6.3 Assignment: CSRF Proof of Concept

Instructions

Estimated Effort Required: 3-5 hours

Learning Outcome: Students will understand how to carry out a CSRF attack and an understanding about the root vulnerabilities that make this type of attack possible.

Assignment Goal: You will create a small set of PHP scripts that are vulnerable to cross-site request forgery and document the process of carrying out an attack on your code.

Preface: The following words should be interpreted as per RFC 2119 for this assignment: must, must not, required, shall, shall not, should, should not, recommended, may, and optional.

Description

Cross-site request forgery is one of the more complex common client-side attack. Cross-site request forgery involves tricking a user into making a sensitive HTTP request to a website without their knowledge. Often this is done by including an iframe in a malicious website that causes the user's browser to make a request to an API in a real website. For example, by visiting badsite.com/bad.html may have an iframe in it that causes anyone who visits it to make a request to a money transfer page mybank.com/transfer.php that transfers money from the victim's account to the attacker's account. The user doesn't necessarily know this happens unless they view the page source on badsite.com or inspect their traffic.

In this assignment, you will build a small set of PHP scripts that are vulnerable to cross-site request forgery and produce a short write-up explaining how to exploit the CSRF

vulnerability. As a starting point, you may wish to look DVWA's CSRF Vulnerabilities and read a walkthrough of exploiting DVWA's low CSRF vulnerability.

Requirements:

1. Your PHP scripts must execute on the most recent version of Apache and PHP available via apt-get for Ubuntu 18.04.
2. Your code must execute on Ubuntu 18.04.
3. Your code must be proof-of-concept quality but may be very underdeveloped when compared to code that would be created for a production-level web application. Developing highly usable interfaces for any element of this demonstration is optional.

Deliverables:

1. Must include a write-up documenting how to carry out the CSRF attack against your PHP scripts
2. Must include your vulnerable PHP scripts
3. Must include a readme text file which provides:
    a. i. Instructions on how to install any additional dependencies your code may have, including compilers/interpreters and development environments that are necessary to run your code.
    ii. Instructions on how to execute your code, if necessary
    iii. Should include a script that can be run to install any additional dependencies your code may have, if applicable. This may include MySQL.

Submissions

No submissions yet. Drag and drop to upload your assignment below.

Drop files here, or click below!

Upload | Choose Existing

You can upload files up to a maximum of 1 GB.

Feedback

Activity Details

Task: Submit to complete this assignment

Due March 2 at 11:55 PM