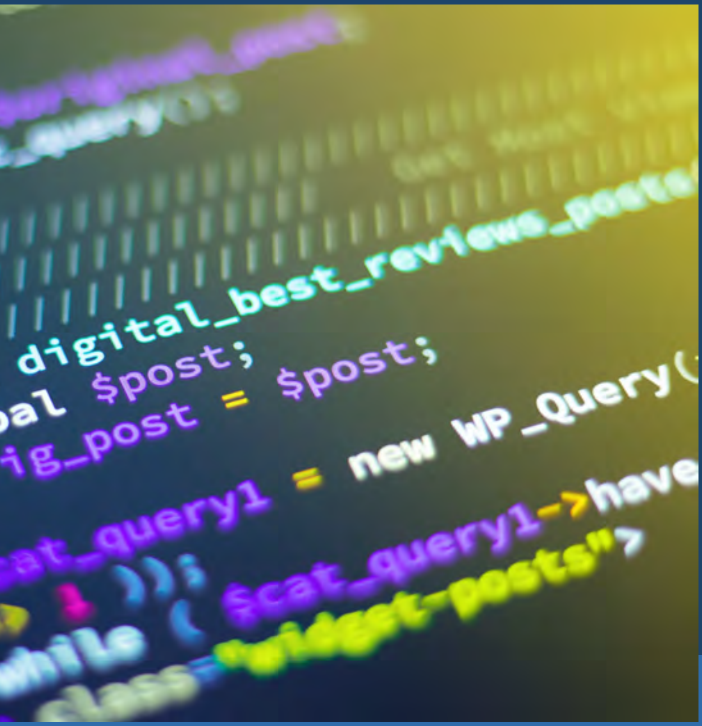
DATA-CORE SYSTEMS



Application Penetration Testing

A Quintessential Primer

Data-Core Systems Inc.

www.datacoresystems.com

Executive Summary

Application Penetration testing is a critical subject for businesses in today’s world. Incorporating penetration testing into your development lifecycle can go a long way to contribute greatly to your organization’s security. However, setting up and planning Penetration testing, or Pen-Testing, can be an uphill road for teams venturing into it. Understanding the rudiments of Pen-Testing can set the foundation for practicing Penetration Testing the right way and derive the best results out of it. This whitepaper aims to provide an idea on how to plan, setup, monitor and manage your application penetration testing practice.

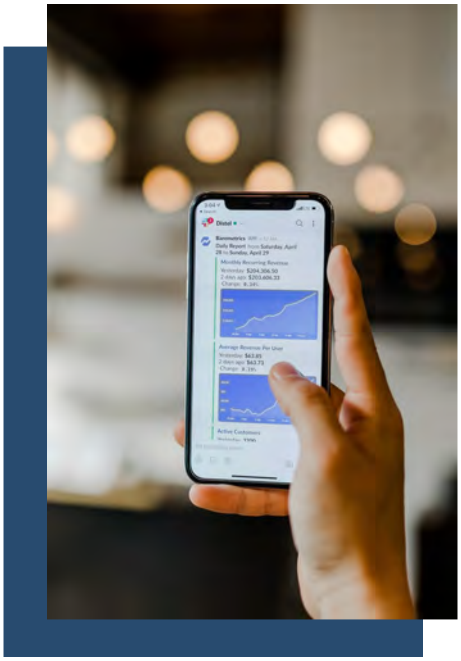
Background & Problem

Today many companies are not focused enough on emboldening the security of their applications yet. The applications are either accessible over the internet or are hosted on a network which is not carefully firewalled and protected. This is leaving a huge scope for cyber attackers or black-hat hackers to exploit the vulnerabilities for illicit purposes. Cyber attackers today work in the most creative and nefarious ways to get past application boundaries. Any application that is deployed without testing and addressing the susceptible points ends up losing critical data, confidential business information, user identity data, credit card data, copyrighted materials and more. In turn, this is costing organizations millions of dollars when their applications become subject to a security breach. Not only do these companies lose money in attempts to retrieve their data, but they're losing time, using a lot of resources that could be spent on more crucial activities to the business, and even losing customers.

Though there can be a gamut of areas where an organization can suffer losses owing to an attack, this whitepaper explores a few that are the most prominent and should be strongly heeded to.

