



Sri Lanka Institute of Information Technology

**Introduction to Web Audit
Individual Assignment
IE2062 – Web Security**

Submitted by:

Student Registration Number	Student Name
IT20606992	M.G.S.M Diwananda

05/06/2022
Date of submission

Table of contents

ACKNOWLEDGEMENT	4
INTRODUCTION.....	4
OBJECTIVES OF THE BUG BOUNTY.....	5
RISK SERVERRITY RATINGS	5
OWASP Top 10 Security Risks and Vulnerabilities	6
ABOUT THE TARGET AND SELECTED DOMAINS	10
INSCOPE.....	11
OUT OF SCOPE	13
VALIDATE THE TARGET	13
ASSESSMENT METHODOLOGY.....	14
INFORMATION GATHERING	15
SUBDOMAIN ENUMERATION	15
1.Subdomain enumeration with Sublist3r	15
2. Subdomain enumeration with Google – fu.....	20
HARVESTING E-MAILS.....	21
1.Email harvesting using theHarvester tool	21
2. Using RocketReach online tool.....	23
DNS ENUMERATION	24
1.DNS Enumeration using DNSenum	24
2. DNS Enumeration using Nmap	27
3. DNS Enumeration using Dnsrecon	28
IDENTIFYING WEBSITE TECHNOLOGY.....	29
1.Using Buildwith	30

FINDING ACHIEVED INFORMATION	31
1.Wayback machine	31
SEARCH FOR OPEN PORTS	33
1.Search for open ports using Nmap tool	33
FIND THE FIREWALL PROTECTION OF TARGET DOMAINS	36
1.Using Wafw00f	36
VULNERABILITY ASSESSMENT AND RECOMMENDATIONS.....	39
Automated scan	39
1.Target domain :- https://www.etoro.com/	40
2. Target domain - https://etoropartners.com/	62
3. Target domain - https://charts.etoro.com/	74
4. Target domain - https://etorox.com/	86
5. Target domain - https://partners.etoro.com/	99
Manual Testing	104
Testing Broken Access Control.....	104
1.Target domain :- https://www.etoro.com/	104
2. Target domain - https://etoropartners.com/	106
3. Target domain - https://charts.etoro.com/	107
4. Target domain - https://etorox.com/	108
5. Target domain - https://partners.etoro.com/	109
Testing SQL Injection	
1.Target domain - https://www.etoro.com/	110
CONCLUSION	111
REFERENCES.....	112

ACKNOWLEDGEMENT

Web security module helped students gain a deeper understanding of web security tactics. However, it is not enough to simply learn about these techniques, we also need to learn how to use them in the real world. This assignment will provide us with a good understanding of how to use tools and rules also better understanding of cyber security and web security strategies.

I would like to express my gratitude to Dr. Lakmal Roopasinghe, Ms. Chethana Liyanapathirana, Ms. Menaka Moonamaldeniya and Ms. Chathu Udagedara for their hard work and dedication in helping me complete this project.

INTRODUCTION

Cyber security is a set of methods and processes that are used to protect against unauthorized access and use of networks and computers. It contributes to the maintenance of confidentiality, integrity, and availability.

Due to the rise of technology, cyber-attacks are becoming more common. Most of these attacks utilize tools and techniques that can cause damage to various networks and servers, such as databases. Hackers can also take advantage of these vulnerabilities by visiting websites and software that are vulnerable to exploitation.

Penetration testing and vulnerability scanning are commonly used to identify and secure vulnerabilities in online assets. Bug bounty programs are also beneficial for organizations that are looking to exploit these bugs. These programs allow individuals to earn money by identifying and exploiting bugs.

OBJECTIVES OF THE BUG BOUNTY

For the bug bounty assignment given for web security module in second year second semester, I selected <https://etoro.com> to do bug bounty. The main aim of this bug bounty assignment is, to identify vulnerabilities of the selected website and report them according to the instructions given by HackerOne.

RISK SEVERITY RATINGS

High	The highest risk associated with a specific vulnerability is represented by the high-risk level. The target application can be successfully exploited, and the application data can be comprised partially or totally by the attacker. The data of the web application may be modified or deleted by the attacker.
Medium	Considerable risks associated with specific vulnerabilities are represented by the medium-risk level. Low level information about the web application can be gained by an attacker when exploiting medium risk vulnerabilities. Medium-risk vulnerabilities should be addressed after mitigating high-risk vulnerabilities.
Low	The lowest risk associated with a specific vulnerability is represented by the low-risk level. This may allow an attacker to obtain some information which are not much critical, but not intended to have knowledge otherwise.

OWASP Top 10 Security Risks and Vulnerabilities

The OWASP top 10 is a list of the 10 most common web application security risks. This is a standard document that helps developers and security professionals identify the most critical issues in web applications.

- [Injection](#)
- [Broken Authentication](#)
- [Sensitive Data Exposure](#)
- [XML External Entities \(XXE\)](#)
- [Broken Access Control](#)
- [Security Misconfiguration](#)
- [Cross-Site Scripting \(XSS\)](#)
- [Insecure Deserialization](#)
- [Using Components with Known Vulnerabilities](#)
- [Insufficient Logging & Monitoring](#)

Risk	Information
<u>Injection</u>	Injection happens when an attacker exploit malicious code to inject (or insert) their own code into a program. Examples of injection:- <ul style="list-style-type: none">▪ SQL injection▪ command injections▪ CRLF injections▪ LDAP injections

<u>Broken Authentication</u>	Getting the correct implementation of session management calls and authentication is very important to prevent unauthorized access to your data. This is why it is important to implement multifactor authentication. This can help prevent attackers from gaining access to your accounts.
<u>Sensitive Data Exposure</u>	Developers can easily connect their applications to third-party services such as Google Maps using an API. However, some of these APIs can be vulnerable to exploitation due to their use of insecure data transmission methods. To minimize the risk of getting access to sensitive data, implementing various security measures such as tokenization, data encryption, and key management.
<u>XML External Entities (XXE)</u>	This vulnerability can be exploited by attackers to upload or include hostile content in XML document. SCA scan can identify these risks in third-party components, and it can warn you about them. Disabling the processing of XML external entities can also reduce the likelihood of exploitation.

<u>Broken Access Control</u>	<p>Unauthenticated users can easily take advantage of access restrictions and privileges that are not being properly enforced. This can allow them to access sensitive files and systems.</p> <p>Although automated processes can test for certain types of errors, such as missing or unauthorized access controls, they are not always able to detect them. This is why it is important to use other methods to check for these issues.</p> <p>Aside from regular testing, implementing secure coding practices and managing your credentials are also important to prevent issues from happening.</p>
<u>Security Misconfiguration</u>	<p>A lot of security configuration errors are similar to those that happen when implementing a poorly designed access control. They can allow attackers to access sensitive data and sites easily. Dynamic testing can help identify these issues.</p>

<p><u>Cross-Site Scripting (XSS)</u></p>	<p>Another common vulnerability that can be exploited by attackers is the ability to access a vulnerable web application's interaction with its users.</p> <p>Examples for XSS: -</p> <ul style="list-style-type: none"> ▪ Reflected XSS ▪ Stored XSS ▪ DOM-based XSS
<p><u>Insecure Deserialization</u></p>	<p>This vulnerability can be used to execute script remotely. It can also allow attackers to perform various attacks, such as privilege escalation and replay attacks.</p>
<p><u>Using Components with Known Vulnerabilities</u></p>	<p>Even if your own code is secure, attackers can still access third-party components without your knowledge. A static analysis can help identify these components in your application. It can also help prevent them from being exploited by analyzing the software composition and APIs of your application.</p>
<p><u>Insufficient Logging & Monitoring</u></p>	<p>Poor monitoring and log errors can introduce a human element to a security risk. Threat actors rely on a lack of monitoring and remediation time to carry out attacks before they can react to prevent you from noticing or reacting.</p>

ABOUT THE TARGET AND SELECTED DOMAINS

EToro is a multinational financial and social trading company based in Israel. It provides various services such as financial and copy trading. Its headquarters are located in Central Israel. It has also registered offices in the US, UK, Australia, and Cyprus.

I completed the bug bounty on www.etoro.com for the assignment. I selected HackerOne (www.hackerone.com) to finish my project. The audit was done for the following URLs.

- <https://www.etoro.com/>
- <https://etoropartners.com/>
- <https://charts.etoro.com/>
- <https://etorox.com/>
- <https://partners.etoro.com/>

The screenshot shows the HackerOne interface for the eToro Bug Bounty Program. At the top, there's a navigation bar with links for Hacktivity, Directory, Opportunities, Inbox, Hacker Dashboard, Job Board, and Leaderboards. On the right side of the header, there are icons for a gift, a bell, and a user profile. Below the header, the main content area features a large green banner for the 'eToro BBP'. The banner includes the eToro logo, a brief description of their vision, a 'Submit report' button, and information about the program being launched in February 2022 and managed by HackerOne. It also includes a 'Bookmark' and 'Subscribe' button. Below the banner, there's a summary section with metrics: 'Reports resolved 104', 'Assets in scope 39', and 'Average bounty \$100-\$250'. Further down, there are two tables: 'Rewards' and 'Response Efficiency'. The 'Rewards' table maps bounty ranges to severity levels: Low (yellow), Medium (orange), High (pink), and Critical (red). The 'Response Efficiency' table shows average response times: 18 hrs for first response and about 1 day for triage. At the bottom of the page, it says 'Last updated on April 6, 2022.' and 'View changes'.

INSCOPE

Scopes

In Scope

Domain	www.etoro.com	█ Critical	\$ Eligible
Domain	etoropartners.com	█ Critical	\$ Eligible
Domain	partners.etoro.com	█ Critical	\$ Eligible
Domain	aggregator.etoro.com	█ Critical	\$ Eligible
Domain	api.etoro.com	█ Critical	\$ Eligible
Domain	billing.etoro.com	█ Critical	\$ Eligible
Domain	billing-pci.etoro.com	█ Critical	\$ Eligible
Domain	candle.etoro.com	█ Critical	\$ Eligible
Domain	candle-src.etoro.com	█ Critical	\$ Eligible
Domain	cashier.etoro.com	█ Critical	\$ Eligible
Domain	cashier-src.etoro.com	█ Critical	\$ Eligible
Domain	charts.etoro.com	█ Critical	\$ Eligible
Domain	push-d-gw.cloud.etoro.com	█ Critical	\$ Eligible
Domain	push-d-hap.cloud.etoro.com	█ Critical	\$ Eligible
Domain	push-demo-hk-lightstreamer.cloud.etoro.com	█ Critical	\$ Eligible
Domain	push-demo-lightstreamer.cloud.etoro.com	█ Critical	\$ Eligible
Domain	push-dn-hap.cloud.etoro.com	█ Critical	\$ Eligible
Domain	push-hap.cloud.etoro.com	█ Critical	\$ Eligible

Domain	push-lightstreamer.cloud.otoro.com		Critical		Eligible
Domain	push-n-hap.cloud.otoro.com		Critical		Eligible
Domain	push-real-hk-lightstreamer.cloud.otoro.com		Critical		Eligible
Domain	etorologsapi.otoro.com		Critical		Eligible
Domain	kyc.otoro.com		Critical		Eligible
Domain	kyc-src.otoro.com		Critical		Eligible
Domain	r.otoro.com		Critical		Eligible
Domain	streams.otoro.com		Critical		Eligible
Domain	sts.otoro.com		Critical		Eligible
Domain	tapi-demo.otoro.com		Critical		Eligible
Domain	tapi-real.otoro.com		Critical		Eligible
Domain	uapi-front.otoro.com		Critical		Eligible
Domain	wallet.otoro.com		Critical		Eligible
Domain	watchlistapi.otoro.com		Critical		Eligible
Domain	otorox.com		Critical		Eligible
Domain	rankings.otoro.com		Critical		Eligible
Domain	delta.app		Critical		Eligible
Android: Play Store	com.otoro.openbook		Critical		Eligible
Android: Play Store	com.otoro.wallet		Critical		Eligible
iOS: App Store	com.otoro.openbook		Critical		Eligible
iOS: App Store	com.otoro.wallet		Critical		Eligible

OUT OF SCOPE

Out of Scope

Domain templates.etoro.com

Domain api-portal.etoro.com

Other Web and Mobile Assets

VALIDATE THE TARGET

The screenshot shows the Hover.com website interface. At the top, there's a navigation bar with links for Domains, Email, About Us, and Blog. On the right side of the bar are Help and Sign In options. Below the navigation, there's a search bar containing "httpsetoro.com", a magnifying glass icon, a shopping cart icon showing "0 ITEMS", and a currency indicator "USD \$0.00". The main content area displays a message: "**httpsetoro.com** is taken. Domain Agents might be able to help." To the right of this message is a green "MAKE AN OFFER" button. Below this, there's a section titled "HERE ARE OTHER GREAT DOMAIN MATCHES" with two suggestions: "httpsetoro.online" (with a description "Stay connected with .ONLINE") and "httpsetoro.org" (with a description "The domain that brings people together"). Both suggestions have price tags of "\$4.99 / \$34.99" and a green plus sign icon. Further down, there's a "FEATURED" section with a result for "httpsetoro.art" (Showcase your masterpiece) and another for "httpsetoro.me". On the right side of the page, there are "FILTERS" with checkboxes for "Show All", "Featured", and "Popular".

Here I used hover.com to validate the target. When I searched the doiman in search bar, the result said that the target is taken. According to the result, we can comfirmed that targeted domain is valid.

ASSESSMENT METHODOLOGY

Before carrying out a vulnerability assessment, it is important that the team members follow proper steps. This process is carried out in accordance with a standard penetration testing procedure.



INFORMATION GATHERING

When it comes to launching an attack or preventing one from happening, information gathering is the first step. This process is carried out with or without the client's consent. We collect as much information as we can about our clients or victims in order to improve our services and prevent them from getting victimized. In case of a bug bounty, our client gives us the limited information about the methodology used for them.

Unfortunately, when it comes to launching illegal attacks, the information gathering process is carried out covertly using illegal methods. However, this information gathering section is very important to ensure that you can achieve the expected success.

SUBDOMAIN ENUMERATION

The process of finding subdomain for one or more domain is known as subdomain enumeration. It helps to find hidden applications and forgotten subdomains in the attack surface.

1.Subdomain enumeration with Sublist3r

Sublist3r is a python tool designed to identify subdomains of websites. This tool helps bug hunters and penetration testers find and collect various domains that they're targeting. It can be used by search engines like Google, Yahoo, Bing, and Baidu.

By default, it is not installed in Kali linux. To install Sublist3r for kali linux we can simply enter the **apt install sublist3r** command on linux terminal and it will install automatically. Or we can download sublist3r through GitHub.

Download URL : <https://github.com/aboul3la/Sublist3r.git>

In here I used **sublist3r -d etoro.com** to get all the subdomains in etoro.com.

```
(kali㉿kali)-[~]
$ sublist3r -d etoro.com


```

Coded By Ahmed Aboul-Ela - @aboul3la

```
[+] Enumerating subdomains now for etoro.com
[+] Searching now in Baidu..
[+] Searching now in Yahoo..
[+] Searching now in Google..
[+] Searching now in Bing..
[+] Searching now in Ask..
[+] Searching now in Netcraft..
[+] Searching now in DNSdumpster..
[+] Searching now in Virustotal..
[+] Searching now in ThreatCrowd..
[+] Searching now in SSL Certificates..
[+] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[+] Total Unique Subdomains Found: 332
www.etoro.com
007.etoro.com
1fdtopcovid19.etoro.com
2fcontent.etoro.com
2fwww.etoro.com
3cc0bed0-d930-4a56-aece-5fee4fdd2035.etoro.com
60partners.etoro.com
7-mtopcovid19.etoro.com
7-candle.etoro.com
7ww.etoro.com
a43.etoro.com
accesadistance.etoro.com
accountstat.etoro.com
admin.etoro.com
affapi.etoro.com
affiliates.etoro.com
aggregator.etoro.com
akhk.etoro.com
akuariummaskoki.etoro.com
alerts.etoro.com
api.etoro.com
api-portal.etoro.com
apptest.etoro.com
aroundthedistance.etoro.com
arrowmask5.etoro.com
arrowmask8.etoro.com
```

asdf.etoro.com
asmodeo.etoro.com
azithromycin.etoro.com
bayanmaskara.etoro.com
beta.etoro.com
bf.etoro.com
billing-pci.etoro.com
blockdmask.etoro.com
blog.etoro.com
blogcatolicovirgenmaria.etoro.com
spektakli.blogspot.etoro.com
bokepcorona.etoro.com
booking.etoro.com
brptportal.etoro.com
c-cignauniversity.etoro.com
candle.etoro.com
cashier.etoro.com
cca.etoro.com
cdn.etoro.com
cekvirus.etoro.com
centrocorona.etoro.com
charts.etoro.com
push-d-hap.cloud.etoro.com
push-demo-hk-lightstreamer.cloud.etoro.com
push-demo-lightstreamer.cloud.etoro.com
push-dn-hap.cloud.etoro.com
push-hap.cloud.etoro.com
push-lightstreamer.cloud.etoro.com
push-ls-n2.cloud.etoro.com
push-ls-w2.cloud.etoro.com
push-ls-wn1.cloud.etoro.com
push-ls-wn2.cloud.etoro.com
push-ls-wn3.cloud.etoro.com
push-n-hap.cloud.etoro.com
push-real-hk-lightstreamer.cloud.etoro.com
cn.etoro.com
cat.nl.eu.criteo.comcandle.etoro.com
271200.genapicloud.comcandle.etoro.com
271696.genapicloud.comcandle.etoro.com
271970.genapicloud.comcandle.etoro.com
www.google.comcandle.etoro.com
ssw.live.comcandle.etoro.com
fe2.update.microsoft.comcandle.etoro.com
trc.taboola.comcandle.etoro.com
ctldl.windowsupdate.comcandle.etoro.com
callbacks-temp.genapicloud.compages.etoro.com
confirmation.etoro.com
connect.etoro.com
click.connect.etoro.com
image.connect.etoro.com
conten.etoro.com

