Local Hosted Web Server http://172.21.35.221/EARS/
Security Audit Report

Date 21/12/016 e.c

Warning

This report contains confidential and privileged information about the security status of **172.21.35.221/EARS/** cyber security management. The information is intended for the private use of **172.21.35.221/EARS/** Access to this information by unauthorized personnel may allow them to compromise your information technology infrastructure or it could be used as a resource to attackers for further attacking analysis. Therefore, INSA recommends keep this information confidential and do not distribute it without the consent or written approval.

This evaluation reveals all relevant vulnerabilities known up to the date of this report and the capability of our testing team. As new vulnerabilities and new security threats emerge daily, it is suggested that the security assessment to be conducted regularly.

Table 1

Company	172.21.35.221/EARS/
Document title	172.21.35.221/EARS/
Date	20/12/2016
Ref. number	
Classification	
Document Type	Report

Table 2

Author	Administration	Date
Cyber Security Audit and Evaluation Division	INSA	20/12/2016

Contact

For more information about this report and its contents please use the following contact details

Organization	**Information Network Security administrator (INSA)**
Division	Cyber Security Audit and Evaluation Division
Contact Person Name	Yetsedaw Getnet
Phone	+251 920028562

Contents

Acronyms

Terminology	Definition
HTTP	Hypertext Transfer Protocol
INSA	Information Network Security Administrator
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
MIME	Multipurpose Internet Mail Extensions
OWASP	Open Web Application Security Project
SMB	Server Message Block

SECTION 1

I.1. Executive Summary

Information Network Security administrator has performed vulnerability assessment and penetration testing on the http://172.21.35.221/EARS/ website. INSA has conducted the security assessment in a manner that simulated malicious actors engaged in an attack against of the http://172.21.35.221/EARS/ website by using different security vulnerability technical tools and best practices and measured the overall security status of the http://172.21.35.221/EARS/

This report contains the details of the vulnerability assessment and penetration testing result along with suggested remedial solutions. The result shows that the application has different vulnerabilities that can expose the http://172.21.35.221/EARS/ website to different threats. These security vulnerabilities can be categorized as follows:

- Poor usage of security Policy,
- Poor security control,

Therefore, http://172.21.35.221/EARS/ should give a serious attention and be committed to manage the security vulnerabilities listed here in the report. Otherwise, the organization may be exposed to different damages. Please note that the solutions recommended here can serve as a starting point to remediate the security weaknesses. Nevertheless, that does not replace researching further by the administrators to provide a better solution.

Summary of findings

Types of Vulnerabilities	Level of Risks			
	HIGH	MEDIUM	LOW	TOTAL
Authentication by pass	✔			
Cleartext submission of password	✔			
Session Cookie Persistence Post-Logout			✔	
Frameable response (potential Clickjacking)			✔	
TOTAL	2		2	4

I.2. **Project Objective**

The main objective of this vulnerability assessment and penetration testing is to identify potential security vulnerabilities for the sake of learning cyber-security and provide technical, managerial, physical and human related recommendations to remediate them.

I.3. **Project scope**

The scope of this security audit is the portal of http://172.21.35.221/EARS/

I.4. Existing security controls

The existing security controls and technologies used on the web application.

Technologies: most technologies are latest and up to date. These products have moderate probability to be exploited by attackers.

Eaglelion Dome Ethiopian System use the following strong security measurement to protect sensitive business data in the event of a hardware malfunction, hacker penetration, and many other threats posed to digitally stored information.

