**Harshdeeep Shrivastava - 20BCY10068**

**Sainyam Agrawal – 20BCY10151**

**Ashwin Shailajan - 20BCE10209**

**Security Awareness Training**

1. **Introduction**

In today's rapidly evolving digital landscape, organizations face a multitude of security threats that can compromise their sensitive information and undermine their operations. Cyberattacks, data breaches, and other malicious activities have become increasingly sophisticated, targeting not only technological vulnerabilities but also exploiting human error and ignorance. As the weakest link in the security chain, employees play a crucial role in protecting an organization's assets. However, without proper knowledge and awareness, they may unintentionally expose the organization to significant risks.

This report focuses on the importance of security awareness training programs in educating employees about potential threats and presents the findings of the foot printing, reconnaissance and various attacks conducted on the provided dummy website(testfire.net)

The report begins by discussing the significance of security awareness training in today's threat landscape, highlighting the changing nature of cyber threats and the critical role employees play in safeguarding organizational assets

Moreover, this report highlights the criticality of security awareness training programs in educating employees about potential threats and safe practices and investigates the given website and provides report about the vulnerabilities discovered, their Common Vulnerability Exposure (CVE) Number, their CVE Score according to Common Vulnerability Scoring System(CVSS), their severity, and impacts.

In summary, report addresses the challenges organizations may encounter when implementing security awareness training initiatives, such as resistance to change, limited resources, and the need for ongoing reinforcement. It offers insights into overcoming these challenges and provides practical recommendations for creating a sustainable and effective security awareness training program.

1. **Information Gathering for Security Awareness Training**

Before developing and delivering security awareness training programs, it is essential to gather relevant information to understand the various aspects of potential threats and safe practices. This section focuses on different methods of information gathering that can provide valuable insights for designing effective security awareness training programs. The following smaller titles explore specific areas of information gathering in the context of security awareness training.

* 1. Email Footprint Analysis

Email Footprint Analysis refers to the process of gathering and analyzing information related to an organization's email communication to identify potential vulnerabilities and risks. The analysis begins by examining the email address format, which can provide clues about naming conventions used by organizations.

2.2 DNS Information Gathering:

DNS (Domain Name System) Information Gathering involves collecting data related to an organization's DNS infrastructure to assess potential security risks and vulnerabilities by examining DNS information, one can gain insights into the infrastructure, services, and potential vulnerabilities associated with a domain.

2.3 WHOIS Information Gathering:

WHOIS Information Gathering involves extracting and analyzing publicly available domain registration information to gain insights into the ownership and administration of domains.

WHOIS records contain details such as domain registrants, contact information, registration dates, and domain expiration dates. By examining WHOIS information, organizations can identify potential risks associated with domains and educate employees on the importance of domain management and protection. This information can be useful for various purposes, such as identifying domain owners, investigating potential misuse, or performing cybersecurity research.

2.4 Information Gathering for Social Engineering Attacks:

Social Engineering attacks exploit human psychology and behavior to manipulate individuals into divulging sensitive information or performing unauthorized actions. Gathering information related to social engineering techniques can help organizations educate their employees about the tactics employed by attackers.

Social engineering attacks often leverage personal or publicly available information to build rapport, establish trust, or deceive individuals. By understanding these techniques and the potential sources of information, employees can become more vigilant and adept at recognizing and mitigating social engineering attempts.

2.5 Information Gathering for Physical Security Assessments:

Physical Security Assessments involve evaluating an organization's physical infrastructure, access controls, and security measures to identify vulnerabilities and potential entry points for unauthorized individuals.

Physical security assessments often involve gathering information about an organization's premises, security policies, surveillance systems, and employee access controls. By raising awareness about physical security risks and best practices, organizations can enhance employee vigilance and contribute to a more secure work environment.

1. **Vulnerability Identification**

Vulnerability identification is a critical component of security awareness training programs, as it enables organizations to understand and address potential weaknesses in their systems and applications. This section focuses on the process of identifying vulnerabilities and provides essential information, including vulnerability names, Common Weakness Enumeration (CWE) codes, and corresponding Open Web Application Security Project (OWASP) categories and descriptions. The following smaller titles cover different aspects of vulnerability identification within the context of security awareness training.

