Web Application Pentest Lab Setup on AWS

posted in PENETRATION TESTING on DECEMBER 3, 2019 by RAJ CHANDEL SHARE

Isn't it going to be nice if you can reach your pen-testing lab from all over the world? As we all know, this is a digital age that makes life easier than our expectations, thus anyone can access their information/data from the cloud. Similarly, a Pentester can design its pen-testing environment for the vulnerable machine on the cloud that can be accessed from anywhere. AWS is probably the most popular cloud service available in today's date, with most companies taking a cloud or hybrid approach towards their infrastructure.

Search

ENTER KEYWORD

Subscribe to Blog via Email

Email Address

SUBSCRIBE

Follow me on Twitter

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

This article is about setting up a vulnerable lab for web penetration in Amazon Web Services (AWS) to perform pen-testing on.

Table of Content

Prerequisite

To set up your own pen-testing environment, you must have AWS account or if not then create an AWS account and login your account.

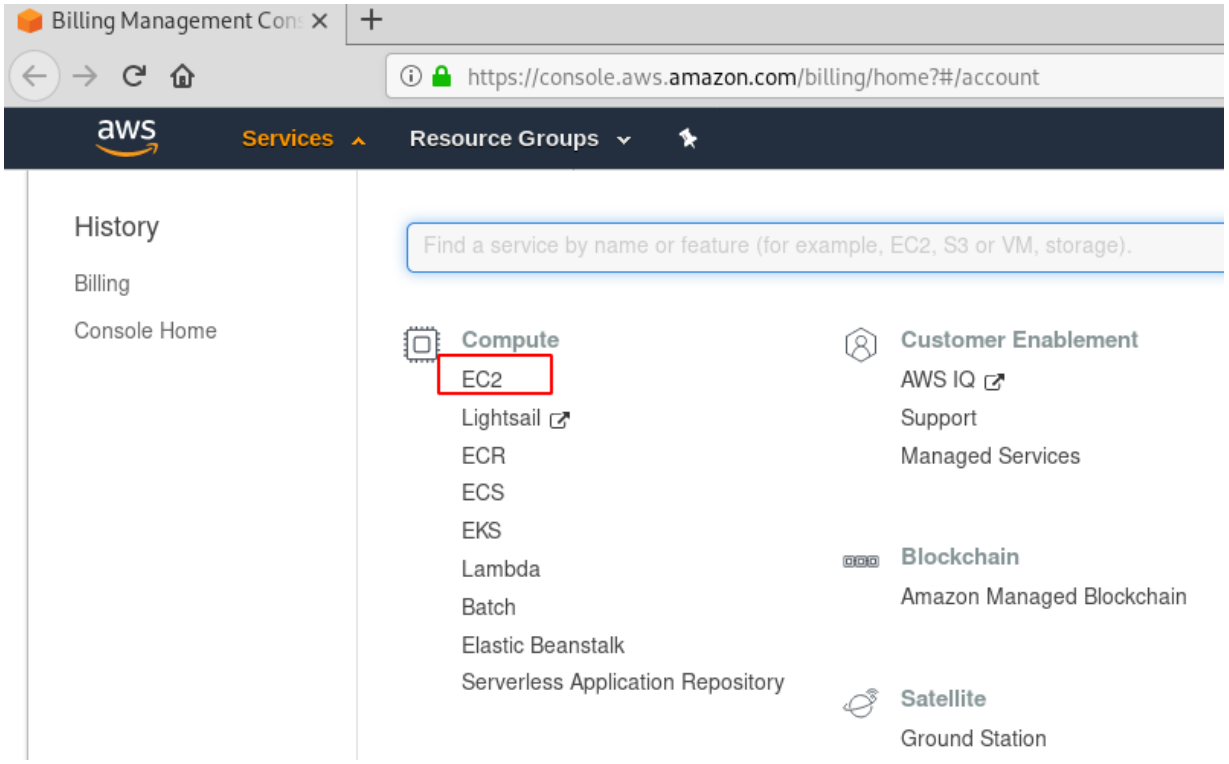
Setup & Configuration of AWS Instance

Let's walk through the process of setting up the lab, we will be making an EC2 instance with Ubuntu Server 18.04 LTS on it. An EC2 instance is referred to as a virtual server in Amazon's Elastic Compute Cloud (EC2) for running applications on

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

the AWS infrastructure. The good thing is that this will not cost you anything to build as AWS has options to setup instances within a certain computing level that are not charged for.

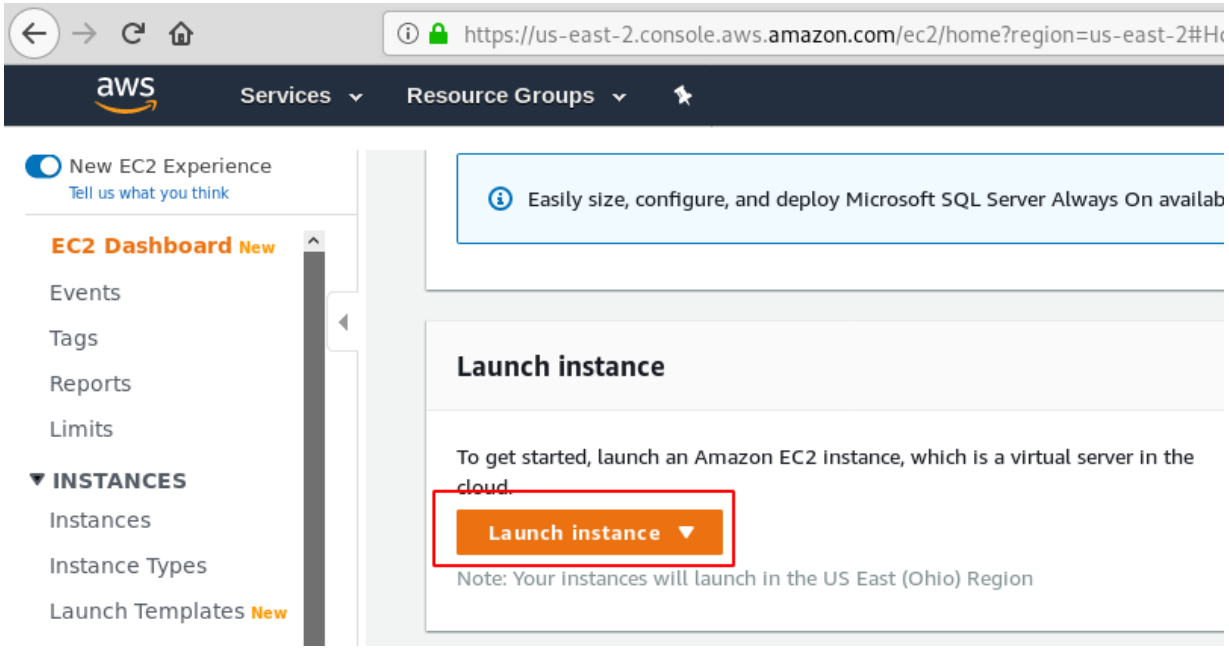
1. Open the **EC2 console** in AWS.