- Root detection

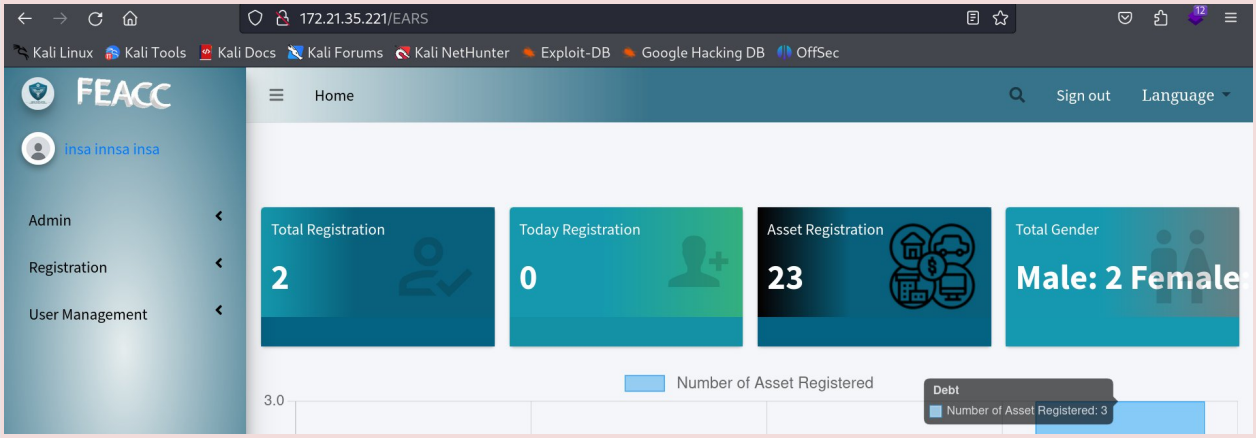
SECTION 2

2.1. Detailed Security Audit Findings

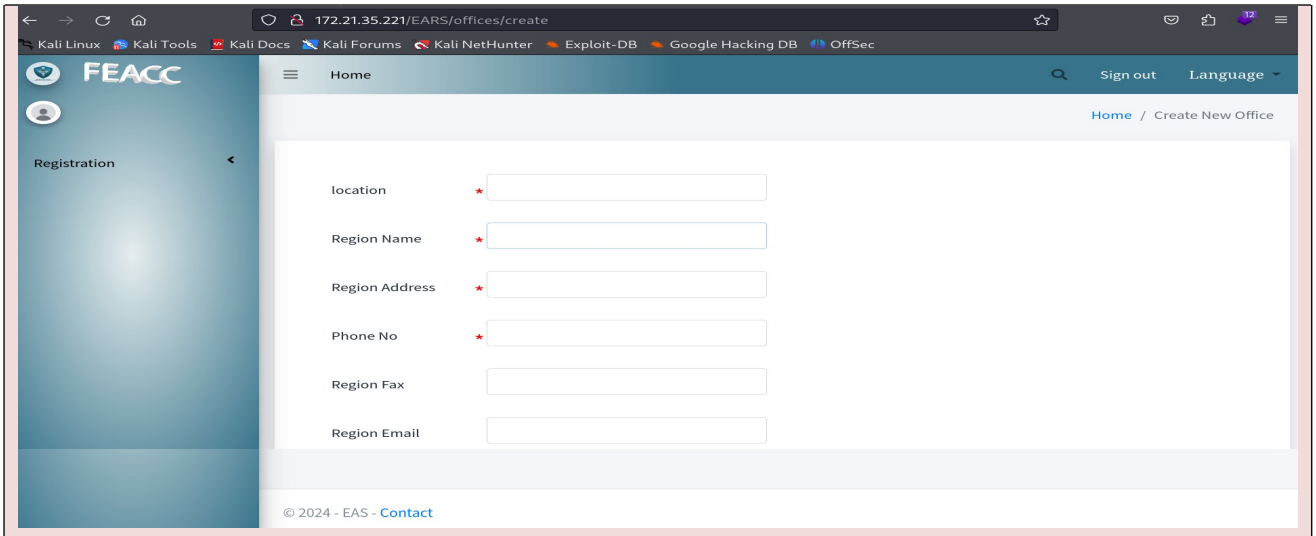
The following tables show the details of the vulnerabilities identified during the security assessment process.

No.	1
Vulnerability Name	Session Cookie Persistence Post-Logout
Target	http://172.21.35.221/EARS/
Vulnerability Description	The session cookie associated with Laravel users remains in the browser even after logging out. This persistence may allow an attacker to hijack the session by using the still-active session cookie, leading to unauthorized access.
Risk Level	Medium
Impact	An attacker could potentially gain access to a user's account after logout, leading to unauthorized actions, data theft, or other malicious activities within the application.
Countermeasure	Ensure the session cookie is securely invalidated and removed from the browser upon logout. Implement additional measures like setting a short expiration time for session cookies and utilizing secure and HttpOnly flags to enhance session security.

