BUGS BD Limited

Your Cyber Security Partner

BugsBD Limited

Company Overview

DEVELOPMENT

INNOVATION

SECURITY

SOLUTION

COMPANY OVERVIEW

BUGS BD Limited

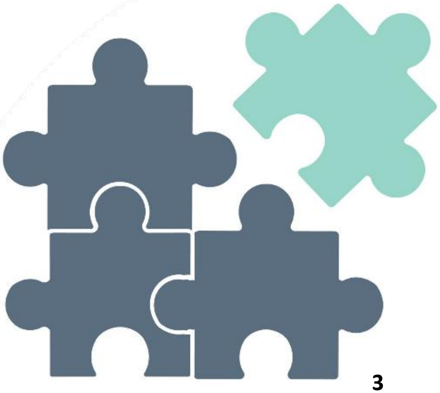
Your Cyber Security Partner

BUGSBD Limited

1/C, Road No. 1, Shyamoli, Dhaka-1207, Dhaka.
Call Us: +880 188 99 7 55 11 , Email: info@bugsbd.com

TABLE OF CONTENT

The great business comes from great people.



BACKGROUND

Bugsbd Limited, the goal is simply to make organizations better at building complex business systems. We design, sell and support software used by systems architects, developers, and operations teams worldwide.

The company was founded in 2015.The company has grown quickly and strategically, in both revenue and staff. Currently, we have over 35 staff members. One of our most distinctive features is that, just like our software, we're fully distributed. We provided services to clients countrywide and overseas. We are spread across 6 countries, covering multiple time zones, conducting our work when it's most suitable for us. During the last 6 years, Bugsbd Limited has successfully implemented more than 80+ projects. Facing new challenges and finding a unique solution for them was the initial inspiration for us to stand up to our present position.

In 2018 Bugsbd Limited achieved one of the best service providing company. We are always focusing exclusively on high quality and cost-effective software development and implementation of services. This unusual, dispersed organization has its challenges, but many more rewards, including hiring the best people in the world, and creating a very productive culture.

About Us

We are enriched by a number of young, energetic and skilled software engineers and security professionals who have already proven their expertise in this field. We have also a strong networking of different skill sets who would help to ensure absolute solution to our valued clients. This is not only an open platform for the professionals and clients but also it is a podium of congregated transmittable of knowledge that creates more expertise as well in this field of security.

The key services provided by BugsBD Limited. are Vulnerability Assessment & Penetration Testing, Web Application Testing, Network Security, Database Security, System Security, Mobile Application Penetration Testing, Cloud Security, Intrusion Detection and Incident Response, Social Engineering, Source Code Review, Email Security, Digital Forensics and many more.

Reliable

It is a renowned offshore company. We believe in building and maintaining long term relationships with all our clients.

Solutions

We endeavor to offer you best solutions in order to acquire your maximum satisfaction. We are the masters in offering effective software development solutions.

Experience

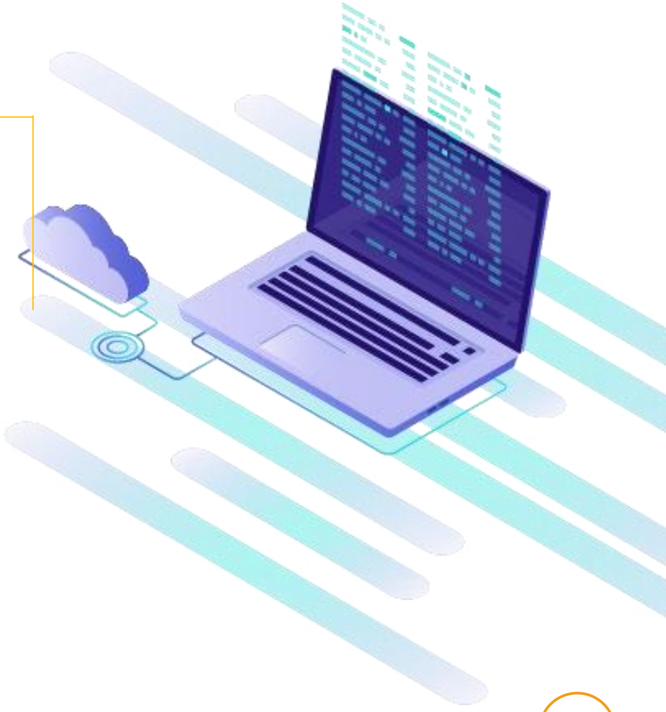
We are pioneer in lambasting problems like web or software development etc. Our experts handle your assigned projects prudently.

Affordable

We have provided best plus affordable web development services to numerous large as well as medium entrepreneurs.

What we do

We provide end-to-end advisory, protection and monitoring services to secure your organization. We advise on your cybersecurity strategy depending on your current level of maturity to help you define your security perimeter, objectives and procedures. Our aim is to protect your systems with our cybersecurity solutions and monitor your system to detect and react in advance of cyber attacks.



Our Mission

We help nations, governments and businesses around the world defend themselves against cybercrime, reduce their risk in the connected world, comply with regulation and transform their operations. Our mission is to make a significant change in the area of Data Protection, User Behavior Analytics, Employee Monitoring and become a worldwide leader. Basing on our innovative solutions and trusted service, we want to make a secure cyber world.

Our Vision

We reduce the vulnerability of the digital environment implementing combined cyber- security and cyber-defense systems that neutralize advanced threats, thereby contributing to the improvement of security. Greater customer relationship is our first priority. We deliver high quality security products and solutions that exceed customer expectations. To maintain great work standards in any organization, we offer outstanding training services and engage high quality professionals. By overcoming the challenges of cyber security, we want to see us as a global technology innovator.

