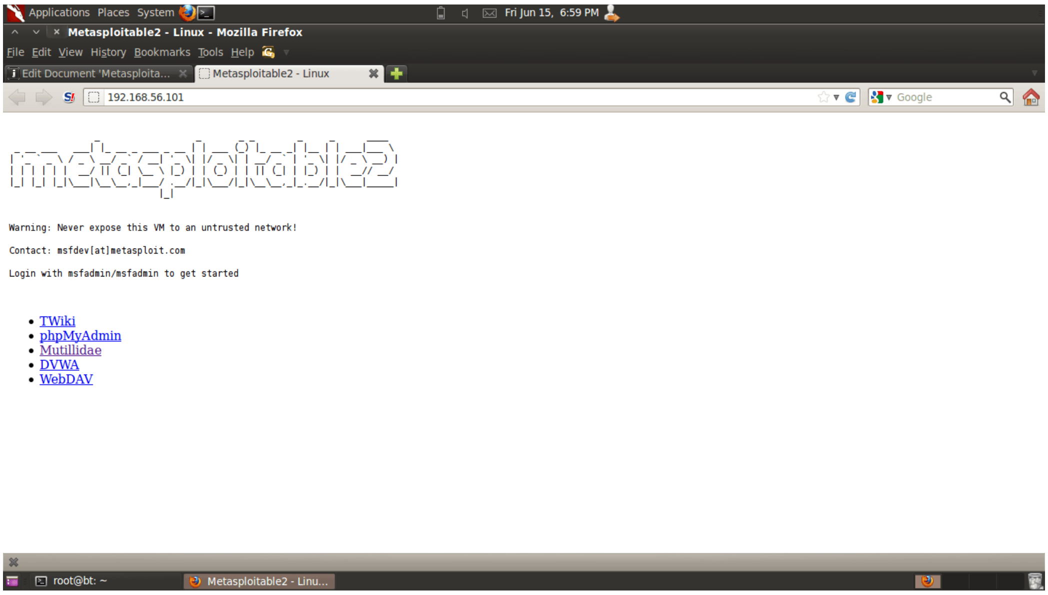
TASK-5

Vulnerable Web Services

Metasploitable 2 has deliberately vulnerable web applications pre-installed. The web server starts automatically when Metasploitable 2 is booted. To access the web applications, open a web browser and enter the URL http://<IP> where <IP> is the IP address of Metasploitable 2. One way to accomplish this is to install Metasploitable 2 as a guest operating system in Virtual Box and change the network interface settings from "NAT" to "Host Only". (Note: A video tutorial on installing Metasploitable 2 is available here.)

In this example, Metasploitable 2 is running at IP 192.168.56.101. Browsing to http://192.168.56.101/ shows the web application home page.


Applications Places System
Fri Jun 15, 6:59 PM
Metasploitable2 - Linux - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Edit Document 'Metasploita...
Metasploitable2 - Linux
192.168.56.101
Google
root@bt: ~
Metasploitable2 - Linu...

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

192.168.56/24 is the default "host only" network in Virtual Box. IP address are assigned starting from "101". Depending on the order in which guest operating systems are started, the IP address of Metasploitable 2 will vary.

To access a particular web application, click on one of the links provided. Individual web applications may additionally be accessed by appending the application directory name onto http://<IP> to create URL http://<IP>/<Application Folder>/. For example, the Mutillidae application may be accessed (in this example) at address http://192.168.56.101/mutillidae/. The applications are installed in Metasploitable 2 in the /var/www directory. (Note: See a list with command ls /var/www.) In the current version as of this writing, the applications are

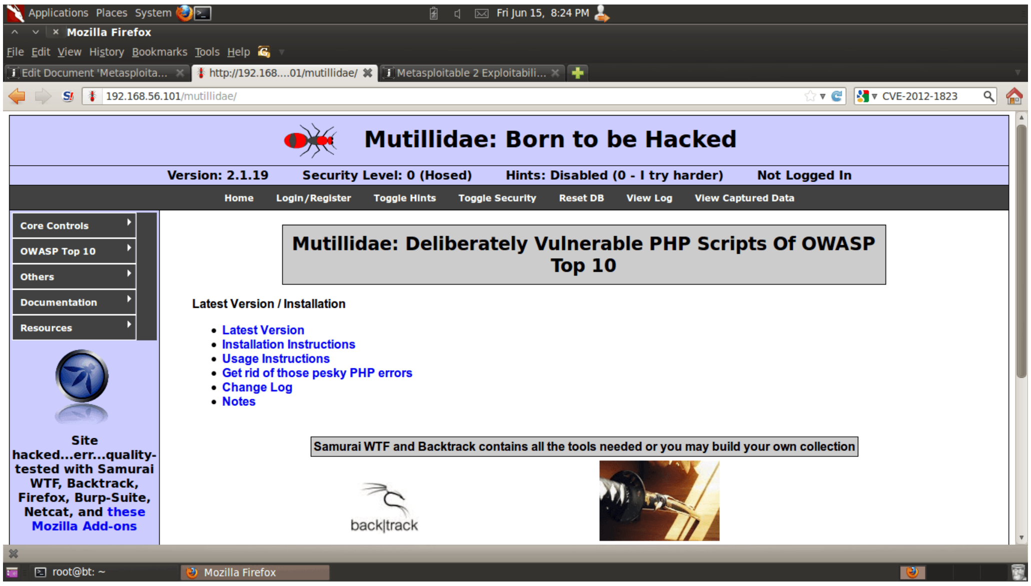
- mutillidae (NOWASP Mutillidae 2.1.19)
- dvwa (Damn Vulnerable Web Application)
- phpMyAdmin
- tikiwiki (TWiki)

