DIGITAL RISK CHECK

DIGITAL RISK CHECK REPORT FOR

Your Domain

www.your-domain.com

Digital Risk Check checks the security posture of www.your-domain.com using a set of important asser on checks.

The generated report can help you in gauging how secure your platform is and the severity of the risks, thereby helping you to solve them quickly. Our tool groups security into four main aspects, namely, Domain, Email, Application, and Network.

Each security aspect will include a couple of asser on checks that drill deep into minute factors in your environment. The report will include the status of each assersion check as well as an overall cyber rating score, that helps you to assess how critcal the situation is.

79
Score

B

www.your-domain.com

Generated on:

Threat Indicators

A Domain Security

The domain represents your brand and any attack on it can cause financial burden, data loss, and can tarnish your brand's reputation. It is essential to ensure that your domain is safe and isn't prone to any cyber attacks.

C Email Security

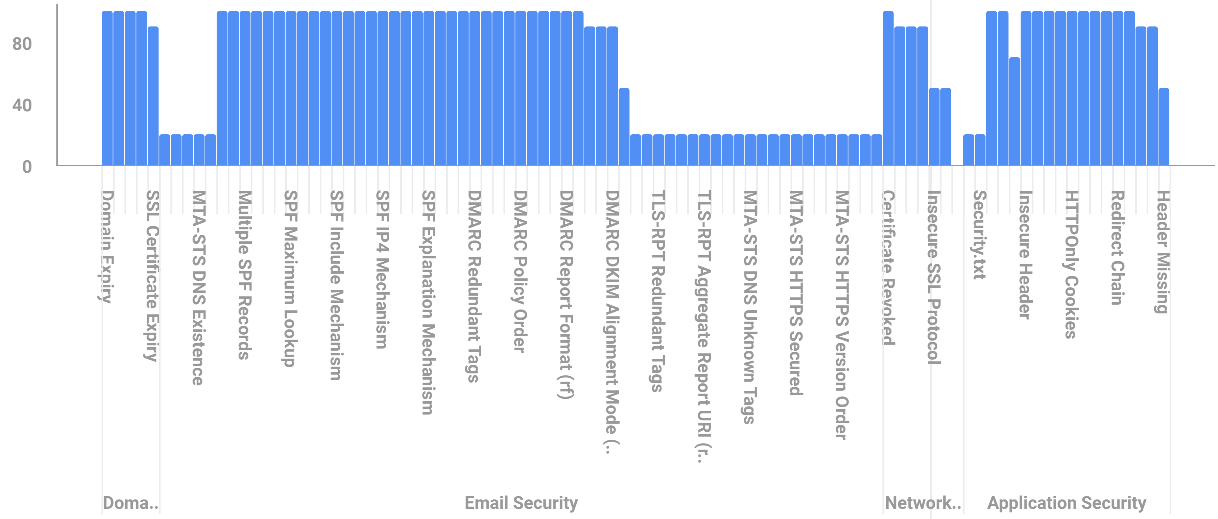
SPF, DKIM and DMARC are simply a set of email authentication methods to prove to ISPs and mail services that senders are truly authorized to send email from a particular domain and, are a way of verifying your email sending server is sending emails through your domain.

C Network Security

With copious amounts of data online and growing number of cyber threats, it is essential to secure the user data by building a secure and stable network. Network security includes the steps that can be taken to ensure the reliability and integrity of all data in a network.

B+ Application Security

Most of the cyber attackers target the vulnerabilities in the application layer. With the enhanced complexity of the application tier, it is essential to test applications for their security. Application security can be ensured by constantly tracking the headers, by checking for any malware injections, defacement attacks, and much more.



Top Assertions

Assertion	Priority
DMARC Policy	High
DMARC Subdomain Policy (sp)	High
TLS-RPT Existence	High
MTA-STS DNS Existence	High
MTA-STS HTTPS Existence	High
Insecure Component Header	High
Security.txt	High
Upper Case in SPF Records	Medium
Insecure SSL Protocol	Medium
Insecure Cipher	Medium

A

Domain Security 98

The domain represents your brand and any attack on it can cause financial burden, data loss, and can tarnish your brand's reputation. It is essential to ensure that your domain is safe and isn't prone to any cyber attacks.

! SSL Certificate Expiry

A site with an expired SSL Certificate will be inaccessible for visitors and it'll be prone to many vulnerabilities. Hence, it is important to stay updated on the expiry dates of your certificates and to get them updated before the date of expiry.

Using this check, Digital Risk Check will track the expiry date of your certificates and will ensure their validity.

