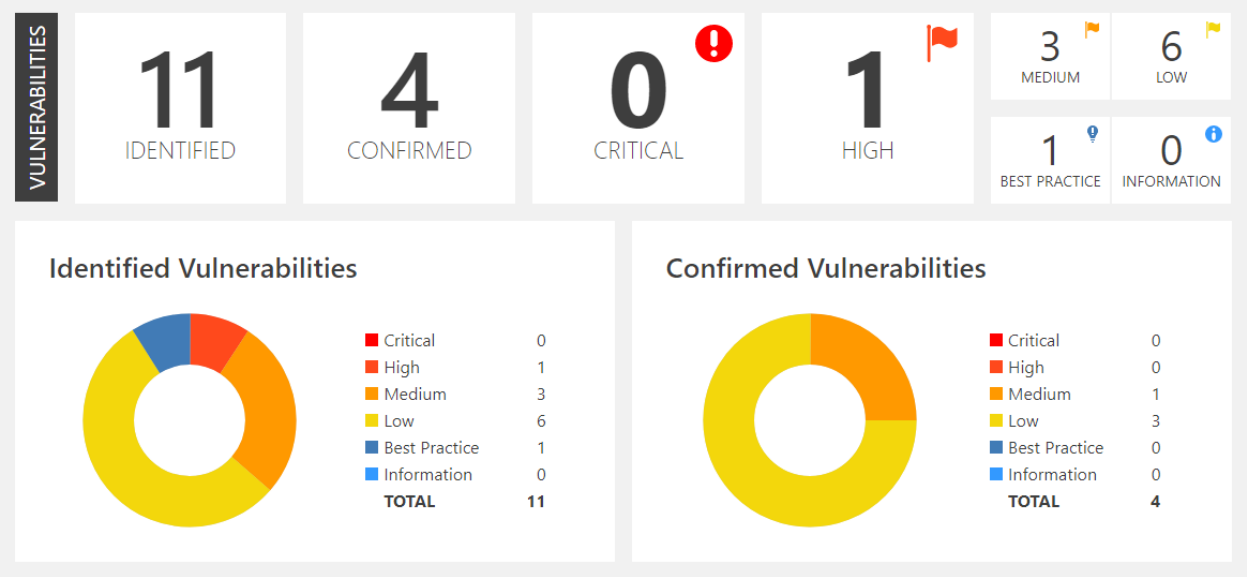
Remedy

Configure your web server to disallow using weak ciphers.

Proof of concept



8.10 Target Domain - https://api-cdn-test.etsy.com



SENSITIVE DATA EXPOSURE

A. Weak Ciphers Enabled

Method: GET

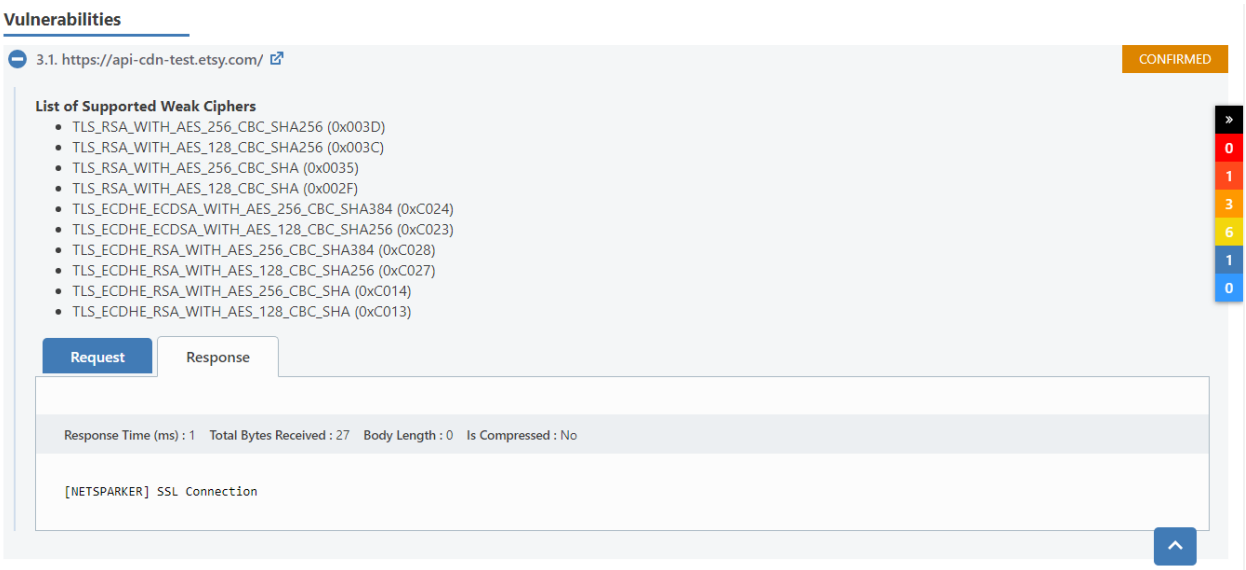
Severity: MIDIUM

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

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

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. 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.**