content.etoro.com
corona-is.etoro.com
corona-po-accountstat.etoro.com
corona-v.etoro.com
coronaaustraliaetcom.etoro.com
corporate.etoro.com
covid19.etoro.com
css3.etoro.com
customersupportapi.etoro.com
deathmaskofmauricetillet-theangel.etoro.com
demo.etoro.com
distance-southwest.etoro.com
distancecalculator.etoro.com
distancedev-math.etoro.com
distanceed.etoro.com
dws1.etoro.com
embed.etoro.com
etorlogs.etoro.com
etoro-asset.etoro.com
etoroblog.etoro.com
etorogrowth.etoro.com
etorologs.etoro.com
etorologsapi.etoro.com
etoropages.etoro.com
faid.etoro.com
fapi-demo.etoro.com
fapi-real.etoro.com
fe-nx-etoro.etoro.com
fe-nx-etoro-il.etoro.com
flash.etoro.com
forgetthedistance.etoro.com
forms.etoro.com
forum.etoro.com
portal.cinfrance.frcandle.etoro.com
intra.notaires.frcandle.etoro.com
front.etoro.com
ftp.etoro.com
ftp1.etoro.com
futureoftrading.etoro.com
go.etoro.com
go2.etoro.com
gp.etoro.com
growth.etoro.com
gtm1.etoro.com
gww.etoro.com
heart-surgery-ntm-infection-lawsuit.etoro.com
helavirus.etoro.com
help.etoro.com
home.etoro.com
host.etoro.com
icemask.etoro.com

il-mag-cellcom.etoro.com
ilcovoditom.etoro.com
imap.etoro.com
imap4.etoro.com
imvaccine.etoro.com
ini-vaccine.etoro.com
insight.etoro.com
interferon.etoro.com
ip.etoro.com
feature-detects.dom-dataset.js.etoro.com
kaviruspnet.etoro.com
korona-na-monetach.etoro.com
koronaii.etoro.com
kumaskagitimakas.etoro.com
kyc.etoro.com
kyc-src.etoro.com
luma.etoro.com
lunpandemimi.etoro.com
m.etoro.com
mail.etoro.com
mail1.etoro.com
mailer.etoro.com
maintenance.etoro.com
mascara.etoro.com
maska.etoro.com
maskedrider.etoro.com
maskeragron.etoro.com
maskingcentral.etoro.com
maskkwon.etoro.com
maskor.etoro.com
maskpoke.etoro.com
maskrtnici.etoro.com
med.etoro.com
media.etoro.com
meta.etoro.com
metamask.etoro.com
mgh.etoro.com
mindenkimaskeppgyforma.etoro.com
mobile.etoro.com
mobiletracking.etoro.com
muhanupothamuluthange.etoro.com
mx.etoro.com
namaskar.etoro.com
netcandle.etoro.com
elb-fra-amz.nimbus.bitdefender.netetorologsapi.etoro.com
newaoivirus.etoro.com
news.etoro.com
ns1.etoro.com
nwww.etoro.com
objectlockdown.etoro.com
obpn.etoro.com

offlinemode.etoro.com
online-distance.etoro.com
openbook.etoro.com
www.openbook.etoro.com
openbookmobile.etoro.com
owa.etoro.com
pages.etoro.com
es.pages.etoro.com
no.pages.etoro.com
pl.pages.etoro.com
se.pages.etoro.com
pages2.etoro.com
pandemia.etoro.com
partners.etoro.com
partners-help.etoro.com
pop3.etoro.com
por.etoro.com
portal.etoro.com
push.etoro.com
quarantine01.etoro.com
quarentena2.etoro.com
quarentenamp.etoro.com
r.etoro.com
raf-azure.etoro.com
rankings.etoro.com
real.etoro.com
redcross.etoro.com
referfriends.etoro.com
register.etoro.com
registration.etoro.com
remote.etoro.com
removevirusmalwares.etoro.com
respirators.etoro.com
respiratorysystemsinfo.etoro.com
respiratorytherapycave.etoro.com
s3.etoro.com
search.etoro.com
second.etoro.com
sftp.etoro.com
sharechart.etoro.com
signin.etoro.com
sinemaskop.etoro.com
site.etoro.com
sleepmask.etoro.com
smtp.etoro.com
smtipi.etoro.com
social2.etoro.com
socialalerts.etoro.com
spao.etoro.com
splunk.etoro.com
src.etoro.com

staticcdn.etoro.com
station.etoro.com
status.etoro.com
stg-go.etoro.com
stimulsoft.etoro.com
stocks.etoro.com
streams.etoro.com
sts.etoro.com
sts-android.etoro.com
suryanamaskar.etoro.com
swedish.etoro.com
sww.etoro.com
tapi-demo.etoro.com
tapi-real.etoro.com
test.etoro.com
the-mask.etoro.com
thevaccinesuk.etoro.com
torologsapi.etoro.com
tracking.etoro.com
tracks.etoro.com
turkish.etoro.com
u002fwww.etoro.com
uapi-front.etoro.com
uppstartsmaskinen.etoro.com
userstatsapi.etoro.com
utazzmaskepp.etoro.com
www.etoro.com
vaccin-voyage-ghparis10.etoro.com
vaccineipfedilling.etoro.com
vaccinelb.etoro.com
vaccinemodeling.etoro.com
vaccinerefrigeration.etoro.com
vaccines.etoro.com
virus0826.etoro.com
virus17virus.etoro.com
virusirto.etoro.com
virusscan.etoro.com
viruswall.etoro.com
viruswriter.etoro.com
visid_incap_172517.etoro.com
vpn.etoro.com
vvvwv.etoro.com
www.etoro.com
ww.w.etoro.com
w2w.etoro.com
w7w.etoro.com
walkingmask.etoro.com
wallet.etoro.com
wap.etoro.com
watchlistapi.etoro.com
webtrader.etoro.com

wgw.etoro.com
widgets.etoro.com
wqw.etoro.com
wsu.etoro.com
wuw.etoro.com
www.etoro.com
w.ww.etoro.com
ww7.etoro.com
wwg.etoro.com
wws.etoro.com
wwu.etoro.com
www.etoro.com
www-ip.etoro.com
www-stg.etoro.com
wxw.etoro.com
xmpp.etoro.com
xn--80aa5alfu.etoro.com
xn--n2a62ca.etoro.com
xn--n2a98ab.etoro.com
xn--vv-4qcaaa.etoro.com
xn--vv-cbcaaa.etoro.com
xn--vv-cdca.etoro.com
xn--vv-epca.etoro.com
xn--vvv-lycaa.etoro.com
xn--vvvv-12e.etoro.com
xn--vvvv-4be.etoro.com
xn--vvvv-pdf.etoro.com
xn--vvvv-tnda.etoro.com
xn--vvvv-z2e.etoro.com
xn--vvvvvv-pydbbbb.etoro.com
xn--vvvvv-rydb.etoro.com
xn--vvvv-7fdb.etoro.com
xn--vvvw-snd.etoro.com
xn--w-0vb77c.etoro.com
xn--w-1vb67c.etoro.com
xn--w-nbcb.etoro.com
xn--w-r6bb.etoro.com
xn--w-s6b7r.etoro.com
xn--wv-4qcaa.etoro.com
xn--wvv-1yca.etoro.com
xn--wvv-3ce.etoro.com
xn--wvv-83d.etoro.com
xn--wvv-93d.etoro.com
xn--wvvv-9fd.etoro.com
xn--wvv-1yc.etoro.com
xn--ww-ccd.etoro.com
xn--ww-epc.etoro.com
xn--ww-fpc.etoro.com
xn--ww-j5c.etoro.com
xn--ww-k5c.etoro.com
xn--y9aaa.etoro.com

In here sublist3r found 332 subdomains of etoro.com

2. Subdomain enumeration with Google-fu

Using Google-fu tool also can used to find subdomains.

The screenshot shows a Google search results page with the query "site:etoro.com -www". The results list various subdomains of etoro.com, including:

- <https://status.etoro.com> › history
- [Incident History - eToro Status](#)
eToro's Incident and Scheduled Maintenance History.
- <https://charts.etoro.com> ›
- [eToro Charts!](#)
Chart. Chart Style; Candle; Bar; Colored Bar; Line; Hollow Candle; Mountain; Chart Scale; Log Scale; Heikin-Ashi; Renko; Clear Drawings. Studies.
- <https://partners.etoro.com> › B10215....
- [Translate this page](#) ›
- [eToro Sign Up](#)
Scopri eToro, il più grande social network di investimenti al mondo, dove milioni di utenti guadagnano copiando gli investimenti dei nostri migliori trader.
- <https://help.etoro.com> › Arabic
- [Translate this page](#) ›
- [Support Center](#)
هذا ... كيف يمكنني الاتصال مع eToro؟ كيف يمكنني على حسابي؟ هل تقدم eToro خدمات إساتيد؟ هل سكون بعاجة إلى ذلك؟
صراحت على صفاتي؟
- <https://go2.etoro.com> › etoro-money-availability
- [Is eToro Money available in your region?](#)
A smarter way to manage your money. Connect eToro Money seamlessly to your investment account to enjoy fee-free deposits, instant withdrawals, and the ability ...
- <https://content.etoro.com> › UFC
- [Join eToro Trading Competition & Win UFC Tickets](#)
We are proud to present the WINNERS of the UFC Trading Competition! Congratulations to the winners and a BIG thank you to all participants for taking part ...
- <https://help.etoro.com> › Education
- [Translate this page](#) ›
- [Formazione - eToro](#)
Cos'è l'estratto conto eToro? Sul tuo estratto conto puoi trovare una panoramica completa di tutte le tue attività di investimento. Qui puoi controllare tutti i ...
- <https://help.etoro.com> › Education
- [Translate this page](#) ›
- [Formação](#)
O que é o Extrato de Conta eToro? Como se fecha uma posição? O que devo fazer para levantar fundos da minha conta? O que é o Take Profit? · Trailing Stop Loss.
- <https://help.etoro.com> › Education
- [Translate this page](#) ›
- [Обучение - eToro](#)
Просматривайте полный обзор всей вашей инвестиционной деятельности в выписке из счета. В ней отображаются все движения по счету, такие как открытые и ...
- <https://help.etoro.com> › account
- [Translate this page](#) ›
- [Mitt konto - Help Center](#)
Det är kundernas ansvar att beräkna och betala tillämpliga skatter i det land eller de länder där de har sin skattehemvist. Vad är eToro kontoutdrag? Se en ...

At the bottom of the search results, there is a navigation bar with the Google logo and a page number indicator showing "1 2 3 4 5 6 7 8 9 10 Next".

Harvesting E-Mails

Email harvesting is the method of gaining many email addresses via several methods. For use in bulk emailing or for spamming is the purpose of harvesting email addresses.

Specialized harvesting software called as harvesting bots or harvesters is the most common technique of email harvesting.

1.Email harvesting using theHarvester tool

theHarvester is a tool which is available in kali linux used to search email accounts, virtual hosts, subdomain names, open ports / banners etc.

I used **-d etoro.com** command to check certain email addresses of targeted domain. And to limit the results I used **-l 500** , and I used Google like this **-b google**

```
(kali㉿kali)-[~]
$ theHarvester -d etoro.com -b google -l 500
*****
* [REDACTED] FIVE EYES [REDACTED] *
* theHarvester 4.0.3 *
* Coded by Christian Martorella *
* Edge-Security Research *
* cmartorella@edge-security.com *
*****
[*] Target: etoro.com
    Searching 0 results.
    Searching 100 results.
    Searching 200 results.
    Searching 300 results.
    Searching 400 results.
    Searching 500 results.
[*] Searching Google.
[*] No IPs found.
[*] Emails found: 10
```

```
_____
alon@etoro.com
darasa@etoro.com
investors@etoro.com
polage@etoro.com
pr@etoro.com
support@etoro.com
ukpartners@etoro.com
x22investors@etoro.com
x22polage@etoro.com
x22pr@etoro.com

[*] Hosts found: 2
_____
www.etoro.com:104.18.35.149, 172.64.152.107
x22www.etoro.com:13.79.184.58

(kali㉿kali)-[~]
```

Harvester was unable to find Ips but theHarvester identified 10 emails and 2 hosts.

2. Using RocketReach online tool

To check for email address from specific domain, we can use this online tool. Before use this tool I created account in <https://rocketreach.co/person> tool. When we are searching specific domain name, we can find email address, phone numbers and other information.

In my case, I found several email address and other eToro related information from this tool.

The screenshot shows the RocketReach search interface. The top navigation bar includes 'Search', 'My Contacts', 'Bulk Lookups', 'Tools', 'Get Chrome Extension', a notification bell with 1 alert, 'Pricing', and a user account section showing 2 notifications and the email 'subashdiwa123@gmail.com'. The main search area has a blue header 'People' and a search bar with placeholder text 'Enter a keyword or LinkedIn url...'. Below the search bar, it says '1 - 10 of about 16,124 results.' and 'Save this search'. A sidebar on the left titled 'Refine By' lists various filters: 'eToro' (selected), 'Name', 'LOCATION', 'Location', 'OCCUPATION', 'Job Title', 'Skills', 'Years of Experience', 'EMPLOYER', 'Company Name or Domain' (set to 'eToro'), 'Employee Count', 'Revenue', 'Industry', 'EDUCATION', and 'Education'. The main content area displays three search results for eToro employees:

- Ronen Assia**: Co-Founder and Executive Director at eToro, located in Israel. Found 4 emails: etoro.com, gmail.com, tradonomi.com, netvision.net.il. Found phones: 1 available on +Phone plans. Includes a 'Get Contact Info' button.
- Shalom Berkovitz**: Chief Financial Officer and Deputy Chief Executive Officer at eToro, located in Israel. Found 4 emails: etoro.com, isa.gov.il, d.co.il, dsnrgm.com. Found phones: 1 available on +Phone plans. Includes a 'Get Contact Info' button.
- Israel Kalush**: VP Engineering at eToro, located in Israel. Found 5 emails: israelkalush@etoro.com (BEST PROFESSIONAL), israelka@etoro.com, +9 more emails, and an 'Improve Results' button. Includes a 'Get Contact Info' button and a note 'Added Israel to "My Contacts"'.

At the bottom right of the search results, there are icons for a smiley face and a speech bubble.

DNS ENUMERATION

Dns Enumeration is the method of identifying all the DNS servers and their other information. This method can use to gather many interesting details about the target before initiate an attack. It gives information such as username, computer names and Ip address of potential target systems.

1.DNS Enumeration using DNSenum

DNSenum is the tool which is default available in kali linux. In here I used **dnsenum -noreverse -o file.xml etoro.com** to retrieve DNS information without any redirections. To avoid reverse lookup used **-noreverse** and to save the output into **file.xml**, I used **-o**.

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ dnsenum --noreverse -o file.xml etoro.com
dnsenum VERSION:1.2.6

--- etoro.com ---

Host's addresses:

etoro.com.          20      IN   A       23.198.122.134

Wildcard detection using: dsqqlbtjvybxm

dsqqlbtjvybxm.etoro.com.    600      IN   A       13.79.184.58

!!!!!!!!

Wildcards detected, all subdomains will point to the same IP address
Omitting results containing 13.79.184.58.
Maybe you are using OpenDNS servers.

!!!!!!!!

Name Servers:

ns1-13.akam.net.        90000    IN   A       193.108.91.13
ns4-64.akam.net.        167954    IN   A       84.53.139.64
ns5-64.akam.net.        38456     IN   A       184.85.248.64
ns7-65.akam.net.        78777     IN   A       96.7.49.65

Mail (MX) Servers:

alt1.aspmx.l.google.com. 291      IN   A       173.194.202.27
aspmx.l.google.com.      179      IN   A       142.251.10.26
alt3.aspmx.l.google.com. 293      IN   A       142.250.141.26
alt4.aspmx.l.google.com. 88       IN   A       142.250.115.27
alt2.aspmx.l.google.com. 291      IN   A       142.250.142.26
```

```
Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for etoro.com on ns7-65.akam.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for etoro.com on ns5-64.akam.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for etoro.com on ns4-64.akam.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for etoro.com on ns1-13.akam.net ...
AXFR record query failed: REFUSED
```

Brute forcing with /usr/share/dnsenum/dns.txt:

es.etoro.com.	600	IN	CNAME	site.etoro.com.
fr.etoro.com.	600	IN	CNAME	site.etoro.com.
it.etoro.com.	600	IN	CNAME	site.etoro.com.
mail.etoro.com.	86400	IN	CNAME	ghs.google.com.
ghs.google.com.	299	IN	A	172.217.174.243
meta.etoro.com.	600	IN	CNAME	www.etoro.com.
www.etoro.com.	600	IN	CNAME	www.failover.etoro.akadns.net.
www.failover.etoro.akadns.net.	300	IN	CNAME	www.etoro.akadns.net.
www.etoro.akadns.net.	300	IN	CNAME	etoro.com.cdn.cloudflare.net.
etoro.com.cdn.cloudflare.net.	300	IN	A	172.64.152.107
etoro.com.cdn.cloudflare.net.	300	IN	A	104.18.35.149
rdg.etoro.com.	84600	IN	A	82.80.101.38
search.etoro.com.	600	IN	CNAME	www.etoro.com.
www.etoro.com.	547	IN	CNAME	www.failover.etoro.akadns.net.
www.failover.etoro.akadns.net.	247	IN	CNAME	www.etoro.akadns.net.
www.etoro.akadns.net.	247	IN	CNAME	etoro.com.cdn.cloudflare.net.
etoro.com.cdn.cloudflare.net.	247	IN	A	172.64.152.107
etoro.com.cdn.cloudflare.net.	247	IN	A	104.18.35.149
smtp.etoro.com.	86400	IN	A	82.166.64.66
test.etoro.com.	600	IN	A	31.168.97.166
vsp.etoro.com.	86400	IN	A	216.75.53.3
webmail.etoro.com.	86400	IN	CNAME	webmail.secureserver.net.
webmail.secureserver.net.	3600	IN	CNAME	email.secureserver.net.
email.secureserver.net.	60	IN	A	173.201.192.148
email.secureserver.net.	60	IN	A	173.201.192.5
email.secureserver.net.	60	IN	A	173.201.193.133
email.secureserver.net.	60	IN	A	45.40.130.41
email.secureserver.net.	60	IN	A	45.40.140.6
email.secureserver.net.	60	IN	A	68.178.252.5
email.secureserver.net.	60	IN	A	173.201.193.20
email.secureserver.net.	60	IN	A	173.201.192.20
email.secureserver.net.	60	IN	A	68.178.252.148
email.secureserver.net.	60	IN	A	68.178.252.133
email.secureserver.net.	60	IN	A	45.40.130.40
email.secureserver.net.	60	IN	A	173.201.193.5
email.secureserver.net.	60	IN	A	173.201.193.148
email.secureserver.net.	60	IN	A	68.178.252.20
email.secureserver.net.	60	IN	A	97.74.135.55
email.secureserver.net.	60	IN	A	173.201.192.133
www.etoro.com.	521	IN	CNAME	www.failover.etoro.akadns.net.
www.failover.etoro.akadns.net.	221	IN	CNAME	www.etoro.akadns.net.
www.etoro.akadns.net.	221	IN	CNAME	etoro.com.cdn.cloudflare.net.
etoro.com.cdn.cloudflare.net.	221	IN	A	104.18.35.149
etoro.com.cdn.cloudflare.net.	221	IN	A	172.64.152.107

etoro.com class C netranges:

23.198.122.0/24
31.168.97.0/24
82.80.101.0/24
82.166.64.0/24
216.75.53.0/24

etoro.com ip blocks:

23.198.122.134/32
31.168.97.166/32
82.80.101.38/32
82.166.64.66/32
216.75.53.3/32

done.

2. DNS Enumeration using Nmap

The Network Mapper also called Nmap is a linux command-line tool that can be used to scan IP address and ports in network. It can also use to detect installed applications, OS system detection and version detection. Network administrators can also find out which services are running on their network, as well as identify vulnerabilities.

I used **nmap -T4 -p 53 --script dns-brute etoro.com** command for DNS enumeration by brute force estimating of popular subdomains.

