Network Security

Project 2

Web Vulnerability, Frequency Analysis, Hash Collision

Instructor: Shiuhpyng Shieh

TA: Wei-Ti Su & Xin-Yu Wang

1. Project Description

In this project, you need to hack Bob's personal blog, and find his intimate picture. You could visit Bob's blog at http://140.113.194.66:xxxxx/blog/. There are some posts and information about Bob, and you may also find some interesting posts related to this project.

2. Project Guide

In this paragraph, we provide some useful terms and skills which are highly related to this project.

a) robots.txt: We use robots.txt to inform the search engine crawlers or robots about which files or path of the website should not be scanned or accessed.

b) Temporary files: Sometimes, the temporary file may leak some important information to the intruders.

c) Frequency analysis: Some weak encryption algorithm can be broken by using frequency analysis.

d) Hash collision: If we can find an input ***x*** for a given hash function ***h*** and hash digest ***d***, such that ***h***(***x***) = ***d***, it's called hash collision.

e) MySQL: MySQL is a very famous SQL database. Bob uses MySQL as the backend database system for his blog.

f) PHP: PHP is a popular general-purpose scripting language that is especially suited to web development. Fast, flexible and pragmatic, PHP powers everything from your blog to the most popular websites in the world. --- PHP Official Website

3. Deliverables

Each student must work individually and submit a .zip file, named by "<YOUR_STUDENT_ID>.zip", for example "0656001.zip", containing:

a) Any source code or program you used in your project. (For online tool, please provide the URL of the online tool.)

b) The intimate picture you found after you hack into Bob's blog. (Right click the image and save the original image as a single file. No compression or quality lost is allowed!)

c) A report, contains

- The steps and details of your hacking. (Briefly explain the concept and idea.)
- What have you learned?
- How to prevent or patch these vulnerabilities?

Any anomaly connection such as DDoS will be traced for punishment.
Deadline : 2018/05/01(Tuesday) 23:59:59