

**CASE STUDY: Ethical hacking using  
penetration testing tool – INVICTI**

**A REPORT**

*Submitted by*

**JACOB KEVIN P [RA2111030010161]**

*Under the Guidance of*

**Dr. D. Deepika**  
Assistant Professor

**DEPARTMENT OF NETWORKING AND COMMUNICATIONS**

*In partial satisfaction of the requirements for the degree of*

**BACHELOR OF TECHNOLOGY  
In  
COMPUTER SCIENCE ENGINEERING  
with specialization in Information Technology**



**SCHOOL OF COMPUTING  
COLLEGE OF ENGINEERING AND TECHNOLOGY  
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**

**KATTANKULATHUR - 603203**

**MAY 2024**

**DEPARTMENT OF NETWORKING AND COMMUNICATIONS  
SCHOOL OF COMPUTING**

**College of Engineering and Technology  
SRM Institute of Science and Technology**



**SRM**  
INSTITUTE OF SCIENCE & TECHNOLOGY  
Deemed to be University u/s 3 of UGC Act, 1956

COLLEGE OF ENGINEERING & TECHNOLOGY  
SRM INSTITUTE OF SCIENCE & TECHNOLOGY  
S.R.M. NAGAR, KATTANKULATHUR – 603203

## **BONAFIDE CERTIFICATE**

Certified that this project report **“Ethical hacking using penetration testing tool - INVICTI”** is the bonafide work of **“JACOB KEVIN P”** of III Year/VI Sem B. Tech (CSE) who carried out the mini project work under my supervision for the course 18CSE386T PENETRATION TESTING AND VULNERABILITY ASSESSMENT in SRM Institute of Science and Technology during the academic year 2023-2024 (Even sem).

SIGNATURE

Dr. D. Deepika

Assistant Professor

Networking and Communications

SIGNATURE

Dr. Annapurani Panaiyappan K

Professor and Head

Networking and Communications

## CASE STUDY ON “Ethical hacking using penetration testing tool - INVICTI”

EVEN Semester (2023-2024)

**Course Code & Course Name :** 18CSE386T – Penetration Testing and Vulnerability Assessment

**Year & Semester :** III/VI

**Report Title :** Ethical hacking using penetration testing tool INVICTI

**Course Faculty :** Dr. D. Deepika

**Student Name :** (RA2111030010161) Jacob Kevin P

### Evaluation:

S.No	Parameter	Marks
1	Problem Investigation & Methodology Used	
2	Tool used for investigation	
3	Demo of investigation	
4	Uploaded in GitHub?	
5	Viva	
6	Report	
	<b>Total</b>	

**Date :**

**Staff Name :**

**Signature :**

## TABLE OF CONTENTS

<b>Sl. No</b>	<b>TITLE</b>	<b>Page No</b>
1	Introduction	5
2	Scope and objective	6
3	About the tool and the application chosen	8
4	Tool installation procedure	12
5	Steps of ethical hacking using the tool	14
6	Screenshots of the implementation	16
7	Conclusion	19
8	References	20

# INTRODUCTION

In an era dominated by digital transactions and online interactions, web applications serve as the cornerstone of modern business operations. From e-commerce platforms to banking portals, these applications facilitate seamless communication, streamline transactions, and enhance user experiences. However, the widespread adoption of web applications has also exposed organizations to a myriad of cybersecurity threats, ranging from SQL injection attacks to cross-site scripting vulnerabilities.

In the face of these evolving threats, cybersecurity professionals are tasked with the formidable challenge of safeguarding web applications against malicious actors while preserving the integrity of sensitive data. To address this challenge, organizations must adopt proactive security measures, including regular penetration testing, to identify and mitigate vulnerabilities before they can be exploited.

This case study embarks on a journey to fortify the security posture of a fictitious e-commerce web application known as "ShopifyX" using Invicti, a leading penetration testing tool. By subjecting ShopifyX to rigorous security assessments, we aim to uncover potential vulnerabilities, assess their impact, and implement robust remediation strategies to fortify the application's defences.