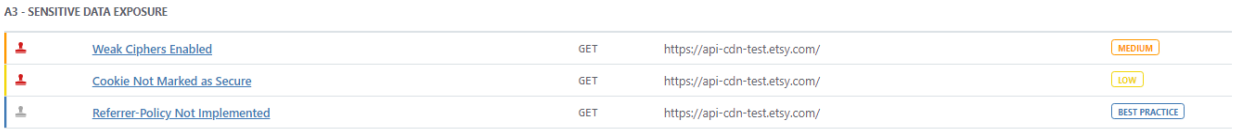
   a.Click Start, click Run, type `regedt32`or type `regedit`, and then click OK.
   b.In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
   c.Set "Enabled" DWORD to "0x0" for the following registry keys:

```
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\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

Proof of concept



Broken Access Control

A. [Possible] Cross-site Request Forgery

Method: GET
Severity: LOW

Netsparker identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.

  - For native XMLHttpRequest (XHR) object in JavaScript;

```
- xhr = new XMLHttpRequest();
- xhr.setRequestHeader('custom-header', 'valueNULL');
```

For JQuery, if you want to add a custom header (or set of headers) to

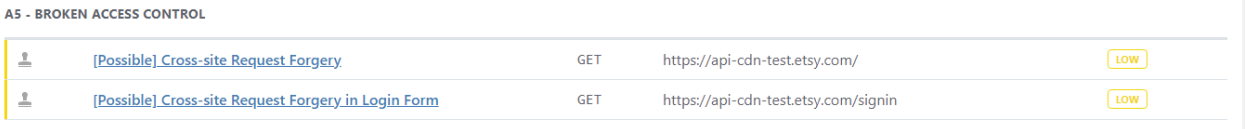
a. **individual request**

```
$.ajax({
    url: 'foo/bar',
    headers: { 'x-my-custom-header': 'some value' }
});
```

b. **every request**

