A

Minor Project Report

On

Cyber Security

By

Koshika Arun

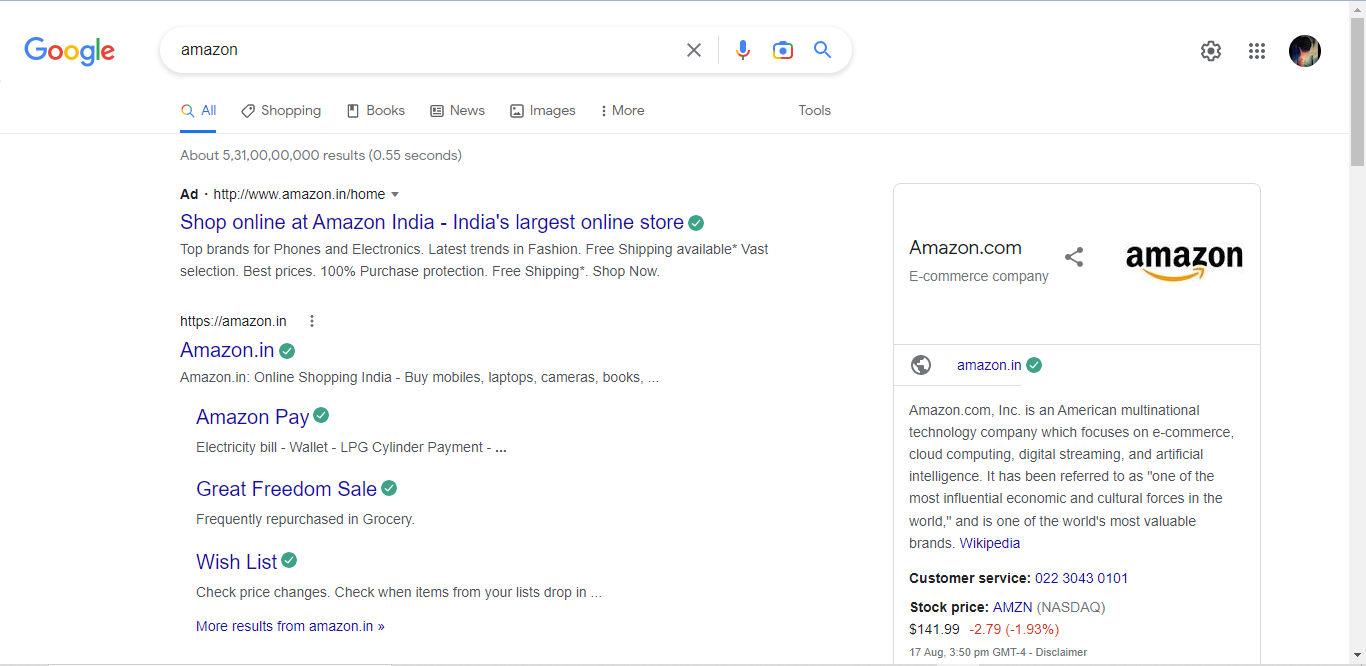
Under the guidance of

VERZEO

• Project Name: Cyber Security July Minor Project

Problem Statement:

**1.Perform Foot printing on Amazon Website and gather information about website by using online Websites (Whois / netcraft / Shodan / dnsdumpster., etc.) as much as possible and write report on gathered info along with screenshots**



**Dnsdumpster.com** 

Domain:amazon.com

Registrar:MarkMonitor Inc.

Registered On:1994-11-01

Expires On:2024-10-30

Updated On:2019-05-07

Status:clientDeleteProhibited

clientTransferProhibited

clientUpdateProhibited

serverDeleteProhibited

serverTransferProhibited

serverUpdateProhibited

Name Servers:ns1.p31.dynect.net

ns2.p31.dynect.net

ns3.p31.dynect.net

ns4.p31.dynect.net

pdns1.ultradns.net

pdns6.ultradns.co.uk

Registrant Contact

Name:Hostmaster, Amazon Legal Dept.

Organization:Amazon Technologies, Inc.

Street:P.O. Box 8102

City:Reno

State:NV

Postal Code:89507

Country:US

Phone:+1.2062664064

Fax:+1.2062667010

Email:email@amazon.com

Administrative Contact

Name:Hostmaster, Amazon Legal Dept.

Organization:Amazon Technologies, Inc.

Street:P.O. Box 8102

City:Reno

State:NV

Postal Code:89507

Country:US

Phone:+1.2062664064

Fax:+1.2062667010

Email:email@amazon.com

Technical Contact

Name:Hostmaster, Amazon Legal Dept.

Organization:Amazon Technologies, Inc.

Street:P.O. Box 8102

City:Reno

State:NV

Postal Code:89507

Country:US

Phone:+1.2062664064

Fax:+1.2062667010

Email:email@amazon.com

**Dnsdumpster.com**

DNS Servers

ns1.p31.dynect.net.

108.59.161.31

ns1.p31.dynect.net ORACLE-BMC-31898

United States

ns2.p31.dynect.net.

108.59.162.31

ns2.p31.dynect.net ORACLE-BMC-31898

United States

ns3.p31.dynect.net.

108.59.163.31

ns3.p31.dynect.net ORACLE-BMC-31898

United States

ns4.p31.dynect.net.

108.59.164.31

ns4.p31.dynect.net ORACLE-BMC-31898

United States

pdns1.ultradns.net.

204.74.108.1

pdns1.ultradns.net ULTRADNS

United States

pdns6.ultradns.co.uk.

204.74.115.1

pdns6.ultradns.co.uk ULTRADNS

United States

MX Records \*\* This is where email for the domain goes...

5 amazon-smtp.amazon.com.

207.171.188.208

smtp-fw-9107.amazon.com AMAZON-02

United States

TXT Records \*\* Find more hosts in Sender Policy Framework (SPF) configurations

amazon.com

HTTP: Server

HTTPS: Server 205.251.242.103

s3-console-us-standard.console.aws.amazon.com AMAZON-02

United States

207-171-168-10.amazon.com

207.171.168.10

207-171-168-10.amazon.com AMAZON-02

United States

halo-datapublish-prod.amazon.com

HTTP: Server

HTTPS: Server 52.46.145.134

AMAZON-02

United States

54-240-196-100.amazon.com

54.240.196.100

54-240-196-100.amazon.com AMAZON-02

United States

54-240-200-110.amazon.com

54.240.200.110

54-240-200-110.amazon.com AMAZON-02

Japan

208-216-183-200.amazon.com

208.216.183.200

UUNET

United States

ab-stage.amazon.com

209.54.182.86

AMAZON-02

United States

blueprints-eu.amazon.com

HTTP: Server

HTTPS: Server 52.95.114.120

AMAZON-02

Ireland

smtp-out-127-10.amazon.com

176.32.127.10

smtp-out-127-10.amazon.com AMAZON-02

Ireland

54-240-196-110.amazon.com

54.240.196.110

54-240-196-110.amazon.com AMAZON-02

United States

cscentral-eu.amazon.com

HTTP: Server

HTTPS: Server 178.236.7.175

cscentral-eu.amazon.com AMAZON-02

Ireland

54-240-200-210.amazon.com

54.240.200.210

54-240-200-210.amazon.com AMAZON-02

Japan

devicepairing.amazon.com

209.54.182.83

AMAZON-02

United States

54-240-200-20.amazon.com

54.240.200.20

54-240-200-20.amazon.com AMAZON-02

Japan

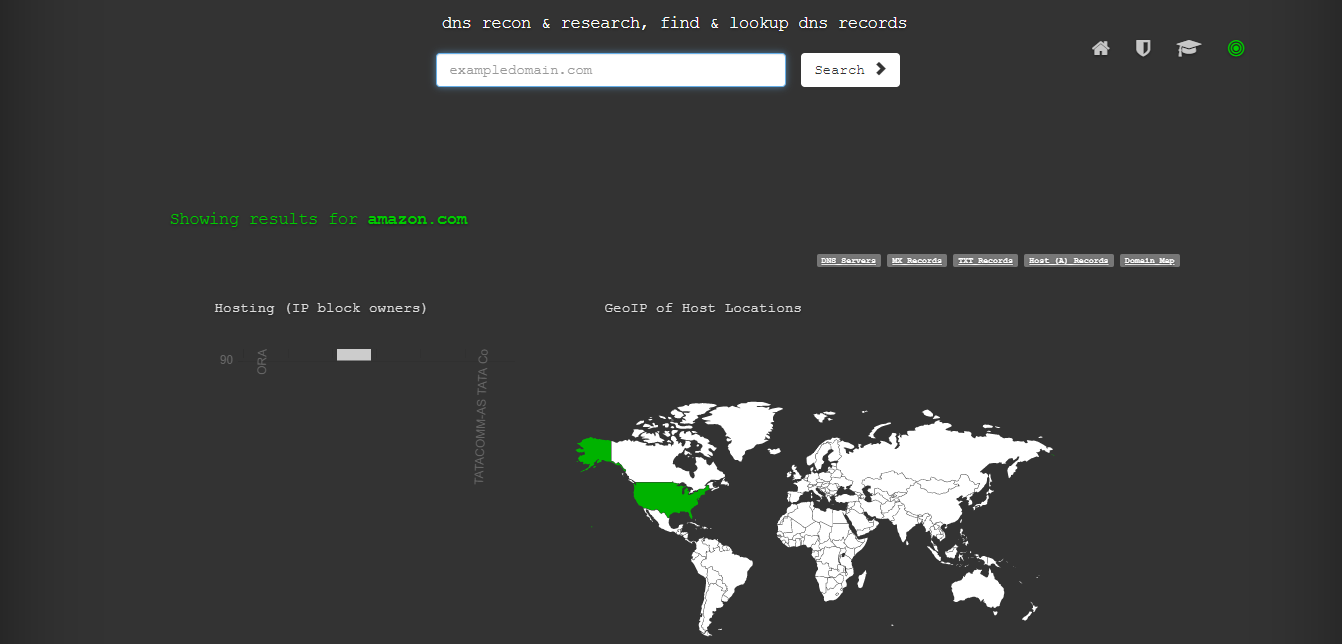
smtp-out-174-110.amazon.com

207.171.174.110

smtp-out-174-110.amazon.com AMAZON-02

United States

54-240-200-10.amazon.com



54.240.200.10

54-240-200-10.amazon.com AMAZON-02

Japan

gru-orca-bak.amazon.com

177.72.243.194

gru-a-orca.amazon.com AMAZON-02

Brazil

208-216-183-20.amazon.com

208.216.183.20

UUNET

United States

sars-eu.amazon.com

HTTP: Server

HTTPS: Server 52.94.217.52

AMAZON-02

Ireland

207-171-168-100.amazon.com

207.171.168.100

207-171-168-100.amazon.com AMAZON-02

United States

kindle-digital-delivery.amazon.com

HTTP: CloudFront

HTTPS: CloudFront 204.246.190.35

server-204-246-190-35.iad50.r.cloudfront.net AMAZON-02

United States

54-240-197-200.amazon.com

54.240.197.200

54-240-197-200.amazon.com AMAZON-02

United States

pdx-orca.amazon.com

54.214.105.19

ec2-54-214-105-19.us-west-2.compute.amazonaws.com AMAZON-02

United States

midway-gateway-1-eu-west-1.aea.amazon.com

HTTP: awselb/2.0

HTTPS: Apache/2.4.51 (Amazon)

HTTPS TECH: AWS ELB 99.80.82.165

ec2-99-80-82-165.eu-west-1.compute.amazonaws.com AMAZON-02

Ireland

207-171-180-10.amazon.com

207.171.180.10

207-171-180-10.amazon.com AMAZON-02

United States

data-eu.amazon.com

HTTP: Server

HTTPS: Server 54.239.33.59

AMAZON-02

Ireland

207-171-181-10.amazon.com

207.171.181.10

207-171-181-10.amazon.com AMAZON-02

United States

isengard-service-infra.amazon.com

HTTP: Server

HTTPS: Server 72.21.206.31

206-31.amazon.com AMAZON-02

United States

eu-central-2.beta.acm-certificates.amazon.com

54.93.144.207

ec2-54-93-144-207.eu-central-1.compute.amazonaws.com AMAZON-02

Germany

aiv-subs.amazon.com

HTTPS: Server 54.239.25.11

AMAZON-02

United States

adtw-eu.amazon.com

HTTP: Server

HTTPS: Server 52.95.122.249

AMAZON-02

Ireland

dilithium-eu.amazon.com

54.239.35.83

AMAZON-02

Ireland

midway-gateway-2-us-east-1.aea.amazon.com

HTTP: Microsoft-IIS/10.0

HTTPS: Microsoft-IIS/10.0

HTTP TECH: IIS,10.0

ASP.NET

HTTPS TECH: IIS,10.0 34.199.249.242

ec2-34-199-249-242.compute-1.amazonaws.com AMAZON-AES

United States

authorcentral.amazon.com

HTTP: Server

HTTPS: Server 176.32.96.12

AMAZON-02

United States

https-sedi-devo.amazon.com

176.32.101.101

AMAZON-02

United States

207-171-187-10.amazon.com

207.171.187.10

207-171-187-10.amazon.com AMAZON-02

United States

208-216-183-100.amazon.com

208.216.183.100

UUNET

United States

andes-service-frontend-gamma.amazon.com

HTTPS: Server 52.94.235.72

AMAZON-02

United States

midway-gateway-2-1.us-east-1.aea.amazon.com

3.226.92.110

ec2-3-226-92-110.compute-1.amazonaws.com AMAZON-AES

United States

207-171-182-210.amazon.com

207.171.182.210

207-171-182-210.amazon.com AMAZON-02

United States

54-240-197-110.amazon.com

54.240.197.110

54-240-197-110.amazon.com AMAZON-02

United States

smtp-out-205-210.amazon.com

72.21.205.210

smtp-out-205-210.amazon.com AMAZON-02

United States

advantage.amazon.com

HTTP: Server

HTTPS: Server 176.32.100.111

AMAZON-02

United States

207-171-182-10.amazon.com

207.171.182.10

207-171-182-10.amazon.com AMAZON-02

United States

208-216-183-210.amazon.com

208.216.183.210

UUNET

United States

207-171-181-110.amazon.com

207.171.181.110

207-171-181-110.amazon.com AMAZON-02

United States

nrt-orca-bak.amazon.com

99.78.208.170

AMAZON-02

Japan

readynow-agg-preprod-fe.amazon.com

HTTPS: Server 54.240.255.122

AMAZON-02

United States

smtp-out-173-200.amazon.com

207.171.173.200

smtp-out-173-200.amazon.com AMAZON-02

United States

adbot.amazon.com

52.46.145.87

AMAZON-02

United States

antaresmapper.amazon.com

52.46.145.215

AMAZON-02

United States

data-na.amazon.com

HTTP: Server

HTTPS: Server 52.46.135.252

AMAZON-02

United States

54-240-196-200.amazon.com

54.240.196.200

54-240-196-200.amazon.com AMAZON-02

United States

smtp-out-127-100.amazon.com

176.32.127.100

smtp-out-127-100.amazon.com AMAZON-02

Ireland

hyd-orca-bak.amazon.com

203.199.181.102

illhyd-203.199.181.102.static.vsnl.net.in TATACOMM-AS TATA Communications formerly VSNL is Leading ISP

India

207-171-168-210.amazon.com

207.171.168.210

207-171-168-210.amazon.com AMAZON-02

United States

sfo-orca-bak.amazon.com

54.214.105.19

ec2-54-214-105-19.us-west-2.compute.amazonaws.com AMAZON-02

United States

paystation-api.amazon.com

Netcraft.org

HTTP: CloudFront 18.67.76.5

server-18-67-76-5.iad89.r.cloudfront.net AMAZON-02

United States

smtp-out-174-100.amazon.com

207.171.174.100

smtp-out-174-100.amazon.com AMAZON-02

United States

207-171-182-200.amazon.com

207.171.182.200

207-171-182-200.amazon.com AMAZON-02

United States

207-171-187-110.amazon.com

207.171.187.110

207-171-187-110.amazon.com AMAZON-02

United States

208-216-183-10.amazon.com

208.216.183.10

UUNET

United States

207-171-187-210.amazon.com

207.171.187.210

207-171-187-210.amazon.com AMAZON-02

United States

ns-700.amazon.com

207.171.178.13

AMAZON-02

United States

207-171-180-100.amazon.com

207.171.180.100

207-171-180-100.amazon.com AMAZON-02

United States

207-171-180-210.amazon.com

207.171.180.210

207-171-180-210.amazon.com AMAZON-02

United States

syd-orca-bak.amazon.com

54.240.205.90

AMAZON-02

Australia

av-na.amazon.com

HTTPS: Server 52.119.196.88

AMAZON-02

United States

midway-gateway-2-4.us-east-1.aea.amazon.com

HTTPS: awselb/2.0 184.73.213.248

ec2-184-73-213-248.compute-1.amazonaws.com AMAZON-AES

United States

207-171-183-100.amazon.com

207.171.183.100

207-171-183-100.amazon.com AMAZON-02

United States

207-171-181-100.amazon.com

207.171.181.100

207-171-181-100.amazon.com AMAZON-02

United States

midway-gateway-4-us-east-1.aea.amazon.com

18.233.203.3

ec2-18-233-203-3.compute-1.amazonaws.com AMAZON-AES

United States

kindle-digital-delivery-preprod.amazon.com

HTTP: CloudFront 18.67.78.14

server-18-67-78-14.iad89.r.cloudfront.net AMAZON-02

United States

207-171-183-10.amazon.com

207.171.183.10

207-171-183-10.amazon.com AMAZON-02

United States

gamma-prime-apis.amazon.com

100.24.76.21

ec2-100-24-76-21.compute-1.amazonaws.com AMAZON-AES

United States

207-171-187-200.amazon.com

207.171.187.200

207-171-187-200.amazon.com AMAZON-02

United States

207-171-183-210.amazon.com

207.171.183.210

207-171-183-210.amazon.com AMAZON-02

United States

154-100.amazon.com

204.177.154.100

UUNET

United States

iad-orca-bak.amazon.com

52.94.254.26

iad-e-orca.amazon.com AMAZON-02

United States

a4k-fe-master.amazon.com

HTTP: Server

HTTPS: Server 52.119.167.100

AMAZON-02

United States

207-171-181-210.amazon.com

207.171.181.210

207-171-181-210.amazon.com AMAZON-02

United States

adtw-na.amazon.com

HTTP: Server

HTTPS: Server 52.46.159.140

AMAZON-02

United States

smtp-out-127-110.amazon.com

176.32.127.110

smtp-out-127-110.amazon.com AMAZON-02

Ireland

207-171-183-200.amazon.com

207.171.183.200

207-171-183-200.amazon.com AMAZON-02

United States

aws-trustedadvisor-dmarc.amazon.com

HTTP: CloudFront 18.67.76.103

server-18-67-76-103.iad89.r.cloudfront.net AMAZON-02

United States

smtp-out-105-200.amazon.com

176.32.105.200

smtp-out-105-200.amazon.com AMAZON-02

Ireland

207-171-180-200.amazon.com

207.171.180.200

207-171-180-200.amazon.com AMAZON-02

United States

54-240-200-100.amazon.com

54.240.200.100

54-240-200-100.amazon.com AMAZON-02

Japan

smtp-out-174-20.amazon.com

207.171.174.20

smtp-out-174-20.amazon.com AMAZON-02

United States

154-210.amazon.com

204.177.154.210

UUNET

United States

gc-na.amazon.com

HTTPS: Server 52.94.235.203

AMAZON-02

United States

cortana-gateway.amazon.com

HTTP: Server

HTTPS: Server 52.46.132.93

AMAZON-02

United States

ags-forum-service.amazon.com

HTTPS: Server 52.46.147.238

AMAZON-02

United States

54-240-197-10.amazon.com

54.240.197.10

54-240-197-10.amazon.com AMAZON-02

United States

54-240-198-210.amazon.com

54.240.198.210

54-240-198-210.amazon.com AMAZON-02

United States

207-171-180-110.amazon.com

207.171.180.110

207-171-180-110.amazon.com AMAZON-02

United States

54-240-200-200.amazon.com

54.240.200.200

54-240-200-200.amazon.com AMAZON-02

Japan

207-171-182-100.amazon.com

207.171.182.100

207-171-182-100.amazon.com AMAZON-02

United States

alexa-domino-eu-prod.amazon.com

52.95.117.162

AMAZON-02

Ireland

dp-rsm-preprod.amazon.com

52.46.150.219

AMAZON-02

United States

**Netcraft.org**

Hosting History

Netblock owner IP address OS Web server Last seen

Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244 99.86.125.142 unknown Server 11-Aug-2022

Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244 13.224.234.121 unknown Server 26-Jul-2022

Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142 104.96.174.101 Linux Server 19-Jul-2022

Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244 99.86.125.142 unknown Server 5-Jul-2022

Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142 104.96.174.101 Linux Server 27-Jun-2022

Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244 99.86.125.142 unknown Server 20-Jun-2022

162.219.225.118 unknown Server 12-Jun-2022

Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244 99.86.125.142 unknown Server 5-Jun-2022

Akamai 88.221.17.57 Linux Server 29-May-2022

162.219.225.118 unknown Server 22-May-2022

SSL/TLS

Assurance Domain validation

Common name www.amazon.com

Organisation Not Present

State Not Present

Country Not Present

Organisational unit Not Present

Subject Alternative Name

Validity period From Oct 12 2021 to Oct 11 2022 (11 months, 4 weeks, 2 days)

Matches hostname Yes

Server Server

Public key algorithm rsaEncryption

Protocol version TLSv1.2

Public key length 2048

Certificate check ok

Signature algorithm sha256WithRSAEncryption

Serial number 0x0e09744170c59dcbe4d1df762486554f

Cipher ECDHE-RSA-AES128-GCM-SHA256

Version number 0x02

Perfect Forward Secrecy Yes

Supported TLS Extensions RFC5746 renegotiation info, RFC4366 server name, RFC4492 EC point formats, RFC5077 session ticket, RFC4366 status request, RFC7301 application-layer protocol negotiation

Application-Layer Protocol Negotiation h2S

Next Protocol Negotiation Not Present

Issuing organisation DigiCert Inc

Issuer common name DigiCert Global CA G2

Issuer unit Not Present

Issuer location Not Present

Issuer country US

Issuer state Not Present

Certificate Revocation Lists http://crl3.digicert.com/DigiCertGlobalCAG2.crl

http://crl4.digicert.com/DigiCertGlobalCAG2.crl

Certificate Hash xU5HXu5WRLQelzqytdQAqNzAepg

Public Key Hash 2532ad1187dce6d7a1db42d8bcdb97701927f136646aa4f3a711ea604d9c3a48

OCSP servers http://ocsp.digicert.com - 100% uptime in the past S24 hours

Performance Graph

OCSP stapling response Certificate valid

OCSP data generated Aug 17 02:33:01 2022 GMT

OCSP data expires Aug 24 01:48:01 2022 GMT

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source Log Timestamp Signature Verification

Certificate Google Argon 2022

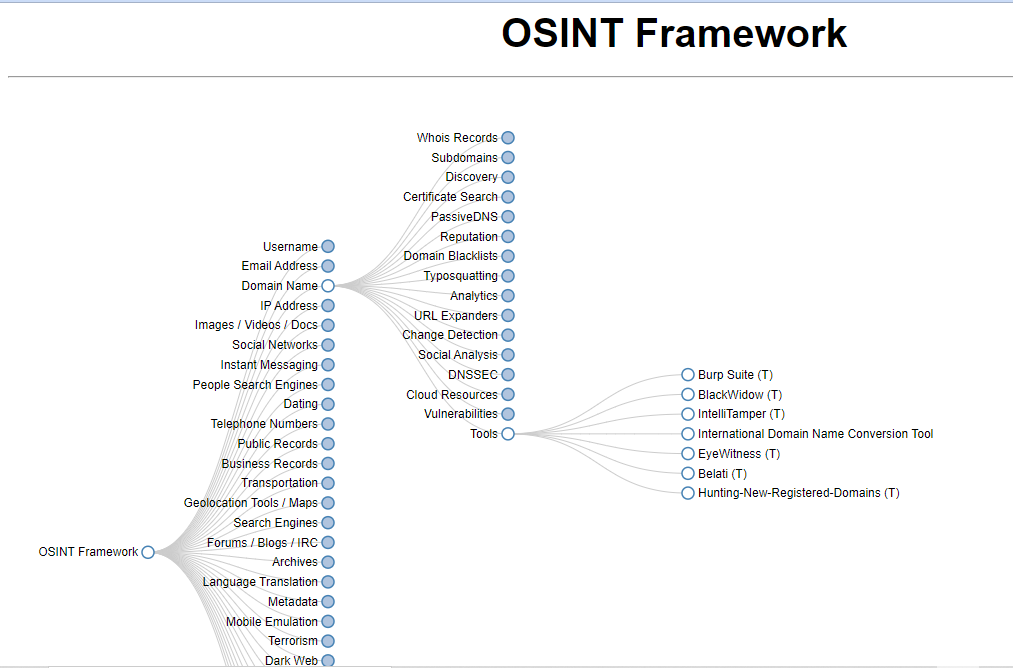
KXm+8J45OSHwVnOfY6V35b5XfZxgCvj5TV0mXCVdx4Q= 2021-10-12 23:43:07 Success

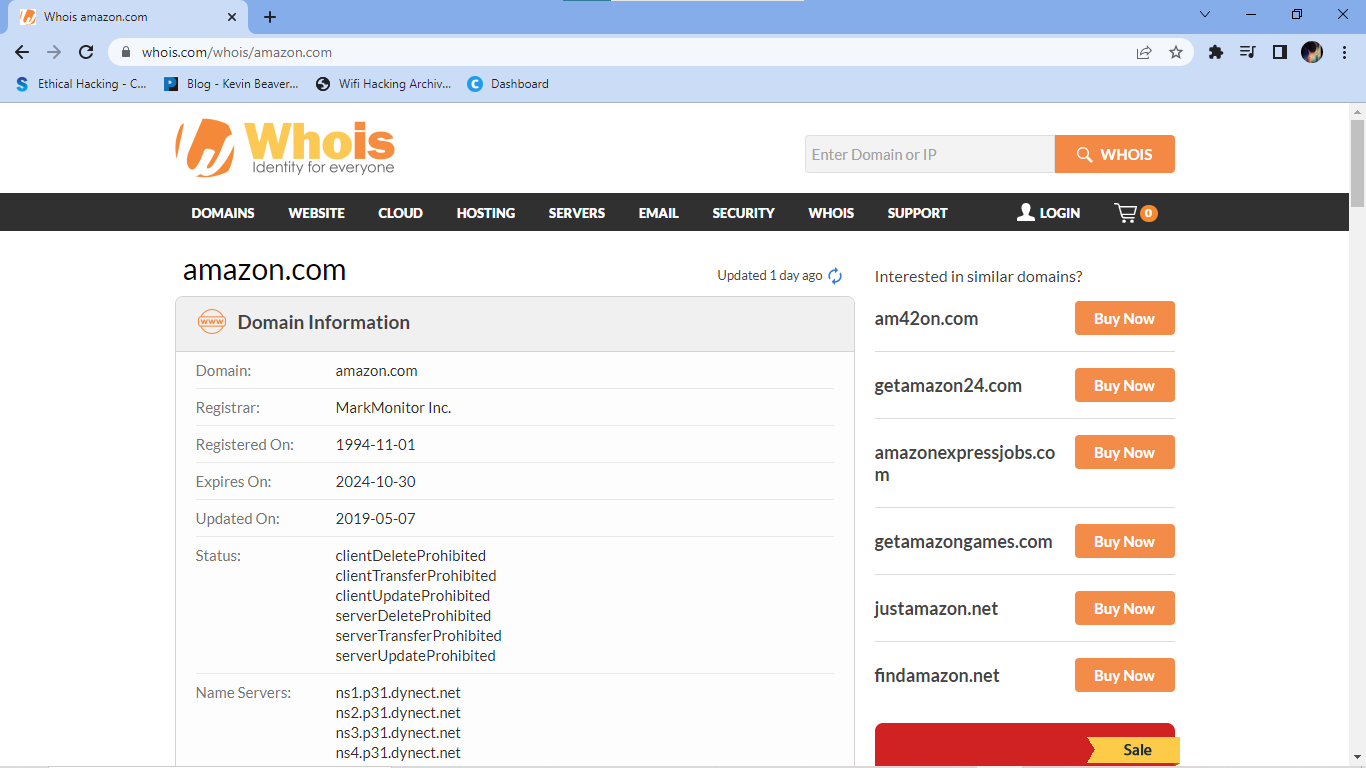
Certificate DigiCert Nessie 2022

UaOw9f0BeZxWbbg3eI8MpHrMGyfL956IQpoN/tSLBeU= 2021-10-12 23:43:07 Success

Certificate Cloudflare Nimbus 2022

QcjKsd8iRkoQxqE6CUKHXk4xixsD6+tLx2jwkGKWBvY= 2021-10-12 23:43:07 Success





Domain Whois record

Queried whois.iana.org with "Amazon"...

domain: AMAZON

organisation: Amazon Registry Services, Inc.

address: 410 Terry Avenue North, Seattle, WA 98109

address: United States

contact: administrative

name: Program Manager, Registry

organisation: Amazon Registry Services, Inc

address: 410 Terry Avenue North, Seattle, WA 98109

address: United States

phone: +1 206 646 5990

fax-no: +1-206-946-7702

e-mail: dotamazon-rzm@amazon.com

contact: technical

name: TLD Registry Services Technical

organisation: Nominet

address: Minerva House,

address: Edmund Halley Road,

address: Oxford Science Park,

address: Oxford

address: OX4 4DQ

address: United Kingdom

phone: +44.1865332211

e-mail: registrytechnical@nominet.uk

nserver: DNS1.NIC.AMAZON 213.248.218.90 2a01:618:402:0:0:0:0:90

nserver: DNS2.NIC.AMAZON 103.49.82.90 2401:fd80:402:0:0:0:0:90

nserver: DNS3.NIC.AMAZON 213.248.222.90 2a01:618:406:0:0:0:0:90

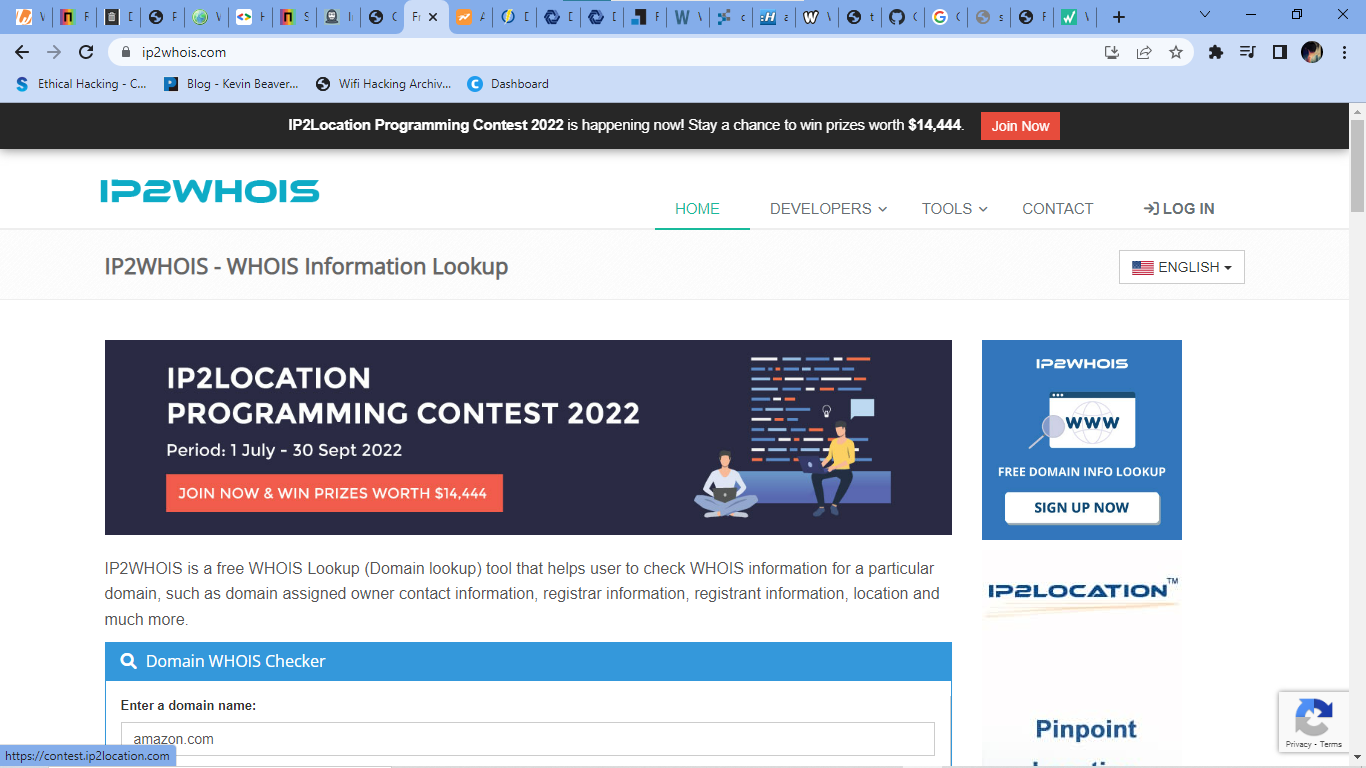
nserver: DNS4.NIC.AMAZON 2401:fd80:406:0:0:0:0:90 43.230.50.90

nserver: DNSA.NIC.AMAZON 156.154.100.3 2001:502:ad09:0:0:0:0:3

nserver: DNSB.NIC.AMAZON 156.154.101.3 2001:502:2eda:0:0:0:0:3

nserver: DNSC.NIC.AMAZON 156.154.102.3 2610:a1:1009:0:0:0:0:3

nserver: DNSD.NIC.AMAZON 156.154.103.3 2610:a1:1010:0:0:0:0:3



ds-rdata: 14854 8 2 4F9F1805F5689BF4AF48F0FA04BEF8727B83EAC65A669E8BF1A5EAFA83350D39

whois: whois.nic.amazon

status: ACTIVE

remarks: Registration information:

remarks: https://www.amazonregistry.com/

created: 2020-05-28

changed: 2021-11-18

source: IANA

Network Whois record

Don't have an IP address for which to get a record

DNS records

name class type data time to live

amazon IN NS dns3.nic.amazon 14258s (03:57:38)

amazon IN NS dns4.nic.amazon 14258s (03:57:38)

amazon IN NS dnsa.nic.amazon 14258s (03:57:38)

amazon IN NS dnsb.nic.amazon 14258s (03:57:38)

amazon IN NS dnsc.nic.amazon 14258s (03:57:38)

amazon IN NS dnsd.nic.amazon 14258s (03:57:38)

amazon IN NS dns1.nic.amazon 14258s (03:57:38)

amazon IN NS dns2.nic.amazon 14258s (03:57:38)

amazon IN RRSIG

type covered: NS (2)

algorithm: RSA/SHA-256 (8)

labels: 1

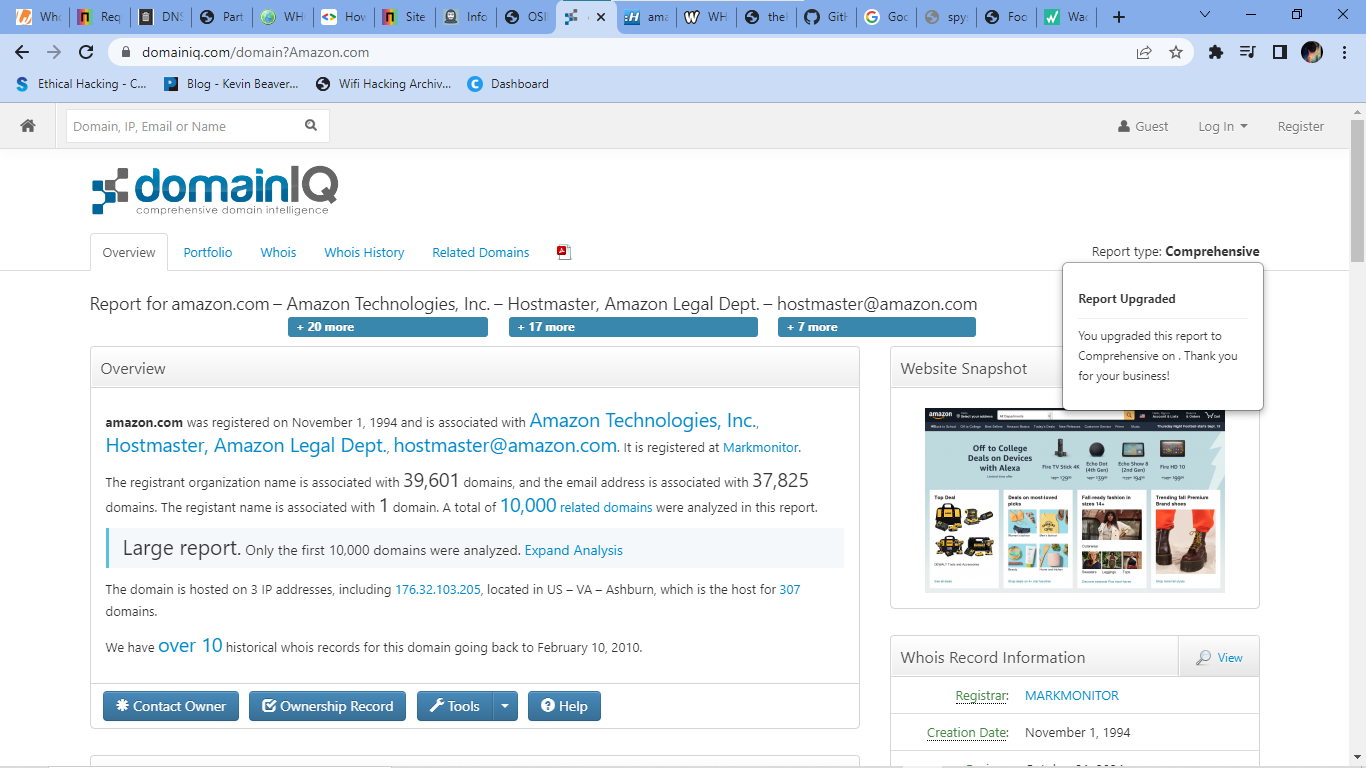
original ttl: 172800 (2.00:00:00)

