Table of Contents

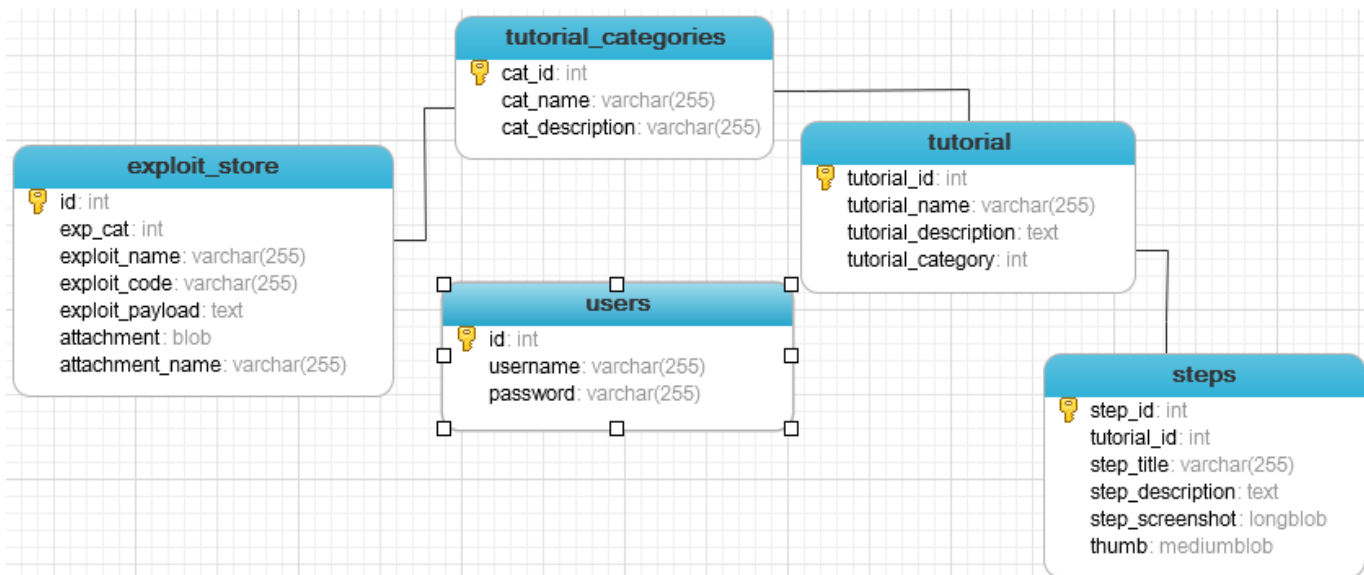# Mth3l3m3nt Tut-Subspace

Why would I want to use this?

Well, For Information Security Consultants there Is always that thing you forget that you used in a previous pentest that you really need for a pentest going on now. So here is where this comes in to just keep all these neat notes and encounters in a nice little loop i.e.

- A **tutorial category manager –** Group your content based on context e.g. Web based attacks, network attacks, SE notes, general concepts etc.
- A **tutorial Manager –** This section ensures that you have a simple description of the "mission" and its code name.
- A **Hacking Process Manager (steps) –** This caters for the nitty grittys of how you wanna do things , and wait for it , it even comes with the ability to attach screenshots to remember the output you got during the mission.
- An **Exploit Store** - This can be best explained with an example. There's always that little exploit script you like to reuse but you have a problem recalling it or finding it everytime you need it and google can prove hell at this point because you just remember some key words. How about having it close to you where you search for your stuff not the world's stuff after you use it this module caters for that. And you can attach the script to the exploit store and categorize your scripts.
- A user manager
- A powerful ajax driven search
- **Print tutorials Module** - Need a text print for the the tutorials you've been gathering ,then here it is quick and easy

This can be used by people from other industries as well as it has a simple workflow :

1. Create major groupings of items (Tutorial Categories) e.g. **cat family**
2. Create consistents or elements that are applicable within the group (Tutorial Manager) – e.g. **Tiger, lion, leopard etc**
3. Give detailed Features of the consistents or elements (Steps) – e.g. **Four legs, long canines etc**
4. Print A manual (Print Tutorials) – e.g. **Tiger Manual → tiger has 4 legs and long canines**

For techies this can be explained as below :

Installing the Tut-Subspace

The installation is quite straight forward.