```
(kali㉿kali)-[~]
$ nmap -T4 -p 53 --script dns-brute etoro.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-23 16:06 +0530
Nmap scan report for etoro.com (23.198.122.134)
Host is up (0.094s latency).
rDNS record for 23.198.122.134: a23-198-122-134.deploy.static.akamaitechnologies.com
PORT      STATE SERVICE
53/tcp    filtered domain
Host script results:
| dns-brute:
|_ DNS Brute-force hostnames:
|   mail.test.etoro.com - 31.168.97.166
|   mail.mail.etoro.com - 216.58.203.19
|   mail.mail.etoro.com - 2404:6800:4009:804::2013
|   mail.s3.etoro.com - 23.198.122.134
|   mail.cdn.etoro.com - 125.214.166.49
|   www.cdn.etoro.com - 125.214.166.51
|   www-failover.etoro.com - 104.18.35.149
|   www.etoro.com - 172.64.152.107
|   toro.manage.etoro.com - 31.222.186.203
|   toro.cms.etoro.com - 23.198.122.134
|   smtp.etoro.com - 82.166.64.66
|   help.etoro.com - 34.255.115.245
|   *A: 13.79.184.58
Nmap done: 1 IP address (1 host up) scanned in 7.99 seconds
23.198.122.0/24
```

3. DNS Enumeration using Dnsrecon

Dnsrecone is a DNS scan tool in kali linux which is facilitate for verity of enumeration such as reverse lookup, Zone transfer, Google lookup, cache snooping, standard record enumeration, Domain Brute-Forcing and Zone walking.

In here I used this tool for get DNS details of etoro.com . And I used **dnsrecon -d etoro.com -D /usr/share/wordlists/dnsmap.txt -t std --xml dnsrecon.xml** command for DNS enumeration.

```
File Actions Edit View Help
[kali㉿kali] ~
└─$ dnsrecon -d etoro.com -D /usr/share/wordlists/dnsmap.txt -t std --xml dnsrecon.xml
[*] std: Performing General Enumeration against: etoro.com ...
[!] Wildcard resolution is not configured on this domain
[!] IP 13.70.138.58
[!] All servers will resolve to this list of addresses!
[!] DNSSEC is not configured for etoro.com
[*] SOA ns1-13.akam.net 193.108.91.13
[*] SOA ns1-13.akam.net 25000:1401::2::d
[*] NS ns7-65.akam.net 96.7.49.65
[*] NS ns1-13.akam.net 193.108.91.13
[*] NS ns1-13.akam.net 2600:1401::2::d
[*] NS ns5-64.akam.net 184.184.248.64
[*] NS ns4-64.akam.net 84.53.139.64
[*] MX aspmx.l.google.com 142.250.4.26
[*] MX aspmx.l.google.com 142.250.4.115.26
[*] MX alt3.aspmx.l.google.com 142.250.141.26
[*] MX alt1.aspmx.l.google.com 173.194.202.26
[*] MX alt2.aspmx.l.google.com 142.250.142.26
[*] MX aspmx.l.google.com 2404:6800:4003:c0::1a
[*] MX alt4.aspmx.l.google.com 2607:FB00:4023:1004::1b
[*] MX alt3.aspmx.l.google.com 2607:FB00:4023:0b::1b
[*] MX alt1.aspmx.l.google.com 2607:FB00:400e::00::1a
[*] MX alt2.aspmx.l.google.com 2607:FB00:4023:c0::1b
[*] A etoro.com 23.13.87.15
[*] TXT etoro.com apple-domain-verification=1etZIAV87QjIrwWT
[*] TXT etoro.com docker-verification=n57t1501-4013-41fa-a4ed-aa655ad5c3e9
[*] TXT etoro.com aliasdomain-verification=MN1cdHPW1Am0Kw/DMMKVLvSfSigsxXbEirvW92hh6fkTAyeITEGohLfwQJ6i3
[*] TXT etoro.com google-site-verification=jY9RctEfSmrgz2-1dk40w
[*] TXT etoro.com MS-w36506504
[*] TXT etoro.com status-page-domain-verification=mms5vrfrjd1
[*] TXT etoro.com v-spf1.ip4:40.67.217.128/29 ip4:91.220.30.0/24 ip4:212.179.161.98/32 ip4:88.202.217.196/32 ip4:82.166.64.69/32 ip4:52.158.127.104/32 ip4:95.183.0.236/32 ip4:52.142.90.27/32 ip4:40.69.79.128/26 ip4:40.119.157.1/32
p4:20.61.213.192/26 include:stspg-customer.com include:_sof.google.com include:_sof.salesforce.com include:cust-spf.exacttarget.com ~alt
[*] TXT _dmarc.etoro.com v=DMARC1; p=reject; rua=mailto:905c9455225e834@rep.dmarcanalyzer.com;mailto:dmarc-notify@etoro.com; ruf=mailto:905c9455225e834@for.dmarcanalyzer.com;mailto:dmarc-notify@etoro.com; sp=None; fo=1;
[*] Enumerating SRV Records
[*] Saving records to XML file: dnsrecon.xml
[*] Saving records to XML file: dnsrecon.xml
```

```
[kali㉿kali] ~
└─$ dnsrecon -h
usage: dnsrecon.py [-h] [-d DOMAIN] [-n NS_SERVER] [-r RANGE] [-D DICTIONARY] [-f] [-a] [-s] [-b] [-y] [-k] [-w] [-z] [--threads THREADS] [--lifetime LIFETIME] [--tcp] [--db DB] [-x XML] [-c CSV] [-j JSON] [--iw]
                  [-enable_check_recursion] [-disable_check_bindversion] [-V] [-v] [-t TYPE]
optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Target domain.
  -n NS_SERVER, --name-server NS_SERVER
                        Domain server to use. If none is given, the SOA of the target will be used. Multiple servers can be specified using a comma separated list.
  -r RANGE, --range RANGE
                        IP range for reverse lookup brute force in formats (first-last) or in (range/bitmask).
  -D DICTIONARY, --dictionary DICTIONARY
                        Dictionary file of subdomain and hostnames to use for brute force. Filter out of brute force domain lookup, records that resolve to the wildcard defined IP address when saving records.
  -f                  Filter out of brute force domain lookup, records that resolve to the wildcard defined IP address when saving records.
  -a                  Perform AXFR with standard enumeration.
  -s                  Perform a reverse lookup search in the SPP record with standard enumeration.
  -b                  Perform Bind enumeration with standard enumeration.
  -y                  Perform Yandex enumeration with standard enumeration.
  -k                  Perform crt.sh enumeration with standard enumeration.
  -w                  Perform deep whois record analysis and reverse lookup of IP ranges found through Whois when doing a standard enumeration.
  -z                  Perform deep WHOIS record analysis and reverse lookup of IP ranges found through Whois when doing a standard enumeration.
  -threads THREADS    Number of threads to use for reverse lookup, forward lookups, brute force and SRV record enumeration.
  -lifetime LIFETIME  Time to wait for a server to respond to a query. default is 3.0
  --tcp               Use TCP protocol to make queries.
  --db DB             SQLite file to save found records.
  -x XML, --xml XML  XML file to save found records.
  -c CSV, --csv CSV  Save output to a comma separated value file.
  -j JSON, --json JSON  Save output to a JSON file.
  -iw                Continue brute forcing a domain even if a wildcard record is discovered.
  -enable_check_recursion
                    Disables check for recursion on name servers
  -disable_check_bindversion
                    Disables check for BIND version on name servers
  -V, --version        Show DNSRecon version
  -v, --verbose        Enable verbose mode
  -t TYPE, --type TYPE
                    Type of enumeration to perform.
                    Possible types:
                      std:          SOA, NS, A, AAAA, MX and SRV.
                      rev:          Reverse lookup of a given CIDR or IP range.
                      brt:          Brute force domains and hosts using a given dictionary.
                      srv:          SRV records.
                      axfr:         Test all NS servers for a zone transfer.
                      bing:         Perform Bing search for subdomains and hosts.
                      yand:         Perform Yandex search for subdomains and hosts.
                      crt:          Perform crt.sh search for subdomains and hosts.
                      snoop:        Perform cache snooping against all NS servers for a given domain, testing all with file containing the domains, file given with -D option.
  tld:              Remove the TLD of given domain and test against all TLDs registered in IANA.
```

IDENTIFYING WEBSITE TECHNOLOGY

1. Using Buildwith

The technology that used to create website can be useful for identifying the vulnerability of a website. Using builtwith.com we can get a better understand about the technology used to create the website.

The screenshot shows the builtwith.com interface for the domain etoro.com. At the top, there's a dark navigation bar with links for 'Log In · Signup for Free', 'Tools ▾', 'Features ▾', 'Plans', 'Customers', 'Resources ▾', a search bar containing 'Website, Tech, Keyword', and a 'Lookup' button. Below the navigation, the URL 'Home / etoro.com Technology Profile' is displayed. The main title 'ETORO.COM' is centered above a horizontal menu bar with tabs: 'Technology Profile' (which is active), 'Detailed Technology Profile', 'Meta Data Profile', 'Relationship Profile', 'Redirect Profile', and 'Company Profile'. The main content area is divided into several sections: 'Analytics and Tracking' (listing Mixpanel, Hotjar, SteelHouse, and Google Optimize 360), 'Profile Details' (showing last detection date, number of technologies, and a link to the page), and a promotional 'WFH Sale' box for unlimited lookups at \$99/year. Below this, there's a 'Buy Now' button and a link to learn more about Advanced features.

This screenshot shows a detailed technology profile for the Name Server of etoro.com. It includes a 'Name Server' section with a 'View Global Trends' link, a '30 to 49 ccTLD Redirects' section with a 'View Global Trends' link, and an 'Akamai DNS' section with a 'View Global Trends' link. Each section contains a brief description and a link to 'Usage Statistics' and 'Download List' for that specific technology.

Content Delivery Network

[View Global Trends](#)

GStatic Google Static Content

[GStatic Google Static Content Usage Statistics](#) · [Download List of All Websites using GStatic Google Static Content](#)

Google has off-loaded static content (Javascript/Images/CSS) to a different domain name in an effort to reduce bandwidth usage and increase network performance for the end user.

CloudFront

[CloudFront Usage Statistics](#) · [Download List of All Websites using CloudFront](#)

Amazon CloudFront is a web service for content delivery. It integrates with other Amazon Web Services to give developers and businesses an easy way to distribute content to end users with low latency, high data transfer speeds, and no commitments.

AJAX Libraries API

[AJAX Libraries API Usage Statistics](#) · [Download List of All Websites using AJAX Libraries API](#)

The AJAX Libraries API is a content distribution network and loading architecture for the most popular, open source JavaScript libraries.

Yahoo Image CDN

[Yahoo Image CDN Usage Statistics](#) · [Download List of All Websites using Yahoo Image CDN](#)
[url] contains links to Yahoo image CDN.

Cloudflare

[Cloudflare Usage Statistics](#) · [Download List of All Websites using Cloudflare](#)

Automatically optimizes the delivery of your web pages so your visitors get the fastest page load times and best performance.

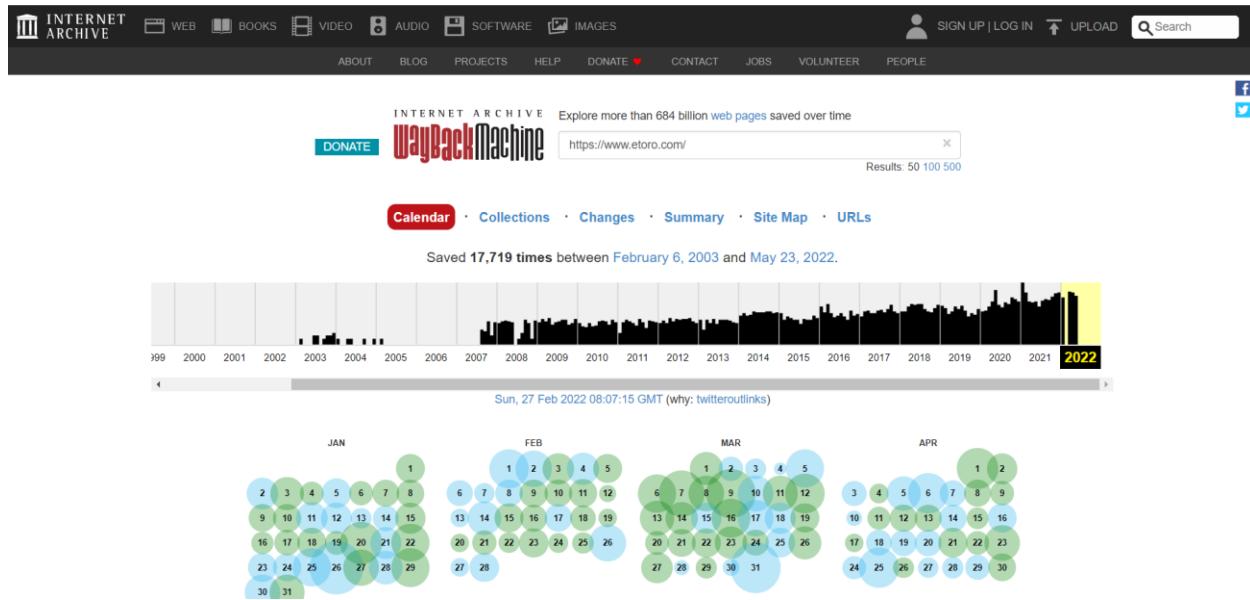
FINDING ACHIEVED INFORMATION

1.Wayback machine

Website URL:- <http://web.archive.org/>

Using wayback machine, we can found some old information of any website we want. Wayback machine is a digital internet archive. It's a collection of more than 684 billion snapshots of web pages. Its contains copies of webpages, videos, audios, books, images etc. Using this website we can get a better understand about any website and its very useful for information gathering.

In here I used this website to find information about etoro.com



INTERNET ARCHIVE Wayback Machine https://www. etoro .com/ 17.719 captures 6 Feb 2003 - 23 May 2022

The screenshot shows the eToro website from May 2015. The header features the eToro logo and navigation links for People, Markets, Trading, Help, and More. A search bar is at the top right. Below the header is a large grid of user profile pictures. A central banner reads "eToro, your social investment network." and "Connect with other traders & investors and copy their trades." A "See how it works!" button with a video icon is visible. To the left, a "Special Offer! Get up to \$1000! Invite Your Friends" box is shown. A green "Start Now" button is prominent on the right. The footer includes a "Join the Carnival" button and a note about cookie usage.

At eToro, the world's leading social investment network, you can tap into the wisdom of the crowds to help you make smarter investment decisions.

Start Now

Special Offer!
Get up to \$1000!
Invite Your Friends

trades opened at eToro

Waiting for web.arc... eToro uses Cookies. When browsing our website, cookies will be stored on your computer. For more information, please see our Cookie Policy x Join the Carnival

eToro in 2015

INTERNET ARCHIVE Wayback Machine https://www. etoro .com/ 17.719 captures 6 Feb 2003 - 23 May 2022

The screenshot shows the eToro website from May 2018. The layout is similar to 2015, with the eToro logo and navigation menu. The main headline is "Trade with confidence on the world's leading social trading network". Below it, a paragraph encourages users to join millions who have discovered smarter investing by copying leading traders. A "Join Now" button is present. On the right, a hand holds a smartphone displaying the eToro mobile app interface, showing a portfolio screen with investment details for EUR/USD and AAPL. The app interface includes a "Portfolio" tab, "INVESTED", "CURRENT", "P/L(\$)", and "P/L(%)".

Trade with confidence on the world's leading social trading network

Join millions who've already discovered smarter investing by automatically copying the leading traders in our community, or get copied yourself to earn a second income!

ARE YOU READY TO TAKE THE BULL BY THE HORNS?

Join Now

BELL 4:21 PM 82% Portfolio INVESTED CURRENT P/L(\$) P/L(%) BUY EUR/USD 29/06/2017 BUY AAPL 11/07/2017

eToro in 2018

SEARCH FOR OPEN PORTS

Any computer based system open ports. Here are some of port numbers and their services.

- 21 – FTP (establish the connection between hosts)
- 22 – SSH (secure shell)
- 25 – SMTP (sending emails to one another across the internet)
- 53 – DNS (domain name service)
- 80 – HTTP (web server)
- 110 – POP3 (email inbox)
- 123 – NTP (Network Time Protocol)
- 143 – IMAP (email inbox)
- 443 – HTTPS (secure web server)
- 465 – SMTPS (send secure email)
- 631 – CUPS (print server)
- 993 – IMAPS (secure email inbox)
- 995 – POP3 (secure email inbox)

Open ports are very important because attackers can get lot of information before initiate an attack.

1.Search for open ports using Nmap tool

I do basic port scan for targeted main domain and sub domains using nmap

Port scan for etoro.com