2. Navigate to “Launch Instance” and click on “Launch Instance”.

Categories

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



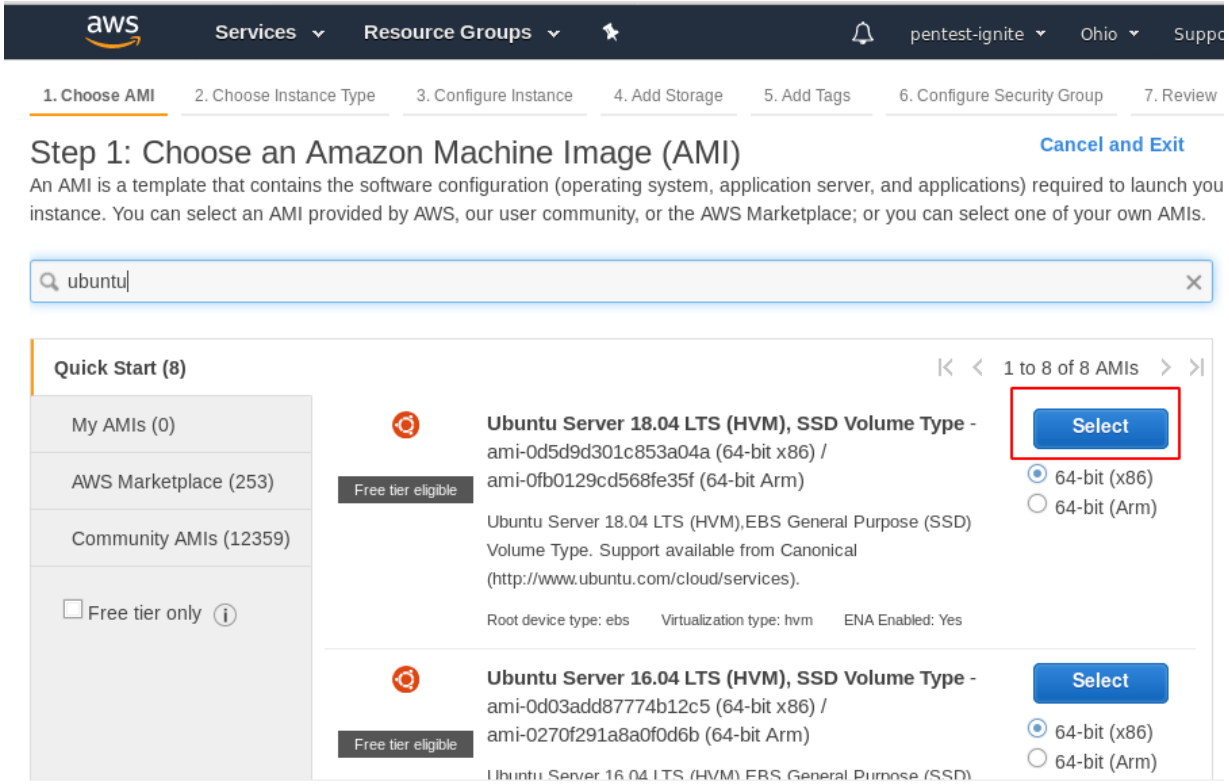
3. Choose the **Amazon machine image** (AMI), this is basically similar to finding the iso file of the OS that you want on your instance. AWS has you covered with most of the popular OS's available in its inventory.
4. Here we looked for ubuntu.
5. Now that we see the OS that we want running on our instance, we need to choose the "64-bit (x86)".

Window Password Hacking
Wireless Hacking

Articles

Select Month

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



6. We now need to choose our instance type, to basically define the amount of hardware this instance will have, we choose the “t2.micro”. This gives us I virtual CPU and 1 GB of RAM.

For most general-purpose workloads, T2 Unlimited instances will provide ample performance without any additional charges.

Features:

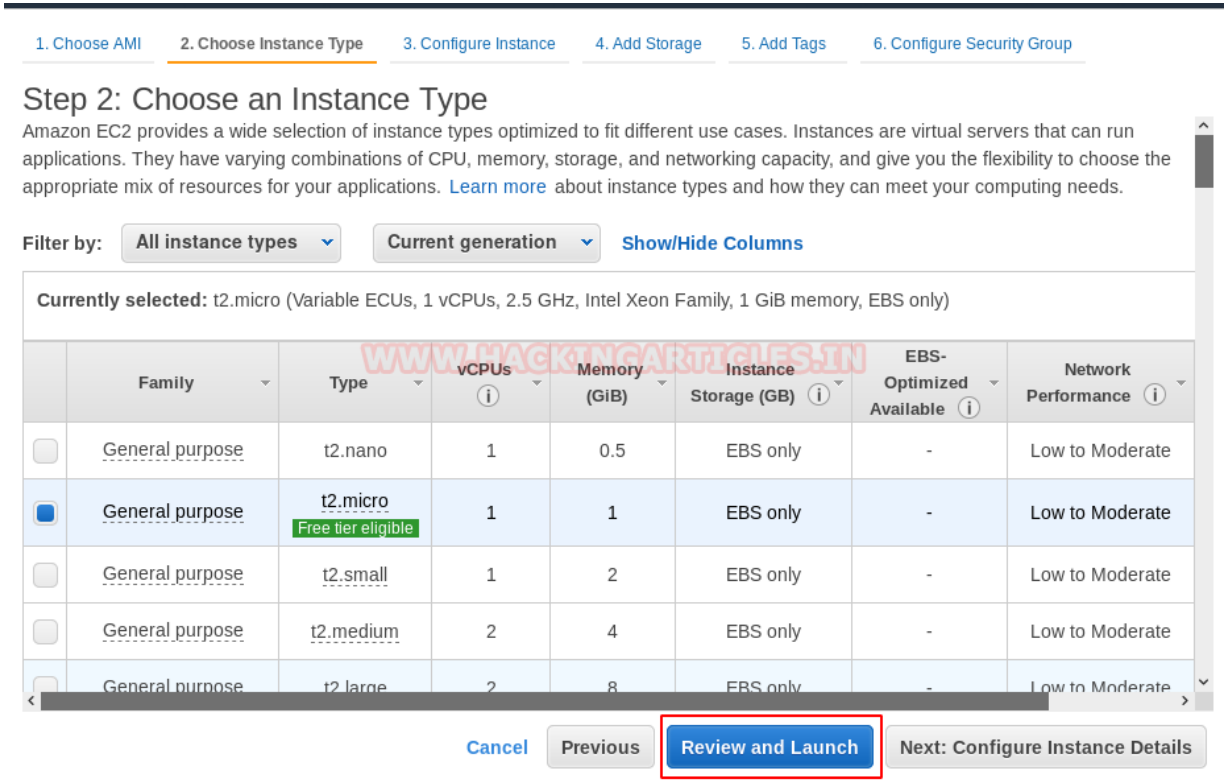
- High-frequency Intel Xeon processors
- Burstable CPU, governed by CPU Credits, and consistent baseline performance
- Lowest-cost general purpose instance type, and Free Tier eligible*

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- Balance of compute, memory, and network resources

