SUMERU

Threat Meter

External Threat Score

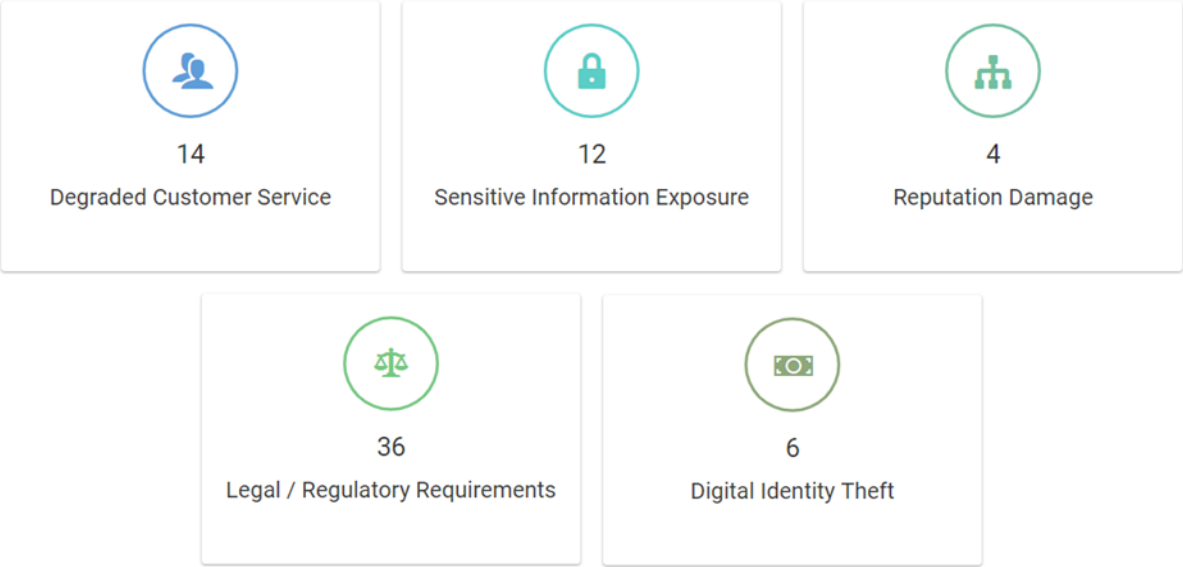
We're your eyes on the internet.
Helping you see what hackers see about you.