- tikiwiki-old
- dav (WebDav)

Mutillidae

The Mutillidae web application (NOWASP (Mutillidae)) contains all of the vulnerabilities from the OWASP Top Ten plus a number of other vulnerabilities such as HTML-5 web storage, forms caching, and click-jacking. Inspired by DVWA, Mutillidae allows the user to change the "Security Level" from 0 (completely insecure) to 5 (secure). Additionally three levels of hints are provided ranging from "Level 0 - I try harder" (no hints) to "Level 2 - noob" (Maximum hints). If the application is damaged by user injections and hacks, clicking the "Reset DB" button resets the application to its original state.

Tutorials on using Mutillidae are available at the webpwnized YouTube Channel.



Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

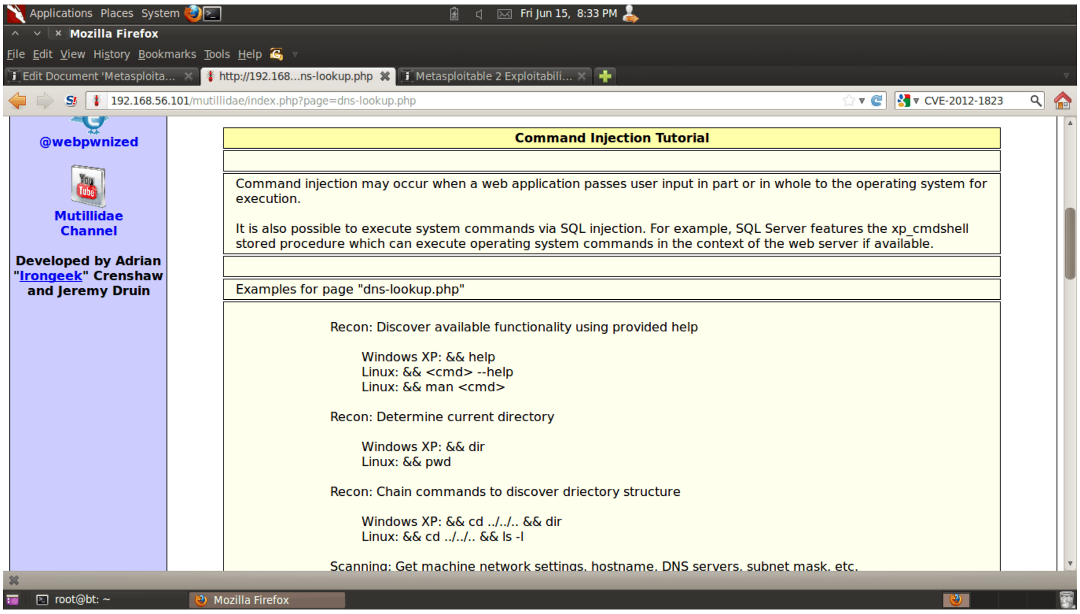
Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

Enable hints in the application by click the "Toggle Hints" button on the menu bar:


Applications Places System
Fri Jun 15, 8:33 PM
Mozilla Firefox
File Edit View History Bookmarks Tools Help
Edit Document 'Metasploita...
http://192.168...ns-lookup.php
Metasploitable 2 Exploitabili...
192.168.56.101/mutillidae/index.php?page=dns-lookup.php
CVE-2012-1823
@webpwnized
Mutillidae Channel
root@bt: ~
Mozilla Firefox

Developed by Adrian "Irongeek" Crenshaw and Jeremy Druin

Command Injection Tutorial

Command injection may occur when a web application passes user input in part or in whole to the operating system for execution.