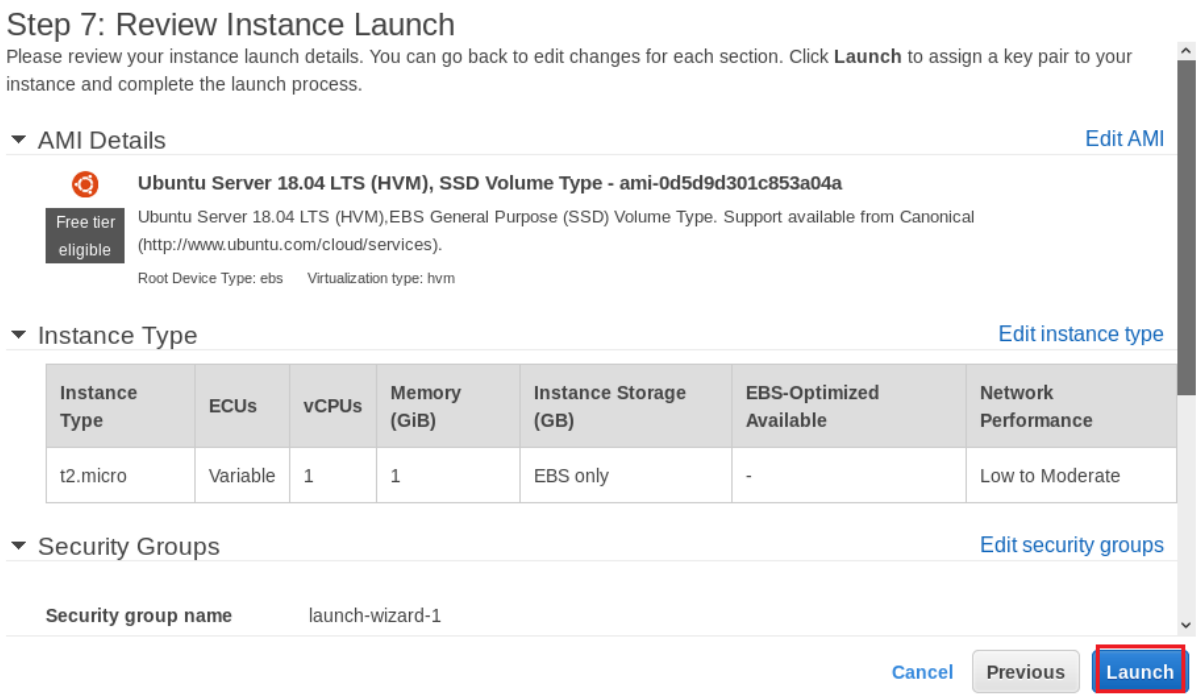
Read more from **here**

7. Once we click on “Review and Launch”, the rest of the options are left as they are, and we click on “launch”.



8. Now let’s launch the instance which will create a key pair to your instance and complete the launch process.

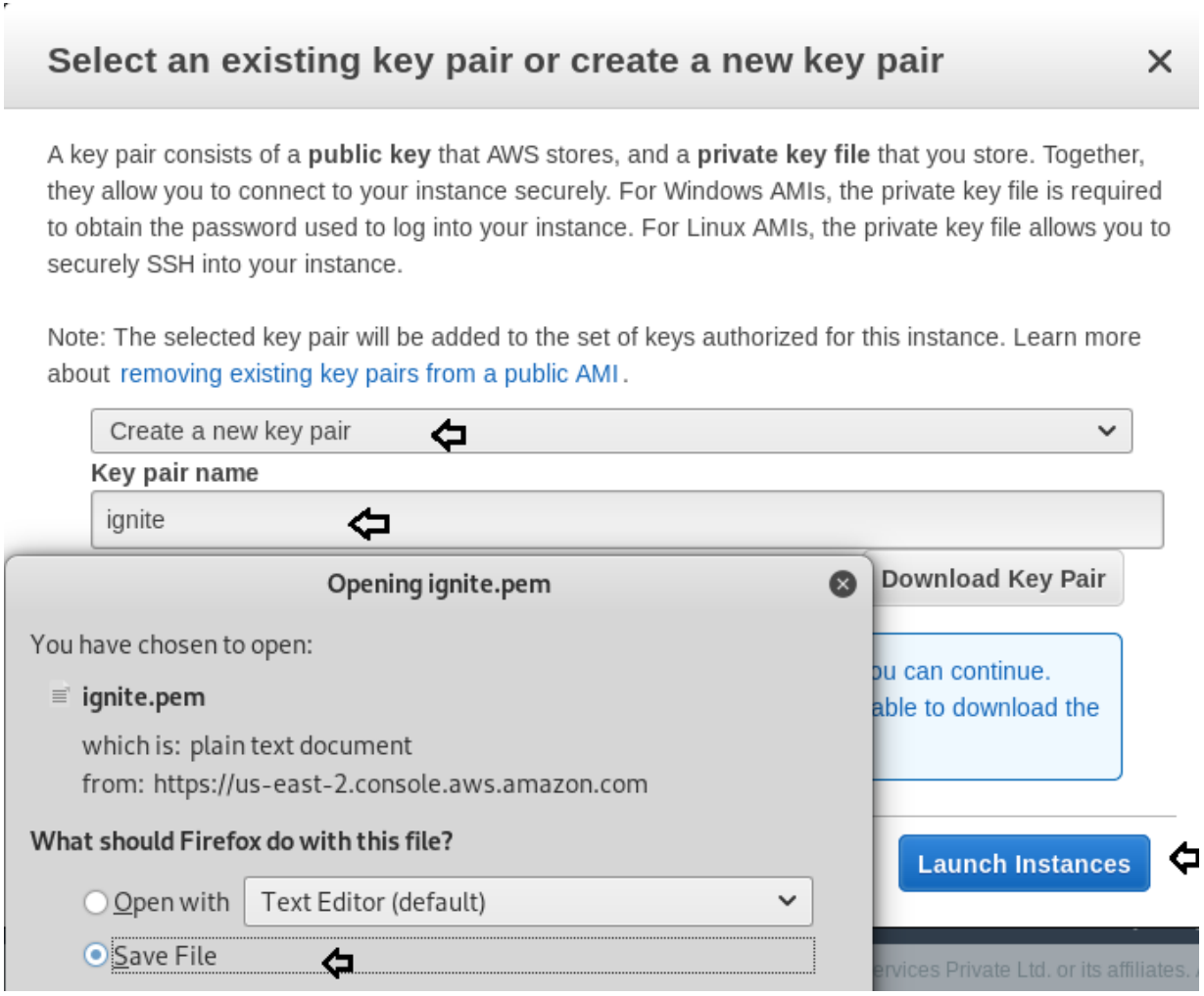
Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



This is a very important step, this is what makes it possible for you to connect to your instance over SSH, the key pair.

9. Choose “Create a new key pair”, give it a name, them download and save the **.pem** file somewhere where you can keep it safe.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

