SecureIt : Complete Web Sceurity chrome extension

Abstract

CSRF is an attack that **forces an end user to execute unwanted actions on a web application** in which he/she is currently authenticated. With a little help of social engineering (like sending a link via email or chat), an attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation, when it targets a normal user. If the targeted end user is the administrator account, a CSRF attack can compromise the entire web application.

CSRF relies on the following:

1.Web browser behavior regarding the handling of session-related information such as cookies and http authentication information

2.Knowledge by the attacker of valid web application URLs

3.Application session management relying only on information which is known by the browser

4.Existence of HTML tags whose presence cause immediate access to an http[s] resource; for example the image tag

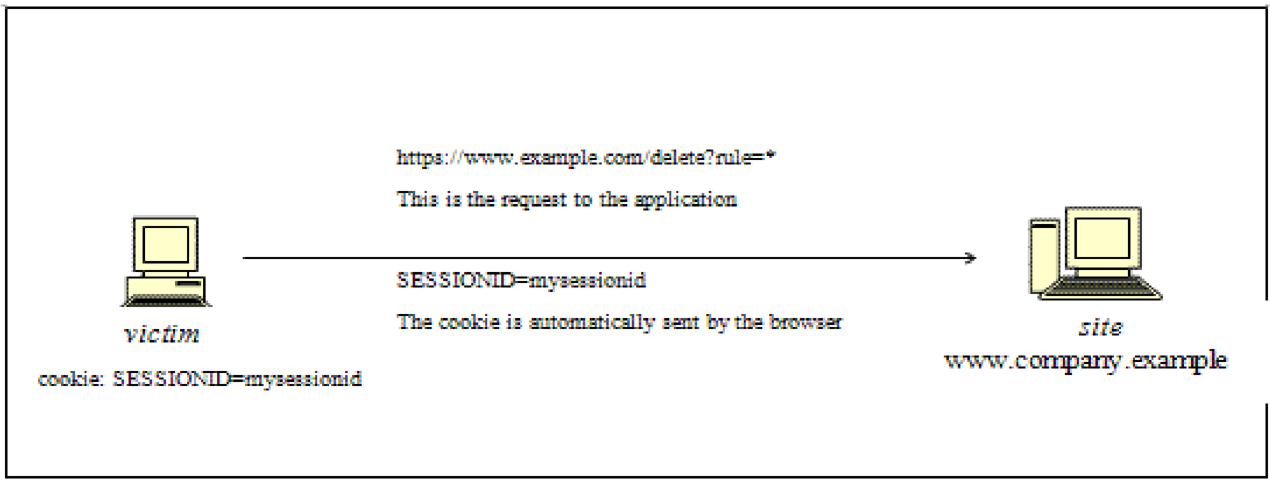
https://www.example.com/delete?rule=*
This is the request to the application
SESSIONID=mysessionid
The cookie is automatically sent by the browser
victim
cookie: SESSIONID=mysessionid
site
www.company.example

Figure 1 : How a Cross Site Request Forgery (CSRF) works

Security Threats : Current scenario

37%	Cross-site scripting
16%	SQL injection
5%	Path disclosure
5%	Denial-of-service attack
4%	Arbitrary code execution
4%	Memory corruption
4%	**Cross-site request forgery**
3%	Data breach (information disclosure)
3%	Arbitrary file inclusion
2%	Local file inclusion
1%	Remote file inclusion
1%	Buffer overflow
15%	Other, including code injection (PHP/JavaScript), etc.

About SecureIt

It is extension to the hacktab security tests chrome extension for CSRF; deploying CSRF testing methods for checking whether a site is CSRF vulnerable or not. It will be helpful for developers, QA and Pen testers.

Further work

There is a scope for AI algorithms in generalising and making web 2.0 (and ahead) secure.

References :

[1]Testing for CSRF (OTG-SESS-005) https://www.owasp.org/index.php/Testing_for_CSRF_(OTG-SESS-005)

[2]Web Security http://en.wikipedia.org/wiki/Web_application_security