Criptografía y seguridad

TRABAJO PRÁCTICO ESPECIAL

Los 25 errores de Software más frecuentes

Alan Pomerantz

Juan José Marinelli

Agustin Marseillan

1. Abstract

En el presente informe se expone la investigación de cuatro de los veinticinco errores presentes en el software más frecuentes, dentro del ámbito informático. Se procede a introducir el tema que contempla a dichos errores, y luego se brinda una descripción técnica del error, junto a ejemplos de código, métodos de detección, niveles de vulnerabilidad y consecuencias sobre un posible exploit sobre dicho error, y por último, formas de mitigar dichos errores. Los errores seleccionados fueron el 2 (dos) “Improper Neutralization of Special Elements used in an OS command (‘OS Command Injection’), 7 (siete) “Use of Hard-coded Credentials” , 12 (doce) “Cross-Site Request Forgery (CSRF)” y 17 (diecisiete) “Incorrect Permission Assignment for Critical Resource”.

1. Introducciòn

Existe una lista ordenada bajo un ranking, conteniendo los errores más frecuentes dentro del ámbito informático, de los que uno como programador debe tener cuidado de no generar, ya que un atacante puede sacar provecho de la situación, generando escenarios no deseables dentro del flujo general dentro de un programa. La lista se puede online encontrar en la siguiente direccion: *http://cwe.mitre.org/top25/* [[1]](#footnote-1)

El presente informe selecciona 4 de estos 25 errores más frecuentes y propone un análisis detallado del mismo.

1. Errores seleccionados
   1. OS Command Injection
      1. Descripción del error
      2. Detalles técnicos del error
      3. Ejemplos de código
      4. Métodos de detección
      5. Nivel de vulnerabilidad y consecuencias posibles de un exploit sobre ese error
      6. Formas de mitigar y/o evitar el error
   2. Use of Hard-Coded Credentials
      1. Descripción del error
      2. Detalles técnicos del error
      3. Ejemplos de código
      4. Métodos de detección
      5. Nivel de vulnerabilidad y consecuencias posibles de un exploit sobre ese error
      6. Formas de mitigar y/o evitar el error
   3. Cross-Site Request Forgery (CSRF)
      1. Descripción del error
      2. Detalles técnicos del error
      3. Ejemplos de código
      4. Métodos de detección
      5. Nivel de vulnerabilidad y consecuencias posibles de un exploit sobre ese error
      6. Formas de mitigar y/o evitar el error
   4. Incorrect Permission Assigment for Critical Resource
      1. Descripción del error
      2. Detalles técnicos del error
      3. Ejemplos de código
      4. Métodos de detección
      5. Nivel de vulnerabilidad y consecuencias posibles de un exploit sobre ese error
      6. Formas de mitigar y/o evitar el error

1. Sitio web perteneciente a la CWE (Community Weakness Enumeration) [↑](#footnote-ref-1)