Security Assessments for IP Camera Solutions

CyRAACS™ Approach Document

Murari Shanker| 9886210050 | ms@cyraacs.com

Our Understanding of Requirements

- D-Link Corporation is a Taiwanese multinational networking equipment manufacturing corporation headquartered in Taipei, Taiwan.
- D-Link is looking to engage a partner to provide security assessment services for the CCTV cameras and related IT Infrastructure as part of their services for a client.
- CyRAACS™ proposes the following activities as part of the Security Assessment services:
  - Security Assessment for CCTV Cameras (IP cameras) and related IT Infrastructure
  - Security Assessment for the DVR playback applications

Need for Security Assessment for IP Cameras

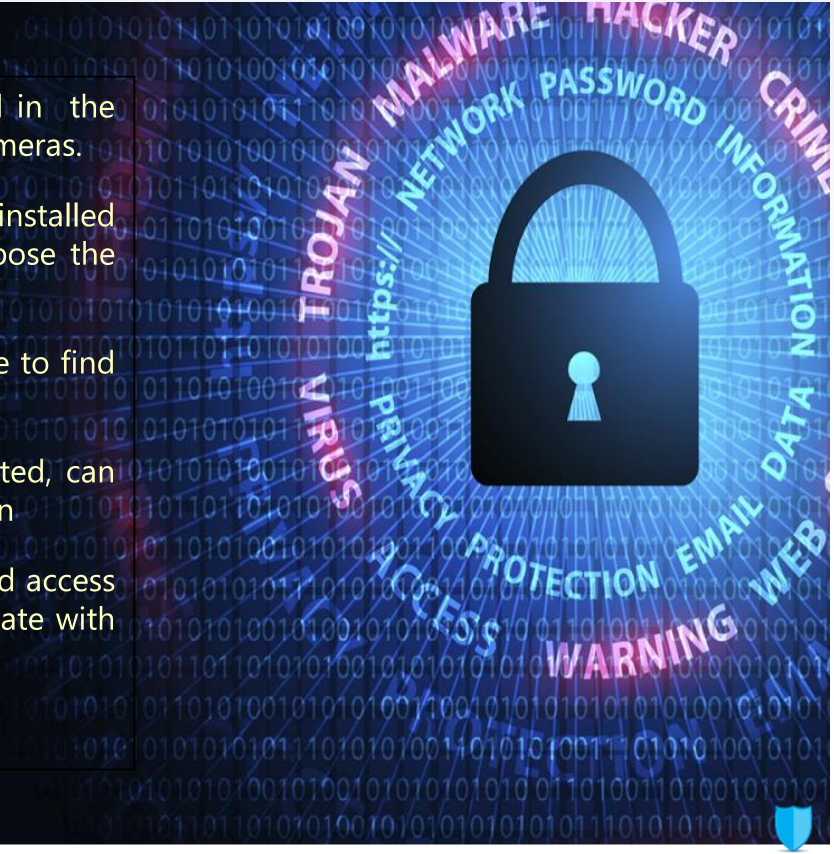
Experts forecast that over 45 billion cameras will be deployed in the world by 2022, and a large percentage of these will be smart cameras.

Studies have indicated that around 5.5 million security cameras installed in homes and offices have serious vulnerabilities that may expose the cameras and pose a serious security risk.

Thanks to their smart capabilities and features, hackers are able to find newer vulnerabilities in smart cameras, IPTV cameras, and DVRs.

All IP cameras use peer-to-peer (P2P) features which if exploited, can allow attackers to bypass firewalls and steal sensitive information

If cyber criminals are able to take control of cameras, they could access the live footage and spy on your home or office & communicate with people around if the camera has a microphone