https://www.sumeruthreatsuite.com/

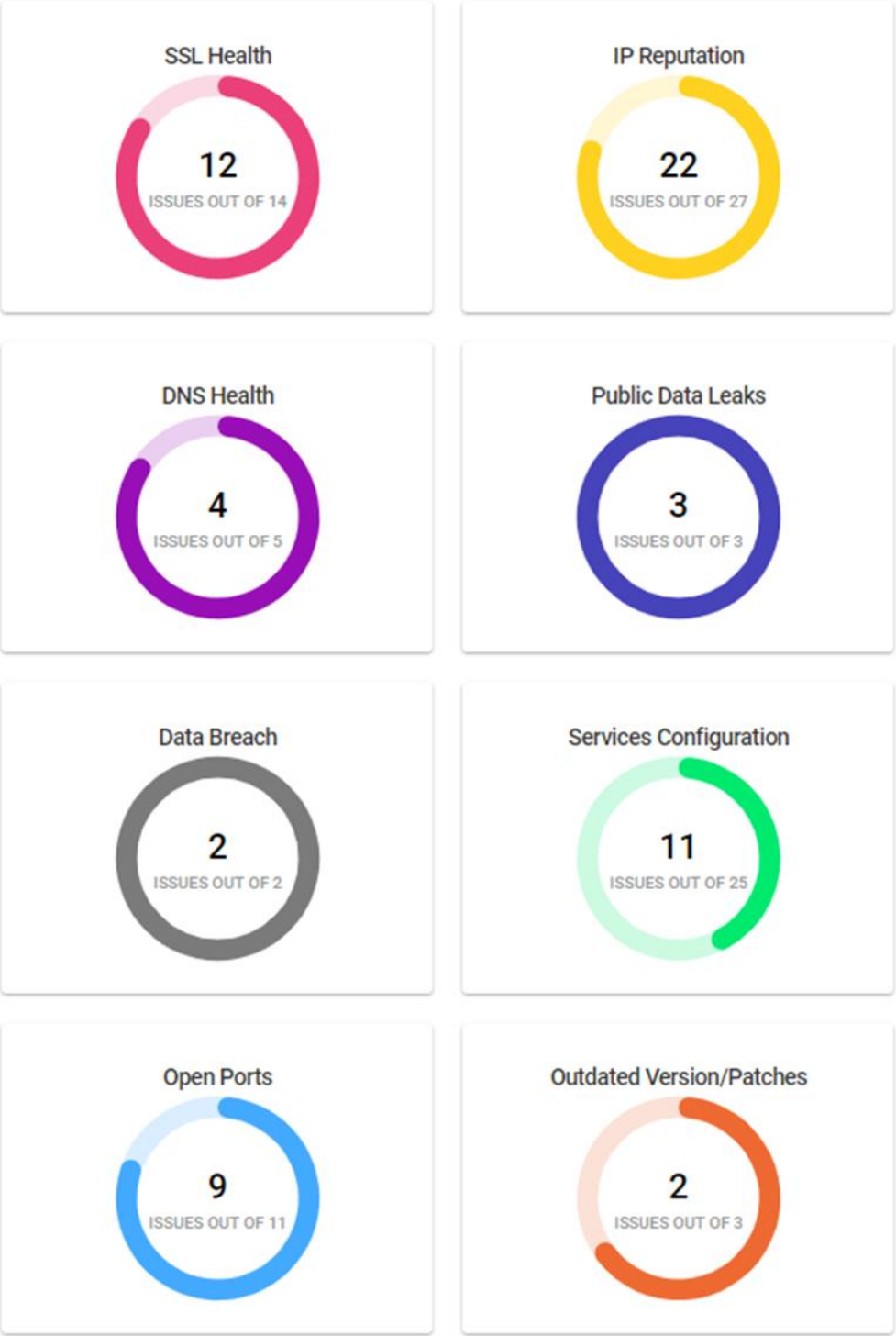
Sample Client

Threat score is **MEDIUM** based on the findings across eight major security categories.

Threat Profile



What affects the threat score?



Risk Details

SSL Health

Transport layer security (TLS) is a protocol that provides communication security between client/server applications that communicate with each other over the Internet. It enables privacy, integrity and protection for the data that's transmitted between different nodes on the Internet.

Impact

The confidentiality of sensitive data may be compromised by the use of a broken or risky cryptographic algorithm. A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current attack methods and resources.

List of Issue

1 Hostname not listed in certificate	
Description	Hostname not listed in certificate is a widespread error that occurs when the Common Name or SAN value of your SSL / TLS certificate does not correspond to the domain name.
Affected URLS	sample.site
Impact	The attacker can perform MitM attack and intercept all communication between your application and the server. It will lead to loss of confidentiality and integrity.
Solutions	While creating the certificate, you have to config the hostname and generate the certificate.

2 Client-Initiated Secure Renegotiation Enabled	
Description	SSL/TLS client-initiated renegotiation is a feature that allows the client to renegotiate new encryption parameters for an SSL/TLS connection within a single TCP connection.
Affected URLS	sample.site
Impact	It will lead to perform man-in-the-middle (MITM) and Denial of Service (DoS) in the application.
Solutions	Please disable SSL/TLS client-initiated renegotiation.

3 Invalid Certificate Chain	
Description	A certificate chain is an ordered list of certificates, containing an SSL Certificate and Certificate Authority (CA) Certificates, that enable the receiver to verify that the sender and all CA's are trustworthy
Affected URLS	sample.site
Impact	Invalid certificate chain will lead to fails to establish HTTPS connection.
Solutions	Please configure server to not only present its own certificate but also any intermediate certificates.

4 Weak Cipher Suites	
Description	We detected that weak ciphers are enabled during secure communication (SSL). You should allow only strong ciphers on your web server to protect secure communication with your visitors.
Affected URLS	sample.site
Impact	Attackers might decrypt SSL traffic between your server and your visitors.
Solutions	Configure your web server to disallow using weak ciphers. **For Apache**, you should modify the SSLCipherSuite directive in the httpd.conf. SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4 **For Microsoft IIS**, you should make some changes to the system registry. Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer. a. Click Start, click Run, type regedt32 or type regedit, and then click OK.

b. In Registry Editor, locate the following registry key:
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
c. Set Enabled DWORD to 0x0 for the following registry keys:

SCHANNEL\Ciphers\DES 56/56

SCHANNEL\Ciphers\RC4 64/128

SCHANNEL\Ciphers\RC4 40/128

SCHANNEL\Ciphers\RC2 56/128

SCHANNEL\Ciphers\RC2 40/128

SCHANNEL\Ciphers\NULL

SCHANNEL\Hashes\MD5

5 TLS v1.0 Enabled

Description	A certificate chain is an ordered list of certificates, containing an SSL Certificate and Certificate Authority (CA) Certificates, that enable the receiver to verify that the sender and all CA's are trustworthy
Affected URLS	sample.site
Impact	Invalid certificate chain will lead to fails to establish HTTPS connection.
Solutions	Please configure server to not only present its own certificate but also any intermediate certificates.

IP Reputation

An IP address earns a negative reputation when suspicious activity, such as spam or viruses originating from that address. We strongly recommend that you perform a digital forensic on any of your systems that correspond to an IP address with a negative reputation, as those systems may have been compromised.

Impact

An IP address earns a negative reputation when suspicious activity, such as spam or viruses originating from that address. All emails sent from that server will be at risk of not being delivered because of the low reputation of that IP. We strongly recommend that you perform a digital forensic on any of your systems that correspond to an IP address with a negative reputation, as those systems may have been compromised.

List of Issue

1 Nszones -Dynamic	
Description	DYN is a list of the world's dynamic IP addresses. Dial up connections, cable, broadband and ADSL customers
Affected URLS	sample.site
Impact	IPs present in the black listing might cause some issue while reaching out to the destination which uses this blacklist and it leads to loss of reputation.
Solutions	Contact the NSzones team to delist your IPs.

2 Megarbl - Spam DB	
Description	MegaRBL is a Blacklist that lists known spammers who hit their honeypot spamtraps. IP addresses listed on MegaRBL are reported to their respective Internet Service Providers. If your IP has been listed by MegaRBL, then that IP address has been detected as sending spam.
Affected URLS	sample.site

Impact	IPs present in the black listing might cause some issue while reaching out to the destination which uses this blacklist and it leads to loss of reputation.
Solutions	This blacklist does support a manual request to remove or delist your IP Address from their database ref - https://mxtoolbox.com/problem/blacklist/megarbl

DNS Health

DNS issue related to websites is always under pressure from business, especially production one.

Impact

This allows an attacker to craft a spoofed email using the organization domain to perform malicious activity. This can lead to loss of reputation and business loss.

List of Issue

1 Misconfigured SPF Record	
Description	A Sender Policy Framework (SPF) record is a type of Domain Name Service (DNS) TXT record that identifies which mail servers are permitted to send email on behalf of your domain. A Misconfigured SPF record may allow spammers to Fake mailing on behalf of the respected organization.
Affected URLS	sample.site
Impact	This issue leads to phishing attacks that are harder to identify as phishing mail by the victim.
Solutions	Please make sure that all the IPs of the organization is present in the SPF record and that are used to send emails ->Like v=spf1 ip4:192.168.1.1 ip4:192.168.1.2 and the end of the record should not use ~all or +all unless it was Soft mode (Test mode). ->If your using any third party service use include to mention the domains like include:example.com ->And always use the -all to end the record. ->A secure record may something looks like below v=spf1 ip4:192.168.1.1 ip4:192.168.1.2 include:example.com -all Use the following online tools to check the secureness of SPF records https://mxtoolbox.com/spf.aspx https://www.dmarcanalyzer.com/spf/checker/

2 Missing DMARC	
Description	DMARC stands for “Domain-based Message Authentication, Reporting & Conformance.” DMARC is a protocol that uses Sender Policy Framework, (SPF) and DomainKeys identified mail (DKIM) to determine the authenticity of an email message.
Affected URLS	sample.site
Impact	Spammers can forge the "From" address on email messages to make messages appear to come from someone in your domain. If spammers use your domain to send spam or junk email, your domain quality is negatively affected. People who get the forged emails can mark them as spam or junk, which can impact authentic messages sent from your domain.
Solutions	Before going to Implement DMARC record, SPF and DKIM should be implemented properly **Implementing DMARC :** -> Add a new record as TXT record, in which DMARC record is something look like this below v=DMARC1; p=quarantine; rua=mailto:reports@dmarc.site; ruf=mailto:reports@dmarc.site; adkim=r; aspf=r; rf=afrf ->The "p" option has three options: none, quarantine, or reject, for how email that violates policies should be handled ->The adkim and aspf options define how strictly DKIM and SPF policy should be applied, with 's' indicating strict and 'r' indicating relaxed ->The RUA provides an address for aggregate data reports, while the RUF provides an address for forensic reports