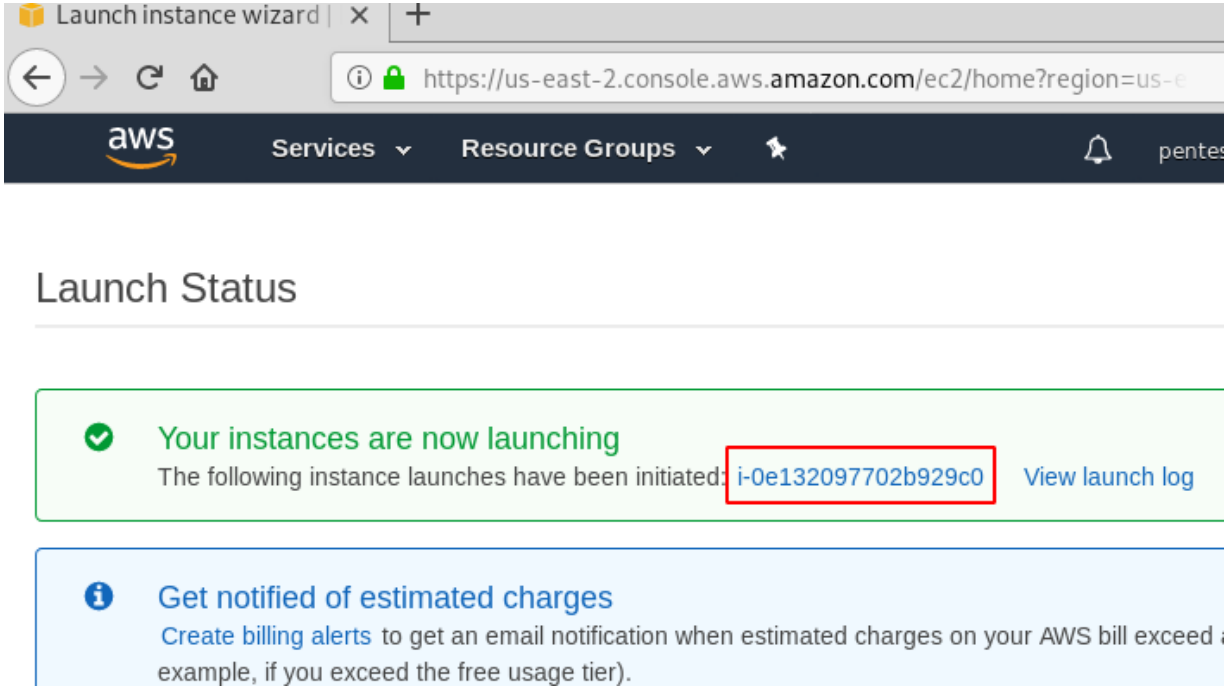


AWS gives you the launch status, tells you about the launch process and shows you that your instance is now launching.

10. Now click on “View Instances” to see what’s happing with our Ubuntu server. Note that it takes a few minutes for the server to be fully deployed, so be patient. Now we see under “Status check” that we have our 2/2 checks, this

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

essentially means that our instance is fully deployed and ready for us to connect to.

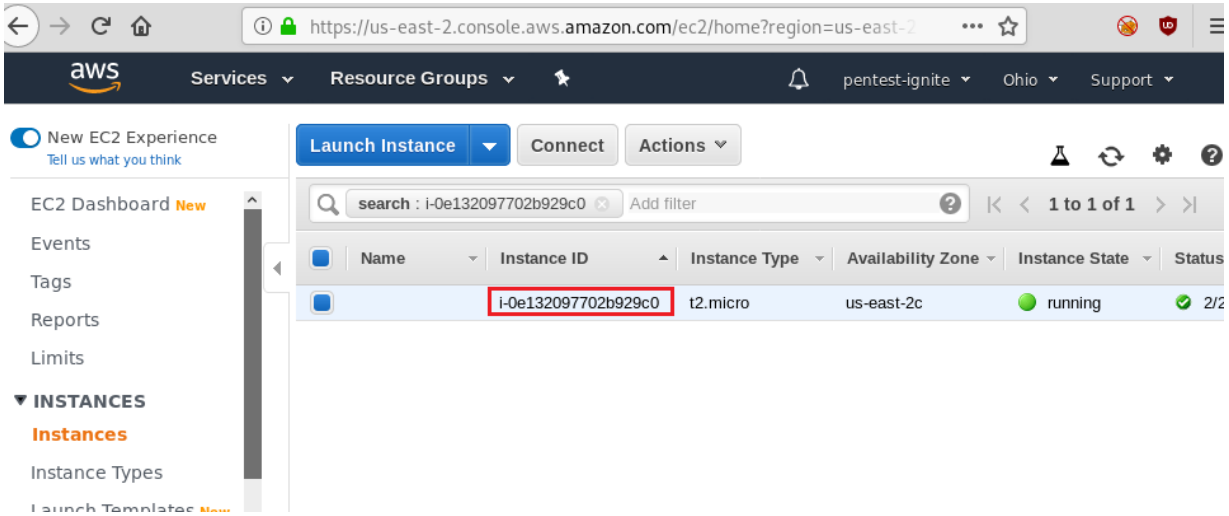


Deployment & Connectivity

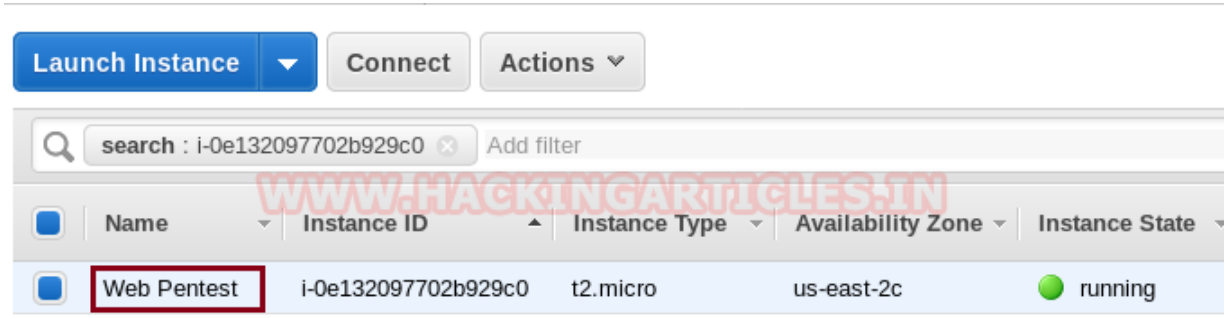
This is the good part, where we get to deploy and connect to our instance in AWS.

1. We choose our instance and click on “Connect”, this takes us to a page with options that defines how we want to connect to our instance, and we choose to connect using a standalone SSH client.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



2. Enter the name for your Instance ID, so that you can easily identify the instance ID from its name.



AWS is very helpful in giving us the particulars for our connection, like the commands to use.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Connect To Your Instance

I would like to connect with

- (•) A standalone SSH client
- ( ) EC2 Instance Connect (browser-based SSH connection)
- ( ) A Java SSH Client directly from my browser (Java required)

To access your instance:

1. Open an SSH client. (find out how to connect using PuTTY)
2. Locate your private key file (ignite.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:

```
chmod 400 ignite.pem
```

4. Connect to your instance using its Public DNS:

```
ec2-18-189-17-168.us-east-2.compute.amazonaws.com
```

Example:

```
ssh -i "ignite.pem" ubuntu@ec2-18-189-17-168.us-east-2.compute.amazonaws.com
```

Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.

If you need any assistance connecting to your instance, please see our connection documentation.

Close

There are many applications you can choose from to connect to the instance, we are connecting to it from Kali Linux.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

3. We first make sure that the **.pem** file that we saved has the right permissions assigned to it, in this case, it needs to be only 'read'. Once that is done, we put in the SSH particulars provided by AWS.

```
Syntax: ssh -I "key.pem" AMIuser@instance-Public-DNS
```