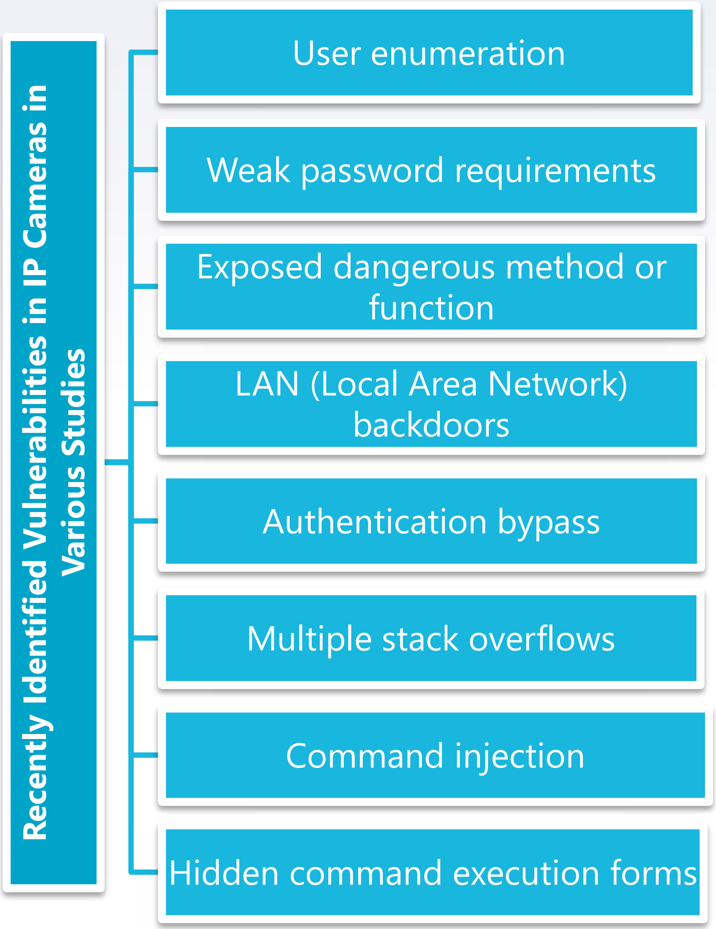
Information Security Threats & Vulnerabilities

IP Cameras and Vulnerabilities

With features from face recognition to various image sensors and connectivity options, such as Bluetooth and Wi-Fi, smart cameras can detect human behaviour and even vehicle number plates, making them a perfect residential or commercial surveillance or tool.

According to recent studies, IP cameras will exceed 45 billion units sold by 2022.

Since IP cameras are connected to the internet 24/7, strict security controls are required to protect from online threats.



Recently Identified Vulnerabilities in IP Cameras in Various Studies

- User enumeration
- Weak password requirements
- Exposed dangerous method or function
- LAN (Local Area Network) backdoors
- Authentication bypass
- Multiple stack overflows
- Command injection
- Hidden command execution forms

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) and applications.
- Regulators and customers are also increasingly demanding tight security controls, while imposing heavy fines in case of security lapses or breaches.
- This has led to organizations to move towards adopting a proactive approach to information security.
- One such component of this proactive strategy is to conduct periodic security assessments for IT Infrastructure and applications to ensure vulnerabilities are identified and remediated in a timely manner.