```
[root@kali]# nmap -sS etoro.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-24 19:48 +0530
Nmap scan report for etoro.com (104.84.161.226)
Host is up (0.021s latency). No server to use. If none is given, the SOA of the target will be used.
rDNS record for 104.84.161.226: a104-84-161-226.deploy.static.akamaitechnologies.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 7.87 seconds
```

Port scan for etoropartners.com

```
[root@kali]# nmap -sS etoropartners.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-24 19:53 +0530
Nmap scan report for etoropartners.com (104.21.22.117)
Host is up (0.026s latency).
Other addresses for etoropartners.com (not scanned): 172.67.204.146 2606:4700:3035::6815:1675 2606:4700:3035::ac43:cc92
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds
```

Port scan for charts.etoro.com

```
[root@kali]# nmap -sS charts.etoro.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-24 19:55 +0530
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 73.60% done; ETC: 19:55 (0:00:05 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 75.50% done; ETC: 19:55 (0:00:04 remaining)
Nmap scan report for charts.etoro.com (104.84.202.82)
Host is up (0.017s latency).
rDNS record for 104.84.202.82: a104-84-202-82.deploy.static.akamaitechnologies.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 15.61 seconds
```

Port scan for etorox.com

```
(root㉿kali)-[~/home/kali]
# nmap -sS etorox.com |disables check for BIND version on name servers
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-24 19:57 +0530
Nmap scan report for etorox.com (104.19.236.38)
Host is up (0.031s latency). of enumeration to perform.
Other addresses for etorox.com (not scanned): 104.19.237.38 2606:4700::6813:ec26 2606:4700::6813:ed26
Not shown: 995 filtered tcp ports (no-response), AAAA, MX and SRV.
PORT      STATE SERVICE          rvl:      Reverse lookup of a given CIDR or IP range.
25/tcp    open  smtp            brt:      Brute force domains and hosts using a given dictionary.
80/tcp    open  http             srv:      SRV records.
443/tcp   open  https           axfr:    Test all NS servers for a zone transfer.
8080/tcp  open  http-proxy      bing:    Perform Bing search for subdomains and hosts.
8443/tcp  open  https-alt       yand:    Perform Yandex search for subdomains and hosts.
                                         crt:    Perform crt.sh search for subdomains and hosts.
Nmap done: 1 IP address (1 host up) scanned in 7.28 seconds  against all NS servers for a given domain, testing
```

Port scan for partners.etoro.com

```
(root㉿kali)-[~/home/kali] DNSrecon version
# nmap -sS partners.etoro.com |verbose
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-24 19:59 +0530
Nmap scan report for partners.etoro.com (104.84.161.226)
Host is up (0.016s latency).std:      SOA, NS, A, AAAA, MX and SRV,
rDNS record for 104.84.161.226: a104-84-161-226.deploy.static.akamaitechnologies.com
Not shown: 997 filtered tcp ports (no-response)ce domains and hosts using a given dictionary.
PORT      STATE SERVICE          srv:      SRV records.
25/tcp    open  smtp            axfr:    Test all NS servers for a zone transfer.
80/tcp    open  http             bing:    Perform Bing search for subdomains and hosts.
443/tcp   open  https           yand:    Perform Yandex search for subdomains and hosts.
                                         crt:    Perform crt.sh search for subdomains and hosts.
```

Find the firewall protection of target domain

1. Using Wafw00f

Kali Linux's wafw00f tool is a web application firewall detection tool that can be used to identify web applications firewall. I used this tool to find my target URL if it's protected by a firewall.

For etoro.com/

```
(root㉿kali)-[~/home/kali]
# wafw00f

File System          404 Hack Not Found
                    405 Not Allowed
                    403 Forbidden
                    500 Internal Error
                    502 Bad Gateway

~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

Usage: wafw00f url1 [url2 [url3 ... ]]
example: wafw00f http://www.victim.org/
wafw00f: error: No test target specified.

[root㉿kali)-[~/home/kali]
# wafw00f https://etoro.com

~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://etoro.com
[+] The site https://etoro.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

For etoropartners.com/

```
[root@kali ~]# ./wafw00f https://etoropartners.com/
File system sample.txt pdsaprivat testcopy allSubdir
W00f! 404 Hack Not Found
Home sample.txt sample.txt sample.txt 405 Not Allowed
plain.txt decrypt.txt privatepath reserved 500 Internal Error
502 Bad Gateway 403 Forbidden
~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://etoropartners.com/
[+] The site https://etoropartners.com/ is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

For charts.etoro.com/

```
[root@kali ~]# ./wafw00f https://charts.etoro.com/
File system sample.txt pdsaprivat testcopy allSubdir
Woof! 404 Hack Not Found
Home sample.txt sample.txt sample.txt 405 Not Allowed
plain.txt decrypt.txt privatepath reserved 500 Internal Error
502 Bad Gateway 403 Forbidden
privatepath reserved 401 Unauthorized
~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://charts.etoro.com/
[+] The site https://charts.etoro.com/ is behind AWS Elastic Load Balancer (Amazon) WAF.
[~] Number of requests: 2
```

For etorox.com/

```
[root@kali ~]# wafw00f https://etorox.com/
```



```
private.pem private.key modded entries
```

~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

```
[*] Checking https://etorox.com/  
[+] The site https://etorox.com/ is behind Cloudflare (Cloudflare Inc.) WAF.  
[~] Number of requests: 2
```

For partners.etoro.com/

```
[root@kali ~]# wafw00f https://partners.etoro.com/
```



```
private.pem private.key modded entries
```

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway 500 Internal Error

~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

```
[*] Checking https://partners.etoro.com/  
[+] The site https://partners.etoro.com/ is behind AWS Elastic Load Balancer (Amazon) WAF.  
[~] Number of requests: 2
```

VULNERABILITY ASSESSMENT AND RECOMMENDATIONS

In this phase, we will analyze all the possible vulnerabilities in our targeted system including OWASP Top 10 vulnerabilities. Also we will come up with the recommendations for each vulnerabilities that assessed. There two ways to assess the vulnerabilities.

- Automated scan
- Manual scan

Automated scan

In here used **Netsparker** to scan vulnerabilities in targeted domains. Netsparker is web application security scan that scan automatically and detect Cross-site scripting (XSS), SQL injection and other vulnerabilities. After scan, Netsparker generate detailed report about vulnerabilities including OWASP Top 10.

1.Target domain :- <https://www.otoro.com/>

1) Out-of-date Version (AngularJS)

- Risk: **High**
- Method: GET

HIGH  | 11

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

Impact

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

AngularJS Improper Input Validation Vulnerability

In AngularJS before 1.7.9 the function `merge()` could be tricked into adding or modifying properties of `Object.prototype` using a `__proto__` payload.

Affected Versions

0.9.0 to 1.7.8

Identified Version

- 1.5.11

Latest Version

- 1.8.3 (in this branch)

Vulnerability Database

- Result is based on 05/24/2022 20:30:00 vulnerability database content.

Certainty



Remedy

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

2) Open Policy Crossdomain.xml Detected

- Risk: **Medium**
- Method: GET

MEDIUM  | 1

CONFIRMED  | 1

Netsparker detected an Open Policy Crossdomain.xml file.

Impact

Open policy Crossdomain.xml file allows other SWF files to make HTTP requests to your web server and see its response. This can be used for accessing one time tokens and CSRF nonces to bypass CSRF restrictions.

Vulnerabilities

2.1. <https://www.etoro.com/crossdomain.xml>

CONFIRMED

Policy Rules

- <allow-access-from domain="*" secure="false" />

Conceptual Proof

```
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<!-- Policy file for xmlsocket://socks.mysite.com -->
<cross-domain-policy>
  <allow-access-from domain="*" secure="false"/>
  <allow-http-request-headers-from domain="*" headers="*" secure="false"/>
</cross-domain-policy>
```

Remedy

Configure your Crossdomain.xml to prevent access from everywhere to your domain.

3) Weak Ciphers Enabled

- Risk: **Medium**
- Method: GET

MEDIUM  | 1

CONFIRMED  | 1

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.

Vulnerabilities

3.1. <https://www.otoro.com/>

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- 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)

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.

4) [Possible] Phishing by Navigating Browser Tabs LOW

- Risk: **Low**
- Method: GET

LOW  | 1

Netsparker identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

Open windows with normal hrefs with the tag `target="_blank"` can modify `window.opener.location` and replace the parent webpage with something else, even on a different origin.

Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack `rel="noopener noreferrer"` attribute, a third party site can change the URL of the source tab using `window.opener.location.assign` and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

Vulnerabilities

4.1. <https://www.etoro.com/en-us/>

External Links

- <https://brokercheck.finra.org/firm/summary/298361>
- <https://www.sipc.org/list-of-members/E>

Certainty

Conceptual proofs

Response

Response Time (ms) : 2562.333 Total Bytes Received : 146378 Body Length : 145866 Is Compressed : No

```
HTTP/1.1 200 OK
alt-svc: h3=":443"; ma=86400, h3-29=:443"; ma=86400
CF-Cache-Status: DYNAMIC
X-Content-Type-Options: nosniff
Server: cloudflare
Connection: keep-alive
Content-Encoding:
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 71107cde89812e86-SIN
Content-Type: text/html
Transfer-Encoding: chunked
Date: Wed, 25 May 2022 18:55:52 GMT
vary:
...
A Securities, Inc.("The BD"), a broker dealer registered with the Securities and Exchange Commission (SEC). The BD is a member of the Financial Industry Regulatory Authority (<a target="_blank" href="https://brokercheck.finra.org/firm/summary/298361">FINRA</a>) and Securities Investor Protection Corporation (<a target="_blank" href="https://www.sipc.org/list-of-members/E">SIPC</a>). eToro USA LLC (NMLS ID: 1769299 ) is not a registered broker-dealer or FINRA member and your cryptocurrency holdings are not FDIC or SIPC insured. Our full disclosures page is <a target="...
...
```

Remedy

- Add `rel=noopener` to the links to prevent pages from abusing `window.opener`. This ensures that the page cannot access the `window.opener` property in Chrome and Opera browsers.
- For older browsers and in Firefox, you can add `rel=noreferrer` which additionally disables the Referer header.

```
<a href="..." target="_blank" rel="noopener noreferrer">...</a>
```

5) Misconfigured X-Frame-Options Header

- Risk: **Low**
- Method: GET

Netsparker detected that the X-Frame-Options HTTP Response header contains an invalid or not widely supported value.

Impact

A broken X-Frame-Options header will expose your users to UI Redressing attacks like Clickjacking. The attacker will load one of the web pages of a vulnerable application in an iframe on their own website. Then the attacker will overlay the iframe with their own HTML elements, which makes it invisible to the user.

Finally, the attacker will place a button element right over one of the buttons that were loaded inside the iframe, for example, the "Delete Account" button on an "Edit Profile" page. Additionally, the attacker will apply a certain CSS property on their own HTML elements, which has the effect that, if your users try to click on the button of the attackers page, they will actually click the "Delete Account" button in the iframe instead.

The only effective way to prevent this is by blocking other sites from loading your website in an iframe. This is what the X-Frame-Options header does. However, the header will not work as intended when an invalid value is set, which might expose your users to client-side attacks such as Clickjacking.

Additionally, the header might be ineffective for the majority of your users if a poorly supported value, such as ALLOW-FROM is set.

Frame Option(s)

- allow-fromfile://*

Certainty



Remedy

Either use the DENY or SAMEORIGIN header value to support the majority of browsers. Additionally, you can define the frame-ancestors Content-Security-Policy directive.

6) Missing X-Frame-Options Header

- Risk: **Low**
- Method: GET

LOW



11

Netsparker detected a missing X-Frame-Optionsheader which means that this website could be at risk of a clickjacking attack.

The X-Frame-OptionsHTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frameor an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Vulnerabilities

10.1. <https://www.otoro.com/>

Certainty



Conceptual proof

```
HTTP/1.1 200 OK
Set-Cookie: TS01047baf=01d53e5818d7a660f5fa0a59d81cfdac6021015267c63536cb905213b6af8616b76b27375a6266d8
3ceee56b6553b04ff6c2c9a4eb; Path=/
Set-Cookie: __cf_bm=IMJ_UNAZJqOzl8aUcMpU7U7UR67CFgIxckx65fKQizE-1653504845-0-AXg2uvobL8P14pvsfDLd10p6I3
852fVa7i03UI0dZeid8qpoRaD+8nZk/g1dNENoQyKDFnutrCuQkmsP0kXQU5nCT7zcpBWL1hltLE/ErGRq; path=/; expires=We
d, 25-May-22 19:24:05 GMT; domain=.etoro.com; HttpOnly; Secure; SameSite=None
Set-Cookie: __cflb=02DiuEAg8LPSYevHEYkaxA3gcDJTcgwA1ZAY5tXjjPaEY; SameSite=None; Secure; path=/; expire
s=Thu, 26-May-22 17:54:05 GMT; HttpOnly
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
X-Content-Type-Options: nosniff
Server: cloudflare
Connection: keep-alive
Content-Encoding:
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/expect-ct"
CF-RAY: 71107a3ffee84d6f-SIN
Content-Type: text/html
Transfer-Encoding: chunked
Date: Wed, 25 May 2022 18:54:05 GMT
vary: Accept-Encoding

<!doctype html>
<html lang="en">
<head>
<link rel="dns-prefetch" href="https://marketing.etorostatic.com" />
<link rel="dns-prefetch" href="https://api-js.mixpanel.com">
<link rel="dns-prefetch" href="https://cdn.mxpn1.com">
<link rel="dns-prefetch" href="https://stats.g.doubleclick.net">
<link rel="dns-prefetch" href="https://www.google-analytics.com">
<link rel="preconnect" href="https://marketing.etorostatic.com">
<link rel="preconnect" dns-prefetch href="https://fonts.googleapis.com">
<link rel="preconnect" dns-prefetch href="https://fonts.gstatic.com/" crossorigin>
<meta charset="utf-8">
<meta name="apple-mobile-web-app-capable" content="yes">
<meta name="viewport" content="width=device-width,minimum-scale=1.0,minimal-ui">
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge" /><script type="text/javascript">(window.NREUM||(N
REUM={})).
```

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
 - X-Frame-Options: DENYIt completely denies to be loaded in frame/iframe.
 - X-Frame-Options: SAMEORIGINIt allows only if the site which wants to load has a same origin.
 - X-Frame-Options: ALLOW-FROM URLIt grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

7) Cookie Not Marked as HttpOnly

- Risk: **Low**
- Method: GET

LOW  | 11

CONFIRMED  | 11

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.

Vulnerabilities

5.1. <https://www.etoro.com/>

CONFIRMED

Identified Cookie(s)

- TS01047baf

Cookie Source

- HTTP Header

Conceptual proof

Response

Response Time (ms) : 439.3932 Total Bytes Received : 163180 Body Length : 162101 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: TS01047baf=01d53e5818d7a660f5fa0a59d81cfdac6021015267c63536cb905213b6af8616b76b27375a6266d8
3ceee56b6553b04ff6c2c9a4eb; Path=/
Set-Cookie: __cf_bm=IMJ_UNAZJqOz18aUcMpU7U7UR67CFgIxckx65fKQizE-1653504845-0-AXg2uvobL8Pl4pvsfDLd10p6I3
852fVa7i03UI0dZeid8qpoRaD+8nZk/g1dNENoQyKDFnutrCuQkmsP0kXQU5nCT7zcpBWL1hltLE/ErGRq; path=/; expires=We
d, 25-May-22 19:24:05 GMT; domain=.etoro.com; HttpOnly; Secure; SameSite=None
Set-Cookie: __cflb=02DiuEAg8LPSYevHEYkaxA3gcDJTcgwA1ZAY5tXjjPaEY; SameSite=None; Secure; path=/; expire
s=Thu, 26-May-22 17:54:05 GMT; HttpOnly
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
X-Content-Type-Options: nosniff
Server: cloudflare
Connection: keep-alive
Content-Encoding:
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 71107a3ffee84d6f-SIN
Content-Type: text/html
Transfer-Encoding: chunked
Date: Wed, 25 MayHTTP/1.1 200 OK
Set-Cookie: TS01047baf=01d53e5818d7a660f5fa0a59d81cfdac6021015267c63536cb905213b6af8616b76b27375a6266d8
3ceee56b6553b04ff6c2c9a4eb; Path=/
Set-Cookie: __cf_bm=IMJ_UNAZJqOz18aUcMpU7U7UR67CFgIxckx65fKQizE-1653504845-0-AXg2uvobL8Pl4pvsfDLd10p6I3
852fVa7i03UI0dZeid8qpoRaD+8nZk/g1dNENoQyKDFnutrCuQkmsP0kXQU5nCT7zcpBWL1hltLE/ErGRq; path=/; expi
...
...
```

Remedy

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

8) Cookie Not Marked as Secure

- Risk: **Low**
- Method: GET

LOW  | 11

CONFIRMED  | 11

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

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

Impact

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

Vulnerabilities

6.1. <https://www.etoro.com/>

CONFIRMED

Identified Cookie(s)