Service Configurations

Security misconfiguration can happen at any level of an application stack, including the network services, platform, web server, application server, database, frameworks, custom code, and pre-installed virtual machines, containers, or storage. Attackers will often attempt to exploit unpatched flaws or access default accounts, unused pages, unprotected files and directories, etc. to gain unauthorized access or knowledge of the system.

Impact

Misconfiguration flaws frequently give attackers unauthorized access to some system data or functionality. Occasionally, such flaws result in a complete system compromise. A misconfigured cloud can leave organization vulnerable to attacks.

1 Cross Origin Resource Sharing	
Description	Cross-origin resource sharing is a mechanism that allows restricted resources on a web page to be requested from another domain outside the domain from which the first resource was served.
Affected URLS	sample.site
Impact	If the site specifies the header Access-Control-Allow-Credentials: true, third-party sites may be able to carry out privileged actions and retrieve sensitive information.

Solutions	**In Apache:**
	Simply add the following line inside either the , , or sections of your server config (usually located in a *.conf file, such as httpd.conf or apache.conf), or within a .htaccess file
	
	Header set Access-Control-Allow-Origin "--your value--"
	
	In Ngnix:
	The following Nginx configuration enables CORS, with support for preflight requests.
	
	#CORS
	location / {
	if ($request_method = 'OPTIONS') {
	add_header 'Access-Control-Allow-Origin' '*';
	add_header 'Access-Control-Allow-Methods' 'GET, POST, OPTIONS';
	#

```
      # Custom headers and headers various browsers *should* be OK with
but aren't
      #
      add_header 'Access-Control-Allow-Headers' 'DNT,User-Agent,X-
Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range';
      #
      # Tell client that this pre-flight info is valid for 20 days
      #
      add_header 'Access-Control-Max-Age' 1728000;
      add_header 'Content-Type' 'text/plain; charset=utf-8';
      add_header 'Content-Length' 0;
      return 204;
    }
    if ($request_method = 'POST') {
      add_header 'Access-Control-Allow-Origin' '*';
      add_header 'Access-Control-Allow-Methods' 'GET, POST, OPTIONS';
      add_header 'Access-Control-Allow-Headers' 'DNT,User-Agent,X-
Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range';
      add_header 'Access-Control-Expose-Headers' 'Content-Length,Content-
Range';
    }
    if ($request_method = 'GET') {
      add_header 'Access-Control-Allow-Origin' '*';
      add_header 'Access-Control-Allow-Methods' 'GET, POST, OPTIONS';
      add_header 'Access-Control-Allow-Headers' 'DNT,User-Agent,X-
Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range';
      add_header 'Access-Control-Expose-Headers' 'Content-Length,Content-
Range';
    }
}
```

2 TRACE HTTP Method Enabled	
Description	The HTTP TRACE method performs a message loop-back test along the path to the target resource, providing a useful debugging mechanism.
Affected URLS	sample.site
Impact	This may lead to Cross Site Tracing (XST) attacks, which could lead to steal a user's cookie even if the cookie has the HTTP Only attribute flag set.

Solutions	We have to disable the trace method enabled in the application.
	
	For Apache,
	Goto the httpd.conf file, and add the line
	
	TraceEnable Off
	
	Then, restart the Apache server.
	
	For IIS,
	Goto the web.config file and add the lines
	
	`<system.web>`
	`  <httpHandlers>`
	`  <add path="*" verb="TRACE" type="System.Web.DefaultHttpHandler" validate="true"/>`
	`  </httpHandlers>`
	`</system.web>`

3 Referrer-Policy	
Description	Referrer-Policy is a security header that can (and should) be included on communication from your website's server to a client.
Affected URLS	sample.site
Impact	The lack of Referrer-Policy header might affect privacy of the users and site's itself. Even sensitive information contained in the URL will be leaked to the cross-site.
Solutions	Please refer the following link to fix the solution. https://sumeru.gitbook.io/sumeru-cyber-security/common-vulnerabilites/security-headers#referrer-policy

