CyRAACS

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CERT-In
Empaneled

VAPT and Secure Code Review Services

CyRAACS Approach Document

cyraacs.com

Murari Shanker | +91-9886210050 | ms@cyraacs.com

Top Vulnerabilities in IT Infrastructure and Applications

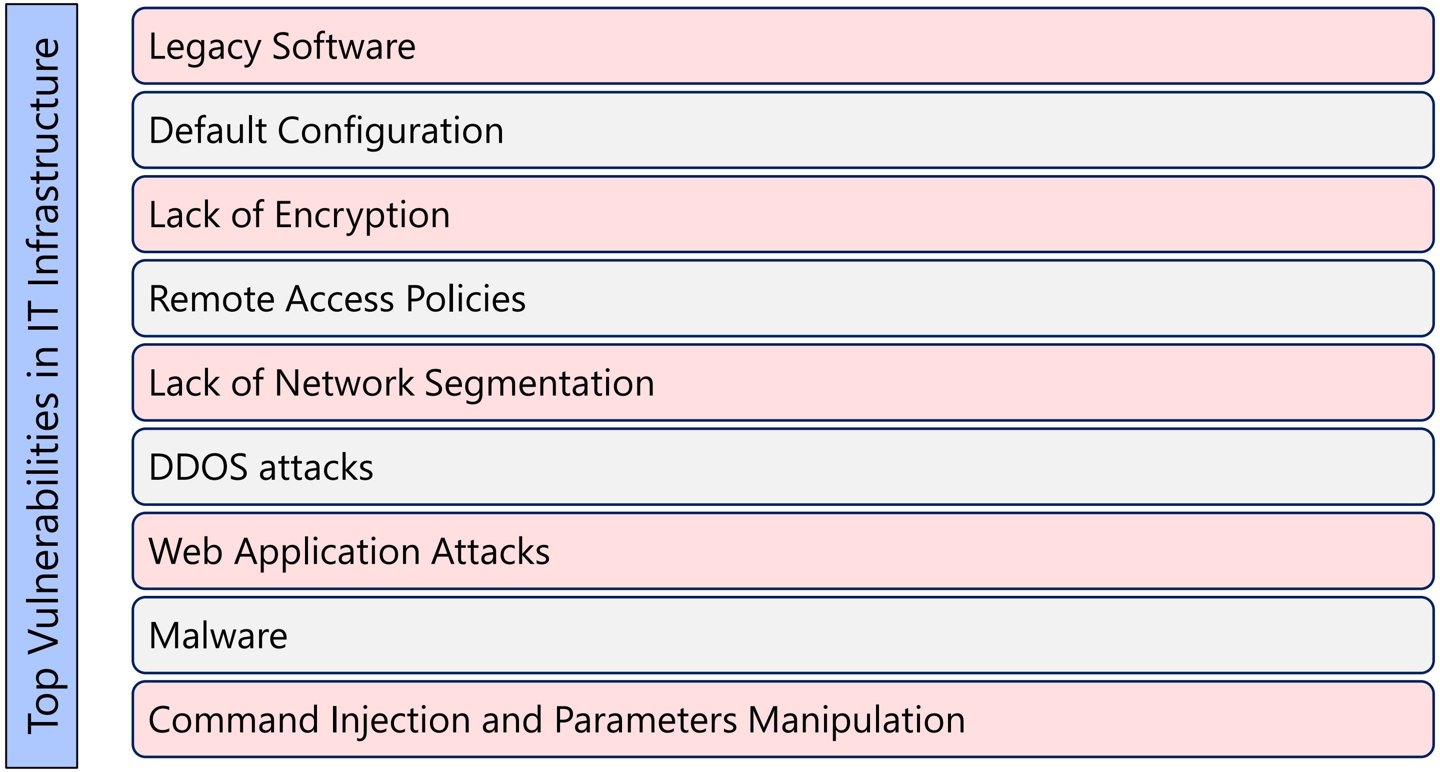
- Application security risks are pervasive and can pose a direct threat to business availability.
- Although it is not a standalone security requirement, its increasing risk to cause denial of service attacks makes it a highly important one.
- Applications are the primary tools that allow people to communicate, access, process and transform information.

Top 10 Vulnerabilities in Applications

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

Top Vulnerabilities in IT Infrastructure and Applications

- With rapid developments in technology and evolving threat landscape, organizations are increasingly required to address the vulnerabilities within their IT Infrastructure (compute, storage, network and security devices).
- Network devices are commonly targeted by hackers to destabilize the entire network or to steal information.



Top Vulnerabilities in IT Infrastructure

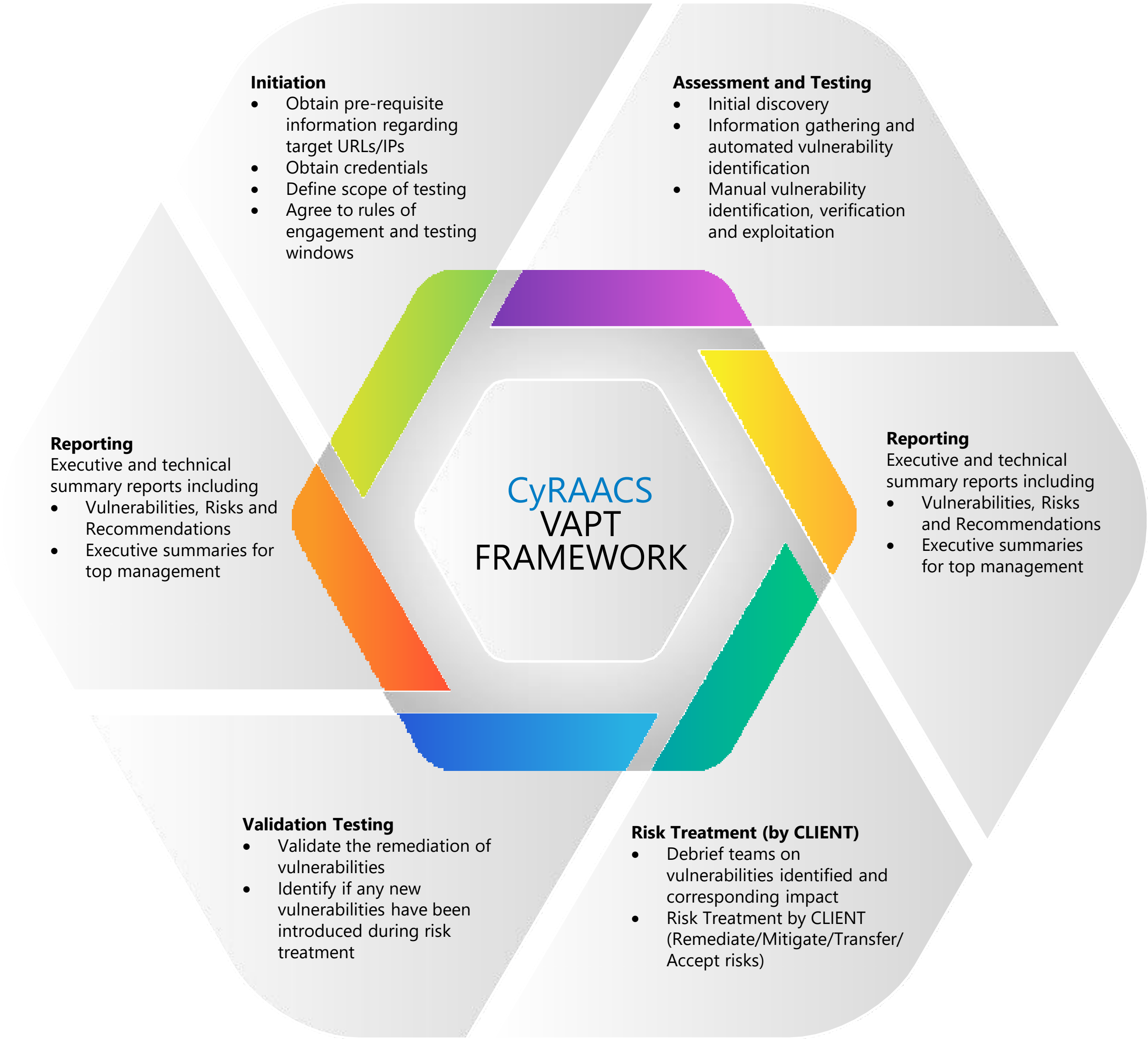
- Legacy Software
- Default Configuration
- Lack of Encryption
- Remote Access Policies
- Lack of Network Segmentation
- DDOS attacks
- Web Application Attacks
- Malware
- Command Injection and Parameters Manipulation

Vulnerability Assessments and Penetration Testing

- Periodic Vulnerability Assessment & Penetration Testing (VAPT) are now mandated by regulatory directives. contractual agreements, standards and frameworks.
- Vulnerability Assessment focuses on creating a list of identified vulnerabilities and establishing a plan to remediate findings.
- The focus of a Penetration Test is to demonstrate success against the testing objective like breaching an organization's border security controls, gaining administrative rights to a key system etc.
- CyRAACS can manage your VAPT requirements and help you mitigate security risks proactively.
- We tailor our comprehensive VAPT Framework to meet customer requirements and leverage our program management, risk management, technical, and analytical skills to deliver quality, proven and cost-effective services.