- TS01047baf

Cookie Source

- HTTP Header

Conceptual proof

Response

Response Time (ms) : 439.3932 Total Bytes Received : 163180 Body Length : 162101 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: TS01047baf=01d53e5818d7a660f5fa0a59d81cfdac6021015267c63536cb905213b6af8616b76b27375a6266d8
3ceee56b6553b04ff6c2c9a4eb; Path=/
Set-Cookie: __cf_bm=IMJ_UNAZJq0z18aUcMpU7U7UR67CFgIxckx65fKQizE-1653504845-0-AXg2uvobL8P14pvsfDLd10p6I3
852fVa7i03UI0dZeid8qpoRaD+8nZk/g1dNENoQyKDFnutrCuQkmsP0kXQU5nCT7zcpBWLlhlLE/ErGRq; path=/; expires=We
d, 25-May-22 19:24:05 GMT; domain=.etoro.com; HttpOnly; Secure; SameSite=None
Set-Cookie: __cfIb=02DiueAg8LPSYevHEYkaxA3gcDJTcgwA1ZAY5tXjjPaEY; SameSite=None; Secure; path=/; expire
s=Thu, 26-May-22 17:54:05 GMT; HttpOnly
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
X-Content-Type-Options: nosniff
Server: cloudflare
Connection: keep-alive
Content-Encoding:
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 71107a3ffee84d6f-SIN
Content-Type: text/html
Transfer-Encoding: chunked
Date: Wed, 25 MayHTTP/1.1 200 OK
Set-Cookie: TS01047baf=01d53e5818d7a660f5fa0a59d81cfdac6021015267c63536cb905213b6af8616b76b27375a6266d8
3ceee56b6553b04ff6c2c9a4eb; Path=/
Set-Cookie: __cf_bm=IMJ_UNAZJq0z18aUcMpU7U7UR67CFgIxckx65fKQizE-1653504845-0-AXg2uvobL8P14pvsfDLd10p6I3
852fVa7i03UI0dZeid8qpoRaD+8nZk/g1dNENoQyKDFnutrCuQkmsP0kXQU5nCT7zcpBWLlhlLE/ErGRq; path=/; expi
...
```

Actions to Take

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

Remedy

Mark all cookies used within the application as secure.

9) Insecure Frame (External)

- Risk: **Low**
- Method: GET

Netsparker identified an external insecure or misconfigured iframe.

Impact

Iframe sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

The Same Origin Policy (SOP) will prevent JavaScript code from one origin from accessing properties and functions - as well as HTTP responses - of different origins. The access is only allowed if the protocol, port and also the domain match exactly.

Here is an example, the URLs below all belong to the same origin as <http://site.com>:

*http://site.com
http://site.com/
http://site.com/my/page.html*

Whereas the URLs mentioned below aren't from the same origin as <http://site.com>:

*http://www.site.com (a sub domain)
http://site.org (different top level domain)
https://site.com (different protocol)
http://site.com:8080 (different port)*

When the `sandbox` attribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

- Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.
- Forms are disabled. The hosted content is not allowed to make forms post back to any target.
- Scripts are disabled. JavaScript is disabled and will not execute.
- Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
- Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the sandbox attribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

- Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.
 - Forms are disabled. The hosted content is not allowed to make forms post back to any target.
 - Scripts are disabled. JavaScript is disabled and will not execute.
 - Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
 - Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.
-

When the sandbox attribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure iframe might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

- It might trick the user into supplying a username and password to the site loaded inside the iframe.
- It might navigate the parent window to a phishing page.
- It might execute untrusted code.
- It could show a popup, appearing to come from the parent site.

Sandbox containing a value of :

- allow-same-origin will not treat it as a unique origin.
- allow-top-navigation will allow code in the iframe to navigate the parent somewhere else, e.g. by changing parent.location.
- allow-forms will allow form submissions from inside the iframe.
- allow-popups will allow popups.
- allow-scripts will allow malicious script execution however it won't allow to create popups.

Frame Source(s)

- <https://www.googletagmanager.com/ns.html?id=GTM-N7SQ5DP>

Conceptual proof

Response

```
Response Time (ms) : 439.3932  Total Bytes Received : 163180  Body Length : 162101  Is Compressed : No

HTTP/1.1 200 OK
Set-Cookie: TS01047baf=01d53e5818d7a660f5fa0a59d81cfdac6021015267c63536cb905213b6af8616b76b27375a6266d8
3ceee56b6553b04ff6c2c9a4eb; Path=/
Set-Cookie: __cf_bm=IMJ_UNAZJqz18aUcMpU7UR67CFgIxckx65fKQizE-1653504845-0-AXg2uvobL8P14pvsfDLd10p6I3
852fVa7i03UI0dZeid8qpoRaD+8nZk/g1dNENoQyKDFnutrCuQkmsP0kXQU5nCT7zcpBWLlhltLE/ErGRq; path=/; expires=Wed, 25-May-22 19:24:05 GMT; domain=.etoro.com; HttpOnly; Secure; SameSite=None
Set-Cookie: __cflb=02DiueAg8LPSYevHEYkaxA3gcDJTcgwA1ZAY5tXjjPaEY; SameSite=None; Secure; path=/; expires=Thu, 26-May-22 17:54:05 GMT; HttpOnly
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
X-Content-Type-Options: nosniff
Server: cloudflare
Connection: keep-alive
Content-Encoding:
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 71107a3ffee84d6f-SIN
Content-Type: text/html
Transfer-Encoding: chunked
Date: Wed, 25 May
...
}
win[appsContainer]['etoroHomePage'] = createinstance('HomePage', 1.1, 'HomePage', {}, true, 'productio
n');
})(window, 'etoroLogger', 'etoroLoggerApps');

</script>

<noscript><iframe src="https://www.googletagmanager.com/ns.html?id=GTM-N7SQ5DP"
height="0" width="0" style="display:none;visibility:hidden"></iframe></noscript>
<style>*****GENERAL*****</style>
```

Remedy

- Apply sandboxing in inline frame

```
<iframe sandbox src="framed-page-url"></iframe>
```

- For untrusted content, avoid the usage of seamless attribute and allow-top-navigation, allow-popups and allow-scripts in sandbox attribute.

10) Internal Server Error

- Risk: **Low**
- Method: GET

LOW  | 11

CONFIRMED  | 11

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

Vulnerabilities

8.1. [https://www.etoro.com/%23%7b28275*28275-\(8109\)%7d/404-page/?aspxerrorpath=/cs-cz/~/aspx](https://www.etoro.com/%23%7b28275*28275-(8109)%7d/404-page/?aspxerrorpath=/cs-cz/~/aspx)

CONFIRMED

Method	Parameter	Value
GET	param2	404-page
GET	aspxerrorpath	/cs-cz/~/aspx
GET	param1	{28275*28275-(8109)}

Conceptual proof

Response

Response Time (ms) : 667.4142 Total Bytes Received : 2637 Body Length : 2110 Is Compressed : No

```
HTTP/1.1 500 Internal Server Error
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
X-Content-Type-Options: nosniff
Server: cloudflare
Connection: keep-alive
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7110b8adbccba126-SIN
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Date: Wed, 25 May 2022 19:44:40 HTTP/1.1 500 Internal Server Error

alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
X-Content-Type-Options: nosniff
Server: cloudflare
Connection: keep-alive
Strict-Transport-Security: max-age=15552000
...
```

Remedy

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.

11.Email Address Disclosure

- Risk: [Information](#)
- Method: GET

INFORMATION  1

Netsparker identified an Email Address Disclosure.

Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Vulnerabilities

19.1. <https://www.etoro.com/cdn-cgi/bm/cv/669835187/api.js>

Email Address(es)

- amdfcruz@gmail.com

Certainty



Conceptual proof

Response

Response Time (ms) : 910.0552 Total Bytes Received : 36193 Body Length : 35662 Is Compressed : No

```
HTTP/1.1 200 OK
alt-svc: h3=":443"; ma=86400, h3-29=:443; ma=86400
Server: cloudflare
x-content-type-options: nosniff
Connection: keep-alive
Content-Encoding:
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 71107cd38a2287f3-SIN
Content-Type: text/javascript
Transfer-Encoding: chunked
Date: Wed, 25 May 2022 18:55:50 GMT
cache-control: max-age=604800, public
Vary:
...
pe: text/javascript
Transfer-Encoding: chunked
Date: Wed, 25 May 2022 18:55:50 GMT
cache-control: max-age=604800, public
Vary: Accept-Encoding

/**
 * @license
 * Copyright (c) 2015 André Cruz <amdfcruz@gmail.com>
 * Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the 'Software'), to deal in the Software without restriction, inc
...

```

Remedy

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

12. Forbidden Resource

- Risk: Information
- Method: GET

INFORMATION  11

CONFIRMED  11

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

21.1. <https://www.otoro.com/>

CONFIRMED

Conceptual proof

Response

Response Time (ms) : 2290.3662 Total Bytes Received : 4506 Body Length : 3925 Is Compressed : No

```
HTTP/1.1 403 Forbidden
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Expires: Wed, 25 May 2022 18:56:10 GMT
X-Content-Type-Options: nosniff
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/expect-ct"
CF-RAY: 71107cf2bab80172-SIN
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Wed, 25 May 2022 18:55:55 GMT
Cache-Control: HTTP/1.1 403 Forbidden

alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Expires: Wed, 25 May 2022 18:56:10 GMT
X-Content-Type-Options: nosniff
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
...
```

Vulnerability summary

199

IDENTIFIED

58

CONFIRMED

0

CRITICAL

11

HIGH



2

MEDIUM



67

LOW



58

BEST PRACTICE



61

INFORMATION



Identified Vulnerabilities



Critical	0
High	11
Medium	2
Low	67
Best Practice	58
Information	61
TOTAL	199

Confirmed Vulnerabilities



Critical	0
High	0
Medium	2
Low	44
Best Practice	0
Information	12
TOTAL	58

2. Target domain - <https://etoropartners.com/>

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

- Risk : Medium
- Method: GET

MEDIUM  | 1

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.

Vulnerabilities

1.1. <https://etoropartners.com/>

Certainty



Conceptual proof

Response

Response Time (ms) : 338.2355 Total Bytes Received : 7639 Body Length : 7068 Is Compressed : No

```
HTTP/1.1 502 Bad Gateway
Set-Cookie: cf_ob_info=502:7118baba9edd4b5c:SIN; path=/; expires=Thu, 26-May-22 18:56:42 GMT
Set-Cookie: cf_use_ob=443; path=/; expires=Thu, 26-May-22 18:56:42 GMT
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Referrer-Policy: same-origin
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
CF-RAY: 7118baba9edd4b5c-SIN
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 26 May 2022 18:56:12 GMT
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
```

Remedy

Configure your webserver so that HTTP queries are forwarded to HTTPS.

2. Weak Cipher Enabled

- Risk : Medium
- Method: GET

MEDIUM



| 1

CONFIRMED



| 1

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.

Vulnerabilities

2.1. <https://etoropartners.com/>

CONFIRMED

List of Supported Weak Ciphers

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)

Request

[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.**

- a. Click Start, click Run, type regedit32 or type regedit, and then click OK.
- b. In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
- c. Set "Enabled" DWORD to "0x0" for the following registry keys:

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

Remedy

Configure your web server to disallow using weak ciphers.

3. Cookie Not Marked as HttpOnly

- Risk: **Low**
- Method: GET

LOW  | 11

CONFIRMED  | 11

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.

Vulnerabilities

3.1. <https://etoropartners.com/>

CONFIRMED

Identified Cookie(s)

- cf_use_ob
- cf_ob_info

Cookie Source

- HTTP Header

Conceptual proof

Response

Response Time (ms) : 1200.0396 Total Bytes Received : 7639 Body Length : 7068 Is Compressed : No

```
HTTP/1.1 502 Bad Gateway
Set-Cookie: cf_ob_info=502:7118ba06892749c0:SIN; path=/; expires=Thu, 26-May-22 18:56:14 GMT
Set-Cookie: cf_use_ob=443; path=/; expires=Thu, 26-May-22 18:56:14 GMT
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Referrer-Policy: same-origin
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
CF-RAY: 7118ba06892749c0-SIN
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 26 May 2022 18:55:44 GMT
Cache-Control: private, max-age=0, no-store, no-cache, must-HTTP/1.1 502 Bad Gateway
Set-Cookie: cf_ob_info=502:7118ba06892749c0:SIN; path=/; expires=Thu, 26-May-22 18:56:14 GMT

Set-Cookie: cf_use_ob=443; path=/; expires=Thu, 26-May-22 18:56:14 GMT

Expires: Thu, 01 Jan 1970 00:00:01 GMT
Referrer-Policy: same-origin
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
CF-RAY: 7118ba06892749c0-SIN
Content-Type: text/html; c
...
```

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

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

4. Cookie Not Marked as Secure

- Risk: **Low**
- Method: GET

LOW  11

CONFIRMED  11

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

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

Impact

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

Vulnerabilities

4.1. <https://etoropartners.com/>

CONFIRMED

Identified Cookie(s)

- cf_use_ob
- cf_ob_info

Cookie Source

- HTTP Header

Conceptual proof

Response

Response Time (ms) : 1200.0396 Total Bytes Received : 7639 Body Length : 7068 Is Compressed : No

```
HTTP/1.1 502 Bad Gateway
Set-Cookie: cf_ob_info=502:7118ba06892749c0:SIN; path=/; expires=Thu, 26-May-22 18:56:14 GMT
Set-Cookie: cf_use_ob=443; path=/; expires=Thu, 26-May-22 18:56:14 GMT
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Referrer-Policy: same-origin
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
CF-RAY: 7118ba06892749c0-SIN
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 26 May 2022 18:55:44 GMT
Cache-Control: private, max-age=0, no-store, no-cache, must-HTTP/1.1 502 Bad Gateway
Set-Cookie: cf_ob_info=502:7118ba06892749c0:SIN; path=/; expires=Thu, 26-May-22 18:56:14 GMT

Set-Cookie: cf_use_ob=443; path=/; expires=Thu, 26-May-22 18:56:14 GMT

Expires: Thu, 01 Jan 1970 00:00:01 GMT
Referrer-Policy: same-origin
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
CF-RAY: 7118ba06892749c0-SIN
Content-Type: text/html; c
...
```

Actions to Take

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

Remedy

Mark all cookies used within the application as secure.

5. Forbidden Resource

- Risk: Information
- Method: GET

INFORMATION  | 4

CONFIRMED  | 4

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

10.1. <https://etoropartners.com/cdn-cgi/images/>

CONFIRMED

Conceptual proof

Response

Response Time (ms) : 79.8855 Total Bytes Received : 842 Body Length : 553 Is Compressed : No

HTTP/1.1 403 Forbidden

```
X-Content-Type-Options: nosniff
Server: cloudflare
CF-RAY: 7118bab3582d9fb3-SIN
Connection: keep-alive
X-Frame-Options: DENY
Content-Type: text/html
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 26 May 2022 18:56:10 GMT
Vary: Accept-Encoding

<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>cloudflare</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

6. Robots.txt Detected

- Risk: **Information**
- Method: GET

INFORMATION  | 1

CONFIRMED  | 1

Netsparker detected a Robots.txt file with potentially sensitive content.

Impact

Depending on the content of the file, an attacker might discover hidden directories and files.

Vulnerabilities

11.1. <https://etoropartners.com/robots.txt>

CONFIRMED

Interesting Robots.txt Entries

- Disallow: /wp-admin/

Remedy

Ensure you have nothing sensitive exposed within this file, such as the path of an administration panel. If disallowed paths are sensitive and you want to keep it from unauthorized access, do not write them in the Robots.txt, and ensure they are correctly protected by means of authentication.

Robots.txt is only used to instruct search robots which resources should be indexed and which ones are not.

The following block can be used to tell the crawler to index files under /web/ and **ignore the rest**:

User-Agent: *

Allow: /web/
Disallow: /

Please note that when you use the instructions above, **search engines will not index your website** except for the specified directories.

If you want to hide certain section of the website from the search engines X-Robots-Tag can be set in the response header to tell crawlers whether the file should be indexed or not:

```
X-Robots-Tag: googlebot:nofollow  
X-Robots-Tag: otherbot: noindex, nofollow
```

By using X-Robots-Tag you don't have to list the these files in your Robots.txt.

It is also not possible to prevent media files from being indexed by putting using Robots Meta Tags. X-Robots-Tag resolves this issue as well.

For Apache, the following snippet can be put into httpd.conf or an .htaccess file to restrict crawlers to index multimedia files without exposing them in Robots.txt

```
<Files ~ "\.pdf$">  
# Don't index PDF files.  
Header set X-Robots-Tag "noindex, nofollow"  
</Files>
```

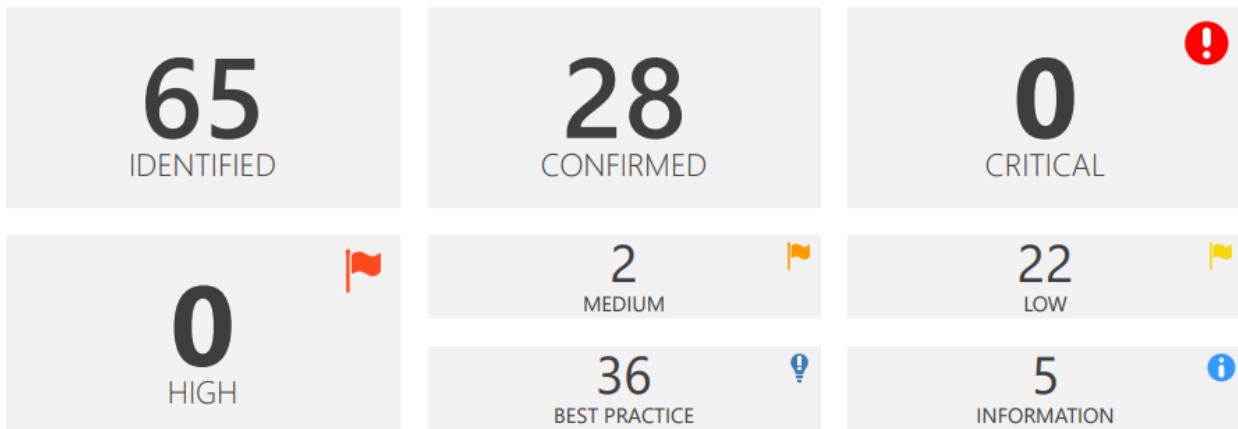
```
<Files ~ "\.(png|jne?g|gif)$">  
#Don't index image files.  
Header set X-Robots-Tag "noindex"  
</Files>
```

Conceptual proof

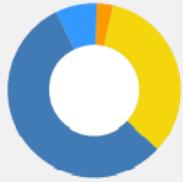
Content-Encoding:

```
User-agent: *  
Disallow: /wp-admin/  
Allow: /wp-admin/admin-ajax.php
```

Vulnerability summary



Identified Vulnerabilities



Critical	0
High	0
Medium	2
Low	22
Best Practice	36
Information	5
TOTAL	65

Confirmed Vulnerabilities



Critical	0
High	0
Medium	1
Low	22
Best Practice	0
Information	5
TOTAL	28

3. Target domain - <https://charts.otoro.com/>

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

- Risk : Medium
- Method: GET

MEDIUM  | 1

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.