4. The .pem file is defined so that the SSH operation knows where the keys are located and that's it, we are in!!. We connect and get to root.

```
root@kali:~# ssh -i "ignite.pem" ubuntu@ec2-18-189-17-168.us-east-2.compute.amazonaws.com
The authenticity of host 'ec2-18-189-17-168.us-east-2.compute.amazonaws.com (18.189.17.168)
ECDSA key fingerprint is SHA256:iFKlp5UChPtdSGaCIiuMcON1EtJ3RibdQ5koCbiJFik.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-18-189-17-168.us-east-2.compute.amazonaws.com,18.189.17.168
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-1051-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Nov 29 15:40:49 UTC 2019

  System load:  0.0               Processes:           85
  Usage of /:   13.6% of 7.69GB   Users logged in:     0
  Memory usage: 14%               IP address for eth0: 172.31.43.31
  Swap usage:   0%

0 packages can be updated.
0 updates are security updates.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-43-31:~$ sudo bash
root@ip-172-31-43-31:~#
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Install Dependencies required for Pentest-lab

Ubuntu is up and running now, let's start it for our pentest purposes, in order to do that we need to have the basic dependencies installed so that we can access web application like DVWA, etc.

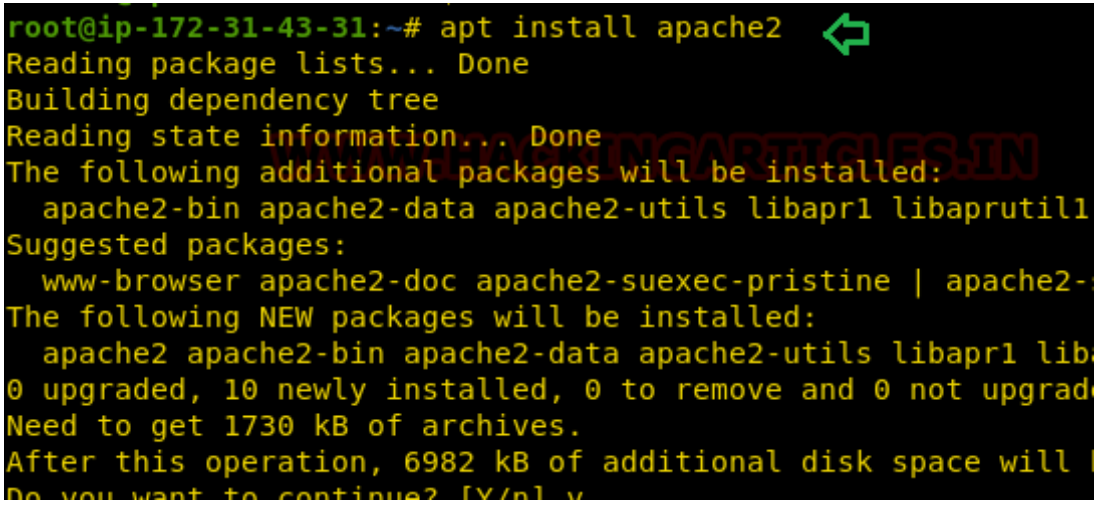
Apache

First, we will install the Apache. Apache is the most commonly used Web server on Linux Systems. Web servers are used to serve web pages requested by the client computers.

1. So, let's first install Apache in the ubuntu by the following command.

```
apt install apache2
```

We have successfully installed apache2, by default apache runs on port 80

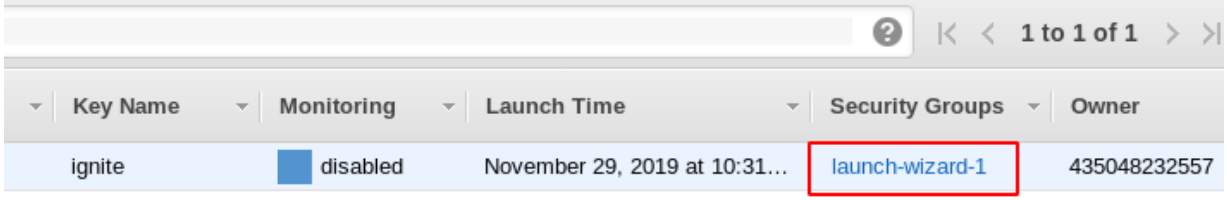


For Apache to function properly we need to open port 80, so let's get to it. We need to edit the security group in order for the Apache service to work. Ports are

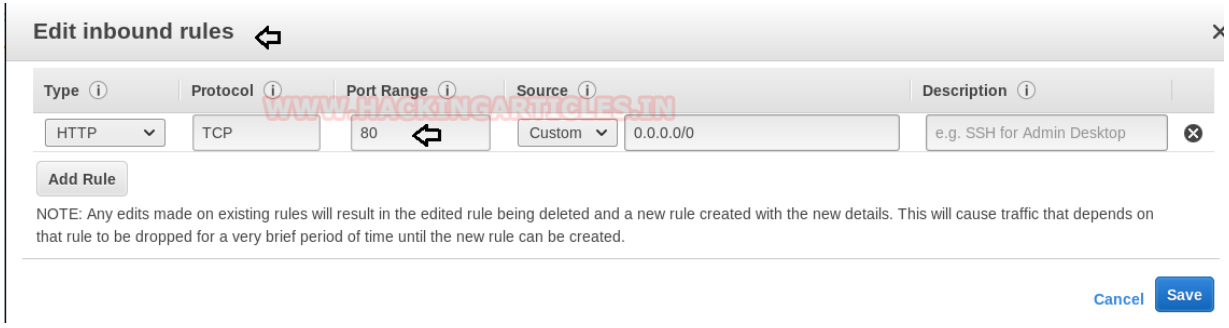
Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

closed by default in AWS, so we can define what we want open.

2. Go to your instance and launch the **security groups wizard-1**.
3. Edit the inbound rules and add HTTP, using TCP protocol over port 80.

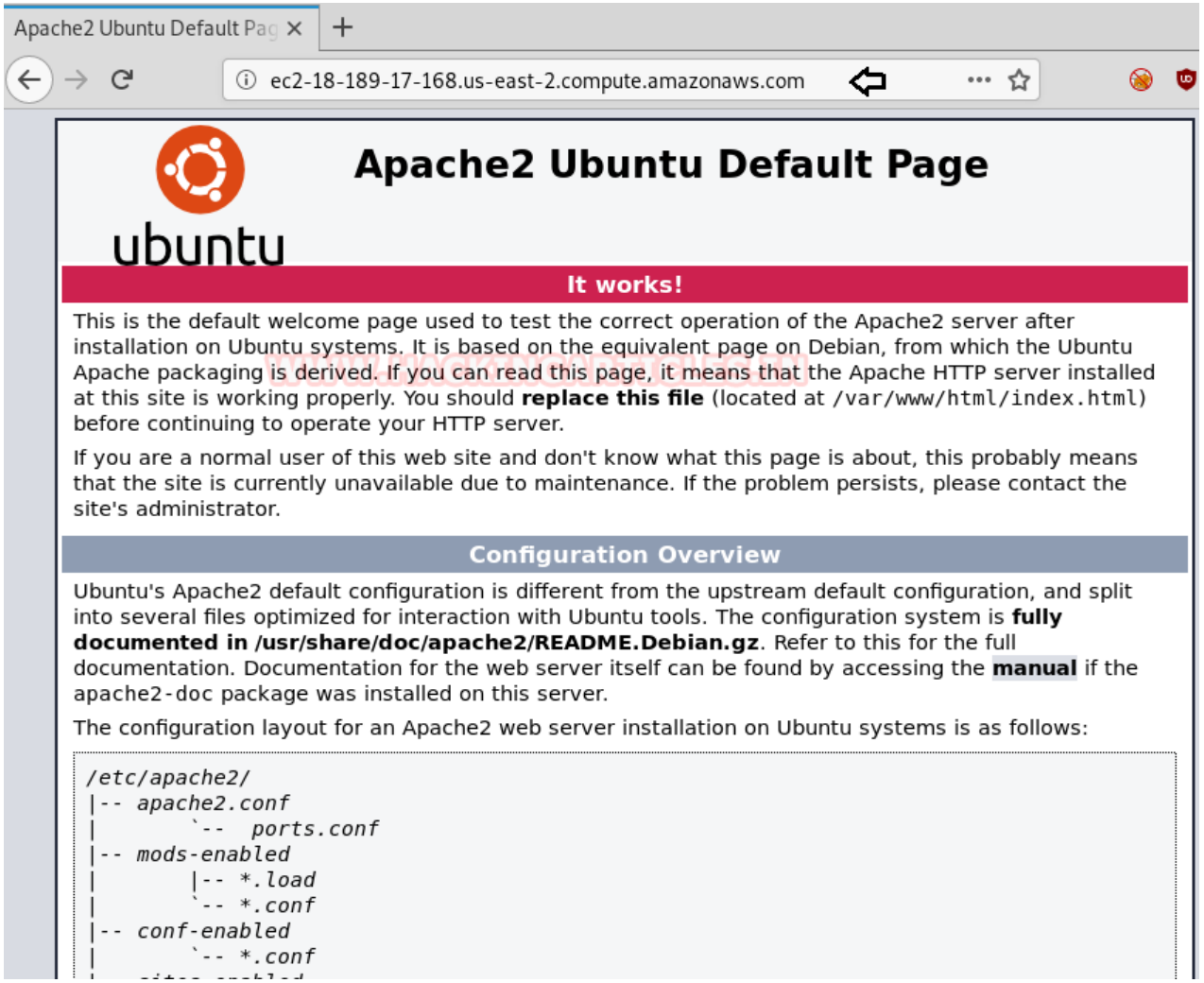


4. The rule has been added, now click on save.



5. Now to validate that Apache is running on our Ubuntu server, we access the IP of the instance in a browser.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



MySQL – Server

The next step is to install MySql-server. This is fairly simple, just type in the command and let Ubuntu do the rest.

