

Cross Site Request Forgery

Monday, October 30, 2017 9:34 PM

- Cross site request forgery is an attack that tricks the victim into loading a page that contains a form, a JavaScript request, or an embedded images such as the one below:

```

```

- When the victim's browser attempts to render the page, it will issue a request to the "me" endpoint at www.mybank.com with the with the specified parameters
- The browser will request the link expecting to get an image, even though it actually is a funds transfer function
- The browser will add all cookies associated with the site when submitting the request
 - Therefore, if the user has authenticated to the site, and has either a permanent or a current session cookie, the site will have no way to distinguish this from a legitimate user request
- In this way, the attacker can make the victim perform actions that they didn't intend to, such as "purchase an item", or any other function provided by the vulnerable website

Solution

Enter..

```

```

Into the message field