It is also possible to execute system commands via SQL injection. For example, SQL Server features the xp_cmdshell stored procedure which can execute operating system commands in the context of the web server if available.

Examples for page "dns-lookup.php"

```
Recon: Discover available functionality using provided help

     Windows XP: && help
     Linux: && <cmd> --help
     Linux: && man <cmd>

Recon: Determine current directory

     Windows XP: && dir
     Linux: && pwd

Recon: Chain commands to discover driectory structure

     Windows XP: && cd ../../.. && dir
     Linux: && cd ../../.. && ls -l

Scanning: Get machine network settings, hostname, DNS servers, subnet mask, etc.
```

The Mutillidae application contains at least the following vulnerabilities on these respective pages:

Page	Vulnerabilities
add-to-your-blog.php	SQL Injection on blog entry SQL Injection on logged in user name Cross site scripting on blog entry Cross site scripting on logged in user name Log injection on logged in user name CSRF JavaScript validation bypass XSS in the form title via logged in username The show-hints cookie can be changed by user to enable hints even though they are not supposed to show in secure mode
arbitrary-file-inclusion.php	System file compromise Load any page from any site
browser-info.php	XSS via referer HTTP header JS Injection via referer HTTP header XSS via user-agent string HTTP header
capture-data.php	XSS via any GET, POST, or Cookie
captured-data.php	XSS via any GET, POST, or Cookie
config.inc*	Contains unencrytped database credentials
credits.php	Unvalidated Redirects and Forwards
dns-lookup.php	Cross site scripting on the host/ip field O/S Command injection on the host/ip field This page writes to the log. SQLi and XSS on the log are possible GET for POST is possible because only reading POSTed variables is not enforced.
footer.php*	Cross site scripting via the HTTP_USER_AGENT HTTP header.
framing.php	Click-jacking
header.php*	XSS via logged in user name and signature The Setup/reset the DB menu item can be enabled by setting the uid value of the cookie to 1
html5-storage.php	DOM injection on the add-key error message because the key entered is output into the error message without being encoded
index.php*	You can XSS the hints-enabled output in the menu because it takes input from the hints-enabled cookie value. You can SQL injection the UID cookie value because it is used to do a lookup You can change your rank to admin by altering the UID value HTTP Response Splitting via the logged in user name because it

Page	Vulnerabilities
	is used to create an HTTP Header This page is responsible for cache-control but fails to do so This page allows the X-Powered-By HTTP header HTML comments There are secret pages that if browsed to will redirect user to the phpinfo.php page. This can be done via brute forcing
log-visit.php	SQL injection and XSS via referer HTTP header SQL injection and XSS via user-agent string
login.php	Authentication bypass SQL injection via the username field and password field SQL injection via the username field and password field XSS via username field JavaScript validation bypass
password-generator.php	JavaScript injection
pen-test-tool-lookup.php	JSON injection
phpinfo.php	This page gives away the PHP server configuration Application path disclosure Platform path disclosure
process-commands.php	Creates cookies but does not make them HTML only
process-login-attempt.php	Same as login.php. This is the action page.
redirectandlog.php	Same as credits.php. This is the action page
register.php	SQL injection and XSS via the username, signature and password field
rene-magritte.php	Click-jacking
robots.txt	Contains directories that are supposed to be private
secret-administrative-pages.php	This page gives hints about how to discover the server configuration
set-background-color.php	Cascading style sheet injection and XSS via the color field
show-log.php	Denial of Service if you fill up the log XSS via the hostname, client IP, browser HTTP header, Referer HTTP header, and date fields
site-footer-xss-discusson.php	XSS via the user agent string HTTP header
source-viewer.php	Loading of any arbitrary file including operating system files.
text-file-viewer.php	Loading of any arbitrary web page on the Interet or locally including the sites password files. Phishing

