Security Analysis of “No Captcha reCaptcha”

Setup-Guide

Please follow the below mentioned instructions to execute the experiment. Also in the last section details about the results and logs are mentioned.

The CNS_Project Folder Contains:

/Attacker: This folder contains chrome extension (Attacker-EXT) for the adversary. Attacker.py Script to be executed at the adversary’s machine. Also it contains chrome extension which disables the Referer header (RefererDisable-EXT)

/Client: This folder contains chrome extension (Client-EXT) for the Victims. ClientSide.py Script to be executed at the victim’s machine.

/Database: This folder contains the file recaptcha.sql which needs to imported in the MySQL database.

/Server: Contains the netbeans JAVA project.

1. How to configure Server and Database
    a. Install Xampp server and start Apache and MySQL services from Xampp control panel
    b. Create a database named recaptcha in phpMyAdmin and import the recaptcha.sql file to load database given in the database folder.
    c. Download and install NetBeans with JAVA EE bundles and glass fish server from https://netbeans.org/downloads/
    d. Open the project named Captcha from the server folder in NetBeans.
    e. Run the server by clicking run button.
    f. Server is deployed on your IP address with port no 8080.
    g. Login on the google reCAPTCHA admin with given test username and password to add your IP Address on the listed domain for cnstest.com.

2. How to configure Victim
    a. Edit variable ‘serverURL’ in ClientSide.py and background.js (in Client-EXT) with URL of your server.
    b. Pack the Client-EXT using Pack extension option given in chrome extension bar.
    c. Zip the Client folder and move Client.zip file to folder ‘Attacker’.
    d. This Zip file will be send to victim by e-mail using Attacker script with all instructions to install.
3. How to configure Attacker

a. Install Python version 2.7 or above and pip by running get-pip.py
b. Install selenium in python using command pip install selenium in command prompt (pip command can be located in C:/Python27/Scripts folder)
c. Edit Attacker.py file and change the server URL (Example: “http://your_ip_address:8080”), change the variable ‘driverPath’ with location of chrome driver provided in Attacker folder
d. Change the variable ‘serverURL’ in file manager.js in Attacker-Ext folder with the URL of your server.
e. Run Attacker script and give the e-mail of the victims you wished to target.
f. Open chrome browser and select extension from the menu.
g. Select option Load unpacked Extension with developer mode selected.
h. Select Attacker-EXT folder to load extension.

Software requirements

1. NetBeans (with Java EE enabled and glass fish server)
2. Windows (To run Attacker and Server)
3. Ubuntu
4. Python
5. Google Chrome

Test Username1 (For Adversary): gargut1994@gmail.com

Test Password1: recaptcha

Test Username2: gargutk1994@gmail.com

Test Password2: recaptcha

Test Username3: gargutka1994@gmail.com

Test Password3: recaptcha

Result && Logs:

The recaptcha.sql file contains two tables:

1. Cookies: Contain the cookies stolen from the Victims.

2. Registration: Contains the User Entry created after the successful attacks
   Total number of entries in the Cookie Table: 1000
   Total number of entries in the Registration Table: 7
3. Log.txt: Contains logs of all the attempts made to break the captcha code.
   In the logs: 192.168.0.20 is the adversary's IP.
   192.168.0.16, 192.168.0.19 and 192.168.0.10 are the Victim's IP Address.
   Total number of attempts in the logs: 418