Top Vulnerabilities in IT Infrastructure & Applications

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

Applications

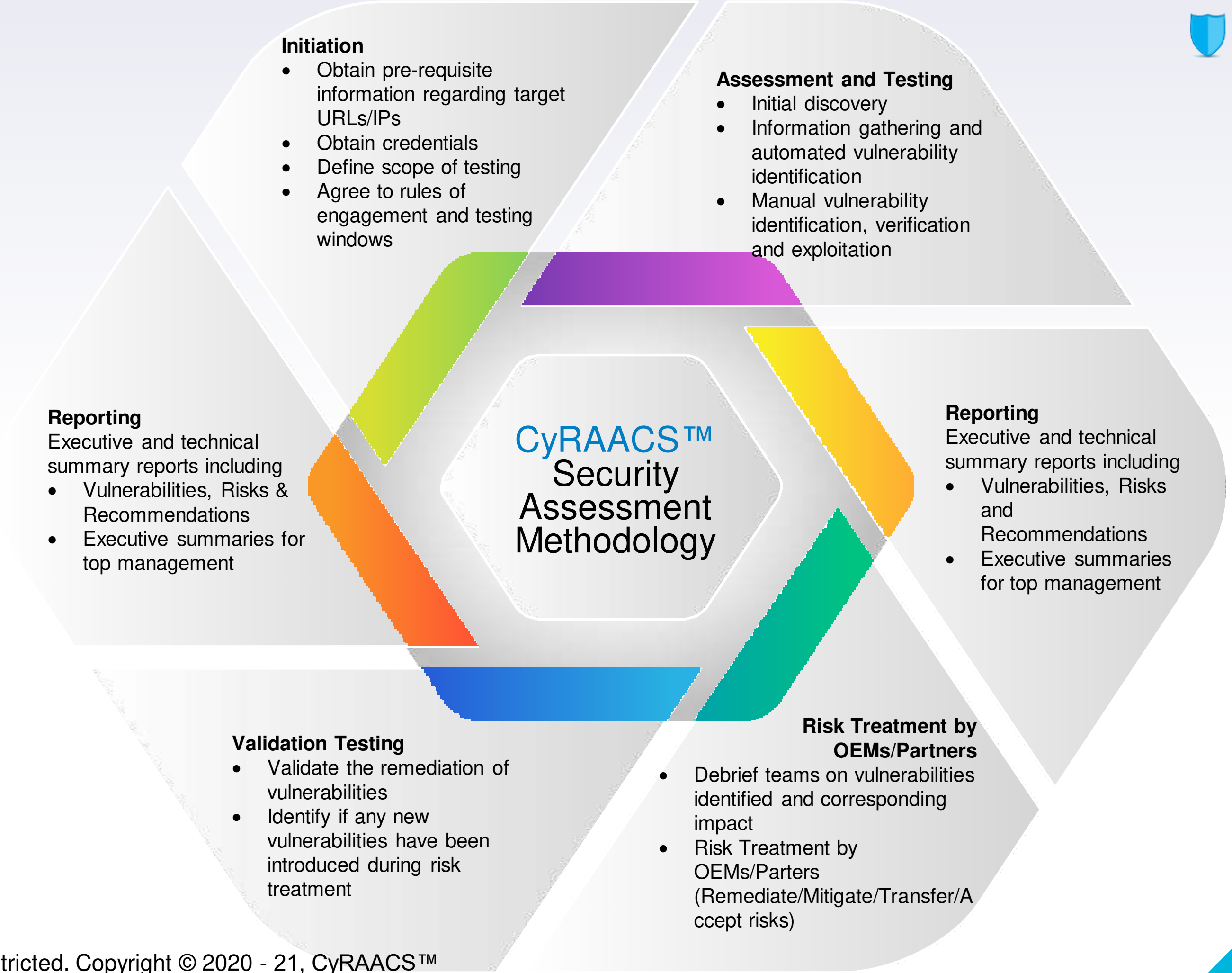
- ✓Injection
- ✓Broken Authentication
- ✓Sensitive Data Exposure
- ✓XML External Entities
- ✓Broken Access Control
- ✓Security Misconfiguration
- ✓Cross-Site Scripting (XSS)
- ✓Insecure Deserialization
- ✓Using Components with Known Vulnerabilities
- ✓Insufficient Logging and Monitoring

CyRAACS™ Proposed Services

Security Assessment

- Security Assessment:
  - **IP cameras**
  - **Network Devices (Switches and Firewalls) related to IP cameras**
- Configuration Review against baseline requirements for IP cameras
- Configuration Review for Servers and Network Devices related to IP cameras
- Security Audit for DVR playback applications

Security Assessment Methodology



CyRAACS™ Security Assessment Methodology

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 OEMs/Partners

- Debrief teams on vulnerabilities identified and corresponding impact
- Risk Treatment by OEMs/Parters (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 & Recommendations
- Executive summaries for top management

Secure Configuration Review

Secure Configuration Review

- A Secure Configuration review is a detailed review and verification of configuration settings of IT infrastructure components to assess the security effectiveness of the IT environment.
- A poorly configured component of the IT Infrastructure can be the weak link that allows an attacker to wreak havoc across the entire IT landscape, causing outages and leaving organizations vulnerable to a security breach.
- Conducting a Secure Configuration Review provides visibility on:

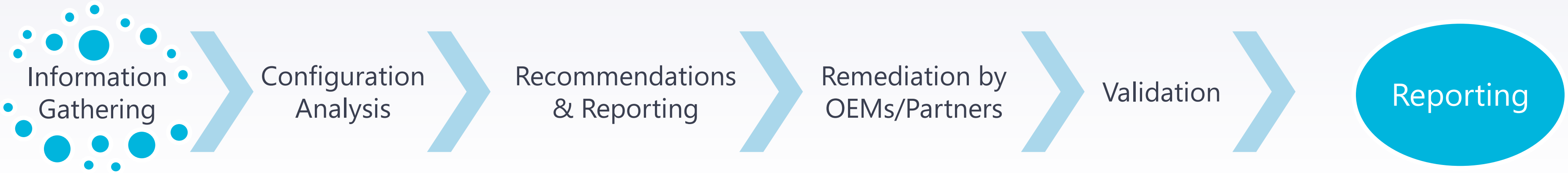
✓ User access control on systems

✓ Password and account policies

✓ Services and applications running on critical systems

✓ Security Patches and their status

Methodology



Information Gathering

Configuration Analysis

Recommendations & Reporting

Remediation by OEMs/Partners

Validation

Reporting

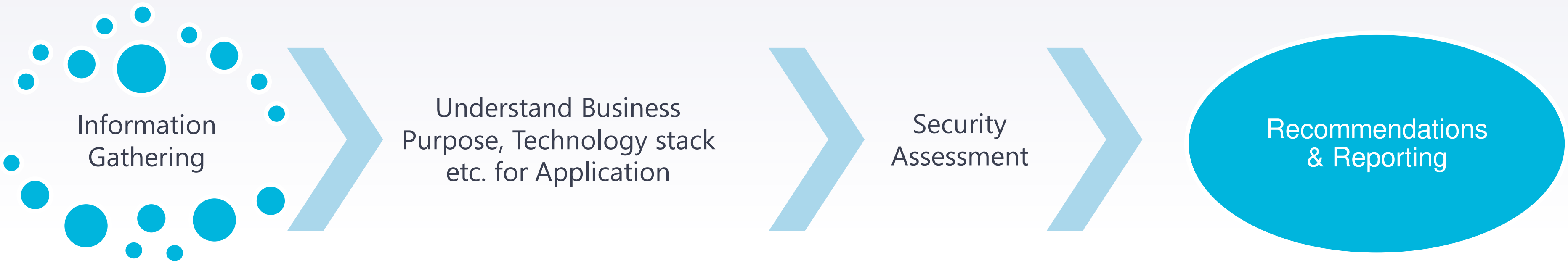
Coverage

- Windows Servers ✓
- Linux Servers ✓
- Firewalls and Switches ✓
- Database Servers
- Web Servers

✓ - include in scope

Security Audit

Methodology



Information Gathering

Understand Business Purpose, Technology stack etc. for Application

Security Assessment

Recommendations & Reporting

Indicative Coverage Areas

- ✓ Authentication and Authorization
- ✓ Access and Privilege Management
- ✓ Configuration Management
- ✓ Session Management
- ✓ Encryption
- ✓ Auditing and Logging
- ✓ Exception Management
- ✓ Input Validation
- ✓ Secure SDLC Process

Indicative Timelines

Activity	W1	W2	W3	W4	W5	W6
Security Assessment	🟦					
Configuration Review for IP Cameras	🟥	🟥				
Configuration Review for Servers and Network Devices	🟦					
Security Audit	🟩	🟩				
Remediation by OEMs/Partners			⬜	⬜		
Validation (optional)					🟦	🟦

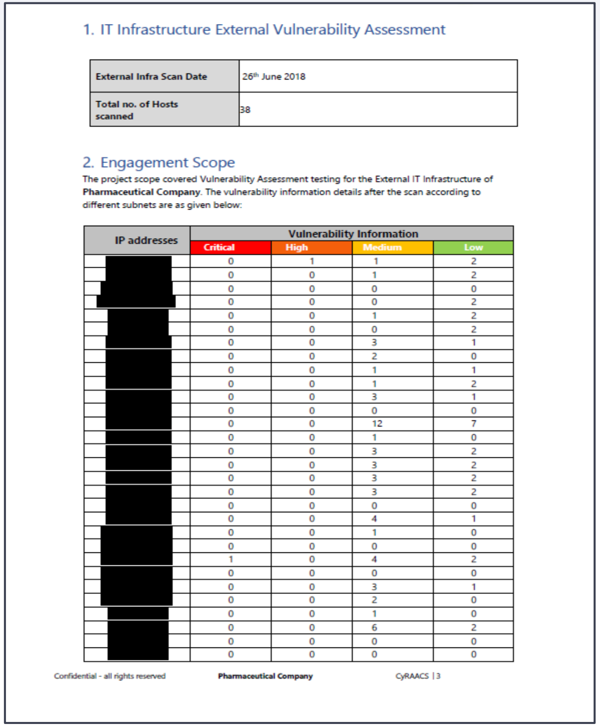
Note:

- The above duration is indicative, detailed project plans will be submitted at the start of the engagement basis the scope.
- All engagement activities will be conducted remotely.
- D-Link/Client will be responsible to provide remote, secure access and necessary privileges for the assessments.