Security Services

We are providing the following services:

Red Team Assessments:

Examine your security with real time simulated attack &

Secure your digital environment with incident response capabilities

Vulnerability Assessment

Vulnerability Assessment is known as vulnerability analysis, is the process of recognizing, analyzing and ranking vulnerabilities in computer systems

Penetration Testing

A penetration test, colloquially known as a pen test, is an authorized simulated cyberattack on a computer system, performed to evaluate the security.

Mobile Security

This penetration testing methodology helps improve transparency and repeat ability for mobile penetration testing.

Source Code Audit

It is the examination of an application source code to find errors overlooked in the initial development phase.

Network Security

Defend networks, data and users with today's fastest, most reliable cyber-attack protection.

Security Consultation

We help organization in starting their Security agenda with the following:

Security Awareness:

Making computer system users aware of their security responsibilities and disseminating correct practices can help user 's change past behaviors.

SOC GAP Assessment:

Conducting a comprehensive analysis of SOC elements (people, process, technology) to determine their efficiency and functionality, and to determine the eligibility of the company's existing foundation elements to construct its in-house SOC system

Penetration Testing:

Will simulate a real-world attack on your networks, applications, devices, and/or people to demonstrate the security level of your key systems and infrastructure and show you what it will take to strengthen it.

Security Risk Assessment:

Perform an assessment to allow organizations to assess, identify and modify their overall security posture and to enable security, operations, organizational management and other personnel to collaborate and view the entire organization from an attacker 's perspective

Security Risk Assessment:

is the process of understanding the threats to an organization based on available data points. But it goes beyond simply collecting data points; there must also be an understanding of how the data relates to the organization.

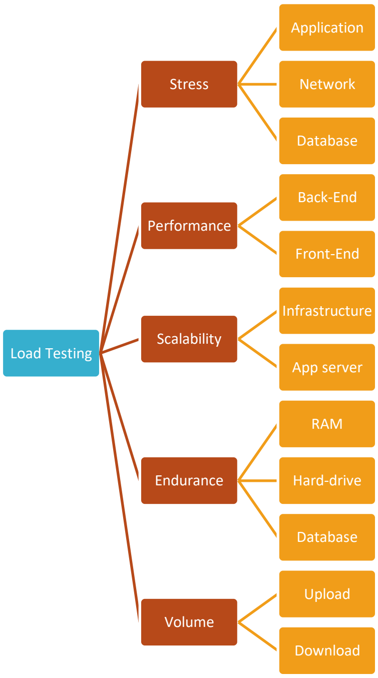
Methodologies

We are using the best methodologies according to the assessment.

Load Testing

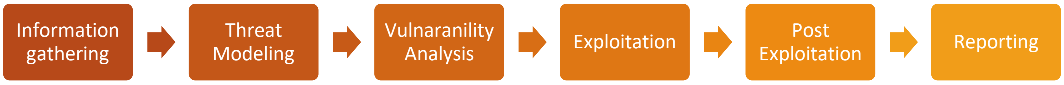
Load testing is the process of putting demand on a software system or computing device and measuring its response.

We produce a methodology flow chart to understand how the load testing working with the assessment.



Penetration

Penetration testing is a critical step in the development of any secure system as it not only stresses the operation, but the implementation and design of a system. It is an authorized and scheduled act that separates a penetration tester from an attacker and has been widely adopted by the organization and institutions.



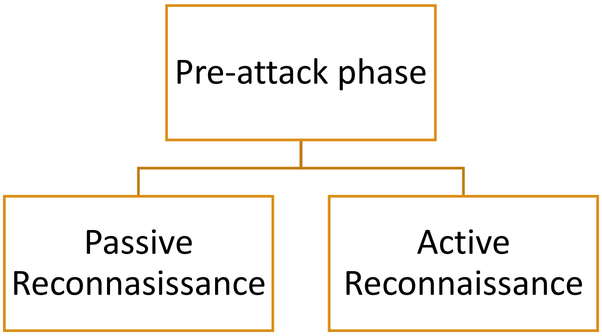
Phases of Penetration Testing

The overall process of penetration testing can be broken into a number of steps or phases. There are three phases namely

(1) Pre-Attack phase, (2) Attack phase and (3) Post-Attack phase

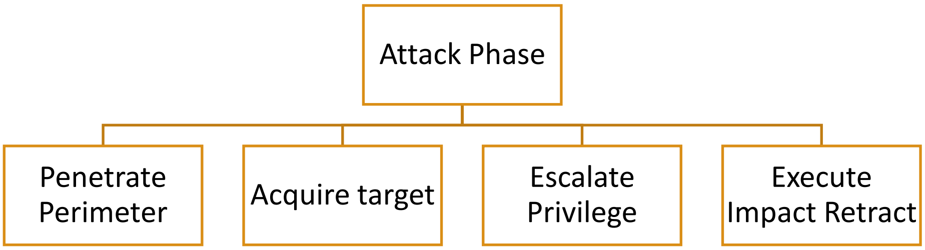
as shown in Figures. The activities in each phase depends on how the rules of engagement have specified that the penetration testing should be conducted. Each phase has been briefly described below from the perspective of black-box approach targeting information systems.

(1) Pre-Attack phase: The pre-attack phase involves reconnaissance or data gathering to discover as much information as possible of the target, nearly all facets of information gathering leverage the power of the Internet. To be successful at reconnaissance, strategy needs to include both passive and active reconnaissance techniques. Passive Reconnaissance makes use of the information resources available on the web

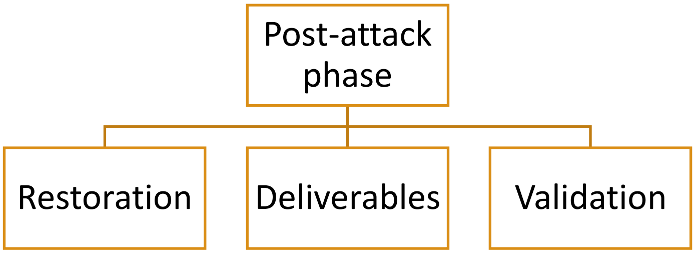


Phases of Penetration Testing

(2) Attack phase: As the name suggests, this attack phase involves the actual compromise of the target. The attacks are performed based on the flaws and vulnerabilities discovered during the pre-attack phase. During this phase, tools can range from exploitive to responsive to find as many vulnerabilities as possible because neither the organization nor the Penetration Tester will know which vulnerability an attacker will choose to exploit first



