IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 14, Issue 5 (Sep. - Oct. 2013), PP 46-51
www.iosrjournals.org

Survey of different Web Application Attacks & Its Preventive Measures

Rajesh M. Lomte[1] , Prof. S. A. Bhura[2]
[1](Computer Science & Engineering Department ,BNCOE,India)
[2](Computer Science & Engineering Department ,BNCOE,India)

Abstract: *Securing web is like securing our nation. Our whole world is Internet dependent In each sector internet is very much essential. So, internet security is very much promising task for us.*
More than 80% attacks are at application layer and almost 90% applications are vulnerable to these attacks. The essential services like banking, education, medicine and defense are internet based application needed high level security services which are essential for the socio-eco growth of the society. In this paper we are discussed the different types of web application attacks like DOS attack, Cross Site Scripting attack(XSS), SQL Injection Attack ,Request Encoding Attack. Survey of these attacks happening in last three to four years .latest happening with these attacks in India & out of India in the year 2012-13 & 13-14. Similarly we are measuring impact of each attack and putting its proposed counter measures.
Keywords: *IDS - Intrusion detection system ,XSS – Cross site scripting, SQL-Sequential query language, DOS-Denial of Services*

I. Introduction

Now a day's web security is biggest issue in the corporate world. The world is highly dependent on the Internet .It is considered as main infrastructure of the global information society. Therefore, the availability of Internet is very critical for the socio-economic growth of the society. The "availability" of Internet and its services means that the information, the computing systems, and the security controls are all accessible and operable in committed state at some random point of time However, the inherent vulnerabilities of the Internet architecture provide opportunities for a lot of attacks on its infrastructure and services.[1] XSS , SQL injection, Sniffing, Request Encoding and DOS attacks which poses an immense threat to the availability of the Internet. An occurrence of these attacks on the web degrades or completely disrupt services to legitimate users by expending communication and/or computational resources of the target. Nowadays to achieve security of distributed systems is a dominant task for any organization including the most modest types of e-commerce, banks and even large state systems However, the increasing number and a variety of system attacks suggest, between among other things, that the design and realization of these systems are often very poor as far as security is concerned. Web security is essential part of business world. [2] Dos Attack is responsible for attackers direct hundreds or even thousands of compromised hosts called zombies against a single target. XSS attack is responsible for the attacker executes malicious code on the victim's machine by exploiting inadequate validation of data flowing to statements that output HTML. SQL Injection Attack is responsible for the attacker executes malicious database statements by exploiting inadequate validation of data flowing from the user to the database. Sniffing (Request Encoding) attack is responsible for data hacking during data transmission. Previous approaches to identifying these kinds of attacks and preventing them includes defensive coding, static analysis, dynamic monitoring, and test generation. These techniques have their own merits but have some drawback like Defensive coding [6] is error-prone and requires rewriting existing software to use safe libraries. Static analysis tools [13] can produce false warnings and do not create concrete examples of inputs that exploit the vulnerabilities.[30].traditional solution for DOS protecting the network connection's confidentiality and integrity, protecting the server from break-in, and protecting the client's private information from unintended disclosure. A lot of protocols and mechanisms [9][5] have been developed that address these issues individually. One area that has been neglected thus far has been that of service availability in the in the presence of DOS. It can take many forms depending on the resources the attacker is trying to exhaust. Because of these attacks Vulnerabilities business market will get hampered and it is headache to the E- business system.[6][15]
This paper will provide the survey of different web application attacks & its protection.

II. Related Work

Most of the traditional works on network intrusion detection focus on misuse-based or anomaly-based recognition of attack signatures. However, traffic generated from an attack to a web application — except for brute force attacks or similar events — is likely to be very similar to normal traffic because, since HTTP is a text based protocol, it is always possible to encapsulate an attack at application layer without

Creating a packet that is anomalous if inspected at network layer. Writing generic network-layer signatures for web-based attacks are thus troublesome, and a source of false positives. On the other hand, host-based IDSs were typically designed to monitor the processes on the protected system (e.g. the web server daemon) rather than the web applications they run. However, nowadays' XSS attacks can perform more sophisticated tasks. This technology, however, works only on reflected XSS attacks, and not on persistent attacks where the injected malicious code is permanently stored on the server-side and is delivered to the browser at a later time. We are going to provide the best solution to protect the web from various web attacks.[13][14]

III. Survey Of Different Web Attacks

DOS,SQL Injection, XSS Attacks:

Following are the figures which are come into picture while looking towards stories of attacker in the last three to four years. 22% of UK companies surveyed experienced a disruptive attack in 2012, compared to 35% of respondents in a recent Neustar North American survey. Overall, UK respondents claimed that over a third (37%) of these attacks lasted more than 24 hours. Overall, UK attacks tended to be longer than in North America, with 22% lasting over a week versus 13% in North America.