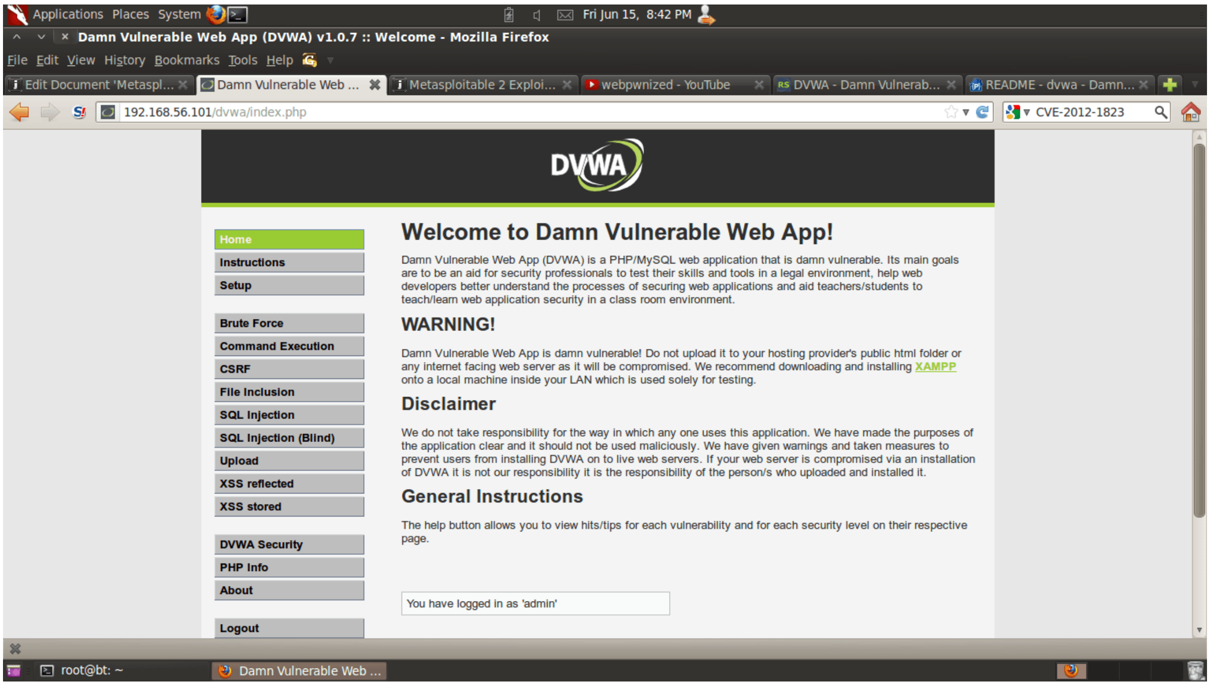
Page	Vulnerabilities
user-info.php	SQL injection to dump all usernames and passwords via the username field or the password field XSS via any of the displayed fields. Inject the XSS on the register.php page. XSS via the username field
user-poll.php	Parameter pollution GET for POST XSS via the choice parameter Cross site request forgery to force user choice
view-someones-blog.php	XSS via any of the displayed fields. They are input on the add to your blog page.

DVWA

From the DVWA home page: "Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.".

DVWA contains instructions on the home page and additional information is available at Wiki Pages - Damn Vulnerable Web App.

- **Default username** - admin
- **Default password** - password



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

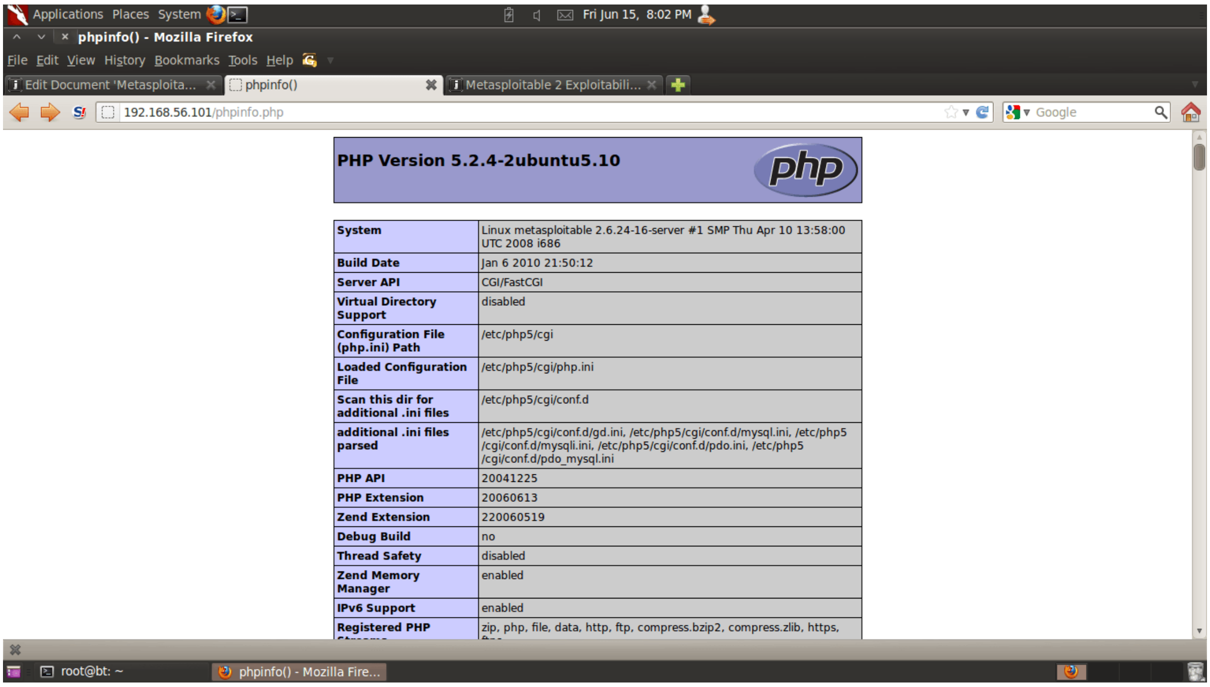
General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Information Disclosure

Additionally, an ill-advised PHP information disclosure page can be found at http://<IP>/phpinfo.php. In this example, the URL would be http://192.168.56.101/phpinfo.php. The PHP info information disclosure vulnerability provides internal system information and service version information that can be used to look up vulnerabilities. For example, noting that the version of PHP disclosed in the screenshot is version 5.2.4, it may be possible that the system is vulnerable to CVE-2012-1823 and CVE-2012-2311 which affected PHP before 5.3.12 and 5.4.x before 5.4.2.


Applications Places System
Fri Jun 15, 8:02 PM
phpinfo() - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Edit Document 'Metasploita...
phpinfo()
Metasploitable 2 Exploitabili...
192.168.56.101/phpinfo.php
Google
root@bt: ~
phpinfo() - Mozilla Fire...

PHP Version 5.2.4-2ubuntu5.10

System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https,

EXPLOITING A WEB SERVER:-

What we will need

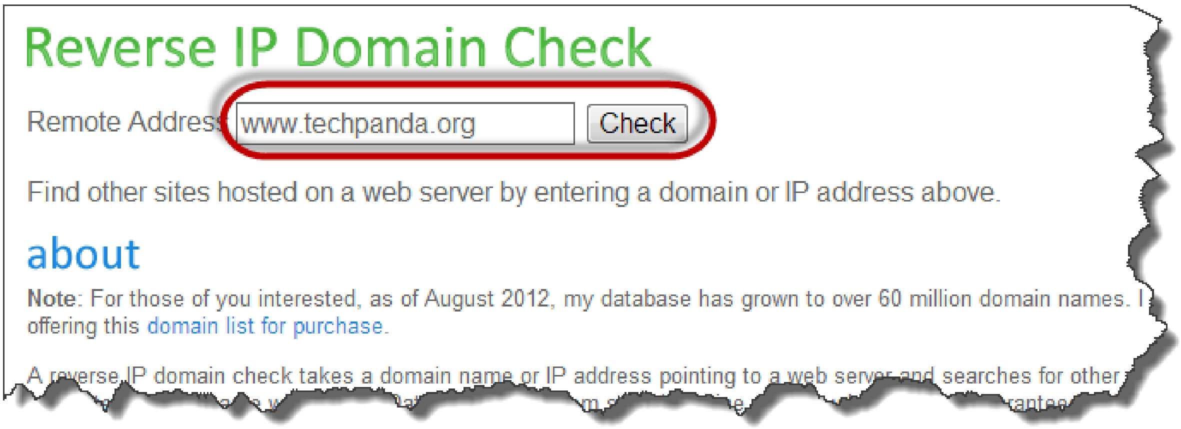
- A target www.techpanda.org
- Bing search engine
- SQL Injection Tools
- PHP Shell, we will use dk shell http://sourceforge.net/projects/icfdkshell/

Information gathering

We will need to get the IP address of our target and find other websites that share the same IP address.

We will use an online tool to find the target's IP address and other websites sharing the IP address

- Enter the URL https://www.yougetsignal.com/tools/web-sites-on-web-server/ in your web browser
- Enter www.techpanda.org as the target



Reverse IP Domain Check

Remote Address www.techpanda.org Check

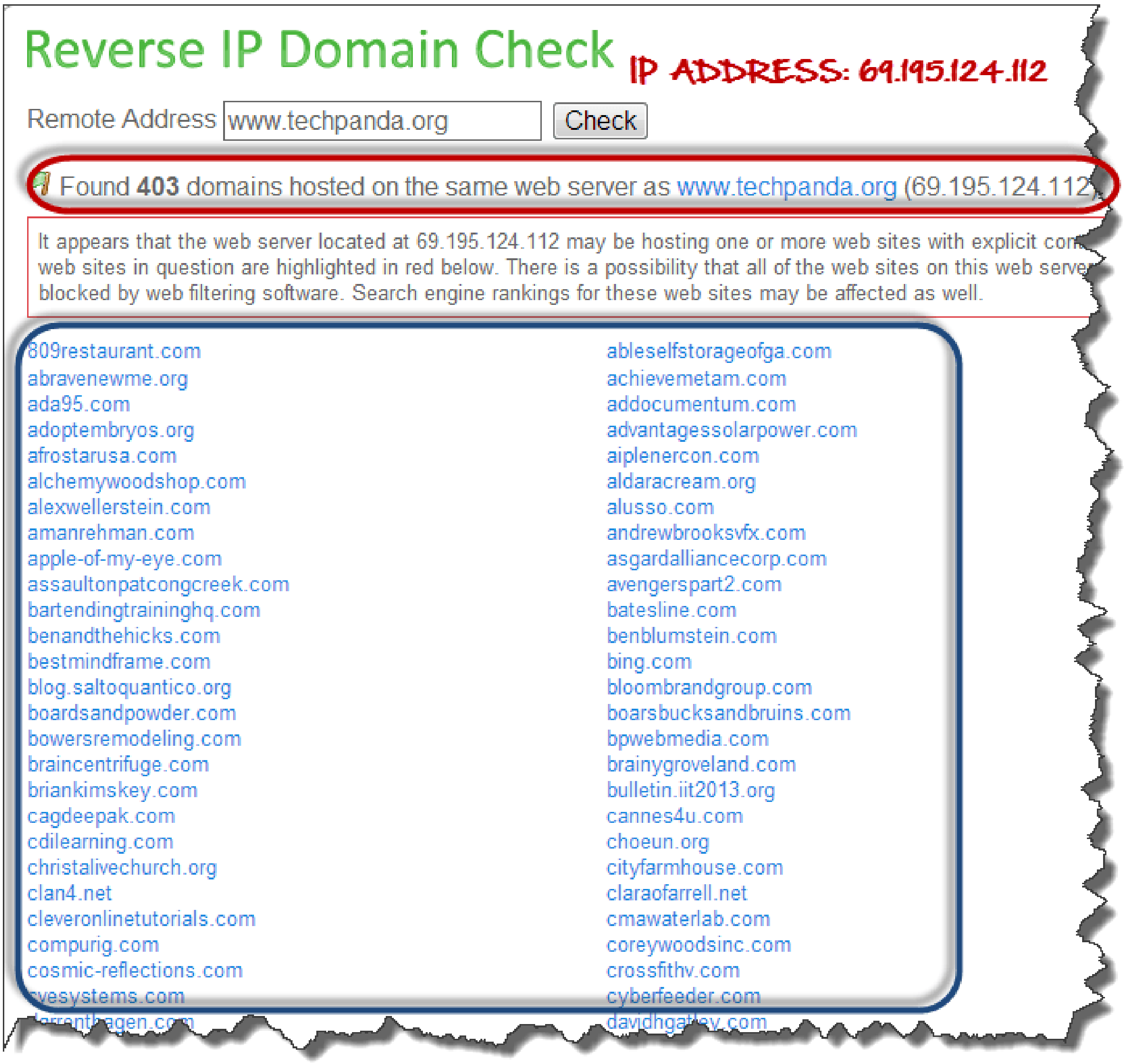
Find other sites hosted on a web server by entering a domain or IP address above.

about

Note: For those of you interested, as of August 2012, my database has grown to over 60 million domain names. I offering this domain list for purchase.

A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other

- Click on Check button
- You will get the following results



Reverse IP Domain Check

Remote Address www.techpanda.org Check

Found **403** domains hosted on the same web server as www.techpanda.org (69.195.124.112)

It appears that the web server located at 69.195.124.112 may be hosting one or more web sites with explicit con web sites in question are highlighted in red below. There is a possibility that all of the web sites on this web serve blocked by web filtering software. Search engine rankings for these web sites may be affected as well.

809restaurant.com ableselfstorageofga.com
abravenewme.org achievemetam.com
ada95.com addocumentum.com
adoptembryos.org advantagessolarpower.com
afrostarusa.com aiplenercon.com
alchemywoodshop.com aldaracream.org
alexwellerstein.com alusso.com
amanrehman.com andrewbrooksvfx.com
apple-of-my-eye.com asgardalliancecorp.com
assaultonpatcongcreek.com avengerspart2.com
bartendingtraininghq.com batesline.com
benandthehicks.com benblumstein.com
bestmindframe.com bing.com
blog.saltoquantico.org bloombrandgroup.com
boardsandpowder.com boarsbucksandbruins.com
bowersremodeling.com bpwebmedia.com
braincentrifuge.com brainygroveland.com
briankimskey.com bulletin.iit2013.org
cagdeepak.com cannes4u.com
cdilearning.com choeun.org
christalivechurch.org cityfarmhouse.com
clan4.net claraofarrell.net
cleveronlinetutorials.com cmawaterlab.com
compurig.com coreywoodsinc.com
cosmic-reflections.com crossfithv.com
cyesystems.com cyberfeeder.com
darrenthagen.com davidhgatley.com

Based on the above results, the IP address of the target is 69.195.124.112

We also found out that there are 403 domains on the same web server.

