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

Date 16/12/016 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, we 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	Phone number	Date
Mekdelawit Bogale	+251935648535	22/08/2024

Contents

Acronyms

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

SECTION 1

I.1. Overview

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,
- Poor server configuration

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.

1.2 Summary of findings

Types of Vulnerabilities	Level of Risks			
	HIGH	MEDIUM	LOW	TOTAL
Insecure Transmission of Credentials	✔			
Authentication by pass	✔			
Cross site-scripting(XSS)		✔		
Frameable response (potential Clickjacking)			✔	
Session Cookie Persistence Post-Logout			✔	
TOTAL	2	1	2	5

1.3 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.

1.4 Project scope

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

1.5 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.

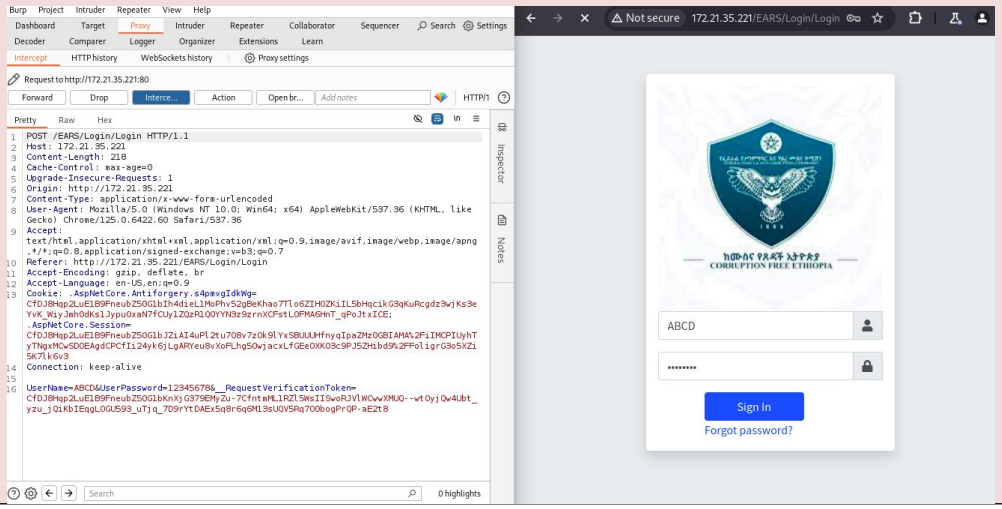
Eaglelion Dome Ethiopian System use the following strong security measurement to protect sensitive business data in the event of a hardware malfunction, hacker penetration, and many other threats posed to digitally stored information.

