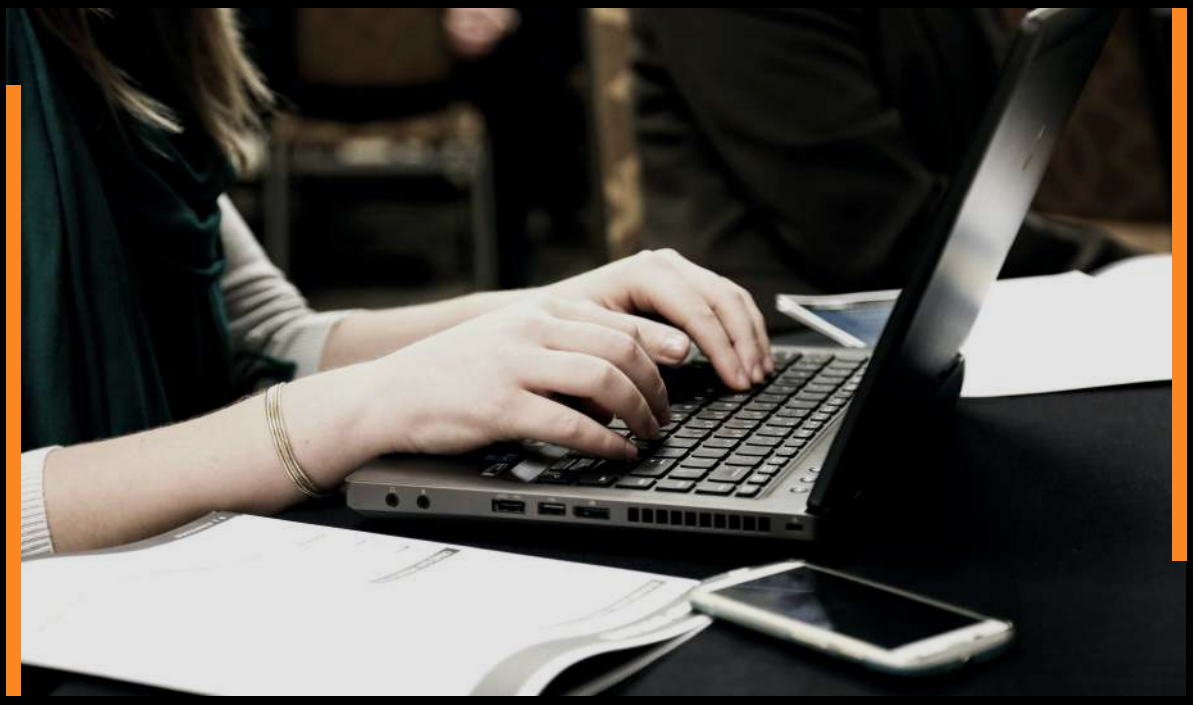
CYBERSRC CONSULTANCY
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

WEB APPLICATION SECURITY TESTING SERVICES

WEB APPLICATION SECURITY TESTING SERVICES



OVERVIEW

Advancements in web applications, web services and other technology have changed the way we do business and access and share information. Many businesses have shifted most of their operations online so employees from remote offices and business partners from different countries can share sensitive data in real time and collaborate towards a common goal.

With the introduction of modern Web 2.0 and HTML5 web applications, the demands of a customer have changed; they want to be able to access any data we want to twenty-four seven. Such demands are also pushing businesses into making such data available online via web applications. A perfect example of this are the online banking systems and online shopping websites.

All of these advancements in web applications have also attracted malicious hackers and scammers, who are always coming up with new attack vectors, because like in any other industry there is money to be gained illegally. And this lead to the birth of a new and young industry; Web Application Security.

COMMON VULNERABILITIES FOUND IN WEB APPLICATIONS INCLUDE

SQL INJECTION

Occurs when a perpetrator uses malicious SQL code to manipulate a backend database so it reveals information. Consequences include the unauthorized viewing of lists, deletion of tables and unauthorized administrative access.

REMOTE FILE INCLUSION

A hacker uses this type of attack to remotely inject a file onto a web application server. This can result in the execution of malicious scripts or code within the application, as well as data theft or manipulation.

