Labs

back to dashboard

CSRF - Basic

EXPIRED

Perform Cross Site Request Forgery attack

15-45 Minutes 250 Points 5/10 Difficulty

Start Stop

✓ You have already completed this exercise.

Mission Statement Verify Flags

CSRF (Cross-Site Request Forgery) is one of the most widely exploited vulnerabilities in web applications.

As the name suggests, it allows an attacker to forge a request from the victim's behalf but a different domain that the attacker controls. In the worst case, an attacker might take over an entire user account without having prior knowledge of credentials.

This lab works on the same level and expects you to craft an attack manually and takeover the user account. You need to perform a Cross-Site Request Forgery attack on csrf.com

Steps to complete the lab:

1. Open csrf.com in the attacker's browser
2. Create a test user with the information requested in the form
3. Open `csrf/` directory located on `/root/Desktop` and edit csrf.html
4. csrf.html is a template for your attack. Populate it with the following form data to exploit the lab
   - Add a *hidden* input field with name `csrf` and value `true`
   - Add a *hidden* input field that edits the "bio" of the victim to "hacked by rootsh3ll"
5. Open http://csrfattack.com:8000 in the same browser and wait for the webpage to load.
   NOTE: It'll show an image
6. If the attack executes successfully, you'll find the flag on csrf.com on page refresh. If not, go to step 4.

Note

The attack must be performed through `http://csrfattack.com:8000`
The HTTP Referrer must report http://csrfattack.com:8000/csrf.html to validate the attack and receive flag on csrf.com