

# THEFORTITUDE

we45's Information Security Newsletter

February 15, 2011



we  
45  
data, fortified

About 'The Fortitude'  
Page 1

Your company needs a VAPT-A  
Case in study  
Page 2

Information Security -  
Leaders' Thought  
Page 4

Zone Transfers-  
Revealed  
Page 5



## About 'The Fortitude'

***True scholarship consists in knowing not what things exist, but what they mean; it is not memory but judgment.***

This quote by the American poet James Lowell Russell is something I found apt to introduce we45's newsletter - The Fortitude. Information Security is a subject that has grown in its importance today all over the world. Individuals and organizations are more interconnected through the web and its ever-expanding array of data and applications. While, this has ushered in a new wave in productivity, efficiency and business opportunities, it has also resulted in an unprecedented cyber-crimewave. Financial Information,

Personal Information and other sensitive information is being targeted by malicious individuals both inside and outside the organization. **Studies show that over 66% of companies in the country reported cyber-attacks and a whopping 51% reported repetitive attacks.**

we45 is a focused Information Security Solutions Company that delivers best-in-class security solutions and consulting for its clients. We believe that our rich experience in Information Security should benefit individuals and organizations all over.

The Fortitude is an Information Security focused journal which will delve into the latest information

security issues. We will bring you news and views from the world of Information Security and equip you with the knowledge to not only be aware of the multifarious threats to critical information but also how it could affect you or your organization.

We will bring our expertise and some industry expertise on a plethora of topics on Information Security to help you keep your environment, as you would want to. **Truly fortified.**

# Your Company needs a VAPT

## A Case in study

By Abhay Bhargav

CTO, we45 Solutions India Pvt Ltd.

February 15, 2011

**IT is a key component of any business today.**

However, how many organizations really know whether their IT environments are actually secure against the countless threats of today? The answer to that is, 'a select few'. Most organizations today have deployed IT across the organization without really assessing the security of these IT deployments. They use key IT components and systems like ERPs, Web Applications, Communication apps like email, messaging servers, etc. Apart from this, they install myriad network devices to stay connected with multiple organizational locations/units or with the Internet. I will quickly take you through a case study of an organization with a large IT deployment and will share some of the results of a security assessment that our company performed for them. The aim of this case study is to highlight the importance of assessing the organization's IT resources for security vulnerabilities and identifying the impact of a security breach by actually penetrating these systems.

Firstly, **Vulnerability Assessment** is the process of systematically identifying and assessing vulnerabilities in the system that might be used by attackers/malware to exploit the system and gain access to critical information. Penetration Testing is the process of exploiting a given vulnerability of the system by an approved security professional or firm in order to identify the impact of the security breach and showcase a proof-of-concept attack to the client organization. The combination of these two services is called **VAPT** in short.

**The Web Application was rife with several vulnerabilities. First the developers had not paid attention to secure coding practices, as a result of which a determined attacker could initiate several web application attacks**

Our company, we45 performs VAPTs for a variety of diverse corporate clientele. For public facing IT components, like Web servers, firewalls and email servers, we attack the component like an external attacker would. We perform internal VAPTs where we identify how an internal attacker (like a malicious or disgruntled employee) might try and

compromise systems and gain access to the organization's business critical information.

Our case study involves performing a VAPT for a large infrastructure company (one of the largest in the country). They have distributed IT deployments across locations and have implemented Oracle ERP applications for automation of their business operations. Additionally, they have also deployed network devices like firewalls, routers and so on. They have also developed and implemented their own B2B web application to integrate their supplier and customer networks. Our task was to identify the vulnerabilities in their IT environment and perform a Penetration Test to identify the depth of access we could get to their critical business information and showcase a proof-of-concept, highlighting the importance of security to their management.

Our first objective is Information Gathering. We perform several tests and use techniques to gather information about a target system we are going to attack. As Sun Tzu says in the 'Art of War', "Know your enemy and know yourself and you can fight a hundred battles without disaster." Our first focus is to gain as much information about the system as possible so we can perform more educated and specific attacks against it at a later time. We performed our information gathering exercise on the client's Internet facing routers, firewalls, web servers, email servers and applications. This provides us with a lot of useful information about a target system. As experienced penetration testers, we know that this information is indispensable when we are assessing vulnerabilities and subsequently, trying to exploit the vulnerabilities to compromise (penetrate) the system.