```
$.ajaxSetup({
    headers: { 'x-my-custom-header': 'some value' }
});
OR
$.ajaxSetup({
    beforeSend: function(xhr) {
        xhr.setRequestHeader('x-my-custom-header', 'some value');
    }
});
```

Proof of Concept



SECURITY MISCONFIGURATION

A. HTTP Strict Transport Security (HSTS) Errors and Warnings

Method: GET

Severity: MIDIUM

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

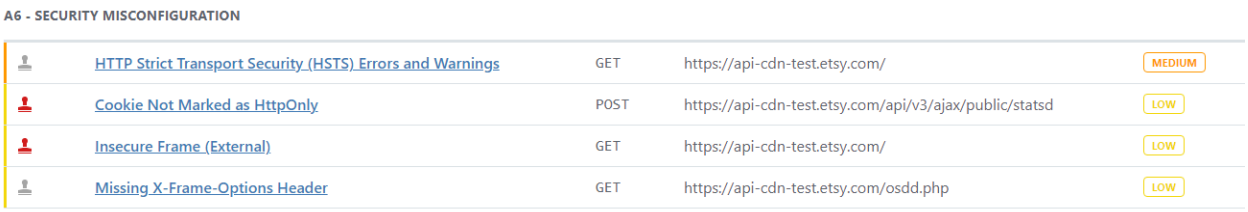
Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, 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 will not 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-agemust be at least 31536000 seconds (1 year)

- The includeSubDomainsdirective must be specified
- The preloaddirective 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)

Proof of Concept



USING COMPONENTS WITH KNOWN VULNERABILITIES

A. Out-of-date Version (Underscore.js)

Method: GET

Severity: HIGH

Netsparker identified that the target web site is using Underscore.js and detected that it is out of date.

Impact

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

Underscore.js Improper Control of Generation of Code ('Code Injection') Vulnerability

The package underscore from 1.13.0-0 and before 1.13.0-2, from 1.3.2 and before 1.12.1 are vulnerable to Arbitrary Code Injection via the template

function, particularly when a variable property is passed as an argument as it is not sanitized.

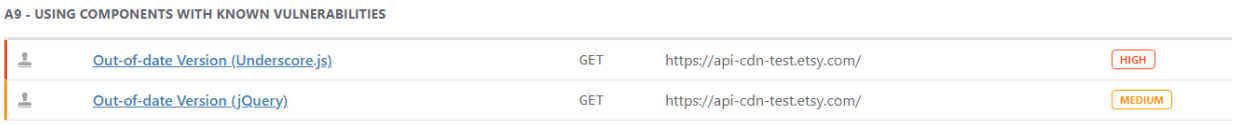
Affected Versions

1.3.2 to 1.12.0

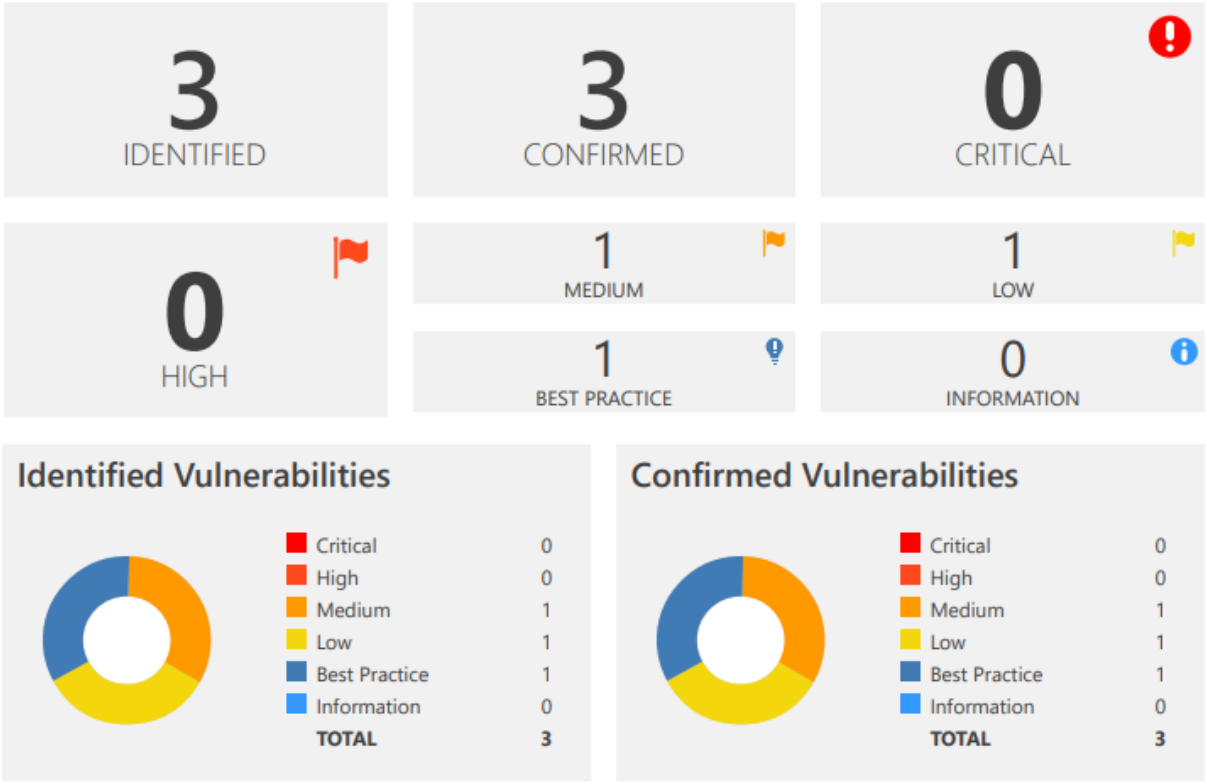
Remedy

Please upgrade your installation of Underscore.js to the latest stable version.

Proof of concept



8.11 Target Domain - https://alm-logs-reciver-1.etsy.com



SENSITIVE DATA EXPOSURE

A. Weak Ciphers Enabled

Method: GET
Severity: MIDIUM

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.

List of Supported Weak Ciphers

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)

Actions to Take

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

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. 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 `regedt32`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\MD5
```