These are some vulnerabilities that were found during static code analysis. To enable these vulnerabilities, place the highlighted text in AltoroJ's WEB-INF folder and enable those properties you would like to enable by uncommenting them

**3.1 Behavioural Vulnerabilities**

* enableAdminFunctions property enables administrative functions in AltoroJ (adding users, changing passwords, etc). Enabling this function and then running AppScan on AltoroJ will likely trash the database and make AltoroJ unusable. You will need to either manually delete the database every time or enable database.reinitializeOnStart and restart Tomcat

**#enableAdminFunctions=true**

* specialLink property changes certain links in AltoroJ (e.g. "Search News Articles" in the authenticated user navigation panel) to the link specified in this property. This allows for demonstrating AppScan's malware detection capabilities. WARNING: It is STRONGLY RECOMMENDED that you USE ONLY SITES THAT DO NOT SERVE ACTUAL MALWARE (use other types of undesired sites)

**#specialLink=http://www.warez.com**

* advancedStaticPageProcessing property enables advanced file/page lookup using Bash or Command Prompt. This exposes AltoroJ to remote command execution and system path traversal WARNING: USE THIS SETTING AT YOUR OWN RISK. USE IT ON PROTECTED SYSTEMS OR IN A VM ONLY ACCESSIBLE FROM THE HOST

**#advancedStaticPageProcessing=true**

* enableFeedbackRetention property turns on AltoroJ functionality to store feedback information in its database. This allows for demonstration of persistent XSS attacks. WARNING: Enabling this function and then running AppScan on AltoroJ will likely trash the database and make AltoroJ unusable. You will need to either manually delete the database every time or enable database.reinitializeOnStart and restart Tomcat

**#enableFeedbackRetention=true**

**3.1 Database Vulnerabilities**

* database.alternateDataSource property allows AltoroJ to connect to an external database (e.g. DB2). This property is the name of the data source configured in tomcat's context.xml which contains details for this database connection. This will also require adding in the appropriate JDBC driver JAR. See the following URL for more details: <https://tomcat.apache.org/tomcat-7.0-doc/jndi-datasource-examples-howto.html> IMPORTANT: If you use this property, you must also set database.reinitializeOnStart to true the first time you run AltoroJ and log into the application. This is required to initialize AltoroJ data. You can disable database.reinitializeOnStart afterwards. Failure to use database.reinitializeOnStart=true at least once will cause AltorJ to fail unless you manually create DB contents

**#database.alternateDataSource=jdbc/AltoroDB**

* database.reinitializeOnStart setting forces AltoroJ to reinitialize its database every time Tomcat is restarted instead of only initializing it if AltoroJ database does not exist. You MUST use this setting at least once if using an external DB.

**#database.reinitializeOnStart=true**

* Some of the Non-Public News Articles, which are hidden from search settings can be found and read after obtaining the source code or by even inspecting the correct element in the browser.