Certainty



Conceptual proof

Response

Response Time (ms) : 113.8422 Total Bytes Received : 72591 Body Length : 71958 Is Compressed : No

```
HTTP/1.1 200 OK
Cache-Control: max-age=300
ETag: "f1bde4626df8c3244b53ed4d1779bd47"
x-amz-request-id: 8FKVPEA3PPG3R476
frame-ancestors: *.otoro.com
frame-ancestors: *.otoro.com
Server: AmazonS3
Accept-Ranges: bytes
Connection: keep-alive
Expires: Thu, 26 May 2022 19:26:20 GMT
x-amz-id-2: CJEEZYTrPiswAJU52SsejMBsqZQ8jSwXq0+udsFnusk3ow9/K94yC9vUPC/5fvfvGHfHn/FmMw4=
Vary: Accept-Encoding
x-amz-meta-s3fox-modifiedtime: 1449592060000
Content-Length: 18883
x-amz-meta-s3fox-filename: 71958
Last-Modified: Tue, 08 Dec 2015 16:35:59 GMT
Content-Type: text/html
Date: Thu, 26 May 2022 19:21:20 GMT
Content-Encoding:
```

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>
```

External References

- [Wikipedia - HTTP Strict Transport Security](#)
- [Configure HSTS \(HTTP Strict Transport Security\) for Apache/Nginx](#)
- [HTTP Strict Transport Security \(HSTS\) HTTP Header](#)
- [Mozilla SSL Configuration Generator](#)

2. Weak Ciphers Enabled

- Risk : Medium
- Method: GET

MEDIUM  | 1

CONFIRMED  | 1

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.

Vulnerabilities

2.1. <https://charts.etoro.com/>

CONFIRMED

List of Supported Weak Ciphers

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)

Request

[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.**

- a. Click Start, click Run, type regedit32 or type regedit, and then click OK.
- b. In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
- c. Set "Enabled" DWORD to "0x0" for the following registry keys:

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

Remedy

Configure your web server to disallow using weak ciphers.

3. Missing X-Frame-Options Header

- Risk: **Low**
- Method: GET

LOW



| 1

Netsparker detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack.

The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Vulnerabilities

5.1. <https://charts.etoro.com/>

Certainty



Conceptual proof

Response

Response Time (ms) : 427.7785 Total Bytes Received : 72561 Body Length : 71958 Is Compressed : No

```
HTTP/1.1 200 OK
Cache-Control: max-age=300
ETag: "f1bde4626df8c3244b53ed4d1779bd47"
x-amz-request-id: 8FKVPEA3PPG3R476
frame-ancestors: *.etoro.com
Server: AmazonS3
Connection: keep-alive
Expires: Thu, 26 May 2022 19:26:01 GMT
x-amz-id-2: CJEEZYTrPiswAJU52SsejMBsqZQ8jSwXq0+udsFnusk3ow9/K94yC9vUPC/5fvfvGHfHn/FmMw4=
Vary: Accept-Encoding
x-amz-meta-s3fox-modifiedtime: 1449592060000
Content-Length: 18883
x-amz-meta-s3fox-filesize: 71958
Last-Modified: Tue, 08 Dec 2015 16:35:59 GMT
Content-Type: text/html
Accept-Ranges: bytes
Date: Thu, 26 May 2022 19:21:01 GMT
Content-Encoding:
```

Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
 - X-Frame-Options: DENY It completely denies to be loaded in frame/iframe.
 - X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.
 - X-Frame-Options: ALLOW-FROM URL It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

Remedy references

- [Clickjacking Defense Cheat Sheet](#)

4. Cookie Not Marked as HttpOnly

- Risk: **Low**
- Method: GET

LOW  | 1

CONFIRMED  | 1

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.

Vulnerabilities

3.1. <https://charts.etoro.com/>

CONFIRMED

Identified Cookie(s)

- _ga
- _gid
- _gat

Cookie Source

- JavaScript

Conceptual proof

Response

Response Time (ms) : 427.7785 Total Bytes Received : 72561 Body Length : 71958 Is Compressed : No

```
HTTP/1.1 200 OK
Cache-Control: max-age=300
ETag: "f1bde4626df8c3244b53ed4d1779bd47"
x-amz-request-id: 8FKVPEA3PPG3R476
frame-ancestors: *.etoro.com
Server: AmazonS3
Connection: keep-alive
Expires: Thu, 26 May 2022 19:26:01 GMT
x-amz-id-2: CJEEZYTrPiswAJU52SsejMBsqZQ8jSwXq0+udsFnusk3ow9/K94yC9vUPC/5fvfvGHfHn/FmMw4=
Vary: Accept-Encoding
x-amz-meta-s3fox-modifiedtime: 1449592060000
Content-Length: 18883
x-amz-meta-s3fox-filesize: 71958
Last-Modified: Tue, 08 Dec 2015 16:35:59 GMT
Content-Type: text/html
Accept-Ranges: bytes
Date: Thu, 26 May 2022 19:21:01 GMT
Content-Encoding:
```

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

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

5. Cookie Not Marked as Secure

- Risk: **Low**
- Method: GET

LOW



| 1

CONFIRMED



| 1

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

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

Impact

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

Vulnerabilities

4.1. <https://charts.otoro.com/>

CONFIRMED

Identified Cookie(s)

- _ga
- _gid
- _gat

Cookie Source

- JavaScript

Conceptual proof

Request

```
GET / HTTP/1.1
Host: charts.etoro.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
```

Response

```
Response Time (ms) : 427.7785 Total Bytes Received : 72561 Body Length : 71958 Is Compressed : No
```

```
HTTP/1.1 200 OK
Cache-Control: max-age=300
ETag: "f1bde4626df8c3244b53ed4d1779bd47"
x-amz-request-id: 8FKVPEA3PPG3R476
frame-ancestors: *.etoro.com
Server: AmazonS3
Connection: keep-alive
Expires: Thu, 26 May 2022 19:26:01 GMT
x-amz-id-2: CJEEZYTrPiswAJU52SsejMBsqZQ8jSwXq0+udsFnusk3ow9/K94yC9vUPC/5fvfvGHfHn/FmMW4=
Vary: Accept-Encoding
x-amz-meta-s3fox-modifiedtime: 1449592060000
Content-Length: 18883
x-amz-meta-s3fox-filesize: 71958
Last-Modified: Tue, 08 Dec 2015 16:35:59 GMT
Content-Type: text/html
Accept-Ranges: bytes
Date: Thu, 26 May 2022 19:21:01 GMT
Content-Encoding:
```

Actions to Take

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

Remedy

Mark all cookies used within the application as secure.

6. Forbidden Resource

- Risk: [Information](#)
- Method: GET

INFORMATION  11

CONFIRMED  11

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

11.1. <https://charts.etoro.com/>

CONFIRMED

Conceptual proof

Response

Response Time (ms) : 325.5473 Total Bytes Received : 528 Body Length : 262 Is Compressed : No

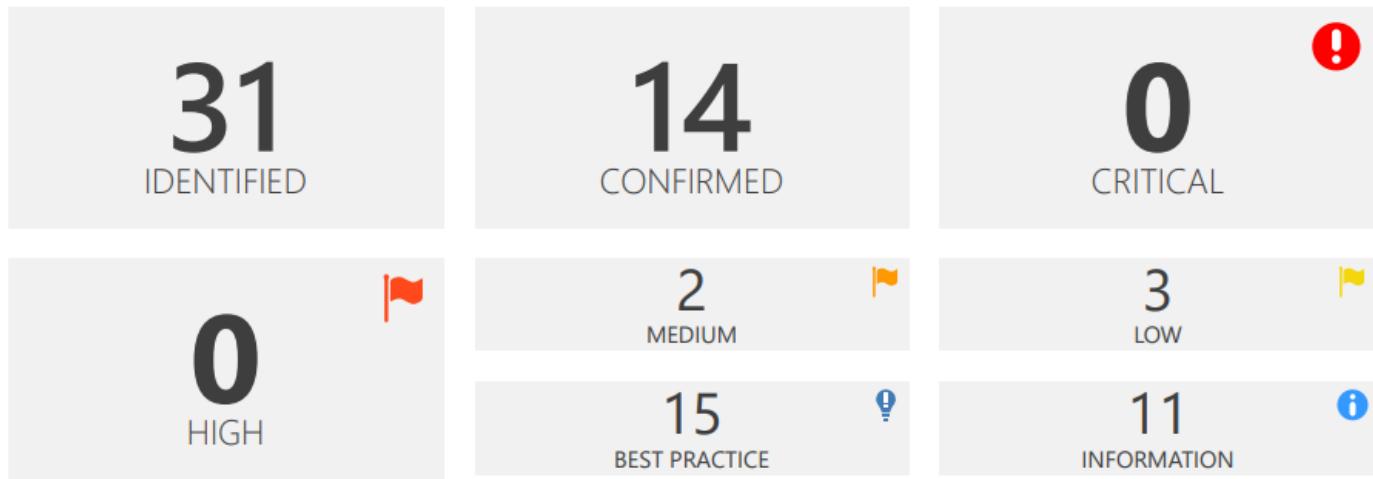
HTTP/1.1 403 Forbidden

```
Server: AkamaiGHost
Content-Length: 262
Expires: Thu, 26 May 2022 19:26:24 GMT
Connection: close
Mime-Version: 1.0
frame-ancestors: *.etoro.com
Content-Type: text/html
Date: Thu, 26 May 2022 19:21:24 GMT
Cache-Control: max-age=300

<HTML><HEAD>
<TITLE>Access Denied</TITLE>
</HEAD><BODY>
<H1>Access Denied</H1>

You don't have permission to access "http#58;#47;#47;charts#46;etoro#46;com#47;" on this server.<
P>
Reference#32;#35;18#46;651d2017#46;1653592884#46;5b56
</BODY>
</HTML>
```

Vulnerability summary



Identified Vulnerabilities



Critical	0
High	0
Medium	2
Low	3
Best Practice	15
Information	11
TOTAL	31

Confirmed Vulnerabilities



Critical	0
High	0
Medium	1
Low	2
Best Practice	0
Information	11
TOTAL	14

4. Target domain - <https://etorox.com/>

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

- Risk : Medium
- Method: GET

MEDIUM  1

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.

Certainty



Conceptual proof

Response

Response Time (ms) : 354.6928 Total Bytes Received : 7625 Body Length : 7054 Is Compressed : No

```
HTTP/1.1 502 Bad Gateway
Set-Cookie: cf_ob_info=502:7118f2250dd3a3f2:SIN; path=/; expires=Thu, 26-May-22 19:34:32 GMT
Set-Cookie: cf_use_ob=443; path=/; expires=Thu, 26-May-22 19:34:32 GMT
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Referrer-Policy: same-origin
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
CF-RAY: 7118f2250dd3a3f2-SIN
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 26 May 2022 19:34:02 GMT
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
```

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>
```

External References

- [Wikipedia - HTTP Strict Transport Security](#)
- [Configure HSTS \(HTTP Strict Transport Security\) for Apache/Nginx](#)
- [HTTP Strict Transport Security \(HSTS\) HTTP Header](#)
- [Mozilla SSL Configuration Generator](#)

2. Weak Ciphers Enabled

- Risk : Medium
- Method: GET

MEDIUM



1

CONFIRMED



1

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.

Vulnerabilities

2.1. <https://etorox.com/>

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- 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

Action 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.

3.Missing Content-Type Header

- Risk: **Low**
- Method: GET

LOW  | 1

Netsparker detected a missing Content-Type header which means that this website could be at risk of a MIME-sniffing attacks.

Impact

MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing.

This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type.

The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image.

Vulnerabilities

5.1. <https://etorox.com/cdn-cgi/>

Certainty



Conceptual proof

Response

```
Response Time (ms) : 254.3787    Total Bytes Received : 389    Body Length : 0    Is Compressed : No
```

```
HTTP/1.1 404 Not Found
CF-Cache-Status: MISS
CF-RAY: 7118f21c98b6016a-SIN
Server: cloudflare
Expires: Thu, 26 May 2022 23:34:00 GMT
Connection: keep-alive
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Transfer-Encoding: chunked
Date: Thu, 26 May 2022 19:34:00 GMT
Cache-Control: public, max-age=14400
Vary: Accept-Encoding
```

Remedy

1. When serving resources, make sure you send the content-type header to appropriately match the type of the resource being served. For example, if you are serving an HTML page, you should send the HTTP header:

```
Content-Type: text/html
```

2. Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.

```
X-Content-Type-Options: nosniff
```

4.Cookie Not Marked as HttpOnly

- Risk: **Low**
- Method: GET

LOW  | 11

CONFIRMED  | 11

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.

Vulnerabilities

3.1. <https://etorox.com/>

CONFIRMED

Identified Cookie(s)

- cf_ob_info
- cf_use_ob

Cookie Source

- HTTP Header

Conceptual proof

Response

Response Time (ms) : 1236.3139 Total Bytes Received : 7586 Body Length : 7015 Is Compressed : No

```
HTTP/1.1 502 Bad Gateway
Set-Cookie: cf_ob_info=502:7118f19b6e7e4993:SIN; path=/; expires=Thu, 26-May-22 19:34:10 GMT
Set-Cookie: cf_use_ob=443; path=/; expires=Thu, 26-May-22 19:34:10 GMT
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Referrer-Policy: same-origin
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
CF-RAY: 7118f19b6e7e4993-SIN
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 26 May 2022 19:33:40 GMT
Cache-Control: private, max-age=0, no-store, no-cache, must-HTTP/1.1 502 Bad Gateway
Set-Cookie: cf_ob_info=502:7118f19b6e7e4993:SIN; path=/; expires=Thu, 26-May-22 19:34:10 GMT

Set-Cookie: cf_use_ob=443; path=/; expires=Thu, 26-May-22 19:34:10 GMT

Expires: Thu, 01 Jan 1970 00:00:01 GMT
Referrer-Policy: same-origin
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
CF-RAY: 7118f19b6e7e4993-SIN
Content-Type: text/html; c
...
```

Actions to Take

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

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

5. Cookie Not Marked as Secure

- Risk: **Low**
- Method: GET

LOW  11

CONFIRMED  11

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

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

Impact

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

Vulnerabilities

4.1. <https://etorox.com/>

CONFIRMED

Identified Cookie(s)

- cf_ob_info
- cf_use_ob

Cookie Source

- HTTP Header

Conceptual proof

Response

Response Time (ms) : 1236.3139 Total Bytes Received : 7586 Body Length : 7015 Is Compressed : No

HTTP/1.1 502 Bad Gateway
Set-Cookie: cf_ob_info=502:7118f19b6e7e4993:SIN; path=/; expires=Thu, 26-May-22 19:34:10 GMT
Set-Cookie: cf_use_ob=443; path=/; expires=Thu, 26-May-22 19:34:10 GMT
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Referrer-Policy: same-origin
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
CF-RAY: 7118f19b6e7e4993-SIN
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 26 May 2022 19:33:40 GMT
Cache-Control: private, max-age=0, no-store, no-cache, must-HTTP/1.1 502 Bad Gateway
Set-Cookie: cf_ob_info=502:7118f19b6e7e4993:SIN; path=/; expires=Thu, 26-May-22 19:34:10 GMT

Set-Cookie: cf_use_ob=443; path=/; expires=Thu, 26-May-22 19:34:10 GMT

Expires: Thu, 01 Jan 1970 00:00:01 GMT
Referrer-Policy: same-origin
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
CF-RAY: 7118f19b6e7e4993-SIN
Content-Type: text/html; c
...

Actions to Take

Actions to Take

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

Remedy

Mark all cookies used within the application as secure.

6. Web Application Firewall Detected

- Risk: Information
- Method: GET

INFORMATION | 1

Netsparker detected that the target website is using a Web Application Firewall (WAF).

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

13.1. https://etorox.com/%3Cscript%3Ealert(0)%3C/script%3E

Method	Parameter	Value
GET	URI-BASED	<script>alert(0)</script>

WAF Name

- Cloudflare

Certainty



7. Forbidden Resource

- Risk: **Information**
- Method: GET

INFORMATION  | 11

CONFIRMED  | 11

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

12.1. <https://etorox.com/>

CONFIRMED

Conceptual proof

Response

Response Time (ms) : 185.4631 Total Bytes Received : 4371 Body Length : 3950 Is Compressed : No

```
HTTP/1.1 403 Forbidden
Expires: Thu, 26 May 2022 19:34:21 GMT
CF-RAY: 7118f2434cad9f8c-SIN
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Thu, 26 May 2022 19:34:06 GMT
Cache-Control: HTTP/1.1 403 Forbidden
```

```
Expires: Thu, 26 May 2022 19:34:21 GMT
CF-RAY: 7118f2434cad9f8c-SIN
Server: cloudflare
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Expect-CT: max-age=604800, report-uri="https://report-ur
...

```

Vulnerability summary

79
IDENTIFIED

34
CONFIRMED

0
CRITICAL

0
HIGH

2
MEDIUM

23
LOW

42
BEST PRACTICE

12
INFORMATION

Identified Vulnerabilities



Critical	0
High	0
Medium	2
Low	23
Best Practice	42
Information	12
TOTAL	79

Confirmed Vulnerabilities



Critical	0
High	0
Medium	1
Low	22
Best Practice	0
Information	11
TOTAL	34

5.Target domain - <https://partners.otoro.com/>

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

- Risk : Medium
- Method: GET

MEDIUM  | 1

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.