Standards	• ISO 27001:2013 • PCI:DSS • SOC 2 • HIPAA • CSA STAR
Regulatory	• NYDFS Cybersecurity Regulations • Gramm–Leach–Bliley Act • Federal Financial Institutions Examination Council • RBI Guidelines • IRDAI Guidelines
Frameworks	• COBIT 5.0 • NIST Special Publication 800-53

VAPT Framework



CyRAACS VAPT FRAMEWORK

Initiation

- Obtain pre-requisite information regarding target URLs/IPs
- Obtain credentials
- Define scope of testing
- Agree to rules of engagement and testing windows

Assessment and Testing

- Initial discovery
- Information gathering and automated vulnerability identification
- Manual vulnerability identification, verification and exploitation

Reporting

Executive and technical summary reports including

- Vulnerabilities, Risks and Recommendations
- Executive summaries for top management

Risk Treatment (by CLIENT)

- Debrief teams on vulnerabilities identified and corresponding impact
- Risk Treatment by CLIENT (Remediate/Mitigate/Transfer/ Accept risks)

Validation Testing

- Validate the remediation of vulnerabilities
- Identify if any new vulnerabilities have been introduced during risk treatment

Reporting

Executive and technical summary reports including

- Vulnerabilities, Risks and Recommendations
- Executive summaries for top management

External Infrastructure Testing

Automated Vulnerability Scanning

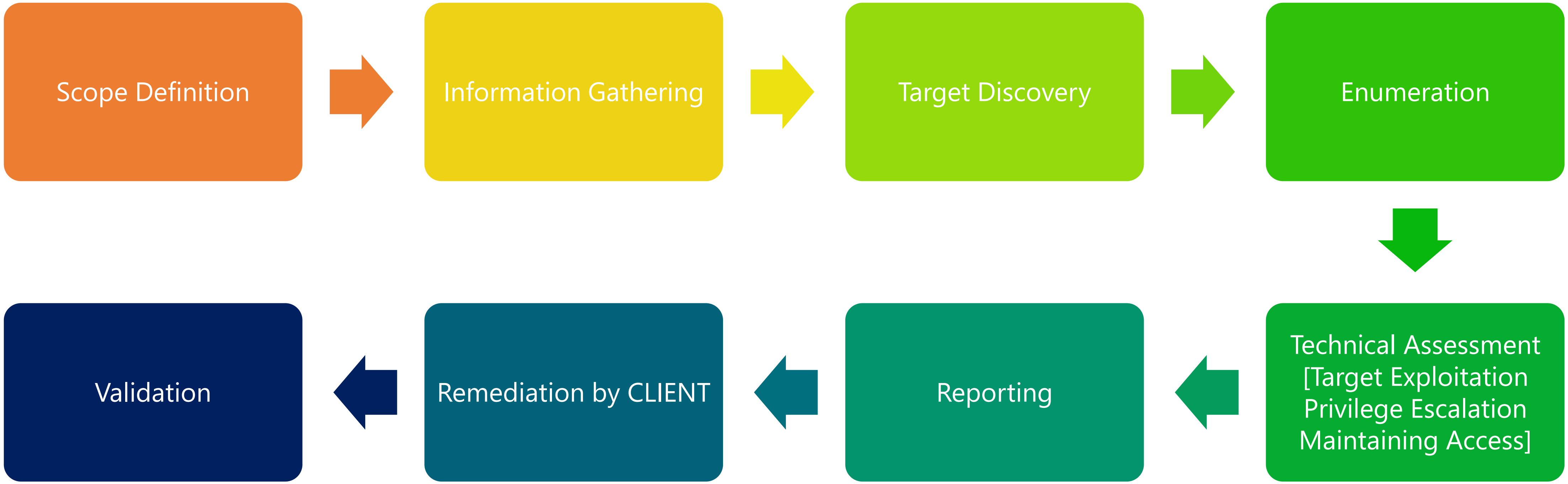
Internal Infrastructure Testing

Web Application Security Assessment

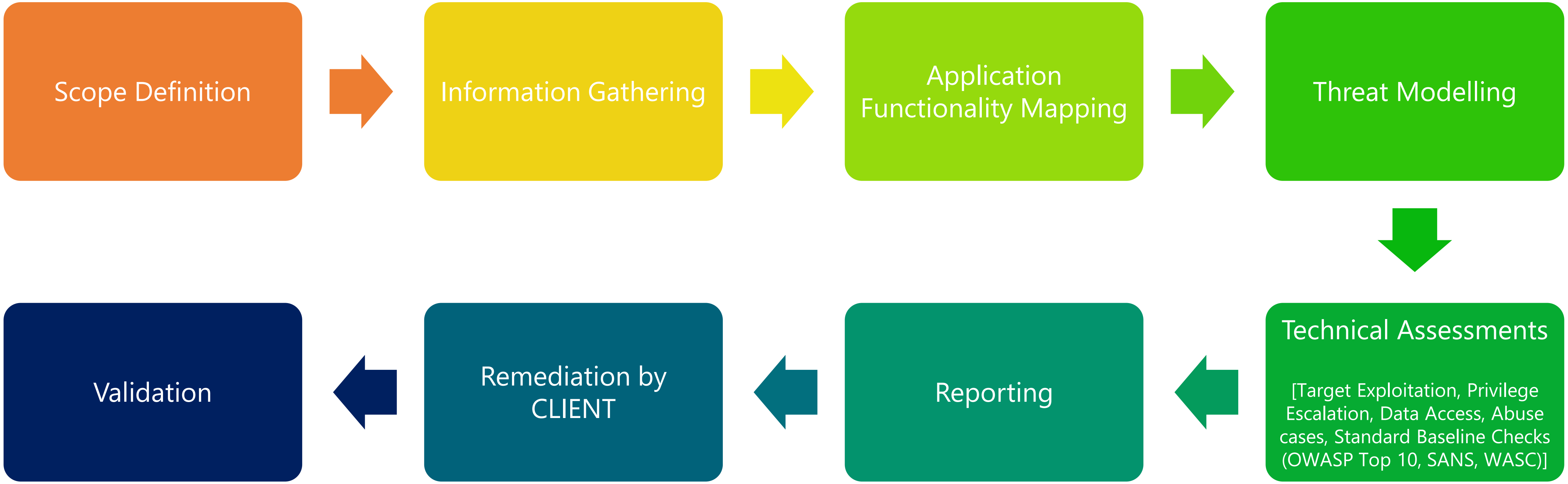
Mobile Application Security Assessment

Secure Code Review

Methodology – Infrastructure Testing



Methodology – Application Security Assessment



Scope Definition

Information Gathering

Application Functionality Mapping

Threat Modelling

Technical Assessments

[Target Exploitation, Privilege Escalation, Data Access, Abuse cases, Standard Baseline Checks (OWASP Top 10, SANS, WASC)]

Reporting

Remediation by CLIENT

Validation

Our Expertise

Tool	Detail
Nessus Professional	Infrastructure Scanning
Qualys	Web Application Scanning
Fortify Web Inspect	Web Application Scanning
Burp Suite	Penetration Testing / Web Application Scanning
Metasploit	Penetration Testing
Wireshark	Infrastructure Scanning
Charles	Infrastructure Scanning
Nikto	Penetration Testing
SQLmap	Penetration Testing / DB Scanner
W3AF	Web Application Scanning
AirCrack-ng	Infrastructure Scanning
Netcat	Multipurpose Tool
TCPDUMP	Infrastructure Scanning / Sniffer
Wireshark	Infrastructure Scanning / Sniffer
Kismet	Infrastructure Scanning
WebScarab	Web Application Scanning
OpenSSL Toolkit	Infrastructure scanning
Fiddler / Firebug	Web Application Scanning
SQLNinja	Penetration Testing / DB Scanner
Nirsoft Suite	Multipurpose Toolset
Sysinternals Suite	Multipurpose Toolset

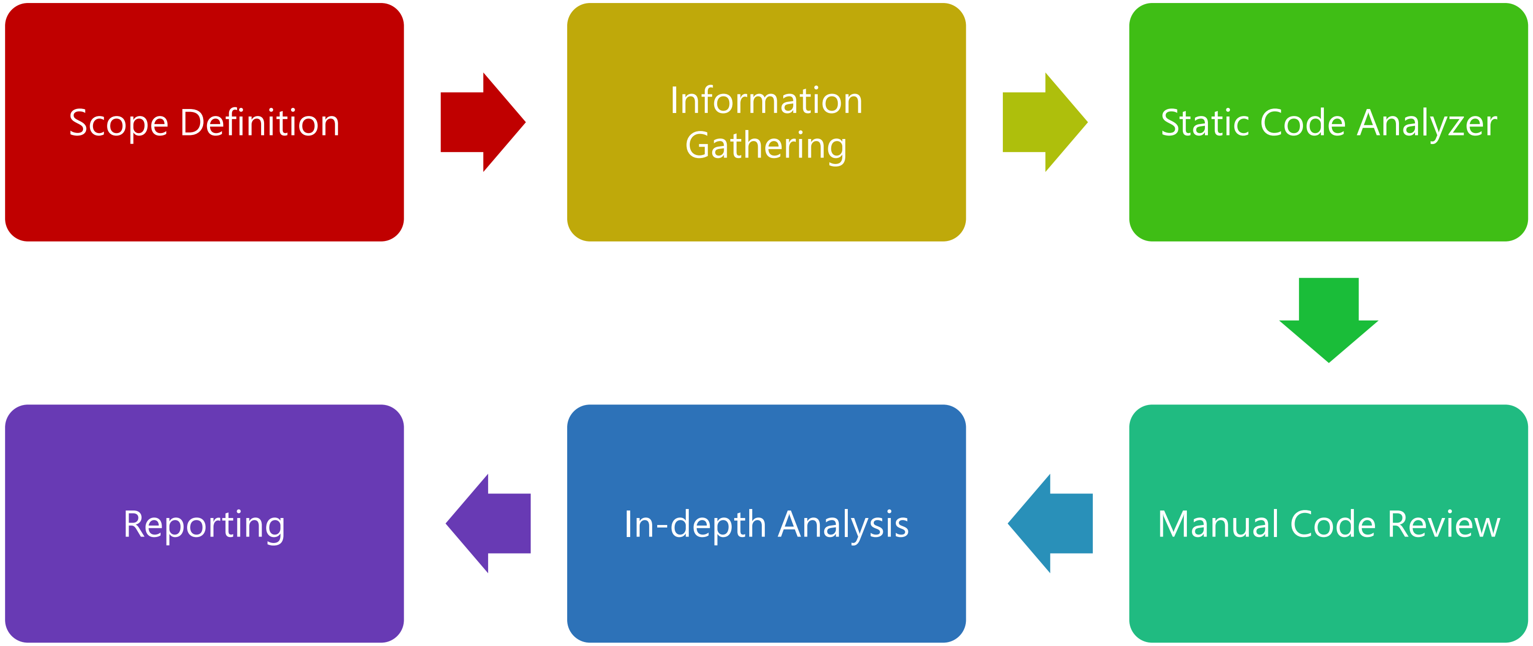
Technology	Specific systems
Operating Systems	Windows, Unix – IBM AIX, Linux, Sun Solaris
Databases	Oracle, MS SQL Server, Sybase, MySQL, SQLBase, Azure DB
Routers	CISCO, Sophos, Fortigate, Aruba
Firewalls	Checkpoint, CISCO Firepower, Linux, Netscreen, Palo Alto, Cyberoam, McAfee NextGen Firewall
IDS	Palo Alto, Crowdstrike, Cisco Firepower NGIPS, McAfee NSP, Trend Micro TippingPoint
Security Monitoring	net Forensics, Splunk, Netwitness, AlienVault, SolarWinds
Mail Servers	Sendmail, Qmail, Microsoft Exchange, Outlook Web Access, Office 365
Web Servers	Apache, NIGNX, IIS, Netscape Enterprise, ColdFusion
Web Technologies	ASP, ASP.NET, JSP, Java Servlets and Applets, Perl, PHP, Python
Programming Languages	C/C++, C#, Visual Basic, Visual C++, .NET, Shell Scripting, Java, PL/SQL, T-SQL

