Proof-of-Concept Report:
SSL Labs Analyzer & PhishTool

Overview

This proof-of-concept (PoC) demonstrates how two tools, SSL Labs Analyzer and PhishTool work, and why are they important in SaaS industry.

Tool Name: SSL Labs Analyser

Description:

SSL Labs Analyzer is an online free tool that scans public web servers to assess their SSL/TLS configurations and security. It provides security grading, and highlights vulnerabilities, and offers practical recommendations for improving transport-layer porotection.

Why use this tool?

We should use SSL Labs Analyzer to easily identify SSL/TLS vulnerabilities and misconfigurations in our web servers, ensuring industry-standard encryption and compliance.

Key Characteristics:

- Free, web-based SSL/TLS scanner
- Provides A+ to F security grading
- Detects protocol and cipher suite support
- Highlights certificate chain issues
- Identifies deprecated or insecure configurations
- Presents detailed vulnerability analysis
- Offers remediation recommendations
- Supports API and command-line integration
- Requires no installation or local setup
- Generates shareable technical reports

How SSL Labs Analyzer Supports Cyber Security Officials

- Rapidly identifies SSL/TLS weaknesses across public-facing servers, helping prevent data breaches and protocol exploits.

- Delivers an easily understandable security grade, making it simple to prioritize remediation efforts and communicate risk to non-technical stakeholders.

- Offers detailed technical findings and actionable recommendations, streamlining the patching of vulnerabilities and strengthening compliance posture.

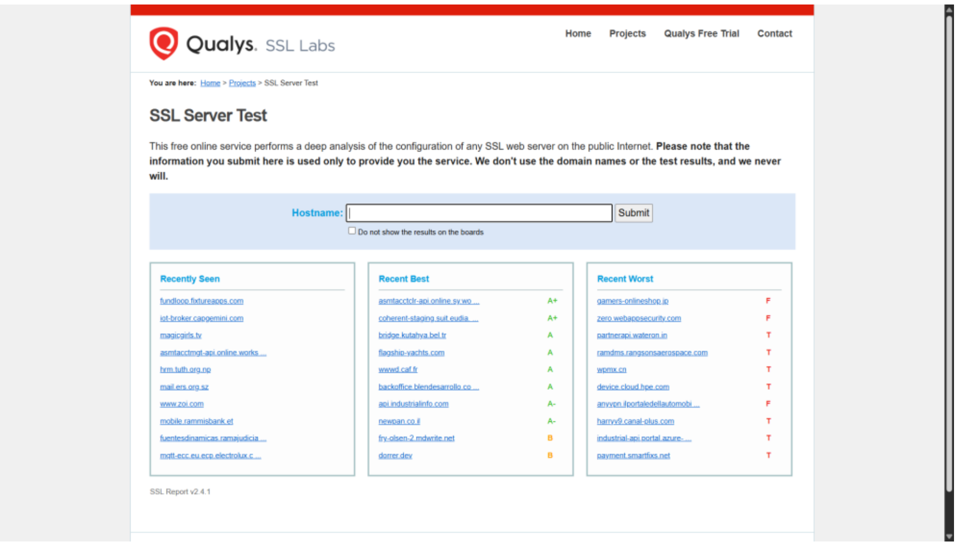
- Supports integration with security automation tools via its API and CLI, enabling continuous monitoring within modern SecOps workflows.

- Facilitates audit readiness by generating shareable reports that document encryption status and risk mitigation actions.

How to use SSL Labs Analyzer?

1. Go to the SSL Labs Analyzer Website

- Visit the SSL Labs Server Test page at: https://www.ssllabs.com/ssltest



You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname: Submit

□ Do not show the results on the boards

Recently Seen

- fundloop.fixtureapps.com
- iot-broker.capgemini.com
- magicgirls.tv
- asmtacctmgt-api.online.works ...
- hrm.tuth.org.np
- mail.ers.org.sz
- www.zoi.com
- mobile.rammisbank.et
- fuentesdinamicas.ramajudicia ...
- mqtt-ecc.eu.ecp.electrolux.c ...

Recent Best	
asmtacctclr-api.online.sy.wo ...	A+
coherent-staging.suit.eudia. ...	A+
bridge.kutahya.bel.tr	A
flagship-yachts.com	A
wwwd.caf.fr	A
backoffice.blendesarrollo.co ...	A
api.industrialinfo.com	A-
newpan.co.il	A-
fry-olsen-2.mdwrite.net	B
dorrer.dev	B

Recent Worst	
gamers-onlineshop.jp	F
zero.webappsecurity.com	F
partnerapi.wateron.in	T
ramdms.rangsonsaerospace.com	T
wpmx.cn	T
device.cloud.hpe.com	T
anyvpn.ilportaledellautomobi ...	F
harryv9.canal-plus.com	T
industrial-api.portal.azure- ...	T
payment.smartfixs.net	T

SSL Report v2.4.1

2. Enter Your Website Address

- In the "Hostname" field, type the domain name of the website you want to check (for example, example.com).

3. Start the Test

- Click the “Submit” button.