Host	Port	Days Left for Expiry
www.your-domain.com	443	87

✓ Domain Expiry

To maintain domain ownership, it is essential to renew the domain name before it expires. Once a domain expires, the domain will deactivated and parked. Once it is deactivated, you will not be allowed to make any changes, neither will the customers be able to access it, leading to negative impacts on your business and brand.

Using this check, Digital Risk Check will track your domain expiry date and the number of days left for expiry.

Registered Domain	Days Left for Expiry
your-domain.com	294

✓ Blocklisted Domain

A blocklist will contain the list of IPs, domains, or email addresses that were reported for spam or any other malicious activity. A blocklisted domain will face a huge drop in the number of visitors and will be marked unsafe leading to a tarnished brand reputation.

Using this check, Digital Risk Check will cross-verify your domain against the popular blocklists to ensure that your domain isn't flagged as a blocklisted one.

Registered Domain	Count	Blocklisted Domains	Reason
www.your-domain.com	0	-	-

✓ Blocklisted IP

An IP address can end up in the blocklist for spamming or for sending numerous messages. All the emails you send from a blocklisted IP will end up in spam or bounce in turn affecting the credibility of your brand. Prevention of DDoS attacks is one of the main intentions of blocklisting IPs.

Digital Risk Check will check your IP address against the popular blocklists databases to verify whether your IP is listed there or not.

Registered Domain	Count	Blocklisted IPs	Reason
www.your-domain.com	0	-	-

✓ Certificate Authority Authorization Check

The check verifies whether the domain contains a valid Certification Authority Authorization (CAA) record. CAA records indicate which Certificate Authorities (CAs) are authorized to issue certificates for a domain.

No issues found

Email Security 64

SPF, DKIM and DMARC are simply a set of email authentication methods to prove to ISPs and mail services that senders are truly authorized to send email from a particular domain and, are a way of verifying your email sending server is sending emails through your domain.

DMARC Policy

A DMARC policy allows the recipient to filter out valid and legitimate emails. If the email is from a non-approved sender, the DMARC policy advises them on how to respond to avoid further threats. The policy tag includes how requests will be handled for the domain and will have three policy options, none, quarantine, and reject. It is a mandatory tag.

Digital Risk Check will check whether the policy is configured in the right way or not.

Record	Policy	Reason
p=none	None	None has no effect on the DMARC record. Make it as reject for better security.

DMARC Subdomain Policy (sp)

The DMARC policy applied to the organization is applicable for the subdomains too. But, it is possible to set separate policies for the subdomains by using the 'sp' tag. If absent, the policy specified by the 'p' tag will be applied for subdomains.

Digital Risk Check will check for the presence of sp tag in the record and will ensure that it's configured with the correct value.

Record	Subdomain Policy	Reason
sp=none	None	None has no effect on the DMARC record. Make it as reject for better security.

TLS-RPT Existence

This check tracks whether there is a TLS-RPT record for the given domain. Further checks will be done if it is found.

Record
-

No issues found

MTA-STS DNS Existence

This check tracks whether there is an MTA-STS record for the given domain in the DNS. Further checks will be done if the record exists.

Record
-

No issues found

!!! MTA-STS HTTPS Existence

Mail Transfer Agent-Strict Transport Security (MTA-STS) HTTPS Existence check analyses whether there is an MTA-STS record for the given domain in the text format. The record should be a part of the URL, https://mta-sts.YOUR-DOMAIN/.well-known/mta-sts.txt. If the record is found, other checks will be done.

Record
-

No issues found

!! Upper Case in SPF Records

An SPF record shouldn't contain upper-casing. This checks ensures whether the SPF record of the domain have any uppercase characters or not. It is best to stick to lower case for the record.

Record
v=spf1 include:xxxxx.com +a +mx +a:xxxxx.com -all

! DMARC Failure Report (fo)

The DMARC Failure Reporting Options (fo) decide what types of reports should be sent out. This is a DMARC tag with the default value 0. Failure reporting options provide requested options for generation of failure reports.

Digital Risk Check will check for the presence of the fo tag to ensure that the failure reporting options are configured correctly.

Record	Failure option	Reason
fo=0	Both	The default value for fo is 0 and the best value will be 1 (any).

! DMARC SPF Alignment Mode (aspf)

This tag refers to the SPF identifier alignment section of the domain policy and indicates whether the domain owner has opted for a strict (s) or relaxed (r) SPF Identifier Alignment mode.

Digital Risk Check will check for the presence of the aspf tag in the record to ensure that the values are valid.

Record	ASPF record	Reason
aspf=r	Relaxed	The alignment can be removed. By default, it is r(Relaxed). For better security, try to use s(strict).

DMARC DKIM Alignment Mode (adkim)

This tag refers to the DKIM Identifier Alignment section of the domain policy and indicates whether the domain owner has opted for a strict (s) or relaxed (r) DKIM Identifier Alignment mode.