- Extract the Source files to the Webroot of your webserver

- Create an empty MySQL Database

- Import the .sql file i.e. mth3lm3nt_tut_subspace.sql

- Update the database connection details to those of your webserver in **includes/dbcommon.php** as below:

- Navigate to http://<your-site-name-or-server-ip>/<folder-where-you-extracted>

- you should get the login page as below:

- Default login credentials are:
  username: **mth3l3m3nt**
  password: **mth3l3m3nt**

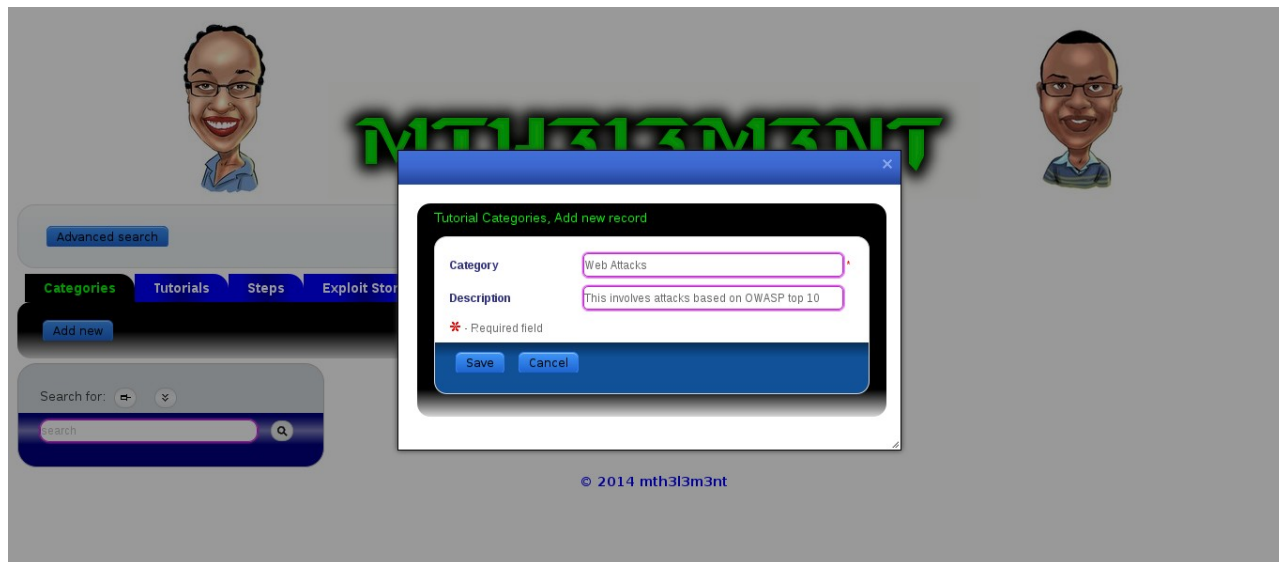- Once logged in the first page will be the main menu

Tutorial Category Manager

This section handles the main categories and is the first place you'd like to have your setup start from:

Before adding anything it would be displayed as below:

Adding Categories is a piece of cake :

- click **Add New** A window as below will appear

- Fill in the details as requrired then click save to save or cancel to ignore changes

    Once you do this you will notice more contextual buttons appear e.g. edit , delete etc all you need to do is select the record you want to edit or delete respectively and click the button.