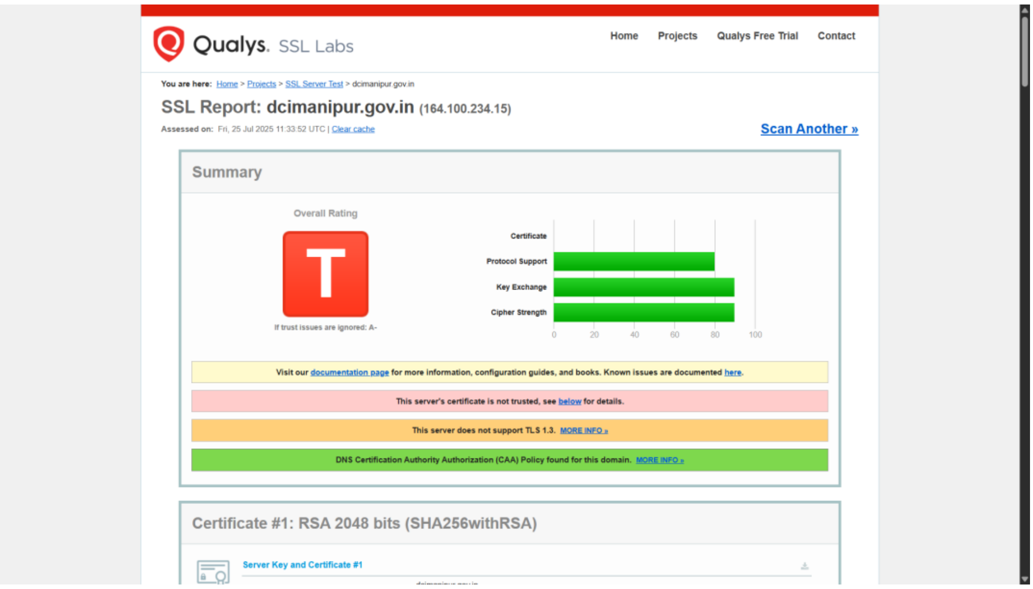
- The analyser will start scanning your website’s SSL/TLS settings.

4. Wait for the Results

- The scan takes a few minutes.
- You can see a progress bar and messages as the test runs.

5. Review the Report

- When finished, you'll see a summary grade (like A+, A, B, etc.).



You are here: Home > Projects > SSL Server Test > dcimanipur.gov.in

SSL Report: dcimanipur.gov.in (164.100.234.15)

Assessed on: Fri, 25 Jul 2025 11:33:52 UTC | Clear cache

Scan Another »

Summary

If trust issues are ignored: A-

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server's certificate is not trusted, see below for details.

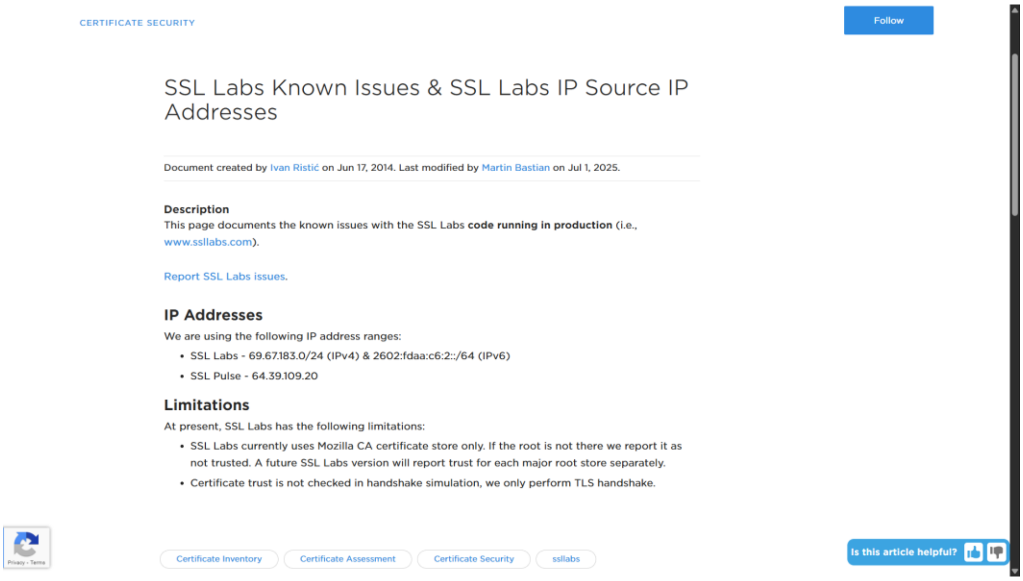
This server does not support TLS 1.3. MORE INFO »

DNS Certification Authority Authorization (CAA) Policy found for this domain. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

- Check the details below for:
  - Supported SSL/TLS versions
  - Cipher suites (encryption methods)
  - Certificate status (valid, expired, trusted, etc.)
  - Vulnerabilities or weak settings



SSL Labs Known Issues & SSL Labs IP Source IP Addresses

Document created by Ivan Ristić on Jun 17, 2014. Last modified by Martin Bastian on Jul 1, 2025.

Description

This page documents the known issues with the SSL Labs **code running in production** (i.e., www.ssllabs.com).

Report SSL Labs issues.