Sample Reports

Snapshot of sample reports from assessment

Sample Report: IT Infrastructure Security Assessment



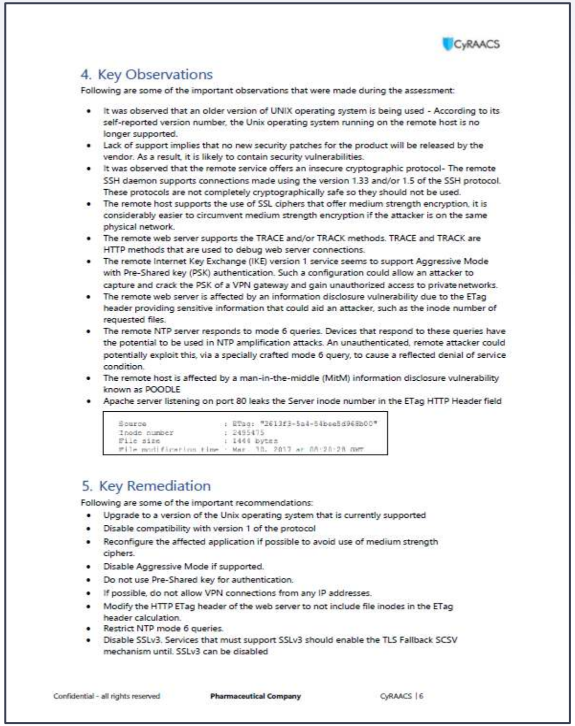
1. IT Infrastructure External Vulnerability Assessment

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



CyRAACS

4. Key Observations

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

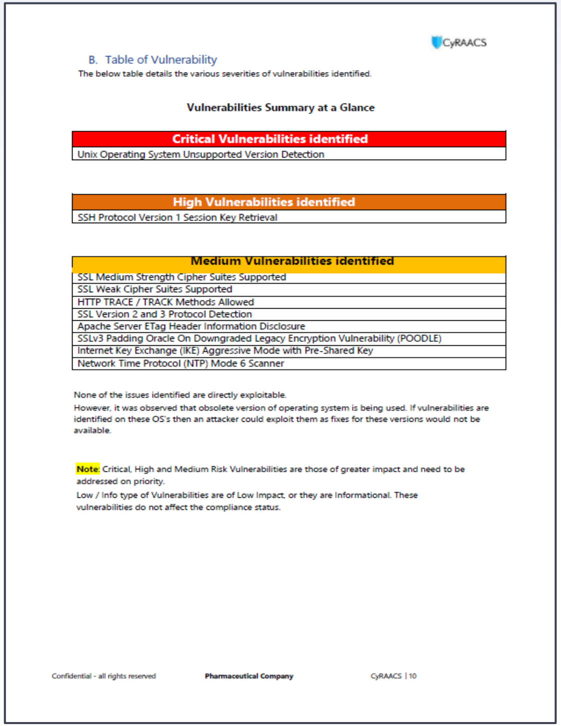
- It was observed that an older version of UNIX operating system is being used - According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.
- Lack of support implies that no new security patches for the product will be released by the vendor. 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 08:20:28 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



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.