CROSS-SITE REQUEST FORGERY (CSRF)

An attack that could result in an unsolicited transfer of funds, changed passwords or data theft. It's caused when a malicious web application makes a user's browser perform an unwanted action in a site to which a user is logged on.

CROSS-SITE SCRIPTING

XSS is an injection attack targeting users in order to access accounts, activate Trojans or modify page content. Stored XSS occurs when malicious code is injected directly into an application. Reflected XSS takes place when malicious script is reflected off of an application onto a user's browser.

THE RESULTS OF THESE ATTACKS CAN LEAD TO THE FOLLOWING

- **Access to Restricted Content**
- **Compromised User Accounts**
- **Installation of Malicious Code**
- **Lost Sales Revenue**
- **Loss of Trust with Customers**
- **Damaged Brand Reputation**

CHALLENGES IN WEB APPLICATION SECURITY TESTING

CODE INJECTION

Using code injection techniques, the attackers can exploit vulnerabilities in a web application by inserting their malicious code. Code injection vulnerabilities are often found in the text input field for users. Common types of code injection vulnerabilities include SQL injection, OS command attacks, dynamic evaluation attacks, and shell injection.

INCREASE IN THE USAGE OF RICH INTERNET

Applications (RIAs) also poses a challenge for security testing of web application. This is due to the fact that the crawling techniques which are used for exploration of the web applications used for earlier web applications do not fulfil the requirements for RIAs.

DATA BREACH

There are numerous statistics high- lighting the average cost of a data breach. Some of the common causes of data breaches include misconfiguration, lost hardware, malware infection, and compromised credentials. In order to avoid data breaches, a wide range of good security practices are required. For example, SSL encryption, access-level privileges regular scanning activities, and organizing regular training sessions for employees to practice good security practices such as identifying phishing attacks, setting up strong passwords, enabling two-factor authentication, etc.

DDOS ATTACKS

DDoS attacks, or Distributed Denial of Service attacks, involve a large number of computers being used by the attackers to send a plethora of requests to the target web application. With the size of DDoS attacks increasing every year, organizations can be affected even without being targeted. A modern-day business avails various services from different vendors. If the attackers target any one of the services offered by a vendor, all the clients of the said vendor are affected.

MALICIOUS INSIDERS

The threat of malicious insiders is an evergreen threat – let it be cyber security industry or any other. While discussing the most common security challenges, malicious insiders cannot be left out. As a mandatory principle, an organization must follow the principle of least privilege, i.e., an employee shall have minimum access level privileges which are required to complete his KRAs. An access control policy is a good starting point. Along with policy implementation, an organization can monitor transactions and activity logs for broader insights.

OUR DETAILED APPROACH

CyberSRC® Security's methodology is an extensive process – which is used for every application Pentesting.

VULNERABILITY SCANNING

Powered by both automation and manual testing, vulnerability scanning is used to identify the loopholes and vulnerability signatures present in the application. It is used to gain an understanding of the baseline of security risks.

WHITE-BOX PENETRATION TESTING

The final category of testing is called white-box testing, which allows the security consultant to have complete open access to applications and systems. This allows consultants to view source code and be granted high-level privilege accounts to the network. The purpose of white-box testing is to identify potential weaknesses in various areas such as logical vulnerabilities, potential security exposures, security misconfigurations, poorly written development code, and lack-of-defensive measures.

GREY-BOX PENETRATION TESTING

Comparatively, a black-box tester begins the engagement from a strict external viewpoint attempting to get in, while the grey-box tester has already been granted some internal access and knowledge that may come in the form of lower-level credentials, application logic flow charts, or network infrastructure maps.

BLACK-BOX PENETRATION TESTING

In a black-box engagement, the consultant does not have access to any internal information and is not granted internal access to the client's applications or network. This type of testing is the most realistic, but also requires a great deal of time and has the greatest potential to overlook a vulnerability that exists within the internal part of network or application.