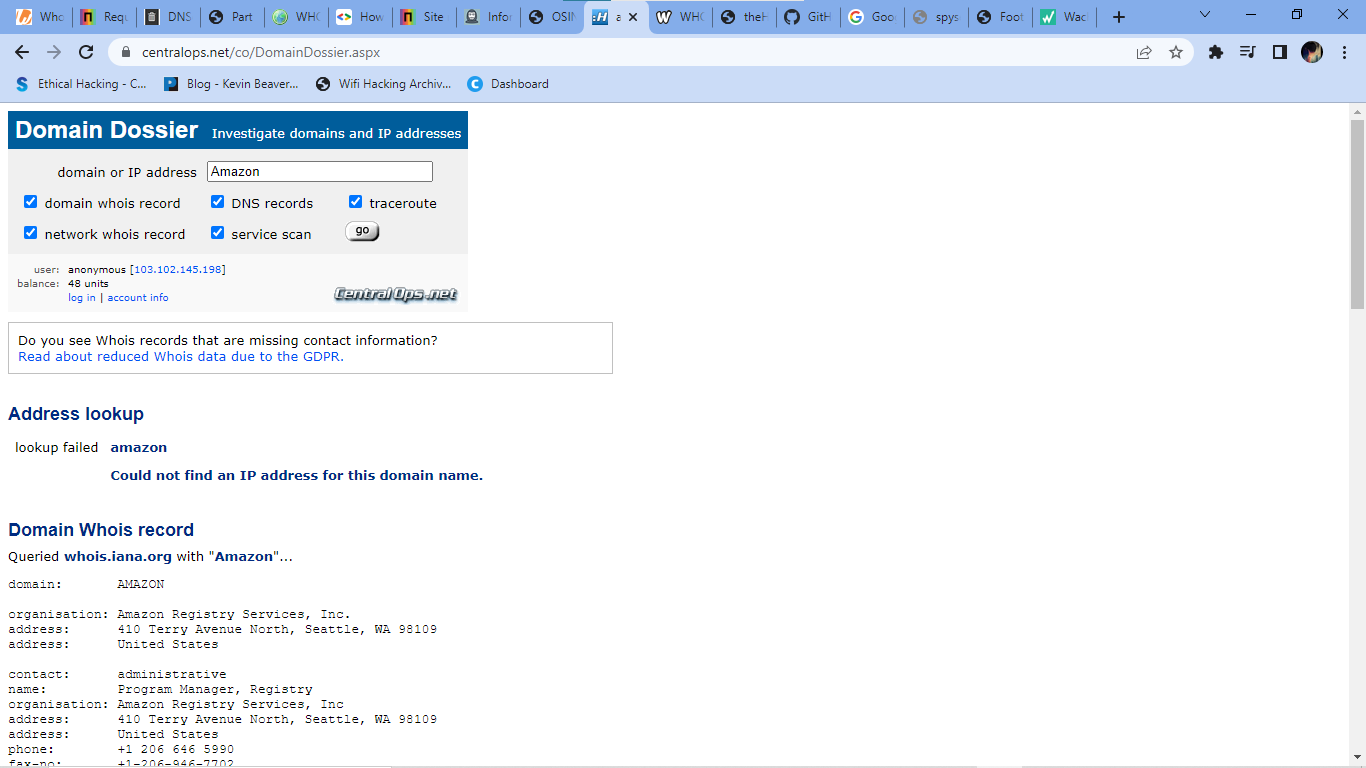
signature expiration: 2022-09-18 12:10:31Z

signature inception: 2022-08-14 11:32:05Z

key tag: 44890

signer's name: amazon

**domainIQ.org** 



Domains on IPDomains on Nameserver

183,566 total.Purchase ListReport

rolex.abudhabi

tudor.abudhabi

tudorwatch.abudhabi

cannabismd.academy

captureone.academy

eclinicalworks.academy

ifs.academy

ifsworld.academy

pega.academy

reusser.academy

startmail.academy

visible.academy

rolex.accountant

tudor.accountant

tudorwatch.accountant

tweet.actor

attends.adult

groupon.adult

hart.adult

houzz.adult

jobamatic.adult

kathyireland.adult

lookout.adult

myheritage.adult

pfizer.adult

rolex.adult

soul.adult

soul-cycle.adult

soulcycle.adult

staples.adult

stumble.adult

stumbleupon.adult

tudor.adult

tudorwatch.adult

tweet.adult

viagra.adult

avinode.aero

breitling.aero

divrt.aero

idg.aero

307 total.Purchase ListExploreWhois

alerts301.info

alerts354.info

list99-rocketmail.com

alerts362.info

subgroup157-mail.com

group140-loans.com

group145-loans.com

subgroup101-mail.com

alerts330.info

alerts391.info

alerts366.info

alerts372.info

subgroup143-mail.com

subgroup185-mail.com

subgroup142-mail.com

group109-loans.com

group132-loans.com

alerts371.info

alerts351.info

group134-loans.com

subgroup163-mail.com

alerts365.info

alerts353.info

subgroup187-mail.com

group119-loans.com

subgroup116-mail.com

list52-rocketmail.com

subgroup137-mail.com

list76-rocketmail.com

alerts393.info

alerts381.info

group141-loans.com

subgroup127-mail.com

list89-rocketmail.com

alerts318.info

alerts383.info

subgroup115-mail.com

list58-rocketmail.com

list65-rocketmail.com

subgroup144-mail.com

176.32.103.1–254

Domains on Subnet

311 total.Purchase ListExplore

evi.com

swiship.com

goodreasd.com

readersunited.com

alerts301.info

alerts354.info

list99-rocketmail.com

alerts362.info

subgroup157-mail.com

group140-loans.com

group145-loans.com

subgroup101-mail.com

alerts330.info

alerts391.info

alerts366.info

alerts372.info

subgroup143-mail.com

subgroup185-mail.com

subgroup142-mail.com

group109-loans.com

group132-loans.com

alerts371.info

alerts351.info

group134-loans.com

subgroup163-mail.com

alerts365.info

alerts353.info

subgroup187-mail.com

group119-loans.com

subgroup116-mail.com

list52-rocketmail.com

subgroup137-mail.com

list76-rocketmail.com

alerts393.info

alerts381.info

group141-loans.com

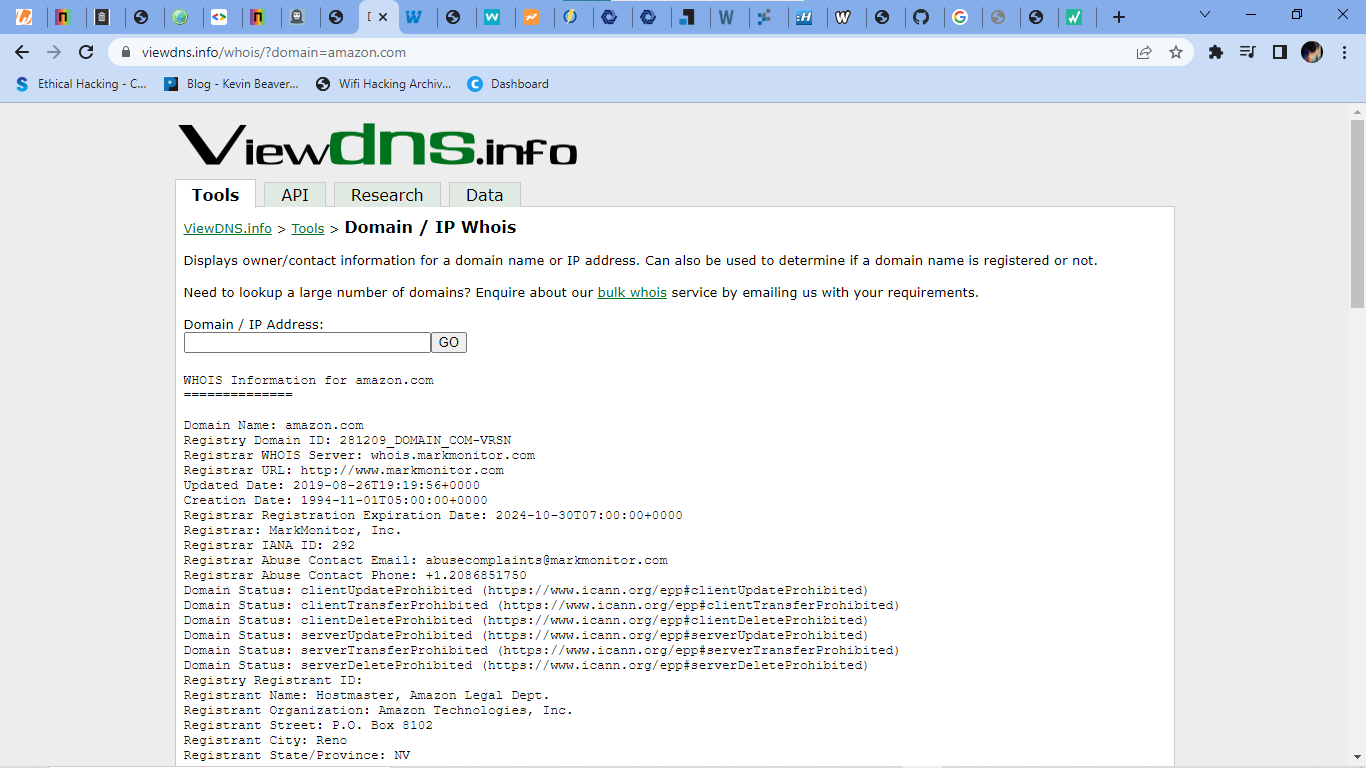
subgroup127-mail.com

list89-rocketmail.com

alerts318.info

alerts383.info

**viewdns.info**

WHOIS Information for amazon.com

==============

Domain Name: amazon.com

Registry Domain ID: 281209\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

Registrar URL: http://www.markmonitor.com

Updated Date: 2019-08-26T19:19:56+0000

Creation Date: 1994-11-01T05:00:00+0000

Registrar Registration Expiration Date: 2024-10-30T07:00:00+0000

Registrar: MarkMonitor, Inc.

Registrar IANA ID: 292

Registrar Abuse Contact Email: abusecomplaints@markmonitor.com

Registrar Abuse Contact Phone: +1.2086851750

Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)

Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)

Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)

Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)

Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)

Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)

Registry Registrant ID:

Registrant Name: Hostmaster, Amazon Legal Dept.

Registrant Organization: Amazon Technologies, Inc.

Registrant Street: P.O. Box 8102

Registrant City: Reno

Registrant State/Province: NV

Registrant Postal Code: 89507

Registrant Country: US

Registrant Phone: +1.2062664064

Registrant Phone Ext:

Registrant Fax: +1.2062667010

Registrant Fax Ext:

Registrant Email: hostmaster@amazon.com

Registry Admin ID:

Admin Name: Hostmaster, Amazon Legal Dept.

Admin Organization: Amazon Technologies, Inc.

Admin Street: P.O. Box 8102

Admin City: Reno

Admin State/Province: NV

Admin Postal Code: 89507

Admin Country: US

Admin Phone: +1.2062664064

Admin Phone Ext:

Admin Fax: +1.2062667010

Admin Fax Ext:

Admin Email: hostmaster@amazon.com

Registry Tech ID:

Tech Name: Hostmaster, Amazon Legal Dept.

Tech Organization: Amazon Technologies, Inc.

Tech Street: P.O. Box 8102

Tech City: Reno

Tech State/Province: NV

Tech Postal Code: 89507

Tech Country: US

Tech Phone: +1.2062664064

Tech Phone Ext:

Tech Fax: +1.2062667010

Tech Fax Ext:

Tech Email: hostmaster@amazon.com

Name Server: pdns1.ultradns.net

Name Server: ns1.p31.dynect.net

Name Server: pdns6.ultradns.co.uk

Name Server: ns3.p31.dynect.net

Name Server: ns4.p31.dynect.net

Name Server: ns2.p31.dynect.net

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

>>> Last update of WHOIS database: 2022-08-15T10:01:25+0000 <<<

For more information on WHOIS status codes, please visit:

https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain’s Registrant, Administrative, or Technical

contact, and such email address is not visible above, you may do so via our web

form, pursuant to ICANN’s Temporary Specification. To verify that you are not a

robot, please enter your email address to receive a link to a page that

facilitates email communication with the relevant contact(s).

Web-based WHOIS:

https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send

your request and the reasons for your request to whoisrequest@markmonitor.com

and specify the domain name in the subject line. We will review that request and

may ask for supporting documentation and explanation.

The data in MarkMonitor’s WHOIS database is provided for information purposes,

and to assist persons in obtaining information about or related to a domain

name’s registration record. While MarkMonitor believes the data to be accurate,

the data is provided "as is" with no guarantee or warranties regarding its

accuracy.

By submitting a WHOIS query, you agree that you will use this data only for

lawful purposes and that, under no circumstances will you use this data to:

(1) allow, enable, or otherwise support the transmission by email, telephone,

or facsimile of mass, unsolicited, commercial advertising, or spam; or

(2) enable high volume, automated, or electronic processes that send queries,

data, or email to MarkMonitor (or its systems) or the domain name contacts (or

its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)

Protecting companies and consumers in a digital world.

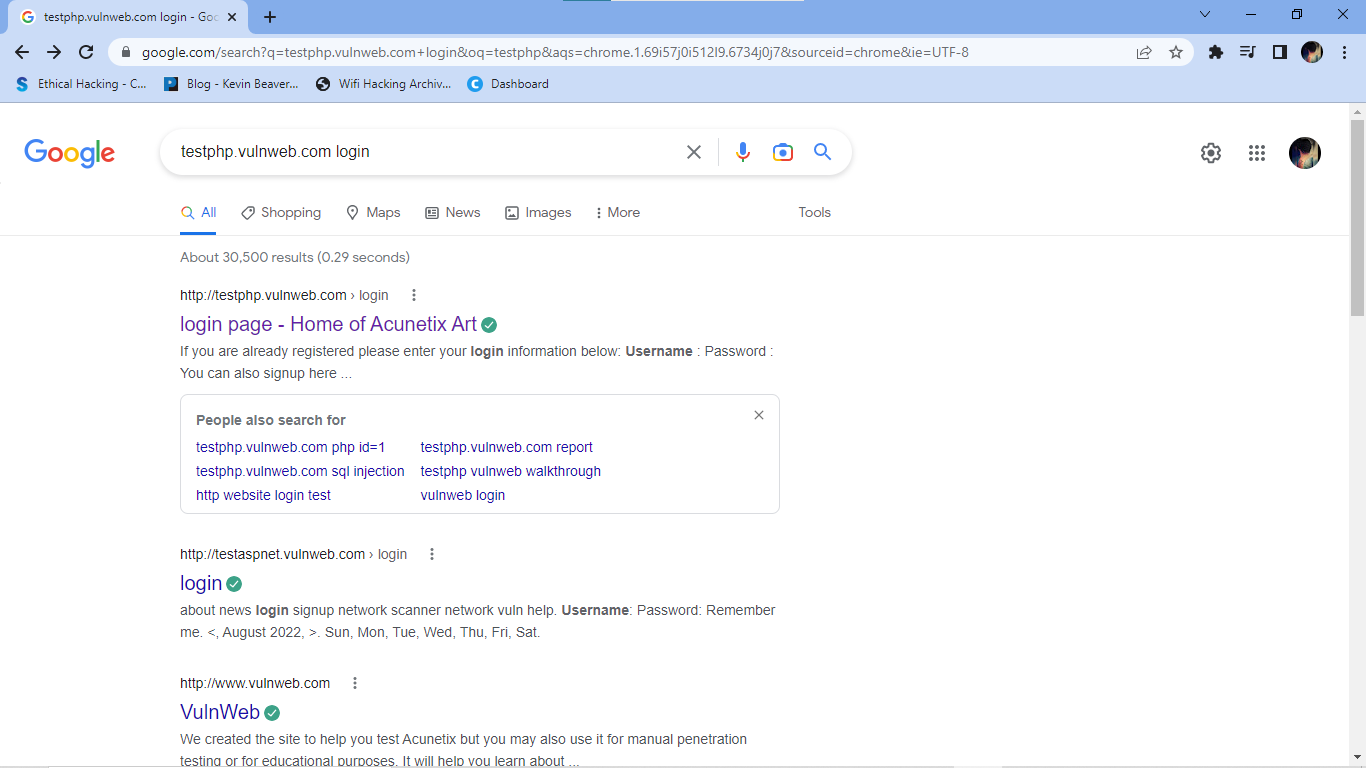
Visit MarkMonitor at https://www.markmonitor.com