Vulnerabilities

1.1. <https://partners.otoro.com/>

Certainty



Conceptual proof

Response

Response Time (ms) : 194.3214 Total Bytes Received : 12016 Body Length : 11592 Is Compressed : No

```
HTTP/1.1 200 OK
x-amz-id-2: DYMxWCOfd/rY7/utiAzlkBKvygLZHgOeRqpFrZBNNnRNcvU10YRw+ner/okVMUn0+73eZdxKoyA=
Server: AmazonS3
x-amz-request-id: 2HFHDRTZ8ZS2C1GD
Content-Length: 2846
Last-Modified: Sun, 24 Apr 2022 10:00:34 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Type: text/html
Content-Encoding:
Connection: keep-alive
Date: Mon, 30 May 2022 18:39:37 GMT
ETag: "10a90d7706de8f21059cb906eeae9800"
```

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>
```

2. Weak Ciphers Enabled

- Risk : Medium
- Method: GET

MEDIUM  | 1

CONFIRMED  | 1

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.

Vulnerabilities

2.1. <https://partners.etoro.com/>

CONFIRMED

List of Supported Weak Ciphers

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)

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.**

- 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.

3.Forbidden Resource

- Risk: [Information](#)
- Method: GET

INFORMATION  | 5

CONFIRMED  | 5

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

4.1. <https://partners.etoro.com/>

CONFIRMED

Conceptual proof

Response

Response Time (ms) : 90.5341 Total Bytes Received : 476 Body Length : 268 Is Compressed : No

HTTP/1.1 403 Forbidden

```
Server: AkamaiGHost
Content-Length: 268
Expires: Mon, 30 May 2022 18:39:47 GMT
Connection: close
Mime-Version: 1.0
Content-Type: text/html
Date: Mon, 30 May 2022 18:39:47 GMT

<HTML><HEAD>
<TITLE>Access Denied</TITLE>
</HEAD><BODY>
<H1>Access Denied</H1>

You don't have permission to access "http##;##;partners##;etoro##;com##;" on this serve
r.<P>
Reference##35;18##;a760c117##;1653935987##;38d62f5d
</BODY>
</HTML>
```

Manual Testing

In here I manually checked the vulnerabilities on targeted domains.

Testing Broken Access Control

A broken access control scenario is a type of attack that allows an attacker to modify or perform actions outside of an systems' authorized access.

1.Target domain - <https://www.etoro.com/>

I tried broken access control by adding `/app/getappInfo` to end of the url to get admins access. But it redirected to the home page.

The screenshot shows the eToro website homepage. The URL in the address bar is <https://www.etoro.com/home/app/getappInfo>. The page features a dark header with the eToro logo and a search bar. On the left, a sidebar shows a user profile for 'SubashM' with options like Home, Watchlist, Portfolio, Discover, and More. A prominent blue button labeled 'Deposit Funds' is visible. The main content area has a large 'Welcome to eToro!' banner with a 'verify' button and a magnifying glass over a document with a checkmark. Below the banner, there's a 'News Feed' section with a placeholder 'What's on your mind?' and a 'Big Movers' section stating 'No big movement to display at the moment'.

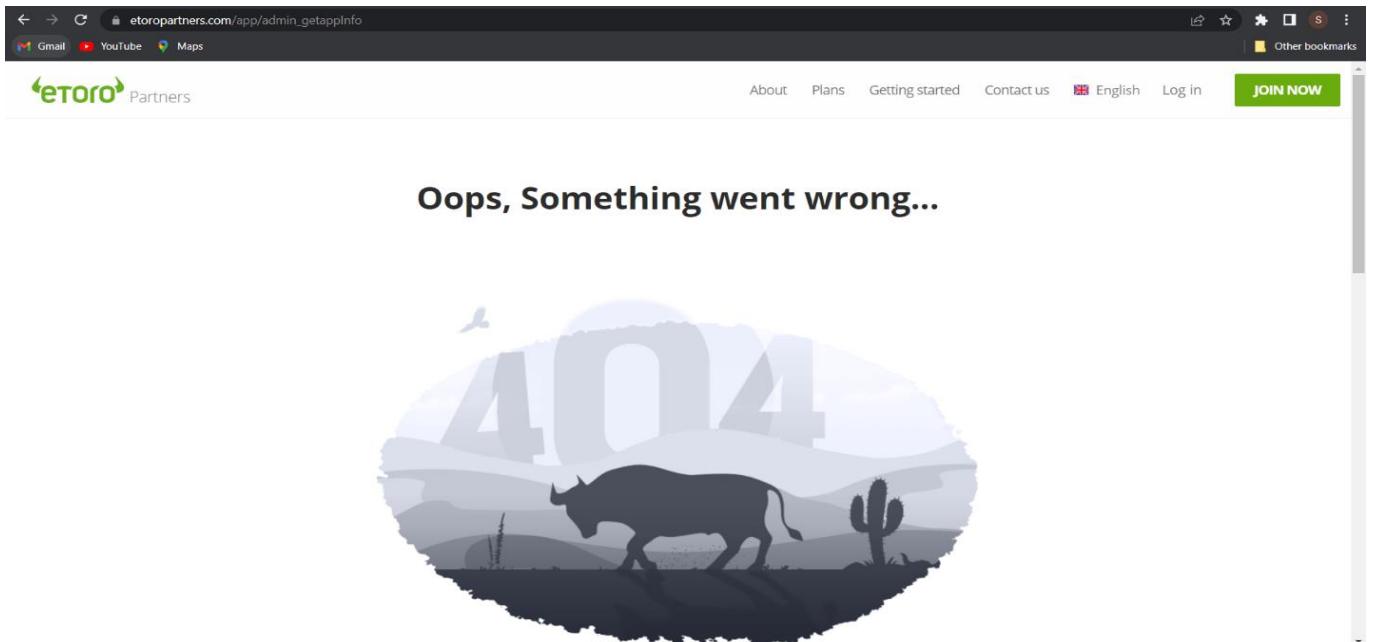
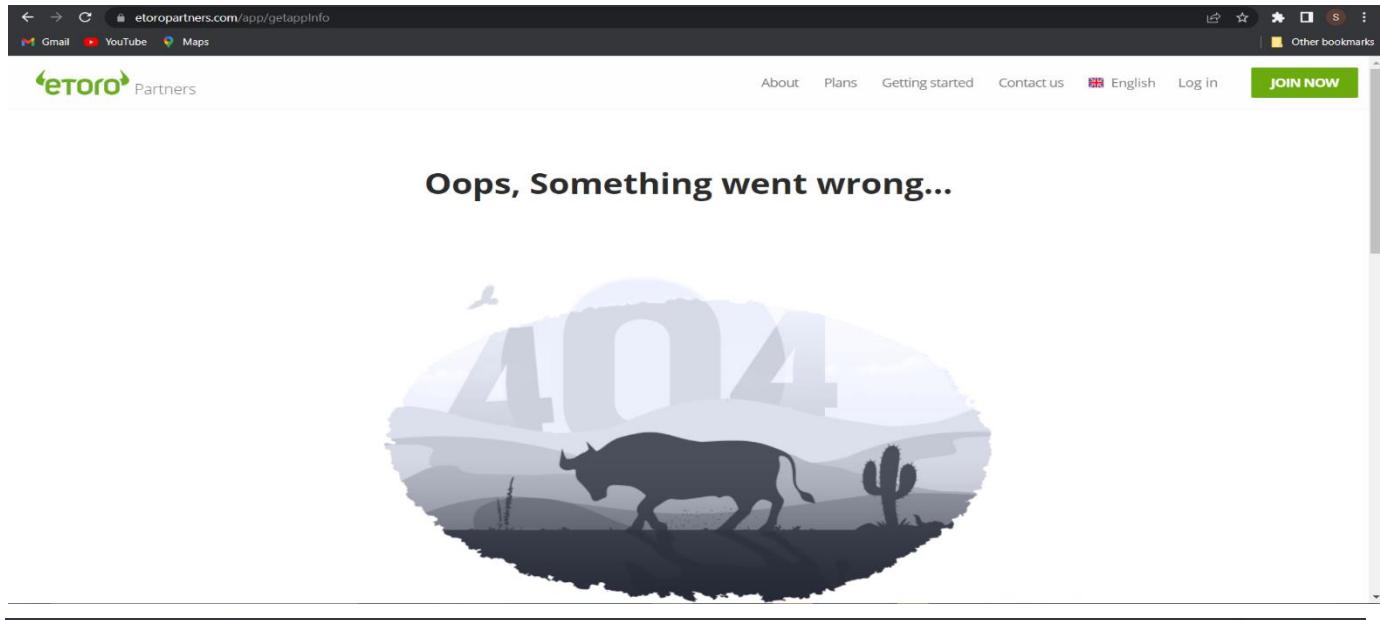
Also I used **app/admin_getappInfo** to admin access. But it also redirected to the home page.

The screenshot shows a web browser window for the eToro website at https://www.eto.com/home/app/admin_getappInfo. The left sidebar displays a user profile for 'SubashM' and navigation links like Home, Watchlist, Portfolio, Discover, More, eToro Club, Invite Friends, Withdraw Funds, and Deposit Funds. A 'Switch to Virtual' button is also present. The main content area features a 'Welcome to eToro!' banner with options to 'Verify Account' or 'Deposit Funds', and a 'verify' button. Above the banner, real-time market data is shown for NSDQ100 (12552.20, -2.63%), UK100 (7591.17, 0%), BTC (29365.30, +0.17%), EURUSD (1.07198, -0.23%), OIL (118.80, +2.29%), and SP500 (41, -1%). Below the banner is a 'News Feed' section with a placeholder 'What's on your mind?' and a 'Big Movers' section stating 'No big movement to display at the moment'. The top navigation bar includes a search bar, a bell icon, and various bookmark icons.

So that this domain is safe from broken access control vulnerability.

2.Target domain - <https://etoropartners.com/>

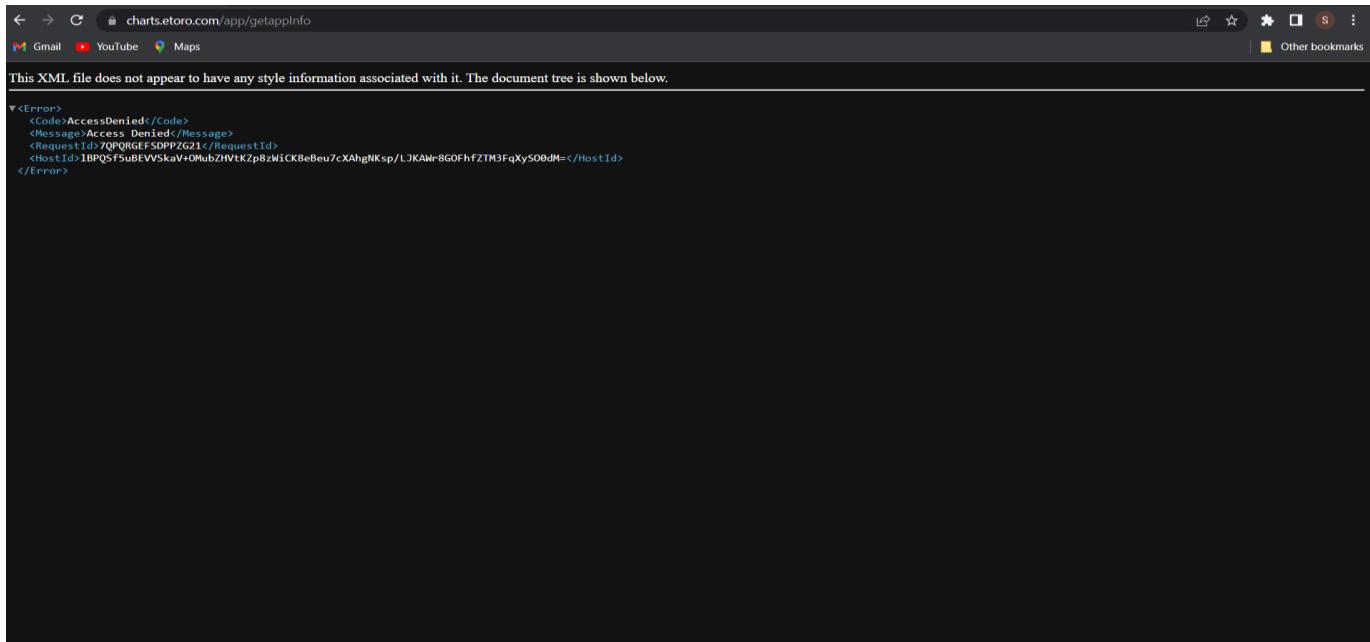
I tried broken access control by adding **/app/getappInfo** and **app/admin_getappInfo** to end of the url to get admins access. But it shown an error.



So that this domain is safe from broken access control vulnerability.

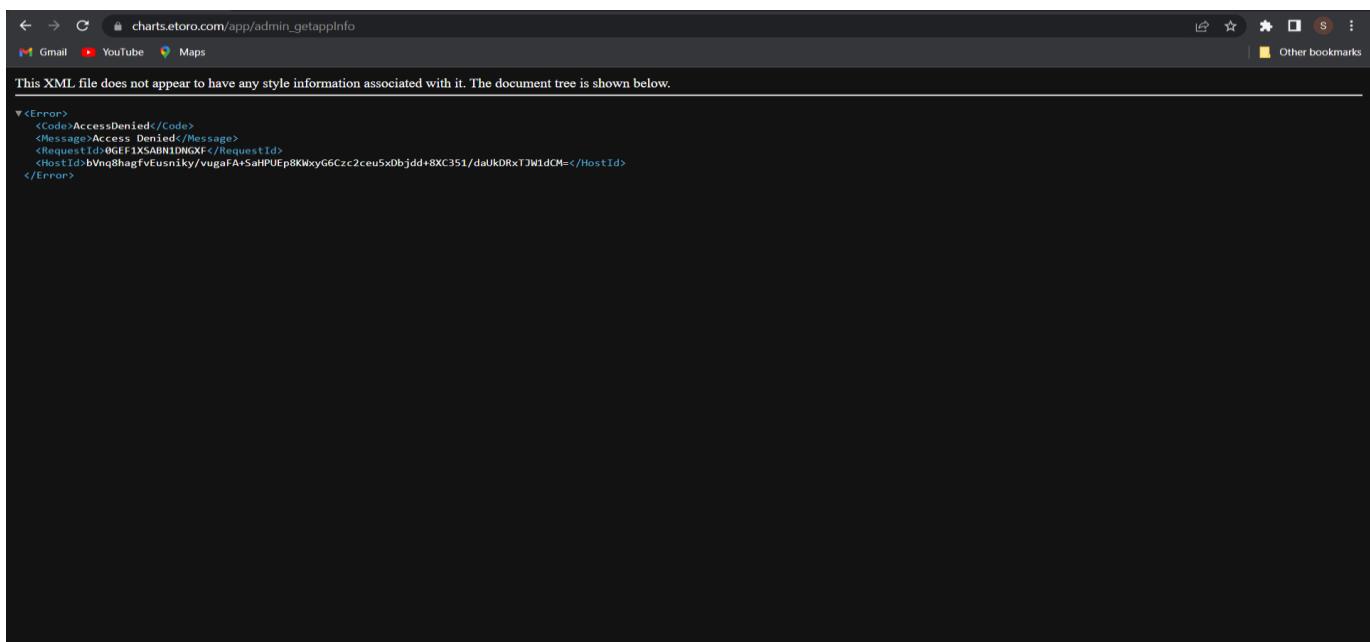
3.Target domain - <https://charts.etoro.com/>

I tried broken access control by adding **/app/getappInfo** and **app/admin_getappInfo** to end of the url. So as a result of this, it shown some XML code.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="utf-8"?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>7QPQIGEFSDPPZG21</RequestId>
  <HostId>IBPQSFS5uBEVVSkaV+OMubZHvtkZp8zWiCK8eBeu7cXAhgNKsp/LJKAWr8GOFhfZTM3FqXyS00dM=</HostId>
</Error>
```

