Cross Site Request Forgery
IN618 Security

Introduction

Cross site request forgery (XSRF) is an exploit that is somewhat related to XSS, but it's different enough to warrant expolration on it's own. Basically, XSS vulnerability is caused when a user's browser trusts the response from a server and gets exploited. In XSRF, the server trusts the request from the browser.

1 Examine the exploit

A simple application at `http://in618.sqrawler.com/xsrf` is vulnerable to XSRF exploits. Try out the site, using you OP user name to log in. Once you see how it works, see if you can deduce how it can be exploited.

After you try exploiting it on your own, make sure that you have a saved message. Keep a tab to the message page open while visiting `http://sec-student.sqrawler.com/~tclark` in a second tab. Now go back and load `http://in618.sqrawler.com/xsrf/home.php` in you other tab. What happened? Can you see how it happened?

2 The exploit

The problem is that, if a user is logged in, anything that causes that user's browser to send an HTTP GET request to `http://in618.sqrawler.com/xsrf/home.php?action=Delete` will deleted that user's saved message. Can you think of some ways we could fix this?