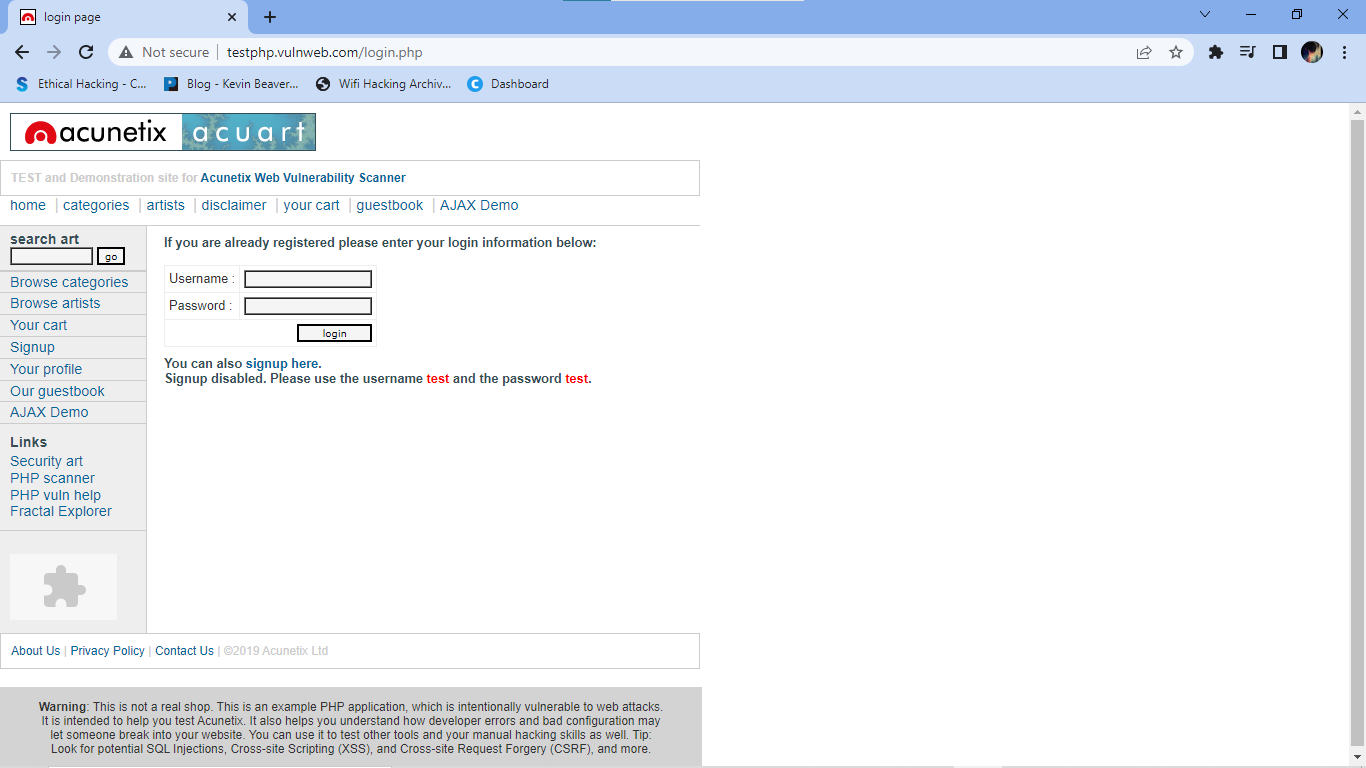
Contact us at +1.8007459229

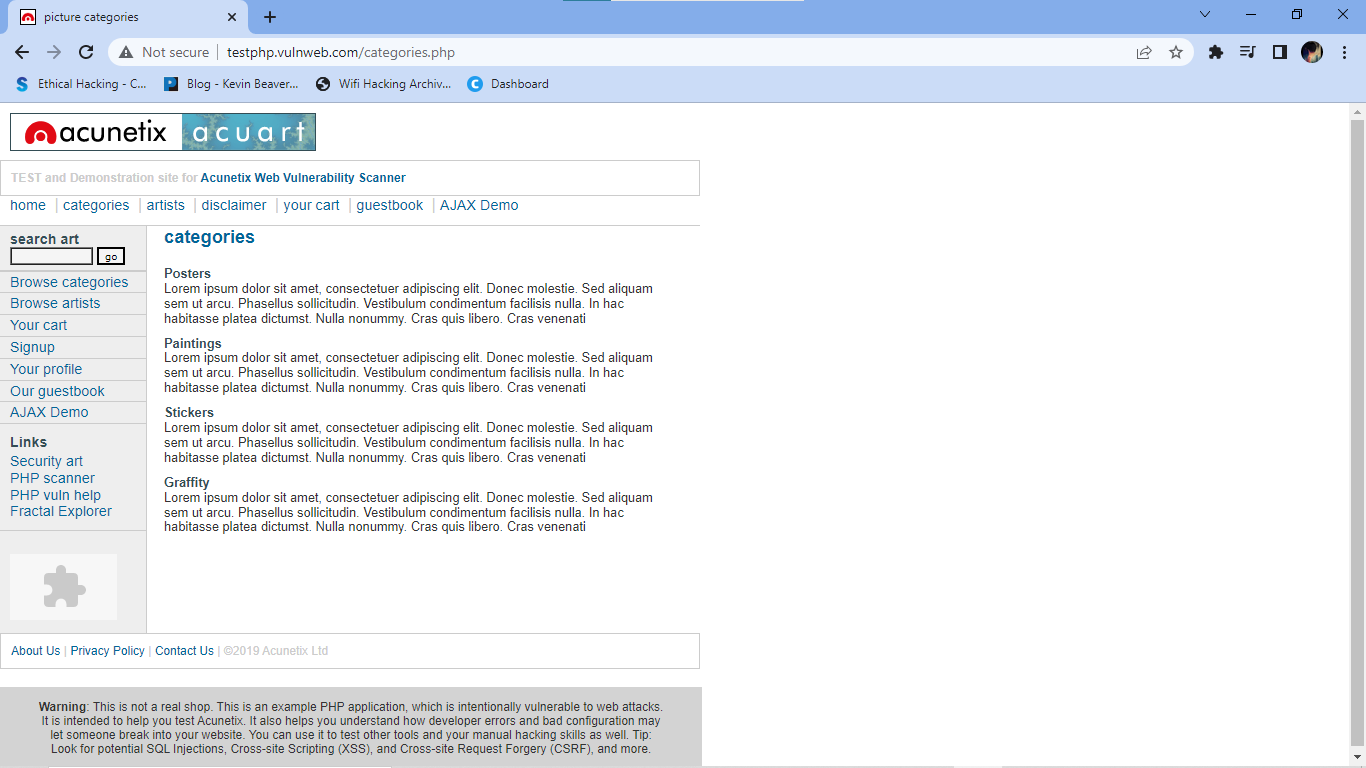
In Europe, at +44.02032062220

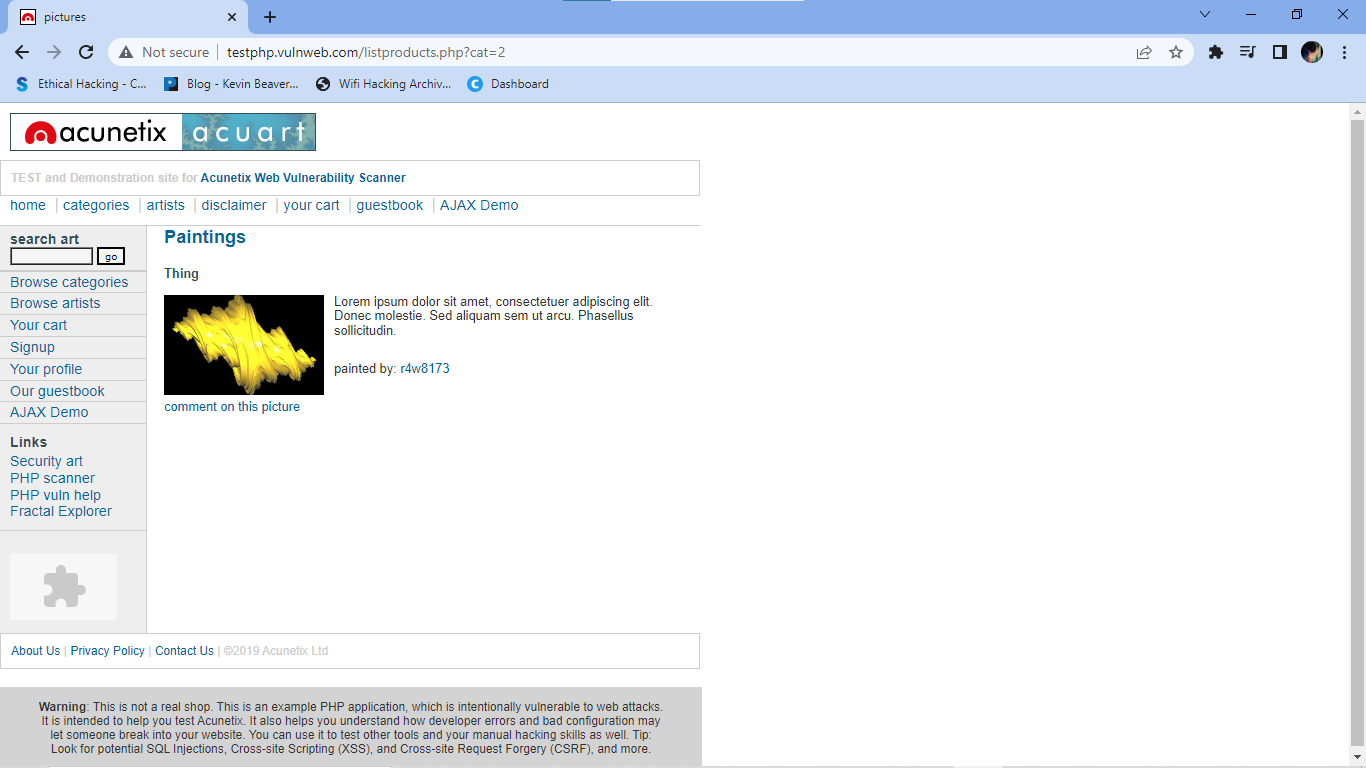
­­­

**2.Perform SQL injection on by on http://testphp.vulnweb.com Write a report along with screenshots and mention preventive steps to avoid SQL injections**