(3) Post-Attack phase: The post-attack phase involves restoring the systems back to their original pre-test state, which includes removing uploaded root kits files or back- door programs, reversing of any access control list (ACL) changes to files or folders or other system or user objects, restoration of the network devices, and network infrastructure, cleaning up the Registry entries added during the exploitation, and removing shares and connections established during the gaining access phase

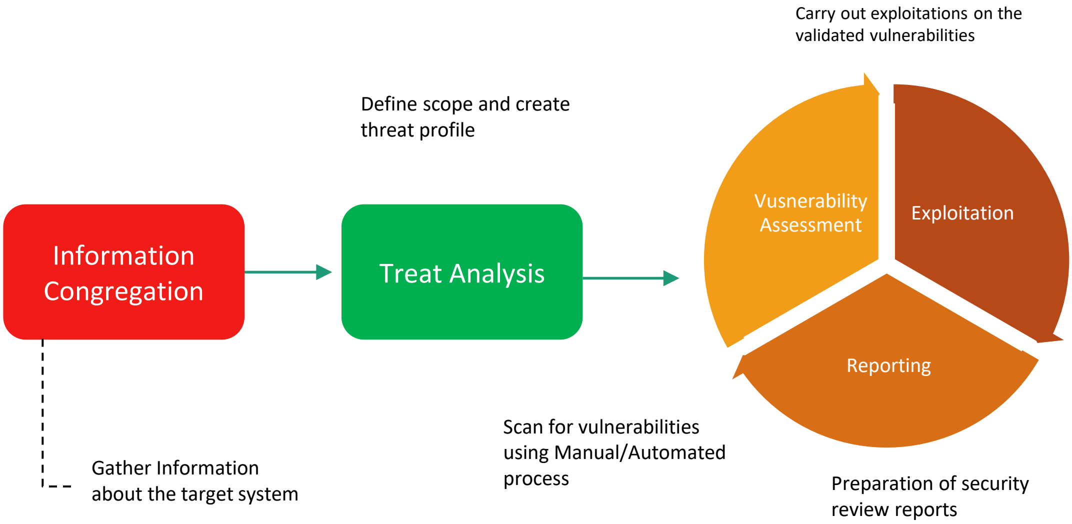


System Vulnerability

The first thing to do in establishing a vulnerability testing plan is to understand system environment for vulnerability testing and define testing scope. The milestone for the System Vulnerability: Checking network security using intrusion detection and prevention systems tools.

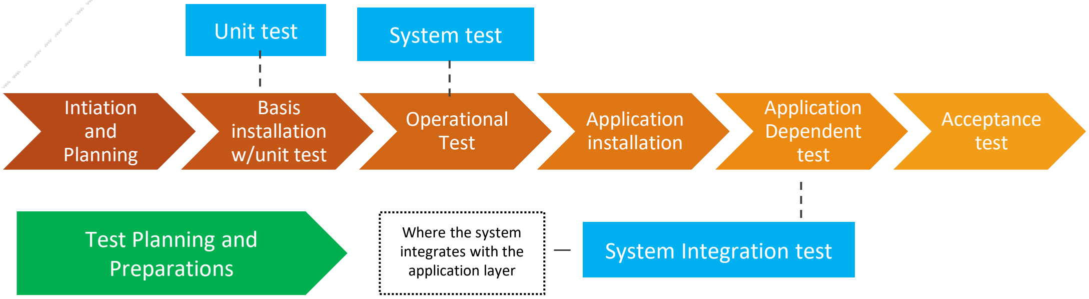
- ✓ *Ensuring all internal and external connections go through an appropriate form of authentication and ensuring this control cannot be bypassed.*
- ✓ *Ensuring that all fields, cookies, https headers/bodies and form fields are validated in compliance with the best international practices.*
- ✓ *Ensuring there are no backdoors in the data validation model.*
- ✓ *Ensuring that all pages enforce the requirement for authentication.*
- ✓ *Ensuring that unauthorized activities in the system cannot take place via cookie manipulation.*
- ✓ *Ensuring that proper data encryption methods and techniques are applied.*

Under these approaches the system vulnerability testing will be follow the bellow methodology


Carry out exploitations on the validated vulnerabilities
Define scope and create threat profile
Information Congregation
Treat Analysis
Vusnerability Assessment
Exploitation
Reporting
Scan for vulnerabilities using Manual/Automated process
Gather Information about the target system
Preparation of security review reports

System Infrastructure

Infrastructure testing is that part of a test project covering the product risks that relate to the target infrastructure. We are covering the areas of system infrastructure with the following milestone and the flowgraph of the testing.


Unit test
System test
Intiation and Planning
Basis installation w/unit test
Operational Test
Application installation
Application Dependent test
Acceptance test
Test Planning and Preparations
Where the system integrates with the application layer
System Integration test

Database testing

The Database is one of the inevitable parts of a Software Application. It does not matter whether it is a web, desktop or mobile, client-server, peer to peer, enterprise or individual business; the Database is required everywhere at the backend. The general test process testing database is not very different from any other application..

