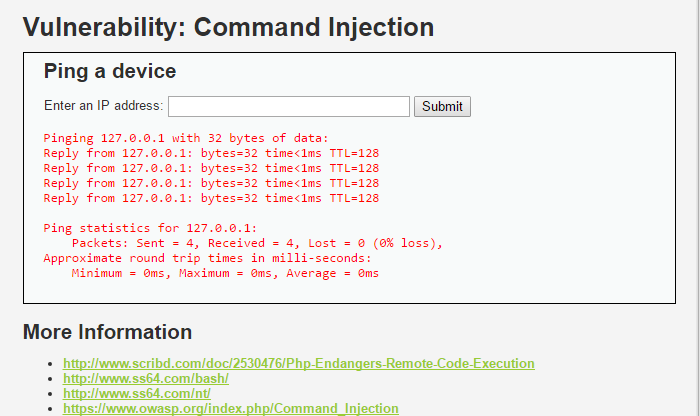
# Remote code Execution

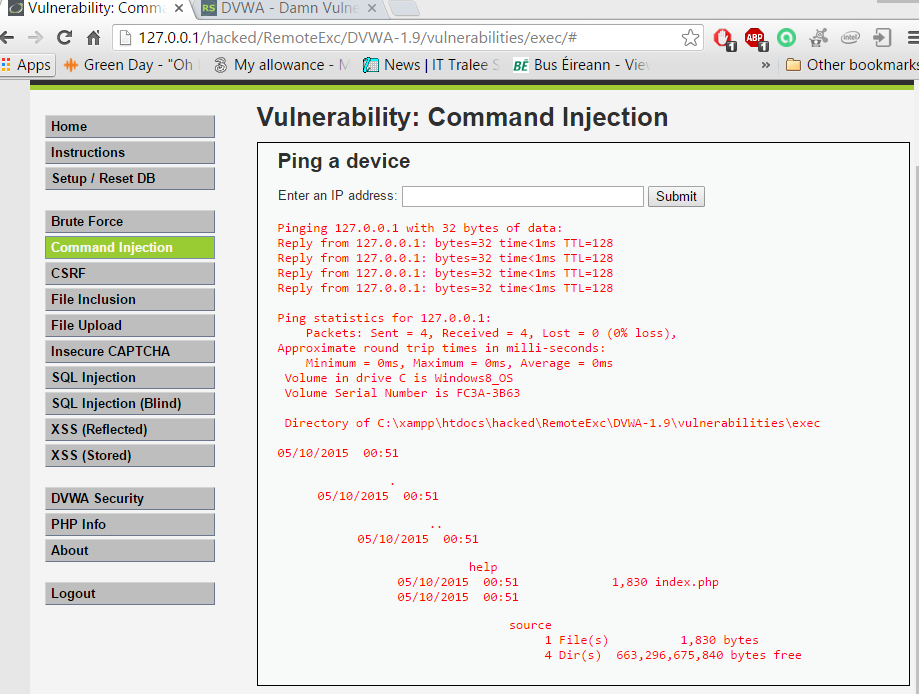
Aim: To retrieve database admin and password.

For this we will use a web called Dam vulnerable web app by Random storm this app can also be used to perform some of the hacks already covered in this procedure. Before you start don’t forget to change the security settings to low, to do this go to DVWA Security and set to low.

If we go to command injection this feature of the web app simply sends a ping to the ip address given, in this case we are using 127.0.0.1

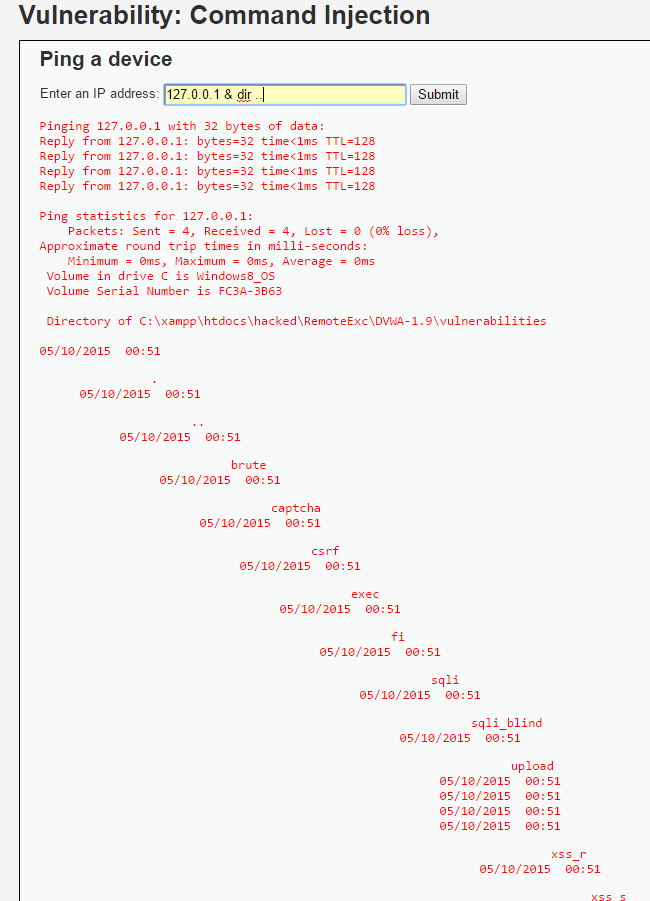


If we enter 127.0.0.1 & dir we get the directory of the DVWA.