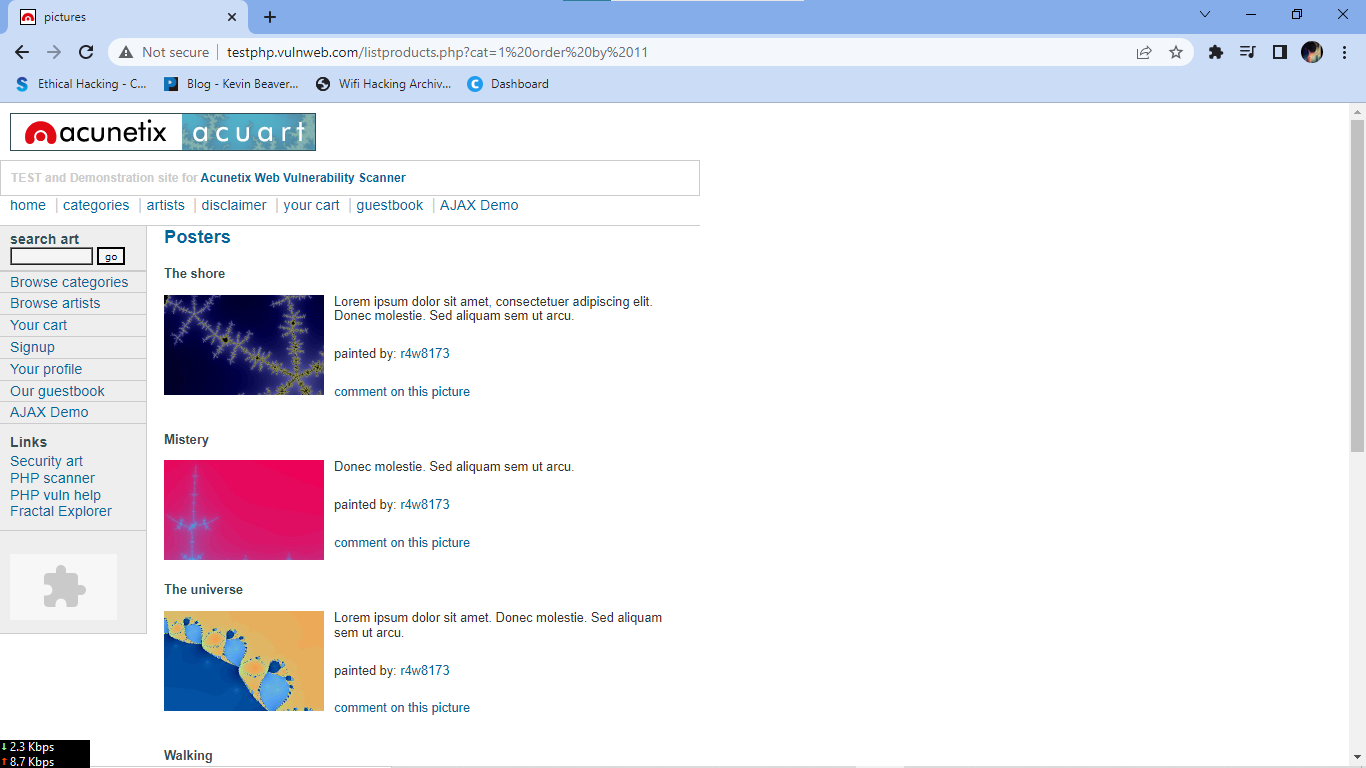


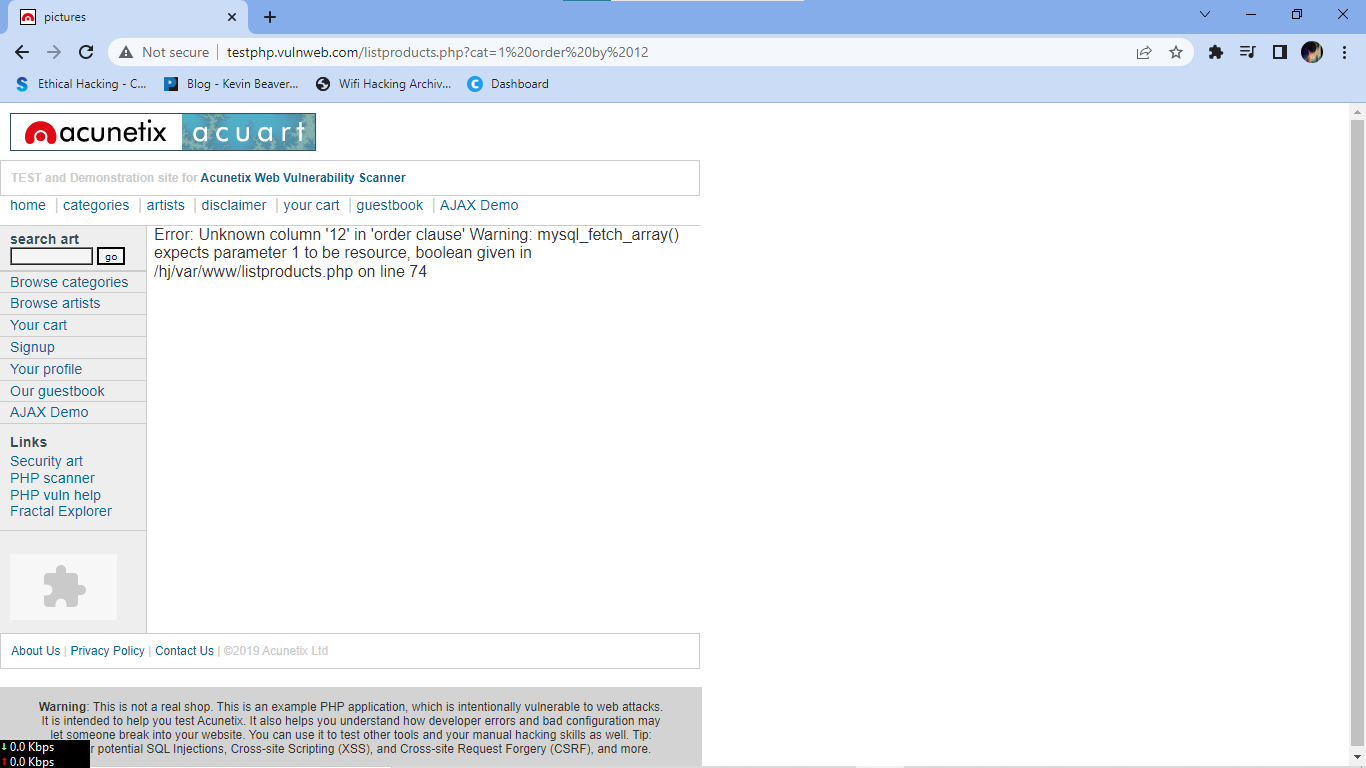


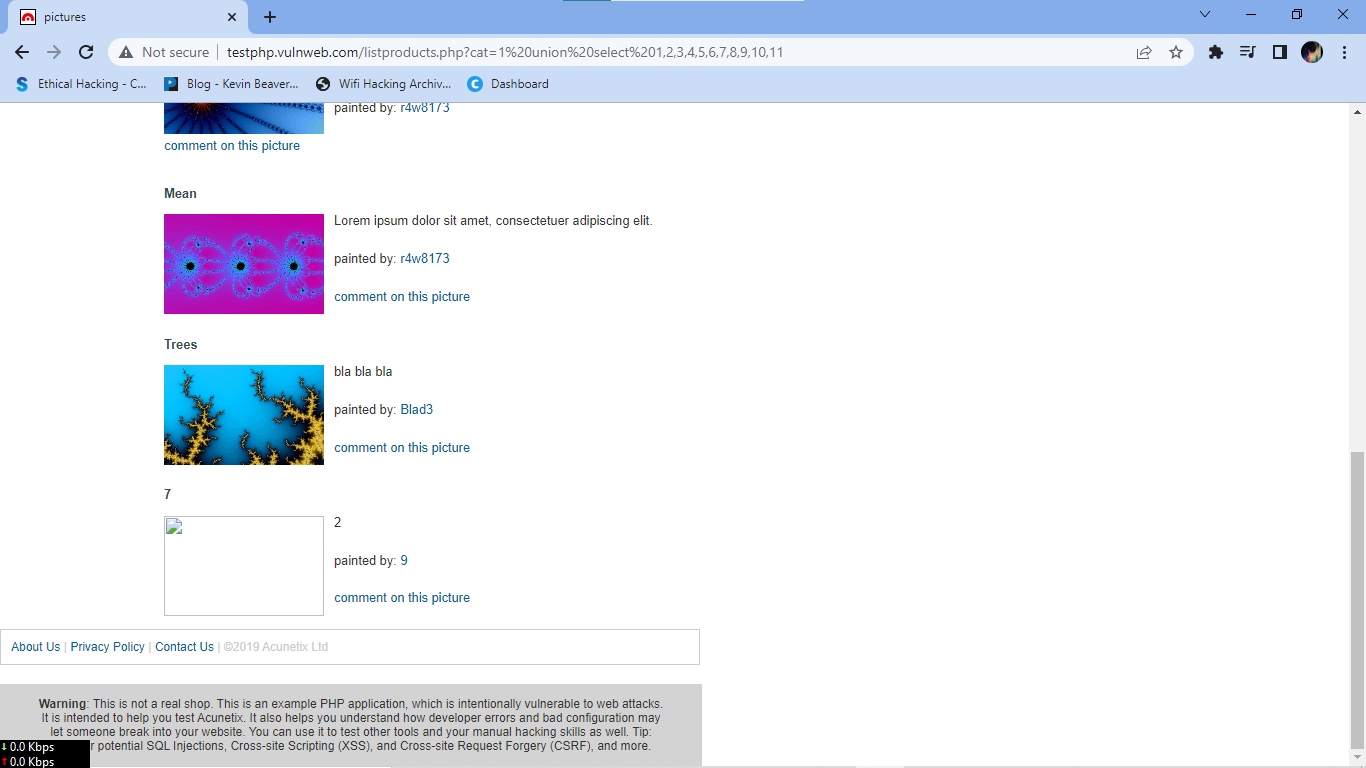


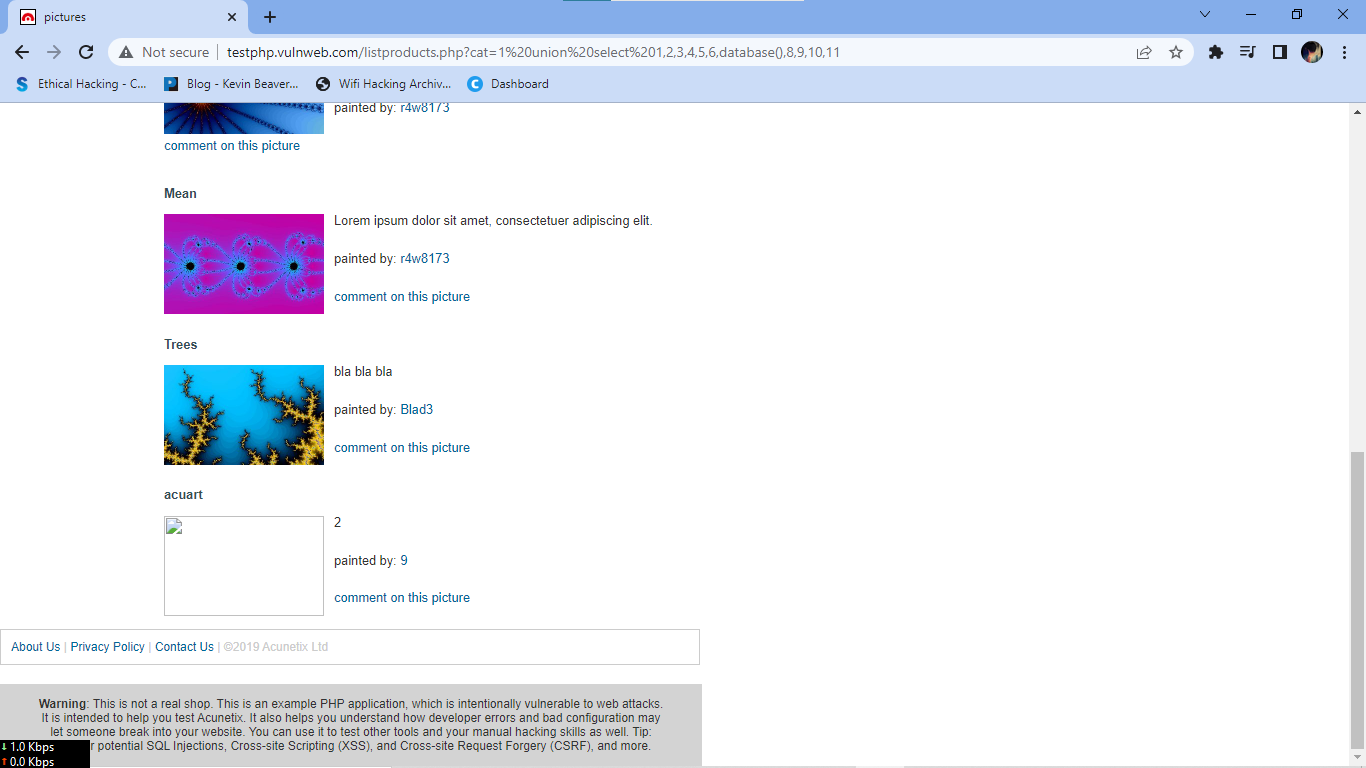


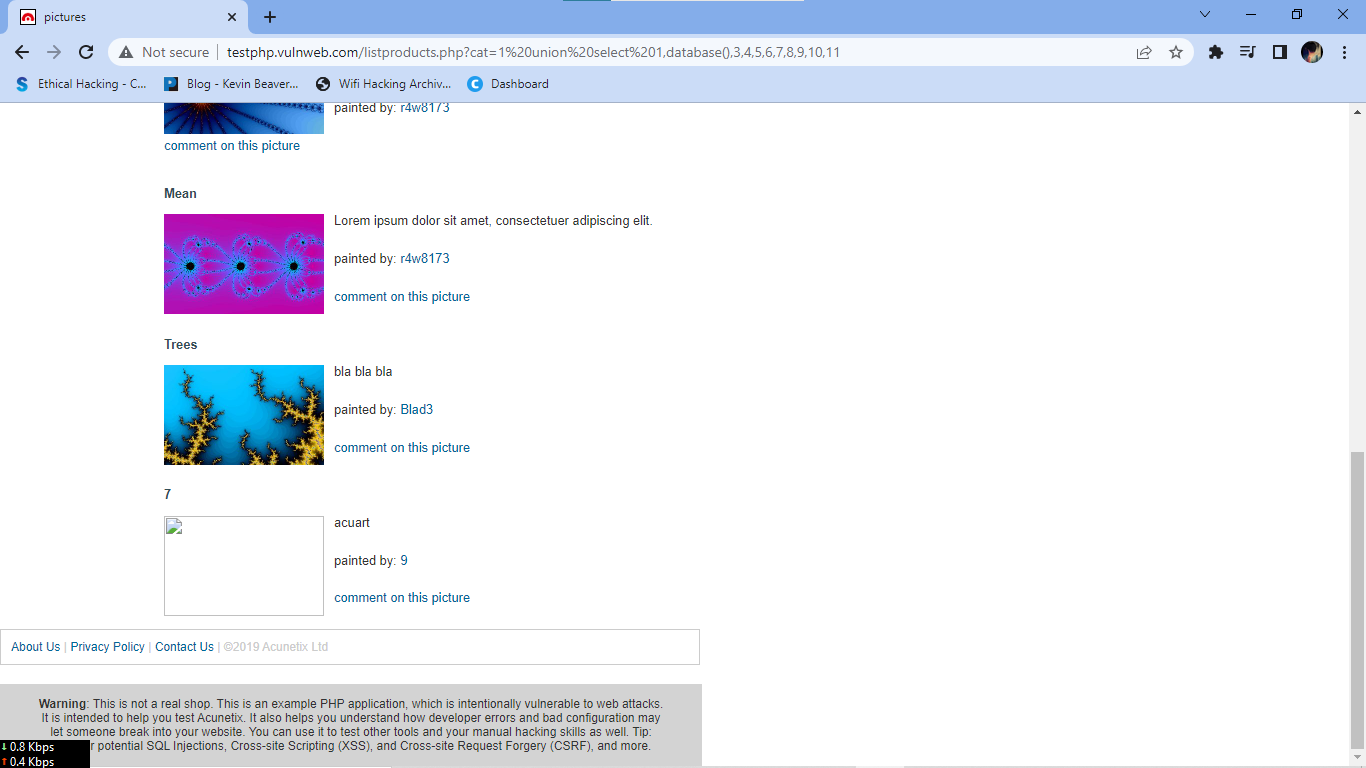


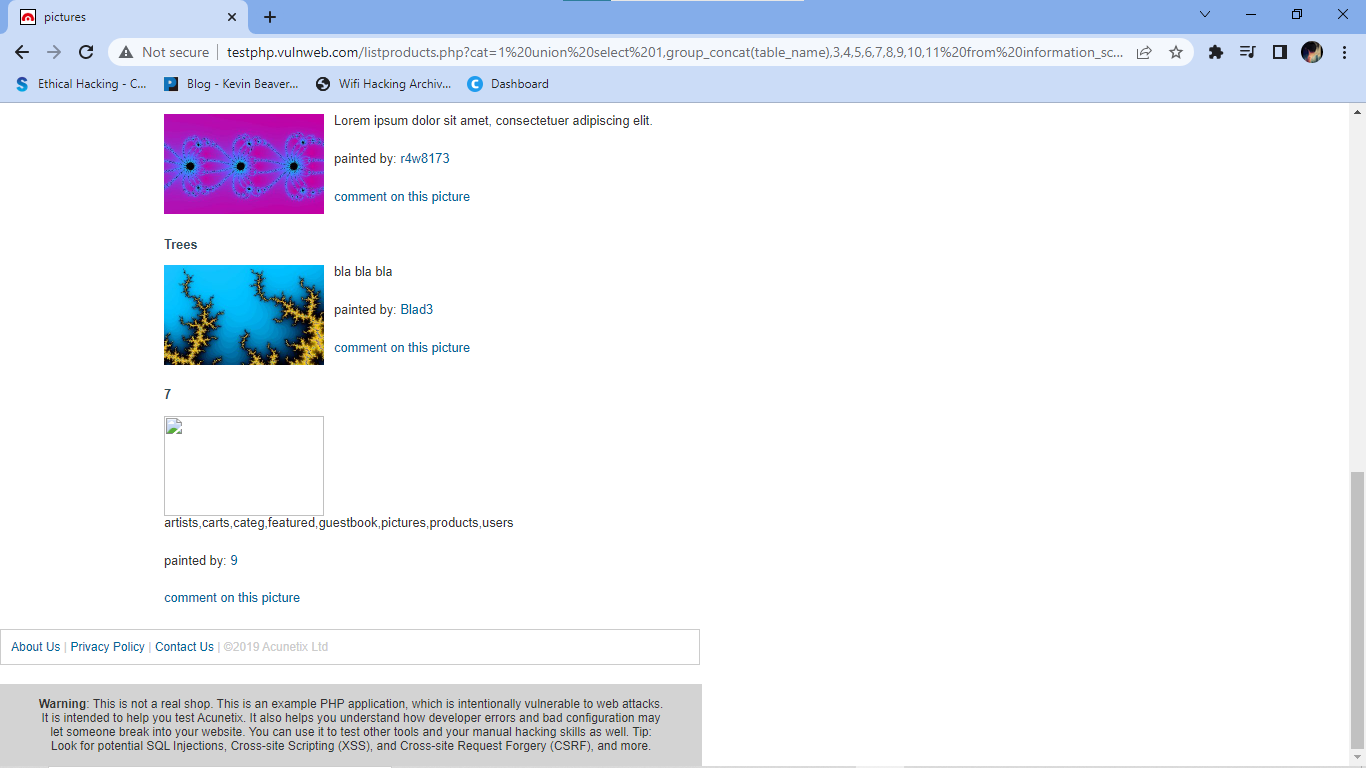


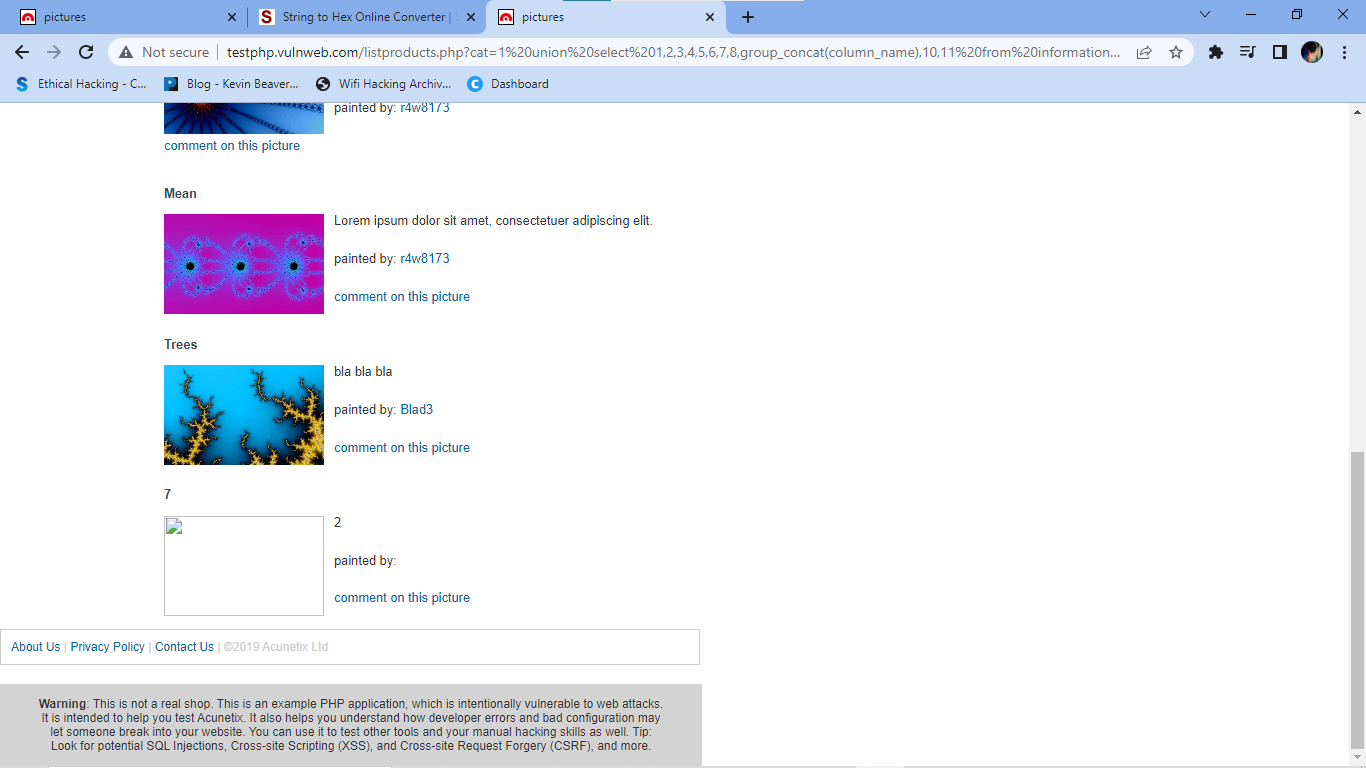


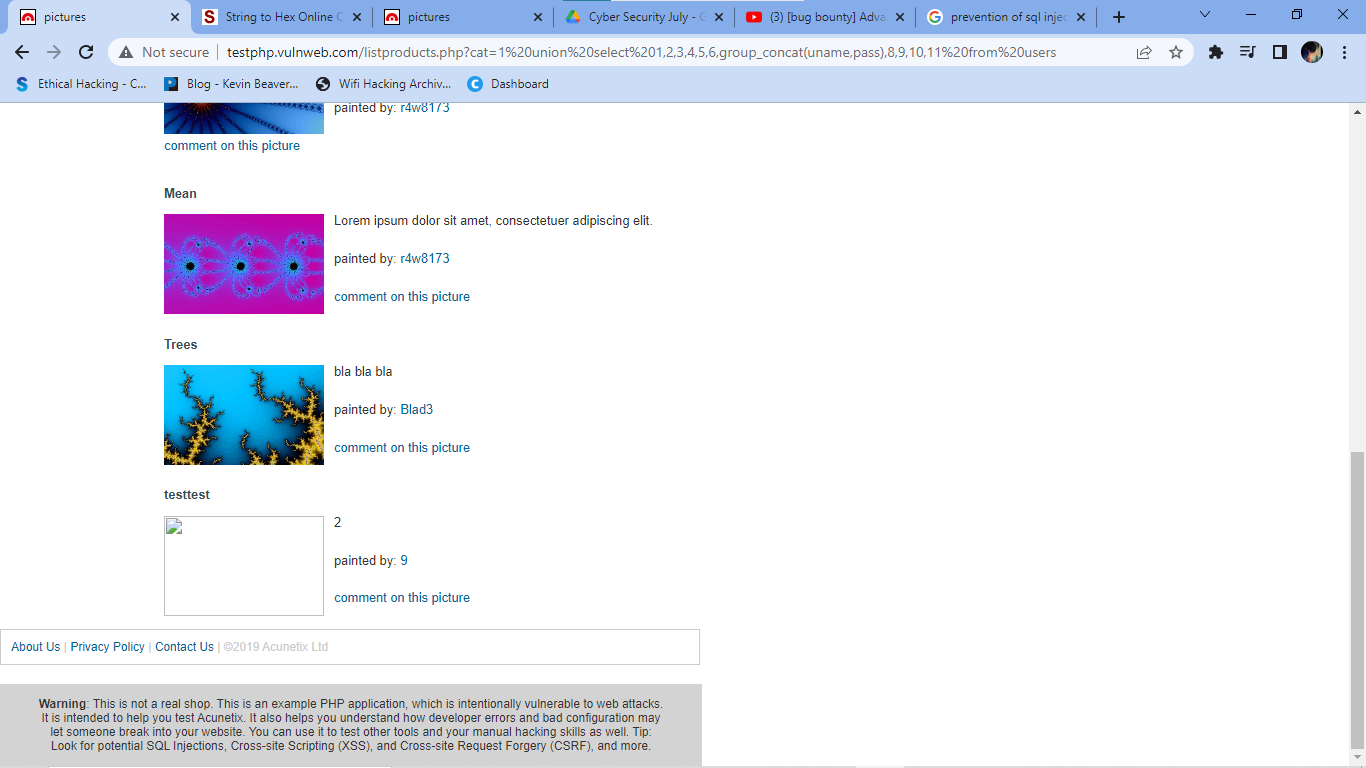












How to Prevent SQL Injection Attacks?

Preventing or mitigating SQL injection attacks is a lot about ensuring that none of the fields are vulnerable to invalid inputs and application execution. yours is manually impossible to actually to check every page and every application on the website, especially when updates are frequent and user-friendliness is the top priority.Nonetheless, security analysts and seasoned developers recommend a number of the subsequent points guarantee your database square measure well protected inside the confinement of the server.

1) Continuous Scanning and Penetration Testing

The automated web application scanner has been the best choice to point out vulnerabilities within the web applications for quite some time now. Now, with SQL injections getting smarter in exploiting logical flaws, website security professionals should explore manual testing with the help of a security vendor.

They can authenticate user inputs against a set of rules for syntax, type, and length. It helps to audit application vulnerabilities discreetly so that you can patch the code before hackers exploit it to their advantage.

2) Restrict Privileges

It is more of a database management function, but enforcing specific privileges to specific accounts helps prevent blind SQL injection attacks. Begin with no privileges account and move on to ‘read-only’, ‘edit’, ‘delete’ and similar privilege levels.

Minimizing privileges to the application will ensure that the attacker, who gets into the database through the application, cannot make unauthorized use of specific data.

3) Use Query Parameters

Dynamic queries create a lot of troubles for security professionals. They have to deal with variable vulnerabilities in each application, which only gets graver with updates and changes. It is recommended that you prepare parameterized queries.

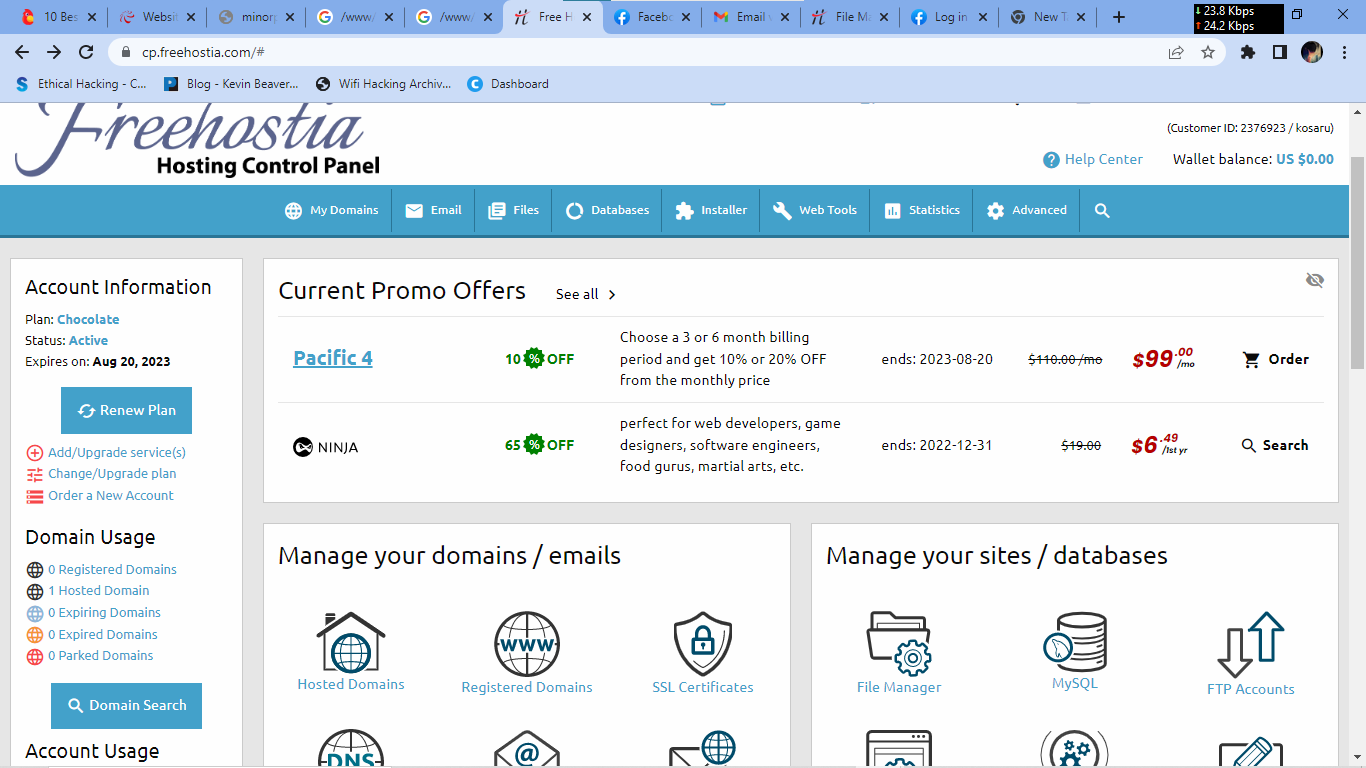
These queries are simple, easy to write, and only pass when each parameter in SQL code is clearly defined. This way, your info is supplied with weapons to differentiate between code and information inputs.

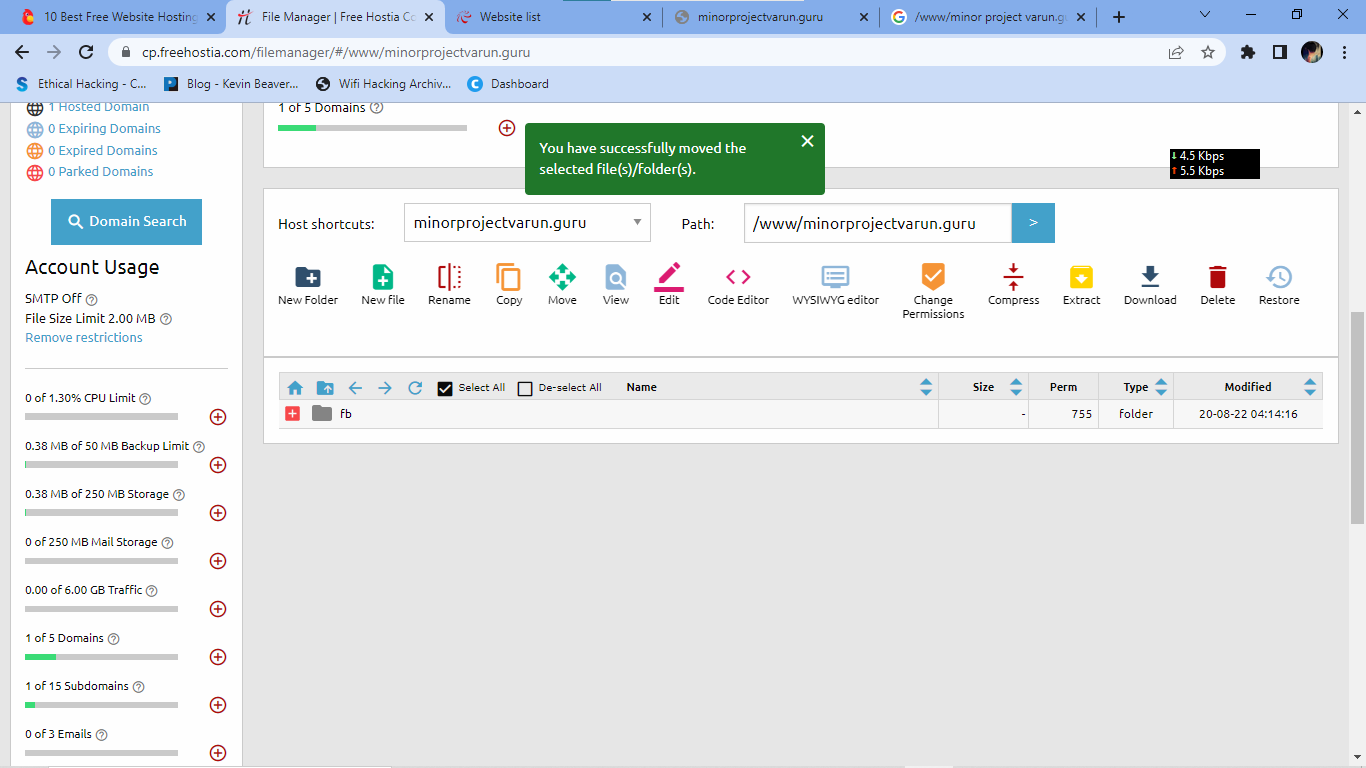
4) Instant Protection

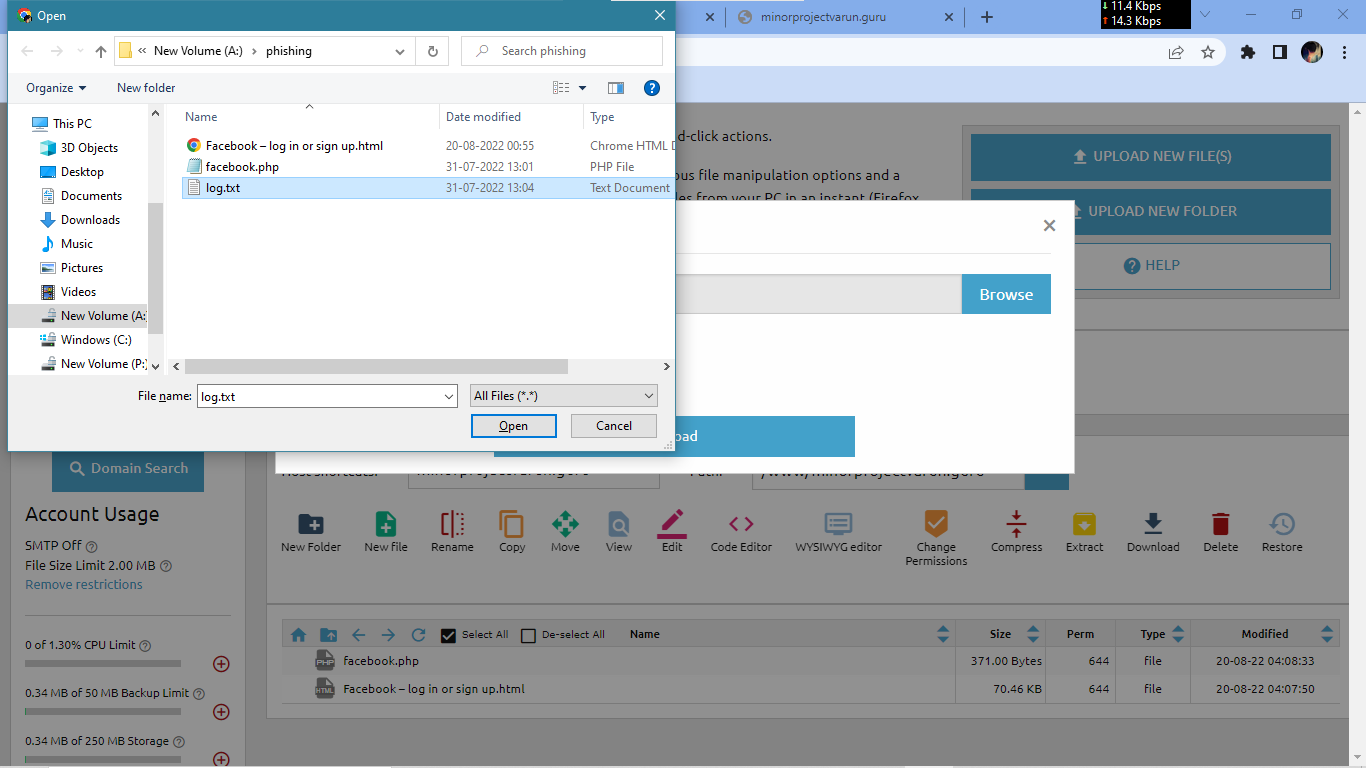
A majority of organizations fail the problems like outdated code, scarcity of resources to test and make changes, no knowledge of application security, and frequent updates in the application. For these, web application protection is the best solution.

