Using Burp to Test for Cross-Site Request Forgery (CSRF)

Cross-site request forgery (CSRF) is an attack which forces an end user to execute unwanted actions on a web application to which they are currently authenticated.

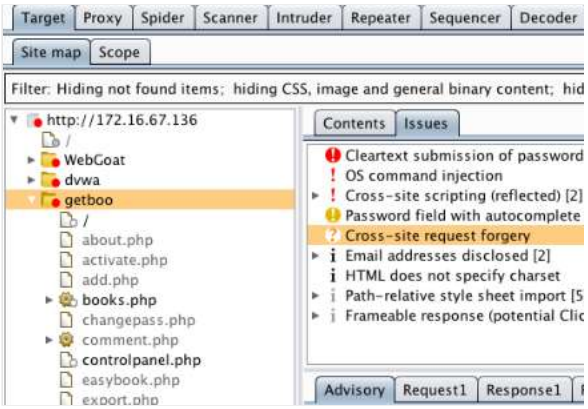
CSRF vulnerabilities may arise when applications rely solely on HTTP cookies to identify the user that has issued a particular request. Because browsers automatically add cookies to requests regardless of the request's origin, it may be possible for an attacker to create a malicious web site that forges a cro domain request to the vulnerable application.

In this example we will be using Burp's CSRF PoC generator to help us hijack a user's account by changing their details (the email address associated w account) on an old, vulnerable version of "GETBOO".

The version of "GETBOO" we are using is taken from OWASP's Broken Web Application Project. Find out how to download, install and use this project.

Burp Scanner is able to locate potential CSRF issues.

The Scanner identifies a number of conditions, including when an application relies solely on HTTP cookies to identify the user, that result in a request being vulnerable to CSRF.



To manually test for CSRF vulnerabilities, first, ensure that Burp is correctly configured with your browser.

In the Burp Proxy "Intercept" tab, ensure "Intercept is off".

Visit the web application you are testing in your browser.

Ensure you are authenticated to the web application you are testing.

In this example by logging in to the application.

You can log in using the credentials user:user.

Access the page you are testing.

Alter the value in the field/s you wish to change, in this case "Email".

In this example we will add a number to the email.

Return to Burp.

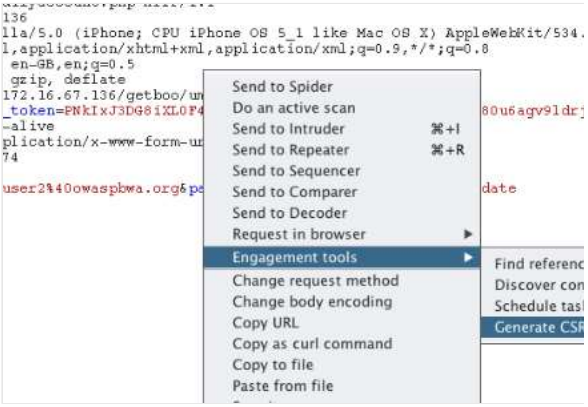
In the Proxy "Intercept" tab, ensure "Intercept is on".

Submit the request so that it is captured by Burp.

In the "Proxy" tab, right click on the raw request to bring up the context menu.

Go to the "Engagement tools" options and click "Generate CSRF PoC".

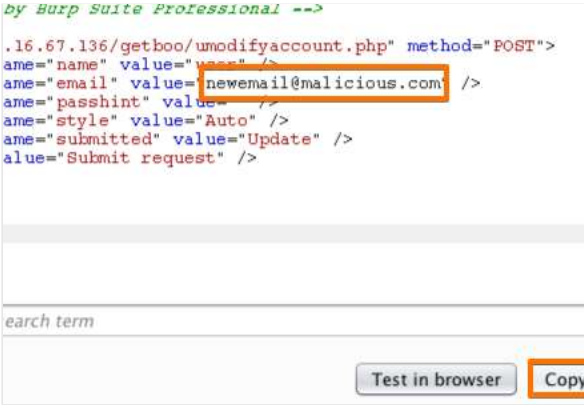
Note: You can also generate CSRF PoC's via the context menu in any location where HTTP requests are shown, such as the site map or Proxy history.



In the "CSRF PoC generator" window you should alter the value of the user supplied input.

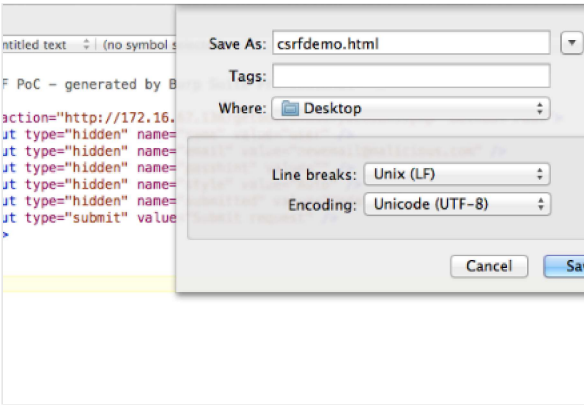
In this example we will change to "newemail@malicious.com".