Through a meticulous examination of Invicti's capabilities and methodologies, this case study illuminates the pivotal role of penetration testing in strengthening web application security. By harnessing the power of Invicti's advanced scanning engines, automated vulnerability detection, and comprehensive reporting functionalities, organizations can proactively identify and address security weaknesses, thereby mitigating the risk of data breaches, preserving user trust, and safeguarding their digital assets in an increasingly hostile cybersecurity landscape.

## SCOPE AND OBJECTIVE

### Scope:

The scope of this penetration testing exercise using Invicti spans across the entire web application ecosystem of ShopifyX, encompassing its frontend and backend components, third-party integrations, APIs, and underlying infrastructure. The assessment will include but not be limited to:

1. Web Application Layer: Comprehensive scanning of the web application's frontend interfaces, including login pages, product catalogs, shopping carts, and checkout processes, to identify vulnerabilities such as input validation flaws, session management issues, and insecure communication protocols.
2. Backend Infrastructure: Examination of the backend components, database servers, and application servers to detect vulnerabilities such as SQL injection, remote code execution, and directory traversal attacks that could compromise the confidentiality and integrity of sensitive data.
3. Third-Party Integrations: Assessment of third-party plugins, libraries, and APIs utilized by the web application to identify potential security risks, including vulnerabilities in third-party code, insecure API endpoints, and data leakage risks arising from integration points.
4. Authentication Mechanisms: Evaluation of authentication mechanisms implemented within the web application, including user authentication, session management, and password policies, to identify weaknesses such as weak password storage, session fixation, and authentication bypass vulnerabilities.
5. Authorization Controls: Assessment of access control mechanisms to ensure that users are granted appropriate privileges based on their roles and responsibilities, identifying authorization bypasses, privilege escalation vulnerabilities, and insecure direct object references.
6. Data Storage and Transmission: Examination of data storage practices, encryption mechanisms, and data transmission protocols to identify risks related to data confidentiality and integrity, including insecure storage of sensitive information, plaintext transmission of credentials, and inadequate encryption practices.

7. Infrastructure Configuration: Review of the underlying infrastructure configuration, including network architecture, firewalls, and server hardening measures, to identify misconfigurations and vulnerabilities that could expose the web application to external threats.

### **Objective:**

The primary objectives of this penetration testing engagement using Invicti are as follows:

1. Identify Vulnerabilities: Conduct a comprehensive assessment of the ShopifyX web application to identify security vulnerabilities, including but not limited to SQL injection, cross-site scripting (XSS), authentication flaws, and insecure configurations.
2. Assess Security Posture: Evaluate the effectiveness of existing security controls and mechanisms implemented within the web application, including authentication, authorization, encryption, and logging, to identify weaknesses and areas for improvement.
3. Prioritize Risks: Prioritize identified vulnerabilities based on their severity, impact, and exploitability, providing actionable insights to help the organization focus its remediation efforts on addressing the most critical security risks first.
4. Validate Findings: Perform manual validation of identified vulnerabilities to confirm their presence and assess their exploitability, ensuring the accuracy and reliability of the assessment results.
5. Provide Remediation Recommendations: Generate detailed reports outlining identified vulnerabilities, their severity levels, and recommended remediation steps, tailored to the organization's specific requirements and constraints, to facilitate the implementation of effective security controls and measures.
6. Enhance Security Awareness: Raise awareness among stakeholders, including developers, system administrators, and management, about the importance of web application security and the potential risks posed by identified vulnerabilities, fostering a culture of security awareness and proactive risk mitigation within the organization.

By defining a comprehensive scope and clear objectives for the penetration testing engagement, organizations can leverage Invicti to conduct thorough assessments, prioritize remediation efforts, and enhance the overall security posture of their web applications.

## ABOUT THE TOOL AND THE APPLICATION CHOSEN

### **Tool - Invicti:**

Invicti is a cutting-edge web application security solution designed to identify and mitigate vulnerabilities in web applications, helping organizations enhance their cybersecurity posture and protect sensitive data from potential threats. Powered by advanced scanning engines and comprehensive security testing methodologies, Invicti offers a wide range of features to facilitate thorough vulnerability assessments and ensure the integrity and resilience of web applications.