Digital Risk Check will check for the presence of the adkim tag in the record to ensure that the values are valid.

Record	ADKIM record	Reason
adkim=r	Relaxed	The alignment can be removed. By default, it is r(Relaxed). For better security, try to use s(strict).

Email Server Certificate

Mail servers are responsible for receiving, routing, and delivering e-mail. This check ensures correct configuration, Starttls support, valid certificates, and its expiry.

Priority	MX Server	IPv4	IPv6	Connection	Certificate	Days Left for Expiry
10	mx.xxxx.com	11.22.333.444	-	✓ STARTTLS	✓ Valid	‼ 59
20	mx2.xxxx.com	11.22.333.444	-	✓ STARTTLS	✓ Valid	‼ 59
50	mx3.xxxx.com	11.22.333.444	-	✓ STARTTLS	✓ Valid	‼ 59

SPF Existence

This check is carried out to ensure whether there are any SPF records present for a domain. Further checks will be done if records exist.

Record
v=spf1 include:xxxx.com +a +mx +a:Server.xxxx.com -all
v=spf1 include:spf.xxxx.com -all
v=spf1 ip4:111.11.111 ip4:22.222.22.222 ip4:333.333.333 ip4:444.444.444 ~all

Multiple SPF Records

A domain name should not contain multiple records. Having multiple SPF records can make your emails fail the SPF authentication tests.

This check helps to ensure whether there is more than one SPF record available for your domain.

No issues found

✓ Extra Space in SPF Record

This check tracks extra spaces in the SPF record of the domain. There are chances that an extra space can be considered as a null record. As it might cause breakage, it is best to remove extra spaces.

No issues found

✓ SPF Unknown Terms

Checks whether the SPF record has any unknown terms. All terms except version(v), all, include, a, mx, ptr, ip4, ip6, exists, redirect, explanation (exp) will be considered as unknown terms.

No issues found

✓ SPF Mechanisms after "all"

This check tracks whether there are mechanisms after "all" in the SPF record. The "all" mechanism specifies whether the incoming messages match or not. All the mechanisms that come after "all" will be ignored.

No issues found

✓ SPF Maximum Lookup

The SPF framework has a threshold limit of 10 DNS lookups to resolve a record. This check analyses whether there are more than 10 lookups in the SPF record. DNS lookups up to 10 per SPF record is allowed, which includes lookups caused by the use of terms like redirect, include, a, mx, ptr, and exists.

No issues found

✓ Redundant SPF Terms

This check identifies redundant terms in the SPF record. The presence of redundant terms can lead to a Permerror..

No issues found

✓ Recursive SPF Redirect

This check detects recursive redirects in the SPF record which can exceed the lookup limits.

No issues found

✓ SPF version

The SPF version tag indicates the SPF protocol version that is mandatory to identify the SPF record's version. This check ensures that the SPF record contains a valid version tag.

No issues found

✓ SPF Include Mechanism

This includes the SPF record of another domain. This check examines the presence of the Include mechanism in the SPF record and verifies the included domain's SPF record.

No issues found

✓ SPF A Mechanism

This mechanism adds domains' IPs and their IP CIDR ranges to the SPF record, if mentioned. This check ensures that the A mechanism in the SPF record is valid and validates the domain's IP address.

No issues found

✓ SPF MX Mechanism

This mechanism includes MX records of specified domains or their CIDR ranges for sending mail on behalf of the domain. This check validates the MX mechanism in the SPF record and checks the MX records of the domain.

No issues found

✓ SPF PTR Mechanism

The PTR mechanism is deprecated. This check identifies the presence of PTR mechanisms in the SPF record.

No issues found

✓ SPF IP4 Mechanism

This mechanism allows specific IP addresses or CIDR ranges to send mail on behalf of the domain. Verify the IP4 mechanisms in the SPF record.

No issues found

✓ SPF IP6 Mechanism

The IP6 mechanism permits specific IP addresses or CIDR ranges to send mail on behalf of the domain. Verify the presence of IP6 mechanisms in the SPF record.

No issues found

✓ SPF Exists Mechanism

This mechanism checks for an A record in the specified domain. If it exists, then the mechanism matches; otherwise, it fails.

No issues found

✓ SPF Redirect Mechanism

This mechanism redirects the SPF record of the domain to another domain. This check verifies the presence of Redirect mechanisms in the SPF record and validate the SPF record of the redirected domain.

No issues found

✓ SPF Explanation Mechanism

This mechanism provides an explanation for SPF record failures. This check verifies the Explanation modifier in the SPF record.

No issues found

✓ SPF All Mechanism

This mechanism positioned as the rightmost element within a record provides a default value for SPF handling. This check helps to assess the configuration of this tag.

