

Forum:[Hack Forums](#)

Thread: [PHP Audit - The art of finding 0days in webapps Part 1](#)

JoinSeventh - December 22, 2012, 5:56 pm

PHP Audit - The art of finding 0days in webapps Part 1

0x01 - Introduction

[+] Who is this tutorial for?

Before we start I just want to state that I assume you have basic understanding about PHP, MySQL and some common vulnerabilities and how they work.

You don't have to be a professional programmer, but you need to be able to read and understand PHP code.

If you feel that you need to learn some more before getting in to this tutorial I'm going to redirect you to some tutorials below:

PHP tutorial:

Code <http://php.net/manual/en/tutorial.php>

MySQL tutorial:

Code <http://dev.mysql.com/doc/refman/5.0/en/tutorial.html>

Vulnerabilities wiki:

Code <https://www.owasp.org/index.php/Category:Attack>

[+] Who am I?

Nobody. I don't take any responsibilities for your actions, if you find your ass in jail after exploiting 8000 vulnerable Wordpress blogs don't blame me for teaching you.

But if you have any questions feel free to hit me up with a mail to join7 [at+] riseup.net

0x02 - Setting up an Audit Environment

[+] Why use an Audit Environment?

You could just download the code you wish to audit, open it in your systems default text editor and start looking for vulnerabilities.

This is not preferable since there are a very high chance of you missing things and it will surely take a lot more time than by using an Audit Environment.

[+] Web server

We want to set up a Web Server where we can upload and test PHP applications.

If you don't have any experience with hosting you might want to have a look at XAMPP:

Code <http://www.apachefriends.org/en/xampp.html>

If you wish to set it up on your own you should install PHP with MySQL.

Additional things as phpmyadmin and MySQL managers are of course useful too.

I'm not going to go into how to set up a Web Server, just google for it if you're having problems.

Note: Since you're going to test possible vulnerable code on this web server I suggest you only use it on trusted networks and NEVER on a host that's public for the rest of the internet thugs out there.

[+] What are we auditing?

Now when we have our server set up we need to install additional stuff like WordPress, Joomla, MyBB or similar depending on what you're going to audit.

If you're going for a standalone CMS or just a PHP application you will of course not need any of the above but you'll probably some time in your career step into a WordPress blog or a MyBB forum. Here are download links and some information on how to install them:

MyBB

Download: <http://www.mybb.com/downloads>

Installing Guide: <http://docs.mybb.com/Installing.html>

Wordpress

Download: <http://wordpress.org/download/>

Installing Guide: http://codex.wordpress.org/Installing_WordPress

Joomla

Download: <http://www.joomla.org/download.html>

Installing Guide: <http://www.joomla.org/about-joomla/getting-started.html>

SMF

[IMG]http://s4.hubimg.com/u/5814063_f520.jpg[IMG]

Download: <http://download.simplemachines.org/>

Installing Guide: <http://wiki.simplemachines.org/smf/Installing>

The list can go on...

0x03 - What to look for

[+] User input:

Most vulnerabilities are possible because the programmer forgets (or uses improper) Input Validation.

This true for SQL Injection, Cross-Site Scripting, File Inclusion, Server Side Include, Code Injection and File Upload vulnerabilities and a lot more.

[-] \$_GET

Quote:An associative array of variables passed to the current script via the URL parameters. Code <http://php.net/manual/en/reserved.variables.get.php>

[-] \$_POST

Quote:An associative array of variables passed to the current script via the HTTP POST method. Code <http://php.net/manual/en/reserved.variables.post.php>

[-] \$_REQUEST

Quote:An associative array that by default contains the contents of \$_GET, \$_POST and \$_COOKIE. Code <http://php.net/manual/en/reserved.variables.request.php>

[-] \$_COOKIE[*/size*]

Quote:An associative array of variables passed to the current script via HTTP Cookies. Code <http://php.net/manual/en/reserved.variables.cookies.php>

[-] \$_SERVER

Quote:\$_SERVER -- \$HTTP_SERVER_VARS [deprecated] — Server and execution environment information Code <http://php.net/manual/en/reserved.variables.server.php>

[-] \$_FILES

Quote:An associative array of items uploaded to the current script via the HTTP POST method. Code <http://php.net/manual/en/reserved.variables.files.php>