```
apt install mysql-server
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
root@ip-172-31-43-31:~# apt install mysql-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libaio1 libcgi-fast-perl libcgi-pm-perl libencode-locale-perl libe
  libio-html-perl liblwp-mediatypes-perl libtimedate-perl liburi-per
Suggested packages:
  libdata-dump-perl libipc-sharedcache-perl libwww-perl mailx tinyca
The following NEW packages will be installed:
  libaio1 libcgi-fast-perl libcgi-pm-perl libencode-locale-perl libe
  libio-html-perl liblwp-mediatypes-perl libtimedate-perl liburi-per
0 upgraded, 21 newly installed, 0 to remove and 53 not upgraded.
Need to get 19.7 MB of archives.
After this operation, 156 MB of additional disk space will be used.
```

PHP

Installing PHP 7.2, simply type the following command.

```
apt install php7.2
```

```
root@ip-172-31-43-31:~# apt install php7.2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libapache2-mod-php7.2 libsodium23 php-common php7.2-cli ph
Suggested packages:
  php-pear
The following NEW packages will be installed:
  libapache2-mod-php7.2 libsodium23 php-common php7.2 php7.2
0 upgraded, 9 newly installed, 0 to remove and 53 not upgrad
Need to get 4007 kB of archives.
After this operation, 17.5 MB of additional disk space will
Do you want to continue? [Y/n] y
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Configuring MySQL

Let's configure MySQL so we have the right kind of credentials for our setup. After it gets logged in you will grant all the privileges to the user of Ubuntu as in our case we have given all the privileges to user raj which will be identified with the password of ubuntu which is 123 in our case and after which we will reset all the previous privileges so that it can start the service with the new changes. For this, the commands are the following.

```
mysql -u root -p
GRANT ALL PRIVILEGES ON *.* TO 'raj'@'%' IDENTIFIED BY '123' WITH GRANT
flush privileges;
```

```
root@ip-172-31-43-31:~# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.7.28-0ubuntu0.18.04.4 (Ubuntu)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> GRANT ALL PRIVILEGES ON *.* TO 'raj'@'%' IDENTIFIED BY '123' WITH GRANT OPTION;
Query OK, 0 rows affected, 1 warning (0.00 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
```

PHPMyAdmin

We need to install phpMyAdmin as well, here is how you do it.

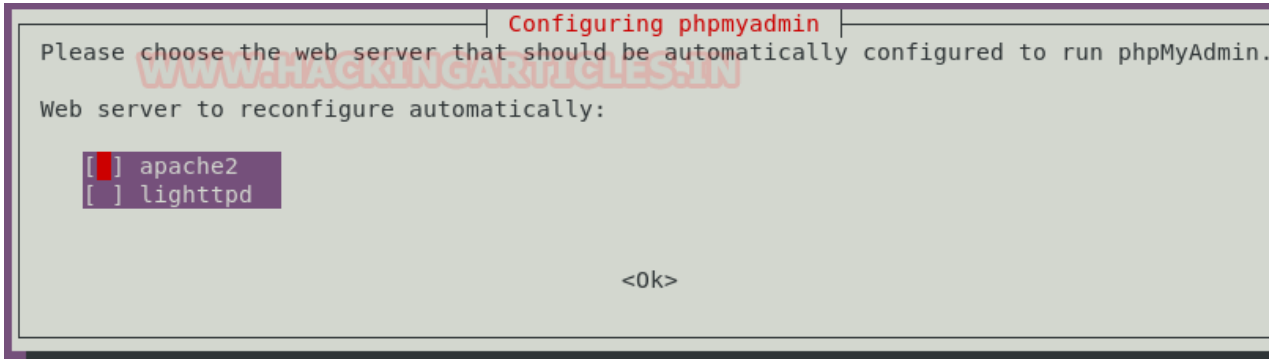
```
apt install phpmyadmin
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
root@ip-172-31-43-31:~# apt install phpmyadmin
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  dbconfig-common dbconfig-mysql fontconfig-config fonts-dejavu-
  libwebp6 libxpm4 libzip4 php-bz2 php-curl php-gd php-mbstring
  php7.2-xml php7.2-zip
Suggested packages:
  libgd-tools php-libsodium php-mcrypt php-gmp php-imagick www-b
The following NEW packages will be installed:
  dbconfig-common dbconfig-mysql fontconfig-config fonts-dejavu-
  libwebp6 libxpm4 libzip4 php-bz2 php-curl php-gd php-mbstring
  php7.2-xml php7.2-zip phpmyadmin
0 upgraded, 36 newly installed, 0 to remove and 53 not upgraded.
```

Phpmyadmin needs to be configured, it needs to know that we want to use apache2 as our web server.

Next, we need to give it the password that we kept while setting up MySQL.