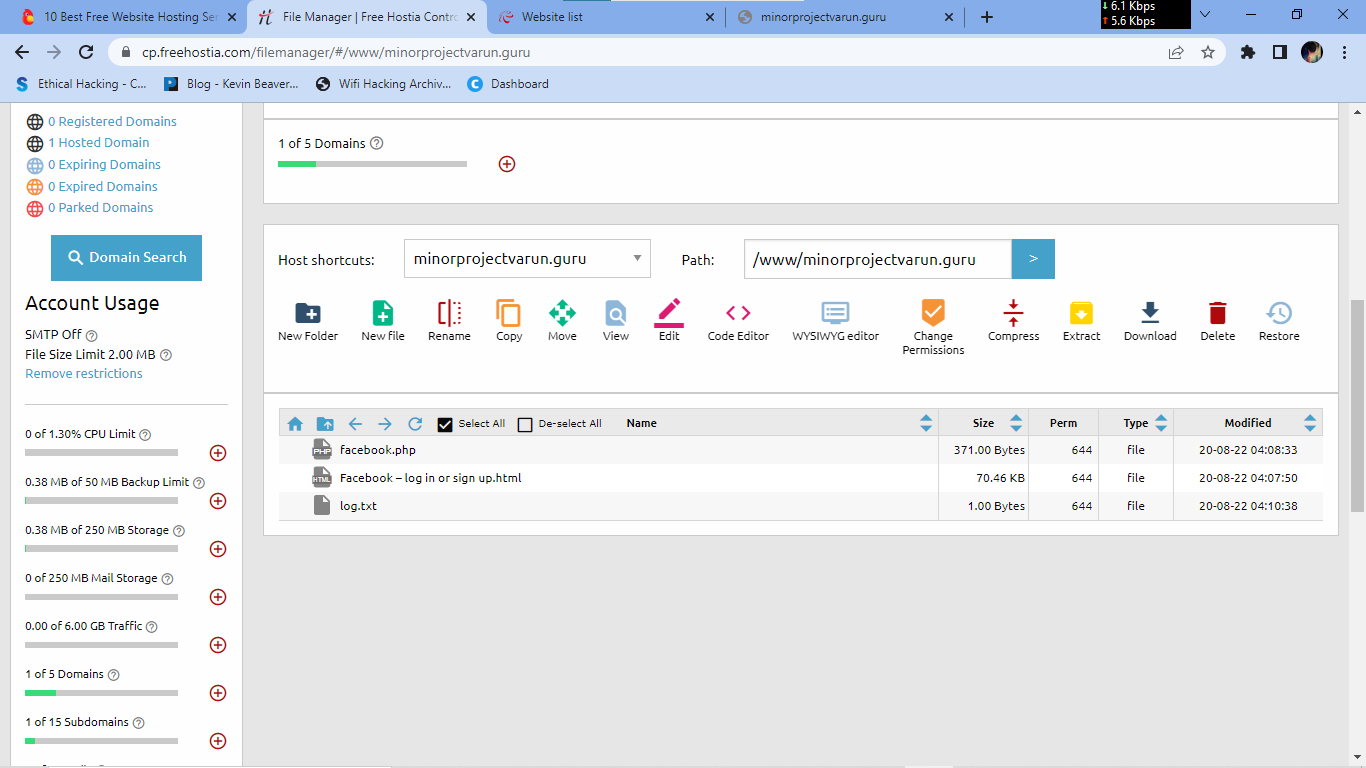
A managed web application firewall can be deployed for immediate mitigation of such attacks. It contains custom policies to block any suspicious input and deny information breach instantly. This way, you do not have to manually look for loopholes and mend problems afterward.

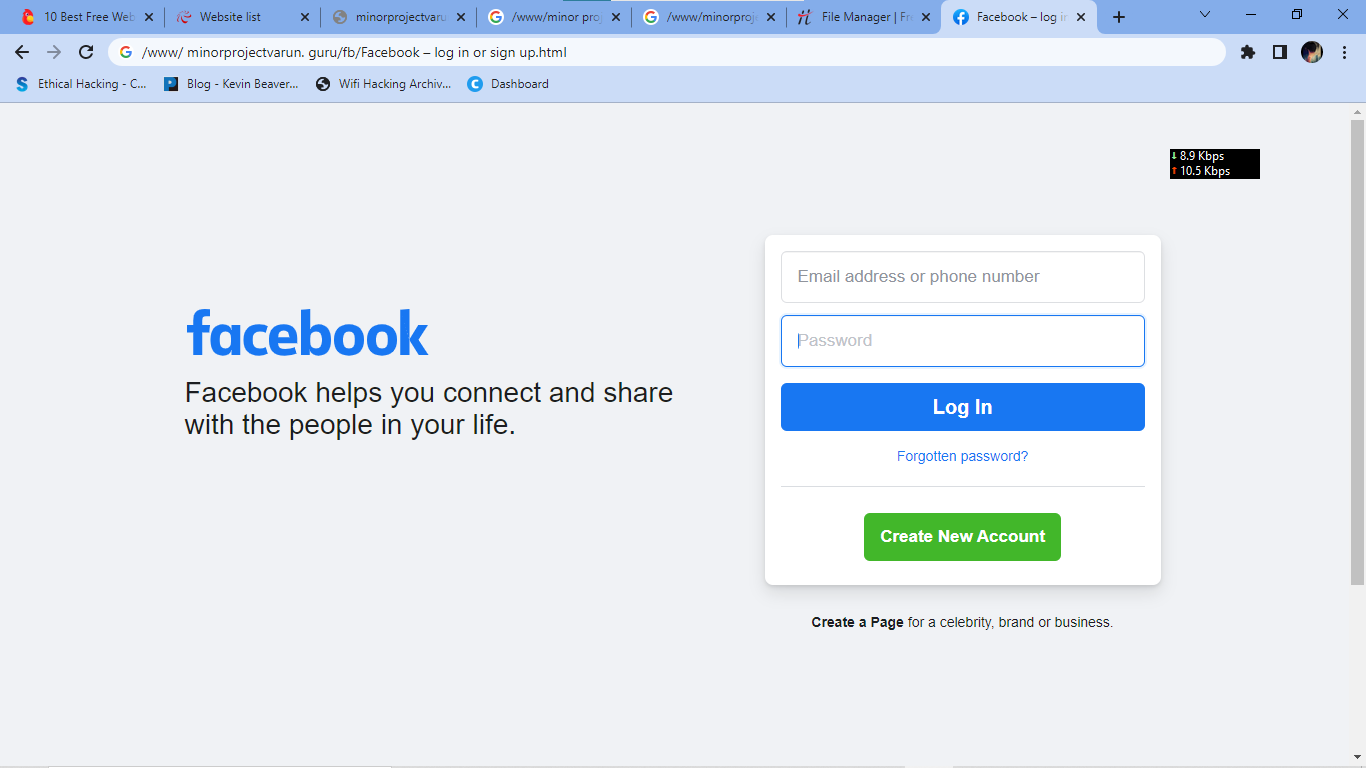
**3. Clone a Facebook page and try to perform Desktop Phishing in your local machine and capture the credentials and write the document along with screenshots and suggest the solution to avoid from phishing**

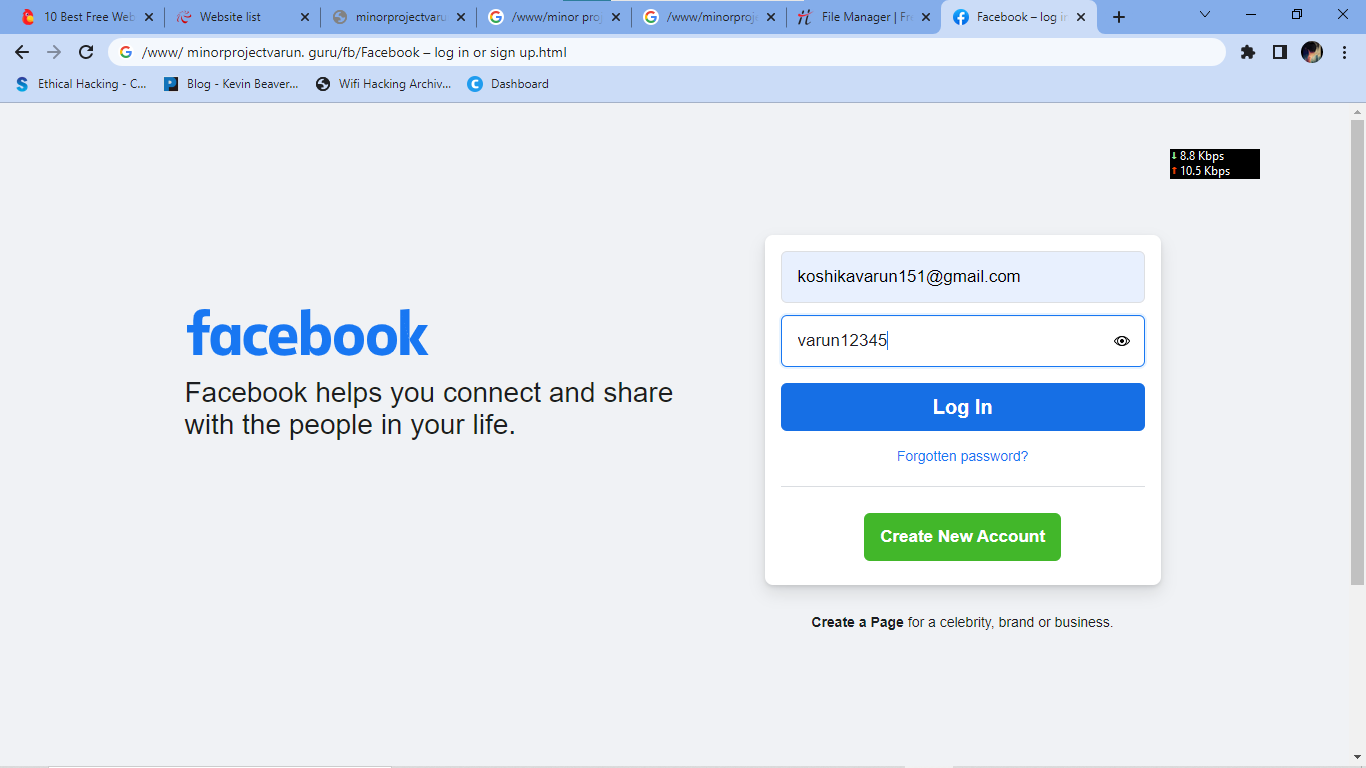
****

****

****

****

****

****

****

**1. Know what a phishing scam looks like**

New phishing attack methods are being developed all the time, but they share commonalities that can be identified if you know what to look for. There are many sites online that will keep you informed of the latest phishing attacks and their key identifiers. The earlier you find out about the latest attack methods and share them with your users through regular security awareness training, the more likely you are to avoid a potential attack.

**2. Don’t click on that link**

It’s generally not advisable to click on a link in an email or instant message, even if you know the sender. The bare minimum you should be doing is hovering over the link to see if the destination is the correct one. Some phishing attacks are fairly sophisticated, and the destination URL can look like a carbon copy of the genuine site, set up to record keystrokes or steal login/credit card information. If it’s possible for you to go straight to the site through your search engine, rather than click on the link, then you should do so.

**3. Get free anti-phishing add-ons**

Most browsers nowadays will enable you to download add-ons that spot the signs of a malicious website or alert you about known phishing sites. They are usually completely free so there’s no reason not to have this installed on every device in your organization.

**4. Don’t give your information to an unsecured site**

If the URL of the website doesn’t start with “https”, or you cannot see a closed padlock icon next to the URL, do not enter any sensitive information or download files from that site. Site’s without security certificates may not be intended for phishing scams, but it’s better to be safe than sorry.

**5. Rotate passwords regularly**

If you’ve got online accounts, you should get into the habit of regularly rotating your passwords so that you prevent an attacker from gaining unlimited access. Your accounts may have been compromised without you knowing, so adding that extra layer of protection through password rotation can prevent ongoing attacks and lock out potential attackers.

**6. Don’t ignore those updates**

Receiving numerous update messages can be frustrating, and it can be tempting to put them off or ignore them altogether. Don’t do this. Security patches and updates are released for a reason, most commonly to keep up to date with modern cyber-attack methods by patching holes in security. If you don’t update your browser, you could be at risk of phishing attacks through known vulnerabilities that could have been easily avoided.

**7. Install firewalls**

Firewalls are an effective way to prevent external attacks, acting as a shield between your computer and an attacker. Both desktop firewalls and network firewalls, when used together, can bolster your security and reduce the chances of a hacker infiltrating your environment.

**8. Don’t be tempted by those pop-ups**

Pop-ups aren’t just irritating; they are often linked to malware as part of attempted phishing attacks. Most browsers now allow you to download and install free ad-blocker software that will automatically block most of the malicious pop-ups. If one does manage to evade the ad-blocker though, don’t be tempted to click! Occasionally pop-ups will try and deceive you with where the “Close” button is, so always try and look for an “x” in one of the corners.

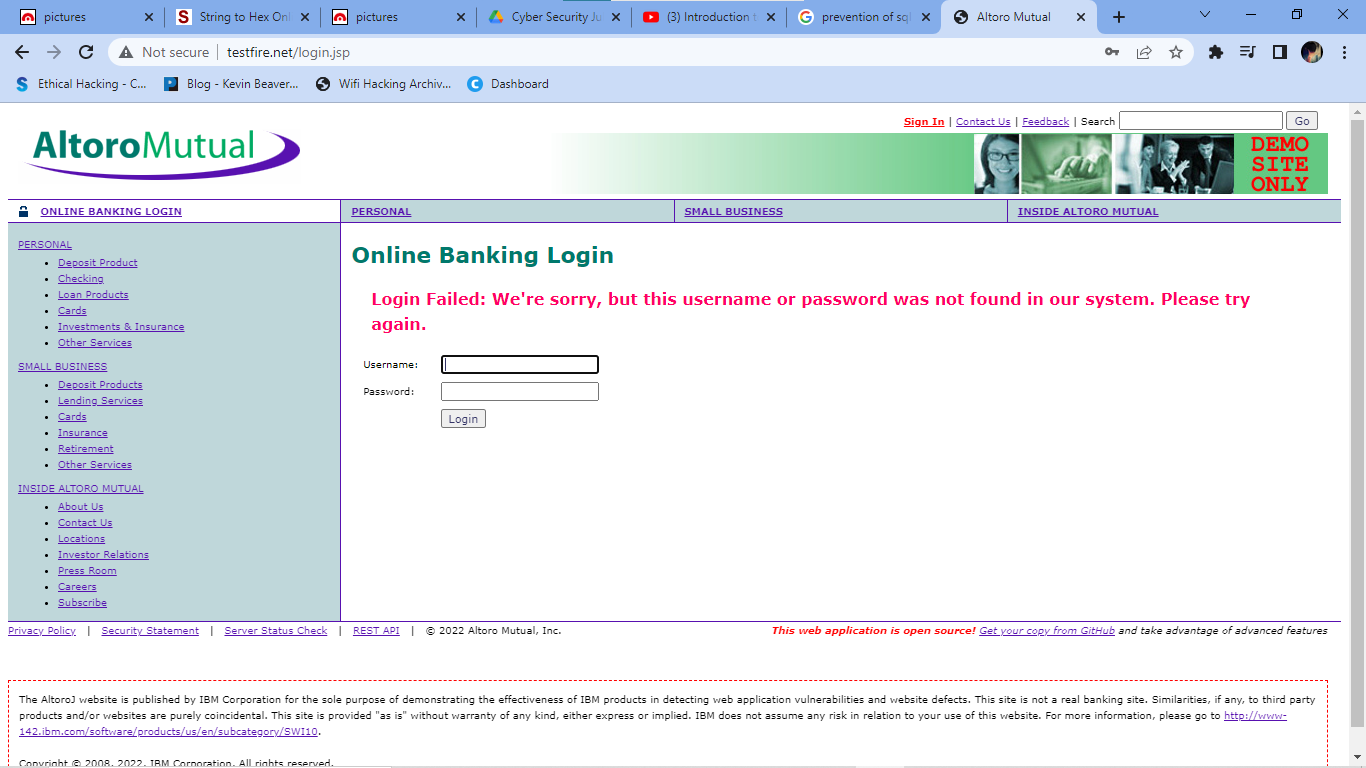
**9. Don’t give out important information unless you must**

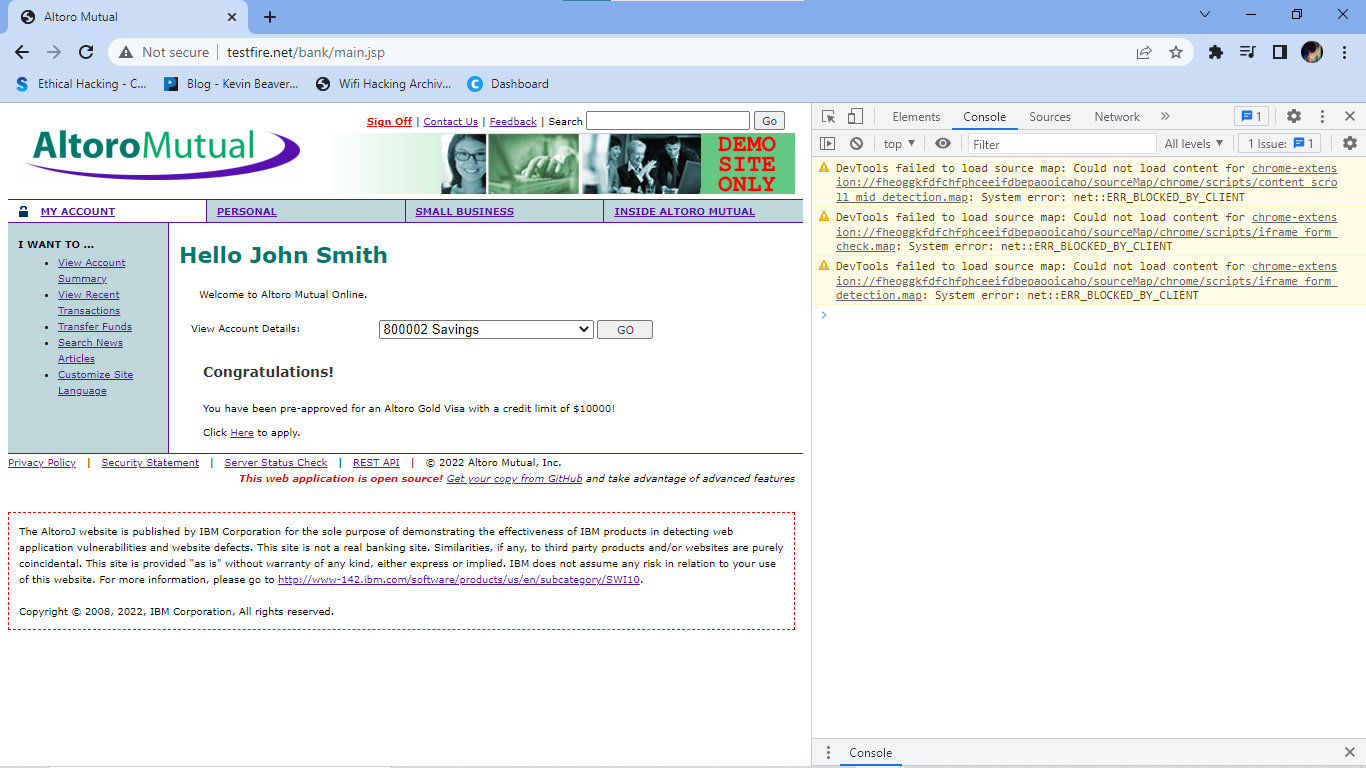
As a general rule of thumb, unless you 100% trust the site you are on, you should not willingly give out your card information. Make sure, if you have to provide your information, that you verify the website is genuine, that the company is real and that the site itself is secure.