- The tables provides our technological knowhow and list of tools that we may use for our assessments.
- Actual usage of tools may vary depending on the engagement requirements

Secure Code Review

- Secure Code Review is used to assess identified business security risks implemented in the application's development life cycle.
- It ensures that the implemented application security checks and mitigations are effective and correct according to the OWASP, NIST, SANS TOP 25 and WEBAPPSEC security standards and guidelines and according to the recommended implementation requirements based on the application development stack / platform.
- The review process identifies the gaps and issues with the implementation from the development and maintenance viewpoint.
- It also ensures adequacy of the implemented measures to withstand the common and widespread security vulnerabilities for all kind of applications.

Our Methodology



Tool	Detail
Fortify SCA	Secure Code Review
PMD	Secure Code Review
Checkstyle	Secure Code Review
FingBugs	Secure Code Review
Source meter	Secure Code Review
SonarQube	Secure Code Review
VCG	Secure Code Review

- The tables provides list of tools that we may use for our assessments.
- Actual usage of tools may vary depending on the engagement requirements

Why CyRAACS

Our Credentials

- Accurate service; automated assessment tools supported by manual verification
- Controlled service; tests designed to ensure no steps are missed and reduce impact on target systems
- Repeatable service; test parameters recorded to allow retesting under the same conditions
- Specific client needs can be included
- Highly skilled and experienced consultants

Quality assurance

- This is not just a slogan; it is central to everything we do.
- There are many factors that distinguish us, but ultimately it is the quality of our people that makes the difference and enables us to deliver seamless, consistent, independent and objective high-quality service, worldwide.

Our Deliverables

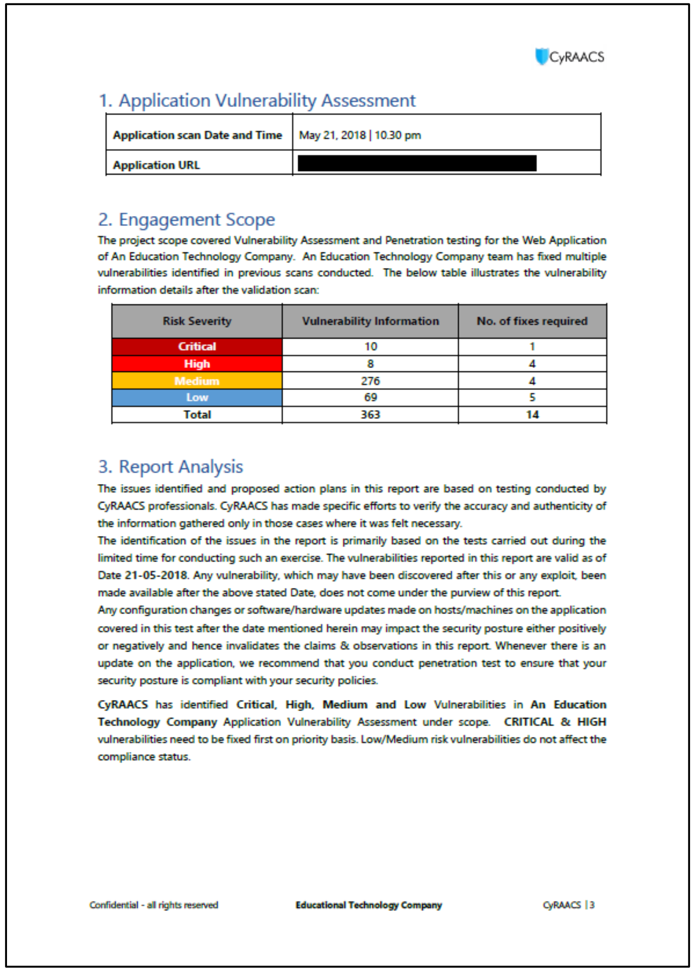
We deliver clear and actionable results:

- Effort put into presenting findings in a clear and actionable report of findings;
- Includes a concise executive summary;
- Summary of findings shows:
  - Priority of each significant vulnerability;
  - Possible remediation actions;
  - Direct links to relevant bulletins, patches and advisories.
- Detailed results are presented in clear language;
- Findings are grouped by Risk level.

Sample Reports

Snapshots of Sample Reports from some of our engagements

Sample Reports – Application VAPT



CyRAACS

1. Application Vulnerability Assessment

Application scan Date and Time	May 21, 2018 | 10.30 pm
Application URL	[redacted]

2. Engagement Scope

The project scope covered Vulnerability Assessment and Penetration testing for the Web Application of An Education Technology Company. An Education Technology Company team has fixed multiple vulnerabilities identified in previous scans conducted. The below table illustrates the vulnerability information details after the validation scan:

Risk Severity	Vulnerability Information	No. of fixes required
Critical	10	1
High	8	4
Medium	276	4
Low	69	5
Total	**363**	**14**

3. Report Analysis

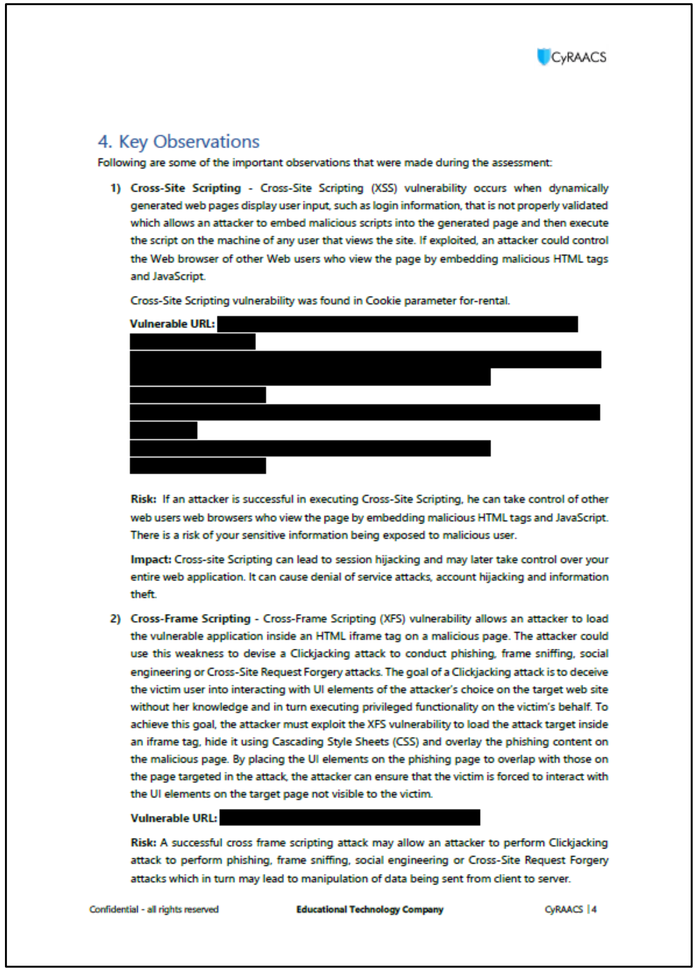
The issues identified and proposed action plans in this report are based on testing conducted by CyRAACS professionals. CyRAACS has made specific efforts to verify the accuracy and authenticity of the information gathered only in those cases where it was felt necessary.

The identification of the issues in the report is primarily based on the tests carried out during the limited time for conducting such an exercise. The vulnerabilities reported in this report are valid as of Date **21-05-2018**. Any vulnerability, which may have been discovered after this or any exploit, been made available after the above stated Date, does not come under the purview of this report.

Any configuration changes or software/hardware updates made on hosts/machines on the application covered in this test after the date mentioned herein may impact the security posture either positively or negatively and hence invalidates the claims & observations in this report. Whenever there is an update on the application, we recommend that you conduct penetration test to ensure that your security posture is compliant with your security policies.

CyRAACS has identified **Critical, High, Medium and Low** Vulnerabilities in **An Education Technology Company** Application Vulnerability Assessment under scope. **CRITICAL & HIGH** vulnerabilities need to be fixed first on priority basis. Low/Medium risk vulnerabilities do not affect the compliance status.