Remedy

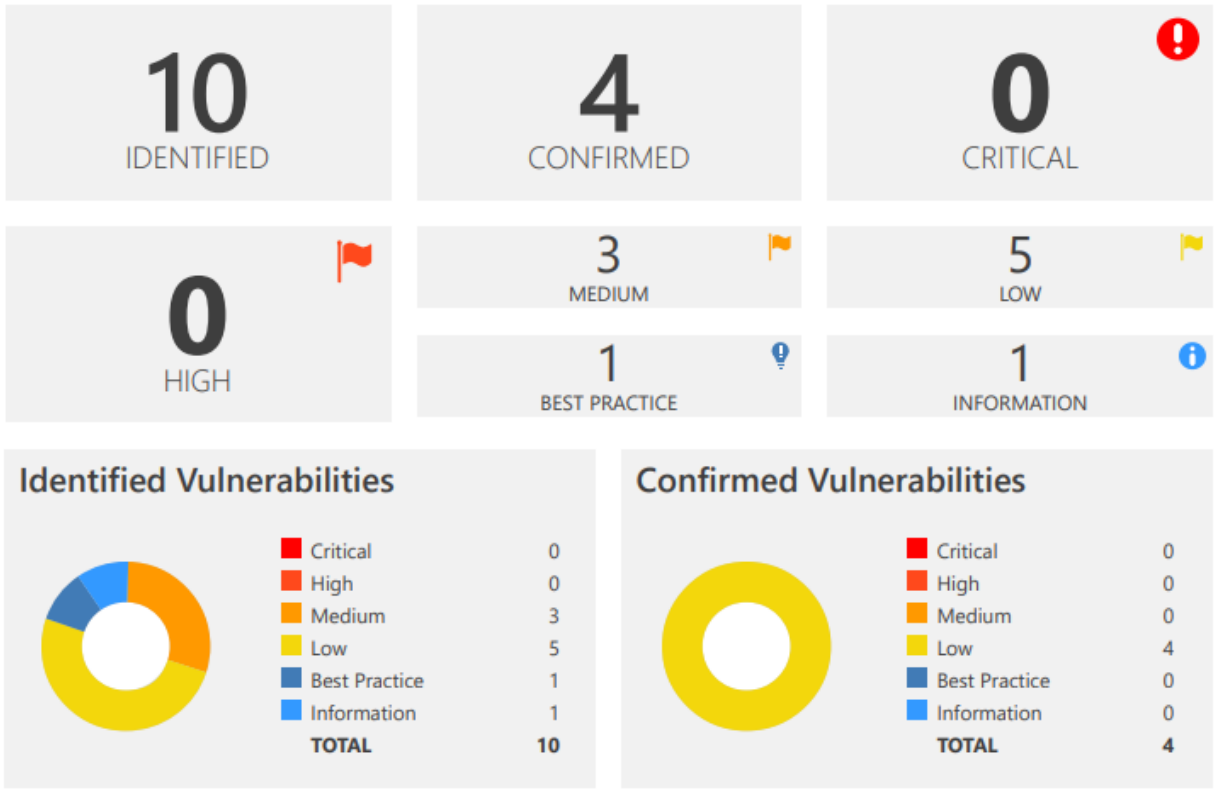
Configure your web server to disallow using weak ciphers.

Proof of Concept

A3 - SENSITIVE DATA EXPOSURE

	Weak Ciphers Enabled	GET	https://alm-logs-reciver-1.etsy.com/	MEDIUM
	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://alm-logs-reciver-1.etsy.com/	LOW
	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://alm-logs-reciver-1.etsy.com/	BEST PRACTICE

8.12 Target Domain - https://community.etsy.com



SENSITIVE DATA EXPOSURE

A. HTTP Strict Transport Security (HSTS) Policy Not Enabled

Method: GET

Severity: MIDIUM

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled. The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation. HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of

time during which the user agent shall access the server in only secure fashion. When a web application issues HSTS Policy to user agents, conformant user agents behave as follows: Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.) If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