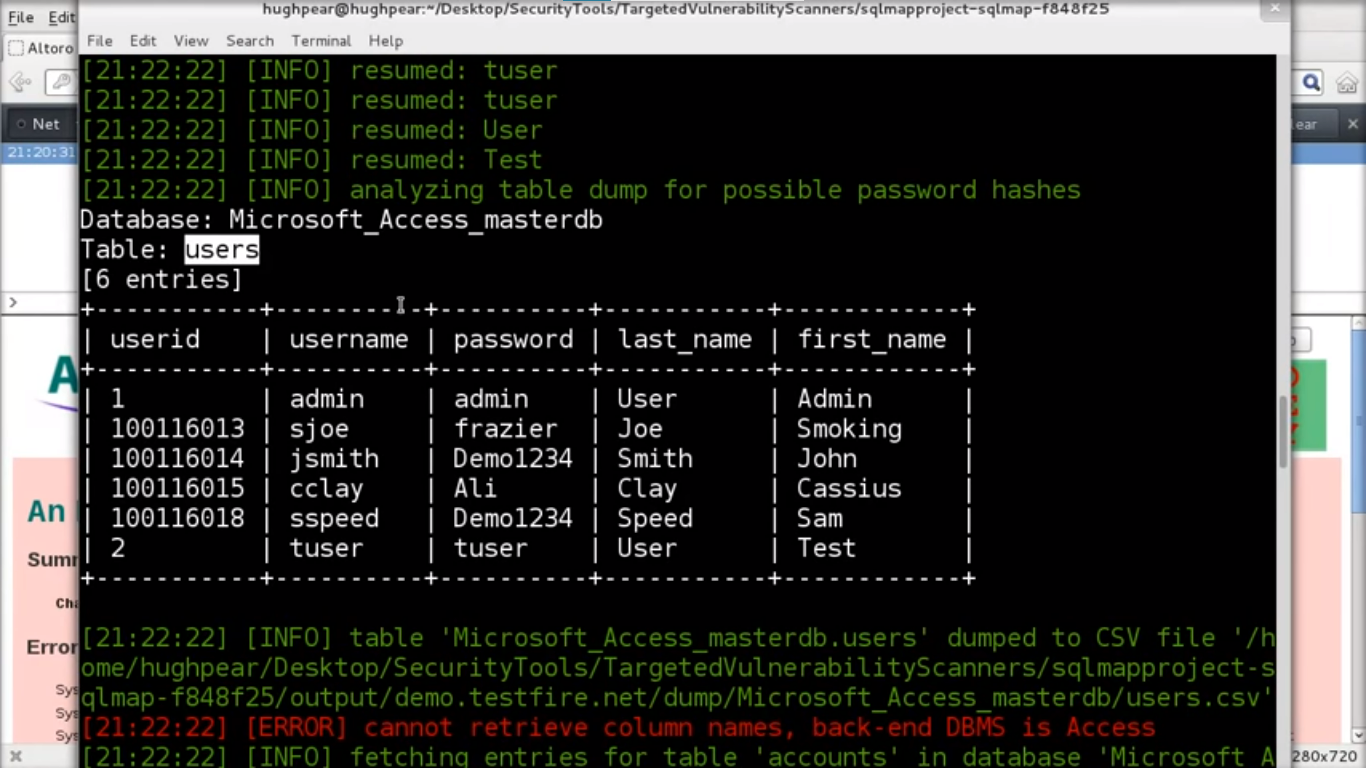
**10. Have a Data Security Platform to spot signs of an attack**

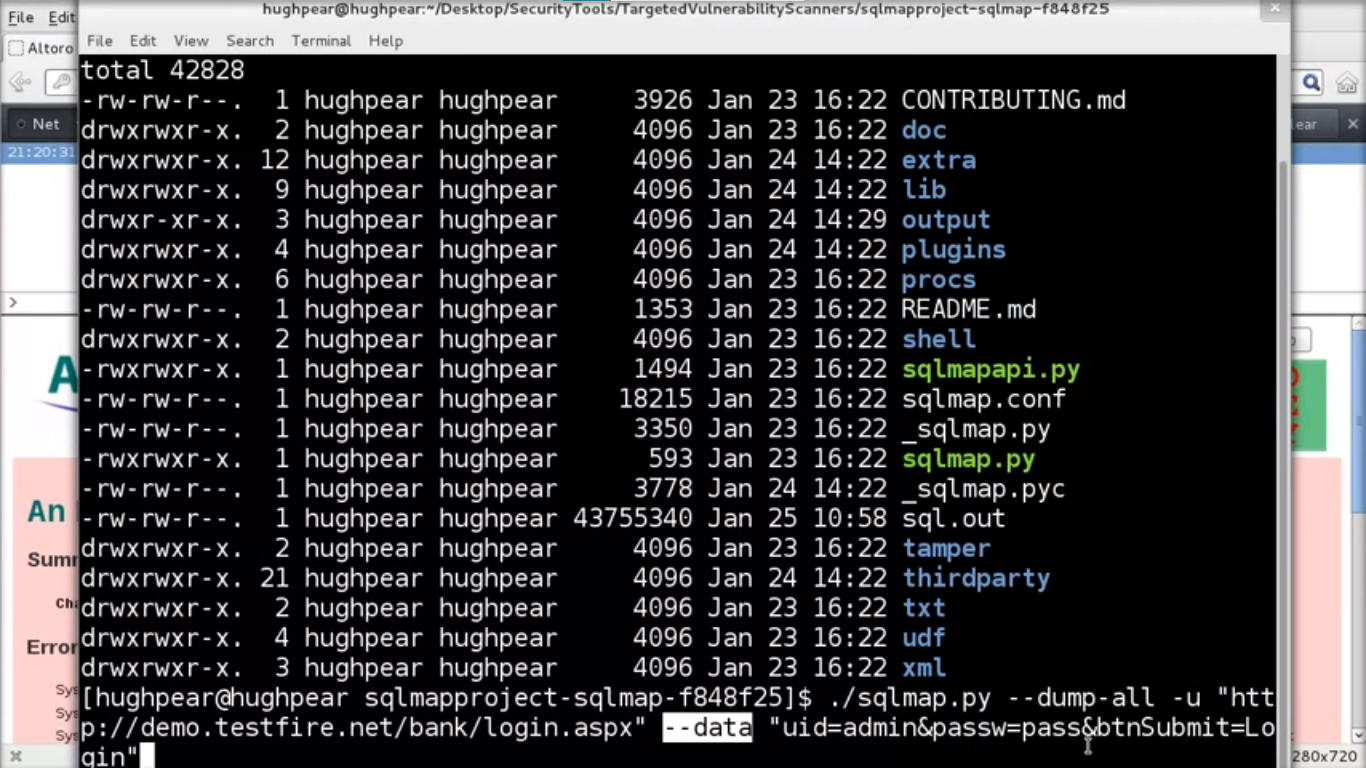
If you are unfortunate enough to be the victim of a successful phishing attack, then it’s important you are able to detect and react in a timely manner. Having a [data security platform](https://www.lepide.com/data-security-platform/) in place helps take some of the pressure off the IT/Security team by automatically alerting on anomalous user behavior and unwanted changes to files. If an attacker has access to your sensitive information, data security platforms can help to identify the affected account so that you can take actions to prevent further damage.

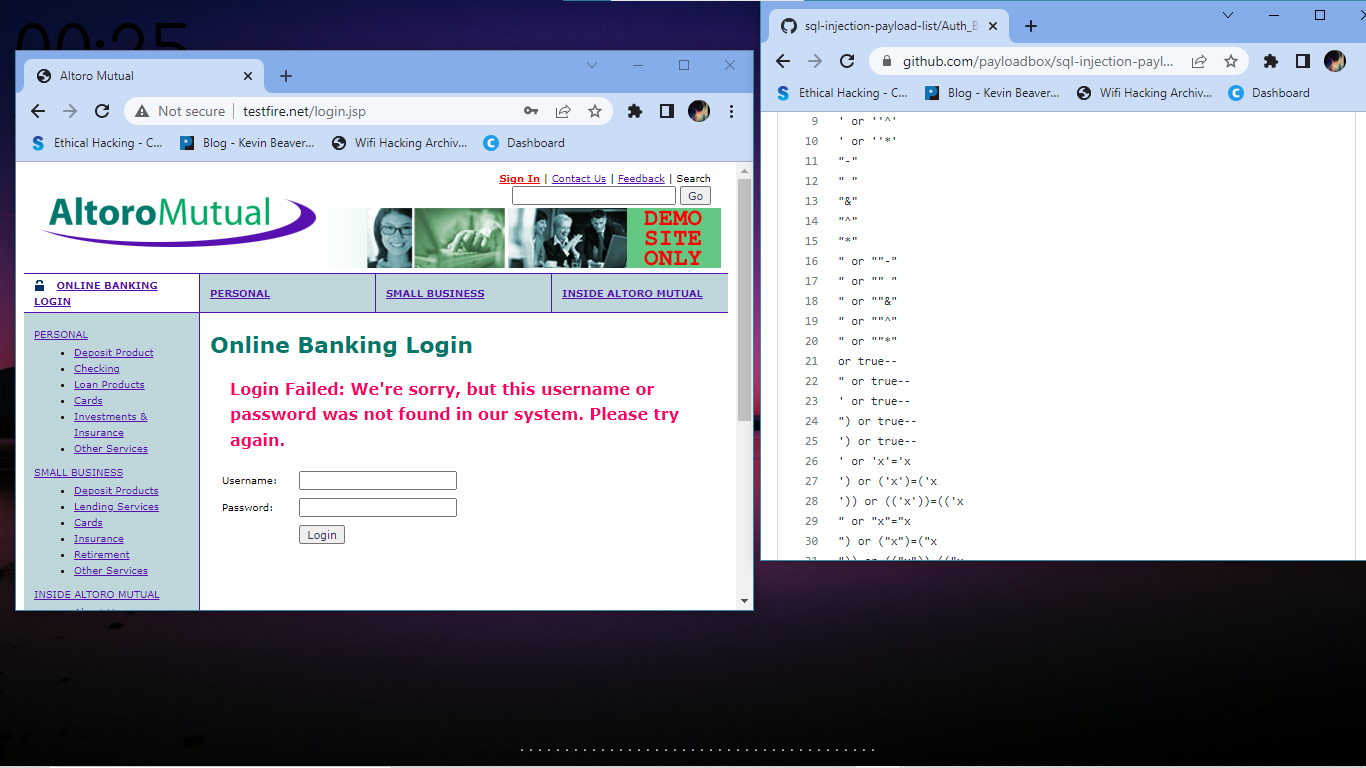
**4.Perform Bypass Authentication on http://demo.testfire.net website with different payloads and make report along with screenshots and mention to mitigation steps to protect**

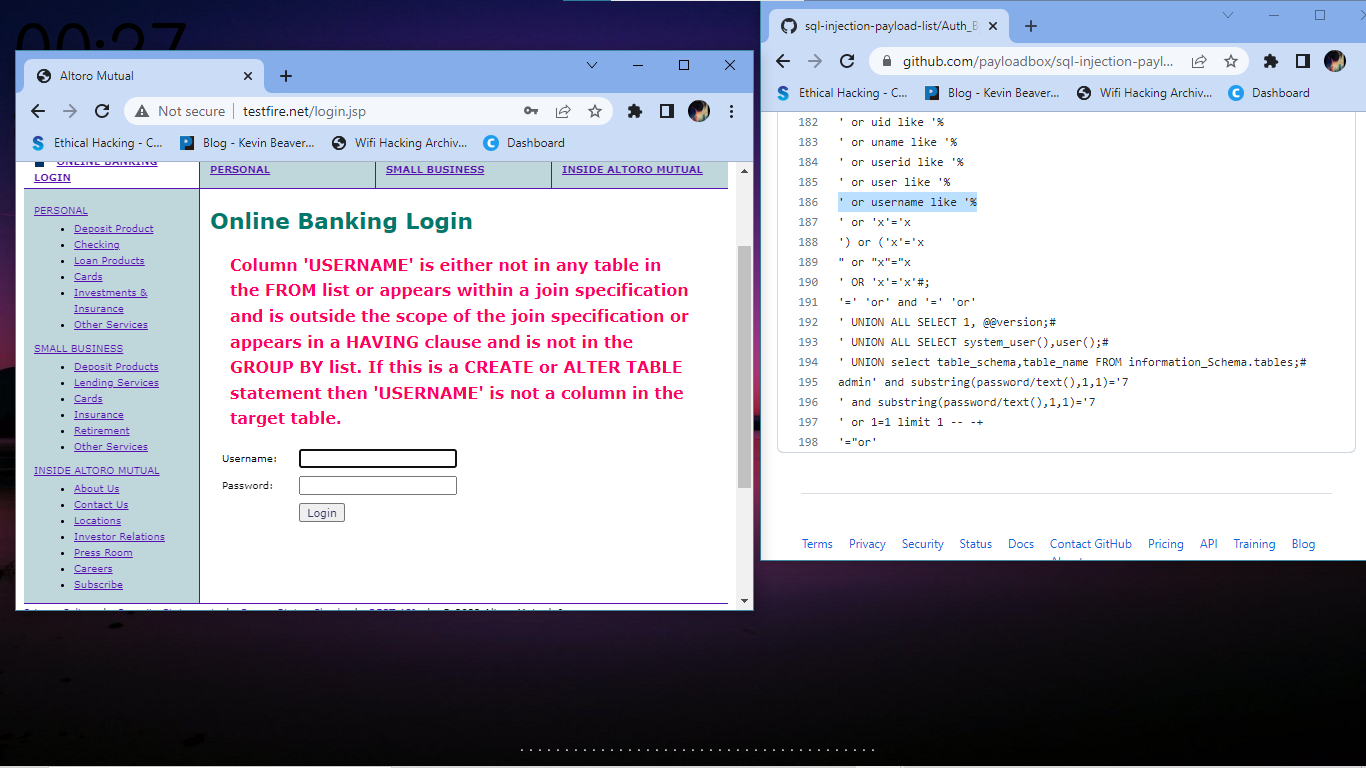


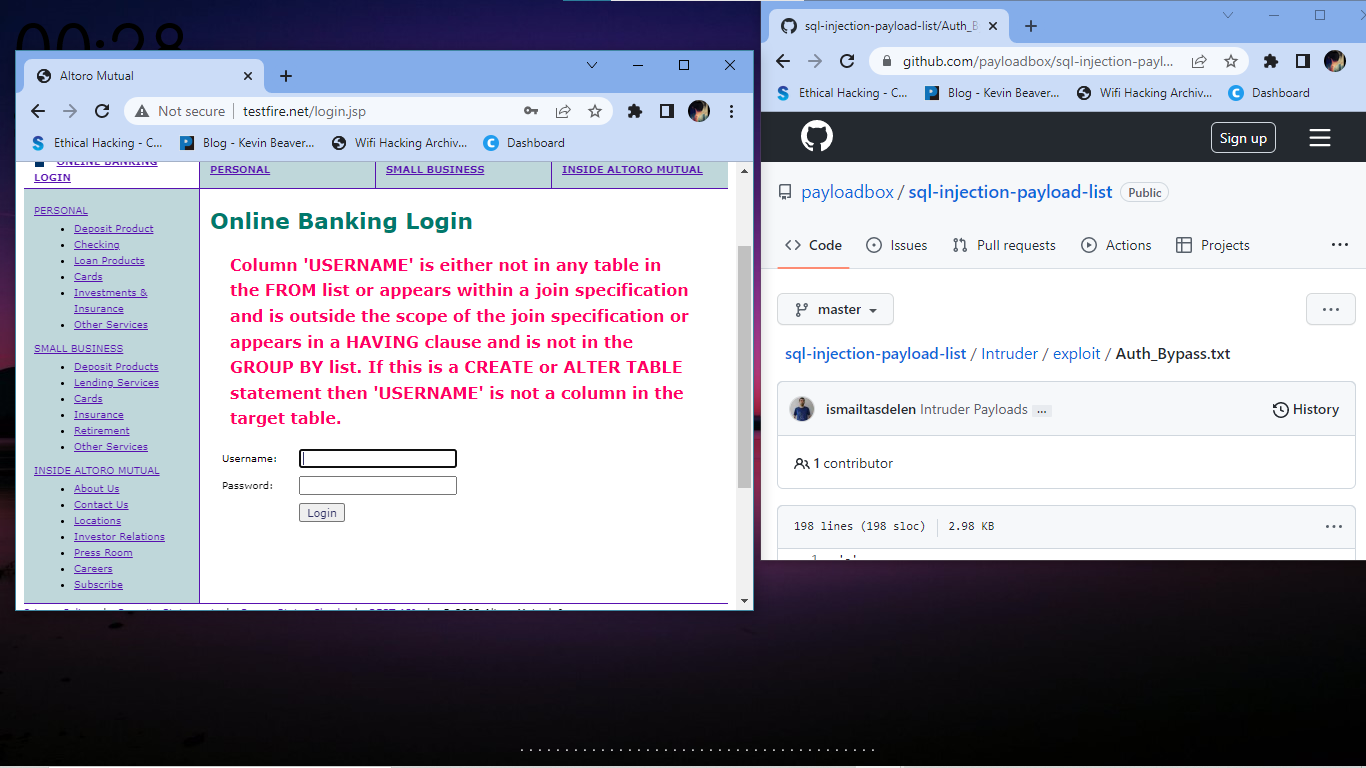


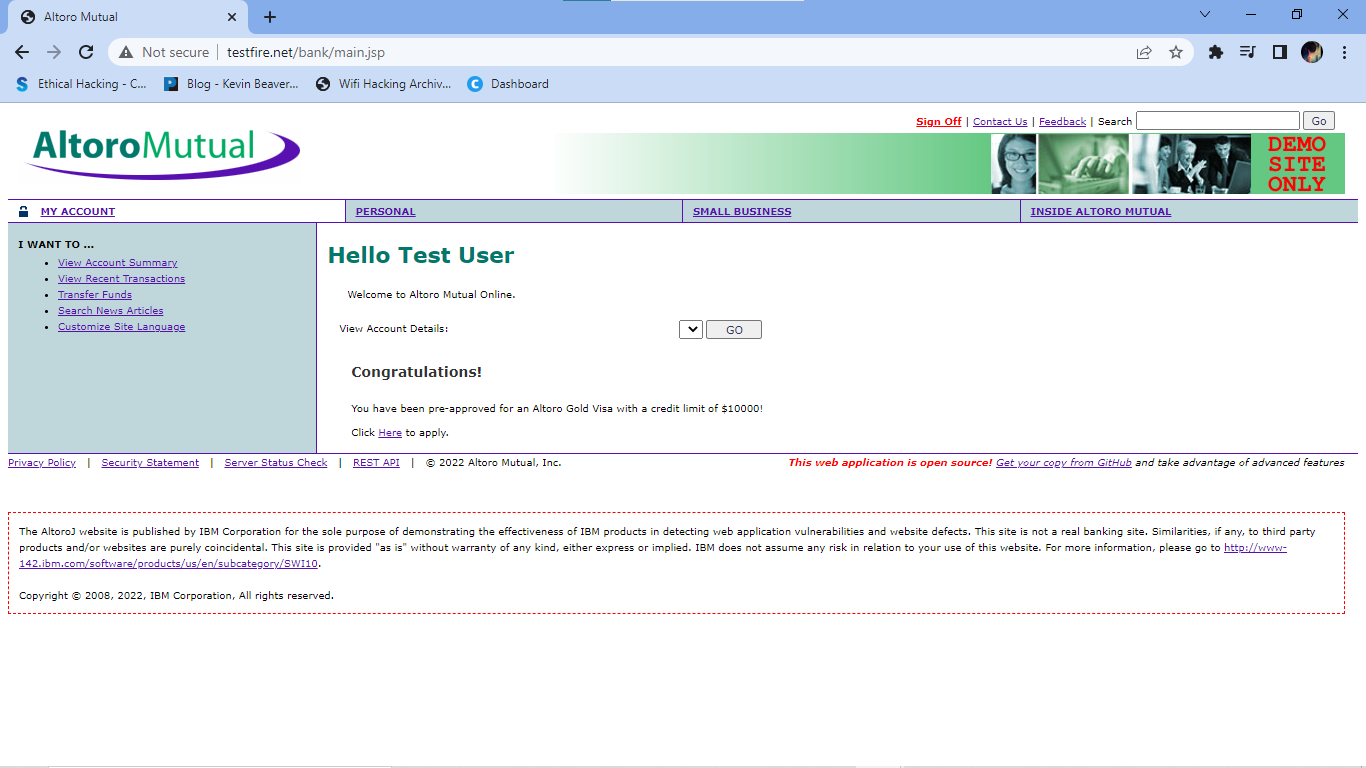












18 Steps to Prevent SQL Injection Attacks

Though SQL injection attacks are still the most dangerous threat to web administrators, the good news is that there are plenty website owners can do to mitigate the danger.

Here are 18 steps you can take to significantly reduce the risk of falling victim to a SQL injection attack:

1. Validate User Inputs

A common first step to preventing SQL injection attacks is validating user inputs. First, identify the essential SQL statements and establish a whitelist for all valid SQL statements, leaving unvalidated statements out of the query. This process is known as input validation or query redesign.