Confidential - all rights reserved **Educational Technology Company** CyRAACS | 3



CyRAACS

4. Key Observations

Following are some of the important observations that were made during the assessment:

1) **Cross-Site Scripting** - Cross-Site Scripting (XSS) vulnerability occurs when dynamically generated web pages display user input, such as login information, that is not properly validated which allows an attacker to embed malicious scripts into the generated page and then execute the script on the machine of any user that views the site. If exploited, an attacker could control the Web browser of other Web users who view the page by embedding malicious HTML tags and JavaScript.

   Cross-Site Scripting vulnerability was found in Cookie parameter for-rental.

   Vulnerable URL: [redacted]

   Risk: If an attacker is successful in executing Cross-Site Scripting, he can take control of other web users web browsers who view the page by embedding malicious HTML tags and JavaScript. There is a risk of your sensitive information being exposed to malicious user.

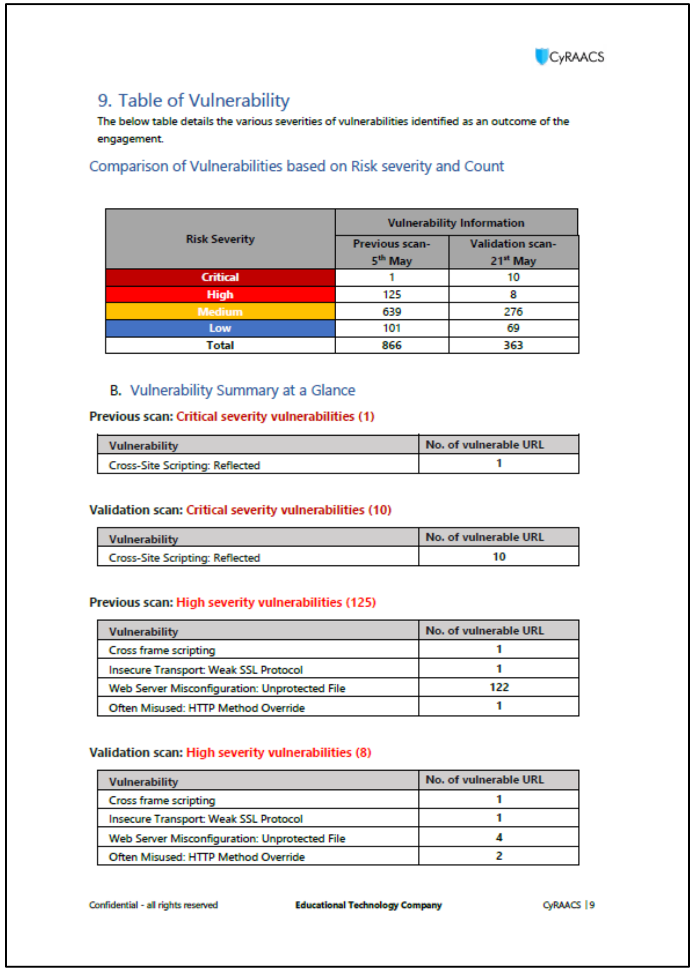
   Impact: Cross-site Scripting can lead to session hijacking and may later take control over your entire web application. It can cause denial of service attacks, account hijacking and information theft.

2) **Cross-Frame Scripting** - Cross-Frame Scripting (XFS) vulnerability allows an attacker to load the vulnerable application inside an HTML iframe tag on a malicious page. The attacker could use this weakness to devise a Clickjacking attack to conduct phishing, frame sniffing, social engineering or Cross-Site Request Forgery attacks. The goal of a Clickjacking attack is to deceive the victim user into interacting with UI elements of the attacker's choice on the target web site without her knowledge and in turn executing privileged functionality on the victim's behalf. To achieve this goal, the attacker must exploit the XFS vulnerability to load the attack target inside an iframe tag, hide it using Cascading Style Sheets (CSS) and overlay the phishing content on the malicious page. By placing the UI elements on the phishing page to overlap with those on the page targeted in the attack, the attacker can ensure that the victim is forced to interact with the UI elements on the target page not visible to the victim.

   Vulnerable URL: [redacted]

   Risk: A successful cross frame scripting attack may allow an attacker to perform Clickjacking attack to perform phishing, frame sniffing, social engineering or Cross-Site Request Forgery attacks which in turn may lead to manipulation of data being sent from client to server.

Confidential - all rights reserved **Educational Technology Company** CyRAACS | 4



CyRAACS

9. Table of Vulnerability

The below table details the various severities of vulnerabilities identified as an outcome of the engagement.

Comparison of Vulnerabilities based on Risk severity and Count

Risk Severity	Vulnerability Information	
	Previous scan- 5th May	Validation scan- 21st May
Critical	1	10
High	125	8
Medium	639	276
Low	101	69
Total	**866**	**363**

B. Vulnerability Summary at a Glance

Previous scan: Critical severity vulnerabilities (1)

Vulnerability	No. of vulnerable URL
Cross-Site Scripting: Reflected	1

Validation scan: Critical severity vulnerabilities (10)

Vulnerability	No. of vulnerable URL
Cross-Site Scripting: Reflected	10

Previous scan: High severity vulnerabilities (125)

Vulnerability	No. of vulnerable URL
Cross frame scripting	1
Insecure Transport: Weak SSL Protocol	1
Web Server Misconfiguration: Unprotected File	122
Often Misused: HTTP Method Override	1

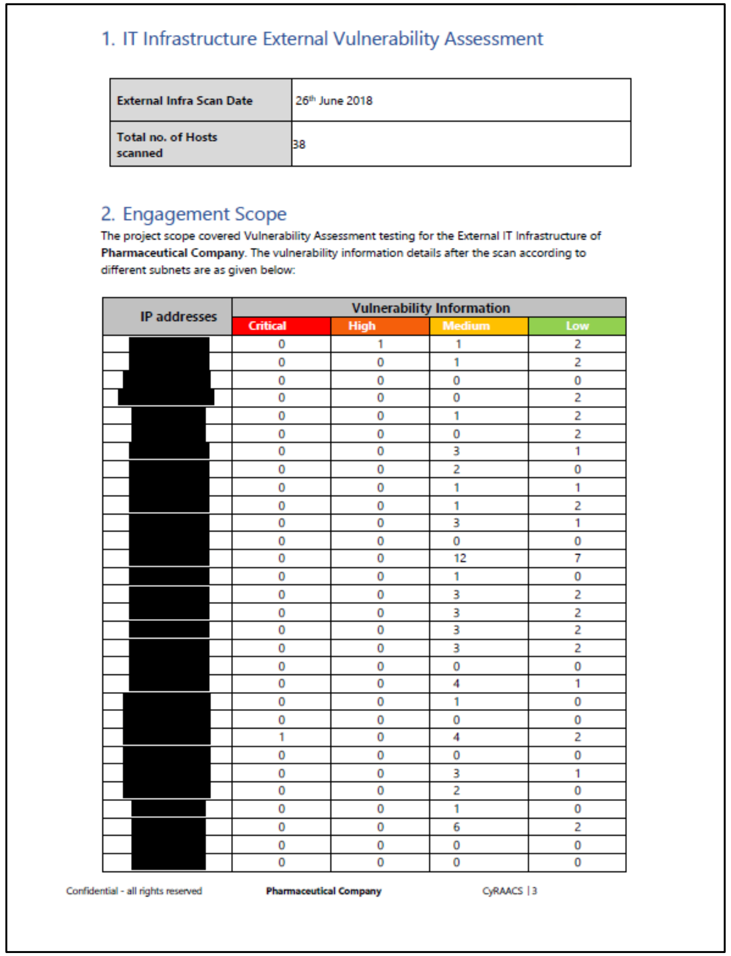
Validation scan: High severity vulnerabilities (8)

Vulnerability	No. of vulnerable URL
Cross frame scripting	1
Insecure Transport: Weak SSL Protocol	1
Web Server Misconfiguration: Unprotected File	4
Often Misused: HTTP Method Override	2

Confidential - all rights reserved **Educational Technology Company** CyRAACS | 9

Sample Reports. For reference purposes only.

Sample Reports – Infrastructure VAPT



1. IT Infrastructure External Vulnerability Assessment

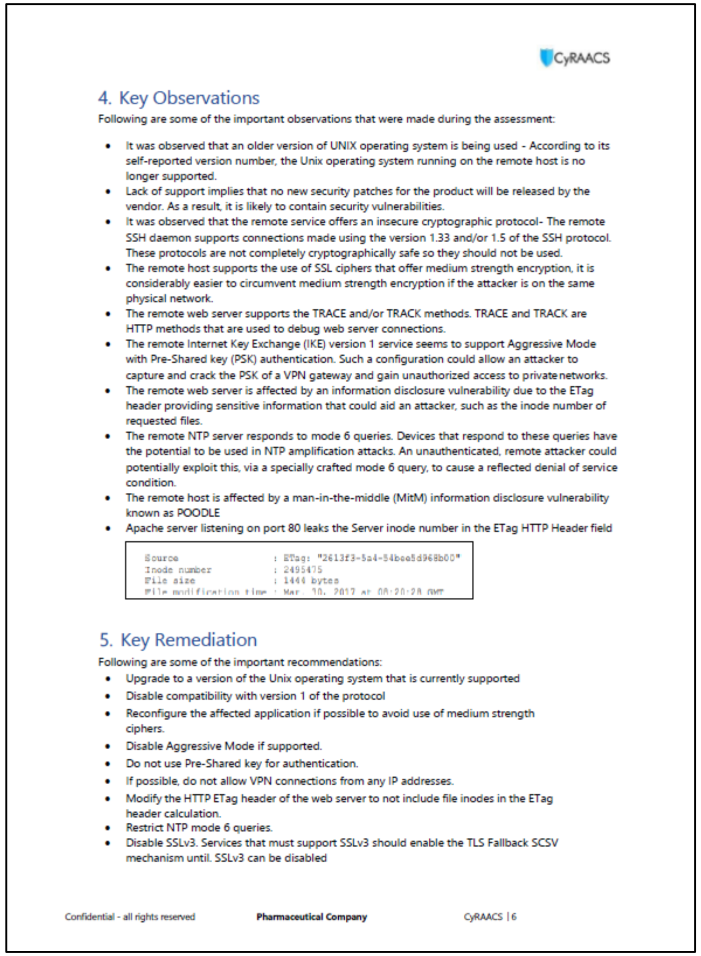
External Infra Scan Date	26th June 2018
Total no. of Hosts scanned	38