IP Addresses

We are using the following IP address ranges:

- SSL Labs - 69.67.183.0/24 (IPv4) & 2602:fdaa:c6:2::/64 (IPv6)
- SSL Pulse - 64.39.109.20

Limitations

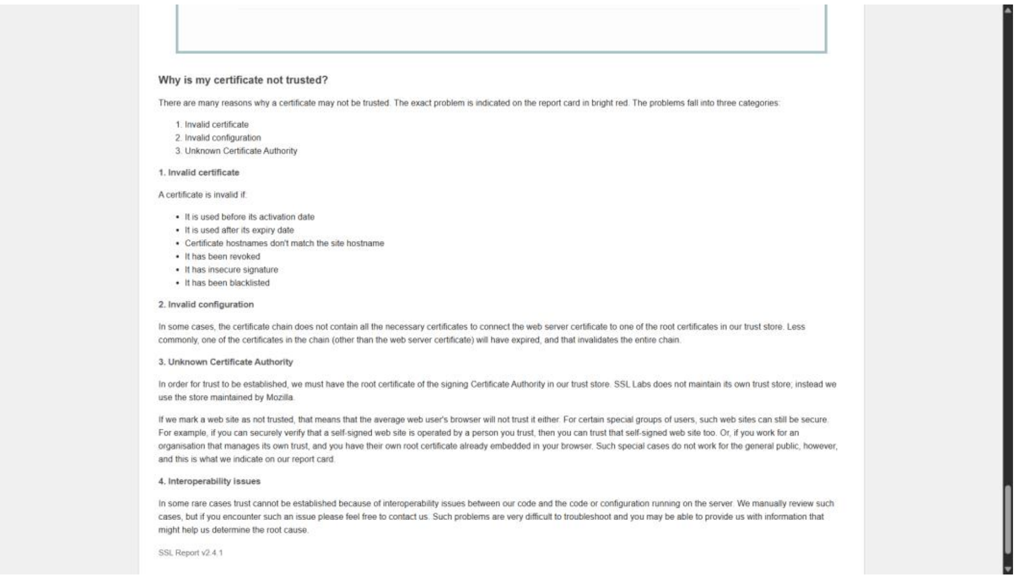
At present, SSL Labs has the following limitations:

- SSL Labs currently uses Mozilla CA certificate store only. If the root is not there we report it as not trusted. A future SSL Labs version will report trust for each major root store separately.
- Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

This link can be referred to for the known issues that might exist: click me

6. Use the Recommendations

- Issues will be highlighted in the results.
- Read the suggestions for how to fix problems (like disabling old protocols or updating certificates).



Why is my certificate not trusted?

There are many reasons why a certificate may not be trusted. The exact problem is indicated on the report card in bright red. The problems fall into three categories:

1. Invalid certificate
2. Invalid configuration
3. Unknown Certificate Authority

1. Invalid certificate

A certificate is invalid if:

- It is used before its activation date
- It is used after its expiry date
- Certificate hostnames don't match the site hostname
- It has been revoked
- It has insecure signature
- It has been blacklisted

2. Invalid configuration

In some cases, the certificate chain does not contain all the necessary certificates to connect the web server certificate to one of the root certificates in our trust store. Less commonly, one of the certificates in the chain (other than the web server certificate) will have expired, and that invalidates the entire chain.

3. Unknown Certificate Authority

In order for trust to be established, we must have the root certificate of the signing Certificate Authority in our trust store. SSL Labs does not maintain its own trust store; instead we use the store maintained by Mozilla.

If we mark a web site as not trusted, that means that the average web user's browser will not trust it either. For certain special groups of users, such web sites can still be secure. For example, if you can securely verify that a self-signed web site is operated by a person you trust, then you can trust that self-signed web site too. Or, if you work for an organisation that manages its own trust, and you have their own root certificate already embedded in your browser. Such special cases do not work for the general public, however, and this is what we indicate on our report card.

4. Interoperability issues

In some rare cases trust cannot be established because of interoperability issues between our code and the code or configuration running on the server. We manually review such cases, but if you encounter such an issue please feel free to contact us. Such problems are very difficult to troubleshoot and you may be able to provide us with information that might help us determine the root cause.

SSL Report v2.4.1

7. Save or Share the Report

- You can bookmark the results or download a PDF for future reference or sharing with your team.

When Should We Use SSL Labs Analyzer?

- **After Configuring or Updating SSL/TLS Settings:** Run a scan whenever we deploy a new web server, update certificates, or change encryption settings.
- **During Regular Security Audits:** Integrate as part of scheduled security reviews to ensure ongoing compliance and hygiene.
- **Before Launching Public-Facing Services:** Test SSL/TLS for new websites, APIs, or applications prior to going live.
- **When Notified of New Vulnerabilities:** Check proactively when major vulnerabilities (like Heartbleed, ROBOT) are reported.
- **If Compliance Is Required:** Use it to validate settings for standards (e.g., PCI DSS, GDPR, HIPAA) that mandate secure transport.
- **After Remediation:** Rerun tests after fixes to confirm problems (such as weak ciphers or expired certificates) are resolved.

Who Should Use SSL Labs Analyzer?

- **Cybersecurity and IT Security Teams:** To assess, monitor, and improve encryption posture of public servers.

- **DevOps and System Administrators:** To validate SSL/TLS configurations during deployment, patching, and maintenance.
- **Compliance and Risk Officers:** To document secure transport-layer configurations for audits and governance.
- **Site Owners and Webmasters:** To quickly check if their websites are secure and trustworthy for users.
- **Penetration Testers and Security Auditors:** As part of vulnerability assessments and reporting for clients.