SOME OF THE TOOLS USED

- Acunetix
- Netsparker
- OWASP Zap
- Nikto
- Burpsuite

KEY AREAS COVERED IN WEB APPLICATION SECURITY

1 Reconnaissance

The first phase in our web application penetration test focuses on collecting as much information as possible about a target application. We conduct this portion of the test through the use of both passive and active reconnaissance by simulating or actively engaging in different types of attack vectors. Example tests include: Error Code Analysis, Fuzzing, Search Engine Recon, App Enumeration, and App Fingerprinting.

2 Business Logic

These are important to most applications that provide business functionality.

3 Information Gathering

Manually review the application, identifying entry points and client-side codes. Classify third-party hosted content.

4 Denial of Service

Improve an application's resilience against denial of service threats by testing for anti-automation, account lockout, HTTP protocol DoS and SQL wildcard DoS. This doesn't cover protection from high-volume DoS and DDoS attacks, which are best countered by a combination of filtering solutions and scalable resources.

5 Client-side Logic

One of the most common web application security weak-nesses is the failure to properly validate input coming from the client or from the environment before using it. This includes cross-site scripting, SQL injection, interpreter injection, locale/Unicode attacks, file system attacks, and buffer overflows.

6 Cryptography

Secure all data transmissions. Has specific data been encrypted? Have weak algorithms been used? Do randomness errors exist?

7 Authentication Testing

Authentication is the process of attempting to verify the digital identity of the sender of a communication. The most common example of this is the logon process. Any weak point in this process can result in a massive data breach if you're not careful. Example testing includes: Brute Force Testing, User Enumeration, Transport Layer Security.

8 Configuration Management

Comprehending the deployed configuration of your server/ infrastructure hosting your web applications is nearly as critical as testing the application itself. Example testing includes: TLS Security, Database Listeners, File Extension Handling, and Cross-Site Tracing.

9 Authorization Testing

Authorization Testing is the part of our methodology that involves understanding how your authorization process works and using that information to circumvent the authorization mechanism. Example testing includes: Directory Traversal, Privilege Escalation, and Bypassing Authorization Controls.

10 Data Input Validation

With modern, JavaScript-heavy webpages, in addition to webpages using other types of client-side technologies (e.g., Silverlight, Flash, Java applets), this type of feature is becoming more prevalent.

11 Web/API Services

Web services have certain elements of exposure just like any other type of protocol or service. What is different is web services can be used on HTTP, FTP, SMTP, or MQ, among other transport protocols. As a result, we'll look for vulnerabilities in web services are similar to other vulnerabilities, such as SQL injection, information disclosure, and leakage, but web services also have unique XML/ parser related vulnerabilities. Example tests include: Information Gathering, Fuzzing, and Replay Testing.

12 Session Management

Session Management is defined as the set of all controls governing the stateful interaction between a user and the web application they are interacting with. Example testing includes: Session Fixation, Cross Site Request Forgery, Cookie Management, and Session Timeout.

CASE STUDIES

Background

- Client is one of the leading KPO company
- The client has been in the industry for over 22+ years with a global presence across 50+ countries
- VAPT is important for the organization to know the potential threats in the application which can affect the organization's business.

Objectives

- Assessment of the application for pentesting
- Identify the vulnerabilities in the application
- Expert recommendations and guidance to cover up gaps and improve information security posture

Challenges

- The client did not have any expertise for security testing of web application
- The client lacked required knowledge of tools used for security testing web.

Our Role

- Application VAPT for the companies website and its other service parties.
- Pentesting of Application and Network
- VAPT reporting and legal advisory

Result/ Benefits

- Successful security testing of web application
- Organization gain comprehensive knowledge on the threat action in their Application
- Detailed report of VAPT and recommendation with preventive measure
- Consultancy on action items required to cover up identified gaps

Industry Sector

KPO

Service Utilized

Application VAPT

Business Areas Challenges

IT & Technology

HOW CYBERSRC® HELP?

Our goal is to help your team zero in on critical issues, understand any potential security vulnerabilities, and help you to identify solutions to ensure your web applications are the strongest they can be from a security standpoint. Through the vigorous processes established in our testing methodology, our experienced pentesters will find any weaknesses and help you establish solid security controls to prevent future data breaches or other exploits. About 80% of our application penetration testing is manual testing, with 20% being automated vulnerability scan testing.