No issues found

✓ DMARC Existence

This check analyses whether there is a DMARC record for the given domain. Further checks will be conducted if there is a record.

Record
v=DMARC1; p=none; rua=mailto:hello@your-domain.com; ruf=mailto:hello@your-domain.com; sp=none; adkim=r; aspf=r

✓ Multiple DMARC Records

This check tracks whether there is more than one DMARC record present for your domain. A domain should contain only one DMARC record. If more than one record is present the record will be deemed invalid.

No issues found

✓ DMARC Redundant Tags

Checks whether the DMARC record has any redundant tags. Tags like version(v), Policy(p), percentage(pct), aggregate report (rua), failure report (ruf), failure reporting options(fo), alignment SPF (aspf), alignment DKIM (adkim), report format (rf), report interval (ri), subdomain policy(sp) can be present once in the record.

No issues found

✓ DMARC Unknown Tags

Checks whether the DMARC record has any unknown tags. Unknown tags are details related to the source IPs of the emails that do not possess a DKIM. Tags except version (v), policy (p), percentage (pct), aggregate report (rua), failure report (ruf), failure reporting options (fo), alignment SPF (aspf), alignment DKIM (adkim), report format (rf), report interval (ri), and subdomain policy(sp) are considered as unknown tags.

No issues found

✓ DMARC Version

The version tag represents the DMARC protocol version. The protocol version is mandatory as it helps to identify the version of the DMARC record.

This check tracks whether the version tag exists and whether the version of the DMARC record is configured in a right way or not.

No issues found

✓ DMARC Version Order

This check tracks whether the version tag is following the right order in listing the details or not.

No issues found

✓ DMARC Policy Order

The policy tag always needs to be followed by the version tag in the record. Change in the position might end up at failure.

Digital Risk Check will check whether the tags are in the correct order.

No issues found

✓ DMARC Percentage

The pct tag in the DMARC record denotes the percentage of messages from the domain owner's mail stream to which the DMARC policy is applied. The purpose of the "pct" tag is to enforce the domain's DMARC policy mechanism. It is ideal to apply the DMARC policy to a couple of emails to ensure an uninterrupted email delivery. By default, the pct value is 100.

Digital Risk Check will check whether the pct value falls within the specified range or not.

No issues found

✓ DMARC Aggregate Report (rua)

This rua tag stands for DMARC Reporting URIs for Aggregate Data which provides complete insight into the sender environment, like the sending source, the sending domain, the IP address of the sender, the volume of emails sent, the percentage of DMARC compliant emails, and the DKIM and SPF authentication results. These reports are generated on a daily basis and will be sent as emails.

Digital Risk Check will check for the presence of the rua tag and whether it is in the desired format.

No issues found

✓ DMARC Failure Report (ruf)

DMARC Reporting URIs for Failure (ruf) Data Reports are generated and sent by email service providers when email authentication fails. This report helps the domain admin to drill deep into why the email authentication failed. The reports will be sent as an email and includes the recipient email address, the SPF/DKIM authentication results, the DKIM signature, etc,.

Digital Risk Check will check for the presence of the ruf tag and whether it is in the desired format.

No issues found

✓ DMARC Report Format (rf)

A DMARC Report provides a lot of details including ISP information, authentication summary, DMARC description, etc,. DMARC reports helps in ensuring email security, authentication, brand reputation, brand visibility and trust. Format to be used for message-specific failure reports. The reports are generated in XML file format and the details in the report are enclosed within tags. The default value is Authentication Failure Reporting Format (afrf).

Digital Risk Check will check for the presence of the rf tag in the record and will ensure that the value is afrf.

No issues found

✓ DMARC Report Interval (ri)

DMARC Report Interval tag (ri) value defines the reporting interval within which reports should be sent. It has a default value of 86400 seconds (24 hours).

Digital Risk Check will check for the presence of the ri tag in the record and will ensure that the tag value is valid.

No issues found

⊖ TLS-RPT Multiple Records

This check tracks whether there are multiple TLS-RPT records for the given domain.The record will be deemed invalid if there are many records.

⊖ TLS-RPT Extra Space

This check analyses whether there are extra spaces in the TLS-RPT record for the given domain. It is best to remove extra spaces.

⊖ TLS-RPT Redundant Tags

Checks whether the TLS-RPT record has any redundant tags. Tags like version (v) and aggregate report (rua) can appear only once in the record.

⊖ TLS-RPT Unknown Tags

Checks whether the TLS-RPT record has any unknown tags. Tags except version(v) and aggregate report (rua) will be considered as unknown tags.

⊖ TLS-RPT Version

The version tag is used to identify the TLS-RPT version. This check analyses whether the version tag is present and whether the version of the TLS-RPT record is correct. The version should be TLSRPTv1.