2. Engagement Scope

The project scope covered Vulnerability Assessment testing for the External IT Infrastructure of **Pharmaceutical Company**. The vulnerability information details after the scan according to different subnets are as given below:

IP addresses	Vulnerability Information			
	Critical	High	Medium	Low
[redacted]	0	1	1	2
[redacted]	0	0	1	2
[redacted]	0	0	0	0
[redacted]	0	0	0	2
[redacted]	0	0	1	2
[redacted]	0	0	0	2
[redacted]	0	0	3	1
[redacted]	0	0	2	0
[redacted]	0	0	1	1
[redacted]	0	0	1	2
[redacted]	0	0	3	1
[redacted]	0	0	0	0
[redacted]	0	0	12	7
[redacted]	0	0	1	0
[redacted]	0	0	3	2
[redacted]	0	0	3	2
[redacted]	0	0	3	2
[redacted]	0	0	3	2
[redacted]	0	0	0	0
[redacted]	0	0	4	1
[redacted]	0	0	1	0
[redacted]	0	0	0	0
[redacted]	1	0	4	2
[redacted]	0	0	0	0
[redacted]	0	0	3	1
[redacted]	0	0	2	0
[redacted]	0	0	1	0
[redacted]	0	0	6	2
[redacted]	0	0	0	0
[redacted]	0	0	0	0

Confidential - all rights reserved **Pharmaceutical Company** CyRAACS | 3



CyRAACS

4. Key Observations

Following are some of the important observations that were made during the assessment:

- It was observed that an older version of UNIX operating system is being used - According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.
- Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
- It was observed that the remote service offers an insecure cryptographic protocol- The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol. These protocols are not completely cryptographically safe so they should not be used.
- The remote host supports the use of SSL ciphers that offer medium strength encryption, it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.
- The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.
- The remote Internet Key Exchange (IKE) version 1 service seems to support Aggressive Mode with Pre-Shared key (PSK) authentication. Such a configuration could allow an attacker to capture and crack the PSK of a VPN gateway and gain unauthorized access to private networks.
- The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.
- The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.
- The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE
- Apache server listening on port 80 leaks the Server inode number in the ETag HTTP Header field

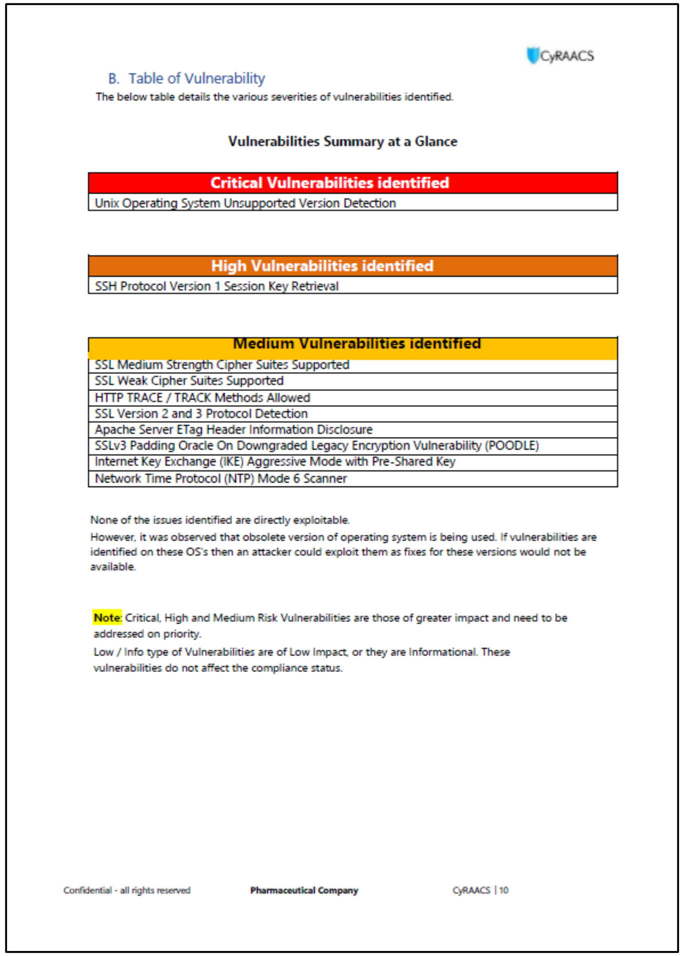
```
Source                 : ETag: "2613f3-5a4-54bee5d968b00"
Inode number           : 2495475
File size              : 1444 bytes
File modification time : Mar. 10, 2017 at 08:20:20 GMT
```

5. Key Remediation

Following are some of the important recommendations:

- Upgrade to a version of the Unix operating system that is currently supported
- Disable compatibility with version 1 of the protocol
- Reconfigure the affected application if possible to avoid use of medium strength ciphers.
- Disable Aggressive Mode if supported.
- Do not use Pre-Shared key for authentication.
- If possible, do not allow VPN connections from any IP addresses.
- Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation.
- Restrict NTP mode 6 queries.
- Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until. SSLv3 can be disabled

Confidential - all rights reserved **Pharmaceutical Company** CyRAACS | 6



CyRAACS

B. Table of Vulnerability

The below table details the various severities of vulnerabilities identified.

Vulnerabilities Summary at a Glance

Critical Vulnerabilities identified
Unix Operating System Unsupported Version Detection

High Vulnerabilities identified
SSH Protocol Version 1 Session Key Retrieval

Medium Vulnerabilities identified
SSL Medium Strength Cipher Suites Supported
SSL Weak Cipher Suites Supported
HTTP TRACE / TRACK Methods Allowed
SSL Version 2 and 3 Protocol Detection
Apache Server ETag Header Information Disclosure
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key
Network Time Protocol (NTP) Mode 6 Scanner

None of the issues identified are directly exploitable.

However, it was observed that obsolete version of operating system is being used. If vulnerabilities are identified on these OS's then an attacker could exploit them as fixes for these versions would not be available.

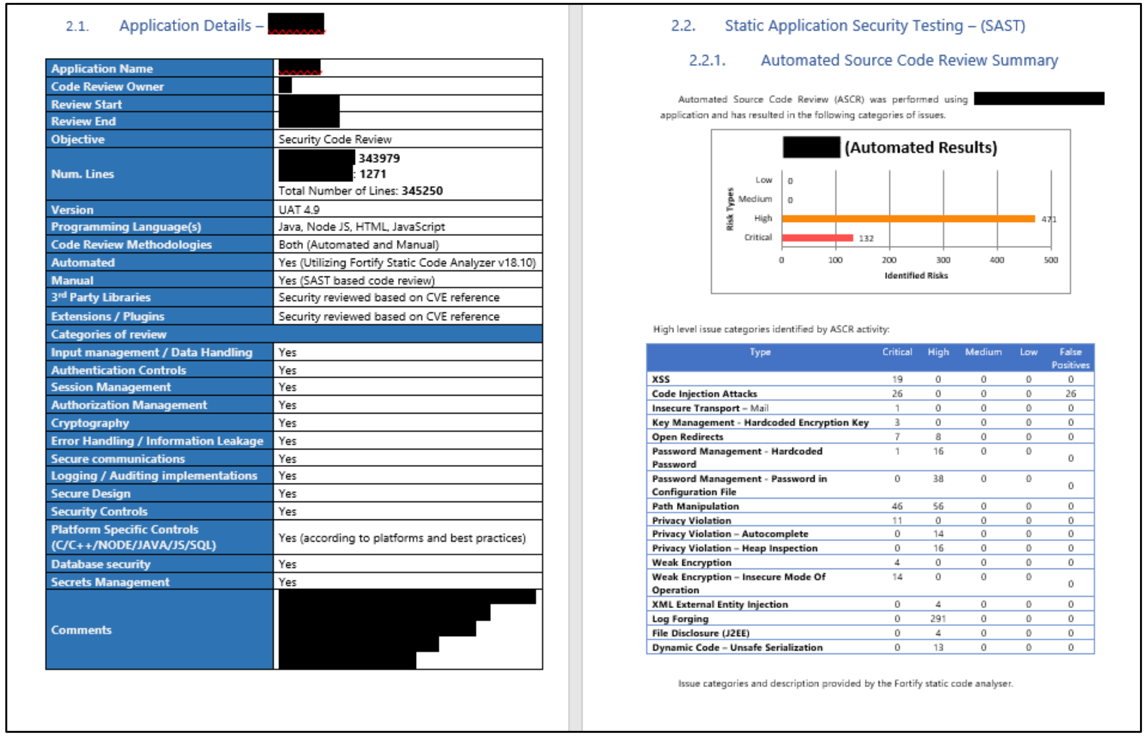
Note: Critical, High and Medium Risk Vulnerabilities are those of greater impact and need to be addressed on priority.

Low / Info type of Vulnerabilities are of Low Impact, or they are Informational. These vulnerabilities do not affect the compliance status.