Loss of Business Data

Losing critical business data to cyber-attacks is one of the most common problems faced by companies today around the globe. Attacks are made targeting databases and data storages either directly or through an application's front-end leveraging its loopholes. This loss can trigger an operational shutdown resulting in considerable financial damages.



Identity Theft

An attacker can manage to acquire complete access to customer or employee databases or data stores gaining complete control of the users' confidential information. Identity data are highly lucrative in the dark web's marketplace and therefore, are highly sought after by cyber criminals. Companies must pay extra caution to keep this data safe and secure following modern ways of encryption and cryptology.

Loss of Privacy

In addition to identity theft, users' personal information like health data, personal emails, messages etc. would be completely exposed to the perpetrator in an event of a successful break-in. This data is either sold to a bidder in the dark web or used for blackmailing and extortion.

Credit Card Fraud

In United States alone, losses incurred by various financial institutions from credit card fraud totaled more than $30 billion in 2018. User credit card or payment information are often stored by engineering teams in databases without using the modern cryptographical standards and architectural practices. This inevitably puts the data at high risk and becomes hospitable for invaders.

Piracy

A vulnerable and unsecure application or software can be a doorway to a network that can put the whole organization at the behest of the attacker. The attacker can gain access to copyrighted or patented assets of the organization under attack for either piracy or to seek ransom in return.

Foundations of Penetration Testing

Types of Penetration Testing

Penetration Testing can be performed broadly in three ways – Black Box Testing, White Box and Grey Box Testing.

Black Box

In a Black Box Penetration Test, no information or very limited information is available to the testing team. Neither the architecture nor the source code is available to the tester at the time of testing. This makes the testing ideal to replicate the actions of a real black-hat hacker who also comes in with no knowledge of the application. However, Black Box testing can be time consuming since it involves the tester to build their attack tactics from scratch.

White Box

In contrast to Black Box Penetration Testing, White Box Penetration Testing is performed with complete information of the application and the platform it is hosted on. The architecture diagrams, network setup, code structure, and cloud configurations are all at the disposal of the tester to exploit. Since the testing is performed with all the information, the testing can be more incisive and elaborate. The issues discovered in this testing are more in-depth and brings more minute loopholes in the design. Whilst white-box testing is not so much alike to a real hacker's attack, it is important to perform this test to prevent further damage done by a hacker once they are able to break in.

Grey Box

Grey Box testing, as the name suggests, takes just enough information from the application to start the testing. The grey box testers are usually provided with certain network and architectural details right at the inception. This approach is most widely followed and is very efficient to find a detailed Penetration Testing report.

Penetration Testing Perspectives

Furthermore, Penetration Testing can be categorized based on the perspective of whether the testing is performed externally or internally to the application.

External Penetration Testing

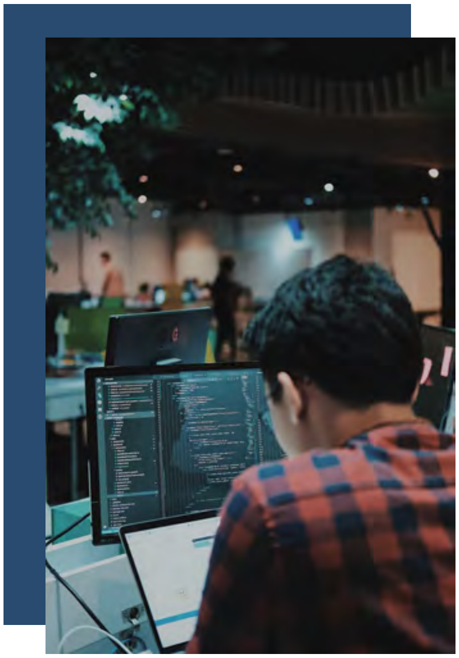
External Penetration Testing is performed by simulating the actions of an external attacker. The tester accesses the application externally either over the internet or via a network pathway. The objective of the Pen-Tester is to establish connection, intrude and extract as much confidential information as possible. The tester might want to get to the database right from the public facing interface to retrieve data. He can also try to overwhelm the application server and/or the database server to cause a Denial of Service to adjudge the resiliency and fault tolerance capacities of the application.