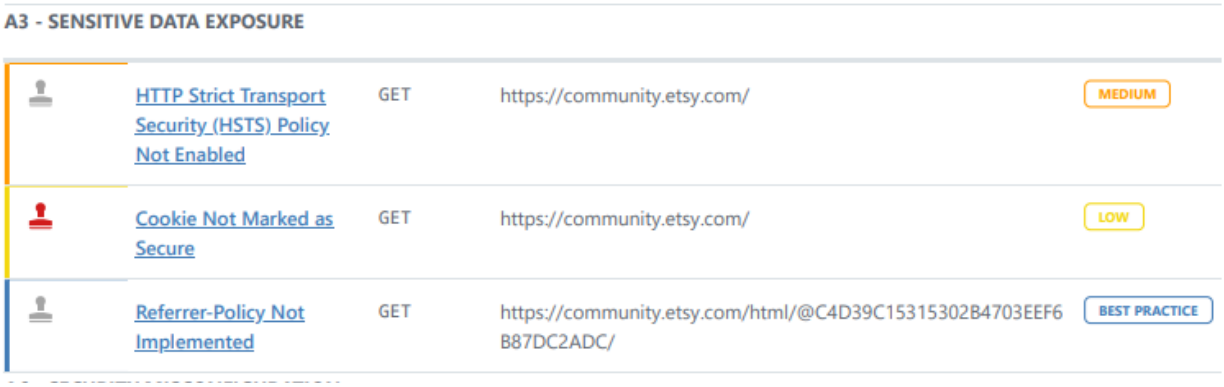
```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
       ServerAlias *
       RewriteEngine On
       RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

      # Further Configuration goes here
      [...]
</VirtualHost>
```

Proof of Concept



SECURITY MISCONFIGURATION

A. Autocomplete is Enabled

Method: GET

Sverity: LOW

Netsparker detected that Autocomplete is Enabled in one or more of the form fields which might contain sensitive information like "username", "credit card" or "CVV".

Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

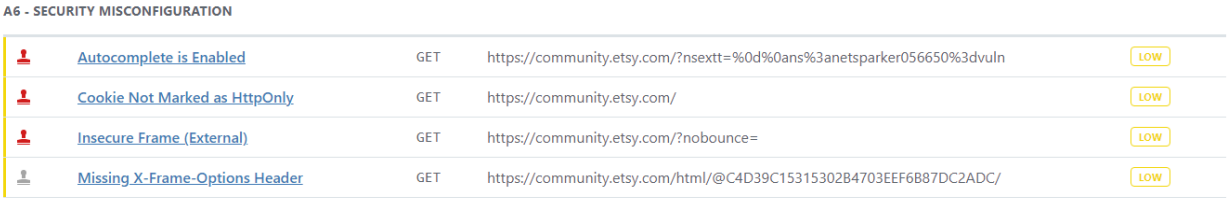
Actions to Take

1. Add the attribute autocomplete="off"to the form tag or to individual "input" fields. However, since early 2014, major browsers don't respect this instruction, due to their integrated password management mechanism, and offer to users to store password internally.
2. Find all instances of inputs that store private data and disable autocomplete. Fields which contain data such as "Credit Card" or "CCV" type data should not be cached. You can allow the application to cache usernames and remember passwords; however, in most cases this is not recommended.
3. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

Required Skills for Successful Exploitation

First and foremost, attacker needs either physical access or user-level code execution rights for successful exploitation. Dumping all data from a browser can be fairly easy, and a number of automated tools exist to undertake this. Where the attacker cannot dump the data, he/she could still browse the recently visited websites and activate the autocomplete feature to see previously entered values.

Proof of Concept



USING COMPONENTS WITH KNOWN VULNERABILITIES

A. [Possible] BREACH Attack Detected

Method: GET
Sverity: MIDIUM

Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.

Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.

Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

Impact

Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

- Inject partial plaintext they have uncovered into a victim's requests
- Measure the size of encrypted traffic

Remedy

Netsparker reported a Possible BREACH Attack issue because the target web page meets the following conditions that facilitate it:

- Served from a server that uses HTTP-level compression (ie. gzip)
- Reflects user-input in the HTTP response bodies
- Contains sensitive information (such as a CSRF token) in HTTP response bodies

To mitigate the issue, we recommend the following solutions:

1. If possible, disable HTTP level compression
2. Separate sensitive information from user input
3. Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
4. Hide the length of the traffic by adding a random number of bytes to the responses.
5. Add in a rate limit, so that the page maximum is reached five times per minute.

B. Out-of-date Version (jQuery)

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.

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

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.

Affected Versions

1.8.0 to 2.2.4

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

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

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.