⊖ TLS-RPT Version Order

This check tracks whether the version tag exists at the beginning of the record. It is should be added at the initial section of the record.

⊖ TLS-RPT Aggregate Report URI (rua)

Email addresses to which the aggregate feedback should be sent. It is listed as comma separated values. This is similar to DMARC rua and supports mailto (attribute) and HTTPS. The report will be sent as an email.

Digital Risk Check will run a check to ensure that at least a single endpoint is present.

⊖ MTA-STS DNS Multiple Records

This check tracks whether there are multiple MTA-STS DNS records for the given domain. The record will be invalid if there are multiple versions.

⊖ MTA-STS DNS Extra Space

This check analyses whether there are any extra spaces in the MTA-STS DNS record for a given domain. It is best to remove extra spaces.

⊖ MTA-STS DNS Redundant Tags

Checks whether the MTA-STS DNS record has any redundant tags. Tags like version (v) and ID (id) can be present only once in the record.

⊖ MTA-STS DNS Unknown Tags

Checks whether the MTA-STS DNS record has any unknown tags. All tags except version (v) and ID (id) will be considered as unknown tags.

⊖ MTA-STS DNS Version

The version tag represents the DMARC protocol version. The protocol version is mandatory as it helps to identify the version of the DMARC record.

This check tracks whether the version tag exists and whether the version of the DMARC record is configured in a right way or not.

⊖ MTA-STS DNS Version Order

This check tracks whether the version tag is present at the start of the record or not. It is mandatory to keep version details of the MTA-STS record in the DNS record.

⊖ MTA-STS DNS Id

MTA-STS DNS Id is a short string used to track policy updates. This string helps to identify the given instance of a policy that senders can use to find last updated date of the policy.

Digital Risk Check will run a check to trace out the Id and to ensure that the Ids contain alphanumeric values.

⊖ MTA-STS HTTPS Secured

The URL of the Mail Transfer Agent-Strict Transport Security (MTA-STS) policy file needs to be HTTPS secured. The MTA will be deemed useless if it is HTTP.

⊖ MTA-STS HTTPS Redundant Tags

Checks whether the MTA-STS HTTPS record has any redundant tags. Tags like version (v), mode, mx and max_age can appear only once in the record.

⊖ MTA-STS HTTPS Unknown Tags

Checks whether the MTA-STS HTTPS record has any unknown tags. All tags except version (v), mode, mx and max_age are considered as unknown tags.

⊖ MTA-STS HTTPS Version

The version tag represents the DMARC protocol version. The protocol version is mandatory as it helps to identify the version of the DMARC record.

This check tracks whether the version tag exists and whether the version of the DMARC record is configured in a right way or not.

MTA-STS HTTPS Version Order

It is mandatory to maintain an order in including the tags and this check tracks whether the version tag is present at the beginning of the record or not. It is important to retain that position.

MTA-STS HTTPS Mode

This check will look for any of the three options, enforce, testing, or none, based on the expected behaviour of sending MTA in the case of a policy validation failure.

MTA-STS HTTPS MX

This check tracks all the allowed MX patterns, the syntax, and whether it is a valid MX record or not. MX indicates that emails for a domain will be handled by it.

MTA-STS HTTPS Max Age

Maximum lifetime of the domain policy. Clients should cache the policy related to their domains. It is mandatory to cache the policy for up to a particular value from the last policy fetch time. To mitigate the risks of attacks during policy refresh time, it is best to keep this value within the range of weeks or greater.

Digital Risk Check will check whether the max_age value is within the specified limit.

C

Network Security 67

With copious amounts of data online and growing number of cyber threats, it is essential to secure the user data by building a secure and stable network. Network security includes the steps that can be taken to ensure the reliability and integrity of all data in a network.

!! Insecure SSL Protocol

Using SSL protocols that aren't secure can make your site prone to data thefts, stealing, vulnerabilities, or other attacks. The presence of a secure protocol will hinder an attacker's attempt to tamper or modify sensitive data.

Digital Risk Check will verify the supported TLS protocol versions and will assess the level of security based on version hierarchy.

Registered Domain	Protocols Supported	
	name	version
www.your-domain.com	TLS	1
	TLS	1.1

Insecure Cipher

A cipher is an algorithm for encryption and decryption of data. Ciphers enable private communication on different networking protocols, including the Transport Layer Security (TLS) protocol that offer encryption of network traffic. They use a system of fixed rules to transform plain text, or a message, into cipher text, a random string of characters. Your application or sever can be prone to vulnerabilities if you haven't configured any order for your ciphers or if there are any insecure ciphers. The chances for an attacker to eavesdrop or tamper your data is high if you've insecure ciphers.