A Atomicity

- Transactions are all or nothing

C Consistency

- Only valied data is saved

I Isolation

- Transactions do not affect each other

D Durability

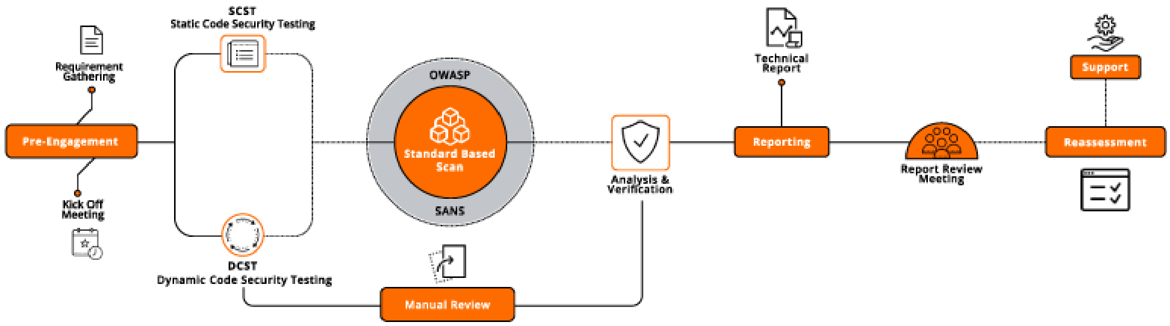
- Written data will not be lost

Business logic

Most security problems are weaknesses in an application that result from a broken or missing security control (authentication, access control, input validation, etc). By contrast, business logic vulnerabilities are ways of using the legitimate processing flow of an application in a way that results in a negative consequence to the organization. From this testing will find the risk factors of Business logics and testing the different layers of the business-like Presentation layer, Business layer and the database layers.

Source code audit

A software code audit is a comprehensive analysis of source code in a programming project with the intent of discovering bugs, security breaches or violations of programming conventions. It is an integral part of the defensive programming paradigm, which attempts to reduce errors before the software is released. It could be including Automatic/Manual, Static/Dynamic, Internal/External, Black box/White box testing. The whole procedure is introduced in a flow graph bellow.

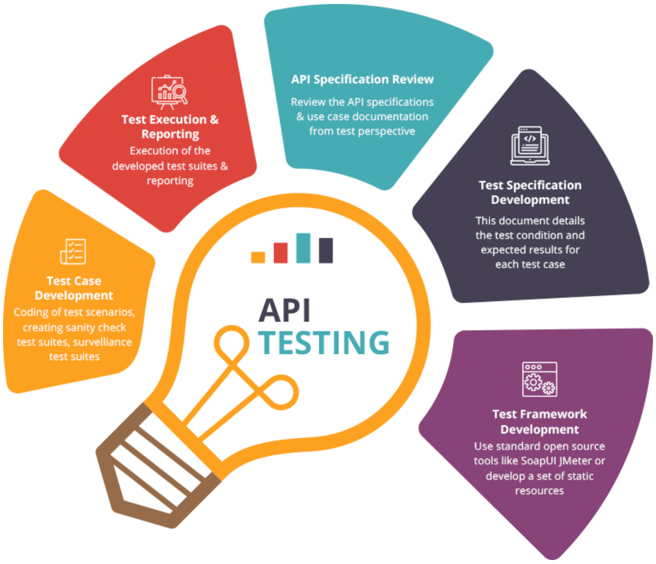


API Testing

Quality Assurance team performs API testing which is a form of Black Box Testing. This testing is conducted post the build is ready. Client, server, and database are the three independent tiers of software architecture.

To ensure the API can handle the expected or higher load, QA engineers validate its functionality and performance by artificially creating or simulating API calls. We'll outline the types of API performance testing. Following Tools used for automated API testing:

Postman client, REST Assured, jMeter etc.


Test Execution & Reporting
Execution of the developed test suites & reporting
API Specification Review
Review the API specifications & use case documentation from test perspective
Test Specification Development
This document details the test condition and expected results for each test case
Test Case Development
Coding of test scenarios, creating sanity check test suites, survelliance test suites
API
TESTING
Test Framework Development
Use standard open source tools like SoapUI JMeter or develop a set of static resources

Web Application Assessment

Website/Web- Application assessment will be done as per latest OWASP guidelines including but not limited to the following: - SQL Injection; Broken Authentication and Session Management; Cross-Site Scripting (XSS); Insecure Direct Object References; Security misconfiguration; Insecure Cryptographic Storage; Authentication; Session Management; Input Manipulation; Output Manipulation; Sensitive Data Exposure; Missing Function Level Access Control; Cross-Site Request Forgery (CSRF); Using Known Vulnerable Components; Un-validated Redirects and Forwards; Failure to Restrict URL Access; Insufficient Transport Layer Protection; Any other attacks, which are vulnerable to the web sites and web Applications .

A Complete Review of the OWASP Top Ten for 2022

- INJECTION
- BROKEN AUTHENTICATION
- SENSITIVE DATA EXPOSURE
- XML EXTERNAL ENTITIES (XXE)
- BROKEN ACCESS CONTROL
- SECURITY MISCONFIGURATION
- CROSS-SITE SCRIPTING (XSS)
- INSECURE DESERIALIZATION
- USING COMPONENTS WITH KNOWN VULNERABILITIES
- INSUFFICIENT LOGGING & MONITORING

Key differences between SAST and DAST:

DAST uses dynamic code analysis to spot runtime problems is one of its main advantages.

SAST is excellent at finding vulnerabilities as code is being produced.

DAST also examines how an application actually responds to an attack, providing valuable information about the likelihood of a vulnerability being exploited.

SAST can pinpoint coding errors, making it simple for developers to identify and address vulnerabilities.