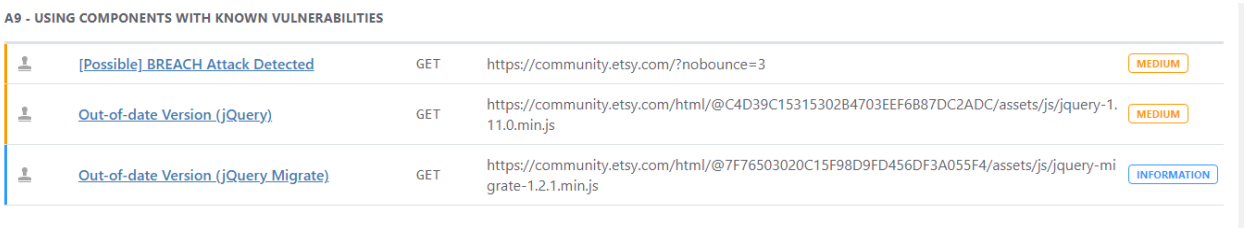
Affected Versions

1.0 to 3.3.1

Remedy

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

Proof of Concept



A9 - USING COMPONENTS WITH KNOWN VULNERABILITIES

[Possible] BREACH Attack Detected	GET	https://community.etsy.com/?nobounce=3	MEDIUM
Out-of-date Version (jQuery)	GET	https://community.etsy.com/html/@C4D39C15315302B4703EEF6B87DC2ADC/assets/js/jquery-1.11.0.min.js	MEDIUM
Out-of-date Version (jQuery Migrate)	GET	https://community.etsy.com/html/@7F76503020C15F98D9FD456DF3A055F4/assets/js/jquery-migrate-1.2.1.min.js	INFORMATION

8.13 Target Domain - https://community-stage.etsy.com

SENSITIVE DATA EXPOSURE

A. Basic Authorization over HTTP

Method: GET
Severity: HIGH

Netsparker identified that the application is using basic authentication over HTTP.

Basic authentication sends username and password in plain text. Generally, using basic authentication is not a good solution.

Impact

If an attacker can intercept traffic on the network, he/she might be able to steal the user's credentials.

Actions to Take

Move all of your directories which require authentication to be served only over HTTPS, and disable any access to these pages over HTTP.

B. HTTP Strict Transport Security (HSTS) Policy Not Enabled

Method: GET
Severity: MIDIUM

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.
The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The

HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
       ServerAlias *
       RewriteEngine On
       RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
      # Use HTTP Strict Transport Security to force client to use secure connections only
      Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

      # Further Configuration goes here
      [...]
</VirtualHost>
```

Proof of Concept

A3 - SENSITIVE DATA EXPOSURE

	Basic Authorization over HTTP	GET	http://community-stage.etsy.com/sitemap.xml	HIGH
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://community-stage.etsy.com/	MEDIUM
	Cookie Not Marked as Secure	GET	https://community-stage.etsy.com/	LOW
	Referrer-Policy Not Implemented	GET	https://community-stage.etsy.com/	BEST PRACTICE

SECURITY MISCONFIGURATION

A. Cookie Not Marked as HTTP Only

Method: GET
Severity: LOW

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.

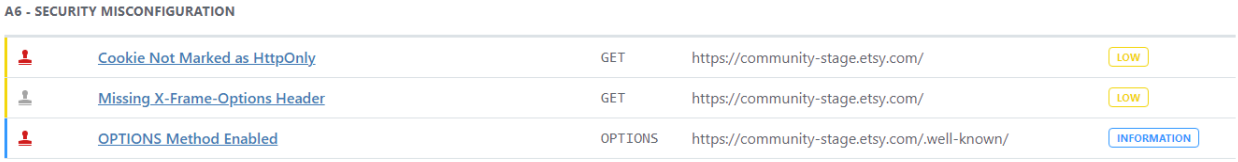
Actions to Take

a. See the remedy for solution.
b. 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 Tunnelto bypass HTTPOnly protection.

Proof of Concept



9. Conclusion

Overall, I found few high risks and medium risks. However, there have some low-risk vulnerabilities but none of them are Critical level. Thus, should be considered those vulnerabilities to keep the website safe.

Etsy is one of the leading e-commerce companies globally and as a result, seeing that when such a well-provided company cannot successfully protect itself from the entire field of cyber-attacks, it shows how complicated the world of web and cybersecurity really is the present.

10. Reference

I. https://www.netsparker.com/
II. https://hackerone.com/etsy?type=team
III. crt.sh | etsy.com
IV. https://cirt.net/Nikto2
V. https://github.com/aboul3la/Sublist3r
VI. https://nmap.org/
VII. https://tools.kali.org/information-gathering/recon-ng
VIII. https://owasp.org/www-project-top-ten/
IX. https://www.cybintsolutions.com/cyber-security-facts-stats/#:~:text=43%25%20of%20cyber%20attacks%20target,experienced%20denial%20of%20service%20attacks
X. https://tools.kali.org/information-gathering/sublist3r#:~:text=Sublist3r%20is%20a%20python%20tool,Bing%2C%20Baidu%2C%20and%20Ask
XI. https://owasp.org/www-project-top-ten/