[+] Possible vulnerable functions:

[-] SQL Injection:

Vulnerable Example:

PHP Code

```
<?php
$id = $_GET['id'];
$news = mysql_query( "SELECT * FROM `news` WHERE `id` = $id
ORDER BY `id` DESC LIMIT 0,3" );
mysql_*
$db->* (For MyBB, look here for more info: http://docs.mybb.com/Plugins-Globals.html &
http://docs.mybb.com/Database\_Methods.html )
$wpdb->* (For WordPress - Look here for more info:
http://codex.wordpress.org/Class\_Reference/wpdb )
```

There are a lot of possibly vulnerable mysql_* functions.

Take a look at this reference for more information about MySQL functions:

Code <http://se1.php.net/manual/en/ref.mysql.php>

Some common functions that are possibly vulnerable:

- mysql_db_query — Selects a database and executes a query on it
- mysql_fetch_array — Fetch a result row as an associative array, a numeric array, or both
- mysql_fetch_field — Get column information from a result and return as an object
- mysql_fetch_row — Get a result row as an enumerated array
- mysql_num_rows — Get number of rows in result
- mysql_result — Get result data

[-] File Inclusion:

Vulnerable Example:

PHP Code

```
<?php
$file = $_GET['file'];
if(isset($file))
{
include("pages/$file");
}
else
{
include("index.php");
}
?>include()
require()
```

If the application doesn't restrict how you include files you can read local files and possibly execute files from a remote server (if `allow_url_fopen` is enabled).

[-] Upload:

PHP Code

```
<?php
$target_path = "uploads/";
$target_path = $target_path . basename($_FILES['uploadedfile']['name']);
if (move_uploaded_file($_FILES['uploadedfile']['tmp_name'], $target_path)) {
echo "The file " . basename($_FILES['uploadedfile']['name']) . " has been uploaded";
} else {
echo "There was an error uploading the file, please try again!";
}
?>$_FILES[]
```

If the application does not restrict what and how files are uploaded, you can upload and execute on the server.

[-] Code Execution:

PHP Code

```
<?php
$myvar = "varname";
$x = $_GET['arg'];
eval("\$myvar = \$x;");
?>passthru()
system()
eval()
exec()
```

Note: Go to Part 2 of this tutorial: <https://hackforums.net/showthread.php?tid=3108156>

SzakaLaka - December 22, 2012, 6:09 pm

Thanks for the tutorial, was looking for one like this for a long time

puremindd - December 22, 2012, 6:09 pm

Props to you for writing a nice indepth tutorial, I just skimmed this, might read it up a little later...also damn vuln webapp is a nice thing to mess with too.

sp3ctrum - December 22, 2012, 6:15 pm

In my opinion probably one of the greatest threads I have seen. Looking over it now. Beyond HQ mate :3

The Ion - December 22, 2012, 7:15 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 :)

| Solo | - December 22, 2012, 7:29 pm

amazing post, thanx for contributing!!!!

J?mes - December 22, 2012, 7:36 pm

You might want to also note that most forums / CMS's + plugins don't actually use \$_GET / \$_POST methods and they use their own functions like MyBB's input function. You're more likely to find a vulnerability searching for the input function in mybb then \$_GET or \$_POST ;).

xx 0x0 xx - December 22, 2012, 7:37 pm

i cant say anything about this tutorial cuz no word can give you what you deserve but thank you soo much for this awesome work really HQ member

SIM-111414 - December 22, 2012, 9:25 pm

Nice tut bro.

Something new I learned today.

Thanks for sharing it.:)

Illicit - December 23, 2012, 1:31 am

C'mon man dont tell them all our secrets ! :O

Joking, great tutorial JoinSeventh and you are one of the best people to here from :3

Although you should include :

PHP Code

```
<?php
```

```
$mybb->input['vuln']; // Input for MyBB
```

```
?>
```

Prominent - December 23, 2012, 1:45 am

Great tutorial JoinSeventh, wish other tutorials would be as interesting as this is.

JoinSeventh - December 23, 2012, 8:48 am

Thanks for the feedback guys, glad you liked it.

Do you think I should make a PDF version of the tutorial?

Noah™ - December 23, 2012, 3:07 pm

that's a real legit tutorial right there +1 rep brah hopefully one day I can find one xD