The next step is the Vulnerability Assessment. Vulnerabilities are identified using a combination of automated and manual discovery techniques. Vulnerabilities are essentially weaknesses in the system caused either by improper development (coding flaws, etc) or improper implementation and configuration (poor passwords, non-secure services running on the target systems, etc). We were able to identify critical flaws in the organization's email server and Oracle application, Web Application and router.

**Critical Security updates had not been applied to the Internet facing router of the organization.** As a result of that, the router was running outdated software that could be exploited by an attacker. The attacker could run exploit code against the target router,

The email server was a web based email application that had not been properly configured. The administrator section of the email server was open for attack. The Oracle Application had been secured using some of the standard Oracle controls. However, there was a backup service. This backup service contained the backups of the Oracle server. This backup service had not been updated with critical security patches for over a quarter. As a result, we were able to run targeted exploit code against the backup service and gain complete access to several months of Oracle Database backup data. The Web Application was rife with several vulnerabilities. Firstly the developers had not paid attention to secure coding practices, as a result of which a determined attacker could initiate several web application attacks.

**Organizations use IT systems extensively for storage, processing and transmission of critical business information. Security is one of the greatest challenges in a digitized environment**

The next step of our assessment was the Penetration Testing phase where we delve one step further in the methodology by trying to exploit the found vulnerabilities in the similar mindset of a malicious attacker – except that we would not cause any damage to the sought after critical information asset.

We used crafted exploit code to gain command-and-control access to the router and successfully compromise it. As

a result of improper patching of the Oracle backup server, we were able to run targeted exploit code against the backup service and gain complete access to several months of Oracle Database backup data. Web applications are an area where we have extensive technical know-how on and therefore it is an area where we end up being more successful as penetration testers. For instance, we were able to get access to the application's database by entering crafted strings in the input fields of the web application. This attack popularly known as SQL injection is one of the most common yet devastating attacks against a web application. Additionally, we were able to find a configuration file of the web application that was unprotected. This configuration file contained sensitive details about the web application's configuration settings and the database settings. In the database settings, we were found the root username and password credentials to the database used by the application. Using this information, we were able to compromise the entire application and demonstrate a very palpable proof-of-concept compromise to our clients

**Organizations use IT systems extensively for storage, processing and transmission of critical business information. Security is one of the greatest challenges in a digitized environment.** If you believe that your organization's business information is critical and needs to be protected against a ever-evolving threats, then Vulnerability Assessment and Penetration Testing would be a great way to identify deep-rooted vulnerabilities and fix them, thereby ensuring that the organization's critical business information stays secure and fortified.

# Information Security-Leaders' Thought

By Mr.Sowmyanarayan Sampath  
CFO-Munich Re India Services, Mumbai.

February 15, 2011

Insurance contracts represent intangible products that are sold on TRUST. The eventuality of this trust lies not just in the payment of benefits on the occurrence of the insured event but maintenance of a confidence reposed in the Insurance companies. As a Re-insurer, Munich Re stands on the epoch of the pyramid of this confidence.

**Munich Re** is fully committed to the European Directive on Data Protection – an ample demonstration of our core value of Confidentiality. This includes all personal data that comes within the possession of Munich Re. In the ordinary course of its business, Munich Re is provided information relating to the financial and medical aspects of proposers and insured. This information is secured through various practices, procedures and systems that collectively embody the Information Security organization.

The receipt, storage, processing, retrieval and dissemination of all personal data is carried out within the Information Security policies of the Group. This commitment begins with the creation of a separate department within the Information Technology division of Munich Re that is charge with the responsibility of implementing and supporting the information security (IS) within the Group. Three key Regional IS teams at Munich, Sydney and Princeton cover the geographical extant of Munich Re's vast operations and manage the various time zones on a 24 hour basis. State of the art login and access are defined based on needs of the functions of individual users within the organization. Access to the Munich Re domain is protected through latest virus and

**Insurance contracts represent intangible products that are sold on TRUST. The eventuality of this trust lies not just in the payment of benefits on the occurrence of the insured event but maintenance of a confidence reposed in the Insurance companies.**

other protection software. The IS department maintains constant vigil on unauthorized accesses to company's information assets and responds swiftly to any infringements that require each country IS to file report of steps taken.