#### Key features of Invicti include:

1. Automated Vulnerability Scanning: Invicti employs automated scanning techniques to thoroughly analyze web applications and identify a wide range of security vulnerabilities, including SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms, among others.
2. Advanced Scanning Engines: Leveraging advanced scanning engines and heuristic analysis techniques, Invicti can detect complex vulnerabilities and security misconfigurations that may evade traditional security testing methods, ensuring comprehensive coverage of potential threats.
3. Customizable Scanning Policies: Invicti offers customizable scanning policies and configurations, allowing organizations to tailor the scanning process to their specific requirements and priorities, ensuring efficient and targeted vulnerability assessments.
4. Actionable Reporting: Invicti generates detailed reports outlining identified vulnerabilities, their severity levels, and recommended remediation steps in a clear and concise format, enabling organizations to prioritize and address security issues effectively.
5. Integration Capabilities: Invicti seamlessly integrates with existing security infrastructure and workflows, enabling organizations to incorporate vulnerability scanning into their DevOps pipelines, continuous integration/continuous deployment (CI/CD) processes, and security incident response procedures.



## **Application - ShopifyX:**

ShopifyX is a fictitious e-commerce web application designed to showcase the functionalities and features commonly found in online retail platforms. As a leading provider of e-commerce solutions, ShopifyX offers a user-friendly interface, robust product management capabilities, secure payment processing, and seamless shopping experiences for customers.

### Key components and functionalities of ShopifyX include:

1. User Authentication: ShopifyX incorporates secure user authentication mechanisms, allowing customers to create accounts, log in securely, and manage their profiles and preferences.
2. Product Catalog: The application features a comprehensive product catalog with detailed descriptions, images, and pricing information, enabling customers to browse and search for products effortlessly.
3. Shopping Cart: ShopifyX includes a shopping cart functionality that allows customers to add products to their cart, review their selections, and proceed to checkout seamlessly.
4. Checkout Process: The checkout process in ShopifyX is streamlined and intuitive, guiding customers through the steps of entering shipping and payment information, applying discounts or promotional codes, and completing their purchases securely.
5. Payment Processing: ShopifyX integrates with secure payment gateways to facilitate payment processing, ensuring the confidentiality and integrity of customer payment information during transactions.

By leveraging Invicti's advanced scanning capabilities and methodologies, organizations can conduct thorough assessments of the ShopifyX web application, identify potential vulnerabilities, and implement proactive measures to strengthen its security posture and protect customer data from cyber threats.

## **Advantages of Invicti:**

1. Comprehensive Vulnerability Detection: Invicti employs advanced scanning engines to comprehensively identify a wide range of vulnerabilities in web applications, including common issues like SQL injection, cross-site scripting (XSS), and security misconfigurations.
2. Automated Scanning: Invicti's automated scanning capabilities enable organizations to conduct regular and thorough vulnerability assessments without the need for manual intervention, saving time and resources.
3. Customizable Scanning Policies: Invicti offers customizable scanning policies, allowing organizations to tailor the scanning process to their specific requirements and priorities, ensuring efficient and targeted vulnerability assessments.
4. Actionable Reporting: Invicti generates detailed reports outlining identified vulnerabilities, their severity levels, and recommended remediation steps in a clear and concise format, enabling organizations to prioritize and address security issues effectively.
5. Integration Capabilities: Invicti seamlessly integrates with existing security infrastructure and workflows, enabling organizations to incorporate vulnerability scanning into their DevOps pipelines, continuous integration/continuous deployment (CI/CD) processes, and security incident response procedures.
6. Continuous Monitoring: Invicti supports continuous monitoring of web applications, allowing organizations to detect and address newly emerging vulnerabilities in real-time, thereby enhancing the overall security posture of their applications.