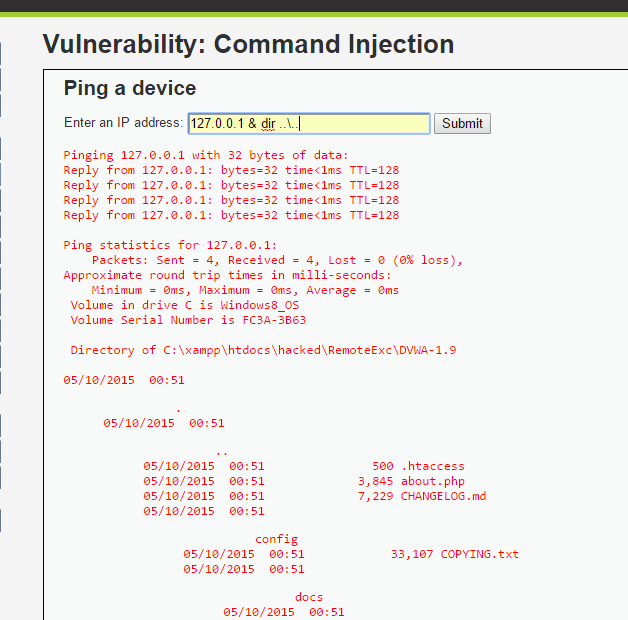
We now know that there is a code execution breech here if we wanted to get more information on our directory.

Enter 1270.0.1 & dir ..



This show us files and folders is we want to access any of these we can but for now we want to get to parent main directory to that

127.0.0.1 & dir ..\..





Here we can see the main directory plus the most interesting directory config. To go to the config directory

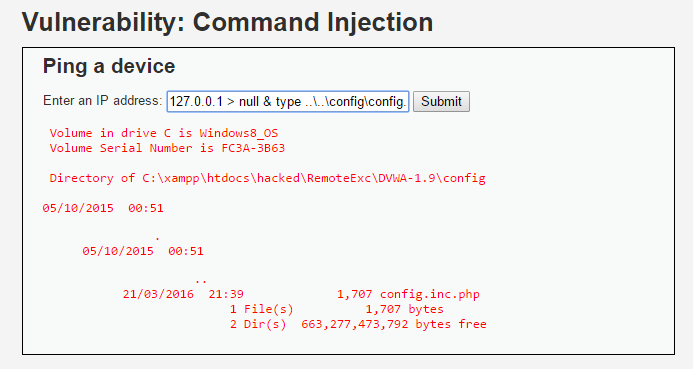
127.0.0.1 > null & dir ..\..\config

> null just removes the ping information but still executes the task and redirects it to null device also known as the bit bucket.



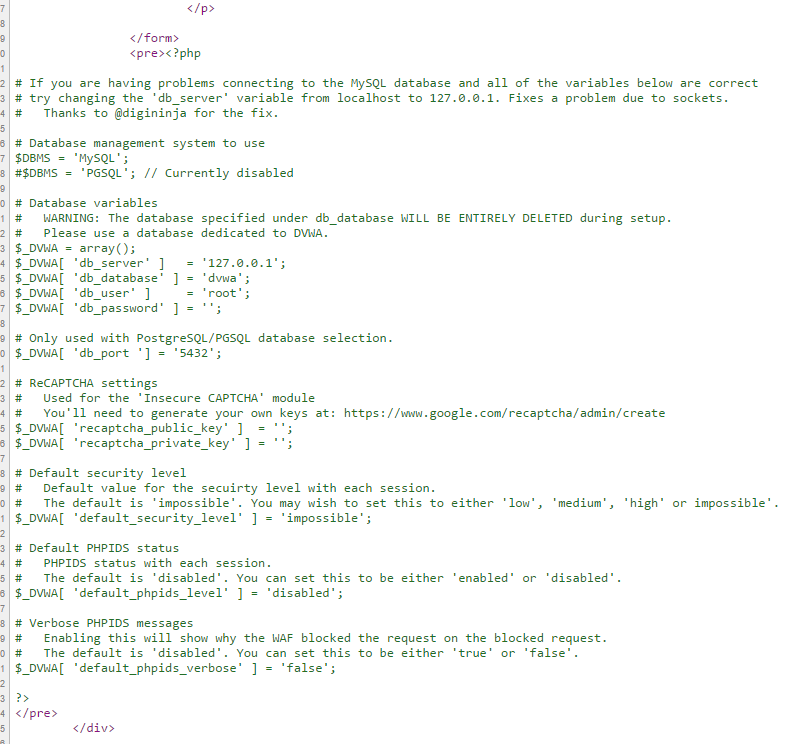
Here we are in the config folder and it only has one file config.inc this might be worth a look, to do that we use the type command this will type out the contents of the file.