Summary Table: Usage Scenarios

Role	When to Use	Purpose
Security Team	Periodic/after changes/vulnerability announcements	Maintain secure configurations
Sysadmin/DevOps	After server or certificate updates	Prevent misconfigurations
Auditors/Compliance	Before/during audits	Meet regulatory standards
Website Owners	Before launch/after fixes	Ensure user trust and safety
Pen Testers	During assessments	Document transport-layer weaknesses

In fact, any web developer can utilize this tool to make their websites secure. And companies should hire cyber security officials to ensure their integrity.

Advantages

- **Comprehensive SSL/TLS Testing:** Assesses all major aspects of SSL/TLS implementation, including protocol support, cipher suites, certificate chains, and known vulnerabilities.
- **Actionable Grading:** Provides an easy-to-understand letter grade (A+ to F), making it straightforward to interpret risk and track progress.
- **Free and Web-Based:** No installation or account required; accessible from any browser.
- **Detailed Reports:** Offers in-depth technical breakdowns, remediation advice, and shareable reports suitable for audit and compliance documentation.
- **Automation Support:** Provides APIs and command-line tools for integration into CI/CD and continuous monitoring workflows.
- **Regular Updates:** Maintains tests for emerging vulnerabilities (like Heartbleed, ROBOT), helping organizations stay up to date.
- **Widely Trusted:** Recognized standard referenced in security best practices and compliance audits.

Flaws and Limitations

- **External-Only Testing:** Only tests publicly accessible hosts; cannot assess internal servers or environments behind firewalls without temporary public exposure.
- **Surface-Level Automation:** While actionable, the tool identifies issues but doesn't automate remediation or configuration changes.
- **Occasional Test Delays:** High demand can cause scan queues, leading to delays in obtaining results, especially for popular or large domains.
- **Limited Contextual Insight:** The tool identifies technical SSL/TLS weaknesses but does not correlate findings with business risk or real-world threat scenarios.
- **Not a Full Vulnerability Scanner:** SSL Labs focuses solely on transport security; it does not test for web application vulnerabilities, misconfigurations outside SSL/TLS, or broader server security issues.
- **Best for Standard Deployments:** Some results and recommendations may not account for unique, non-default configurations or specialized enterprise needs.
- **Potential False Positives/Negatives:** Certain edge cases or advanced setups (like custom load balancers/proxies) may not be properly interpreted, possibly resulting in errors or incomplete findings.

Tool Name: PhishTool

Description:

PhishTool is a cloud-based tool that helps cybersecurity teams quickly analyze suspicious emails. It automatically looks inside emails to find signs of phishing, like fake links or harmful attachments, and creates easy-to-understand reports to help stop email attacks faster — all without needing to install anything on your computer.

Why use this tool?

We should use PhishTool because it helps quickly find and understand phishing emails to keep our systems safe. It automatically checks emails for fake links and harmful attachments without needing install. This speeds up the response and protects users from email attacks.

Key Characteristics:

- Cloud-based phishing email analysis and response platform
- Automates extraction and enrichment of email metadata, headers, attachments, and URLs

- Integrates threat intelligence and OSINT for deep phishing campaign analysis
- Provides detailed forensic reports and IoC (Indicators of Compromise) extraction
- Supports Microsoft 365 and Google Workspace mailbox integration for automated email ingestion
- Enables team collaboration with real-time analysis updates and case management
- Offers browser-based usage with no local installation required
- Includes automated phishing alert processing with classification and prioritization
- Supports integration with third-party APIs and SOAR tools for workflow automation
- Designed to speed up triage, reduce analyst workload, and improve phishing incident response effectiveness

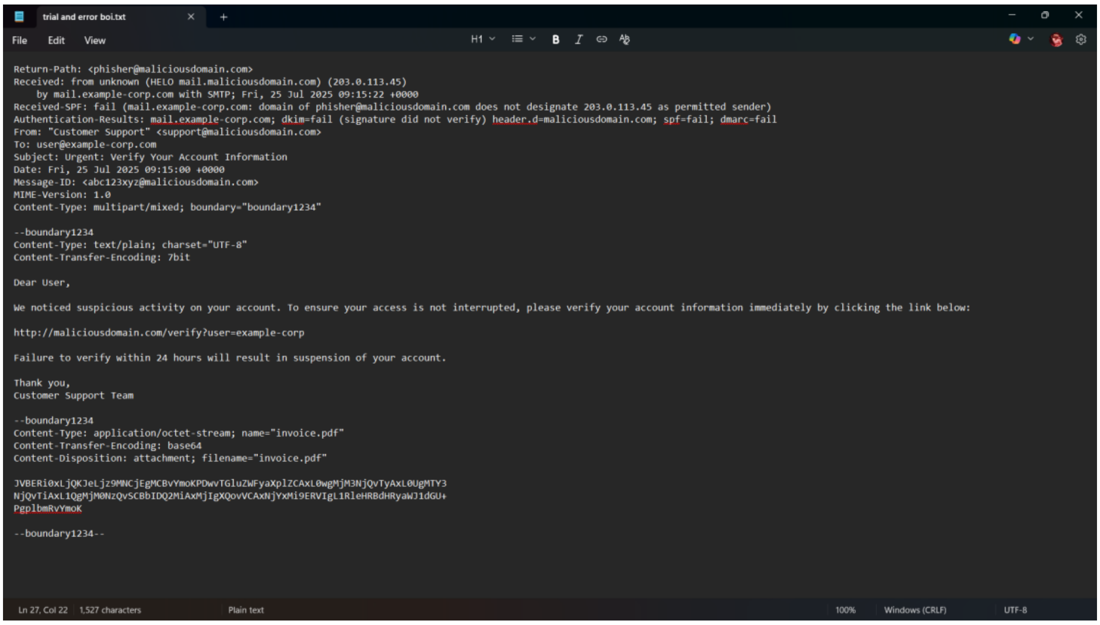
How PhishTool Helps Cybersecurity Professionals