Lab Setup

We are done with installing all the dependencies for our setup and are now ready to install our pentest labs.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

DVWA

let's navigate to the "html" folder to download and install DVWA. Once that is done, we need to move the config.inc.php.dist file for further configurations.

```
cd /var/www/html
git clone https://github.com/ethicalhack3r/DVWA
cd /dvwa/config
mv config.inc.php.dist config.inc.php
```

```
root@ip-172-31-43-31:~# cd /var/www/html
root@ip-172-31-43-31:/var/www/html# git clone https://github.com/ethicalhack3r/DVWA
Cloning into 'DVWA'...
remote: Enumerating objects: 2995, done.
remote: Total 2995 (delta 0), reused 0 (delta 0), pack-reused 2995
Receiving objects: 100% (2995/2995), 1.52 MiB | 12.04 MiB/s, done.
Resolving deltas: 100% (1318/1318), done.
root@ip-172-31-43-31:/var/www/html# cd DVWA/
root@ip-172-31-43-31:/var/www/html/DVWA# ls
CHANGELOG.md  README.md  config  dvwa      favicon.ico  ids_log.php  instructions.php  logou
COPYING.txt   about.php  docs    external  hackable     index.php    login.php         php.i
root@ip-172-31-43-31:/var/www/html/DVWA# cd config/
root@ip-172-31-43-31:/var/www/html/DVWA/config# ls
config.inc.php.dist
root@ip-172-31-43-31:/var/www/html/DVWA/config# mv config.inc.php.dist config.inc.php
root@ip-172-31-43-31:/var/www/html/DVWA/config#
```

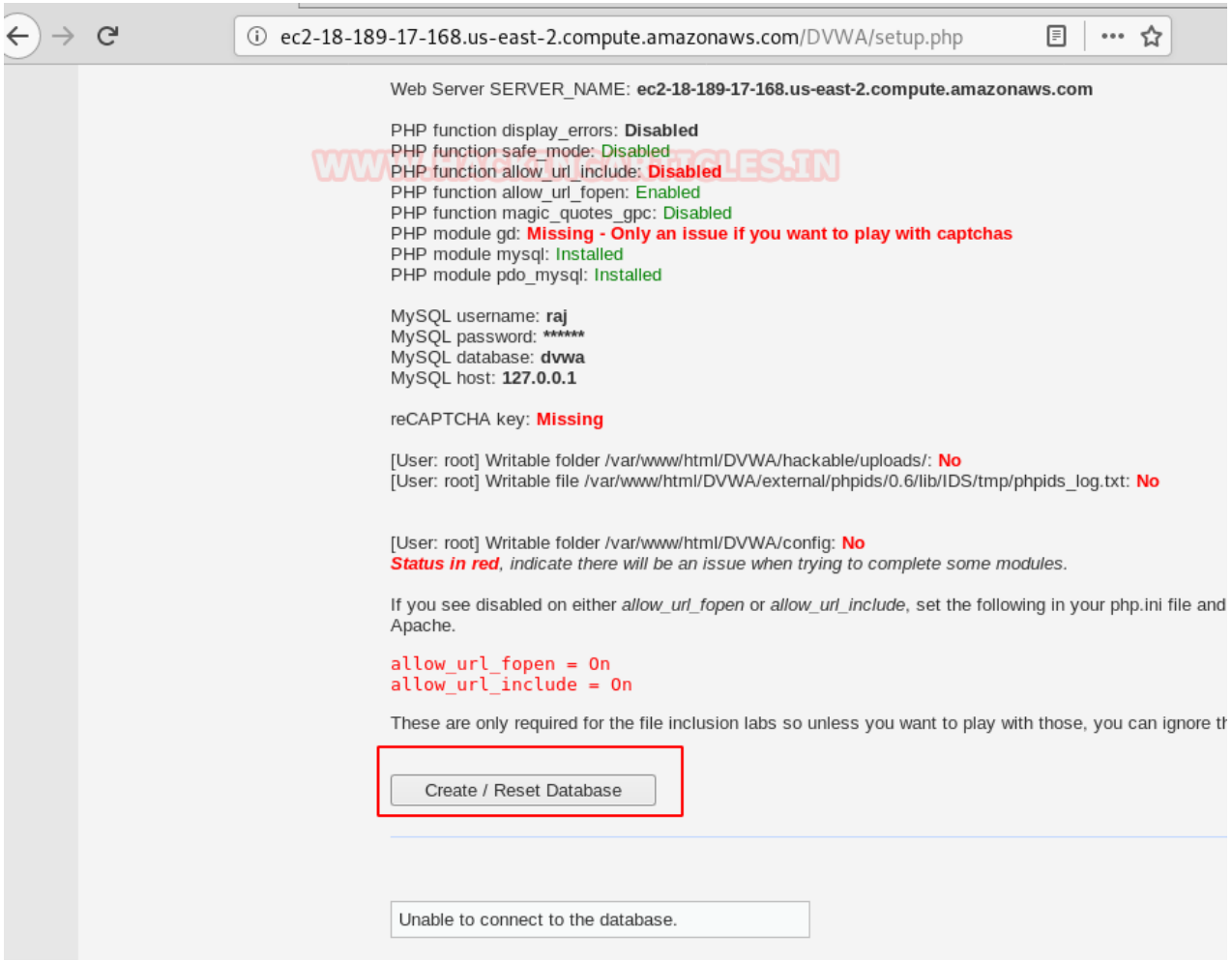
Open the **config.inc.php** file in a text editor and put in the database credentials that we had set up earlier. We only need to modify 2 fields: db_user and db_password.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE E
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must u
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'raj';
$_DVWA[ 'db_password' ] = '123';

# Only used with PostgreSQL/PGSQL database selection.
$_DVWA[ 'db_port '] = '5432';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.googl
```

Now we open DVWA in our web browser and click on “Create/Reset Database”.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Time, to login to our DVWA!

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

SQL Injection – Dhakkan

Our vulnerable web app is up and running, now we want to install a lab for SQL injections, we will be using the Dhakkan sqli lab.

Here's how to set it up. We download it into the html folder to host it, next we move the "sqlilabs" folder to the "sqli". Next, we need to edit the database credentials so that the lab can function properly. Open the db-creds.inc file in a text editor.

```
git clone http://github.com/Rinkish/Sqli_Edited_Version
cd Sqli_Edited_Version/
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
ls
mv sqlilabs/ ../sqli
cd sqli
cd sql-connections/
```

```
root@ip-172-31-43-31:/var/www/html# git clone http://github.com/Rinkish/Sqli_Edited_Version
Cloning into 'Sqli_Edited_Version'...
warning: redirecting to https://github.com/Rinkish/Sqli_Edited_Version/
remote: Enumerating objects: 406, done.
remote: Total 406 (delta 0), reused 0 (delta 0), pack-reused 406
Receiving objects: 100% (406/406), 6.39 MiB | 13.03 MiB/s, done.
Resolving deltas: 100% (81/81), done.
root@ip-172-31-43-31:/var/www/html# ls
DVWA  Sqli_Edited_Version  index.html
root@ip-172-31-43-31:/var/www/html# cd Sqli_Edited_Version/
root@ip-172-31-43-31:/var/www/html/Sqli_Edited_Version# ls
README.md  sqlilabs
root@ip-172-31-43-31:/var/www/html/Sqli_Edited_Version# mv sqlilabs/ /var/www/html/sqli
root@ip-172-31-43-31:/var/www/html/Sqli_Edited_Version# cd ..
root@ip-172-31-43-31:/var/www/html# cd sqli
root@ip-172-31-43-31:/var/www/html/sqli# ls
 Less-1    Less-15   Less-20   Less-25a  Less-28a  Less-33   Less-39   Less-44   Less-5    Less-55   Le
 Less-10   Less-16   Less-21   Less-26   Less-29   Less-34   Less-4    Less-45   Less-50   Less-56   Le
 Less-11   Less-17   Less-22   Less-26a  Less-3    Less-35   Less-40   Less-46   Less-51   Less-57   Le
 Less-12   Less-18   Less-23   Less-27   Less-30   Less-36   Less-41   Less-47   Less-52   Less-58   Le
 Less-13   Less-19   Less-24   Less-27a  Less-31   Less-37   Less-42   Less-48   Less-53   Less-59   Le
 Less-14   Less-2    Less-25   Less-28   Less-32   Less-38   Less-43   Less-49   Less-54   Less-6    Le
root@ip-172-31-43-31:/var/www/html/sqli# cd sql-connections/
root@ip-172-31-43-31:/var/www/html/sqli/sql-connections# ls
db-creds.inc  functions.php  setup-db-challenge.php  setup-db.php  sql-connect-1.php  sql-connect.php  sq
root@ip-172-31-43-31:/var/www/html/sqli/sql-connections#
```

Now that the file is open, we put in the username and password.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
<?php

//give your mysql connection username n password
$dbuser ='raj';
$dbpass ='123';
$dbname ="security";
$host = 'localhost';
$dbname1 = "challenges";


?>
```

Now browse this web application from through this Public-DNS/sqli and click on Setup/reset Databases for labs. Now the sqli lab is ready to use.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Success! Sqli is up and running.