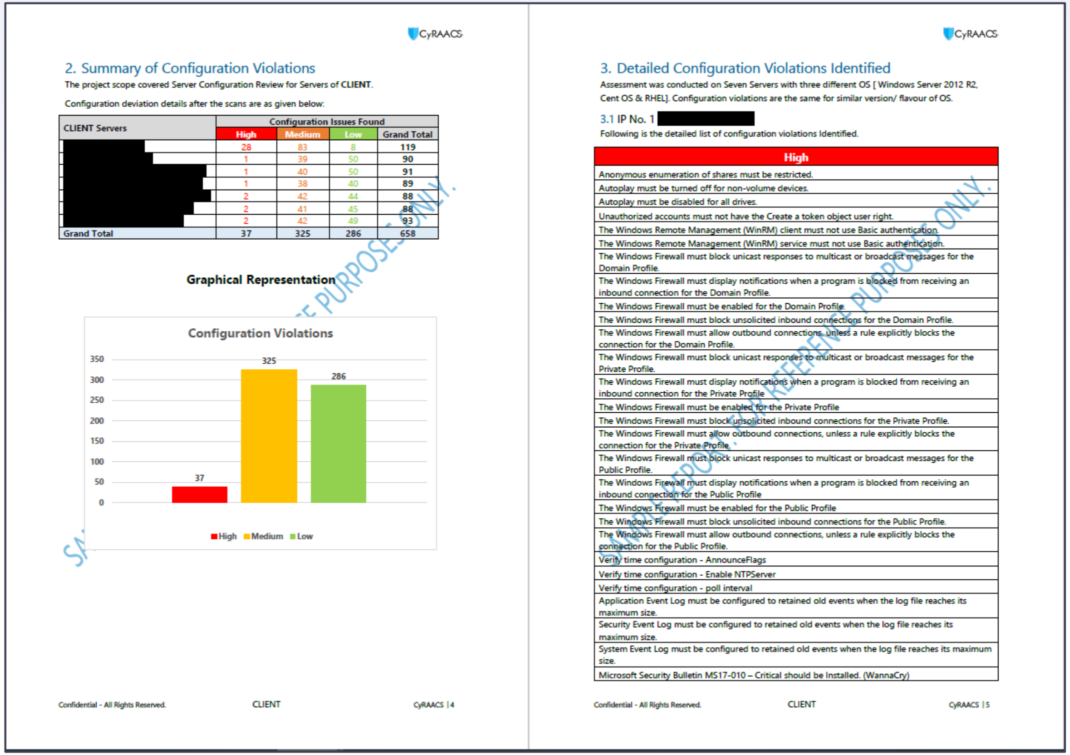
However, it was observed that obsolete version of operating system is being used. If vulnerabilities are identified on these OS's then an attacker could exploit them as fixes for these versions would not be available.

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.

*Sample reports for reference purpose only.

Sample Report: Configuration Review



2. Summary of Configuration Violations

The project scope covered Server Configuration Review for Servers of **CLIENT**.

Configuration deviation details after the scans are as given below:

CLIENT Servers	Configuration Issues Found			
	High	Medium	Low	Grand Total
[redacted]	28	83	8	119
[redacted]	1	39	50	90
[redacted]	1	40	50	91
[redacted]	1	38	40	89
[redacted]	2	42	44	88
[redacted]	2	41	45	88
[redacted]	2	42	49	93
Grand Total	37	325	286	658

Graphical Representation

3. Detailed Configuration Violations Identified

Assessment was conducted on Seven Servers with three different OS [Windows Server 2012 R2, Cent OS & RHEL]. Configuration violations are the same for similar version/ flavour of OS.

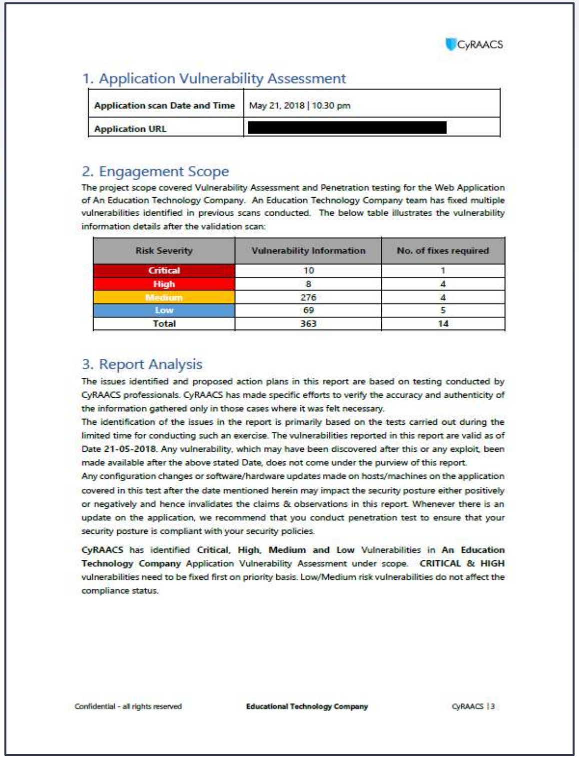
3.1 IP No. 1 [redacted]

Following is the detailed list of configuration violations Identified.