In the same window, click "Copy HTML".



Open a text editor and paste the copied HTML.

Save the file as a HTML file.

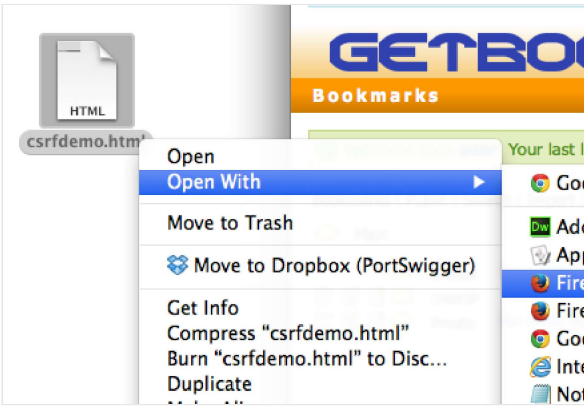


In the Proxy "Intercept" tab, ensure "Intercept is off".

If necessary, log back in to the application.

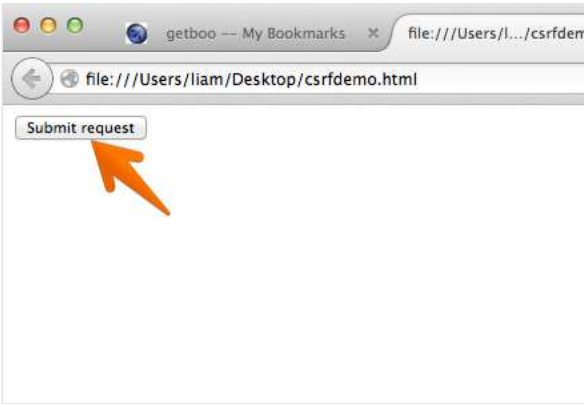
Initially we will test the attack on the same account.

Open the HTML file in the same browser.

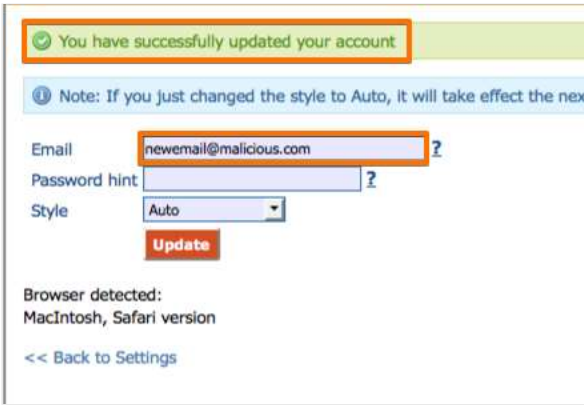


Dependent on the CSRF PoC options you may need to submit the request or it may be submitted automatically.

In this case we are submitting the request manually.

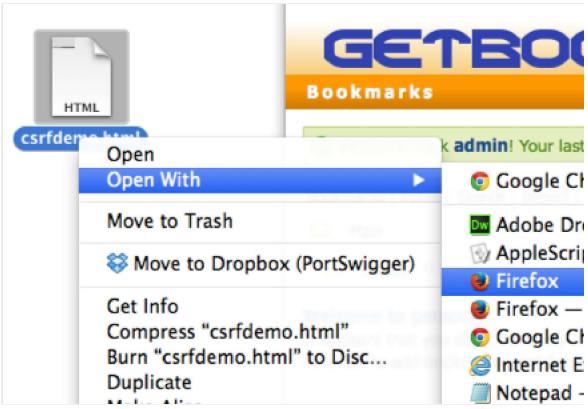


If the attack has been successful and the account information has been successfully changed, this serves as an initial check to verify whether the attack is plausible.



Now login to the application using a different account (in this example the admin account for the application).

Once you are logged in, perform the attack again by opening the file in the same browser.



The attack is successful if the account information in the web application has been altered.

A successful attack shows that the web application is vulnerable to CSRF.

For the attack to fire in a real world environment, the victim needs to access a page under the attacker's control while authenticated.

In our example web application, a new password can be set for the account using the email address. In this way an attacker could gain full ownership of the account.

Related articles:

- Burp's CSRF PoC generator
- Getting started with Burp Proxy
- Getting started with Burp Scanner