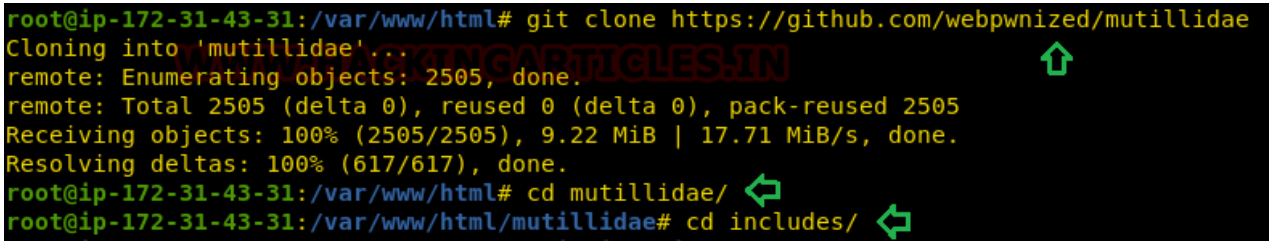
Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

OWASP Mutillidae II

Last but not least, we will install OWASP Mutillidae II and that will conclude our setup for now.

So, let's start by navigating to the "html" folder and downloading Mutillidae. Once downloaded, we navigate to the "includes" folder.

```
1 git clone https://github.com/webpwnized/mutillidae
2 cd mutillidae
3 cd includes
4 ls
5 nano database-config.inc
```



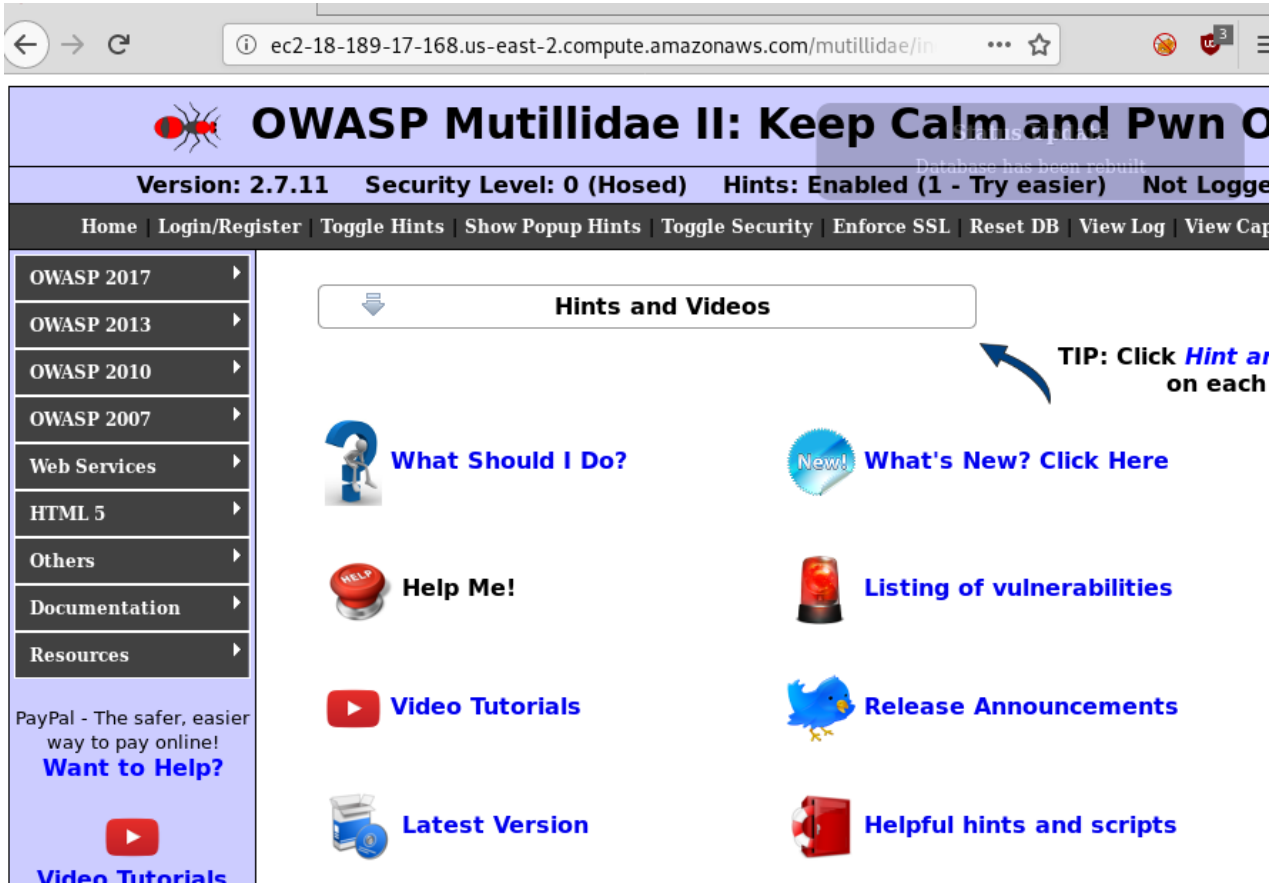
Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Once in, modify the database access file to prove the credentials we had set up earlier.

```
<?php
define('DB_HOST', '127.0.0.1');
define('DB_USERNAME', 'raj');
define('DB_PASSWORD', '123');
define('DB_NAME', 'mutillidae');
?>
```

Now we will open this our local browser by the following URL: Public-DNS/mutillidae where we will find an option of reset database. Just click on it to reset the database. Let's launch Mutillidae using our browser.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD



Voila!! Your Ubuntu instance is ready for you to start your AWS pentest journey. You have your connectivity, dependencies and labs all configured and ready to go.

We at Hacking Articles always try to bring you the most industry-relevant content. Since the cloud is now the thing most companies are moving towards and raising curiosity about ways to keep the cloud secure, this is article is just to get you ready for our new articles on cloud penetration testing, so stay tuned.

Have fun and stay ethical.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

About The Author

Abhimanyu Dev is a Certified Ethical Hacker, penetration tester, information security analyst and researcher. Connect with him **here**

Share this:

Like this:

Loading...

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

NEXT POST

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

← LINUX PRIVILEGE ESCALATION USING CAPABILITIES

WINDOWS FOR PENTESTER: CERTUTIL →

2 Comments → WEB APPLICATION PENTEST LAB SETUP ON AWS

BAIDY December 3, 2019 at 8:36 pm

Thanks again Raj … This is a great article

REPLY ↓

RAJ CHANDEL December 4, 2019 at 4:24 am

thank you very much. keep visitng

REPLY ↓

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Name *

Email *

Website

Notify me of follow-up comments by email.

Notify me of new posts by email.

POST COMMENT

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD