Maxwell Fusco
HW 4 Act 2 Step 2

### The Issue

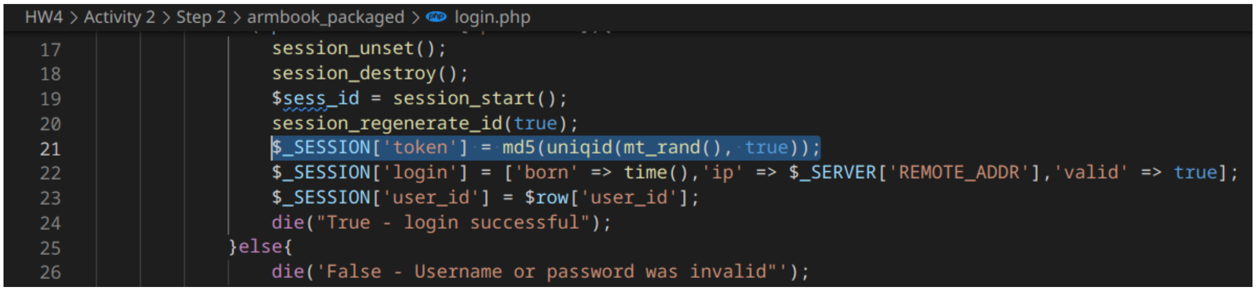
There was no way to check whether a request was being sent from the user clicking on a random link or if they were clicking a button on the armbook website. This allowed anyone to send links that were able to make requests on behalf of anyone clicking the link.

### The Fix

I Implemented CSRF Token. CSRF tokens are randomly generated tokens which do nothing other than be able to tell whether a request was made from the same session that the user is in. This is done by requiring the random token be imputed as validation for any request that are needed to be secure.

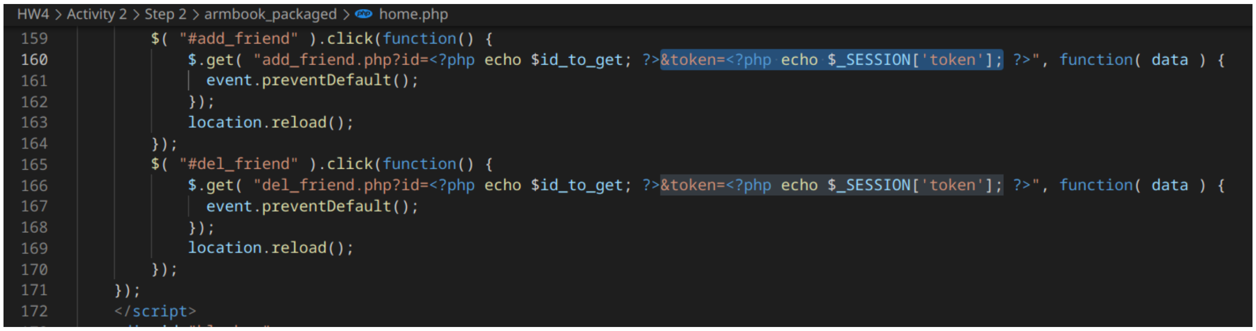
### How I Did It

1) Create CSRF token when the user correctly authenticates

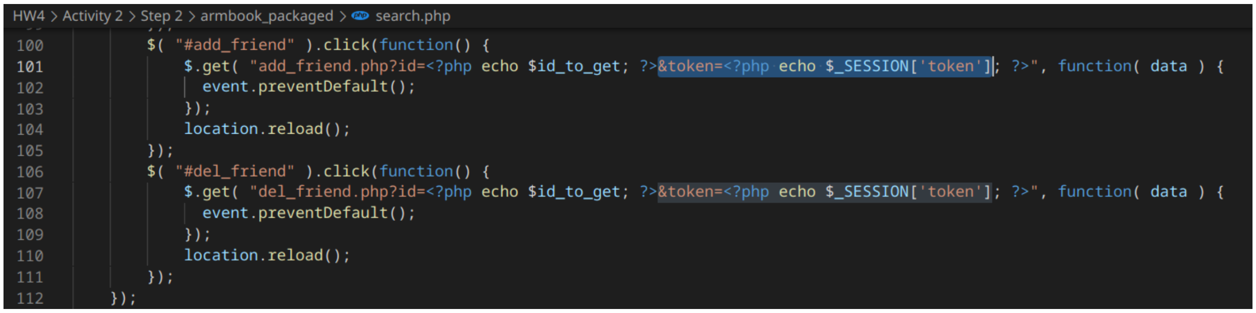


```
                session_unset();
                session_destroy();
                $sess_id = session_start();
                session_regenerate_id(true);
                $_SESSION['token'] = md5(uniqid(mt_rand(), true));
                $_SESSION['login'] = ['born' => time(),'ip' => $_SERVER['REMOTE_ADDR'],'valid' => true];
                $_SESSION['user_id'] = $row['user_id'];
                die("True - login successful");
            }else{
                die('False - Username or password was invalid"');
```

2) Add CSRF token to add_friend and del_friend requests in home.php and search.php

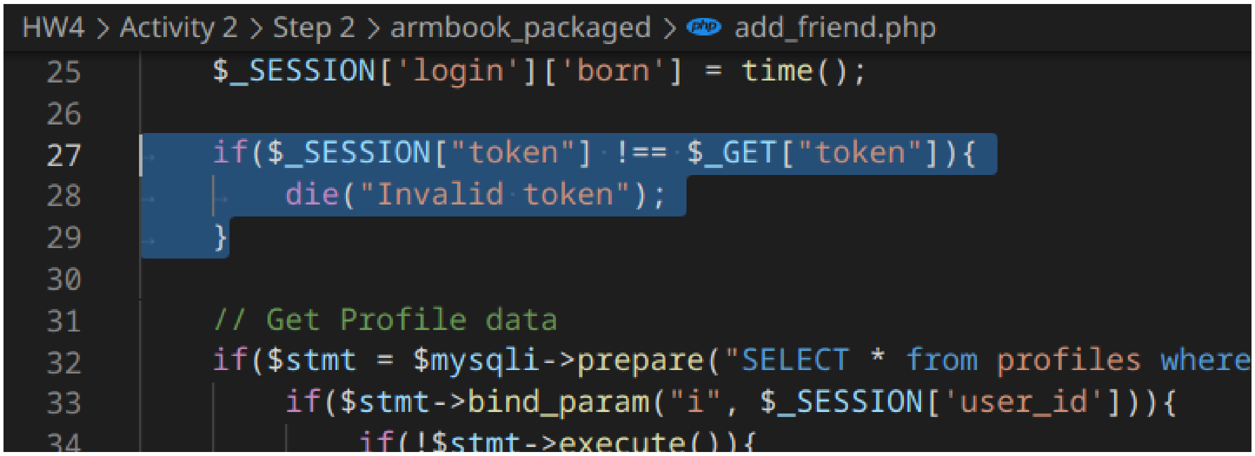


```
        $( "#add_friend" ).click(function() {
            $.get( "add_friend.php?id=<?php echo $id_to_get; ?>&token=<?php echo $_SESSION['token']; ?>", function( data ) {
              event.preventDefault();
            });
            location.reload();
        });
        $( "#del_friend" ).click(function() {
            $.get( "del_friend.php?id=<?php echo $id_to_get; ?>&token=<?php echo $_SESSION['token']; ?>", function( data ) {
              event.preventDefault();
            });
            location.reload();
        });
    });
    </script>
```



```
        $( "#add_friend" ).click(function() {
            $.get( "add_friend.php?id=<?php echo $id_to_get; ?>&token=<?php echo $_SESSION['token']; ?>", function( data ) {
              event.preventDefault();
            });
            location.reload();
        });
        $( "#del_friend" ).click(function() {
            $.get( "del_friend.php?id=<?php echo $id_to_get; ?>&token=<?php echo $_SESSION['token']; ?>", function( data ) {
              event.preventDefault();
            });
            location.reload();
        });
    });
```

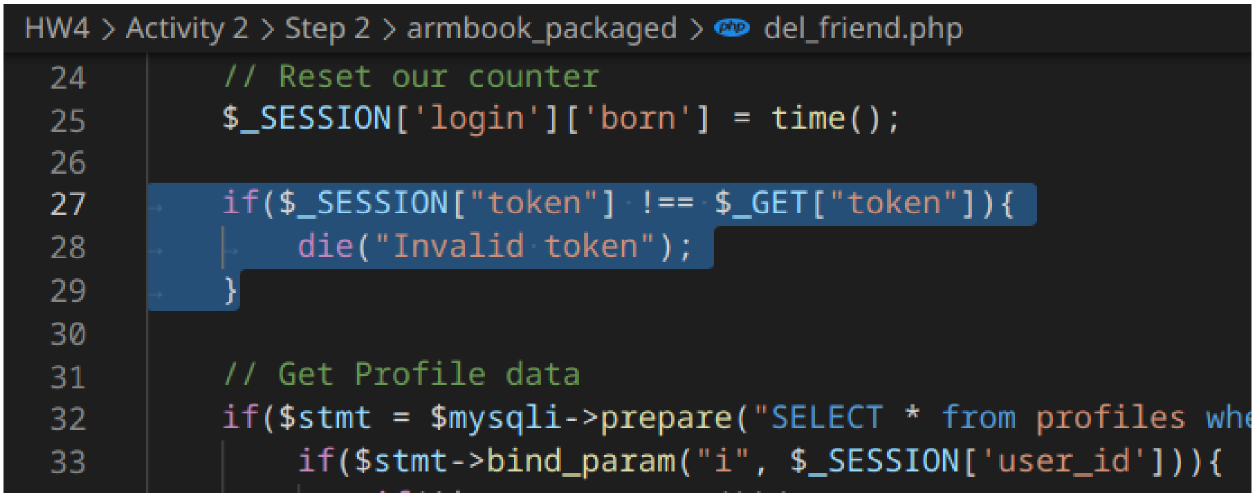
3) Check CSRF token when add_friend.php or del_friend.php request is made


HW4 > Activity 2 > Step 2 > armbook_packaged > add_friend.php

```php
    $_SESSION['login']['born'] = time();

    if($_SESSION["token"] !== $_GET["token"]){
        die("Invalid token");
    }

    // Get Profile data
    if($stmt = $mysqli->prepare("SELECT * from profiles where
        if($stmt->bind_param("i", $_SESSION['user_id'])){
            if(!$stmt->execute()){
```


HW4 > Activity 2 > Step 2 > armbook_packaged > del_friend.php

```php
    // Reset our counter
    $_SESSION['login']['born'] = time();

    if($_SESSION["token"] !== $_GET["token"]){
        die("Invalid token");
    }

    // Get Profile data
    if($stmt = $mysqli->prepare("SELECT * from profiles whe
        if($stmt->bind_param("i", $_SESSION['user_id'])){
```

4) Profit B)