### **Disadvantages of Invicti:**

1. Cost: Invicti may be cost-prohibitive for smaller organizations or those with limited budgets, as it is a premium solution that may require significant investment.
2. Complexity: Invicti's advanced features and capabilities may be complex for novice users to navigate, requiring specialized training and expertise to maximize its effectiveness.
3. False Positives: Like any automated scanning tool, Invicti may occasionally generate false positive results, requiring manual verification and validation to distinguish genuine vulnerabilities from false alarms.
4. Limited Coverage: While Invicti offers comprehensive scanning capabilities, it may not detect all possible vulnerabilities or security weaknesses in a web application, necessitating supplementary manual testing and assessment.
5. Dependency on Updates: Invicti's effectiveness relies on regular updates and maintenance to ensure compatibility with the latest web application technologies and emerging security threats, requiring ongoing investment and support from the vendor.

## TOOL INSTALLATION PROCEDURE

Installing Invicti involves a few steps to ensure proper setup and configuration. Below is a detailed installation procedure:

a. Download Invicti: Visit the official website of Invicti and navigate to the download section. Choose the appropriate version of Invicti based on your operating system (Windows, Linux, or macOS). Click on the download button to initiate the download process.

b. Extract the Installation Package: Once the download is complete, locate the downloaded file (usually a compressed archive such as .zip or .tar.gz) and extract its contents to a designated folder on your system.

c. Installation Wizard: Navigate to the extracted folder and locate the installation executable file (e.g., setup.exe for Windows). Double-click on the executable file to launch the installation wizard.

d. Accept License Agreement: The installation wizard will prompt you to review and accept the license agreement. Carefully read the terms and conditions, and if you agree, select the option to accept the agreement.

e. Choose Installation Directory: Specify the directory where you want to install Invicti. You can either choose the default installation directory or select a custom location based on your preferences. Click "Next" to proceed.

f. Select Components: Invicti may offer the option to select additional components or features during the installation process. Choose the components you wish to install, such as plugins or additional tools, and click "Next" to continue.

g. Configure Settings: Depending on your requirements, the installation wizard may prompt you to configure certain settings such as proxy settings or update preferences. Adjust these settings according to your preferences and click "Next" to proceed.

h. Start Installation: Once you have reviewed and confirmed all the installation settings, click on the "Install" or "Start Installation" button to begin the installation process.

i. Wait for Completion: The installation process may take some time to complete, depending on your system specifications and the selected components. Allow the installation wizard to proceed, and wait until the process is finished.

j. Activation: After the installation is complete, you may need to activate your Invicti license. Follow the on-screen instructions to activate your license using the provided activation key or license file.

k. Finish Installation: Once activation is successful, the installation wizard will notify you that the installation is complete. Click on the "Finish" button to exit the installation wizard.

## STEPS OF ETHICAL HACKING USING THE TOOL

a. **Scoping and Reconnaissance:** The initial phase of any ethical hacking engagement involves scoping the project and gathering reconnaissance data. This includes identifying the target application, understanding its architecture, functionality, and technology stack, and delineating the boundaries within which the assessment will be conducted. Thorough reconnaissance ensures that the testing efforts are focused and aligned with the goals of the organization.

b. **Configuration and Setup:** Once the scope is defined, configuring Invicti is the next crucial step. This involves setting up the scanning parameters, authentication mechanisms (if required), and customizing scan policies to meet the specific needs of the application and the organization. Configuration also includes selecting the appropriate scanning depth, crawl settings, and attack verification options to ensure a comprehensive assessment.

c. **Initiate Scan:** With the configuration completed, Invicti is ready to begin the scanning process. Initiating the scan involves launching the tool and pointing it towards the target URL of the application. Invicti systematically crawls the application, mapping out its structure, identifying entry points, and probing for vulnerabilities across various components such as web forms, URLs, and parameters.

d. **Analysis of Scan Results:** As Invicti progresses through the scanning process, it generates detailed reports containing a wealth of information about the vulnerabilities discovered within the application. Analysts meticulously analyze these scan results, categorizing vulnerabilities based on severity levels (e.g., critical, high, medium, low) and prioritizing them for remediation based on their potential impact on the security of the application.