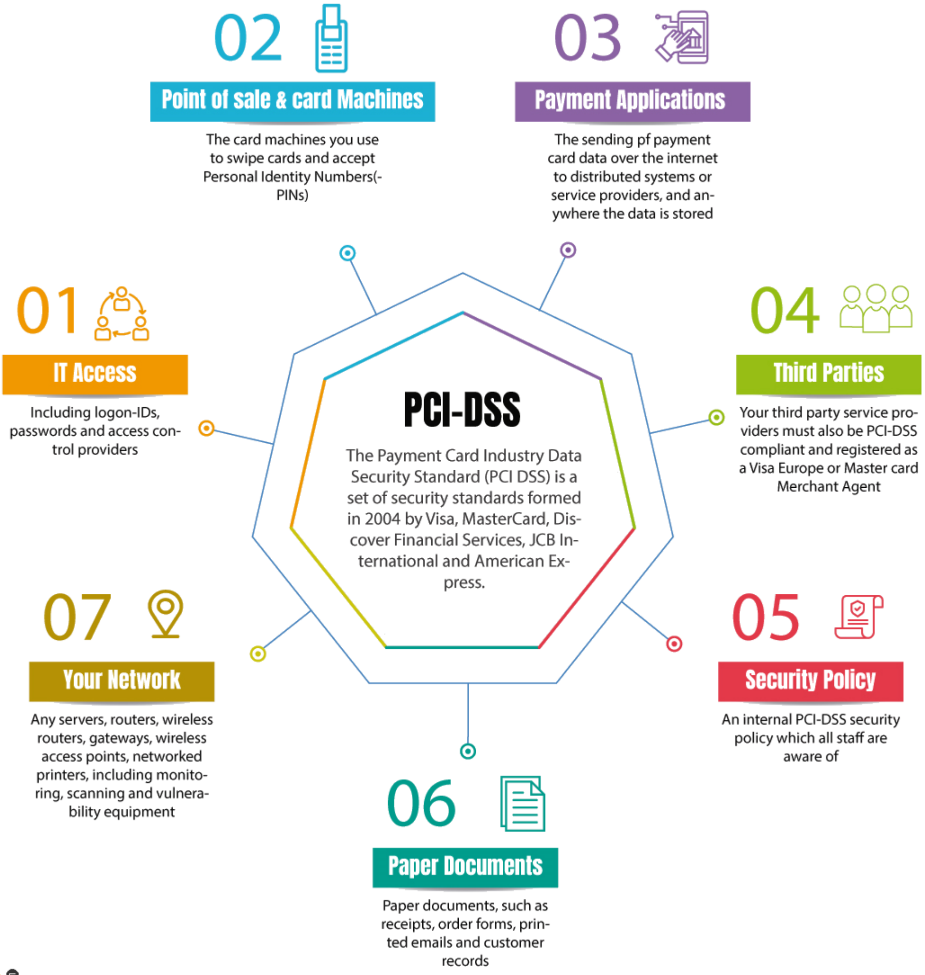
PCI Compliance Services

At BugsBD Limited, we understand the importance of maintaining PCI compliance for businesses that process, store, or transmit credit card information.

Our PCI Compliance service is designed to help businesses achieve and maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS).

Our Approach

Our approach to PCI Compliance is based on a thorough understanding of the requirements and guidelines set forth by the PCI Security Standards Council. We work closely with our clients to understand their unique business and security requirements, and then develop a customized approach to achieving and maintaining PCI compliance.



PCI-DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards formed in 2004 by Visa, MasterCard, Discover Financial Services, JCB International and American Express.

01 IT Access

Including logon-IDs, passwords and access control providers

02 Point of sale & card Machines

The card machines you use to swipe cards and accept Personal Identity Numbers(-PINs)

03 Payment Applications

The sending pf payment card data over the internet to distributed systems or service providers, and anywhere the data is stored

04 Third Parties

Your third party service providers must also be PCI-DSS compliant and registered as a Visa Europe or Master card Merchant Agent

05 Security Policy

An internal PCI-DSS security policy which all staff are aware of

06 Paper Documents

Paper documents, such as receipts, order forms, printed emails and customer records

07 Your Network

Any servers, routers, wireless routers, gateways, wireless access points, networked printers, including monitoring, scanning and vulnerability equipment

Service Tasks

- Conduct a comprehensive review of the business's current security posture and risk profile
- Develop a customized PCI compliance plan that meets the business's specific needs and requirements
- Implement security controls and policies to meet PCI DSS requirements, including network security, access control, and more
- Conduct regular security assessments and audits to ensure ongoing compliance with PCI DSS
- Provide remediation support as needed to address any identified security gaps or issues

Deliverables

- A customized PCI compliance plan that is tailored to the business's needs and requirements
- Implementation of security controls and policies to meet PCI DSS requirements
- Regular security assessments and audits to ensure ongoing compliance with PCI DSS
- Remediation support to address any identified security gaps or issues

Benefits of Our PCI Compliance Service

- Helps businesses achieve and maintain compliance with PCI DSS requirements
- Reduces the risk of data breaches and credit card fraud
- Provides peace of mind for business owners and their customers
- Demonstrates a commitment to security and customer data protection.

ISO 27001 Services

At BugsBD Limited, we understand the importance of information security for businesses of all sizes. Our ISO 27001 service is designed to help organizations achieve and maintain compliance with the International Organization for Standardization's (ISO) 27001 standard for information security management.

Our Approach

Our approach to ISO 27001 is based on a thorough understanding of the standard's requirements and guidelines. We work closely with our clients to understand their unique business and security requirements, and then develop a customized approach to achieving and maintaining ISO 27001 compliance.

Service Tasks

- Conduct a comprehensive review of the organization's current security posture and risk profile
- Develop a customized ISO 27001 compliance plan that meets the organization's specific needs and requirements
- Implement security controls and policies to meet ISO 27001 requirements, including risk assessment, access control, and more
- Conduct regular security assessments and audits to ensure ongoing compliance with ISO 27001
- Provide remediation support as needed to address any identified security gaps or issues

Benefits of ISO 27001 Implementation

Brings your organization to compliance with legal, regulatory, and statutory requirements.

Market differentiation due to positive influence on company prestige.

Increases vendor status of your organization.

Increase in overall organizational efficiency and operational performance.

Minimizes internal and external risks to business continuity.

ISO 27001 certification is recognized on a worldwide basis.

