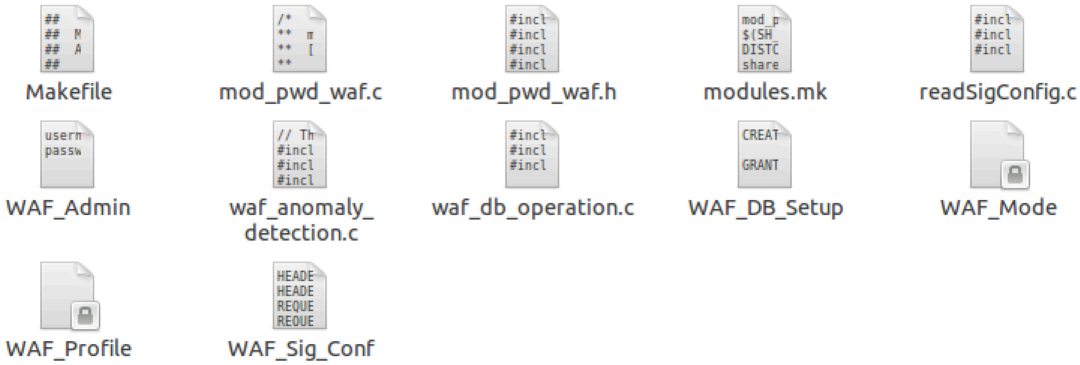
File Description

In this folder , there are four folders:

Waf_Code folder

This folder contains all the code and configuration files for our WAF apache module.

In this folder, there are severl files:



1. mod_pwd_waf.c, mod_pwd_waf.h, readSigConfig.c, waf_anomaly_detection.c, waf_db_operation.c: These files are the source code for our WAF project.

2. WAF_Admin: the administrator username and password required to change between Training and Detection mode. Data Format: first line “user=admin”, second line “password=123”. Change to desired username and password. No space.

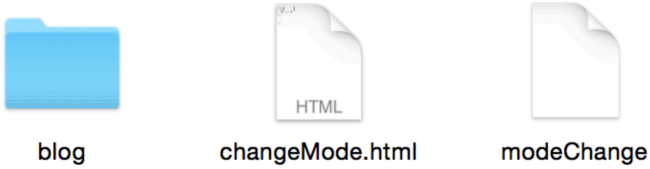
3. WAF_Sig_Conf: Signature file which contains characteristic of maliciousness. Data Format: “REQUEST_METHOD:GET,PARAMETER:*,CONTAINS:”<script>””. One line for each rule. No space except comment part or no empty line in the end.

4. WAF_Profile: generated information for anomaly detection. User should not modify this file.

5. WAF_Mode: store current mode. User should not modify this file.

Web_Application_Code folder

This folder contains all files for our web application. All files in this folder should in the path:/var/www/html



1. blog folder: Contains our Web application blog website. This website is used to test our WAF.

2. changeMode.html and modeChange: These two files are used for change WAF mode.

Data folder

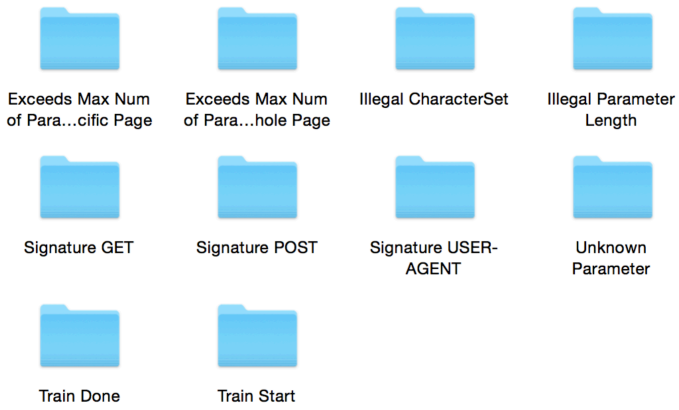
This folder contains all data exported from database.

1. training_data.sql: This file is the data exported form MySQL database, which is the database data we trained our WAF for Anomaly Detection. You can run it in MySQL to show our training records.

2. web_db.sql: This file is the data exported from MySQL database, which is the data for our web application- blog website. You can run it in MySQL to get website records.

TestVideo folder

This folder contains all Flash we recorded for our WAF, you can check all our WAF function by watching the Flash.



1.Exceeds Max Num of Parameter for Specific Page:
Screenshot for the case when number of parameters exceeds the max num of the this specific page.
In our example, '/blog/public/user_main.php' has only one parameter at Training, but now it has two parameters(user_id and u).

2.Exceeds Max Num of Parameter for Whole Page:
Screenshot for the case when number of parameters exceeds the max num of all pages.
In this example, '/test.html' is never visited in Training. And the max num of parameters accross all pages is 7.
user access this page at Detection Mode with 8 parameters.

3.Illegal CharacterSet:
Screenshot for the case when the parameter has illegal characters.
In this example, parameter 'username' in '/blog/public/user_signup.php' allows all letters and number, but this username contains character '@'.

4.Illegal Parameter Length:
Screenshot for the case when the parameter length exceeds its limit.
In this example, length of 'user_id' is 2, std=0. This user_id length exceeds 2.

5.Unknown Parameter:
Screenshot for the case when the parameter is not seen in Train Mode.
In this example, '/blog/public/user_signup.php' has no parameter called "d" in Train Mode.

6.Signature GET:
Screenshot for the case when the GET request contains malicious string.
In this example, GET request contains "select" or "javascript", which is defined in WAF_Sig_Conf.

7.Signature POST:
Screenshot for the case when the POST request contains malicious string.
In this example, POST request contains "../../../../", which is defined in WAF_Sig_Conf.

8.Signature USER-AGENT:
Screenshot for the case when the HEADER request contains malicious string.
In this example, HEADER contains "bot", which is defined in WAF_Sig_Conf.

9.Train Start:
Screenshot to start training mode. And table info at that time.

10.Train Done:
Screenshot to stop training mode. And table info at that time.