Tutorial Manager

This bit handles the tutorials in general like a simple code name and description. Before adding any records it displays as below:

- Adding a tutorial "Mission" again is quite easy just click add new and fill in the relevant fields : note that those denoted by * are required
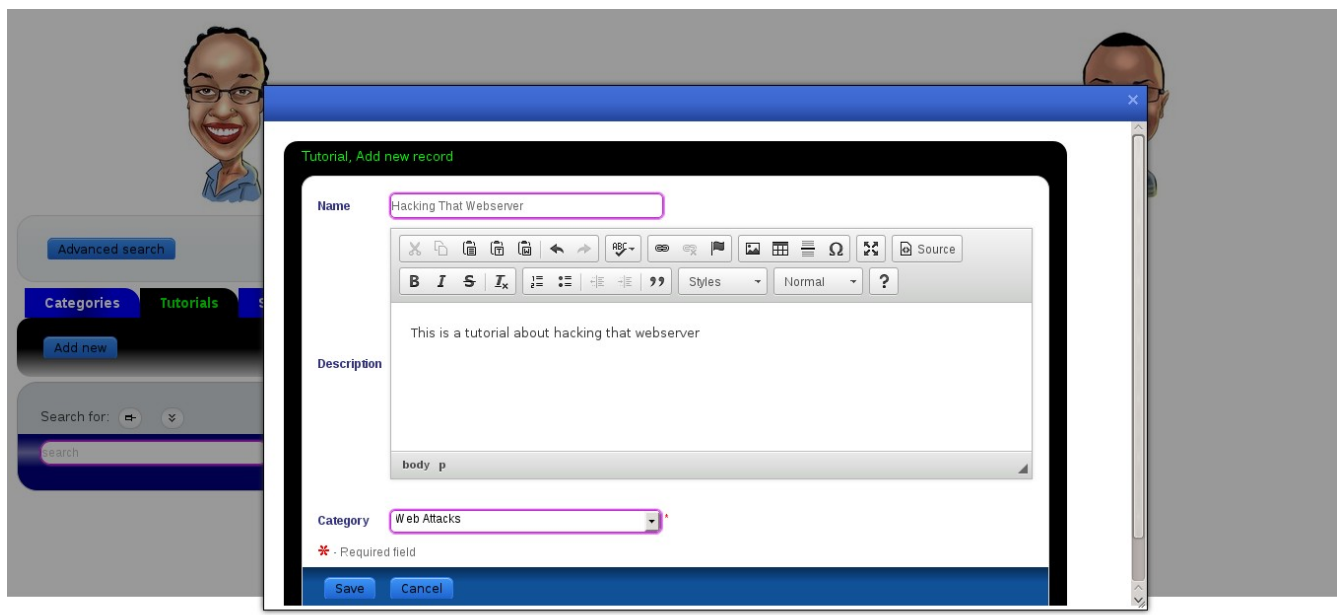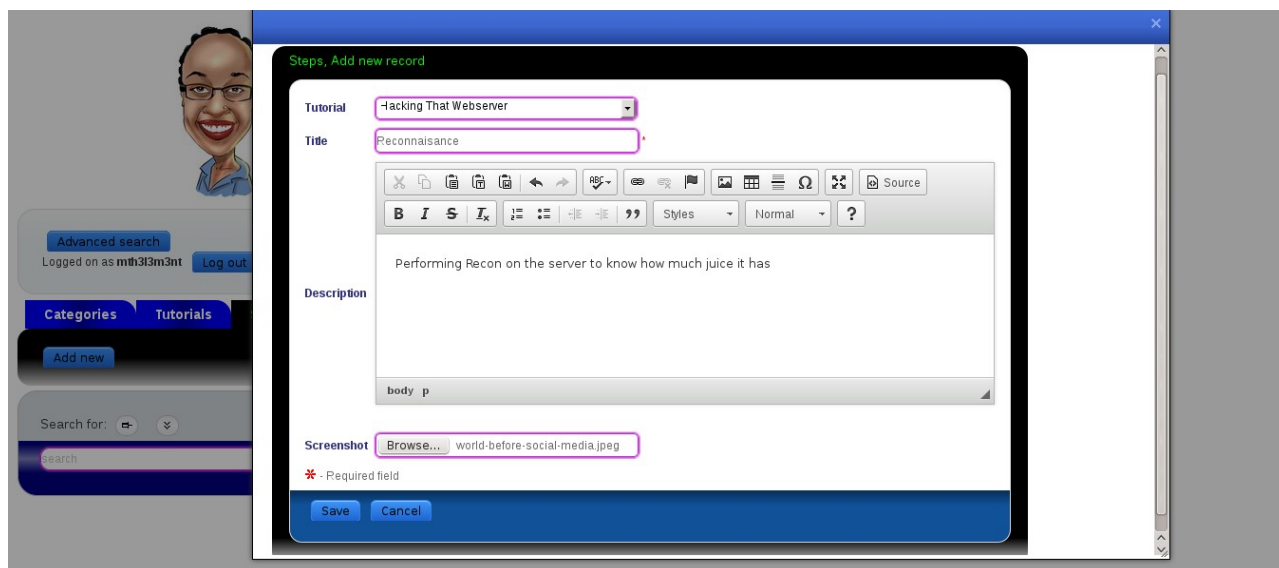