Confidential - all rights reserved **Pharmaceutical Company** CyRAACS | 10

Sample Reports. For reference purposes only.

Sample Report – Secure Code Review



2.1. Application Details – [redacted]

Application Name	[redacted]
Code Review Owner	[redacted]
Review Start	[redacted]
Review End	[redacted]
Objective	Security Code Review
Num. Lines	[redacted] **343979** [redacted]: **1271** Total Number of Lines: **345250**
Version	UAT 4.9
Programming Language(s)	Java, Node JS, HTML, JavaScript
Code Review Methodologies	Both (Automated and Manual)
Automated	Yes (Utilizing Fortify Static Code Analyzer v18.10)
Manual	Yes (SAST based code review)
3rd Party Libraries	Security reviewed based on CVE reference
Extensions / Plugins	Security reviewed based on CVE reference
Categories of review	
Input management / Data Handling	Yes
Authentication Controls	Yes
Session Management	Yes
Authorization Management	Yes
Cryptography	Yes
Error Handling / Information Leakage	Yes
Secure communications	Yes
Logging / Auditing implementations	Yes
Secure Design	Yes
Security Controls	Yes
Platform Specific Controls (C/C++/NODE/JAVA/JS/SQL)	Yes (according to platforms and best practices)
Database security	Yes
Secrets Management	Yes
Comments	[redacted]

2.2. Static Application Security Testing – (SAST)

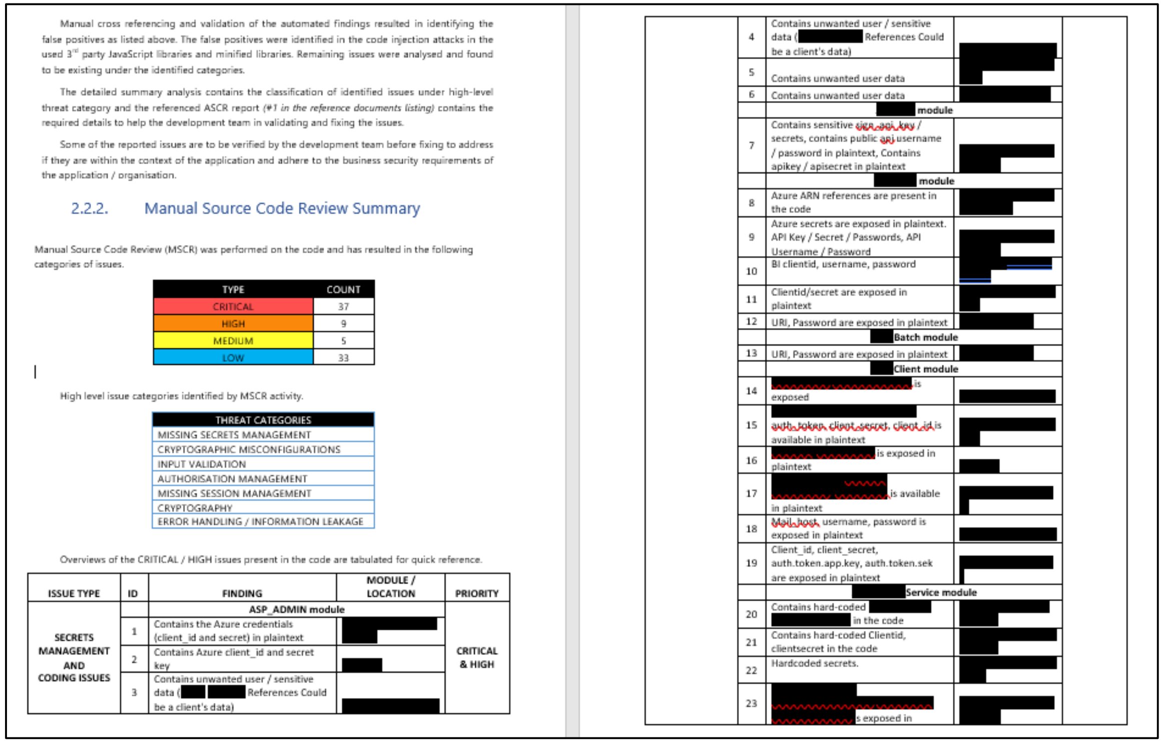
2.2.1. Automated Source Code Review Summary

Automated Source Code Review (ASCR) was performed using [redacted] application and has resulted in the following categories of issues.

High level issue categories identified by ASCR activity:

Type	Critical	High	Medium	Low	False Positives
XSS	19	0	0	0	0
Code Injection Attacks	26	0	0	0	26
Insecure Transport – Mail	1	0	0	0	0
Key Management - Hardcoded Encryption Key	3	0	0	0	0
Open Redirects	7	8	0	0	0
Password Management - Hardcoded Password	1	16	0	0	0
Password Management - Password in Configuration File	0	38	0	0	0
Path Manipulation	46	56	0	0	0
Privacy Violation	11	0	0	0	0
Privacy Violation – Autocomplete	0	14	0	0	0
Privacy Violation – Heap Inspection	0	16	0	0	0
Weak Encryption	4	0	0	0	0
Weak Encryption – Insecure Mode Of Operation	14	0	0	0	0
XML External Entity Injection	0	4	0	0	0
Log Forging	0	291	0	0	0
File Disclosure (J2EE)	0	4	0	0	0
Dynamic Code – Unsafe Serialization	0	13	0	0	0

Issue categories and description provided by the Fortify static code analyser.



Manual cross referencing and validation of the automated findings resulted in identifying the false positives as listed above. The false positives were identified in the code injection attacks in the used 3rd party JavaScript libraries and minified libraries. Remaining issues were analysed and found to be existing under the identified categories.

The detailed summary analysis contains the classification of identified issues under high-level threat category and the referenced ASCR report *(#1 in the reference documents listing)* contains the required details to help the development team in validating and fixing the issues.

Some of the reported issues are to be verified by the development team before fixing to address if they are within the context of the application and adhere to the business security requirements of the application / organisation.

2.2.2. Manual Source Code Review Summary

Manual Source Code Review (MSCR) was performed on the code and has resulted in the following categories of issues.

TYPE	COUNT
CRITICAL	37
HIGH	9
MEDIUM	5
LOW	33

High level issue categories identified by MSCR activity.

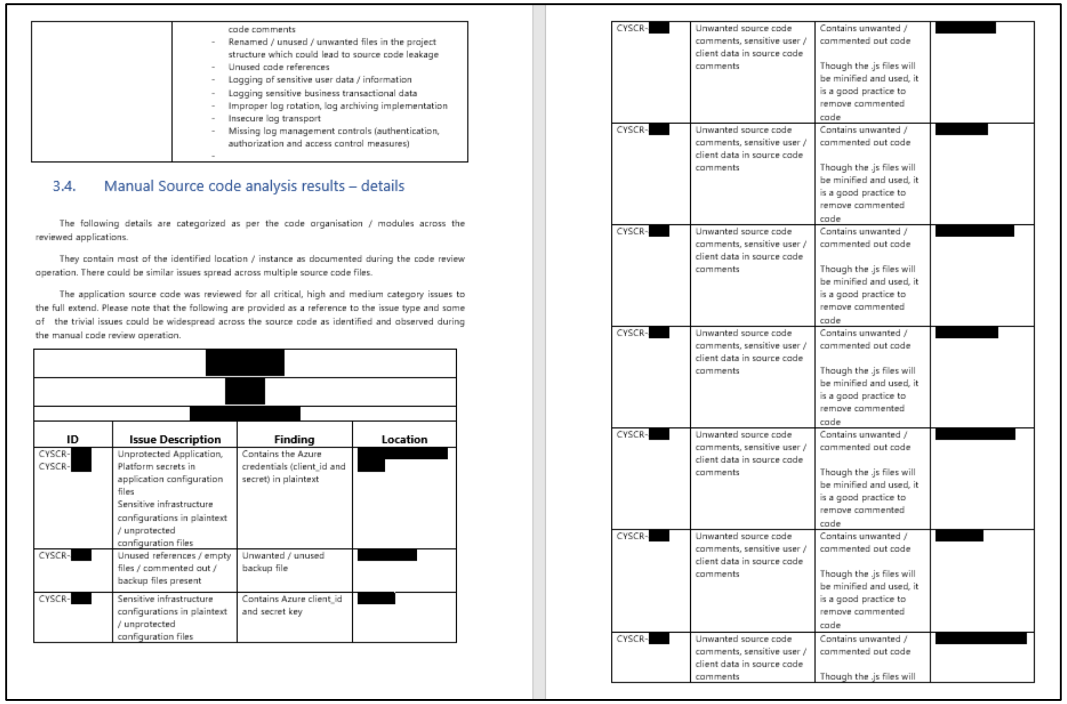
THREAT CATEGORIES
MISSING SECRETS MANAGEMENT
CRYPTOGRAPHIC MISCONFIGURATIONS
INPUT VALIDATION
AUTHORISATION MANAGEMENT
MISSING SESSION MANAGEMENT
CRYPTOGRAPHY
ERROR HANDLING / INFORMATION LEAKAGE

Overviews of the CRITICAL / HIGH issues present in the code are tabulated for quick reference.