Additionally, you should configure inputs for user data by context. For example, input fields for email addresses can be filtered to allow only the characters in an email address, such as a required “@” character. Similarly, phone numbers and social security numbers should only be filtered to allow the specific number of digits for each.

While this action alone won’t stop SQLi attackers, it is an added barrier to a common fact-finding tactic for SQL injection attacks.

2. Sanitize Data By Limiting Special Characters

Another component of safeguarding against SQL injection attacks is mitigating inadequate data sanitization. Because SQLi attackers can use unique character sequences to take advantage of a database, sanitizing data not to allow string concatenation is critical.

One way of doing this is configuring user inputs to a function such as MySQL’s mysql\_real\_escape\_string(). Doing this can ensure that any dangerous characters such as a single quote ‘ is not passed to a SQL query as instructions. A primary method of avoiding these unauthenticated queries is the use of prepared statements.

3. Enforce Prepared Statements And Parameterization

Sadly, input validation and data sanitization aren’t fix-alls. It’s critical organizations also use prepared statements with parameterized queries, also known as variable binding, for writing all database queries. By defining all SQL code involved with queries, or parameterization, you can distinguish between user input and code.

While dynamic SQL as a coding technique can offer more flexible application development, it can also mean SQLi vulnerabilities as accepted code instructions. By sticking with standard SQL, the database will treat malicious SQL statements inputted like data and not as a potential command.

4. Use Stored Procedures In The Database

Similar to parameterization, using stored procedures also requires variable binding. Unlike the prepared statements approach to mitigating SQLi, stored procedures reside in the database and are called from the web application. Stored procedures are also not immune to vulnerabilities if dynamic SQL generation is used.

Organizations like OWASP say only one of the parameterized approaches is necessary, but neither method is enough for optimal security. Crafting parameterized queries should be done in conjunction with our other recommendations.

5. Actively Manage Patches And Updates

Vulnerabilities in applications and databases that are exploitable using SQL injection are regularly discovered and publicly identified. Like so many cybersecurity threats, it’s vital organizations stay in tune with the most recent news and apply patches and updates as soon as practical. For SQLi purposes, this means keeping all web application software components, including database server software, frameworks, libraries, plug-ins, and web server software, up to date.

If your organization struggles to consistently patch and update programs, a patch management solution might be worth the investment.

6. Raise Virtual Or Physical Firewalls

We strongly recommend using a software or appliance-based web application firewall (WAF) to help filter out malicious data.

Firewalls today, including NGFW and FWaaS offerings, have both a comprehensive set of default rules and the ease to change configurations as needed. If a patch or update has yet to be released, WAFs can be handy.

A popular example is the free, open-source module ModSecurity, available for Apache, Microsoft IIS, and nginx web servers. ModSecurity provides a sophisticated and ever-evolving set of rules to filter potentially dangerous web requests. Its SQL injection defenses can catch most attempts to sneak SQL through web channels.

7. Harden Your OS And Applications

This step goes beyond mitigating SQL injection attacks in ensuring your entire physical and virtual framework is working intentionally. With the big news of supply chain compromises in 2020, many are looking to NIST and other industry-standard security checklists to harden operating systems and applications.

Adopting application vendor security guidelines can enhance an organization’s defensive posture and help identify and disable unnecessary applications and servers.

8. Reduce Your Attack Surface

In cybersecurity, an attack surface refers to the array of potential entry points for attackers. So in the context of SQLi attacks, this means disposing of any database functionalities that you don’t need or further safeguarding them.

One such example is the xp\_cmdshell extended stored procedure in the Microsoft SQL Server. This procedure can spawn a Windows command shell and pass a string for execution. Because the Windows process generated by xp\_cmdshell has the same security privileges as the SQL Server service account, the attacker can cause severe damage.

9. Establish Appropriate Privileges And Strict Access

Given the power SQL database holds for an organization, it’s imperative to enforce least privilege access policies with strict rules. If a website only requires the use of SELECT statements for a database, there’s no reason it should have additional INSERT, UPDATE, or DELETE privileges.

Further, your database should only be accessed with admin-level privileges when necessary, nevermind granting others access. Using a limited access account is far safer for general activity and ultimately limits an attacker’s access if the less-privileged credential is compromised.

10. Limit Read-Access

Connected to the principle of least privilege for SQL injection protection is configuring read-access to the database. If your organization only requires active users employing read-access, it’s undoubtedly easier to adopt. Nevertheless, this added step is imperative for stopping attackers from altering stored information.

11. Encryption: Keep Your Secrets Secret

It’s best to assume internet-connected applications are not secure. Therefore encryption and hashing passwords, confidential data, and connection strings are of the utmost importance.

Encryption is almost universally employed as a data protection technique today and for a good reason. Without appropriate encryption and hashing policies, sensitive information could be in plain sight for an intruder. While only a part of the security checklist, Microsoft notes encryption, “transforms the problem of protecting data into a problem of protecting cryptographic keys.”

12. Deny Extended URLs

Another tactic by SQLi attackers is sending excessively long URLs causing the server to fail at logging the complete request. In 2013, eSecurityPlanet reported on how attackers exploited Foxit by sending users long URLs that would trigger a stack-based buffer overflow.

Microsoft IIS, as another example, is built to process requests over 4096 bytes long. However, the web server software fails to place the contents of the request in the log files. Attackers can then go undetected while performing queries. To avoid this, set a limit of 2048 bytes for URLs.

13. Don’t Divulge More Than Necessary In Error Messages

SQL injection attackers can learn a great deal about database architecture from error messages, ensuring that they display minimal information. Use of the “RemoteOnly” customErrors mode (or equivalent) can display verbose error messages on the local machine while ensuring that an external attacker gets nothing more than the fact that his or her actions resulted in an unhandled error. This step is critical in safeguarding the organization’s internal database structure, table names, or account names.

14. No Shared Databases Or User Accounts

Shared databases by multiple websites or applications can be a recipe for disaster. And the same is true for user accounts that have access to various web applications. This shared access might provide flexibility for the managing organization or administrator, but it also unnecessarily poses a more significant risk.

Ideally, any linked servers have minimal access to the target server and can only access the mission-critical data. Linked servers should have distinct logins from any process on the target server.

15. Enforce Best Practices For Account And Password Policies

While it might go without saying, organizations must follow the best account and password policies for foolproof security. Default and built-in passwords should be changed upon receipt and before usage, with regularly scheduled password updates. Suitable passwords in length and character complexity are essential for all SQL server administrator, user, and machine accounts.

16. Continuous Monitoring Of SQL Statements

Organizations or third-party vendors should continually monitor all SQL statements of database-connected applications for an application, including documenting all database accounts, prepared statements, and stored procedures. With visibility into how SQL statements function, it’s much easier to identify rogue SQL statements and vulnerabilities. In this continued review, admins can delete and disable unnecessary accounts, prepared statements, and stored procedures.

Monitoring tools that utilize machine learning and behavioral analysis like PAM and SIEM can be excellent add-ons to your network security.

17. Perform Regular Auditing And Penetration Testing

Regular audits of your database and application security are becoming increasingly necessary, including auditing logs for suspicious activity, group and role memberships privileges, and variable binding terms.

Just as crucial as auditing for malicious behavior is conducting penetration tests to see how your defenses respond to an array of potential attacks, including SQLi. Most penetrating testing companies can find threats such as cross-site scripting, retired software, unpatched vulnerabilities, injections, and insecure passwords.

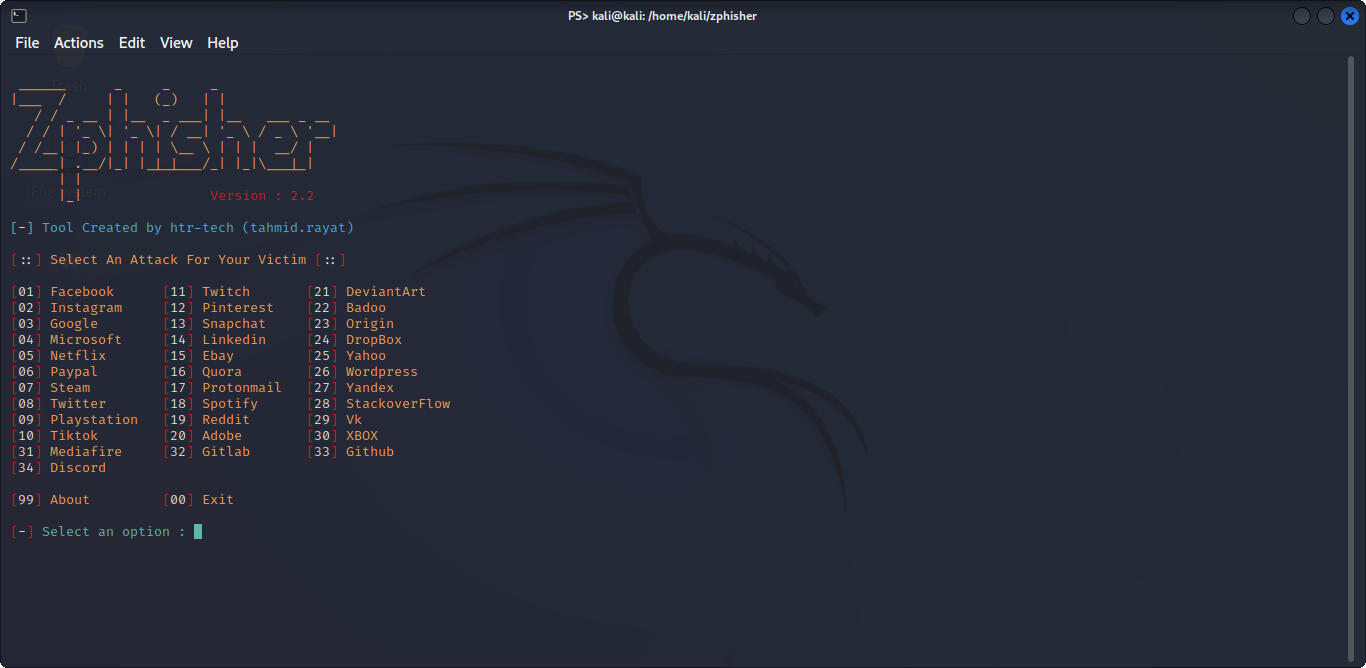
18. Code Development & Buying Better Software

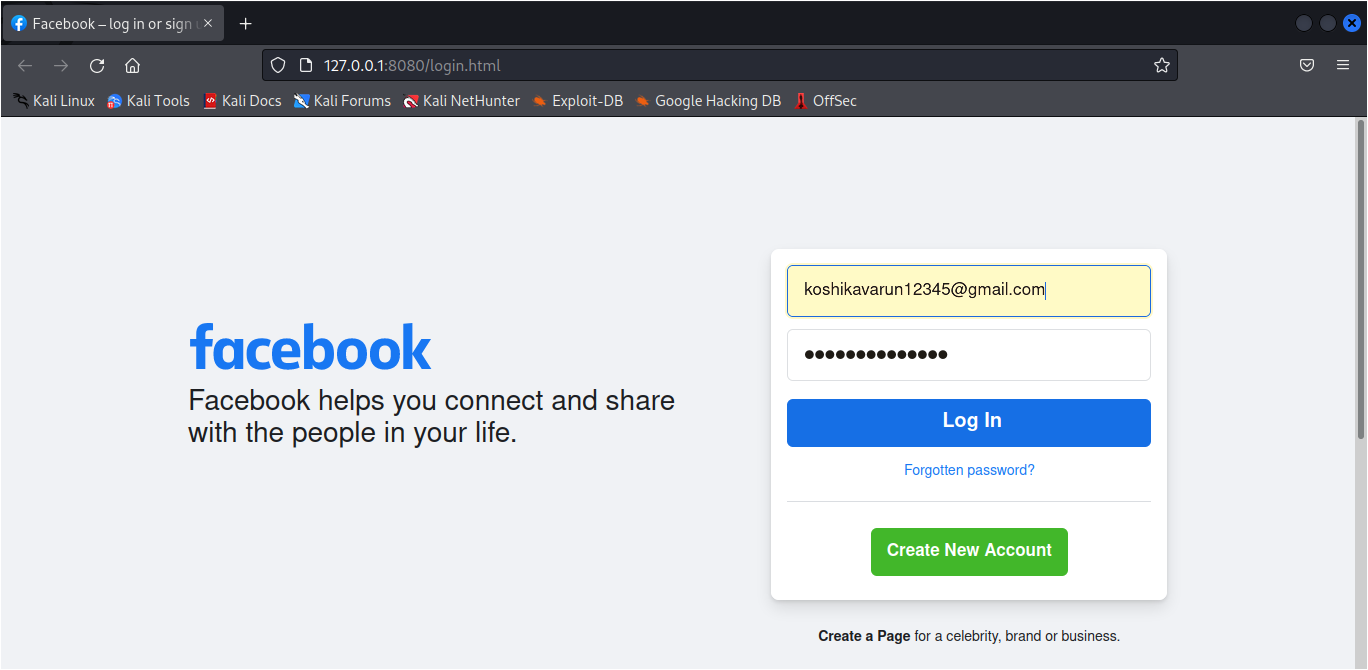
In the vast market of software solutions, there’s certainly a hierarchy of solutions. While enterprise organizations can cover the cost of expensive third-party solutions and might even develop the software further in-house, smaller organizations rightfully work with less or consider free, open-source tools.

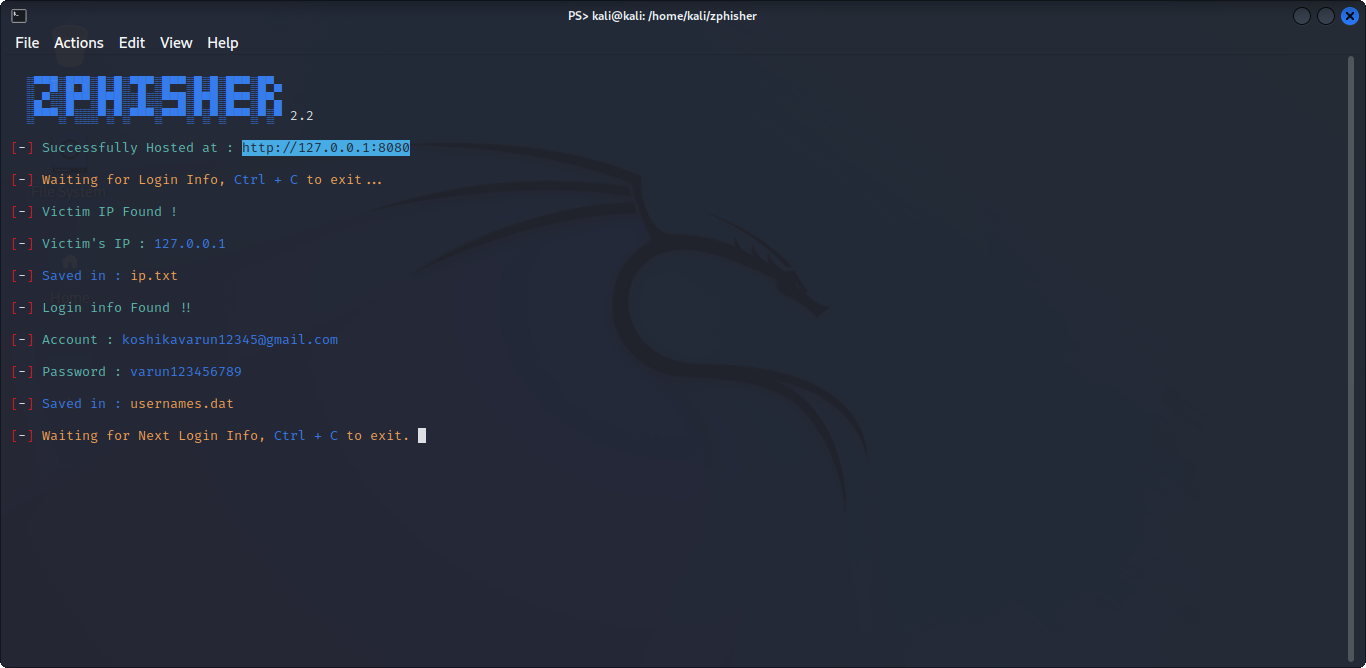
Though, to a great extent, vendor code writers are ultimately responsible for flaws in custom applications for a client. Organizations considering vendors must be keen on this and ensure the contract terms reflect this code review duty.

--------------------------------------------------------------------------------------------------------------------------

**5. Use SET toolkit to perform automation task on phishing and capture the details and write a report on this attack and protection from social engineering attacks**







1. Keep Informed About Phishing Techniques – New phishing scams are being developed all the time. Without staying on top of these new phishing techniques, you could inadvertently fall prey to one. Keep your eyes peeled for news about new phishing scams. By finding out about them as early as possible, you will be at much lower risk of getting snared by one. For IT administrators, ongoing security awareness training and simulated phishing for all users is highly recommended in keeping security top of mind throughout the organization.

2. Think Before You Click! – It’s fine to click on links when you’re on trusted sites. Clicking on links that appear in random emails and instant messages, however, isn’t such a smart move. Hover over links that you are unsure of before clicking on them. Do they lead where they are supposed to lead? A phishing email may claim to be from a legitimate company and when you click the link to the website, it may look exactly like the real website. The email may ask you to fill in the information but the email may not contain your name. Most phishing emails will start with “Dear Customer” so you should be alert when you come across these emails. When in doubt, go directly to the source rather than clicking a potentially dangerous link.

3. Install an Anti-Phishing Toolbar – Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare them to lists of known phishing sites. If you stumble upon a malicious site, the toolbar will alert you about it. This is just one more layer of protection against phishing scams, and it is completely free.

4. Verify a Site’s Security – It’s natural to be a little wary about supplying sensitive financial information online. As long as you are on a secure website, however, you shouldn’t run into any trouble. Before submitting any information, make sure the site’s URL begins with “https” and there should be a closed lock icon near the address bar. Check for the site’s security certificate as well. If you get a message stating a certain website may contain malicious files, do not open the website. Never download files from suspicious emails or websites. Even search engines may show certain links which may lead users to a phishing webpage which offers low cost products. If the user makes purchases at such a website, the credit card details will be accessed by cybercriminals.

5. Check Your Online Accounts Regularly – If you don’t visit an online account for a while, someone could be having a field day with it. Even if you don’t technically need to, check in with each of your online accounts on a regular basis. Get into the habit of changing your passwords regularly too. To prevent bank phishing and credit card phishing scams, you should personally check your statements regularly. Get monthly statements for your financial accounts and check each and every entry carefully to ensure no fraudulent transactions have been made without your knowledge.

6. Keep Your Browser Up to Date – Security patches are released for popular browsers all the time. They are released in response to the security loopholes that phishers and other hackers inevitably discover and exploit. If you typically ignore messages about updating your browsers, stop. The minute an update is available, download and install it.

7. Use Firewalls – High-quality firewalls act as buffers between you, your computer and outside intruders. You should use two different kinds: a desktop firewall and a network firewall. The first option is a type of software, and the second option is a type of hardware. When used together, they drastically reduce the odds of hackers and phishers infiltrating your computer or your network.

8. Be Wary of Pop-Ups – Pop-up windows often masquerade as legitimate components of a website. All too often, though, they are phishing attempts. Many popular browsers allow you to block pop-ups; you can allow them on a case-by-case basis. If one manages to slip through the cracks, don’t click on the “cancel” button; such buttons often lead to phishing sites. Instead, click the small “x” in the upper corner of the window.

9. Never Give Out Personal Information – As a general rule, you should never share personal or financially sensitive information over the Internet. This rule spans all the way back to the days of America Online, when users had to be warned constantly due to the success of early phishing scams. When in doubt, go visit the main website of the company in question, get their number and give them a call. Most of the phishing emails will direct you to pages where entries for financial or personal information are required. An Internet user should never make confidential entries through the links provided in the emails. Never send an email with sensitive information to anyone. Make it a habit to check the address of the website. A secure website always starts with “https”.

10. Use Antivirus Software – There are plenty of reasons to use antivirus software. Special signatures that are included with antivirus software guard against known technology workarounds and loopholes. Just be sure to keep your software up to date. New definitions are added all the time because new scams are also being dreamed up all the time. Anti-spyware and firewall settings should be used to prevent phishing attacks and users should update the programs regularly. Firewall protection prevents access to malicious files by blocking the attacks. Antivirus software scans every file which comes through the Internet to your computer. It helps to prevent damage to your system.

You don’t have to live in fear of phishing scams. By keeping the preceding tips in mind, you should be able to enjoy a worry-free online experience.

Remember there is no single fool-proof way to avoid phishing attacks,