CSRF Protection

Overview

Cross site request forgery is a class of attack that forces an end user to execute unwanted actions on Jenkins. Because of the way this attack works, even Jenkins that's running inside a corporate firewall is vulnerable. A common way to exploit this is by spear phishing.

Enabling Protection

To protect against this class of attacks, go to "Manage Jenkins" > "Configure Global Security" and select "Prevent Cross Site Request Forgery exploits." This option is enabled by default in new installations starting Jenkins 2.x, but if you are still on 1.x or upgrading existing installations to 2.x, this option is off by default.

Or with groovy:

csrf.groovy

```
import hudson.security.csrf.DefaultCrumbIssuer
import jenkins.model.Jenkins

def instance = Jenkins.instance
instance.setCrumbIssuer(new DefaultCrumbIssuer(true))
instance.save()
```

Gotchas

- If you have scripts and other programs that access Jenkins via REST API, they can be impacted. See its CSRF section for more information about how to update those scripts.