e. **Validation and Exploitation:** Validating the existence and exploitability of identified vulnerabilities is a critical step in the ethical hacking process. Invicti provides tools and functionalities to simulate attacks and exploit vulnerabilities, allowing testers to confirm their presence and assess their potential impact on the application's security posture. Techniques such as SQL injection, cross-site scripting (XSS), and others are employed to validate vulnerabilities and demonstrate their exploitability.

f. **Manual Verification and Validation:** While Invicti automates much of the scanning and vulnerability identification process, manual verification is essential to ensure the accuracy and reliability of the findings. Ethical hackers may employ

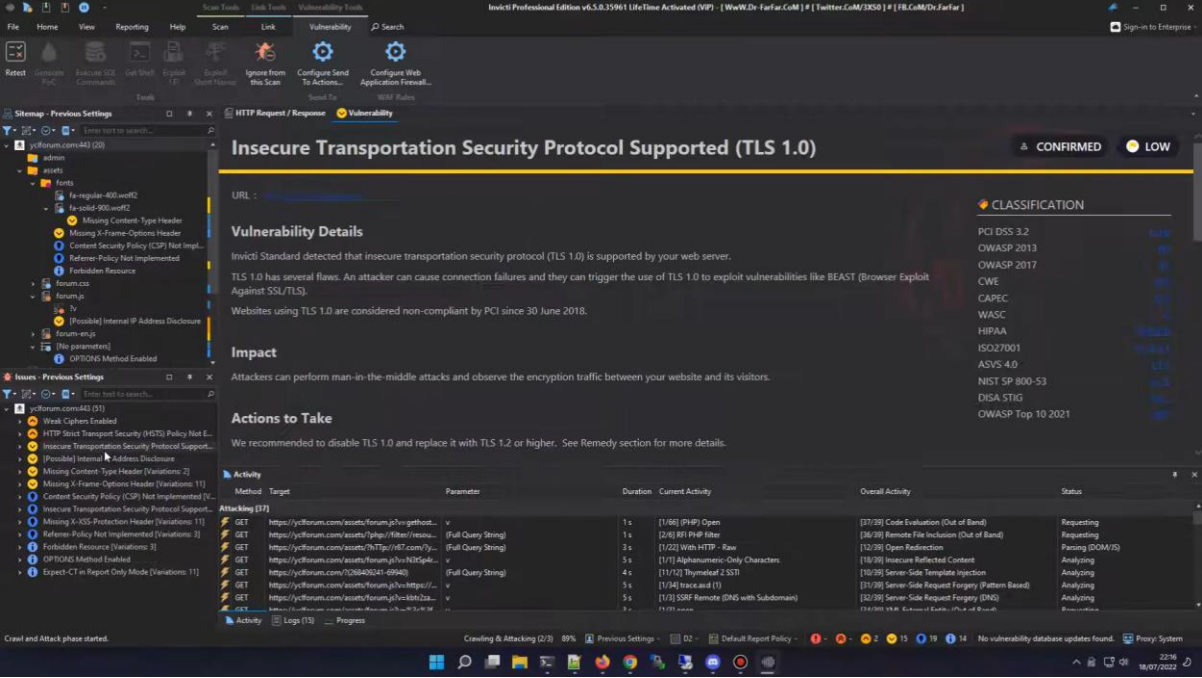
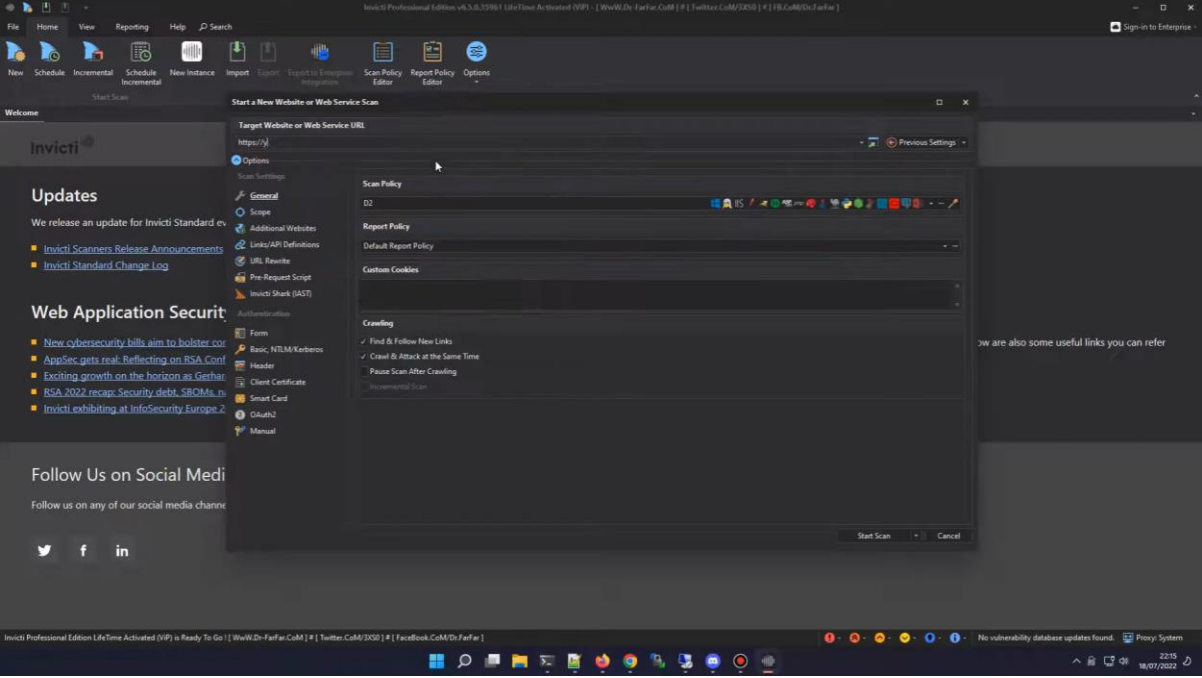
additional manual testing techniques and tools to further validate identified vulnerabilities, explore potential attack vectors, and assess the real-world impact on the application's security.

g. **Documentation and Reporting:** Once the testing phase is complete, compiling a comprehensive report is paramount. The report documents the findings of the penetration test, including details of the vulnerabilities discovered, their severity levels, potential impact on the application, and actionable recommendations for remediation. The report serves as a valuable resource for stakeholders, providing insights into the security posture of the application and guiding decision-making regarding security enhancements.

h. **Post-Testing Activities:** Following the completion of the penetration test, ethical hackers engage in post-testing activities to ensure that the findings are appropriately addressed and remediated. This may involve debriefing sessions with stakeholders to discuss the results, prioritizing and implementing remediation efforts, and conducting follow-up assessments to validate the effectiveness of the security controls implemented. Additionally, lessons learned from the testing process are documented and incorporated into future security assessments to continually improve the organization's security posture.

By meticulously following these steps and leveraging the capabilities of Invicti, ethical hackers can conduct thorough penetration tests, identify vulnerabilities, and help organizations strengthen their defences against cyber threats effectively.

## SCREENSHOTS OF THE IMPLEMENTATION







File Home View Reporting Help Scan Link Vulnerability Search

New Schedule Incremental Schedule Incremental New Instance Import Export Export to Invicti Enterprise Scan Policy Editor Report Policy Editor Options


Start Scan Scan Session Tools

Sitemap - Previous Settings

Controlled Scan

Vulnerability Browser View Knowledge Base Viewer

[Possible] Source Code Disclosure (ColdFusion) MEDIUM

Certainty : 

URL : <https://www.quora.com/search?q=../../../../../../../../../../proc/version%00.php>

CLASSIFICATION

OWASP 2013 A5

OWASP 2017 A3

CWE 540

Issues - Previous Settings

www.quora.com:443 (201)

[Probable] Local File Inclusion

Weak Ciphers Enabled

[Possible] Source Code Disclosure (ColdFusion)

[Possible] Source Code Disclosure (Generic)

[Possible] Source Code Disclosure (PHP)

Activity

Method	Target	P...	Duration	C...
GET	https...	oid	2 s	[2...
GET	https...	n...	2 s	[8...
GET	https...	s...	1 s	[7...
GET	https...	oid	1 s	[4...
GET	https...	s...	1 s	[2...
GET	https...	t...	4 s	[1...

Attacking [6]

Passive Analysis [1]

File Home View Reporting Help Scan Link Vulnerability Search Sign-in to Enterprise

New Schedule Incremental Schedule Incremental New Instance Import Export Export to Invicti Enterprise Scan Policy Editor Report Policy Editor Options

Start Scan Scan Session Tools

Sitemap - Previous Settings

Controlled Scan

HTTP Request / Response Vulnerability Knowledge Base Viewer

Weak Ciphers Enabled MEDIUM CONFIRMED

URL : <https://www.quora.com/>

List of Supported Weak Ciphers :

- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x000A)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002F)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xC013)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xC014)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x003C)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003D)

Activity

Method	Target	Duration
GET	https...	1 s
GET	https...	1 s
GET	https...	3 s
GET	https...	1 s
GET	https...	1 s
GET	https...	1 s

Attacking [7]

Progress

Auto save finished successfully - 12/5/2022 12:15:00 AM

Crawling and Attacking (2/3) - 40%

Previous Settings

AIIO5-AllWebServer-AllAppServer-Microsoft SQL Server-MySQL-Oracle-PostgreSQL-MongoDB-Other

Knowledge Base (20)

AJAX / XML HTTP Requests [35]

Comments [1]

Cookies [500]

Crawling Performance [13]

Email Addresses [9]

External CSS Files [1]

External Frames [3]

External Scripts [13]

File Extensions [4]

Form Validation Errors [8]

Interesting Headers [4]

JavaScript Files [1]

MIME Types [10]

Not Found [161]

Out of Scope Links [500]

Scan Performance [53]

Site Profile [1]

Slowest Pages [10]

SSL [1]

URL Rewrite [4]

Activate Windows

Knowledge Base (20)

Invicti Assistant (3)

## CONCLUSION

In conclusion, the utilization of Invicti for penetration testing has demonstrated its efficacy in enhancing the security posture of the target application. Through meticulous scoping, comprehensive configuration, and systematic scanning, Invicti efficiently identified vulnerabilities ranging from common weaknesses to critical security flaws. The detailed analysis of scan results facilitated the prioritization of remediation efforts, enabling organizations to address the most severe threats first.

Furthermore, the validation and exploitation of identified vulnerabilities underscored the importance of thorough testing in uncovering potential attack vectors and assessing their impact on the application's security. Invicti's capabilities, coupled with manual verification and validation, ensured the accuracy and reliability of the findings, providing stakeholders with actionable insights to mitigate risks effectively.

The documentation and reporting phase encapsulated the findings of the penetration test, offering stakeholders a comprehensive overview of the security posture of the application. The actionable recommendations outlined in the report serve as a roadmap for improving security controls and mitigating vulnerabilities, thereby bolstering the overall resilience of the organization against cyber threats.

Post-testing activities, including debriefing sessions, remediation efforts, and continuous improvement initiatives, underscore the iterative nature of security testing and the commitment to ongoing enhancement of security practices. By leveraging the insights gleaned from the penetration test and incorporating lessons learned into future assessments, organizations can proactively mitigate emerging threats and adapt to evolving cybersecurity challenges.

In essence, Invicti's role in the penetration testing process extends beyond mere vulnerability identification; it serves as a catalyst for organizational resilience, driving informed decision-making, and fostering a culture of proactive security. By embracing Invicti as a cornerstone of their security strategy, organizations can fortify their defences, safeguard critical assets, and mitigate the ever-present threat of cyber-attacks.

## REFERENCES

1. <https://www.invicti.com/learn/>
2. <https://www.invicti.com/support/invicti-quick-start-guide/>
3. <https://www.appsecsanta.com/invicti>
4. <https://www.invicti.com/case-studies/>
5. <https://www.prnewswire.com/news-releases/new-invicti-research-reveals-proof-based-scanning-automatically-confirms-94-of-direct-impact-vulnerabilities-with-99-98-accuracy-301385889.html>