Information Network Security Administration (INSA)

WEB APPLICATION TESTIN REQURMENT

Greetings! Dear [Client's Name],

As you are well aware, INSA assumes a paramount role in upholding the national-level cyber security landscape by conducting comprehensive cyber security audits, evaluations. Our expertise extends to meticulously assessing the security of web applications, APIs, internal web portals, in-house developed applications and systems, mobile applications, and IT infrastructures at both the national and company levels. INSA empowers organizations to enhance their cyber security posture, mitigating risks and safeguarding critical information from malicious actors. Partnering with INSA ensures that your digital ecosystem remains resilient, secure, and prepared for the dynamic cyber security landscape of today and tomorrow. To facilitate the security audit you **should** provide all the necessary documents and information

- Updated Trade License
- Tin Number
- System/product Patent writing or certificate

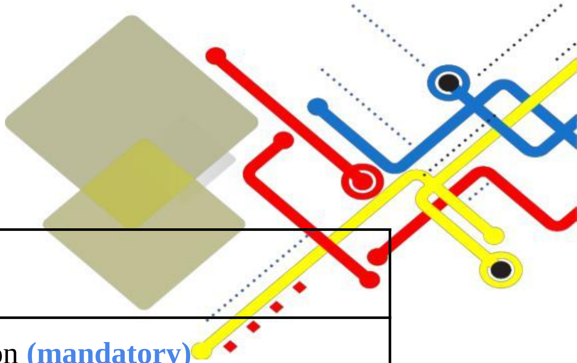
For our technical team to conduct a thorough assessment We request that you gather these materials on a CD and deliver them to our office located at Wollo Sefer. Alternatively, you may also mail them to the address provided below:

Note! You should be reply requirement within five days (5)

Mr . Tilahun Ejigu (ph.d candidate)
Cyber Security Audit Division Head@INSA
Bsc computer science, MSc.(Computer Science) &
BA(Business Management)
Mail: tilahune@insa.gov.et , Mobile: +251937456374

Required information's/Documents for Web application

Web Application Documentation: - this document should contain at least the following core points.



1. **Business Architecture and Design**	
Business Architecture and Design	you should provide this information **(mandatory)**
Data Flow Diagram	
System Architecture Diagram	

2. **Features of the web application**	
Features of the web application	you should provide this information **(mandatory)**
Development frameworks	
libraries (plugins)	
third-party integrations	
any custom development	
Actor/user type	
Dependencies, system minimum requirements	

Implemented security standards	
Are there any devices in place that may impact the results of a penetration test such as a firewall, intrusion detection/prevention system, web application firewall, or load balancer?	

3. Define the specific scope clearly and precisely like this table (Mandatory)

Name of the Assets to be Audit	URL/IP	Test Account as required by the tester
public web portal/sites		
Internal web portal		
Internal local Applications		
public Applications		

4. Security functionality document:

sample security Functionality	How has that security Functionality has been implemented?
User Roles and Access Control	
Authorization Mechanisms	
Input Validation and Sanitization	
Session Management	
Error Handling and Logging	

Secure Communications	

5. Secure coding standard document (if there)	
sample coding rule/guidelines used	List possible secure coding practice you have used?
OWASP Secure Coding Practices	
Secure Input Handling	
Secure File Handling	
Authentication and Session Management	
Software Patching and Updates	
Review Third-Party Components	
Secure Communication	

6. Previous security test report document: - if it is tested before. (If it is applicable).	
Previous security test report document	List possible secure coding practice you have used?
First phase security testing doc	
Re-audit security testing doc	

7. Your Contact information and communication channel

Name	Role	Address (mail and Mobile)

Note!! The document contained

1. cover page and correct company name
2. Background of organization
3. Introduction
4. Objective of this certificate requested
5. Conclusion