127.0.0.1 > null & type ..\..\config\config.inc.php





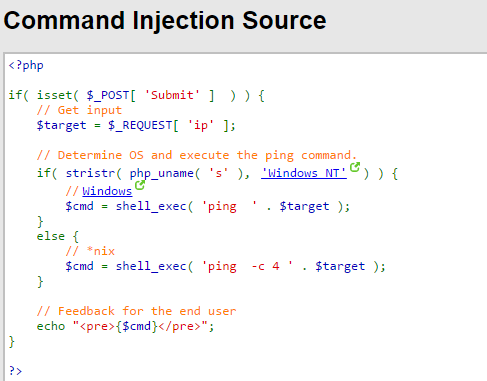
It looks like nothing happened but we go the page source: Right click view page source

 Everything in green is our file and now if we see we can see the admin name and password for the database.



## Solution

Let’s go to starting page and this time click on the view source button.





Here there is an if statement determining whether if our system is windows or Linux machine. Once it knows it executes the shell\_exec here we have the breech. Shell\_exec will execute any commands it receives and dos not have any filtering of what is should not run.

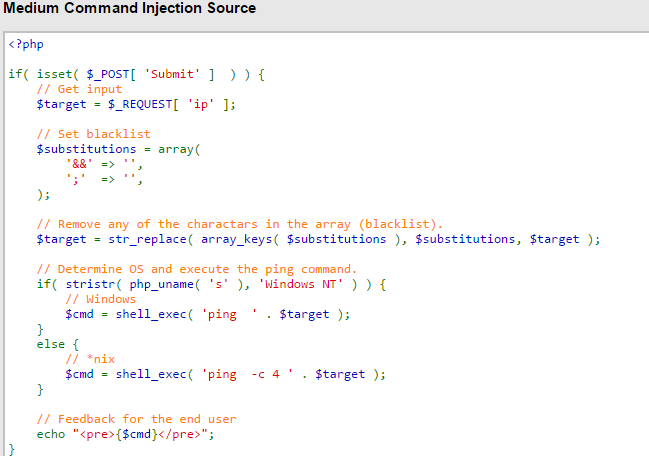
Click on the Compare all levels button



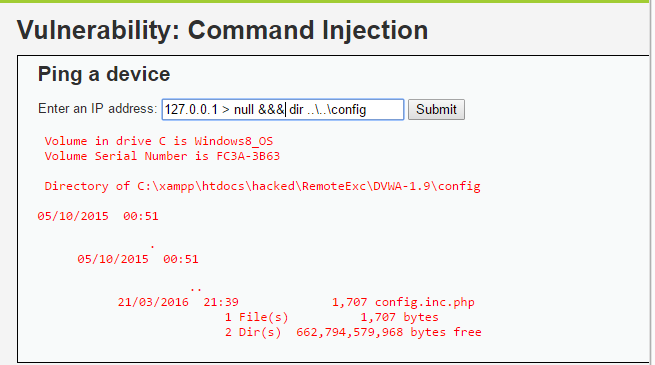
When compared to impossible setting there are differences first there is a check for a session token this prevents cross site forgery same as we spoke of before. Next it gets the input and uses stripslashes to remove any backslashes after that breaks up into 4 octets using explode method returning an array of strings. Checks if each string or octet is a number if all are numbers put it back together.

If we look at Medium and High they use blacklist which blocks any unwanted characters that are entered however this limited as not every variation of characters ids taken under consideration.

### Medium



Here I just entered three &&& and was able to get access to the config folder. Also they code does remove backslashes.



Legal Disclaimer

* **As a condition of your use of this Web site, you warrant to computersecuritystudent.com that you will not use this Web site for any purpose that is unlawful or that is prohibited by these terms, conditions, and notices.**
* **In accordance with UCC § 2-316, this product is provided with "no warranties, either express or implied." The information contained is provided "as-is", with "no guarantee of merchantability."**
* **In addition, this is a teaching website that does not condone malicious behavior of any kind.**
* **Your are on notice, that continuing and/or using this lab outside your "own" test environment is considered malicious and is against the law.**
* **� 2012 No content replication of any kind is allowed without express written permission.**