- Assign the tutorial to its respective category then save.

Steps (Hacking Process)

Well this section helps you simply track the nitty gritty's of your mission . When empty you'd expect this:

- Add a new step everytime you do something e.g. Scanned with nmap for services, stirred the flour for the baking contest etc the dialogue to add is as below:

- Add a screenshot if you wanna remember what you got when you did it. Then detail what was

done in this step and assign the step to the relevant mission

- Save or cancel to ignore changes , contextual buttons appear after this as below:

Print Tutorials

This module makes everyones work easier. It simply aggregates your steps or mission processes into a manual.

When you visit this page you should see a summary as below:

- This page has only one tutorial at the moment when they are many you can simply select the field to the left to show only one per page or all. They will be grouped arranging steps per tutorial from first to last.

- To view only one tutorial per page you can select groupings per page on the left and set it to 1 or the number you wish. This is the number that will be printed into a manual, assumption is one is ideal for specialization. If it isnt on the first page when you choose one the ajax search can help you find it such that it is the only one in view.

- Next just click export to excel icon to get it in excel or printer friendly version to view it in the browser from where you can print to pdf.

  Note: Export to word has been disabled for now has a few styling issues.
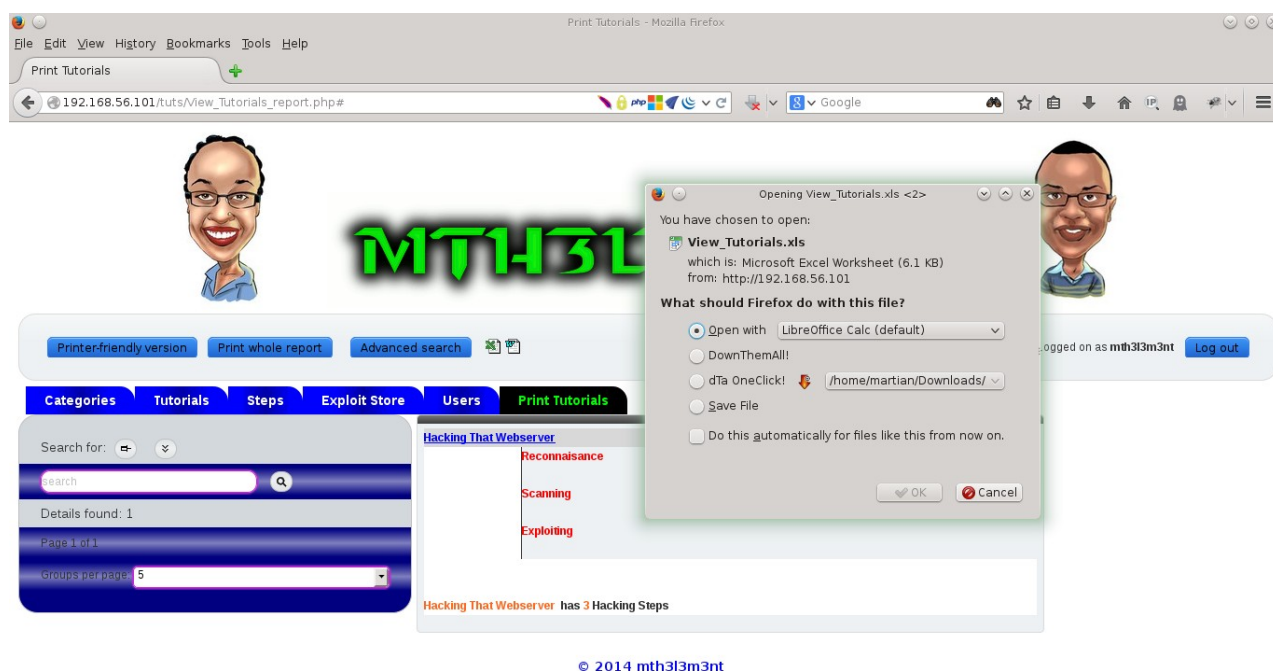
- Expect a page as below on clicking printer friendly version:

Hacking That Webserver

Reconnaisance

Performing Recon on the server to know how much juice it has

Scanning

Scanning the thing like crazy

Exploiting

Exploiting The thing like crazy

Hacking That Webserver has 3 Hacking Steps

Page 1 of 1

Printed By Mth3l3m3nt Tut Subspace

Exploit Store

This is just a store for those things that appear mission to mission and you wanna have a minibank to hold them.

- Adding items here is easy just click add new and fill in the relevant fields then click save.

- You need to assign the exploits to a category too to make it easier to filter and you can attach

any file for download , even php files are allowed but will be saved for download not direct access so they will not be rendered on page sorry :P .
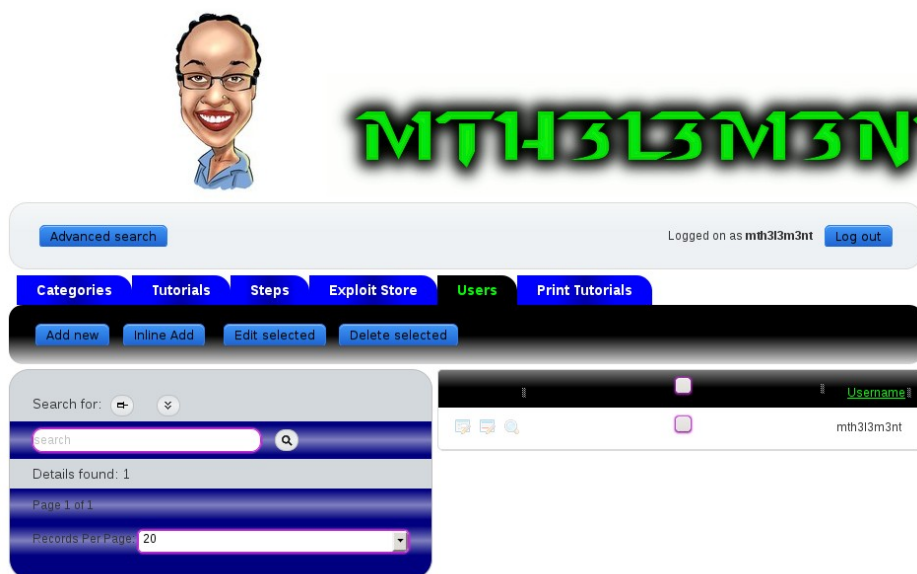
User Management

This is not the very complex Access control systems you see daily. Based on the nature of the application you are either in or out so all users have access to all pages as long as they have valid credentials.

The default are:

username: **mth3l3m3nt**

password: **mth3l3m3nt**
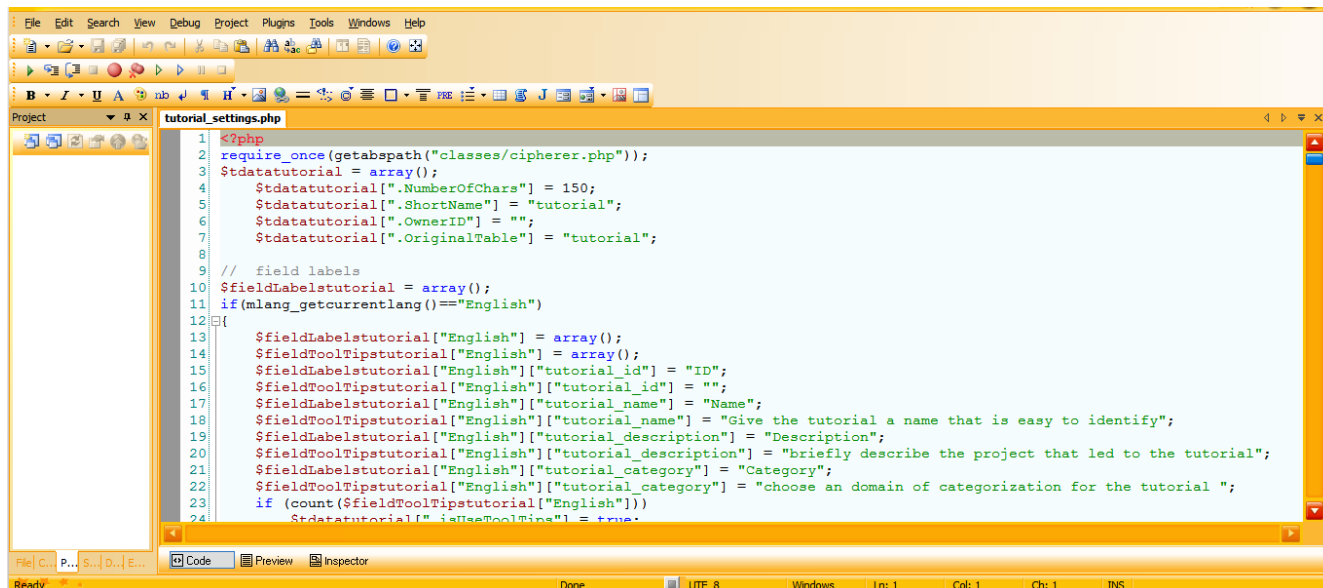

Adding a user is as below:

Abit Non Novice Tutorial

Override Styling

- You can override styling using the mystyle.css file

  1. ctlSearchTip – class styling for the search box /panel and its constituents

  2. runner-button – class styling for all the buttons on the site

  3. Most of the other stuff is generic e.g. input buttons etc so style overrides on html elements should work.

<u>Modifying Behaviour on Pages/Modules</u>

This includes modifying items related to labels for the site e.g. change tutorial in tutorial table to show the title as hackpractice you edit the label in : tutorial_settings.php

- Tutorial_settings.php → settings for the tutorial page

- View_Tutorials_settings.php → settings for the print tutorials page

- tutorial_categories_settings.php → tutorial categories settings page

- steps_settings.php → settings for the hacking process or steps page

- exploit_store_settings.php → settings for the exploit store module/page

These files are located in the include folder . Other settings other than labeling you can change include:

- ✔ Change Searching ability options

- ✔ Changing Export Ability options

- ✔ Edit Page Queries

- ✔ Modify Table Keys

- ✔ Change Import Settings

- ✔ Change Export Settings

✔ Change Print Settings for the page

Other things of relevance include:

- Header.php → Contains the Header of the site

- footer.php → contains the footer of the site

- Errors.xml → Edit site errors related to mysql and other functions to custom text.

- Cookie.js → handles the main cookiesfor sessions across the site.

- English.php → found in the include\lang\ to change regular site messages for various actions e.g. record saved.

The Variables used across the site for each page can be found in include\dal however changing this would mean updating all the other pages too

Changing the format for excel exports is done from the plugins folder through the phpExcel Plugin (http://www.codeplex.com/PHPExcel) – visit the site for documentation.

The rich text editor is handled by the CKEditor (http://ckeditor.com) visit site for more information.

The rest of the code pages are pretty self explanatory but I dont believe you'd wanna change it , it would be redoing the whole thing again :D ;).

That's all for now .

For changes , problems or feature requests and all that stuff:

- Martian (munir.n.n@gmail.com)

- r00t3r (ruthefrain@gmail.com)