Analysis of an IIS hosted Private Cloud Web Application: Hacker's Perspective

Nilaykumar Kiran Sangani, *Member, IAENG,* and Nand Kumar

***Abstract*— Rapid growth of applications gives way to deliver business solutions via the web. SMEs develop browser based applications powered by web servers in private cloud environment and backend databases. As the web dependency increases, so do the hacking events. With every application that a SME brings online and each e-business that goes live, malicious hackers are waiting to attack. SMEs lack the knowledge pertaining to web application security, to safeguard their data and services. This happens due to lack of in-house technical experts and security architects or less budgets to carry out the security vulnerability and penetration testing. They should be aware that how insecure developments will open doors for the hackers to hack into their web applications. Exploring the modus operandi of hacking a web application will aid them in sensing the attack vectors.**

***Index Terms*— Cyber Security, Small and Medium Enterprises, Web Application Security, Hacking IIS Sites**

I. INTRODUCTION

WEB application security is a modern and out of ordinary subject. For all the concerned parties, the stakes are high; for businesses that derive growing returns from Internet commerce, for users who trust web applications with insightful information, and for criminals who can make immense capital by pilfering payment details or compromising bank accounts. Reputation plays a vital role because very few people would want to do business with an insecure website. As a result, few organizations disclose details about their own security vulnerabilities or breaches. Hence, it is not a trivial task to obtain reliable information about the state of the web application security today.

In the beginning days of the Internet, the WWW consisted of web sites which were fundamentally stacks of information or databases containing static documents. Web browsers were primarily invented as a means of retrieving and displaying information. The flow of this information was static, just a one-way, from server to browser. The security incidents which arose from hosting a website were chiefly related to loopholes found in web server software. If an invader compromised a web server, he usually would not be able to achieve the right of entry to any sensitive data, for the reason that the information held on the server was open to public viewing. A hacker characteristically would just be able to modify the files on the server, to despoil the website's contents or use the server's storage and bandwidth to share malwares [1] [8].

In the current time, Internet is just about unrecognizable from its previous existence. The conventional sites on the web are in reality, applications. They are vastly serviceable and rely on collaborative flow of data connecting the server and the browser. Functionalities such as Login/Logout, financial transactions, authorization of users etc. are being implemented. In today's websites, the best part is the content that is generated; dynamic and catering to the desires of diverse users [2]. There are web sites which process classified and sensitive information. Considering the above, web application security is unquestionably an immense concern. End-users will not want to accept a web application if they are under the perception that their information will be breached by illegal entities [8].

II. LITERATURE SURVEY

The Internet is in full function today. Pertaining to today's highly advanced and spirited world, each and every organization irrespective of being a large grown or a SME, needs a website to amplify its brand awareness, online visibility and revenue generation [3]. Today, if a business does not have a website then it seems to be obsolete.

Small and Medium Enterprises have started to comprehend the importance of having a website for their business growth from the past few years. They have increased their presence, availability and interactivity via the Internet. These days SMEs manage all their businesses/ transactions / surveys etc. via web applications. It opens up the accessibility of their businesses on all versions of the web browsers and smart devices.

For SMEs, clientele happiness along with a rise in profits is the most important element for their success. This they can attain via enhancing their visibility on web applications [8]. SMEs either deploy their custom created static/ dynamic applications, or hire vendors who provide SaaS for various web applications such as CRM, Social Media, Mobility Solutions, etc. to their customers [4].

Manuscript received Dec 22, 2013; revised January 28, 2014.

N.K.K.Sangani is working with Abu Dhabi Company for Onshore Oil Operations (ADCO), Abu Dhabi, U.A.E. as an IT Security Planning Analyst. (email: sanganinilay@hotmail.com)

N.Kumar is Lecturer with the Computer Science Department, Birla Institute of Technology and Science Pilani, Dubai Campus, U.A.E.(email: nandkumar@bits-dubai.ac.ae)

ISBN: 978-988-19252-5-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

III. Research Gap

Cyber Security terrorization is mounting and getting more complicated and harder to perceive. SMEs are still in their traditional outlook that firewalls, software anti-viruses and other software are adequate to shield their network and web applications. In the midst of cyber-crime which is fast escalating, it is essential that SMEs are sentient of the security threats. A thriving company works on the foundation of revenue expansion and loss avoidance [5].

SMEs are vastly affected when any one or both of these business necessities suffer. Data leak, server downtime, name failure etc. can easily turn away new and existing customers if such situations are not brought under control [2] [5].