Digital Risk Check will run a check to trace out weak ciphers with less than 128 bits, NULL ciphers, ciphers without encryption, etc., to avoid vulnerabilities.

Registered Domain	Insecure Ciphers			
	Status	Ciphers	Size (bits)	Protocol Version
www.your-domain.com	Weak	ECDHE-RSA-AES128-SHA	128	TLSv1
	Weak	AES128-SHA	128	TLSv1
	Weak	ECDHE-RSA-AES256-SHA	256	TLSv1
	Weak	AES256-SHA	256	TLSv1
	Weak	ECDHE-RSA-AES128-SHA	128	TLSv1.1
	Weak	AES128-SHA	128	TLSv1.1
	Weak	ECDHE-RSA-AES256-SHA	256	TLSv1.1
	Weak	AES256-SHA	256	TLSv1.1
	Weak	ECDHE-RSA-CHACHA20-POLY1305	256	TLSv1.2
	Weak	ECDHE-RSA-AES128-SHA	128	TLSv1.2
	Weak	AES128-SHA	128	TLSv1.2
	Weak	ECDHE-RSA-AES256-SHA	256	TLSv1.2
	Weak	AES256-SHA	256	TLSv1.2
	Weak	ECDHE-RSA-AES128-SHA256	128	TLSv1.2
	Weak	AES128-SHA256	128	TLSv1.2
	Weak	ECDHE-RSA-AES256-SHA384	256	TLSv1.2
	Weak	AES256-SHA256	256	TLSv1.2

Valid SSL Certificate

An SSL Certificate is supposed to have a validity of 13 months or less. An expired SSL Certificate can make your site prone to phishing attacks, man-in-the-middle attacks, and data breaches. Moreover, it is essential to ensure that the certificate was issued by a trusted certificate authority and that the root certificate is a valid one. If not, "The certificate is not issued by a trusted certificate authority" or "SSL Certificate Not Trusted" errors will be raised.

Digital Risk Check will run a check to ensure that your certificate hasn't expired and that it is issued by a valid certificate authority.

Registered Domain	Expiry Date
www.your-domain.com	Sat Mar 09 08:50:43 CET 2024

SSL Chain Expiry

The SSL Certificate Chain is a list of certificates that include the root certificate, intermediate certificates, and the end-user certificate. The intermediate certificate along with the server certificate helps to complete the trust chain and makes the certificate chain efficient. When an intermediate certificate in your chain expires, SSL errors will be thrown and you won't be able to install any other certificates on your platform.

Digital Risk Check will be checking the expiry of all your intermediate certificates and the number of days left for their expiry.

Registered Domain	Expiry Date
www.your-domain.com	Sat Mar 09 08:50:43 CET 2024

Vulnerabilities

SSL Vulnerabilities arise because of improper configuration of the SSL certificates. The most common vulnerabilities include BEAST, POODLE, POODLE (TLS), ROBOT, RC4 Vulnerability, CBC Vulnerability, AEAD, etc,.This vulnerability can lead to session hijackings, man-in-the-middle attacks, text command injections, and many other security issues.

Digital Risk Check will check the SSL certificates to trace out any of the above mentioned vulnerabilities.

Registered Domain	Vulnerabilities	Status			
www.your-domain.com	1.0	✓ RC4	✗ ROBOT	✓ FREAK	✓ CRIME
		✓ CBC	✓ FallbackScsv	✓ POODLE	✓ RENEGOTIATION
		✓ PoodleTls	✓ HeartBleed	✓ CHACHA20	✓ LOGJAM
		✓ AEAD	✓ FORWARDSECRECY	✓ DROWN	✓ BEAST

Certificate Revoked

A certificate is revoked when there are signs that the private key has been tampered with or is done immediately before the date of expiry as an act of invalidation. The revoked certificates will be stored in the Certificate Revocation List (CRL) managed by the certifying authority. It is not possible to check and verify that your certificates aren't there in the CRL. Hence, the easiest way to do that is using Online Certificate Status Protocol (OCSP).

Digital Risk Check will run OCSP checks to verify whether your certificates have been revoked or not.

Your current license does not support this feature.

DNSSEC Validation

Domain Name System Security Extensions (DNSSEC) is an extension of the Domain Name Server (DNS) protocol that allows DNS responses to be digitally signed and authenticated. It adds cryptographic signatures to the existing DNS records and helps the DNS resolver to verify authenticity of the responses. This can help in identifying fake DNS records created through cache poisoning or during man-in-the-middle attacks.

Digital Risk Check will check if DNSSEC is enabled for the domain, whether there is any breakage in the chain, and whether the DNS records like A, AAAA, SOA, NS, MX, and TXT are signed with a valid key.