High
Anonymous enumeration of shares must be restricted.
Autoplay must be turned off for non-volume devices.
Autoplay must be disabled for all drives.
Unauthorized accounts must not have the Create a token object user right.
The Windows Remote Management (WinRM) client must not use Basic authentication.
The Windows Remote Management (WinRM) service must not use Basic authentication.
The Windows Firewall must block unicast responses to multicast or broadcast messages for the Domain Profile.
The Windows Firewall must display notifications when a program is blocked from receiving an inbound connection for the Domain Profile.
The Windows Firewall must be enabled for the Domain Profile.
The Windows Firewall must block unsolicited inbound connections for the Domain Profile.
The Windows Firewall must allow outbound connections, unless a rule explicitly blocks the connection for the Domain Profile.
The Windows Firewall must block unicast responses to multicast or broadcast messages for the Private Profile.
The Windows Firewall must display notifications when a program is blocked from receiving an inbound connection for the Private Profile
The Windows Firewall must be enabled for the Private Profile
The Windows Firewall must block unsolicited inbound connections for the Private Profile.
The Windows Firewall must allow outbound connections, unless a rule explicitly blocks the connection for the Private Profile.
The Windows Firewall must block unicast responses to multicast or broadcast messages for the Public Profile.
The Windows Firewall must display notifications when a program is blocked from receiving an inbound connection for the Public Profile
The Windows Firewall must be enabled for the Public Profile
The Windows Firewall must block unsolicited inbound connections for the Public Profile.
The Windows Firewall must allow outbound connections, unless a rule explicitly blocks the connection for the Public Profile.
Verify time configuration - AnnounceFlags
Verify time configuration - Enable NTPServer
Verify time configuration - poll interval
Application Event Log must be configured to retained old events when the log file reaches its maximum size.
Security Event Log must be configured to retained old events when the log file reaches its maximum size.
System Event Log must be configured to retained old events when the log file reaches its maximum size.
Microsoft Security Bulletin MS17-010 – Critical should be Installed. (WannaCry)

*Sample reports for reference purpose only.

Sample Report: Security Audit



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

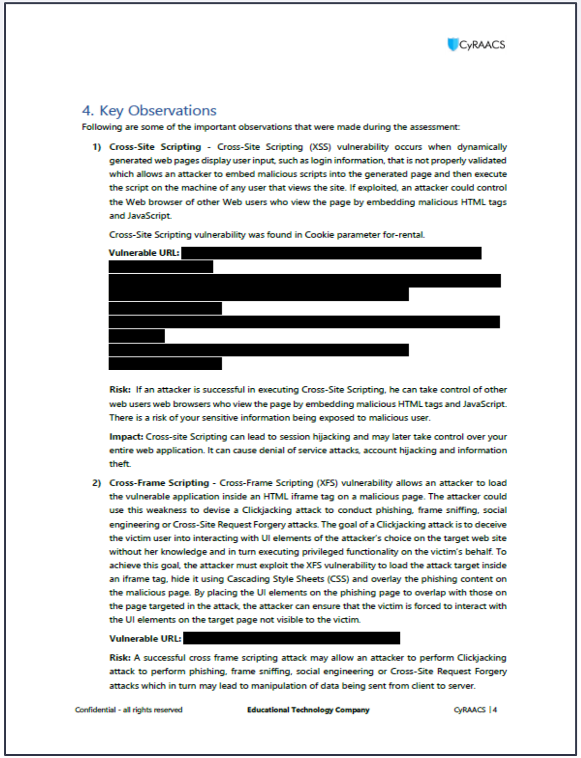
The issues identified and proposed action plans in this report are based on testing conducted by CyRAACS professionals. CyRAACS has made specific efforts to verify the accuracy and authenticity of the information gathered only in those cases where it was felt necessary.

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.

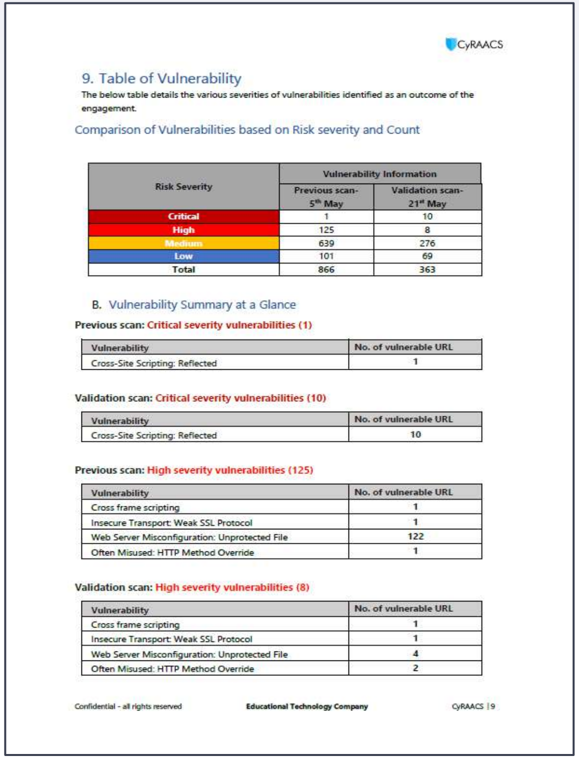
   Impact: Cross-site Scripting can lead to session hijacking and may later take control over your entire web application. It can cause denial of service attacks, account hijacking and information theft.

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 purpose only.

CyRAACS™

Your Trusted Security Partner

www.cyraacs.com

Overview

90+ Satisfied clients

200+ engagements & repeated customers

Delivered services across all industry verticals

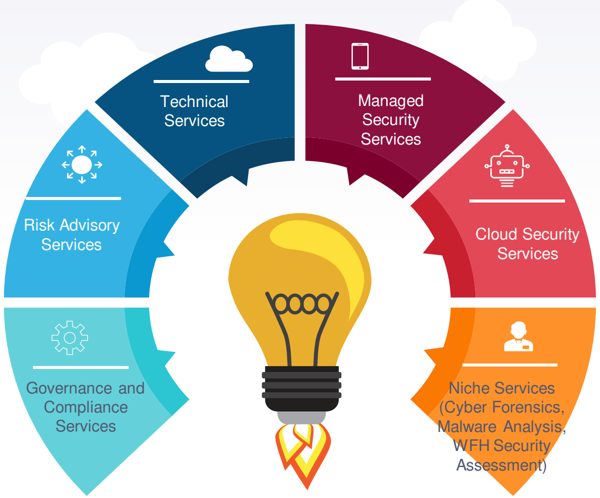
Global Engagements North America & Middle East

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR™

CERT-In Empaneled

Full suite of services in Compliance Lifecycle

- ✓ Framework
- ✓ Assessment
- ✓ Implementation
- ✓ Audit



Technical Services
Managed Security Services
Risk Advisory Services
Cloud Security Services
Governance and Compliance Services
Niche Services (Cyber Forensics, Malware Analysis, WFH Security Assessment)

Laws
Transparency
Standards
Requirements
Compliance
Regulatory
Governance
Policies
Risks

- Proven track record of delivering challenging projects
- Tailor-made & Sustainable Cyber Security Solutions to Clients
- Sustenance Support for Cyber Security
- Extended Security arm for our clients

Experience in Information Security and Data Privacy Standards/Frameworks

CSA STAR CERTIFICATION | PCI DSS COMPLIANT | SOC 2 TYPE 2 | CALIFORNIA CONSUMER PRIVACY ACT | GDPR READY | ISO 27001 | FISMA / NIST 800-53 CERTIFIED

Consultants with leading industry certifications CISSP, CISA, CEH, CISM etc

Leadership

Cyber security risks continue to pose a formidable challenge to organizations of all sizes and across industry verticals. Rapidly evolving threat landscape, regulatory scrutiny, and new age technology advancements further add to the complexity. Organizations need to adopt a strategy with the right balance of technology, processes and capabilities to stay ahead.

CyRAACS™ is the brainchild of Suresh Iyer and Murari Shanker, industry veterans who have tremendous experience in tacking these challenges in their role as global CISOs for Multinational Companies. They possess a unique blend of deep domain expertise, strategic know-how and industry experience. They act as the guiding force in our endeavor to build robust and sustainable cyber security solutions for clients.

Suresh Iyer

Co-Founder & Chief Executive Officer

Murari Shanker

Co-Founder & Chief Operating Officer

Our Expertise

Tool	Detail
Nessus Professional	Infrastructure 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
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

Why CyRAACS™

Quality assurance

- ✓ Quality assurance 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 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

Why CyRAACS™

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.

We are Eager to work with you !

Take charge of your company's cyber security with CyRAACS™ !