In today's world, information keeps on increasing at a rapid rate which in turn is pushing the SMEs to set up web applications. To defend the company's liability, SMEs need to secure knowledge while hosting their web applications in order to guard them from external threats by the hackers [3]. Attackers are always focused to disrupt their application and gain unauthorized access to their data [3]. SMEs should have the basic knowledge in understanding the threats associated within a web application.

Web applications are the principal targets for hackers to transmit their attacks. Having 200 million websites in operation makes it quite effortless for the attackers to select their target. The web is so cosmic; there is something for everyone on the internet. For SMEs, web security is not a concern. Application security is one of the imperative factors of any business IT strategy which is barely understood by the executives of the SMEs as it does not side with their business goals [3] [4].

In the existing market, SMEs are massively dependent on the Internet to extend their services and solutions to a big community. Employment opportunities are shaped, which in turn increase the country's financial system [3]. Around 65% of the SMEs build up or outsource web application development to cart out their production. This helps them to contemplate on their planned business goals and map their budget more competently [3]. While implementing web applications, SMEs would like to have a safe and sound IT environment. However, very often this necessity comes into variance with other priorities [7]. Many attempts have been made to define why SMEs fail to adapt a secure development/ cyber security strategies to protect themselves. This failure can be classified as follows [6] [7]:

- Cost: Implementing cyber security measure draws away resources from the main business, in both cash and human form.
- Complexity: Executing appropriate measures requires a significant amount of expertise and dedicated technology, in order to achieve appropriate levels of security.
- Terminology: The information and language surrounding cyber security is impenetrable to the average business person.

The aim of this research is to construct an identification model of the hacks associated with the web application, to help SMEs focus on web application attacks that are likely to have an impact on, and affect, the organization.

IV. SMEs and Web Applications

Hackers have turned their focus to SMEs. In September 2012, Bitfloor suffered a web security breach in the theft of Bitcoins worth $250,000, as compared to a fortune 500 company whose value was 6000 times plus. However, the small breach for Bitfloor had put them out of market business [9]. Like Bitfloor, most of the SMEs conduct their businesses on the Web. Another instance of a SME getting hacked is of the billing and customer support provider, WHMCS in May 2012, by stealing thousands of passwords and credit card details from their systems [9].

SMEs are implementing network and patch solutions, making their network perimeter secured. Looking at this, hackers have shifted their focus and pursue attacks via web applications [9]. According to Gartner Group, 70% of the cyber-attacks take place at the application layer [9]. SMEs are showcasing their businesses/ products/ solutions via web applications which raise their market presence and contribute within the economy of the respective country [10]. SMEs believe that security implementations such as firewalls, anti-virus solutions, IDP solutions etc., contribute to the security of web applications [9].

Rise in the web application threats clearly suggest that the web is becoming popular. Until and unless these threats are not understood, the security to implement against these harmful hackers will not be an easy task to tackle with, especially for SMEs [11].

SMEs have very little knowledge in order to protect their web applications. Hackers and attackers are always finding ways and means to attack web applications created by SMEs. The latter are mainly concerned about their business profits without giving importance to the web application security [12]. They must understand that having applications in web will directly open doors to the hacking community, in order to exploit their business and data [12]. They lack in understanding the different types of threats which exist in applications hosted in a web environment [12].

In the past few years, security and privacy of data hosted online have become one of the major concerns [12]. Not understanding how a hacker targets web applications, makes it very difficult for them to secure it. Per Symantec, there has been a 72% increase in the cyber-attacks targeting small businesses [13].

V. Website Hack

For the purpose of this research, a test site in ASP.NET 2.0 hosted on IIS server has been created. It replicates a private cloud environment to exhibit live hacking scenarios.

ISBN: 978-988-19252-5-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Hack 1: Password Sniffing: The hacker can sniff the password once the credentials are entered by the end-user [10].

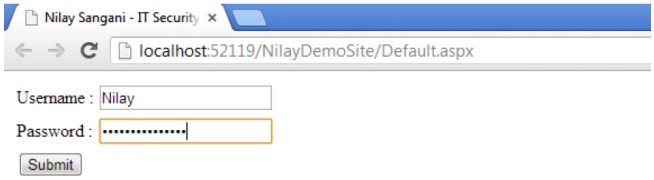

Fig.1: Password Sniffing

From the above Figure 1, the end-user has entered the credentials on the website.

Steps:
a) In Figure 2, a proxy is being used to intercept and analyze the request.

Fig. 2: Analyzing the request

b) Hacker is able to view the credentials (Figure 3) via sniffing which are getting passed in a clear text format.

