`

**VERIFIER**

START

GET csrf code from generator

STORE received token in server

READ HTML request sent by appender

COMPARE CSRF token in the request to server storage.

IF(‘csrf’ from HTML request == ‘csrf stored in server)

THEN send response to user

ELSE IF(‘csrf’ from HTML request != ‘csrf stored in server)

THEN inform user of attack

TERMINATE session’

END

**APPENDED**

START

OBTAIN CSRF token string from generator

ADD token to intercepted code

FORWARD request from interceptor to server

END

**GENERATOR**

START

IF generator activated from crawler

THEN

COMPUTE string of random characters

SET string as ‘csrf’ or ‘csrf\_test\_name’

SEND one copy to server

SEND one copy to appender

TERMINATE generator

END

**INTERCEPTOR**

START

INSTALL Application

ASK user to allow the application to act as proxy

ALLOW application to intercept requests

ACTIVATE proxy to application, after user grants access

USER sends request, generating HTTP Request

INTERCEPTION of request via proxy link

END

**CRAWLER**

START

READ input from interceptor(source code)

DETERMINE presence of key word in first line(eg-> csrf,csrf\_test\_name, csrf\_token)

IF word found

THEN

CHECK for token

TERMINATE crawler

FORWARD request to server

ELSE IF word not found

THEN

ACTIVATE generator

TERMINATE crawler

END

START

INTERCEPT request sent by user(via Burpsuite)

IF the request has CSRF Tokens

THEN forward request

ELSE IF request doesn't have CSSRF tokens

THEN

GENERATE CSRF Token

APPEND generated token to request

SEND request to server for storage.

SEND appended request with CSRF token to server.

COMPARE CSRF token in the request to server storage.

IF comparison successful

THEN send response to user

ELSE IF comparison unsuccessful

THEN inform user of attack

TERMINATE session’

END