Security

EliteSecurityConsultants

Penetration Test Report

December 21st, 2019

Executive Summary

The main aim of the penetration test is to make sure that the login system is safe and secure from Cyber criminals. I performed a series of tests on the login page using various attack vectors and found out the following listed issues. The issues have been classified as **High,Low,Critical**,

Summary of Results

During the test, I came to find the following issues

1. **Strict Transport Security not enforced**

Severity: low

Issue Detail

7 instances of this issue were identified, at the following locations:

- /login
- /vendor/css/bootstrap.css
- /vendor/fonts/fontawesome.css
- /vendor/fonts/ionicons.css
- /vendor/fonts/linearicons.css
- /vendor/fonts/open-iconic.css
- /vendor/fonts/pe-icon-7-stroke.css

Issue Background

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

Issue Remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

2. **Password Field with autocomplete enabled**

   Issue: Low but certain

   <u>Issue detail</u>

2 instances of this issue were identified, at the following locations:

- /login
- /register

Issue Background

Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.

<u>Issue Remediation</u>

To prevent browsers from storing credentials entered into HTML forms, include the attribute **autocomplete="off"** within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields).

3. **XSS Vulnerability**

   After trying a number of xss attacks, the attacks failed. A sign that the login page is bulletproof to xss attacks

4. **SQL Injection**

   SQL injection attacks failed. Page safe.

5. **Live Host Header Injection.**

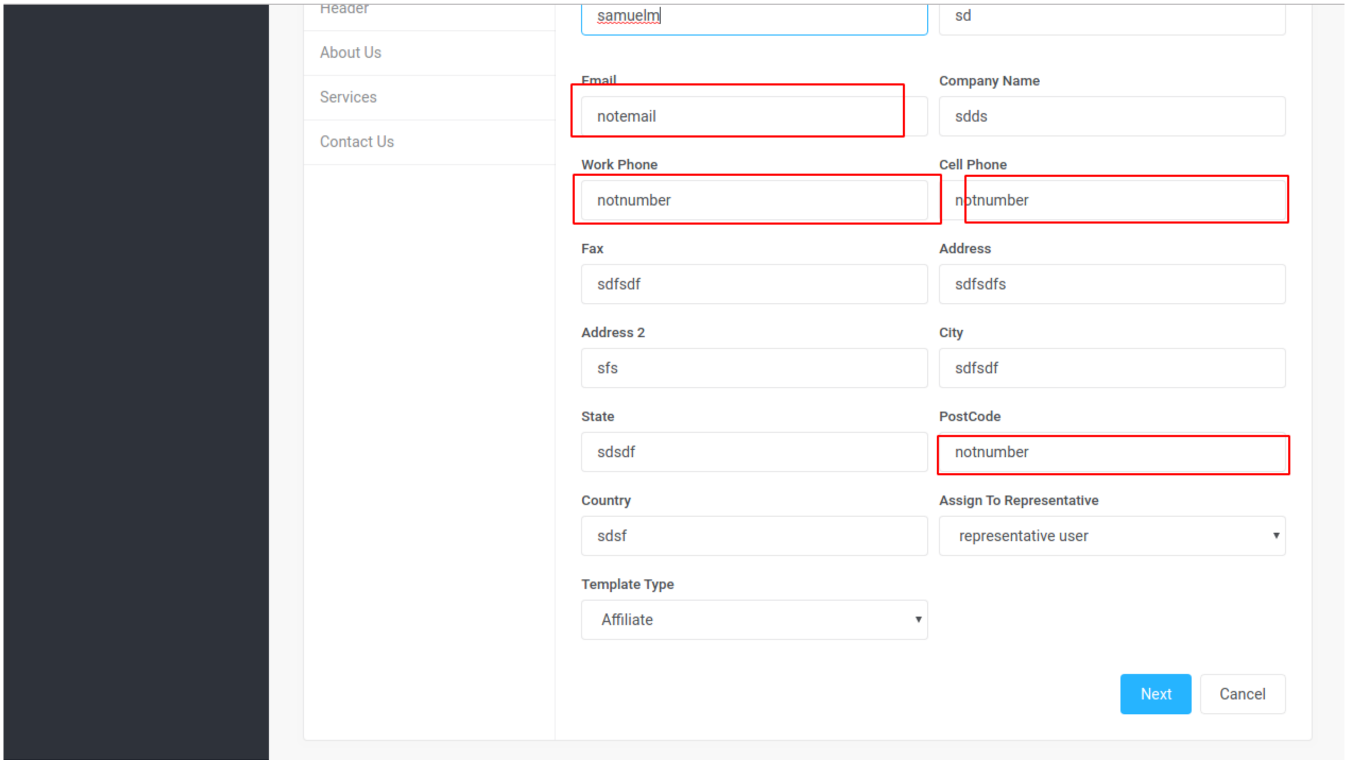
   The login page is also safe to live host header injection

The System

The aim of the pentest was to determine if the system is safe. However, the system code reviews shows a properly folllowed code convention using Object Oriented Paradigm in Php. The project is developed using Laravel, a popular and a secure web development application framework.Laravel handles and blocks any illegal character input by the user since it was designed to with a security aspect in mind. However, there were some few issues with validations though the levels were low.

- Poor Validations

The developer never did validations to form inputs. Eg. The email field should let one input email only. Below is a screenshot of the fields that were to be validated.



samuelm
sd

Email: notemail
Company Name: sdds
Work Phone: notnumber
Cell Phone: notnumber
Fax: sdfsdf
Address: sdfsdfs
Address 2: sfs
City: sdfsdf
State: sdsdf
PostCode: notnumber
Country: sdsf
Assign To Representative: representative user
Template Type: Affiliate

Otherwise, all the other aspects of the applications and the server were secure.

- I would like to recommend that you update and upgrade your virtual machine since with some recon methodologies, I was able to determine that it runs on an ubuntu server running apache 2.4.29 Which has some security flaws.Please follow the above recommendation and your infrastructure will be secure.

Thanks