ISSUE TYPE	ID	FINDING	MODULE / LOCATION	PRIORITY
SECRETS MANAGEMENT AND CODING ISSUES		**ASP_ADMIN module**		CRITICAL & HIGH
	1	Contains the Azure credentials (client_id and secret) in plaintext	[redacted]	
	2	Contains Azure client_id and secret key	[redacted]	
	3	Contains unwanted user / sensitive data ([redacted] [redacted] References Could be a client's data)	[redacted]	
	4	Contains unwanted user / sensitive data ([redacted] References Could be a client's data)	[redacted]	
	5	Contains unwanted user data	[redacted]	
	6	Contains unwanted user data	[redacted]	
		[redacted] **module**		
	7	Contains sensitive sign_api_key / secrets, contains public api username / password in plaintext, Contains apikey / apisecret in plaintext	[redacted]	
		[redacted] **module**		
	8	Azure ARN references are present in the code	[redacted]	
	9	Azure secrets are exposed in plaintext. API Key / Secret / Passwords, API Username / Password	[redacted]	
	10	BI clientid, username, password	[redacted]	
	11	Clientid/secret are exposed in plaintext	[redacted]	
	12	URI, Password are exposed in plaintext	[redacted]	
		[redacted] **Batch module**		
	13	URI, Password are exposed in plaintext	[redacted]	
		[redacted] **Client module**		
	14	[redacted] is exposed	[redacted]	
	15	[redacted] auth_token, client_secret, client_id is available in plaintext	[redacted]	
	16	[redacted] is exposed in plaintext	[redacted]	
	17	[redacted] is available in plaintext	[redacted]	
	18	Mail_host, username, password is exposed in plaintext	[redacted]	
	19	Client_id, client_secret, auth.token.app.key, auth.token.sek are exposed in plaintext	[redacted]	
		[redacted] **Service module**		
	20	Contains hard-coded [redacted] [redacted] in the code	[redacted]	
	21	Contains hard-coded Clientid, clientsecret in the code	[redacted]	
	22	Hardcoded secrets.	[redacted]	
	23	[redacted] s exposed in	[redacted]	

Sample Reports. For reference purposes only.

Sample Report – Secure Code Review



	code comments - Renamed / unused / unwanted files in the project structure which could lead to source code leakage - Unused code references - Logging of sensitive user data / information - Logging sensitive business transactional data - Improper log rotation, log archiving implementation - Insecure log transport - Missing log management controls (authentication, authorization and access control measures) -

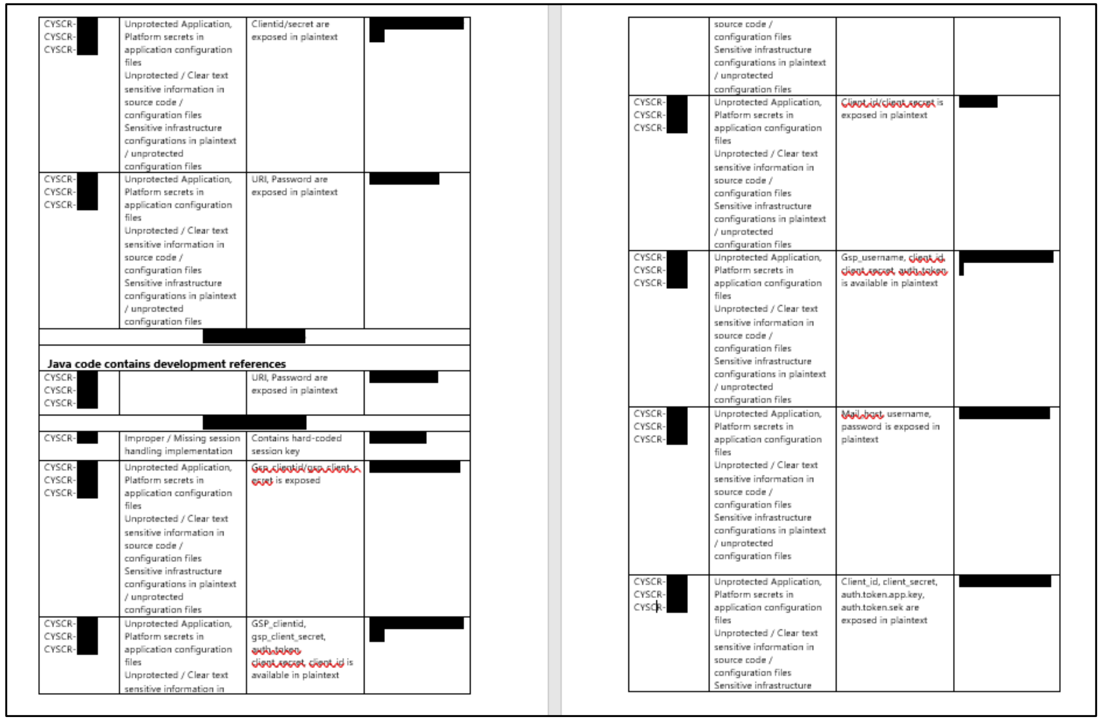
3.4. Manual Source code analysis results – details

The following details are categorized as per the code organisation / modules across the reviewed applications.

They contain most of the identified location / instance as documented during the code review operation. There could be similar issues spread across multiple source code files.

The application source code was reviewed for all critical, high and medium category issues to the full extend. Please note that the following are provided as a reference to the issue type and some of the trivial issues could be widespread across the source code as identified and observed during the manual code review operation.

[redacted]			
[redacted]			
[redacted]			
ID	**Issue Description**	**Finding**	**Location**
CYSCR- CYSCR- [redacted]	Unprotected Application, Platform secrets in application configuration files Sensitive infrastructure configurations in plaintext / unprotected configuration files	Contains the Azure credentials (client_id and secret) in plaintext	[redacted]
CYSCR- [redacted]	Unused references / empty files / commented out / backup files present	Unwanted / unused backup file	[redacted]
CYSCR- [redacted]	Sensitive infrastructure configurations in plaintext / unprotected configuration files	Contains Azure client_id and secret key	[redacted]
CYSCR- [redacted]	Unwanted source code comments, sensitive user / client data in source code comments	Contains unwanted / commented out code Though the .js files will be minified and used, it is a good practice to remove commented code	[redacted]
CYSCR- [redacted]	Unwanted source code comments, sensitive user / client data in source code comments	Contains unwanted / commented out code Though the .js files will be minified and used, it is a good practice to remove commented code	[redacted]
CYSCR- [redacted]	Unwanted source code comments, sensitive user / client data in source code comments	Contains unwanted / commented out code Though the .js files will be minified and used, it is a good practice to remove commented code	[redacted]
CYSCR- [redacted]	Unwanted source code comments, sensitive user / client data in source code comments	Contains unwanted / commented out code Though the .js files will be minified and used, it is a good practice to remove commented code	[redacted]
CYSCR- [redacted]	Unwanted source code comments, sensitive user / client data in source code comments	Contains unwanted / commented out code Though the .js files will be minified and used, it is a good practice to remove commented code	[redacted]
CYSCR- [redacted]	Unwanted source code comments, sensitive user / client data in source code comments	Contains unwanted / commented out code Though the .js files will be minified and used, it is a good practice to remove commented code	[redacted]
CYSCR- [redacted]	Unwanted source code comments, sensitive user / client data in source code comments	Contains unwanted / commented out code Though the .js files will	[redacted]



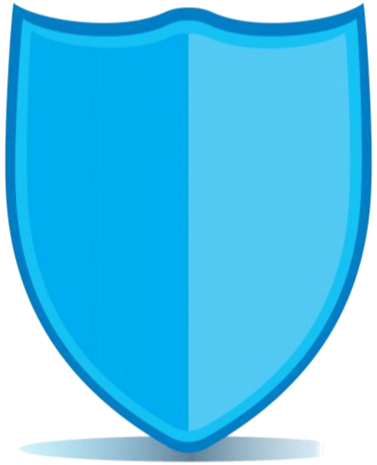
CYSCR- CYSCR- CYSCR- [redacted]	Unprotected Application, Platform secrets in application configuration files Unprotected / Clear text sensitive information in source code / configuration files Sensitive infrastructure configurations in plaintext / unprotected configuration files	Clientid/secret are exposed in plaintext	[redacted]
CYSCR- CYSCR- CYSCR- [redacted]	Unprotected Application, Platform secrets in application configuration files Unprotected / Clear text sensitive information in source code / configuration files Sensitive infrastructure configurations in plaintext / unprotected configuration files	URI, Password are exposed in plaintext	[redacted]
[redacted]			
Java code contains development references			
CYSCR- CYSCR- CYSCR- [redacted]		URI, Password are exposed in plaintext	[redacted]
[redacted]			
CYSCR- [redacted]	Improper / Missing session handling implementation	Contains hard-coded session key	[redacted]
CYSCR- CYSCR- CYSCR- [redacted]	Unprotected Application, Platform secrets in application configuration files Unprotected / Clear text sensitive information in source code / configuration files Sensitive infrastructure configurations in plaintext / unprotected configuration files	Gsp_clientid/gsp_client_secret is exposed	[redacted]
CYSCR- CYSCR- CYSCR- [redacted]	Unprotected Application, Platform secrets in application configuration files Unprotected / Clear text sensitive information in source code / configuration files Sensitive infrastructure configurations in plaintext / unprotected configuration files	GSP_clientid, gsp_client_secret, auth_token client_secret, client_id is available in plaintext	[redacted]
CYSCR- CYSCR- CYSCR- [redacted]	Unprotected Application, Platform secrets in application configuration files Unprotected / Clear text sensitive information in source code / configuration files Sensitive infrastructure configurations in plaintext / unprotected configuration files	Client_id/client_secret is exposed in plaintext	[redacted]
CYSCR- CYSCR- CYSCR- [redacted]	Unprotected Application, Platform secrets in application configuration files Unprotected / Clear text sensitive information in source code / configuration files Sensitive infrastructure configurations in plaintext / unprotected configuration files	Gsp_username, client_id, client_secret, auth_token is available in plaintext	[redacted]
CYSCR- CYSCR- CYSCR- [redacted]	Unprotected Application, Platform secrets in application configuration files Unprotected / Clear text sensitive information in source code / configuration files Sensitive infrastructure configurations in plaintext / unprotected configuration files	Mail_host, username, password is exposed in plaintext	[redacted]
CYSCR- CYSCR- CYSCR- [redacted]	Unprotected Application, Platform secrets in application configuration files Unprotected / Clear text sensitive information in source code / configuration files Sensitive infrastructure	Client_id, client_secret, auth.token.app.key, auth.token.sek are exposed in plaintext	[redacted]

Sample Reports. For reference purposes only.