Fig. 3: Credentials in clear text format

Hack 2: Cross Site Scripting (XSS): Through XSS, a hacker has the ability to hijack application sessions/ cookies/ sensitive parameter values. This takes place by planting of a malicious script which allows a hacker to impersonate a valid user by allowing the former to modify any information within the application. In simple terms, the attacker can send untrusted request to the website impersonating the legitimate user [10].

Steps:
a)The hacker executes XSS attack via Query String Parameters and modifies them (Figure 4) by inserting a malicious script.

Fig. 4: JavaScript XSS attack via Query String Parameter

b) End-user receives the malicious script (Figure 5) inserted by the hacker

Fig. 5: XSS Attack

Hack 3: Response Manipulation: In this case, the attacker takes advantage of an invalidated input, inserted by the end-user within the application, and modifies the response to launch further harmful attacks.

Steps:
a) User has an interface of inserting their e-mail address and in the response there is a thank you message for the submission (Figure 6).

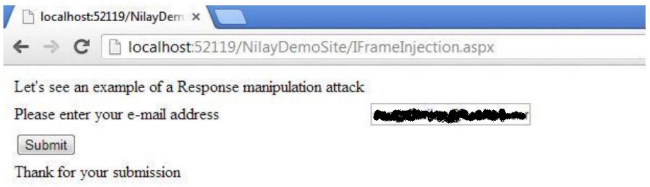

Fig. 6: End-User View

b) After analyzing the response, the hacker finds out the response parameter for the confirmation of the message 'Thank you for your submission' is vulnerable. Taking advantage of this parameter, the hacker will redirect the user to his/ her own crafted malicious message which redirects the user to a fake website (Figure 7).

Fig. 7: Response Manipulation

c) Once the hacker has manipulated the response, the end-user will receive a page like below (Figure 8). The hacker has manipulated the response by adding a <href> tag to redirect the user to a malicious link.

Fig. 8: End user's view after Response Manipulation

Hack 4: SQL Injection: A hacker always tries to penetrate into the database by inserting custom crafted data via the input fields of a web application.

Steps:
a) For the purpose of research and viewing of an attack on a database, a database named 'NilayITSecurityDemo' and a

ISBN: 978-988-19252-5-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

table named 'NilaySQLInjection' have been created (Figure 9).

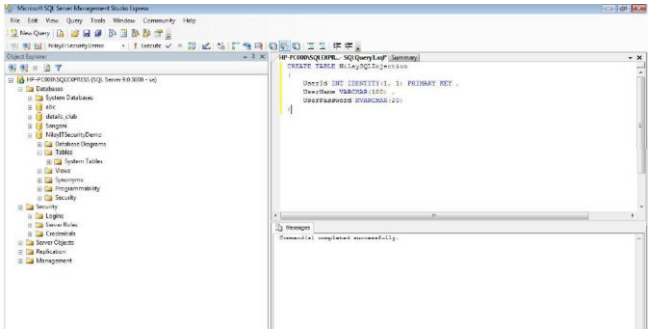

Fig. 9: Create table NilaySQLInjection

b) The users are inserted into the table created.

c) The hacker has the view of the website and will try to extract the login credentials of the users of the web application (Figure 10).

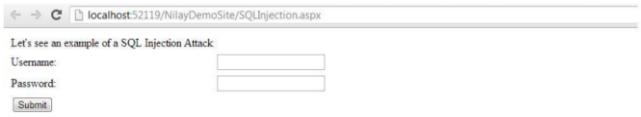

Fig. 10: Page Created to Perform SQL Injection Attack

d) Hacker tries all various possibilities to extract the usernames and passwords.

i) To extract the table name (Figure 11), hacker has supplied fuzzed inputs.

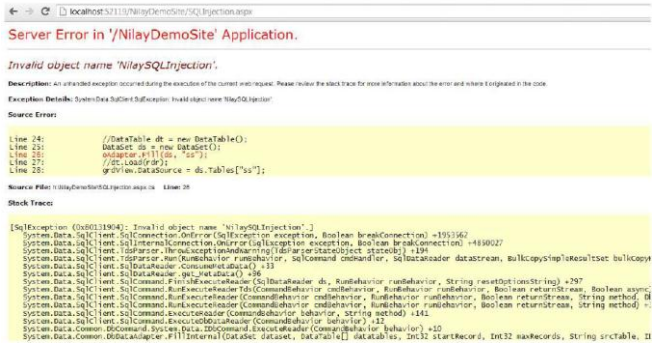

Fig. 11: SQL Injection – Disclosure of the Table Name 'NilaySQLInjection'

ii) Inserting ' OR 1=1 - - gives the username and password details of all the users (Figure 12).