Your current license does not support this feature.

B+

Application Security 87

Most of the cyber attackers target the vulnerabilities in the application layer. With the enhanced complexity of the application tier, it is essential to test applications for their security. Application security can be ensured by constantly tracking the headers, by checking for any malware injections, defacement attacks, and much more.

Insecure Component Header

The X-Powered-By header contains details related to the technologies used by the server. This can help attackers in finding the vulnerabilities. Hence, it is better to remove all X-Powered-By headers.

Digital Risk Check will check for the presence of X-Powered-By header thereby helping you to prevent attacks by fingerprinting your tech stack.

Registered Domain	Insecure Headers	
https://www.your-domain.com	x-powered-by	PleskLin

Security.txt

security.txt is a standardised approach for websites to establish clear security policies.

No issues found

Header Missing

HTTP headers are added to the servers to improve the security of the application. Headers protect the application by hindering attackers from exploiting the vulnerabilities. A couple of headers like x-content-type-options, x-xss-protection, content-security-policy, x-frame-options, strict-transport-security,and server should be present mandatorily.

Digital Risk Check will check at regular intervals to check whether the required headers are present or not.

Registered Domain	Missed Header	Raw Headers	
https://www.your-domain.com	x-xss-protection content-security-policy x-frame-options	status	200
		date	Tue, 12 Dec 2029 09:25:59 GMT
		content-type	text/html; charset=UTF-8
		vary	User-Agent,Accept-Encoding
		last-modified	Wed, 06 Dec 2023 10:03:30 GMT
		cache-control	max-age=0, no-cache, no-store, must-revalidate
		pragma	no-cache
		expires	Mon, 29 Oct 1923 20:30:00 GMT
		x-cache-status	BYPASS
		x-powered-by	PleskLin
		cf-cache-status	DYNAMIC
		report-to	{"endpoints":[{"url":"https:\/\/a.nel.xxxx.com\/report\/v3?s=xxxxxxxxxx nel","max_age":604800}
		nel	{"success_fraction":0,"report_to":"cf-nel","max_age":604800}
		strict-transport-security	max-age=0; includeSubDomains; preload
		x-content-type-options	nosniff
		server	cloudflare
		cf-ray	8344ec575ee466a3-AMS
		content-encoding	br
		alt-svc	h3=":443"; ma=86400

! Defacement

As the word implies, during a defacement attack, a defacer might inject malicious content onto the webpage. This can bring in financial loss along with a negative impact on the brand's reputation. Following strict security measures like avoiding common vulnerabilities, securing source code, or securing your database regular updates of third-party softwares used, elimination of vulnerabilities, and use of strong passwords can help in keeping defacement on check.

Digital Risk Check will check for modification in the page content or critical elements to ensure the integrity of the page.

Registered Domain	Reason	Script Defaced (%)	Text Defaced (%)	Image Defaced (%)	Anchor Defaced (%)	Iframe Defaced (%)
https://your-domain.com/website-uptime-monitoring	-	5	0	0	0	0
https://your-domain.com	-	4	0	0	0	0
https://your-domain.com/about-us	-	5	0	0	0	0

! Permissions Policy

It specifies the web features, APIs, or resources that are allowed or restricted on the webpage. This check enhances security and privacy and helps to stay away from potential risks and vulnerabilities.

No issues found

! Referrer Policy

It defines rules for sharing information about the source webpage (referrer) when a user clicks a link or loads any external content. This helps websites to control the level of referrer data disclosure, thus balancing user privacy and security.

No issues found

✓ Brand Reputation

Retaining the customer trust and the credibility of the brand is crucial for any business entity. With important data transactions happening through the websites, any issue that affects the security of the webpage can impact your brand's reputation. Hence, it is essential to ensure that you're offering a secure online space for your customers.

Digital Risk Check will cross check your website with Google's list of blocklisted URLs to ensure that it isn't present.

Registered Domain	Reason	Overall
https://www.your-domain.com	-	0

Phishing

Phishing attackers use emails, text messages, or calls to steal sensitive information like social security number, passwords, or credit card details or manipulate people to download malware-infected files.It is the most common type of social engineering attack. Phishing attacks can result in huge financial loss, identity theft, and loss of brand reputation.

Digital Risk Check will check your site against the Google list of webpages affected by phishing attacks to ensure that your site isn't listed there.

Registered Domain	Reason
https://your-domain.com	-
https://your-domain.com/privacy-policy	-
https://www.your-domain.com	-
https://your-domain.com/terms-and-conditions	-
https://your-domain.com/solutions	-
https://your-domain.com/archive	-
https://your-domain.com/contact	-
https://your-domain.com/about-us	-

Defacement

As the word implies, during a defacement attack, a defacer might inject malicious content onto the webpage. This can bring in financial loss along with a negative impact on the brand's reputation. Following strict security measures like avoiding common vulnerabilities, securing source code, or securing your database regular updates of third-party softwares used, elimination of vulnerabilities, and use of strong passwords can help in keeping defacement on check.

Digital Risk Check will check for modification in the page content or critical elements to ensure the integrity of the page.

Registered Domain	Reason	Script Defaced (%)	Text Defaced (%)	Image Defaced (%)	Anchor Defaced (%)	Iframe Defaced (%)
https://your-domain.com/archive	-	0	0	0	0	0
https://your-domain.com/about-us	-	0	0	0	0	0
https://your-domain.com/solutons	-	0	0	0	0	0
https://www.your-domain.com	-	0	0	0	0	0

Insecure Header

HTTP headers help in providing enhanced protection by preventing several vulnerabilities that can put your application's security in jeopardy. An insecure header may not help in preventing the users from connecting to an unencrypted site.

Digital Risk Check checks for headers that are not configured correctly and may make the application vulnerable to attacks.

Registered Domain	Insecure Headers
https://www.your-domain.com	-

Insecure Server Header

The server header provides information related to the software used by the origin server. This information can help attackers trace out the security loopholes. It is best to limit the amount of information that'll be included in the server header.

Digital Risk Check will check the server header to ensure that it contains only the necessary details and may not be providing sensitive information to attackers.

Registered Domain	Insecure Headers
https://www.your-domain.com	-

✓ Enforce HTTPS Header

The enforce HTTPS header informs browsers that the site should be accessed only using HTTPS. Even if attempts to connect are made from HTTP that will be automatically converted to HTTPS. This is a safer option than redirecting HTTP to HTTPS.

Digital Risk Check will be running checks to ensure that there are enforce HTTP headers present at your end.

Registered Domain	Missed Header
https://www.your-domain.com	-

✓ Insecure Cookies

Cookies are small texts sent by the site you visit to your browser. If the cookie isn't configured properly or if the transport security setting isn;'t configured correctly, any hacker can access sensitive data stored in the cookies. This is possible even if you own a valid SSL certificate.

Digital Risk Check will regularly check the cookies to ensure that they are configured correctly.

Registered Domain	Insecure Cookies
https://www.your-domain.com	-

✓ HTTPOnly Cookies

An HTTPOnly cookie includes a tag added to it that prevent the client-side from accessing the data in the cookie. This tag protects the data from being viewed by any entity other than the server. HTTPOnly cookies are secure and it is a best practice to use HTTPOnly cookies while handling sensitive data.

Digital Risk Check will run checks regularly to ensure that cookies have the HTTPOnly flag.

Registered Domain	Insecure Cookies
https://www.your-domain.com	-

✓ Secure Cookies

If a cookie is tagged with a secure flag, then such cookies won't be transferred over risky, unencrypted HTTP networks. if there is no secure flag, the cookie is susceptible to attacks.It is best to use the secure flag for cookies while transferring sensitive data.

Digital Risk Check will check whether the cookie has a secure flag.

Registered Domain	Insecure Cookies
https://www.your-domain.com	-

Malware

Malware refers to any malicious files that can harm a network, a service, and can be a potential threat to the end users. They are used in different forms like advertisements, email attachments, phishing emails, text messages, etc,. Slower performance, numerous pop-ups blocking your screen, browser redirections, or infection warnings can imply that your machine has been compromised. This can expose your valuable credentials to cyber criminals.

Digital Risk Check will perform a client-side malware scanning approach where the pages will be crawled to extract all the files available on each page. After which, these pages will be scanned and checked for malicious content.

Registered Domain	Malware Count
https://www.your-domain.com	0

Infected Pages

Pages which contain more than one malware-infected file will be deemed as infected pages. Infected pages can be used by attackers to steal highly sensitive data or other credentials. Hence, it is important to ensure that your pages aren't infected.

Digital Risk Check will run regular checks to ensure that your files/pages are secure.

Registered Domain	Infected Pages Count
https://www.your-domain.com	0

Redirect Chain

It involves examining a series of HTTP redirects when accessing a webpage. This analysis ensures that each redirect maintains or strengthens essential security headers, like content security policy (CSP) or HTTP strict transport security (HSTS). It helps prevent security risks by ensuring that security configurations are consistently enforced throughout the redirection process, safeguarding against potential vulnerabilities or information exposure.

No issues found

Directory Listing

Directory listing on a domain can cause security risks by exposing directory structures and potentially sensitive data. To address this issue, you can disable directory listing, use proper permissions, create index pages, implement access controls, conduct regular security audits, employ a Web Application Firewall, and much more.

No issues found