- Rapid detection of phishing emails
- Automated extraction of indicators of compromise (IoCs)
- Reduces analyst workload and manual investigation
- Integrates with security tools and workflows
- Supports team collaboration and case management
- Provides detailed forensic reports
- Enables faster incident response and containment
- Enhances threat intelligence with external data sources

How to Use PhishTool:

1. Get Your Suspicious Email Ready

- Save the suspicious email (usually from your inbox or mail client) as a file—formats like .eml or .msg work best.



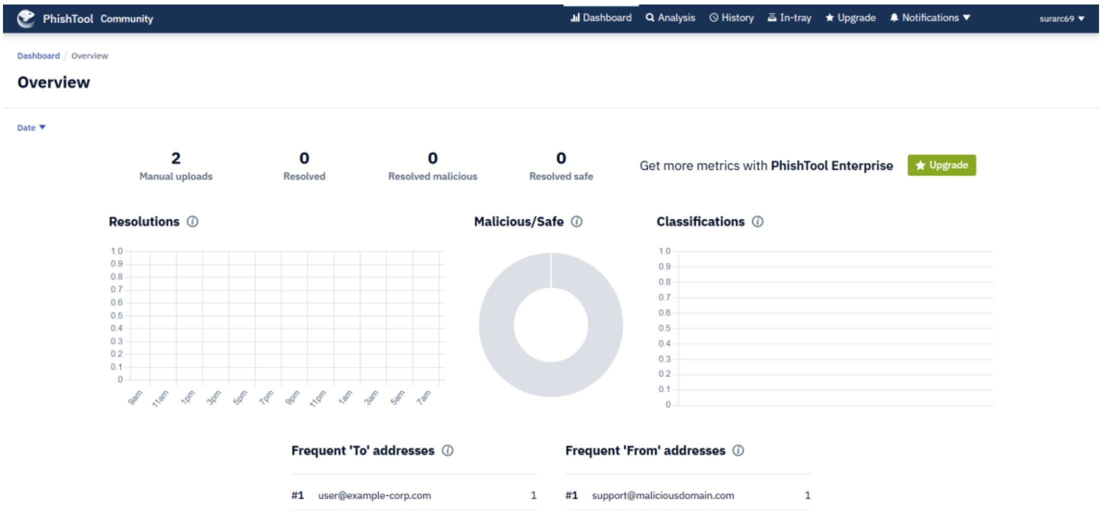
```
Return-Path: <phisher@maliciousdomain.com>
Received: from unknown (HELO mail.maliciousdomain.com) (203.0.113.45)
    by mail.example-corp.com with SMTP; Fri, 25 Jul 2025 09:15:22 +0000
Received-SPF: fail (mail.example-corp.com: domain of phisher@maliciousdomain.com does not designate 203.0.113.45 as permitted sender)
Authentication-Results: mail.example-corp.com; dkim=fail (signature did not verify) header.d=maliciousdomain.com; spf=fail; dmarc=fail
From: "Customer Support" <support@maliciousdomain.com>
To: user@example-corp.com
Subject: Urgent: Verify Your Account Information
Date: Fri, 25 Jul 2025 09:15:00 +0000
Message-ID: <abc123xyz@maliciousdomain.com>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="boundary1234"

--boundary1234
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 7bit

Dear User,

We noticed suspicious activity on your account. To ensure your access is not interrupted, please verify your account information immediately by clicking the link below:

http://maliciousdomain.com/verify?user=example-corp

Failure to verify within 24 hours will result in suspension of your account.

Thank you,
Customer Support Team

--boundary1234
Content-Type: application/octet-stream; name="invoice.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="invoice.pdf"

JVBERi0xLjQKJeLjz9MNCjEgMCBvYmoKPDwvTGluZWFyaXplZCAxL0wgMjM3NjQvTyAxL0UgMTY3
NjQvTiAxL1QgMjM0NzQvSCBbIDQ2MiAxMjIgXQovVCAxNjYxMi9ERVIgL1RleHRBdHRyaWJ1dGU+
PgplbmRvYmoK

--boundary1234--
```

- Make sure the file includes all parts of the email: headers, body, and any attachments.

2. Open PhishTool in Your Browser

- Go to the PhishTool website.

- Log in with your account if needed—no installation is required because it's all cloud-based.