The Group uses several in-house applications including ERP system for underwriting and accounting. A host of applications are also available to customers that provide support in their risk management processes. These applications are generally web based and again stringent access control procedures are maintained through basic login and password of acceptable complexity that require to be changed periodically that are not allowed to be repeated until a certain number of times.

The IS department includes a professional Vulnerability Assessment and Penetration testing team that reviews the controls on access of these hosted applications. The IS responsibility also covers the physical access to information storage systems and devices. The office layout plans, access to server storage sites of each office is reviewed and approved by the IS department including through personal visits from the Regional IS teams. All hardware used for access to information assets are standardized and approved centrally after due consideration for security standards.

To conclude, various facets of the information access are secured by the organization to maintain the highest standards of customer commitment that makes Munich Re one of the foremost brands in the financial services sector.

# Zone Transfers - Revealed!

By Rahul Raghavan

Senior Security Analyst, we45 Solutions India Pvt Ltd

February 15, 2011

## Knock Knock

Imagine you surrender your house along with your valuables, under the supervision of a trusted "security" personnel and leave for your vacation. During the course of your visit, a stranger comes along and asks the security guard about people in the house. As frightening as it might sound, if his answer were to be something that discloses the following- The inmates of the house, their professions, where they work, their daily routine, who keeps their valuables where and so on. This very clearly is not is expected from the trusted guard. Not only is he expected to keep mum about any reply, the last thing that is expected of him, is "sensitive data disclosure upon a simple straightforward query by an unauthorized person". This is the closest real world parallel that could be drawn to a Zone Transfer Vulnerability with web applications.

## Who is Who?

Web applications and websites are hosted upon unknown clouds and servers on the internet. These applications have addresses tagged to them just as how normal houses and buildings do. This is called an IP address which is what computers and network devices look and query for when we look type in the name of the website in our browser windows. The translation of an IP address to and from a humanly understandable name (e.g: www.google.com, www.hotmail.com called domain names) is done by a service called Domain Name Service (DNS).

They are like telephone directory services that map IP addresses to their respective domain names except that main fact that a domain mapping system is very private and confidential. Now just like there are innumerable large number of names in a telephone directory, there

are more number of websites on the world wide web. Therefore, it is quite understandable that such mappings

**As a proven statistics, derived from we45's website security assessments, more than 65% of websites are vulnerable to zone transfer attacks at some level or the other.**

would be run through millions of virtual "pages". These pages are called Zones or Zone Files. Every zone file contains certain certain number of mapping entries and are stored on servers called name servers and authoritative name servers. When someone queries for google.com, the authoritative name server that contains the zone entry for google.com would direct and map the request to the respective IP address.

Web Applications that host mission critical applications on the world wide web often contain more that one entry in the zone file. Typically, an organization whose website is www.organization.com, would contain allied applications like www.mail.organization.com, www.payrollsystem.organization.com, ftp.organization.com and so on. Certain applications are internal to an organization and should not be ideally visible to the outside world.

However, the mapping entries for these applications would or might contain in the same zone file as the publicly accessible website. There are very simple tools that an external user or

a hacker can use against these servers (containing the zone file), as a result of which, the entire contents of the zone file is presented to him in black and white. This means that in addition to the public website information, the hacker now is in possession with addresses of internal, confidential web services of an organization- applications that the hacker did not even know that existed until a moment ago. This is called a Zone Transfer Vulnerability, and is one of the most common vulnerability that exists among the majority of websites and web applications hosted.

As a proven statistics, derived from we45's website security assessments, more than 65% of websites are vulnerable to zone transfer attacks at some level or the other.

A zone transfer vulnerability is quite clearly more disastrous than a mere case of address leakage. Not an attack by itself, it is THE most valuable entry point to an organization's web application mapping. Organizations today are going to the web by hosting their websites and web applications on a shared or virtual private servers, where their application space is shared by many others on the same server.