Significantly limits security and privacy breaches.

Provides a process for Information Security and Corporate Governance.

Reduces operational risk while threats are assed and vulnerabilities are mitigated.

Provides your organization with continuous protection that allows for a flexible, effective, and defensible approach to security and privacy.

Reporting Format

The overall report format that apply for technical summary is following:

Interim Reports & Post Execution Activities

It is recommended that the report should contain any and all the findings that impact the security posture of the assessed entity even in cases where exploitation did not occur. In the testing phase, all relevant tests need to be conducted as per the project schedule and satisfactory report should be obtained from the concerned authorities of NABARD before preparing it for execution. Potential risks posed by known vulnerabilities, ranked in accordance with NVD/CVSS base scores associated with each vulnerability. Note that external vulnerability scans must be performed by an ASV and the risks ranked in accordance with the CVSS.

Reporting Format

The overall report format that apply for technical summary is following:

Severity Scoring

Since all the vulnerabilities identified may not have equal severity so in order to prioritize remediation of the penetration test findings, risk ranking is to be assigned for each detected security issue. The Report should clearly document how the severity/risk ranking is derived. Vendor may refer the applicable industry standard or any suitable severity ranking mentioned below: -

- **Common Vulnerability Scoring System (CVSS)**
- **Common Vulnerabilities and Exposure (CVE)**
- **Common Weakness Enumeration (CWE)**
- **National Vulnerability Database (NVD)**
- **Open Source Vulnerability Database (OSVDB)**
- **Bugtraq ID (BID)**

In case of custom scoring is adopted during the risk-ranking process, the report should clearly justify with acceptable reasoning for the modification of industry-standard scores and also in case of arriving at a score for a vulnerability that does not have an industry-standard score defined.

BugsBD Limited provide CVE assignment information to the CNA level above them using the following format. The use of this format facilitates the automation of CVE assignment.

[CVEID]: [THREAT]: [IMPACT]: [STATUS]: [REFERENCES]: [REMEDIATION]:

Reporting Format

The overall report format that apply for technical summary is following:

Vulnerability Metrics

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. The official CVSS documentation can be found at https://www.first.org/cvss/

Vulnerability Severity Ratings: We provide qualitative severity rankings of "Low", "Medium", "High", “Critical” for CVSS v3.1 base score ranges for this project

CVSS v3.1 Ratings	
Severity	**Base Score Range**
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Sample Report

The overall report format that apply for technical summary is following:

Technical Summary

Scope

This section includes the scope of the assessment and it included the following information:

Host: example.com	IP: [192.168.0.1]

Risk Rating

The table below gives a key to the risk naming and colors used throughout this report to provide a clear and concise risk scoring system.

SL	CVSS v3. Score	Description	Risk Rate
1	9.0 – 10	A vulnerability was discovered that has been rated as critical. This requires resolution as quickly as possible.	CRITICAL
2	7.0 - 8.9	A vulnerability was discovered that has been rated as high. This requires resolution in a short term.	HIGH
3	4.0 – 6.9	A vulnerability was discovered that has been rated as medium. This should be resolved throughout the ongoing maintenance process.	MEDIUM
4	1.0 – 3.9	A vulnerability was discovered that has been rated as low. This should be addressed as part of routine maintenance tasks.	LOW
5	0 – 0.9	A discovery was made that is reported for information. This should be addressed in order to meet leading practice.	INFO

Findings Overview section

This section includes the findings of the assessment.

Ref	Description	Risk
######-1-1	SQL Injection	CRITICAL
######-1-2	SQL Injection	CRITICAL
######-1-3	Unrestricted File Upload	CRITICAL
######-1-4	Unauthorized Access	CRITICAL
######-1-5	Sensitive Data Exposure	HIGH
######-1-6	Cross Site Scripting	HIGH
######-1-7	HTML Injection	HIGH
######-1-8	Security Misconfiguration	MEDIUM
######-1-9	Full Path Disclosure	MEDIUM

Technical Details Section

This section includes the details of the finding including the summary descriptions impacts and remediations.

Summary

	Severity:	<RISK LEVEL>	Ref ID: XXXXXX-1-1
	Confidence:	Confident	
	Host:	www.example.com	
	Path:	<where is the vulnerability found>	
	Method	<Methods that are used to exploit >	

Description

This section includes with the description of the vulnerability and how it was exploit.

Request

This section includes the request which are used to exploit the vulnerability.

Response

After the request what expect as response. Describes properly that will help a developer to reproduce the vulnerability to mitigate it.

Impact

Details the impacts of the vulnerability.

Remediation

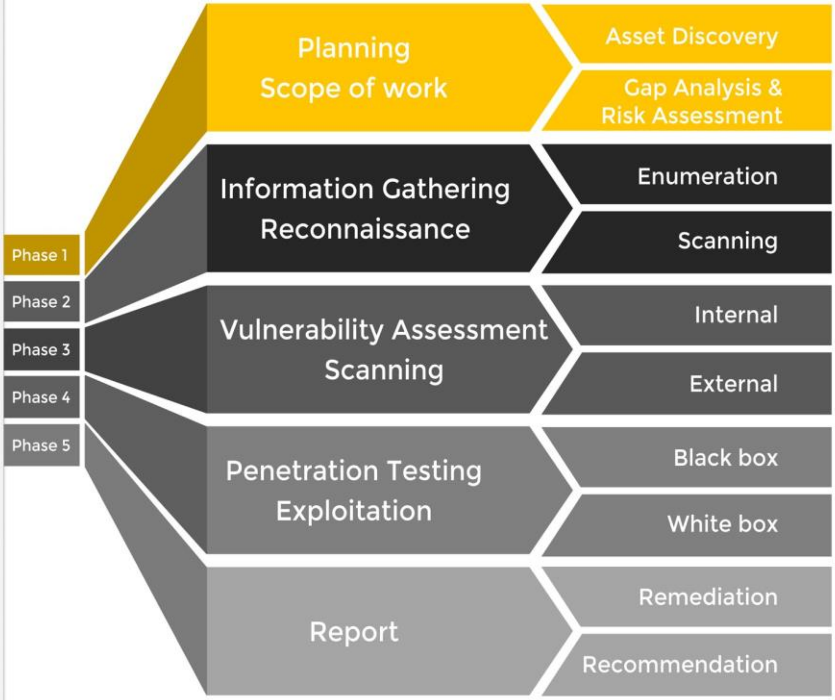
Prevention in future and the remediation are includes in this section.