Our next step is to scan the other websites for SQL injection vulnerabilities. Note: if we can find a SQL vulnerable on the target, then we would directly exploit it without considering other websites.

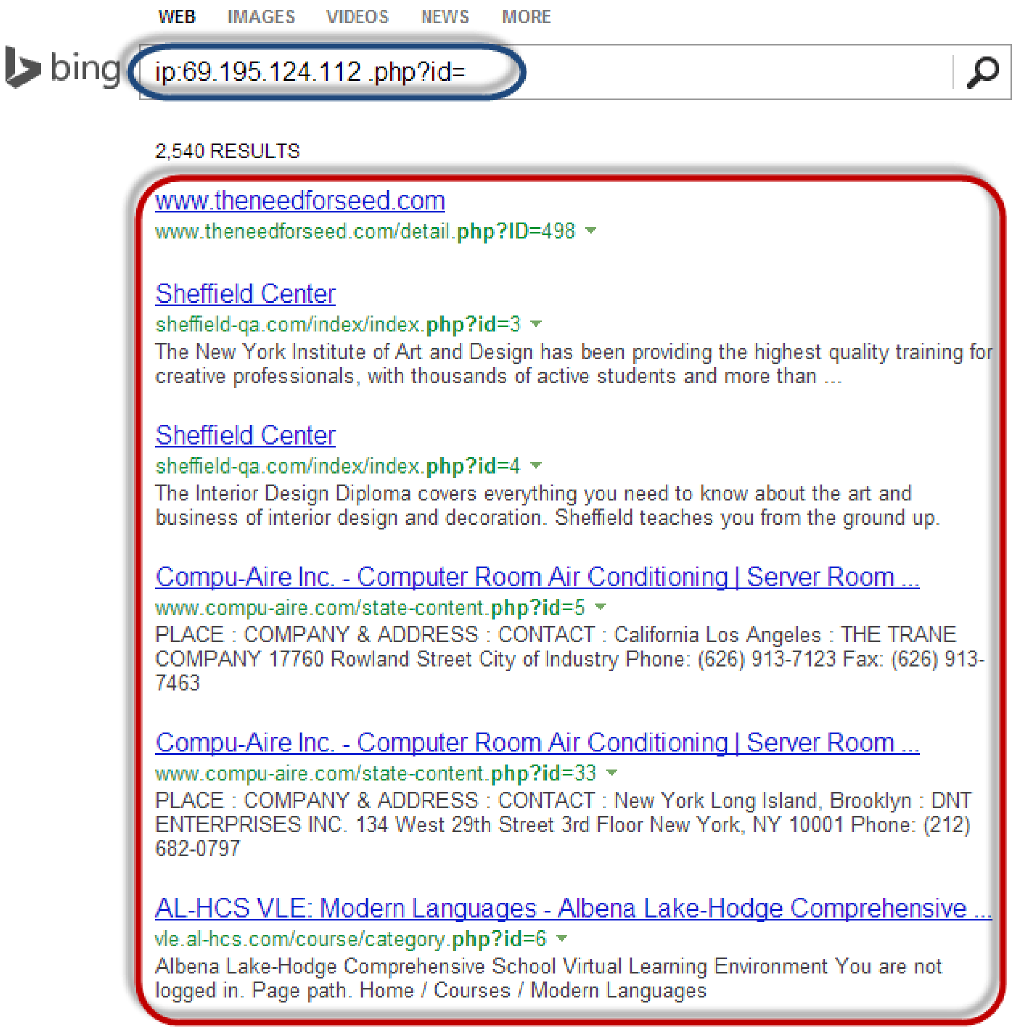
- Enter the URL www.bing.com into your web browser. This will only work with Bing so don't use other search engines such as google or yahoo
- Enter the following search query

ip:69.195.124.112 .php?id=

HERE,

- "ip:69.195.124.112" limits the search to all the websites hosted on the web server with IP address 69.195.124.112
- ".php?id=" search for URL GET variables used a parameters for SQL statements.

You will get the following results



ip:69.195.124.112 .php?id=

2,540 RESULTS

www.theneedforseed.com
www.theneedforseed.com/detail.php?ID=498

Sheffield Center
sheffield-qa.com/index/index.php?id=3
The New York Institute of Art and Design has been providing the highest quality training for creative professionals, with thousands of active students and more than …

Sheffield Center
sheffield-qa.com/index/index.php?id=4
The Interior Design Diploma covers everything you need to know about the art and business of interior design and decoration. Sheffield teaches you from the ground up.