Considering such a scenario, and assuming a very probable case that the entries of all these organizations' main and allied website addresses are on the same zone file, a zone transfer attack would disclose the information of not just one website but all the websites and web applications which are part of that zone entry. This would give an attacker ample opportunities to launch planned exhaustive attacks. This is quite the reason why a zone attack is considered the entry point to most vulnerable targets, since this vulnerability is discovered in one of the early stages of a

## News Bytes

- we45 featured as one of the **Top 20 Startups** in the **State of Karnataka** at the BangaloreIT.biz Conference, 2010
- we45 introduces **Corporate Annual Information Security Plans**
- we45 conducts **Free Website/Web Application Vulnerability Scanning Camp**

```
pratikriyaa.com.      900    IN      SOA      ns1.webstarts.com. admin.webstar
ts.com. (
                                2009113011      ; Serial
                                43200      ; Refresh
                                900      ; Retry
                                1814400      ; Expire
                                8400 ) ; Minimum TTL
pratikriyaa.com.      900    IN      NS       ns1.webstarts.com.
pratikriyaa.com.      900    IN      NS       ns2.webstarts.com.
pratikriyaa.com.      900    IN      A        208.38.155.73
pratikriyaa.com.      900    IN      MX       10 ASPMX.L.GOOGLE.com.
pratikriyaa.com.      900    IN      MX       20 ALT1.ASPMX.L.GOOGLE.com.
pratikriyaa.com.      900    IN      MX       30 ALT2.ASPMX.L.GOOGLE.com.
pratikriyaa.com.      900    IN      MX       40 ASPMX2.GOOGLEMAIL.com.
pratikriyaa.com.      900    IN      TXT      "v=spf1 include:aspmx.googlemail
.com ~all"
calendar.pratikriyaa.com. 900    IN      CNAME    ghs.GOOGLE.com.
mail.pratikriyaa.com.  900    IN      CNAME    ghs.GOOGLE.com.
start.pratikriyaa.com. 900    IN      CNAME    ghs.GOOGLE.com.
www.pratikriyaa.com.   900    IN      A        208.38.155.73
```

The above figure shows one zone transfer vulnerable website that was intentionally created by us for illustrative purposes.

The figure depicts the zone file that was obtained by using a tool that checks for zone transfer vulnerabilities. As one can see from the above image, the zone file contains a lot of information like the name servers for the particular website and also information like the mail exchange server details and few more applications that have been hosted on the same server. An external user can draw a lot of sensitive information from this zone file and launch extensive attacks as discussed in the above sections.

### **Attack Insulation**

This typically should be handled by the organization in charge of the server procurement and deployment. A detailed web application security assessment should ideally catch a zone transfer vulnerability although sadly this is not the case.

This simple yet deadly vulnerability is often not given its righteous importance during a security assessment. Organizations hosting web application especially in a shared server environment should give paramount importance to make sure that their zone records are not compromised. These are vulnerabilities that occur when a zone file is transferred from a primary server to a secondary server on request. Web server administrators should diligently disable or securely control zone transfers during server and application deployment. Organizations' technical and web application configuration team must be trained to be aware of such vulnerabilities and imparted knowledge to take appropriate mitigation steps towards securing their organizations critical assets. They should also get their server and application configuration assessed by a professional security firm from time to time to insulate themselves from such attacks and for optimal security.

If you would like to contribute your articles to 'The Fortitude', please send your article (600-750 words) to [fortitude@we45.com](mailto:fortitude@we45.com). Our last date for receiving entries for our April Newsletter is April 15th 2011. Our Newsletter committee will inform you if your article is selected.

For any feedback on this issue of 'The Fortitude' please write to us at [fortitude@we45.com](mailto:fortitude@we45.com). Your comments are appreciated.



Note: The views expressed by authors in this newsletter are purely their own and do not represent the views of we45 Solutions India Pvt ltd.

**we45 Solutions India Pvt. Ltd.**

#1439, 22nd Main, Banashankari 2nd Stage

Bangalore - 560070, Karnataka, India

Phone: +91-80-42124067

Fax: +91-80-42124017

Email: [enquiry@we45.com](mailto:enquiry@we45.com)