Working Procedure

Manual Penetration Testing

It's the process to identify security vulnerabilities in an application by evaluating the system or network with various malicious techniques. The weak points of a system are exploited in this process through an authorized simulated attack.
The purpose of this test is to secure important data from outsiders like hackers who can have unauthorized access to the system. Once the vulnerability is identified it is used to exploit the system in order to gain access to sensitive information.
A penetration test is also known as pen test and a penetration tester is also referred as an ethical hacker. Penetration Testing We can figure out the vulnerabilities of a computer system, a web application or a network through penetration testing.

A penetration test tells whether the existing defensive measures employed on the system are strong enough to prevent any security breaches. Penetration test reports also suggest the countermeasures that can be taken to reduce the risk of the system being hacked.



Phase 1
Phase 2
Phase 3
Phase 4
Phase 5

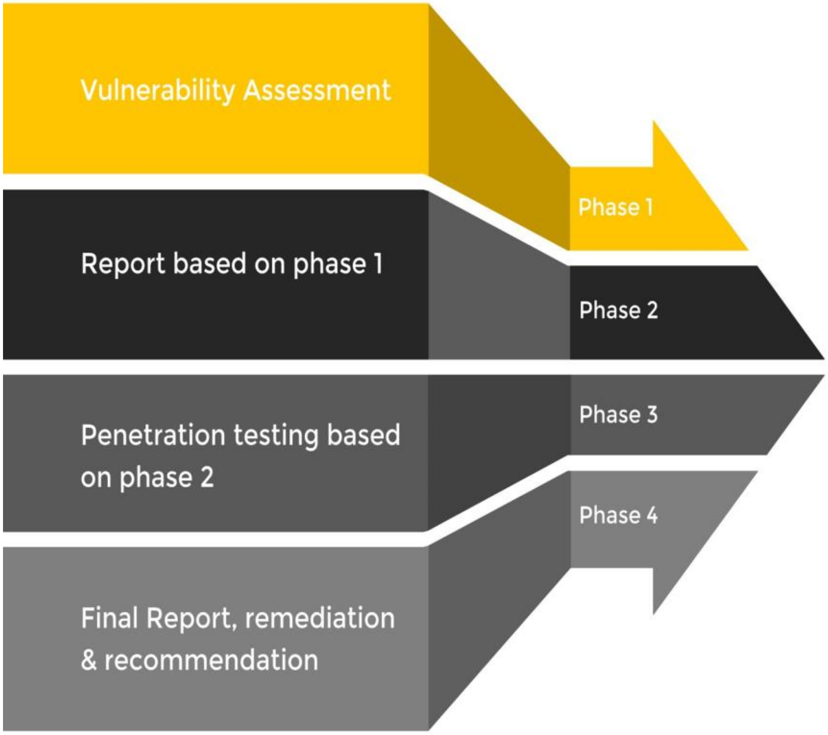
Planning
Scope of work
Asset Discovery
Gap Analysis &
Risk Assessment

Information Gathering
Reconnaissance
Enumeration
Scanning

Vulnerability Assessment
Scanning
Internal
External

Penetration Testing
Exploitation
Black box
White box

Report
Remediation
Recommendation



Vulnerability Assessment
Phase 1

Report based on phase 1
Phase 2

Penetration testing based on phase 2
Phase 3

Final Report, remediation & recommendation
Phase 4

Automated Penetration Testing

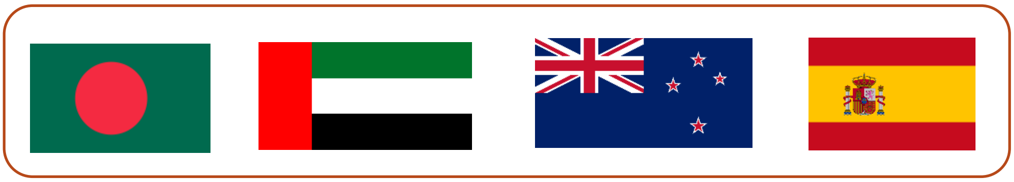
There is a considerable amount of confusion in the industry regarding the differences between vulnerability scanning and penetration testing, as the two phrases are commonly interchanged.