Evidence:



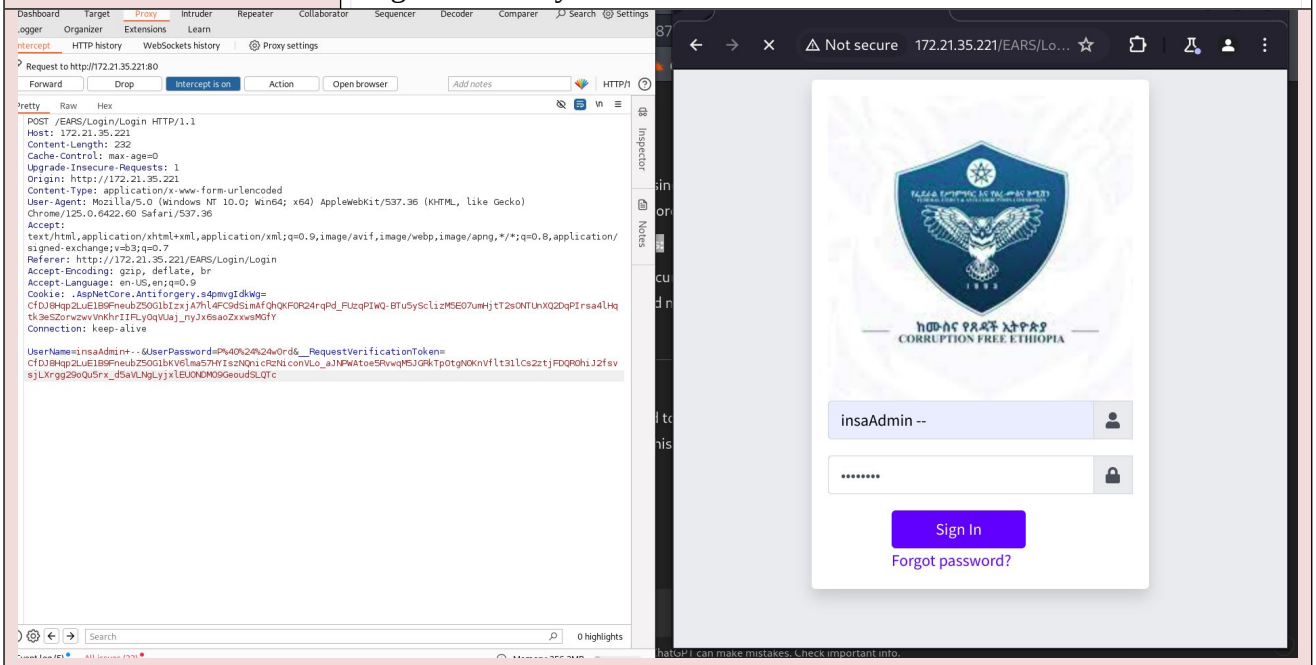
No.	2
Vulnerability Name	Authentication by pass
Target	http://172.21.35.221/EARS/asset http://172.21.35.221/EARS/assets/index http://172.21.35.221/EARS/roles http://172.21.35.221/EARS/roles/index http://172.21.35.221/EARS/home/privacy http://172.21.35.221/EARS/home/error http://172.21.35.221/EARS/organizations/search http://172.21.35.221/EARS/orgainization/create http://172.21.35.221/EARS/offices/create
Vulnerability Description	Several endpoints within the application hosted on http://172.21.35.221/EARS/ are accessible without requiring user authentication. • This indicates a failure in access control mechanisms, where unauthenticated users can access sensitive areas of the application that should be restricted to authenticated and authorized users.
Risk Level	High
Impact	Information Disclosure: Sensitive data may be exposed to unauthorized users, such as organizational details, roles, and asset information. Data Manipulation: Unauthenticated users could potentially create, modify, or delete organizational or office records, which could lead to data integrity issues. Privilege Escalation: Attackers could exploit these vulnerabilities to gain higher privileges within the application, potentially leading to further exploitation. System Compromise: If any of these endpoints can be leveraged to execute malicious actions, it could result in a complete system compromise.
Countermeasure	Implement Proper Access Controls: Security Testing Patch Management: Input Validation:



Evidence:

No.	3
Vulnerability Name	Cleartext submission of password
Target	http://172.21.35.221/EARS/login/login
Vulnerability Description	During testing, it was discovered that the application hosted on http://172.21.35.221/EARS/transmits user passwords in cleartext over the network. This means that when users enter their credentials, the application sends the password in an unencrypted format. This issue was observed during the login process and possibly in other areas where password submission is required
Risk Level	high

Impact	**Eavesdropping:** Attackers on the same network can intercept the cleartext passwords as they are transmitted, allowing them to gain unauthorized access to user accounts. **Account Compromise:** Once an attacker obtains a password through interception, they can use it to log in as the legitimate user, leading to account compromise and potential misuse of the user's privileges. **Data Breach:** If an attacker gains access to multiple user credentials, it could lead to a large-scale data breach, especially if users reuse passwords across different services. **Reputation Damage:** The discovery of such a vulnerability can severely damage the organization's reputation, as users lose trust in the security of the application.
Countermeasure	Enforce HTTPS: Use Strong Encryption Protocols: Secure Coding Practices: Password Hashing: Regular Security Audits:



Evidence:

No.	4
Vulnerability Name	Frameable response (potential Clickjacking)
Target	http://172.21.35.221
Vulnerability Description	The website hosted at http://172.21.35.221/ does not implement proper defenses against clickjacking attacks. It allows its content to be embedded in iframes, which can be exploited to trick users into performing unintended actions on the site.
Risk Level	low
Impact	An attacker can craft a malicious website that embeds the target site within an invisible iframe, tricking users into interacting with the embedded site without their knowledge. This could lead to: • Unauthorized actions being performed on behalf of the user. • Disclosure of sensitive information if combined with other social engineering attacks.
Countermeasure	Implement X-Frame-Options: Use Content Security Policy (CSP): Regular Security Audits:
Evidence:	

SECTION 3

3.1. Conclusion

We conclude that the overall security of the http://172.21.35.221/EARS/ needs improvement. We hope that the issues mentioned in this report will be addressed quickly as soon as possible by the responsible body.

Experience has shown that a focused effort to address the problems outlined in this report can result in dramatic security improvements. For systems to remain secure, however, security posture must be evaluated and improved continuously, Assigning the responsible person or establishing the organizational structure that will support these ongoing improvements is essential in order to maintain control of information systems.

SECTION 4

4.1. Appendix

4.1.1. Audit Report Format

The result of the security test is organized in a table format, which has the following rows:

No.	
Target	These are assets like <target> that has been evaluated.
Vulnerability	A weakness on the asset that could expose the organization to a security threat.
Vulnerability Description	It is a clarification of the identified vulnerability/weakness. The reason why the vulnerability exists is described here.
Risk Level	This describes the opportunity the vulnerability opens to the attacker. The risk levels are classified as **High**, **Medium** and **low**
Impact	This is to describe a damage that will be happened if the vulnerabilities identified are exploited by a malicious party
Countermeasure	This describes the technical, managerial, physical and human related recommendations to mitigate potential risks.
Evidence: This is a screenshot taken to prove that the vulnerability exists.	

4.1.2. Applied Methodology

To conduct the penetration testing, we used many methodologies. Some methodologies used to test the application are mentioned below:

- following up Application security checklist
- following up OWASP testing guide
- Application security testing tools

4.1.3. Risk Calculation

Throughout the document, each risk calculated has been listed in a table under section 3 as a finding and categorized as a **High-Risk**, **Medium-Risk**, or **Low-Risk**. INSA used the following Risk calculation formula to calculate the risks.

Risk= Likelihood*impact

High risk: - these findings identify conditions that could directly result in the compromise of the web application. These include getting access to the website by resetting user accounts of different user levels i.e. normal user up to administrator user level. This will allow an attacker to perform tasks on administrator user level.

Medium risk: - these findings identify conditions that do not immediately or directly result in the compromise but do provide a capability to gain control on the web application. These includes the session cookie does not expire after the users click on log out. These will allow attackers to login and perform tasks using the cookie once they steal it from legitimate user.

Low risk: - these findings identify conditions that provide information that could be used in combination with other information to gain insight into how to compromise the web application. These include vulnerabilities like information disclosure and displaying server banners.