ABOUT US

CyberSRC® forays into domains of Cyber Security, Data Privacy, Assurance and Governance. Our aim is to assist enterprises, MSMEs, SMEs & others enhance their capabilities for cybersecurity defence, minimise enterprise security and assurance risks, manage security operations and achieve regulatory compliance. Our team consists of several consultants and advisors. We have collaborated with multi-partners in order to provide support for end-to-end security solutions and implementation support.

WHY CYBERSRC®?

We are team of qualified professionals with rich experience of multiple industries such as Manufacturing, BFSI, Insurance, Healthcare, NBFCs & others. Our consultants are industry experts and have proven track records, some of the renowned certificates that our consultants hold such as CISA, CISSP, COBIT, CEH, CCNA, OSCP, ISO 9001 LA/LI, ISO 27001, ITIL LA/LI, PMP, to name a few. We believe in adding value to your business which is enabled through our Centre of Excellence (Coe) and, we have end-to-end capability for Program Build – Operations – Transformation. We have the ability to jump start and execute projects in Managed Services mode globally and flexible delivery models. Our Vision is to be one of the World's most trusted advisory & solution provider for Cyber Security, Data Protection an Assurance practices.

WHAT WE DO

SECURITY ASSESSMENT SERVICES

1. Vulnerability and Penetration Testing Services

- Web Application VA/PT
- Mobile Application VA/PT
- Network Security VA/PT
- Database Security Assessment
- Cloud Security Assessment
- Wireless/WIFI Devices Assessment
- API & Web Services

2. Source Code Review

3. Configuration Review and Hardening Testing

4. Firewall/ Network Devices Security Review

SPECIALISED CYBER SECURITY SERVICES

1. External Threat Intelligence

- Phishing Domain Detection
- Rogue Applications Detection
- Source Code Leaks
- Social Media Abuse
- Brand Abuse
- Dark Web Monitoring
- Take Down support

2. Phishing Campaigns/ Stimulation

- Phishing
- Smishing
- Vishing

3. Incident response & Malware Analysis
4. Forensics Analysis
5. Root Cause Analysis
6. Red Teaming Exercise
7. Honeypot as Service

- Web Attack Mitigation
- Network Attack Mitigation
- Shadow Surveillance

CONSULTING, COMPLIANCE AND & AUDIT SERVICES

1. ISO Compliance

- ISO 27001 ISMS
- ISO 9001 QMS
- ISO 27701 PIMS

2. Information System Assurance & Audit

- **RBI**
  - Payment & Settlement Systems (PSS)
  - NBFC
  - Co-Operative Banks
  - Prepaid Payment Instruments PPI
  - CISA
  - P2P Lending
- **IRDA ISNP**
- **SEBI**
- **AADHAAR**
  - UIDAI AADHAAR
  - ESIGN ASP
- **OTHER**
  - GST SUVIDHA PROVIDER
  - NPCI

3. Regulatory Compliance

- PCI DSS
- SOX
- SOC 1, SOC 2 & SOC 3

4. Privacy Compliance

- General Data Protection
- Regulation (GDPR)
- ISO 27701 PIMS
- California Consumer Privacy Act (CCPA)
- Brazilian General Data Protection Law (LGPD)
- Personal Information Protection and Electronic Documents Act (PIPEDA, Canada)
- Singapore Personal Data Protection Act (PDPA)
- Health Insurance Portability and Accountability Act (HIPAA)

5. Risk Management

- Virtual Chief Information Security Officer (V-CISO)
- Third Party Risk Management
- IT Risk Management

CONTACT US

CYBERSRC CONSULTANCY
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

+91 9718933141, 0120-4160448

info@cybersrcc.co

www.cybersrcc.com

Head Office: Unit 605, 6th Floor, World Trade Tower, Sector 16, Noida (UP)- 201301
Other Office:
London (UK): Kemp House 152-160 City Road, London, UK (EC1V 2NX)