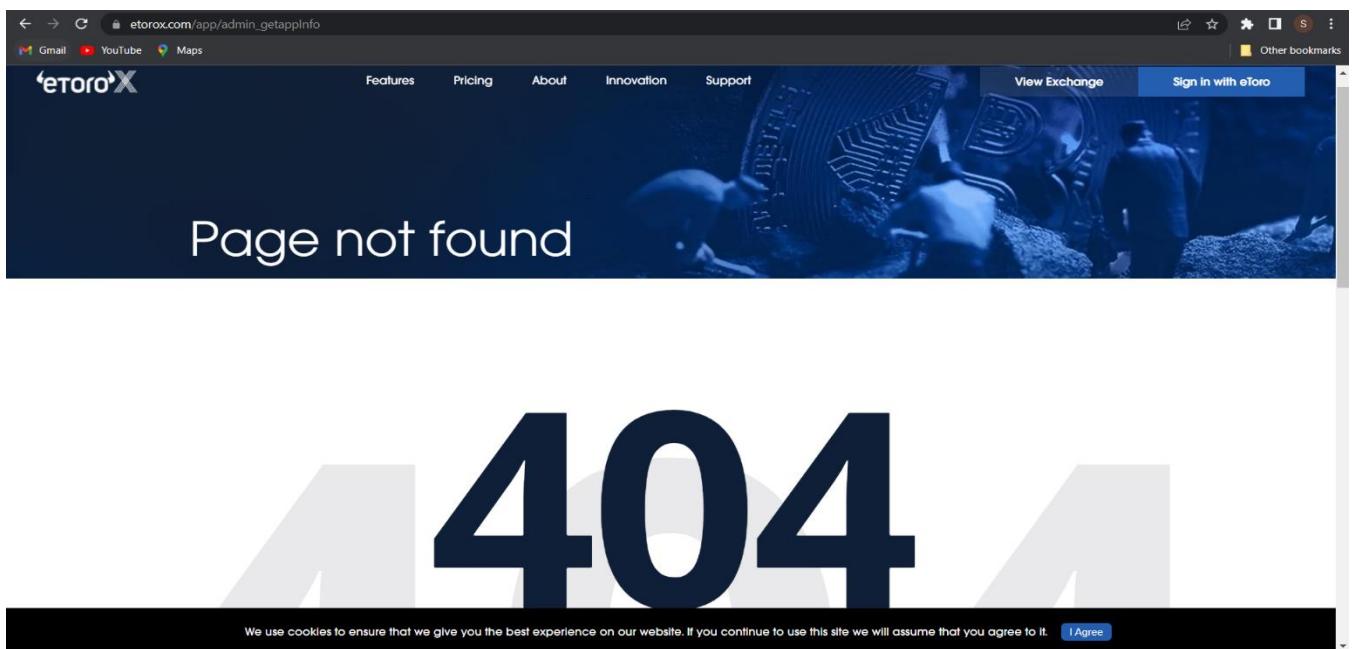
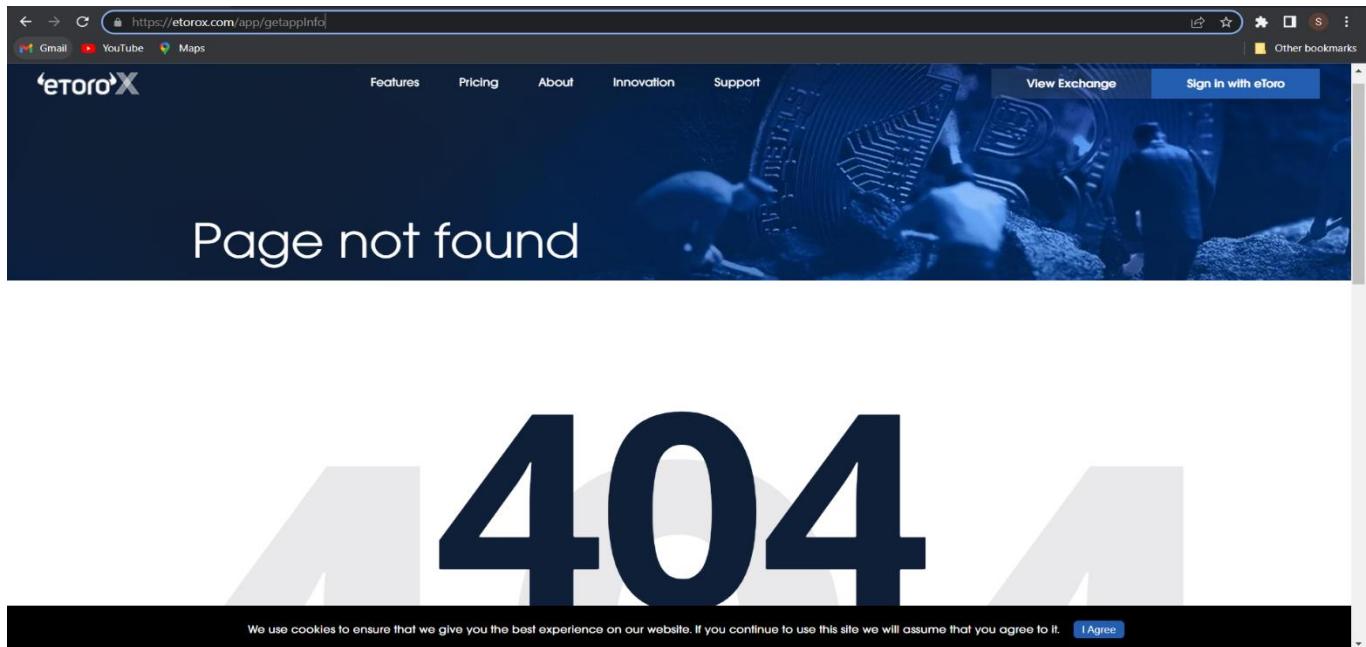


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="utf-8"?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>0GEF1XSABH1DNGXF</RequestId>
  <HostId>bVnq8hagfvEusniky/vugaFA+SaHPUEp8KwxyG6Czc2ceu5xDbjdd+8XC351/daUkDRxTJW1dCM=</HostId>
</Error>
```

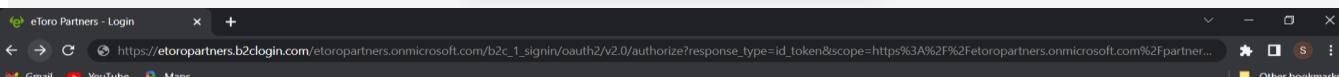
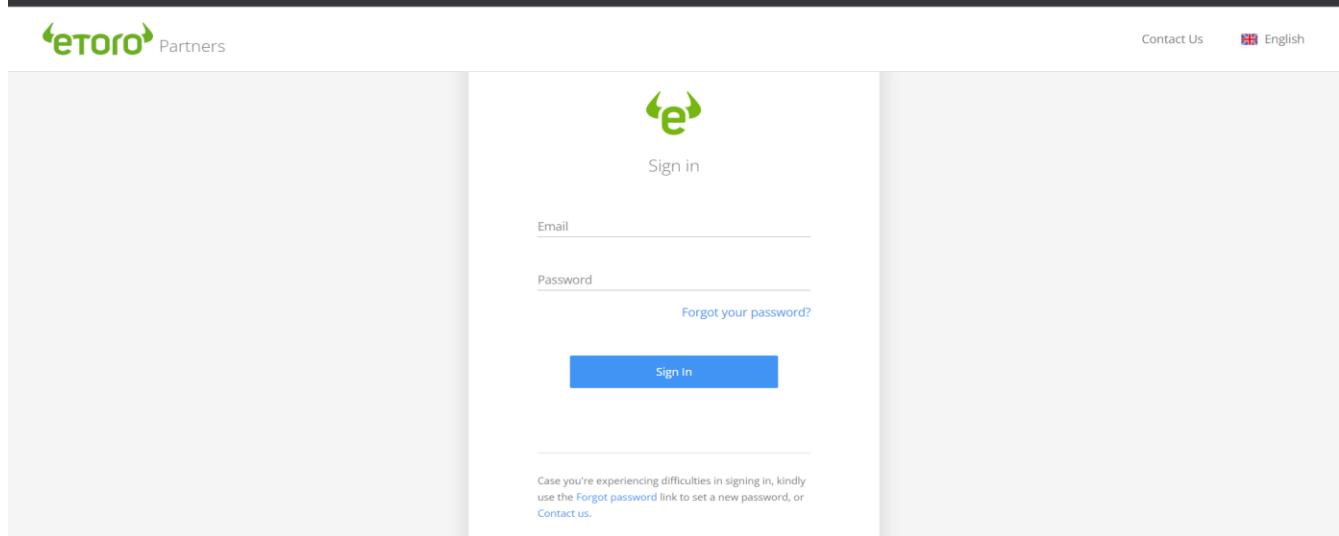
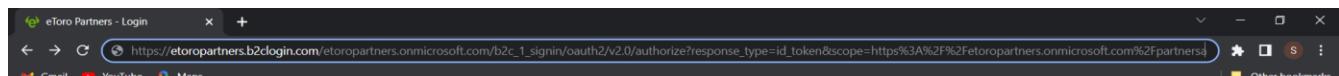
4.Target domain - <https://etorox.com/>

I tried broken access control by adding **/app/getappInfo** and **app/admin_getappInfo** to end of the url to get admins access. But it shown an error.



5.Target domain - <https://partners.etoro.com/>

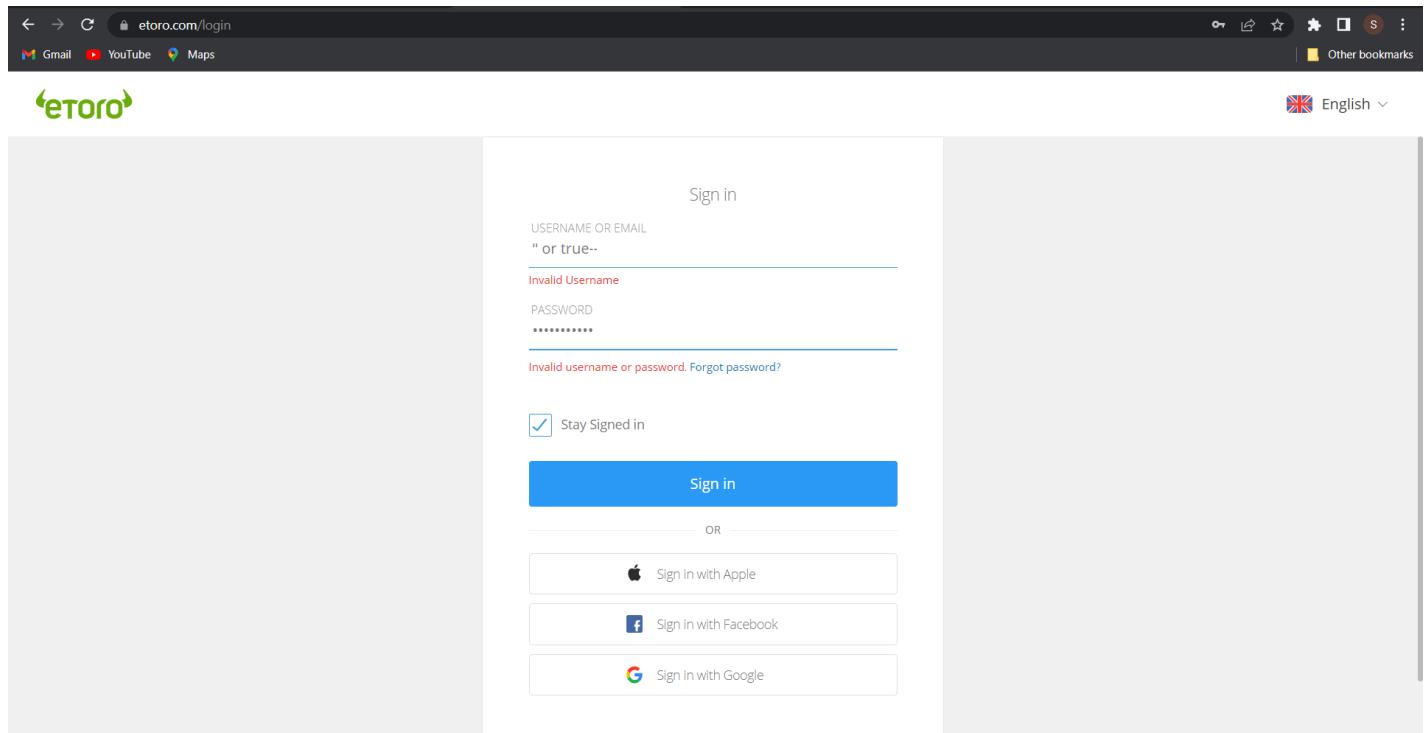
I tried broken access control by adding **/app/getappInfo** and **app/admin_getappInfo** to end of the url. But it redirected to the same page.

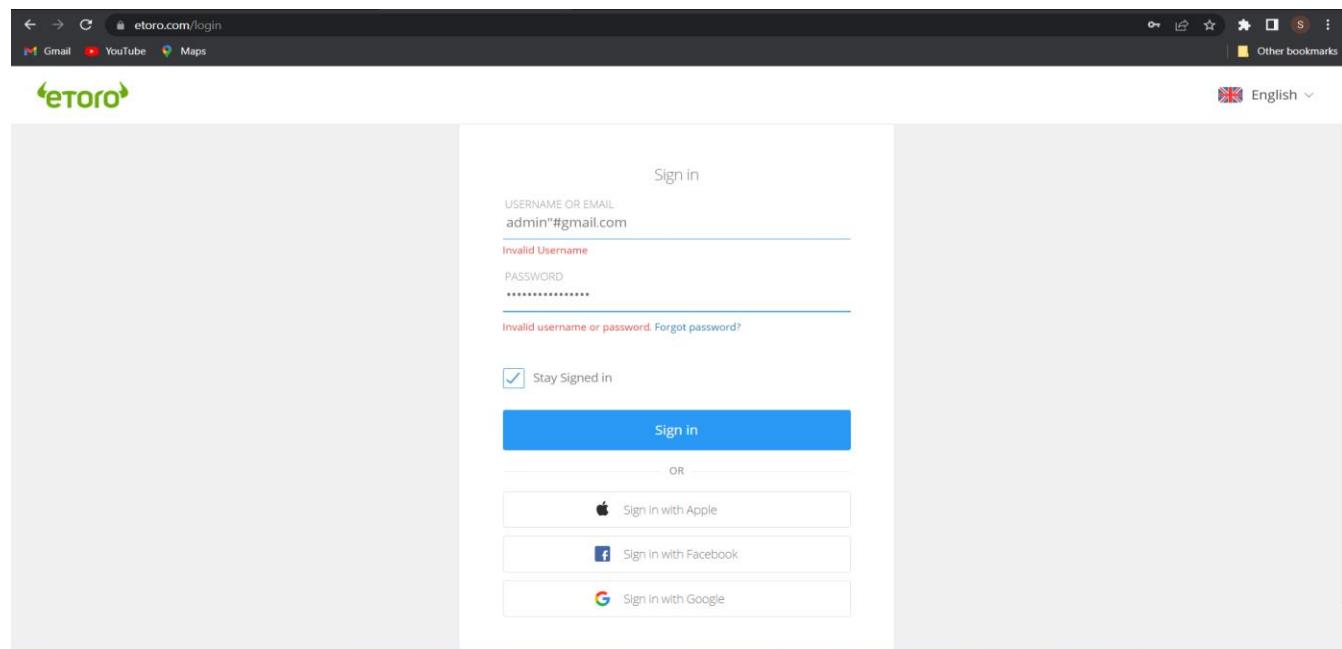
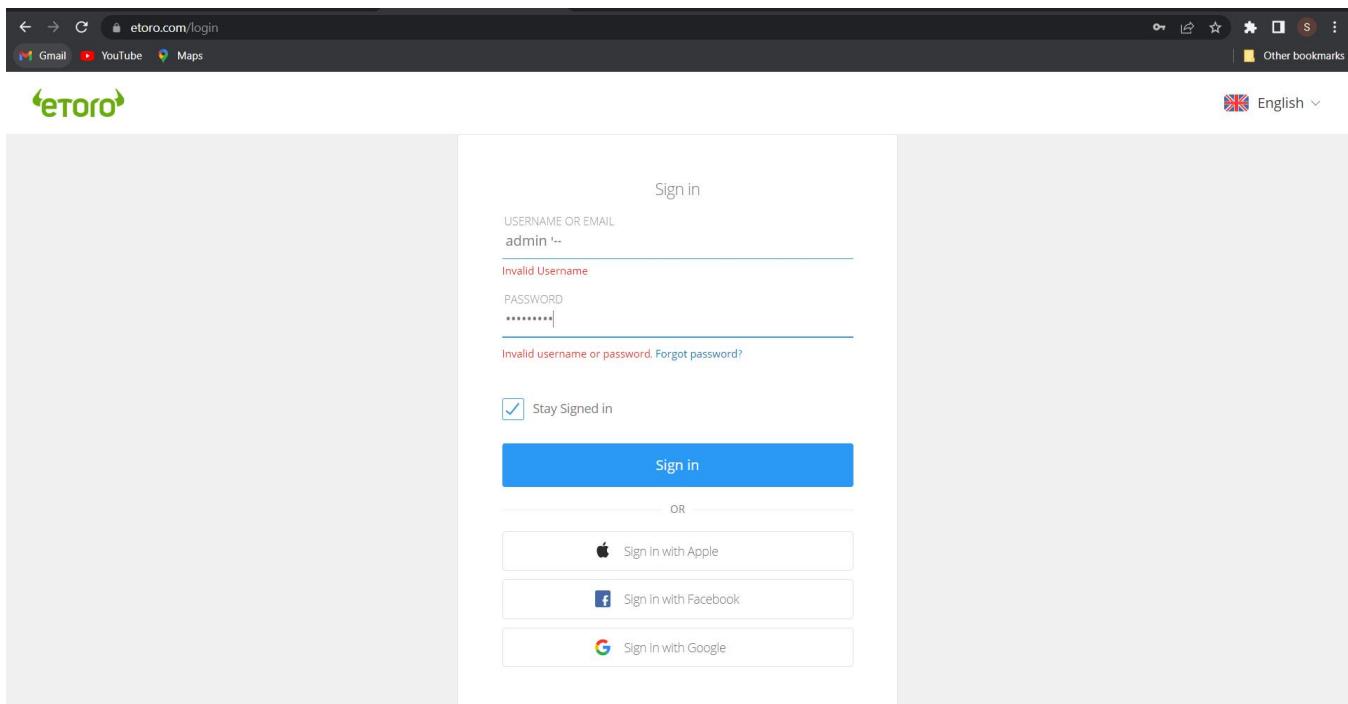


Testing SQL Injection

1.Target domain - <https://www.etoro.com/>

This domain has login page. So that I tried some SQL injection to this domain to identify whether there is a SQL injection vulnerability.





The site was detected the script even before I click on the sign in button. And also the site identify if the email address has unwanted characters. So that this domain is not vulnerable to SQL injection.

Conclusion

The report included a vulnerability assessment of the etoro.com web domain, as well as its five sub-domains. This was done in two phases: the information gathering phase, and the vulnerability assessment. Both phases were carried out in a standard manner, and the report was made available to the client's terms, subject to change. Both automated and manual tests were used to do this vulnerability assessment. This report describes the various techniques and tools used to gather information about a vulnerable system. It also describes the findings of the vulnerability assessment and the steps that are being taken to minimize these vulnerabilities. Although no critical vulnerabilities were discovered, medium and low level vulnerabilities were found on targeted domains.

References

- <https://owasp.org/www-project-top-ten/>
- <https://www.kali.org/tools/sublist3r/>
- <https://github.com/aboul3la/Sublist3r>
- <https://www.kali.org/tools/theharvester/>
- <https://github.com/laramies/theHarvester>
- <https://www.kali.org/tools/dnsenum/>
- <https://github.com/fwaeytens/dnsenum>
- <https://www.kali.org/tools/dnsrecon/>
- <https://github.com/darkoperator/dnsrecon>