Overview

2	0	0	0
Manual uploads	Resolved	Resolved malicious	Resolved safe

Get more metrics with **PhishTool Enterprise**

Resolutions

Malicious/Safe

Classifications

Frequent 'To' addresses

#1	user@example-corp.com	1

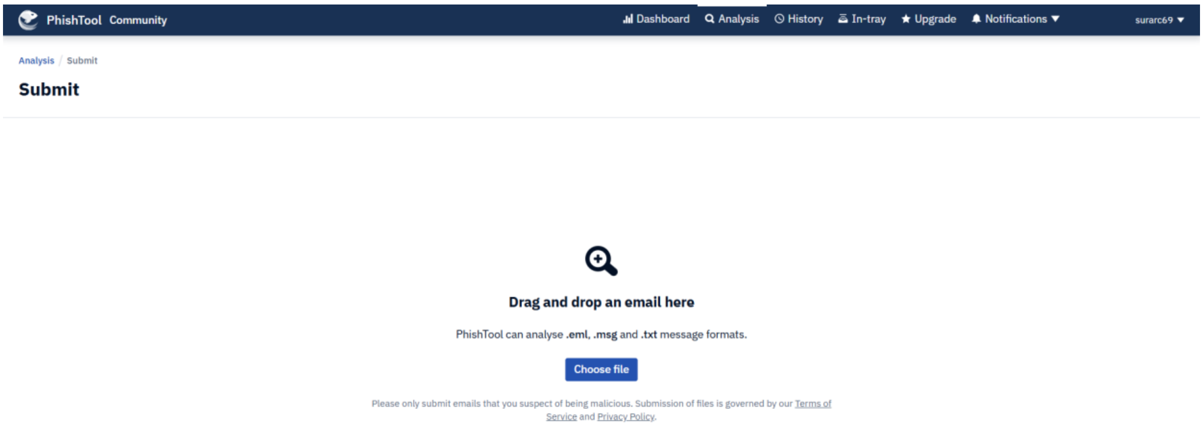
Frequent 'From' addresses

#1	support@maliciousdomain.com	1

3. Upload the Email for Analysis

- Find the section or button labelled "Submit" or "Upload Email."

- Drag and drop the email file or click to browse and select it from your computer.



Submit

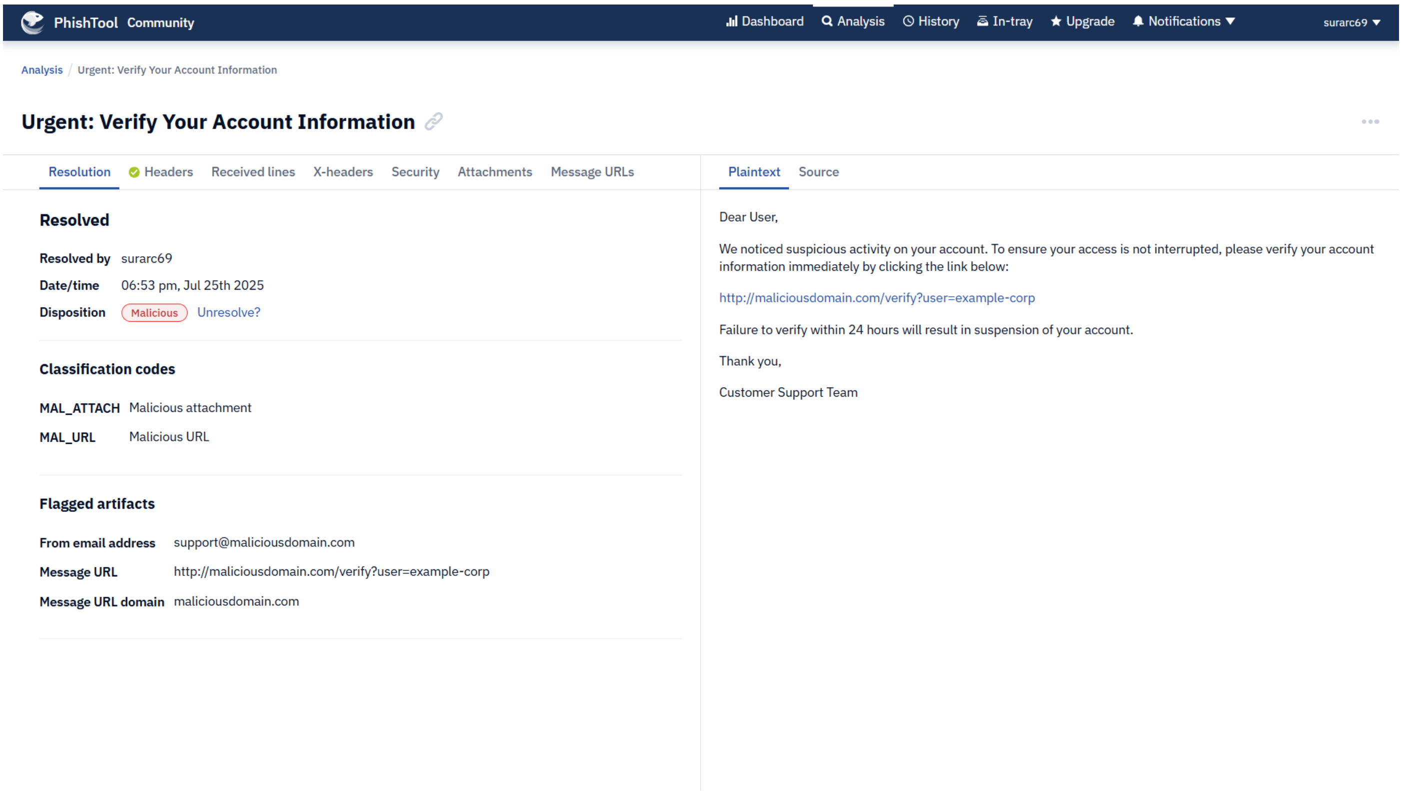
Drag and drop an email here

PhishTool can analyse **.eml**, **.msg** and **.txt** message formats.