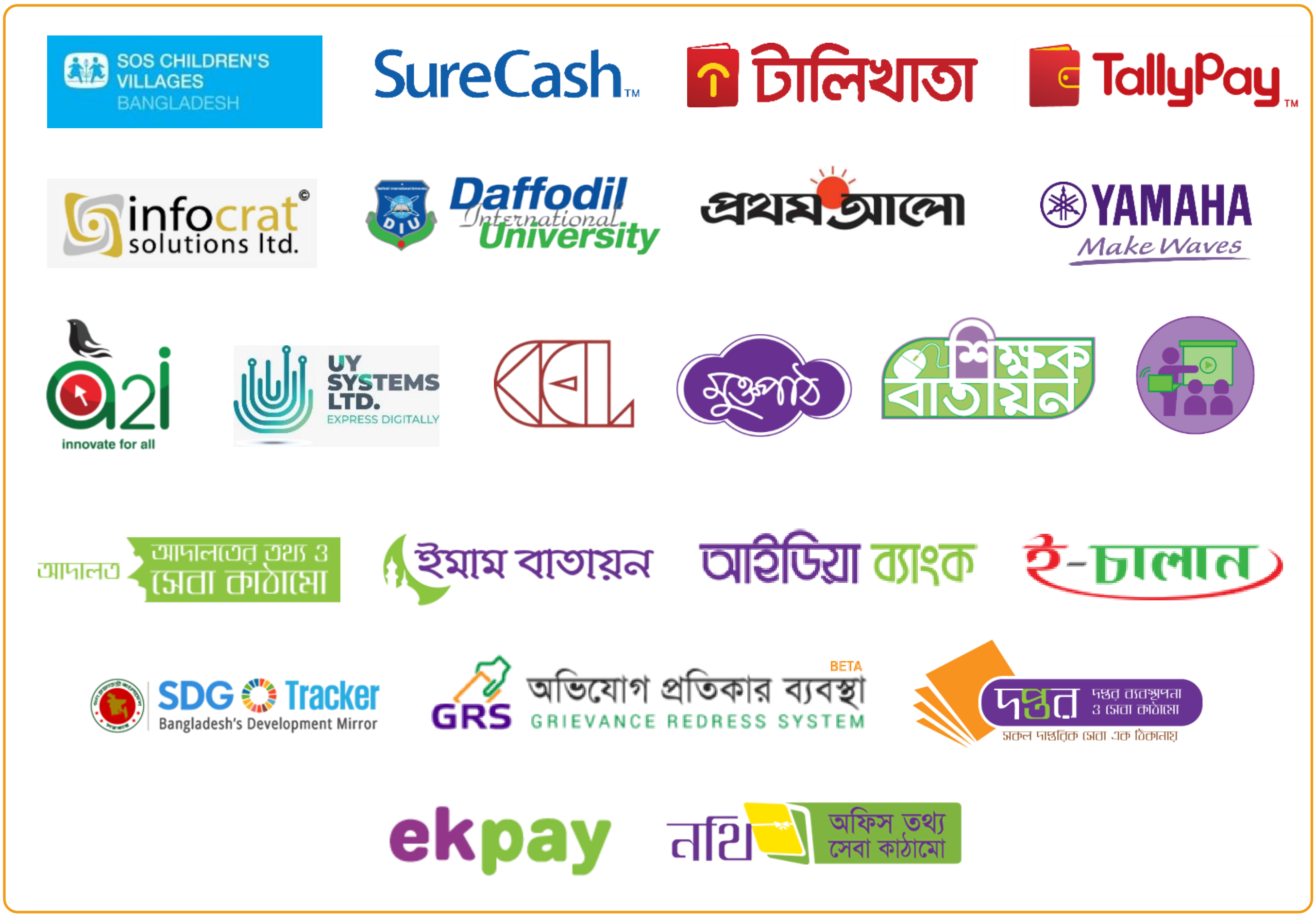
However, their meaning and implications are very different. A vulnerability assessment simply identifies and reports noted vulnerabilities, whereas a penetration test (Pen Test) attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible.

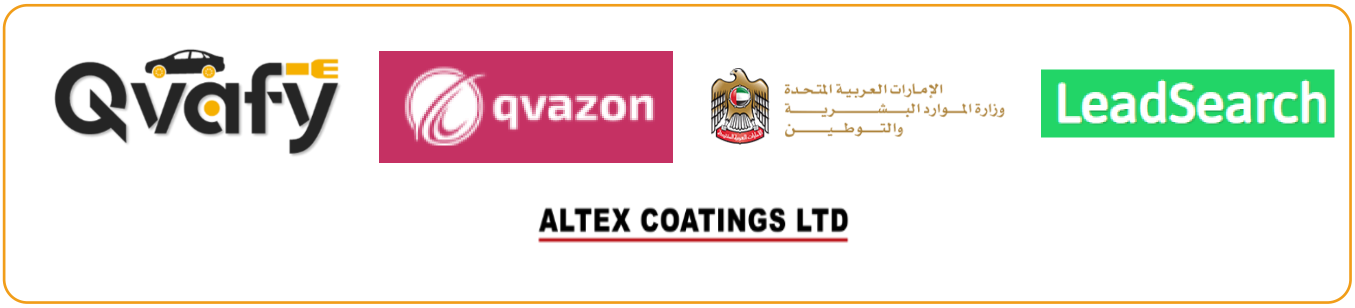
Penetration testing typically includes network penetration testing and application security testing as well as controls and processes around the networks and applications, and should occur from both outside the network trying to come in (external testing) and from inside the network.

BRINGS CLIENTS

A FORTUNE WITH REAL RESULTS




SOS CHILDREN'S VILLAGES BANGLADESH
SureCash™
টালিখাতা
TallyPay™
infocrat© solutions ltd.
Daffodil International University
প্রথম আলো
YAMAHA Make Waves
a2i innovate for all
UY SYSTEMS LTD. EXPRESS DIGITALLY
মুক্তপাঠ
শিক্ষক বাতায়ন
আদালত আদালতের তথ্য ও সেবা কাঠামো
ইমাম বাতায়ন
আইডিয়া ব্যাংক
ই-চালান
SDG Tracker Bangladesh's Development Mirror
GRS অভিযোগ প্রতিকার ব্যবস্থা BETA GRIEVANCE REDRESS SYSTEM
দপ্তর দপ্তর ব্যবস্থাপনা ও সেবা কাঠামো সকল দাপ্তরিক সেবা এক ঠিকানায়
ekpay
নথি অফিস তথ্য সেবা কাঠামো



FUTURE PLAN

“The area of Information Security is rising up in world in very recent. The future plan of BugsBD Limited. is not only ensure the information security but also establish some good opportunities for Information Security Researchers in the world.

BUGS BD Limited

Your Cyber Security Partner

" Working together to keep your organization safe. "

1/C, Shyamoli, Road-01
Dhaka-1207, Dhaka

info@bugsbd.com

(+880) 1761616261
(+880) 1889975511

www.bugsbd.com