- Root detection

SECTION 2

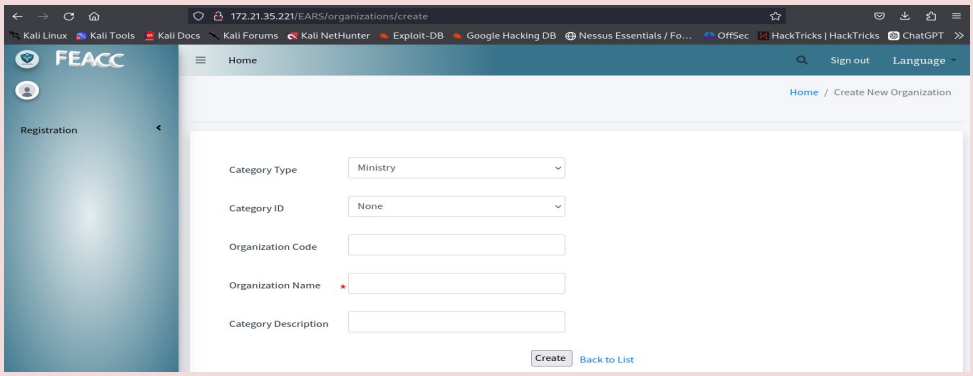
2.1. Detailed Security Audit Findings

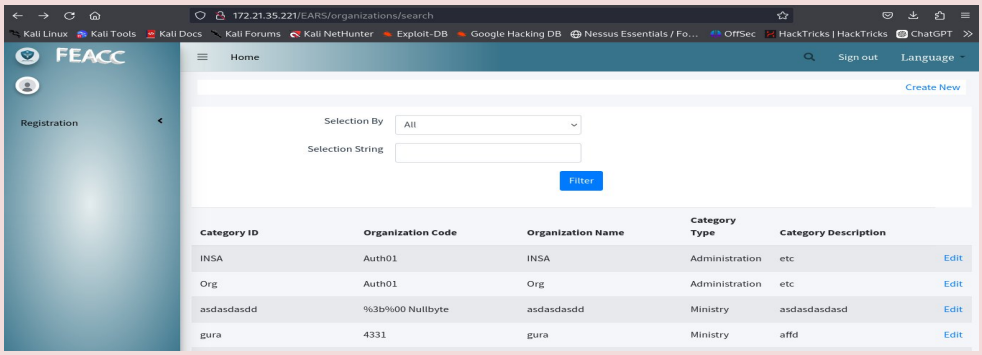
The following tables show the details of the vulnerabilities identified during the security assessment process.

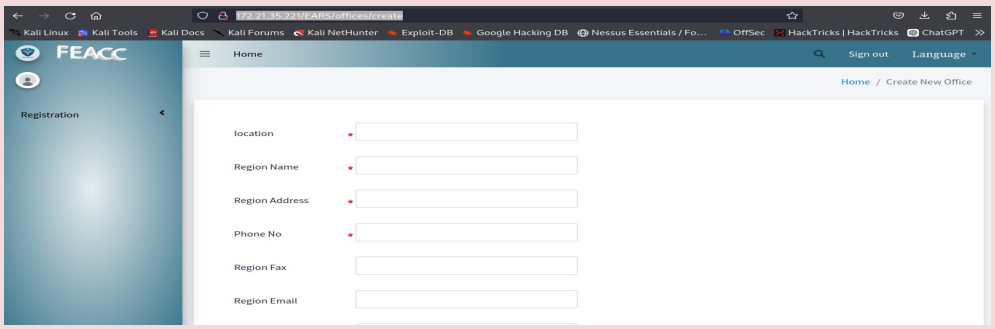
No.	1
Vulnerability Name	Insecure Transmission of Credentials
Target	http://172.21.35.221/EARS/login/login
Vulnerability Description	The target http://172.21.35.221/EARS/login/logintransmits user passwords in cleartext over the network. This vulnerability occurs when sensitive information, such as passwords, is transmitted over a network in plain text without encryption.
Risk Level	High
Impact	Exposing passwords in cleartext during transmission can lead to unauthorized access, account compromise, and potential data breaches.
Countermeasure	Using HTTPS to ensure that data is encrypted during transmission. By Implement HSTS to force the use of HTTPS and prevent users from downgrading to an insecure connection. Using Strong Encryption Protocols
Evidence: 	

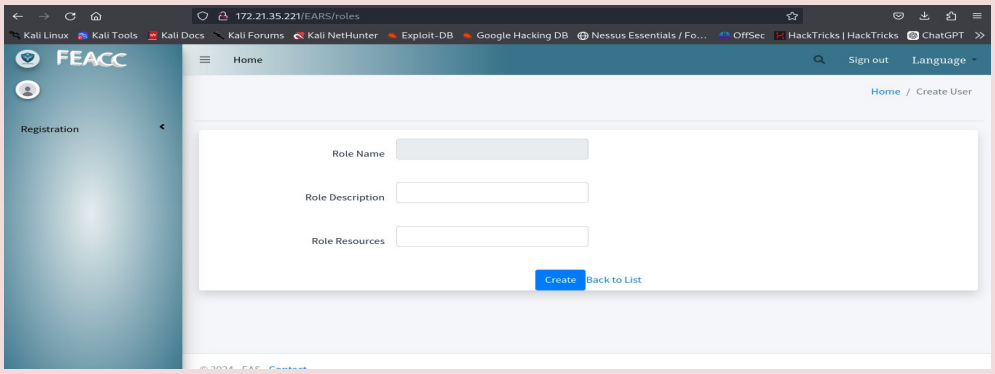
No.	2
Vulnerability Name	Authentication by pass
Target	http://172.21.35.221/EARS/ http://172.21.35.221/EARS/assets/index http://172.21.35.221/EARS/roles http://172.21.35.221/EARS/roles/index http://172.21.35.221/EARS/home/privacy http://172.21.35.221/EARS/home/error http://172.21.35.221/EARS/organizations/search 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/login/login can be 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	Sensitive data is exposed to unauthorized users, such as organizational details, roles, and asset information. Unauthenticated users could potentially create, modify, or delete organizational or office records, which could lead to data integrity issues. System Compromise: If any of these endpoints can be leveraged to execute malicious actions, it could result in a complete system compromise.
Countermeasure	Implementing strong Authentication Mechanism Secure Session Management Patch Management Input Validation