Internal Penetration Testing

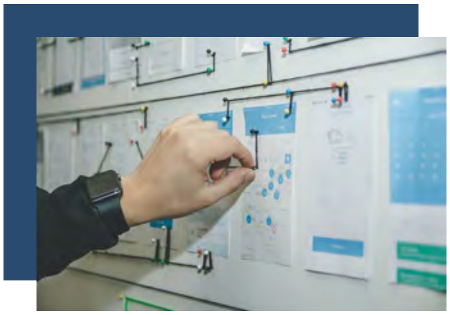
Internal Penetration Testing is performed with an intention to replicate the possible modus operandi of an attacker once they have gained access to the system. The pen-tester will try to attain root access or user rights with the highest privileges to be able to alter the function ality of the application or stop it completely. The tester might try to search for proprietary algorithms in the codebase to see if it is readily accessible. The pen-tester can also get to the database and see if the records such as sensitive as user information, payment information, health information, etc. could be altered or dumped into an external storage.

Structure of Penetration Testing

Penetration Testing can get highly elaborate and extensive depending on the scale at which it is planned and performed. By and large, organizations split the whole project in seven distinct phases. This can be termed as the Penetration Testing Lifecycle.



Planning and Scoping



A penetration testing project starts with planning and scoping. This phase covers understanding the requirement, the project scope, risks involved, timeline, budget, vendor selection, scope discussion, signing an NDA, and the project setup. It is important to understand that a penetration tester would essentially be an attacker, but a hired attacker with no nefarious intent. The tester's objective is to explore every possible option to break into your solution and gather confidential information out of the system. It can get a bit confusing and doubtful for your peers to accept and thus it is critical to keep all the concerned stakeholders in confidence before the testing is performed on your application.

Reconnaissance

Once the Penetration Testing team is assigned the job of performing the tests, the pen-testers will ask for necessary information like the website URL, a brief functional detail of the application, and likes depending on the stage and requirements for the testing. During the Reconnaissance phase, the tester will try to procure as much information as possible about the application and the platform it is hosted on. Assessments are performed to figure out server types, operating system, performance, up times, peak hours information using server responses, network traffics and even using contorted searches on a search engine like Google. This information is used to extensively profile an application under the hammer and leverage it for identifying vulnerable points of entry.

Vulnerability Assessment

Vulnerability Assessment involves assessing vulnerable points of the application through various ways of exploitation using the profile created under Reconnaissance. The tester delves into launching attacks at every vulnerable point of the application with an objective to break in and perform tasks that he is not authorized to do in the solution. Few of the primary attacks that are performed are scraping the server directories to dump all server files for reading, targeting FTP and SMTP ports to understand the network topography, push cross-site scripts to perform illegal operations on forms, inject code to attack the database, executing code from a remote machine, and overwhelm the server with inestimable packet pushes.

Gaining Access

Gaining Access can be too easy or too hard and generally takes the most amount of time. The tester uses the vulnerable points to break in and gain complete access to the application. Once the tester is inside an unauthorized zone, they will try to do a perimeter check and search for objects of interest. The tester then collects and records as much data and information as possible.

Maintaining Access

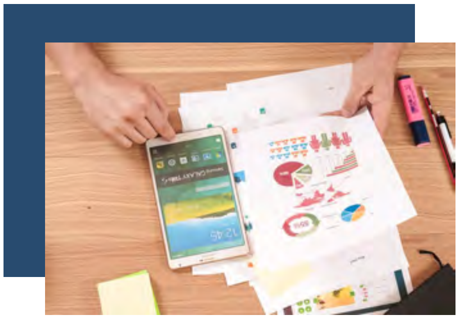
The tester would try to elevate their access by assuming administrative rights over the application. Once they can elevate themselves, the solution might be completely at their behest. They would try to maintain access for as long as possible thwarting every chance of getting ousted. The tester can try to block authorized users from logging in or accessing confidential data from the database. Every exploit is recorded in the report with necessary details of the modules traversed.

Artifact Collection

Artifact Collection is often an optional phase in the Penetration Testing Life Cycle. The tester might want to keep certain information and data that they could lay their hands on as a testament to the vulnerabilities exploited.