4 X-XSS-Protection	
Description	The HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks
Affected URLS	sample.site
Impact	It will leads to perform Cross-site scripting in the application.
Solutions	Please refer the following link to fix the solution. https://sumeru.gitbook.io/sumeru-cyber-security/common-vulnerabilites/security-headers#x-xss-protection

5 Content-Security-Policy	
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to distribution of malware.
Affected URLS	sample.site
Impact	If your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability
Solutions	Please refer the following link to fix the solution. https://sumeru.gitbook.io/sumeru-cyber-security/common-vulnerabilites/security-headers#content-security-policy

6 X-Frame-Options	
Description	The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame>, <iframe>, <embed> or <object>. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.
Affected URLS	sample.site
Impact	It will lead to perform Clickjacking in the application.
Solutions	Please refer the following link to fix the solution. https://sumeru.gitbook.io/sumeru-cyber-security/common-vulnerabilites/security-headers#x-frame-options

7 Strict-Transport-Security	
Description	The HTTP Strict-Transport-Security response header (often abbreviated as HSTS) lets a web site tell browsers that it should only be accessed using HTTPS, instead of using HTTP.
Affected URLS	sample.site
Impact	It will lead to perform eavesdropper and active man-in-the-middle (MITM) attacks in the application.
Solutions	Please refer the following link to fix the solution. https://sumeru.gitbook.io/sumeru-cyber-security/common-vulnerabilites/security-headers#strict-transport-security

8 X-Content-Type-Options	
Description	The X-Content-Type-Options response HTTP header is a marker used by the server to indicate that the MIME types advertised in the Content-Type headers should not be changed and be followed.
Affected URLS	sample.site
Impact	The application will be vulnerable to MIME sniffing.
Solutions	Please refer the following link to fix the solution. https://sumeru.gitbook.io/sumeru-cyber-security/common-vulnerabilites/security-headers#x-content-type-options

9 Cookie Attribute - Secure	
Description	Secure flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response. The purpose of the secure flag is to prevent cookies from being observed by unauthorized parties due to the transmission of cookie in clear text.
Affected URLS	sample.site
Impact	If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope.
Solutions	Please refer the following link to fix the solution. https://sumeru.gitbook.io/sumeru-cyber-security/common-vulnerabilites/http-only-and-secure-flag

10 Cookie Attribute - HttpOnly	
Description	HttpOnly is a flag added to cookies that tell the browser not to display the cookie through client-side scripts (document.cookie and others)
Affected URLS	sample.site
Impact	An attacker can use this information to get cookie by cross site scripting (XSS) which could lead to session hijacking.
Solutions	Please refer the following link to fix the solution. https://sumeru.gitbook.io/sumeru-cyber-security/common-vulnerabilites/http-only-and-secure-flag

11 Version Disclosure	
Description	Version disclosure is response headers contain the version information about the development framework used for the application.
Affected URLS	sample.site
Impact	This information can help an attacker to perform further attacks..
Solutions	Here is the link to remove the versions in the application. https://sumeru.gitbook.io/sumeru-cyber-security/common-vulnerabilites/version-disclosure

12 Cpanel Available Publicly	
Description	cPanel is publicly available on the target server. An attacker can get the information about the application to perform further attacks.
Affected URLS	sample.site
Impact	An attacker can run brute force attack against the cPanel and can perform further server related attacks that may lead to entire server compromise.
Solutions	For the /cpanel url, remove/change these lines or similar matched lines located on the httpd.conf (webserver config) file: ScriptAliasMatch ^/?cpanel/?$ /usr/local/cpanel/cgi-sys/redirect.cgi ScriptAliasMatch ^/?webmail/?$ /usr/local/cpanel/cgi-sys/wredirect.cgi ScriptAliasMatch ^/?whm/?$ /usr/local/cpanel/cgi-sys/whmredirect.cgi Then run the following commands for the changes to take effect. /usr/local/cpanel/bin/apache_conf_distiller --update /scripts/rebuildhttpdconf /etc/init.d/httpd restart

13 Cookie Attribute - HttpOnly	
Description	PhpMyAdmin is publicly available on the target server. A attacker can get the information about the application to perform further attack
Affected URLS	sample.site
Impact	An attacker can run brute force attack against the PhpMyAdmin and find the password and can access, modify or delete all MySQL databases
Solutions	For removing phpMyAdmin page, sudo dpkg -P 19hpMyAdmin sudo rm -f /etc/apache2/conf.d/19hpMyAdmin.conf sudo service apache2 restart