Compu-Aire Inc. - Computer Room Air Conditioning | Server Room ...
www.compu-aire.com/state-content.php?id=5
PLACE : COMPANY & ADDRESS : CONTACT : California Los Angeles : THE TRANE COMPANY 17760 Rowland Street City of Industry Phone: (626) 913-7123 Fax: (626) 913-7463

Compu-Aire Inc. - Computer Room Air Conditioning | Server Room ...
www.compu-aire.com/state-content.php?id=33
PLACE : COMPANY & ADDRESS : CONTACT : New York Long Island, Brooklyn : DNT ENTERPRISES INC. 134 West 29th Street 3rd Floor New York, NY 10001 Phone: (212) 682-0797

AL-HCS VLE: Modern Languages - Albena Lake-Hodge Comprehensive ...
vle.al-hcs.com/course/category.php?id=6
Albena Lake-Hodge Comprehensive School Virtual Learning Environment You are not logged in. Page path. Home / Courses / Modern Languages

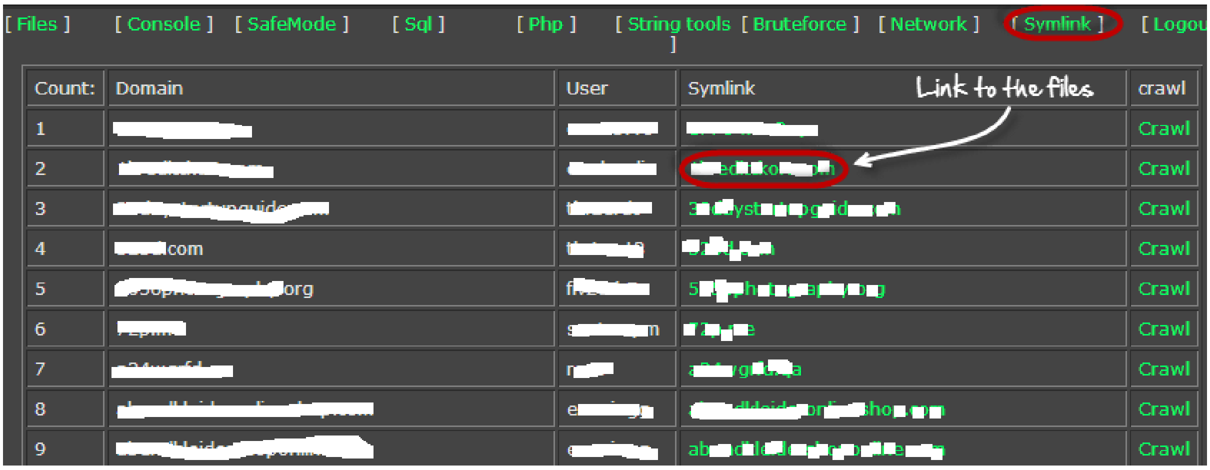
As you can see from the above results, all the websites using GET variables as parameters for SQL injection have been listed.

The next logic step would be to scan the listed websites for SQL Injection vulnerabilities. You can do this using manual SQL injection or use tools listed in this article on SQL Injection.

Uploading the PHP Shell

We will not scan any of the websites listed as this is illegal. Let's assume that we have managed to login into one of them. You will have to upload the PHP shell that you downloaded from http://sourceforge.net/projects/icfdkshell/

- Open the URL where you uploaded the dk.php file.
- You will get the following window



Link to the files

Count:	Domain	User	Symlink	crawl
1	[redacted]	[redacted]	[redacted]	Crawl
2	[redacted]	[redacted]	[redacted]	Crawl
3	[redacted]	[redacted]	[redacted]	Crawl
4	[redacted]	[redacted]	[redacted]	Crawl
5	[redacted]	[redacted]	[redacted]	Crawl
6	[redacted]	[redacted]	[redacted]	Crawl
7	[redacted]	[redacted]	[redacted]	Crawl
8	[redacted]	[redacted]	[redacted]	Crawl
9	[redacted]	[redacted]	[redacted]	Crawl

- Clicking the Symlink URL will give you access to the files in the target domain.

Once you have access to the files, you can get login credentials to the database and do whatever you want such as defacement, downloading data such as emails, etc.

Summary:-

- Web server stored valuable information and are accessible to the public domain. This makes them targets for attackers.
- The commonly used web servers include Apache and Internet Information Service IIS
- Attacks against web servers take advantage of the bugs and Misconfiguration in the operating system, web servers, and networks
- Popular web server hacking tools include Neosploit, MPack, and ZeuS.
- A good security policy can reduce the chances of been attacked