

Deref Specification

Browser Requirement

- Firefox 4.0+
- Google Chrome

Server Requirement

- 2 different domain names
- 2 Apache servers
- PHP5 with BITSET & GMP extensions
- MySQL

Firefox Plugin Installation

- Open Firefox
- Click [Help – Troubleshooting Information] in menu bar
- Click [Open Containing Folder]
- Create a blank file called [deref2011@gmail.com] in your folder and open it
- Write the path to your untared deref folder (ex. /home/user/plugin/deref/)
- Start Firefox, accept the plugin installation
- Enable DeRef by choosing [Tools – DeRef] in menu bar and disable it by closing the DeRef window

Chrome Plugin Installation

- In [DerefSigner.js] change the address in line 67, 68 and 73 into your server url
- Open Chrome
- Goto [chrome://flags] and enable experimental extension API
- Click [Tools – Extension] and enable [Developer mode]
- Click [Load unpacked extension]
- Browse to your untared extension folder then load
- DeRef will be enabled after installation, choosing [Tools – Extension] and untick [Enable] to disable it

Wordpress 2.0 Installation

- Untar [wordpress-2.0.tar.gz] and copy all files to your website root directory. It would be [/var/www/], if you are using Apache Web Server in Linux environment.
- Visit the Wordpress in your browser and follow the steps in the Wordpress to configure it. During the configuration, you need to setup a database in MySQL database server for the Wordpress.
- Create a user account with the user name [attacker] and password [123456]. This is for login CSRF.
- Copying all the files in [/patch] to the Wordpress directory.
- Change the hostname(www.server.com) in [wp-login.php], [validScope] and [sensitive] to your hostname
- Create a backup for the file [/var/www/wp-content/themes/default/header.php]

Malicious Pages Hosting

- Copy the files [csrf.html, loginCSRF.html, clickjacking.html] to another web server's website root directory.
- Copy the file [ssrf.html] to the Wordpress's web server. Suppose the website's root directory is [/var/www/], copy the file to [/var/www/trudy/]. We do this to model that [http://www.server.com/] and [http://www.server.com/trudy/] are maintained by different owners.
- Change the hostname(www.server.com) in [csrf.html, loginCSRF.html, clickjacking.html and ssrf.html] to the Wordpress's hostname.