Brian Cullinan

9/29/2010

HW2

The subject input is not validated. This is a huge vulnerability because the subject can send mail command to the mail post server like “reset” and then send a completely different message all together and use the mail server as a slave for spamming.

The body of the message is not validated, so malicious HTML links could be sent to the $to address. As well as malicious attachments and images. Using a function like htmlspecialchars() to replace all html tags with their html characters such as < being converted to &lt; will prevent HTML from being used in the message body.

The $from is used directly on the command line without validation, this could be exploited to display different information and even send the user and password list for the server to the mail program.

$subject is not validate when printed out to the page, this could be used to submit malicious messages and display malicious links to the user after the form has been submitted. A better way to make sure this form is being submitted is to check the HTTP\_REFERRER, preventing XSRF. A unique token could be cached in a database and submitted with the form, that way the form must be submitted by the user from within the browser, this would prevent automating an attack and making this server a slave for spamming.