ePLDT
Web Builder

ePLDT Web Builder Security

March 2017

TABLE OF CONTENTS

OVERVIEW

ePLDT Web Builder is a robust platform and the websites populated on the platform are accessed on a daily basis by many thousands of visitors on a daily basis, therefore, system security is a major part of the solution reliability, and is well tested in the real world on a daily basis.

ePLDT Web Builder maintains website data which is edited by site designers and site owners and is being served to the public. ePLDT Web Builder data does not include sensitive data such as credit card information.

The ePLDT application is deployed on top of the robust and secure cloud infrastructure.

This document provides a description of the security elements included in the ePLDT eclipse product.

- Chapter 1: Describes the ePLDT application security elements.
- Chapter 2: Describes the ePLDT infrastructure and network security elements.

APPLICATION SECURITY

Security Elements

The main building blocks of the ePLDT application security are:

User & Role Management

The application includes Strict User, Role Management enabling separate authorization rules for users such as Administrators, Site Owners, Web Designers and end users

User / Reseller Hierarchy Management

The application supports the management of a hierarchy of resellers. This feature allows multiple resellers to work on the same instance without being able to access each other's data.

User Authentication on access to protected assets and services

The system authenticates users according to the credentials they provide when registering into the system or according to credentials provided by a fulfillment team member. The system requires the user to enter a strong password.

Admin application protection

The administration Application is accessed over HTTPS. Access to this application can be limited to a specific IP address reducing the risk of intrusion into sensitive administration functionality.

Editor application protection

The Editor Application is accessed over HTTPS.

Spam Prevention protected by CAPTCHA mechanism

The application supports online forms which are vulnerable for spamming in order to prevent spamming the system provides both captcha mechanism provisioning and a minimum time limit – both used to identify machines trying to post a form.

Web Service Protection

The application provides a set of web services for integration with external systems. The Web Services can only be accessed from an approved IP address.

Protection against web site SQL Injection scenarios

The application prevents users from injecting SQL. The system uses only strong parameter binding and rejects any SQL as input.

Protection against web site Cross Site Scripting XSS scenarios

The system filters out any attempt to enter dangerous scripts and characters.

Password encryption

The system encrypts user passwords in the database using a one direction encryption. Passwords can't be restored or recovered. The system allows users to change their password in case it is lost.

File Upload Validation

Uploaded files are validated against a list of allowed types. The system will not allow users to upload dangerous file types such as server side scripts.

SSL

The admin and editor web-application are running over HTTPS to ensure encrypt communication between the client and our servers on any administrative and site editing operations.

INFRASTRUCTURE AND NETWORK SECURITY

Security Elements

The main building blocks of the ePLDT infrastructure and network security are:

Cloud Infrastructure Security

The ePLDT application is deployed on top of the cloud infrastructure. ePLDT operates the cloud infrastructure that you use to provision a variety of basic computing resources such as processing and storage. The cloud infrastructure includes the facilities, network, and hardware as well as some operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of these resources. The cloud infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards. ePLDT customers can be sure their web solution is built on top of some of the most secure computing infrastructure in the world.

The IT infrastructure that Cloud Infrastructure Security provides to its customers is designed and managed in alignment with best security practices and a variety of IT security standards, including:

Firewall

The application servers are grouped under a security group which is protected by a firewall. The firewall allows access through well-defined ports and protocols. The firewall is setup to allow users access on HTTP port 80 and HTTPS port 443.

The firewall is setup to allow administrators access on SSH port 22 on a specific ePLDT client IP address.

SSH Private Key protection

ePLDT administrators use SSH to manage the application servers on Cloud. SSH access is protected by private key security. This level of security assures that only ePLDT administrators can access the application servers for maintenance.

Robot attack prevention

Access and Error logs are regularly scanned for robot attempts. Robots are identified both manually and automatically and unauthorized robot clients IPs are blocked regularly.

Malicious HTTP Requests prevention

HTTP requests are always checked for well-known malicious URLs. These requests are rejected automatically by the system using pre-defined rewrite rules.

Hardening

The system components (such as PHP and Apache) are hardened to assure most updated security patches are deployed and unnecessary modules are removed.