**<publication>**

**<id>4</id>**

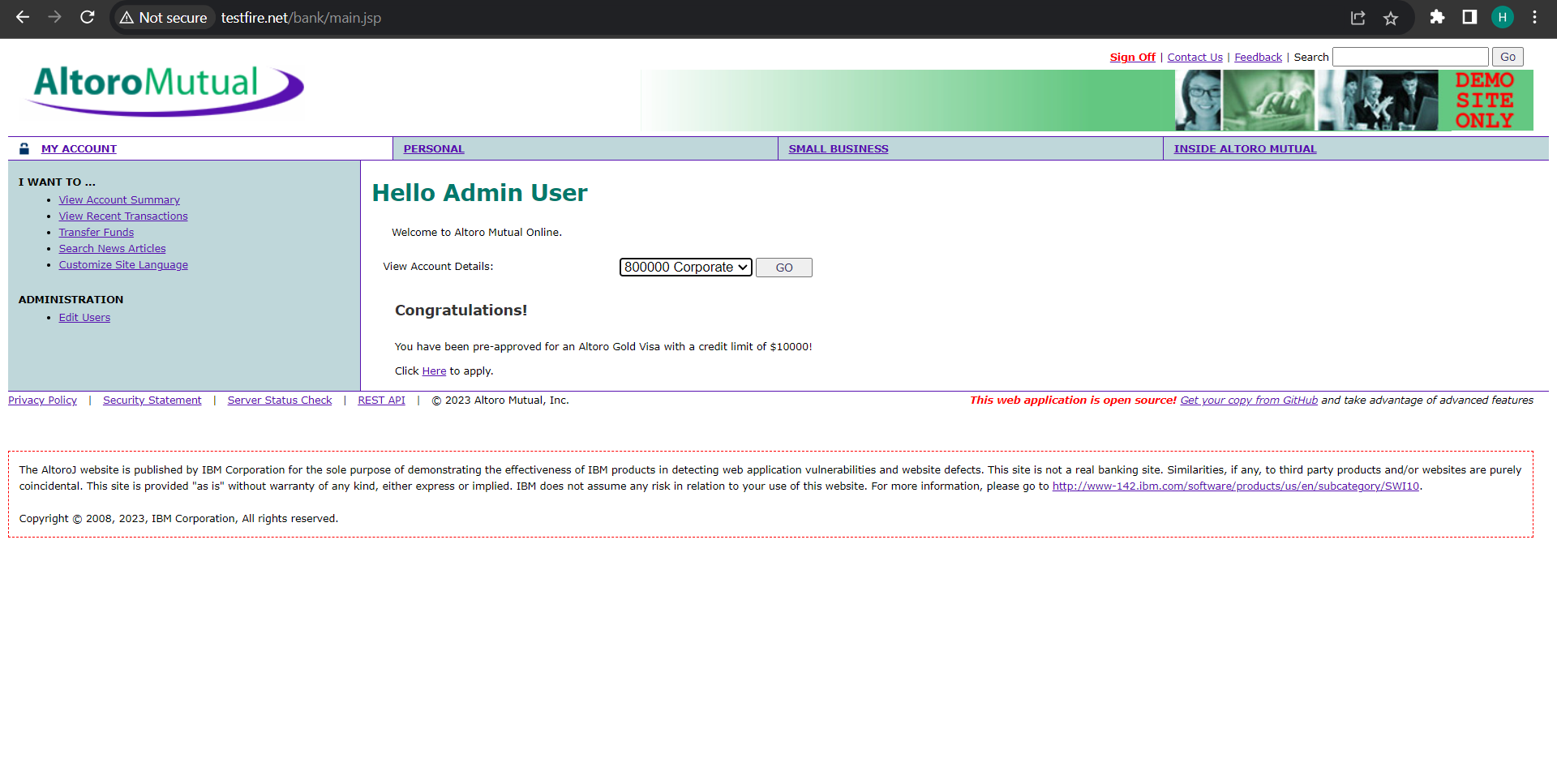
**<date>1/8/2004</date>**

**<title>Altoro Mutual bank about to purchase 10 AppScan and 50 AppScan DE from Watchfire inc.</title>**

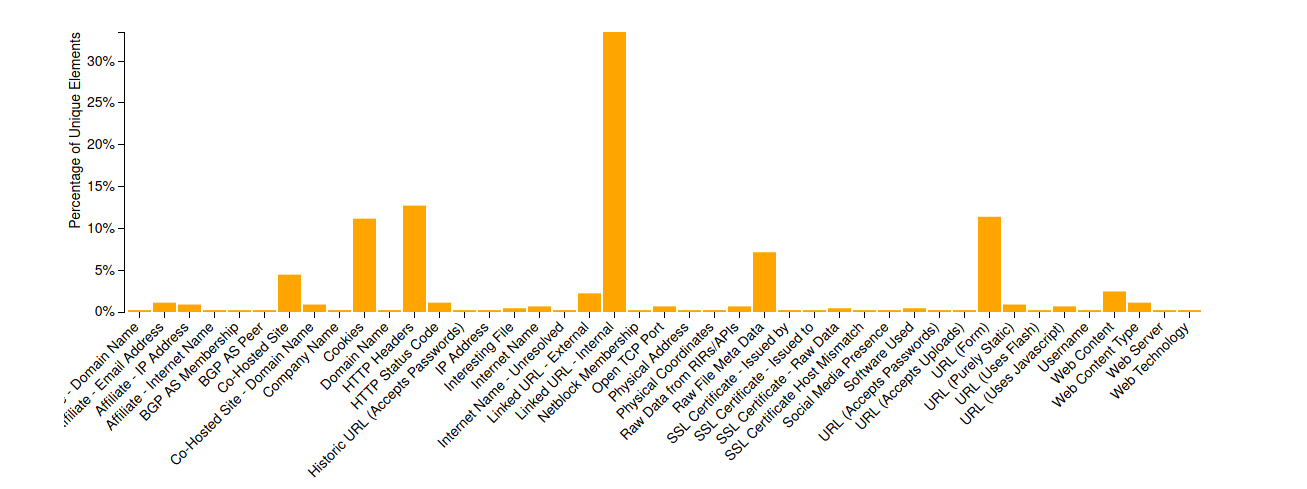
**<isPublic>False</isPublic>**

**</publication>**

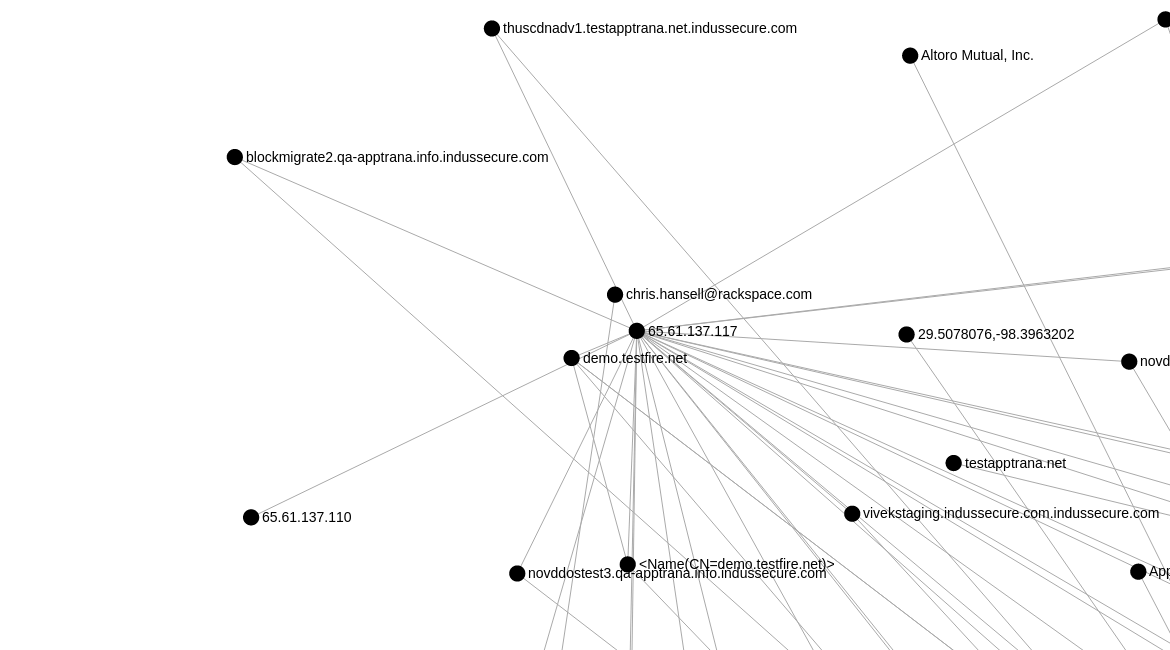
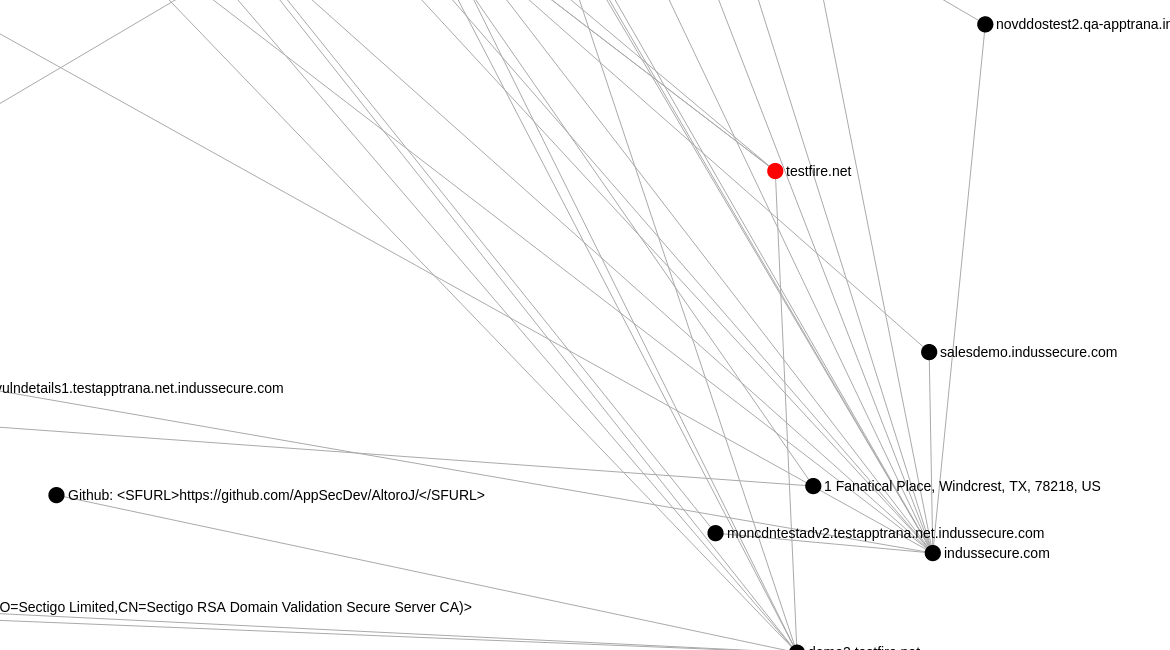
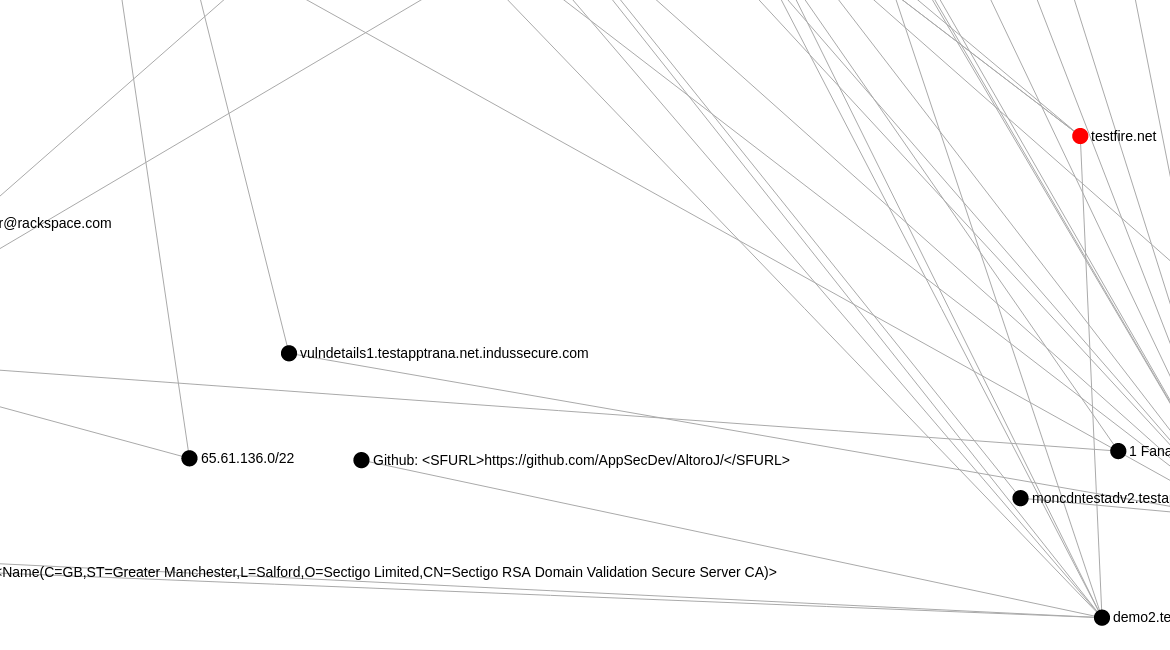
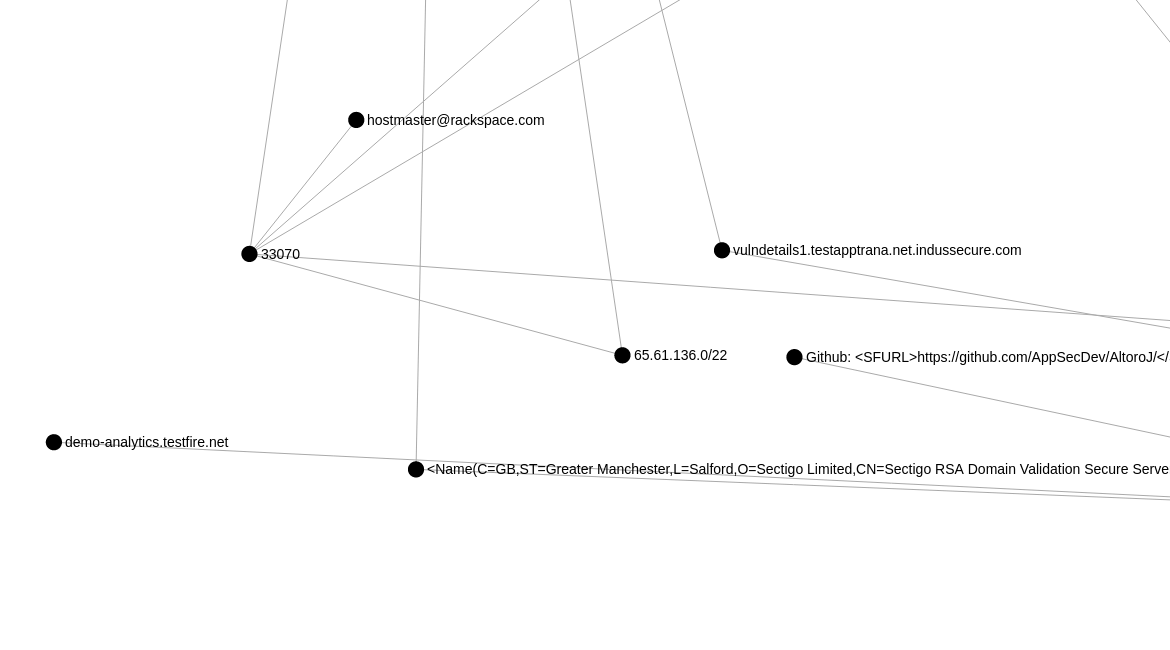
* The website is also vulnerable to XSS attacks
* Upon further dynamic analysis, it was found that the Website is Vulnerable to SQL Injection attacks. During the login process, if some special characters are given in password, the process crashes, this denotes that the username and password are being processed in clear text and no encryption or hashing algorithms are being used. To gain access of admin level clearance use Username = admin and Password = ‘ or 1=1-- . This plays with the sql syntax used to process the password and makes the condition true by using 1=1--.



Web Scraping Output Graphs:



Internet Web Graph



Server IP Address: 65.61.137.117

Public Key type: rsa

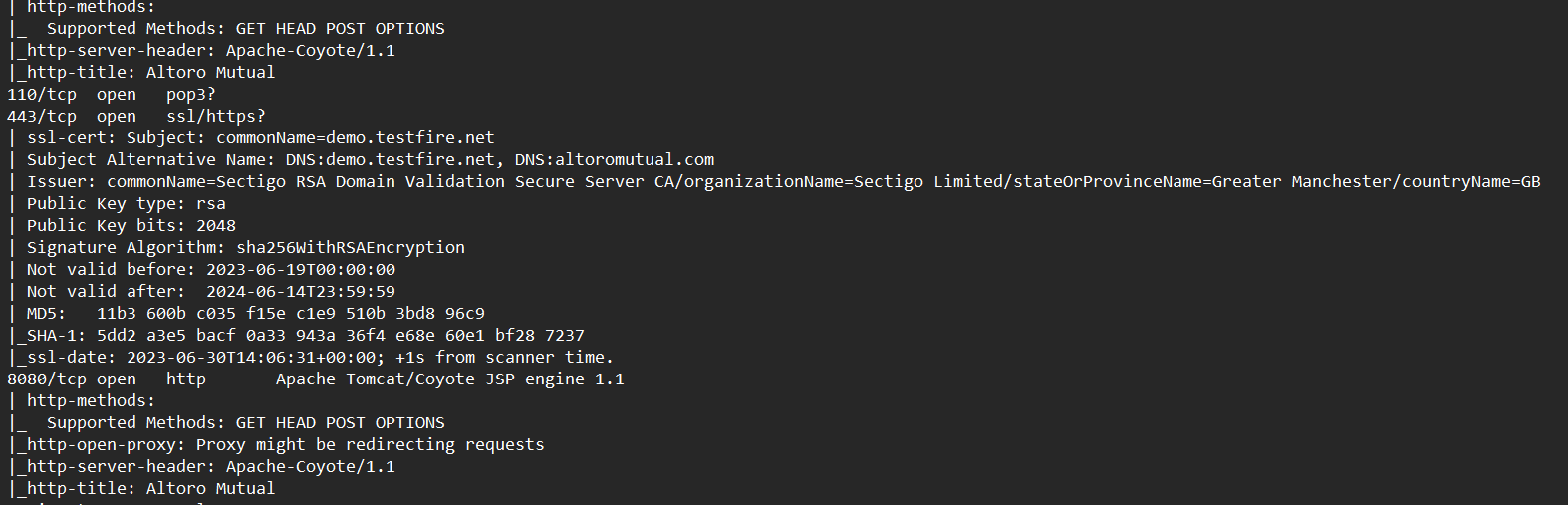
Public Key bits: 2048

Signature Algorithm: sha256WithRSAEncryption

HTTP Version User: HTTP 1.1/0

Open TCP Ports: 25/tcp , 80/tcp , 110/tcp , 443/tcp , 8080/tcp

Digital Certificate Details Extracted by Nmap



**Business Impact Assessment**

**Introduction:**

Conducting a comprehensive business impact assessment is a crucial step in understanding the potential consequences of vulnerabilities on an organization's operations, assets, and reputation.It involves assessing the consequences of various risks and threats, both internal and external, to determine their potential effects on key business processes, resources, and overall business continuity. By analyzing the potential business impact of each vulnerability, organizations can prioritize their mitigation efforts, allocate resources effectively, and make informed decisions to protect critical business functions. This section focuses on the process of conducting a business impact assessment and understanding the potential consequences of vulnerabilities.

**1. Conducting a Business Impact Assessment:**

Introduction: A business impact assessment involves evaluating the potential impact of vulnerabilities on critical business functions, processes, and assets.

By conducting a thorough assessment, organizations can identify vulnerabilities that have the highest potential to disrupt operations, compromise sensitive information, or result in financial losses. This assessment enables organizations to prioritize remediation efforts and implement appropriate controls to mitigate the identified risks effectively.

**2. Understanding Potential Consequences of Vulnerabilities:**

Introduction: To conduct an effective business impact assessment, it is crucial to understand the potential consequences that vulnerabilities can have on the organization.

Vulnerabilities can have a range of consequences, including financial losses, operational disruptions, regulatory non-compliance, damage to reputation, and legal implications. Understanding these consequences enables organizations to quantify the potential impact and make informed decisions regarding risk mitigation strategies.

**3. Assessing the Risk to the Business:**

Introduction: Assessing the risk to the business involves evaluating the likelihood and potential impact of vulnerabilities on critical business functions and assets.This process is essential for effective risk management and enables organizations to make informed decisions regarding risk mitigation strategies.

By assessing the risk, organizations can prioritize their resources and efforts to address vulnerabilities that pose the highest risk. This assessment considers factors such as the likelihood of exploitation, the potential impact on business operations, and the existing controls and safeguards in place.

By conducting a thorough analysis of the potential business impact of each vulnerability and understanding the potential consequences, organizations can make informed decisions about the allocation of resources and the implementation of controls and safeguards. This assessment provides valuable insights for designing targeted security awareness training programs and prioritizing mitigation efforts to protect the organization's critical assets and functions.

**Vulnerability Path and Parameter Identification**

**Introduction**:

Identifying vulnerability paths and parameters is crucial for understanding how attackers can exploit weaknesses in systems and applications. By recognizing these paths and parameters, organizations can effectively implement preventive measures and educate employees on secure coding practices. This section explores various methods, types, tools, best practices, and challenges associated with vulnerability path and parameter identification.

**1. Methods for Identifying Vulnerability Paths and Parameters:**

Introduction: Identifying vulnerability paths and parameters requires a systematic approach to analyze systems, applications, and code to uncover potential entry points and data inputs that could be exploited by attackers.

Different methods can be employed, such as manual code review, dynamic analysis, static analysis, and penetration testing. These methods help identify the flow of data and the entry points where vulnerabilities may exist.

**2. Types of Vulnerability Paths and Parameters:**

Introduction: Vulnerability paths and parameters can manifest in different forms, depending on the nature of the application and the type of vulnerability being targeted.

Common types of vulnerability paths include input validation, authentication, authorization, session management, and data storage. Understanding these types helps organizations identify the specific areas where vulnerabilities may be present and develop appropriate countermeasures.

**3. Common Tools and Techniques for Identifying Vulnerability Paths and Parameters:**

Introduction: Several tools and techniques are available to assist in identifying vulnerability paths and parameters within systems and applications.

Tools such as static code analyzers, vulnerability scanners, and web application security scanners can automate the identification process and provide insights into potential vulnerabilities. Additionally, manual techniques, including manual code review and penetration testing, offer a deeper understanding of application vulnerabilities.

**4. Best Practices for Vulnerability Path and Parameter Identification:**

Introduction: Following best practices in vulnerability path and parameter identification ensures a thorough and effective analysis of systems and applications.

Best practices include conducting regular security assessments, adopting a layered defense approach, leveraging automated scanning tools, involving security experts, and fostering a culture of security awareness and collaboration within the organization.

**5. Challenges and Limitations of Vulnerability Path and Parameter Identification:**

Introduction: Vulnerability path and parameter identification may come with challenges and limitations that organizations need to consider.

Challenges may include complex application architectures, obfuscated code, limited access to source code, false positives/negatives from automated tools, and the need for skilled personnel. Recognizing these challenges allows organizations to develop strategies to overcome them and improve the effectiveness of vulnerability identification processes.

By utilizing appropriate methods, understanding different vulnerability path and parameter types, leveraging tools and techniques, following best practices, and addressing challenges, organizations can enhance their vulnerability identification efforts. This, in turn, enables the development of targeted security awareness training programs and the implementation of necessary security controls to safeguard systems and applications from potential exploits.

**Detailed Instruction for Vulnerability Reproduction**

**Introduction:**

Providing detailed instructions for vulnerability reproduction is essential for effective communication between security researchers and developers. Clear and comprehensive instructions help ensure that vulnerabilities are accurately understood and can be properly addressed. This section focuses on the importance of detailed instructions, the components of well-written instructions, steps for reproducing vulnerabilities, best practices for writing effective instructions, tools and techniques for verifying fixes, as well as the challenges and limitations associated with vulnerability reproduction instructions.

**1. Importance of Providing Detailed Instructions:**

Introduction: Detailed instructions play a crucial role in conveying the necessary information for security researchers and developers to understand and address vulnerabilities accurately.

Clear instructions provide a consistent and reproducible approach, allowing for thorough analysis and validation of vulnerabilities. They help minimize misinterpretation and facilitate effective collaboration between security researchers and developers, leading to timely and successful resolution of identified vulnerabilities.

**2. Components of a Well-Written Vulnerability Reproduction Instruction:**

Introduction: Well-written vulnerability reproduction instructions should include specific components to ensure clarity and accuracy in the vulnerability identification and resolution process.

Components may include a concise vulnerability description, system configuration details, prerequisite conditions, step-by-step instructions for reproducing the vulnerability, expected and observed behaviors, sample code or data inputs, and any additional supporting information.

**3. Steps for Reproducing Vulnerabilities:**

Introduction: Reproducing vulnerabilities involves recreating the conditions and actions that lead to the vulnerability's discovery.

Step-by-step instructions should be provided, outlining the necessary setup, test environment configuration, inputs, interactions, and expected outcomes to reproduce the vulnerability consistently. This systematic approach helps security researchers and developers validate the reported vulnerability and analyze its root cause.

**4. Best Practices for Writing Effective Vulnerability Reproduction Instructions:**

Introduction: Writing effective vulnerability reproduction instructions requires adherence to certain best practices to ensure clarity, accuracy, and reproducibility.

Best practices may include using a standardized template, providing clear and concise language, using screenshots or illustrations to enhance understanding, including all relevant information and dependencies, and organizing the instructions logically.

**5. Tools and Techniques for Verifying Vulnerability Fixes:**

Introduction: Verifying vulnerability fixes is an important step in the vulnerability resolution process, ensuring that the identified vulnerabilities have been properly addressed.

Tools and techniques such as code review, security testing frameworks, penetration testing, and automated vulnerability scanners can assist in verifying the effectiveness of fixes. These tools and techniques aid in detecting any residual vulnerabilities or potential regressions.

**6. Challenges and Limitations of Vulnerability Reproduction Instructions:**

Vulnerability reproduction instructions may face challenges and limitations that can impact their effectiveness.

Challenges may include complex system configurations, dependencies on specific environments or data, inadequate information provided by the reporter, limited access to source code, or differences in testing environments. Addressing these challenges requires clear communication and collaboration between security researchers and developers.

By providing detailed instructions, including the necessary components, following best practices, and utilizing appropriate tools and techniques, organizations can facilitate accurate vulnerability reproduction, validation of fixes, and effective resolution. This promotes a collaborative and efficient approach to vulnerability management, ultimately strengthening the overall security posture of the organization.