One Host To Rule Them All

CTF Challenge Mid Project Report

IT18139440 – H.H.D Kalhara

IT18132410 – A.D.H Jinadasa

Table of Contents

Theme / audience

CTF competitions are a powerful tool not only for the security specialist to train themselves in a possible work-related situation but also for students.

The target audience of this project is for developers who are new to php web application development and new to Laravel framework. The developers can be school students who are studying ICT for Ordinary Level and Advance Level and undergraduates who are following IT related degrees or diplomas.

Therefore, institutes that offer web development courses can use this CTF to educate their students about web security with hands-on experience.

Implementation

Ubuntu 18.04 minimum installation is selected to act as the server in the implementation. The server can be accessed by port 22 (SSH) and port 80 (HTTP). Therefore, SSH and HTTP services are hardened to secure the server. Laravel is installed on top of apache HTTP server to act as framework to the CTF web application.

SSH service is hardened to disable direct root logins, login using empty passwords, deny kerberos authentication, deny GSSAPI authentication, deny challenge response authentication, disable tunneling and forwarding, deny using graphical user interface over SSH, deny setting environment variables and MaxAuthTries and LoginGraceTime is defined to defend against brute force attacks. Connection keep alive time is not defined because users have to spend more time in the CTF box.

Laravel 5.6.29 is installed using composer to act as framework to the CTF web application. Two mysql databases are connected to the web application, one for storing information of users data and progress. Which is secured by laravel functions. And the second database is used from sqli challenge. Which is unsecured.

Apache2 http server is hardened to hide server version info in response header, directory browsing is disabled users cannot browse through directories using web browsers, Etag is disabled to prevent leakage of inode number, multipart MIME boundary, and child process through response header, HTTP request types are limited to GET,POST and HEAD, HTTP 1.0 protocol is disabled, Server side includes are disabled in options and system service protection is added to prevent users from overriding apache settings using htaccess.

Planned CTF Levels

Level > 1

Cryptography challenge part one.

Users get to download zip file containing 3 text files each containing cryptic text messages each encrypted using different methods. Text file number 3 contains the first flag that is required to unlock level 2. Basic cryptanalysis and basic linux skills will be tested.

Level > 2

Cryptography challenge part two.

Once unlocked level 2 users will get another zip file containing 5 encrypted files. Similar to before users have to go to various processes to get the next flag. Some events user have to write a script to decrypt the messages . Basic cryptanalysis, basic Linux skills and scripting knowledge will be tested.

Level > 3

Forensic challenge

Once the level 3 unlocked user will get wireshark data file users have to review and analyze the data packets and by writing a specific filter will disclose the flag to the next level. User will be able to sharpen his/her knowledge about packet analysis.

Level > 4

Social engineering and Brute force

In level 4 there is a login page users have breakin to it in order the get the flag. User can follow the clues provided by the developers. Users can either brute force using common password lists or they can build a possible password list by investigation given hints. User will learn concepts of open source intelligence and get to know PHP authentication methods and vulnerabilities and hacking tools.

Level > 5

SQLi challenge

Users get landed on a new login page. Where users have to inject a sql injection to login to continue the challenge. Once users successfully bypass the login they are taken to a page that shows information about 'outposts' these data is obtained from a different table. Search box is provided to filter data shown in the page. Users have to utilize this search box to pass sql injection code to the database to obtain the flag. Basic sql injection knowledge and relational database knowledge is tested in this challenge.

Level > 6

Session Hijacking

Users are prompted with a "Assess Deny" page. In order to gain access users have to use burpsuite to find their way to gain access.

Level > 7

Steganography challenge

Users are given an image file, the flag is hidden inside the image. The goal is to find the flag using a steganography tool or manually.

Level > 8

PWN challenge

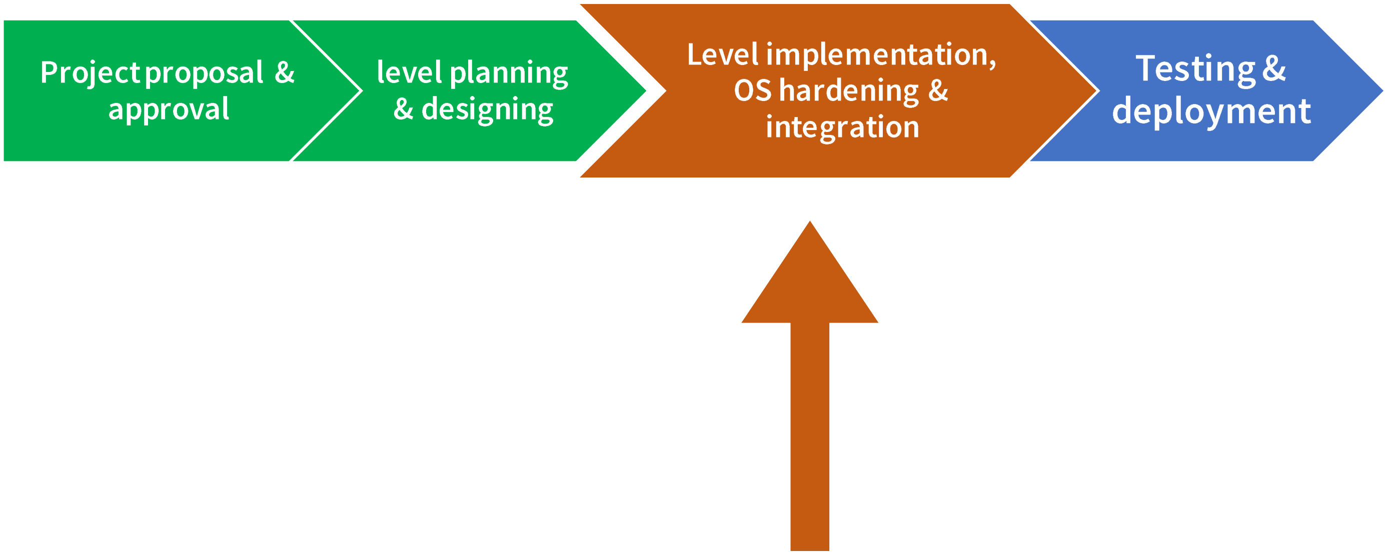
Users are given sftp access to a non privilege account where access is limited. In the sftp directory two files are created. Users have to compare the files and find the hidden flag value inside. This challenge tests knowledge about linux commands.

Level > 9

Reverse engineering challenge

Users are given assembly code once correct value is passed to program flag is revealed users have to reverse engineer the program to identify the correct value.

Current progress



Project proposal & approval

level planning & designing

Level implementation, OS hardening & integration

Testing & deployment

We were able to complete level 1,2, and 4. We are currently working on the OS hardening and Web implementing. We are planning to complete total of five levels by the end of this week.

Video URL: -

https://mysliit.sharepoint.com/:f:/s/CTF2021-Onehosttorootthemall/EtSOu4uDiMxJuN_juhY3uRoBMmS9DGzNV1qkA-HbnCCvPA?e=zgsrsY

GitHub: -

https://github.com/kalhara14/ISP-CTF