Reporting

All of the previous steps are recorded and documented into a comprehensive report for the development and networking teams to start working on the fixes. A pen-test report should be comprehensive and lucid enough to be legible by both the engineering audience and the business stakeholders. The report contains a summary which is generally targeted towards a neutral audience followed by technical details for the engineering teams. The technical section contains details of the vulnerabilities, exploits, and possible remediations. The remediation suggestions are intended to help the developers fix the issues quickly.



10 Steps for Security Project Planning

In an effort to mitigate security breaches and their effects, organizations need to implement security testing in every deployment and update of their applications. Security is highly critical and must find a place right at the project planning phase. There are some key steps to effectively plan your penetration testing project.

1. Understand the need for Penetration Testing to build robust and secure applications for your organization or your customers.
2. Liaise with your engineering team to understand the scope of the application that needs to be Pen-tested.
3. Identify and document the scope of the project, determine the goals, project a tentative timeline and assess a budget for the project.
4. Work with your engineering and compliance team to understand the sensitivity of the data hosted and the risks involved in sharing or exposing the data.
5. Contact a vendor like Data-Core Systems to discuss your requirements and objectives, timelines and limited paraphernalia to give them an overview of the project.
6. Sign a Non-Disclosure Agreement (NDA) with the vendor to protect your data.
7. Work with your engineering team to help the vendor get the solution essentials to start the testing.
8. Identify a threshold of tolerance for the vulnerabilities in your solution for each criticality level of high, medium and low.
9. Make sure the report provided by the vendor is comprehensible and lucid enough for developers to start working on the issues.
10. Iterate until all vulnerabilities have been remediated or the vulnerability weightage is below the intended threshold of tolerance.

Benefits

By implementing security testing, organizations can save time, money, and resources through:

- Reduced risk of cyber attacks
- Safeguarding data
- Protecting company image
- Improving trust from customers
- Avoiding damages and losses incurred from attacks
- Avoiding expenses from damages suffered

Things to Consider

1. **Testing Scope**
   It might be possible that the testing has not covered all points of vulnerability, due to timeline limitations, scope limitations, access limitations or any reason whatsoever. Thus, it is important to do repetitive tests at certain intervals, more importantly whenever there are feature modifications and updates.

2. **Production System**
   If you should be performing the testing on your production server, if your production cannot afford any downtime or any hammering and manhandling, it is prudent to do the testing on a pre-production landscape.

3. **Applicability**
   Performing penetration testing might be time consuming and labor intensive. It also requires you to allocate a portion of your budget to either assign the job to a vendor or hire security personnel to do it internally. But it is also a hard truth, that no solution, big or small, are prone to attacks. If your application has the scope to store data or is a gateway to storages containing sensitive information or you are accepting payment information from your user, it is highly advisable that you put significant effort in making your application safe for your users.

Summary

Penetration Testing is a great way to build a secure and robust solution that is critical in today’s day and age. Your customers expect your application to protect their data and any breach of that trust can prove to be detrimental to the image of your brand and business. Not only is it beneficial from the perspective of your customers but also an effective way to keep your own company’s data and assets safe from the clutches of the attackers. Your Penetration Testing vendor should be capable enough to help you achieve the security your application deserves and work in close collaboration with your engineering team offering all the assistance required for you to meet your security goals.

Data-Core’s penetration testing team is highly skilled and meticulous in performing penetration testing. Working with government enterprises to secure their software infrastructures on a massive scale is just one example of how we’ve helped protect millions of bytes of sensitive data. With these experiences under our belt, we’re well equipped and uniquely positioned to help you on your Pen-Testing journey.

Data is at the core of what we do.

Our world is being re-imagined through Analytics, Artificial Intelligence and Automation. Data-Core Systems is a digital transformation solution provider helping businesses reshape their future. We are a proven partner with a passion for client satisfaction, combining technology innovation, business process expertise and a global, collaborative workforce.

DATA-CORE SYSTEMS

Data-Core Systems Inc.

1500 John F. Kennedy Blvd.
Suite 624
Philadelphia, PA 19102

Tel: 215 243 1990
Toll Free: 877 327 4838
Fax: 215 243 1978

dcs@datacoresystems.com
www.datacoresystems.com