About Us

Seamless Security through Collaboration and Innovation

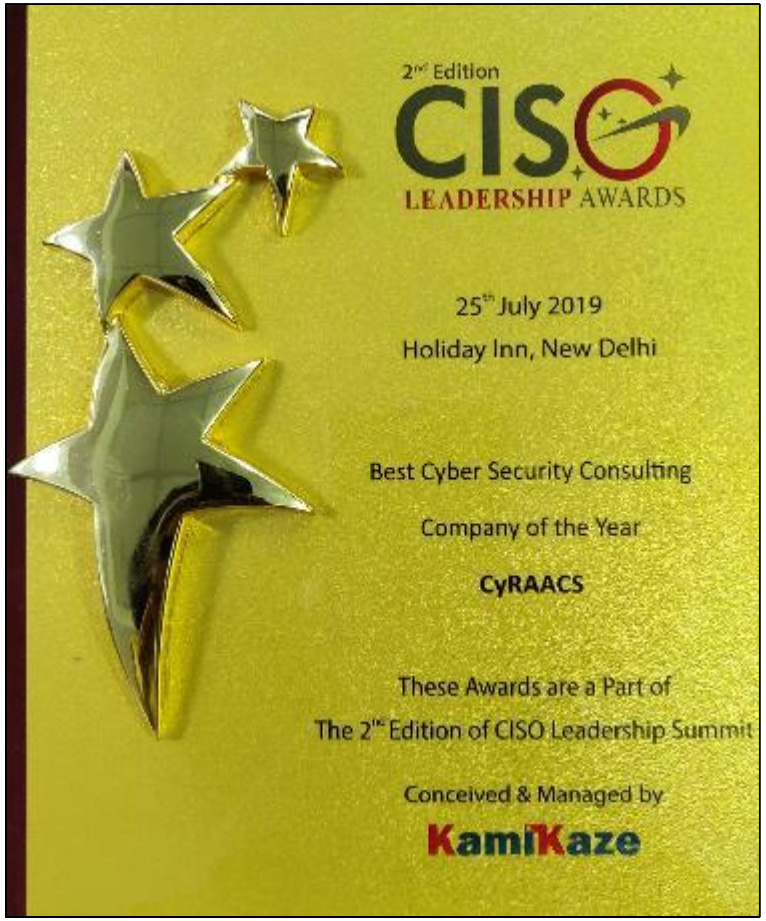
- CyRAACS was established to provide robust and sustainable cyber security solutions to organizations. Our focus is to tailor and integrate our solutions into client environments seamlessly, so they can focus on their core business completely.
- We work as an Extended Arm for our clients, managing their information security objectives and enhancing their posture.
- We accomplish this by Collaboration, Commitment, Innovation and Passion.
- We offer the full suite of services in Compliance Lifecycle – Framework, Assessment, Implementation and Audit services.
- Our Technical Services include Vulnerability Assessment and Penetration Testing, Code Reviews and niche services like Malware Analysis, Forensics, Study of Indicators of Compromise and Indicators of Attack.
- We are empaneled with **CERT-In** (Computer Emergency Response Team – India) and **Qualified Security Assessor** for PCI DSS.



Your Trusted Security Partner

About Us

- Proven track record of delivering complex projects across varied domains such as BFSI, Born-in-the-Cloud, Logistics, IT/ITES, Manufacturing, Pharma etc.
- Extensive experience in Information Security and Data Privacy Standards/Frameworks such as ISO 27001, PCI DSS, SOC 2, NIST 800-53, CSA STAR, GDPR,CCPA etc.
- Over 90 happy clients and 200+ successful engagement deliveries
- Cyber Security Solutions tailor-made to Client requirements
- Consultants with Leading Industry Certifications CISSP, CISA, CEH, CISM etc.



2nd Edition

CISO

LEADERSHIP AWARDS

25th July 2019

Holiday Inn, New Delhi

Best Cyber Security Consulting

Company of the Year

CyRAACS

These Awards are a Part of

The 2nd Edition of CISO Leadership Summit

Conceived & Managed by

KamiKaze

The Best Cyber Security Consulting Company of the Year – CISO Leadership Awards 2019

Our Leadership

Suresh Iyer
Co-Founder and CEO

- Over 28 Years of Experience in Technology, IT Security, Risk Management and Privacy areas
- Has served in CXO positions in many global organisations like Ocwen Financials, Altisource, Aditya Birla Minacs, eFunds and Bank of America
- An eminent speaker and panellist in many industry and security forums

- Multi-disciplinary leader with over 30 years of industry experience areas of Technology, Data Centre, IT Operations, Information Security etc.
- Has held CXO positions for global organizations such as Concentrix, Altisource, Convergys, Mphasis, IBM etc.
- **Qualified Security Assessor** for PCI DSS and Certified Information Security Manager

Murari Shanker
Co-Founder and COO

Signature Services

Governance and Compliance Services

- Control Assurance Services
- QSA Services for PCI DSS
- Third Party Risk Management
- Policy Management

Risk Advisory Services

- Information Security Risk Management
- Information Security Maturity Model Assessment
- Business Continuity Management

Technical Services

- Data Flow Analysis
- Vulnerability Assessment and Penetration Testing
- Secure Code Review
- Compliance As a Service for PCI DSS

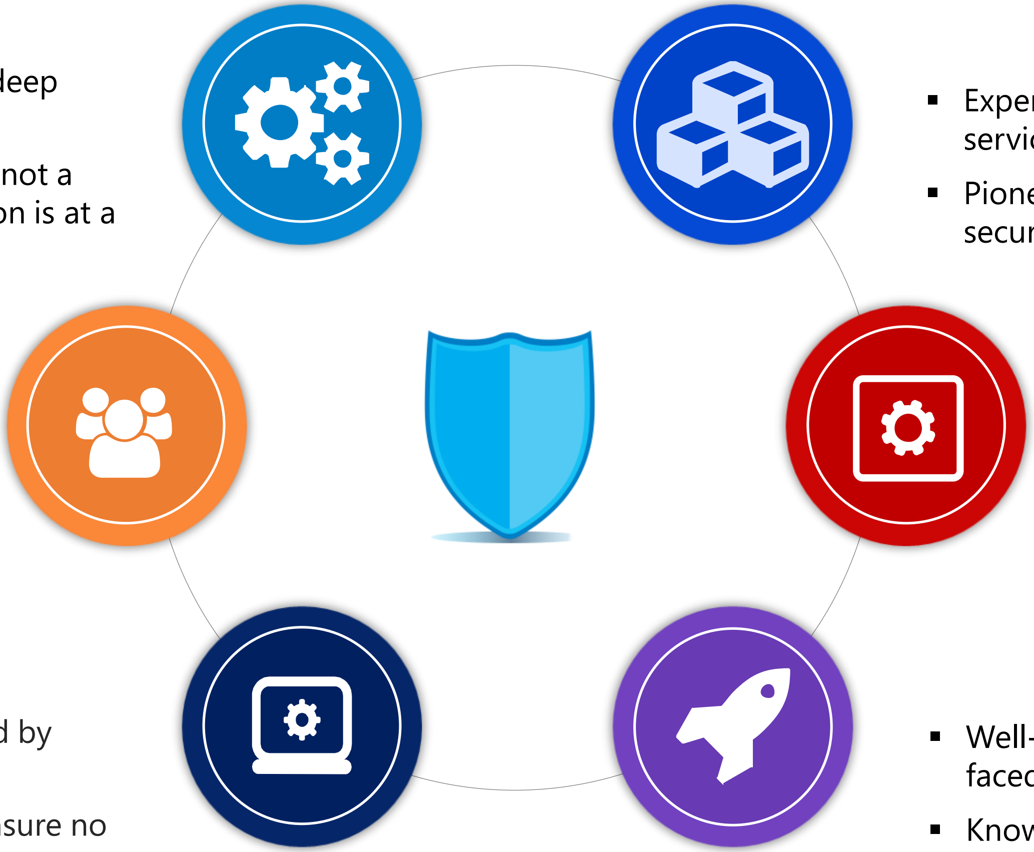
Managed Security Services

- CISO Services
- Managed VAPT Services

Other Capabilities

- Cyber Forensics
- Advance Malware Analysis
- Study of Indicators of Compromise
- Study of Indicators of Attack
- Balanced Scorecard for Information Security

Our Credentials



Consulting Done Right

- Combination of technology, security and deep industry sector experience
- Offer a unique consultative approach and not a “One Size fits all” one, as every organization is at a unique stage in its cyber security journey

Qualified Teams

- Requisite blend of functional and technical skills to deliver cyber security assessments for clients

Technical Proficiency

- Automated assessment tools supported by manual verification
- Controlled service; tests designed to ensure no steps are missed and reduce impact on target systems
- Repeatable service; test parameters recorded to allow retesting under the same conditions

Rich Experience

- Experience in delivering cyber security and data privacy services, including large-scale security programs
- Pioneer in providing tailored and sustainable cyber security solutions

Assessment Framework and Methodology

- Comprehensive framework aligning to security industry standards
- Flexible methodologies and tools to meet client requirements

Deep Domain Expertise

- Well-informed views on the risks and challenges faced by clients
- Knowledgeable opinions backed by experiences and data from earlier engagements
- Insights and best practices specific to client

CyRAACS

PCI Security Standards Council®
QUALIFIED SECURITY ASSESSOR™

CERT-In
Empaneled

VAPT and Secure Code Review Services

CyRAACS Approach Document

cyraacs.com

Murari Shanker | +91-9886210050 | ms@cyraacs.com