14 Missing Pragma	
Description	The Pragma HTTP/1.0 general header is an implementation-specific header that may have various effects along the request-response chain. It is used for backwards compatibility with HTTP/1.0 caches where the Cache-Control HTTP/1.1 header is not yet present.
Affected URLS	sample.site
Impact	"Pragma: no-cache" is equivalent to "Cache-Control: no-cache".
Solutions	A safe set of HTTP response headers may look like: Cache-Control: private, no-cache, no-store, max-age=0, no-transform Pragma: no-cache Expires: 0

15 Transport Layer Security	
Description	Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Service Layer (SSL).
Affected URLS	sample.site
Impact	It will lead to perform Man in middle attacks (MiTM), Poodle and DDoS attacks.
Solutions	Remove the weak ciphers used in TLSv1.0,1. Upgrade the TLS version to TLSv1.2.

Open Ports

Unnecessary open ports on a server are a security vulnerability that can potentially allow a hacker to exploit services on your network. If those services are unpatched, a hacker can easily take advantage of the system by running a simple port scan to discover the open ports.

Impact

All ports are potentially at risk of attack. No port is natively secure. Each port and underlying service has its risks. A port with default configuration or insecure configuration can have numerous vulnerabilities such as anonymous authentication, directory traversals, man-in-the-middle, Remote Code Executions, and cross-site scripting. Weak authentication on some of the open ports will allow attacker to successfully brute force the credentials and get into the

List of Issue

1 FTP	
Description	FTP Default port '21/20' is open publicly in the mentioned IP(s).
Affected URLS	sample.site
Impact	This port can easily be discovered, and once discovered these ports are now susceptible to vulnerabilities of the listening applications
Solutions	Please disable the FTP default ports (20/21) in the server and start using SFTP or SSH for secure file transfer.

2 MYSQL	
Description	MYSQL Default port '3306' is open publicly in the mentioned IP(s).
Affected URLS	sample.site
Impact	This port can easily be discovered, and once discovered these ports are now susceptible to vulnerabilities of the listening applications
Solutions	PLease disable the mysql default port (3306) in the server.

3 SMTP	
Description	A SMTP server that works as an open relay, is a email server that does not verify if the user is authorized to send email from the specified email address. Therefore, users would be able to send email originating from any third-party email address that they want.
Affected URLS	sample.site
Impact	This port can easily be discovered, and once discovered these ports are now susceptible to vulnerabilities of the listening applications
Solutions	Please disable the FTP default ports (20/21) in the server and start using SFTP or SSH for secure file transfer.

Outdated Version

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.

Impact

Outdated version of a software component may have multiple vulnerabilities. Exploits will be available publicly for the components with known vulnerability. The impact could range from minimal to complete host takeover and data compromise

List of Issue

1 Web Server	
Description	The version of web server that the application uses now is outdated and there is no patch/support provided from the vendor
Affected URLS	sample.site
Impact	There will be no fixes released by the vendor for future upcoming vulnerabilities
Solutions	Please update the latest version of application available with the vendor

2 Application Stack	
Description	The Version of Application used in the server is outdated and no longer supported by the vendor
Affected URLS	sample.site
Impact	There will be no fixes released by the vendor for future upcoming vulnerabilities
Solutions	Please update the latest version of application available with the vendor

Sample Client

Threat Meter Input: sample.site

Auto Discovered: Publicly available Email IDs

a@sample.site	j@sample.site
b@sample.site	k@sample.site
c@sample.site	l@sample.site
d@sample.site	m@sample.site
e@sample.site	n@sample.site
f@sample.site	o@sample.site
g@sample.site	p@sample.site
h@sample.site	Q@sample.site
i@sample.site	r@sample.site

Note:

- All the data shown in this report are PUBLICLY AVAILABLE for ANYONE. We have NOT carried out any intrusive scanning on the applications or servers directly.

Contact Us

Shelvin Narayan
CEO
Sumeru Australia Pty Ltd

Sumeru Australia Pty Ltd.
www.sumerusolutions.com

: Level 8, 11 York street, Sydney 2000 NSW Australia.

☎ : +61 – 408 598 864

✉ : shelvin@sumerusolutions.com