Evidence:

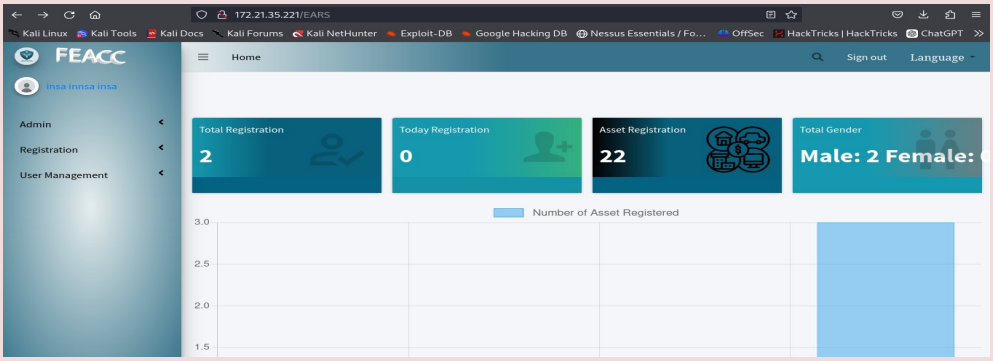

172.21.35.221/EARS/organizations/create
FEACC
Home
Sign out
Language
Registration
Home / Create New Organization
Category Type
Ministry
Category ID
None
Organization Code
Organization Name
Category Description
Create
Back to List


172.21.35.221/EARS/organizations/search
FEACC
Home
Sign out
Language
Registration
Create New
Selection By
All
Selection String
Filter
Category ID
Organization Code
Organization Name
Category Type
Category Description
INSA
Auth01
INSA
Administration
etc
Edit
Org
Auth01
Org
Administration
etc
Edit
asdasdasdd
%3b%00 Nullbyte
asdasdasdd
Ministry
asdasdasdasd
Edit
gura
4331
gura
Ministry
affd
Edit


172.21.35.221/EARS/offices/create
FEACC
Home
Sign out
Language
Registration
Home / Create New Office
location
Region Name
Region Address
Phone No
Region Fax
Region Email


172.21.35.221/EARS/roles
FEACC
Home
Sign out
Language
Registration
Home / Create User
Role Name
Role Description
Role Resources
Create
Back to List

No.	3
Vulnerability Name	Frameable response (potential Clickjacking)
Target	http://172.21.35.221/EARS/
Vulnerability Description	The website hosted at http://172.21.35.221/EARS/ 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	This could lead to: Unauthorized actions being performed on behalf of the user. and also Disclosure of sensitive information if combined with other social engineering attacks.
Countermeasure	Implementing X-Frame-Options , Use Content Security Policy (CSP) and also Regular Security Audits
Evidence: 	

No.	4
Vulnerability Name	Session Cookie Persistence Post-Logout
Target	http://172.21.35.221/EARS/
Vulnerability Description	The server might not be correctly invalidating the session on logout, meaning the session ID stored in the cookie remains valid.
Risk Level	low
Impact	The user might remain looged into sensitive accounts if the session persists,even after they've attempted to logout. And if malicious actor gains access to a persistent session cookie, they could use it to impersonate the user.
Countermeasure	Setting cookies with appropriate expiration time and ensure they are deleted upon logout. Force session invalidation using secure cookies
Evidence: 	

No.	5
Vulnerability Name	Cross site-scripting(XSS)
Target	http://172.21.35.221/EARS/
Vulnerability Description	Used to bypass access controls, such as the same-origin policy
Risk Level	Medium
Impact	Can steal session cookies and hijack users sessions and also used to phish users by displaying fake login forms. Can modify the content displayed on the affected website
Countermeasure	Input validation and sanitization and ensure that being output to the browser is properly escaped, especially when inserting into other code context.
Evidence:	

SECTION 3

3.1.Conclusion

I can conclude that the overall security of the http://172.21.35.221/EARS/ needs improvement. I hope that the issues I mentioned in this report will be addressed.

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:

4.1.2. Applied Methodology

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

- following up OWASP testing guide
- Application security testing tools

4.1.1. 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**.

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.