Please only submit emails that you suspect of being malicious. Submission of files is governed by our Terms of Service and Privacy Policy.

4. Let PhishTool Analyse the Email

- The platform will quickly scan the uploaded email.
- It checks for fake links, suspicious attachments, spoofed addresses, and failed security checks.



Urgent: Verify Your Account Information

Resolved

Resolved by surarc69

Date/time 06:53 pm, Jul 25th 2025

Disposition Malicious Unresolve?

Classification codes

MAL_ATTACH	Malicious attachment
MAL_URL	Malicious URL

Flagged artifacts

From email address	support@maliciousdomain.com
Message URL	http://maliciousdomain.com/verify?user=example-corp
Message URL domain	maliciousdomain.com

Dear User,

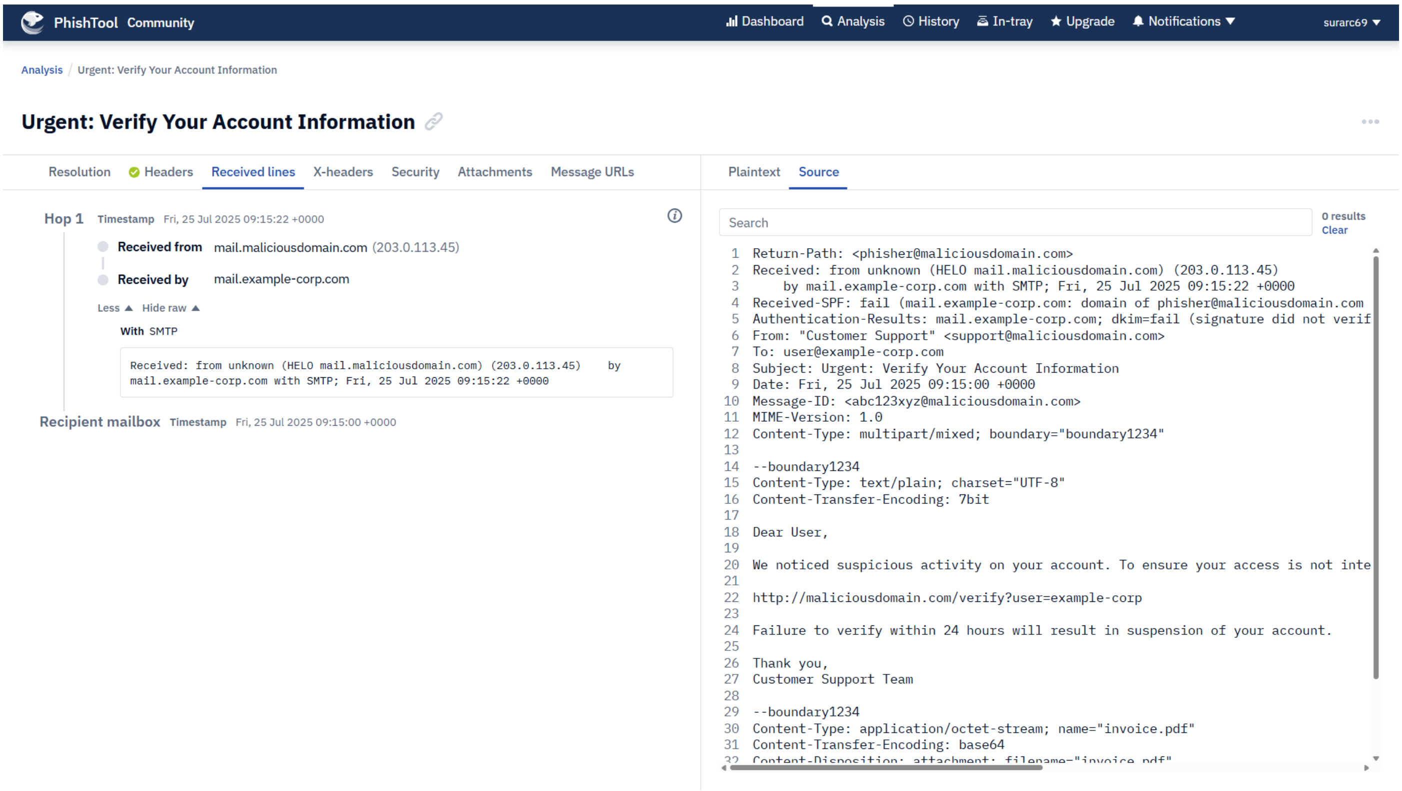
We noticed suspicious activity on your account. To ensure your access is not interrupted, please verify your account information immediately by clicking the link below:

http://maliciousdomain.com/verify?user=example-corp

Failure to verify within 24 hours will result in suspension of your account.