Fig. 12: SQL Injection

Hack 5: Fuzzing: Hacker supplies negative inputs in order to break the application's business logic or functionality etc. The main aim is to disrupt the application's workflow logic targeting the actual behavior.

a) Supplying negative inputs

Steps:

a) In order to break the function logic and see the application's exception behavior, the hacker performs a fuzz test in all the input fields by supplying negative parameters.

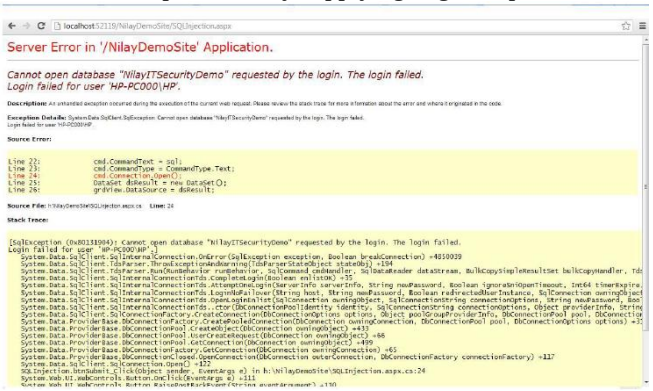

Fig. 13: Sensitive Exception Details

Based on the above (Figure 13), the hacker is able to get to know the Database name, the server name where the MSSQL is hosted, and the path where the application is residing. Having such information in hand enables the hacker to plan further exploits.

VI. Conclusion

Web applications security has been an ever-growing concern since the creation of Internet. Major organizations are still in receipt of being hacked in spite of having the best security controls or information security consultants in place. SMEs are highly dependent on web applications to showcase their business solutions or services. However, they lack the knowledge pertaining to the breach of web application by the hackers. In order to protect their data, services and reputation, they should understand the protocol of a web application hack.

This research is supported by an exhaustive study and live exhibition of how a .NET web application gets breached. It specifically targets SMEs to understand the different possibilities of attack which can disrupt their businesses.

VII. Future Work

Future work will include an implementation of controlling the security, safeguarding the web applications, and hardening the Windows Server OS & IIS, in order to protect a Small and Medium Organization demonstrated within this research from the various web application attacks.

Acknowledgment

I would like to extend my sincere gratitude to Ms. Meenal Bharath Kumar for her copy editing assistance.

REFERENCES

[1] Building Advanced Web Applications for Small and Medium Enterprises, K2B Solutions.
[2] W. Huang; R. Li; C. Maple; H. Yang.; D. Foskett; V.Cleaver., "Web Application Development Lifecycle for Small Medium-Sized Enterprises (SMEs) (Short Paper)," Quality Software, 2008, QSIC '08. The Eighth International Conference on, vol., no., pp.247, 252, 12-13 Aug. 2008.
[3] N.K.Sangani; T.Vithani; P.Velmurugan; M.Madiajagan, "Security & Privacy Architecture as a service for Small and Medium Enterprises," Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on , vol., no., pp.16,21, 8-10 Dec. 2012.
[4] International Federation of Accountants, 'The Role of Small and Medium Practices in Providing Business Support to Small- and Medium- sized Enterprises', Information Paper, April 2010.
[5] C.Onwubiko; A.P. Lenaghan, "Managing Security Threats and Vulnerabilities for Small to Medium Enterprises," Intelligence and Security Informatics, 2007 IEEE, vol., no., pp.244, 249, 23-24 May 2007.
[6] 'THE GFI SOFTWARE SME SECURITY REPORT', GFI, March 2009.
[7] D.Prince, N.King, "Towards Digitally Secure Business Growth", Small Business Cyber Security Workshop 2013.
[8] Hypertext Transfer Protocol, "RFC 2616 Fielding, et al."
[9] Jeremiah Grossman, 'THE TOP FIVE MYTHS OF WEBSITE SECURITY-A Focus on Small-to-Mid-Sized Enterprises', White Hat Security, January 2013.
[10] N.Sangani, B.Vijayakumar ,'Cyber Security Scenarios and Control for Small and Medium Enterprises', Informatica Economica, vol. 16 no. 2/2012.
[11] 'Towards a comprehensive Internet security strategy for SMEs', GFI White Paper.
[12] D.Lacey, B.James,'Review of Availability of Advice on Security for Small/Medium Sized Organizations', Information Commissioner's Office, March 2010.
[13] Rohit Sethi, '5 Safeguards From Watering Hole Attacks, Chinese Hackers', Fox Business, June 2013.

ISBN: 978-988-19252-5-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)