1. The problem is in the file of ‘install/index.php’

|  |
| --- |
| // Switch to a saved profile as requested  if (isset($\_REQUEST['profile'])) {  expSettings::activateProfile($\_REQUEST['profile']);  expTheme::removeSmartyCache(); //FIXME is this still necessary?  expSession::clearAllUsersSessionCache();  flash('message', gt("New Configuration Profile Loaded"));  header('Location: ../index.php');  } |

1. Follow the function of ‘activateProfile’

|  |
| --- |
| public static function activateProfile($profile)  {  if (is\_readable(BASE . "framework/conf/profiles/$profile.php") &&expUtil::isReallyWritable(  BASE . "framework/conf"  )  ) {  //FIXME do we need to delete current config first??  copy(BASE . "framework/conf/profiles/$profile.php", BASE ."framework/conf/config.php");  // tag it with the profile name  $fh = fopen(BASE . "framework/conf/config.php", "a");  fwrite(  $fh,  "\n<?php\ndefine(\"CURRENTCONFIGNAME\",\"$profile\");\n?>"  ); // add activated profile name to end of profile  fclose($fh);  }  } |

1. What we control the $profile may used by function ‘copy’, and it is not filtered. We can use it to override the framework/conf/config.php file