Thank you,

Customer Support Team



Urgent: Verify Your Account Information

Hop 1 Timestamp Fri, 25 Jul 2025 09:15:22 +0000

Received from mail.maliciousdomain.com (203.0.113.45)

Received by mail.example-corp.com

With SMTP

```
Received: from unknown (HELO mail.maliciousdomain.com) (203.0.113.45)    by
mail.example-corp.com with SMTP; Fri, 25 Jul 2025 09:15:22 +0000
```

Recipient mailbox Timestamp Fri, 25 Jul 2025 09:15:00 +0000

```
Return-Path: <phisher@maliciousdomain.com>
Received: from unknown (HELO mail.maliciousdomain.com) (203.0.113.45)
    by mail.example-corp.com with SMTP; Fri, 25 Jul 2025 09:15:22 +0000
Received-SPF: fail (mail.example-corp.com: domain of phisher@maliciousdomain.com
Authentication-Results: mail.example-corp.com; dkim=fail (signature did not verif
From: "Customer Support" <support@maliciousdomain.com>
To: user@example-corp.com
Subject: Urgent: Verify Your Account Information
Date: Fri, 25 Jul 2025 09:15:00 +0000
Message-ID: <abc123xyz@maliciousdomain.com>
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="boundary1234"

--boundary1234
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 7bit

Dear User,

We noticed suspicious activity on your account. To ensure your access is not inte

http://maliciousdomain.com/verify?user=example-corp

Failure to verify within 24 hours will result in suspension of your account.

Thank you,
Customer Support Team

--boundary1234
Content-Type: application/octet-stream; name="invoice.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="invoice.pdf"
```

5. Review the Results

- You'll see a summary page showing if the email is safe, suspicious, or malicious.
- Look at the key details: flagged links, domains, malicious attachments, or any email authentication failures (like SPF/DKIM/DMARC).

6. Take Action Based on the Findings

- If the email is flagged as phishing, use the provided details (malicious link, sender address, etc.) to block threats or alert your IT/security team.
- Export or download the analysis report if you need it for records or compliance.

7. Repeat as Needed or Batch Upload

- You can scan more emails by uploading them one by one, or (if your setup allows) connect PhishTool with your company's mailbox for automatic scanning.

Tip:

All steps happen in your browser—no software to install, and you can use PhishTool from any device connected to the internet. It's designed for simplicity so anyone in a security or IT role can investigate suspicious emails fast and easily.

When Should We Use PhishTool?

- **When we receive a suspicious or strange email:** Anytime we or our team gets an email that looks like it might be a phishing attempt, scam, or contains unusual links or attachments.

- **During regular security checks:** Use PhishTool to scan emails reported by employees or picked up by our mail security system.

- **Before opening unknown attachments or links:** Always check potentially risky emails with PhishTool to avoid accidental infections.

- **After new phishing threats are announced:** If there's news about a phishing campaign, scan similar emails to stay protected.

- **While investigating security incidents:** Use PhishTool to analyse emails as part of incident response to quickly spot threats.

Who Should Use PhishTool?

- **IT and Cybersecurity Teams:** For fast analysis and response to suspicious emails in organizations.

- **Security Operations Center (SOC) analysts:** To automate phishing investigation, reduce manual work, and improve detection.

- **System administrators:** To validate user-reported suspicious emails and stop possible breaches.

- **Any employee or user:** Anyone unsure about an email's safety can use PhishTool to get a quick verdict (if permitted in your company).

Advantages

- Quickly analyses suspicious emails for phishing threats

- Automates detection of malicious links, attachments, and fake senders

- Easy to use—cloud-based with no installation needed

- Integrates with Microsoft 365, Google Workspace, and threat intelligence sources

- Provides detailed forensic reports and indicators for blocking threats

- Reduces manual work for security teams

- Speeds up response to phishing incidents

- Helps teams collaborate on investigations

Flaws

- Only works with emails you can upload—doesn't automatically scan all inboxes unless integrated

- Requires an internet connection (cloud-based; not usable offline)

- May miss very new or highly advanced phishing tricks if threat intelligence isn't updated

- Some features (bulk analysis, advanced integrations) may need paid version
- Not a full security suite—focuses mainly on email analysis, not full endpoint protection
- Occasional false positive or false negative results, like all automated tools

In conclusion, both SSL Labs Analyzer and PhishTool are powerful allies for anyone striving to be a better cybersecurity researcher. By using SSL Labs Analyzer, we can easily spot weaknesses in how websites protect information in transit—helping us learn what strong, modern encryption should look like and how to fix common mistakes. PhishTool, on the other hand, gives us hands-on practice with real phishing emails, letting us quickly dissect suspicious messages, find hidden threats, and see exactly how attackers try to trick users. Together, these tools sharpen our ability to think like both a defender and an investigator: they teach us where security gaps often appear, encourage critical analysis, and give us practical ways to improve the digital defences of any organization. In short, they make us smarter, faster, and more effective at protecting people and data in today's digital world.

Date: 25th July 2025

Author: Adwitya Deep Verma

Purpose: Assignment as an intern at Digisuraksha Parhari Foundation.