Key sectors reported higher rates of attack: Among those companies attacked, the highest percentages were found in telecommunications (53%), ecommerce (50%) and online retail (43%). By contrast, the North American survey found the financial sector to be the most targeted with 44%, versus 17% in the UK. Neustar notes that the recent attacks on US banks are the likely reason for this disparity, but these attacks have opened the doors for others to mimic the tactics, such as recent DDoS attacks against Dutch banking systems in April 2013.Downtime hits the bottom line: DDoS attacks inflict a grave toll on revenues regardless of industry, but the survey found that some suffer more than most. The industries with the highest losses from an outage were financial services and telecommunications companies. [3]

Respondents from the financial sector noted that 26% of Part of the Chinese Internet went down early Sunday morning in what the government is calling the largest denial-of-service attack it has ever faced .The attack began at 2 a.m. Sunday morning and was followed by a more intense attack at 4 a.m., according to the China Internet Network Information Center, Denial-of-service attacks cause disruptions by overwhelming a computer or network with a high level of online activity. Usually the attacks originate from networks of computers that have been hijacked by malware or viruses.By Monday the problem seemed to have been solved, with Chinese Internet users able to access websites such as Sina Corp.'s social networking site Weibo smoothly.

CloudFlare Chief Executive Matthew Prince said the company observed a 32% drop in traffic for the thousands of Chinese domains on the company's network during the attack compared with the same time 24 hours earlier.

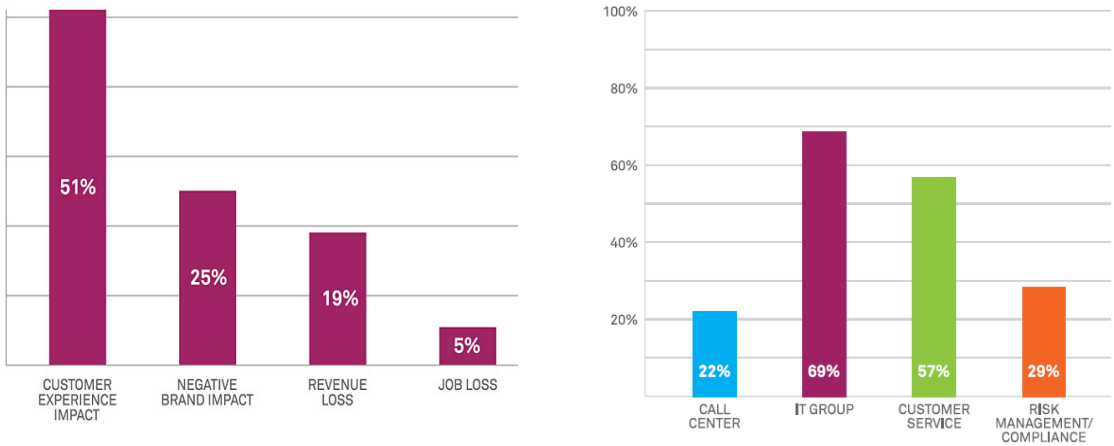


Figure 1 Figure 1 Fig. Financial loss in various sectors due to DOS attack & Areas of Greatest Cost Increases in a DDoS Attack

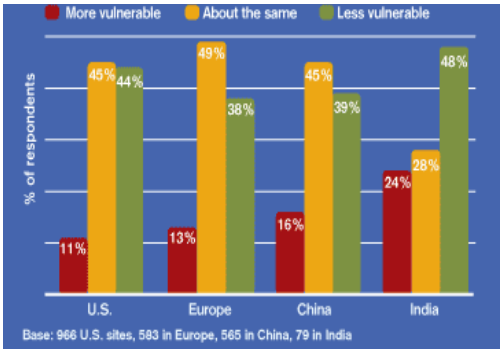
Sony Hacked in April to June 2011, Sony is by far the most famous recent security attack. After its Playstation network was shut down by LulzSec, Sony reportedly lost almost $171 million. The hack affected 77 million accounts and is still considered the worst gaming community data breach ever. Attackers stole valuable information: full names, logins, passwords, e-mails, home addresses, purchase history, and credit card numbers. Hacked in June 2011, Citigroup was not a difficult target for hackers. They exploited a basic online vulnerability and stole account information from 200,000 clients. Because of the hacking, Citigroup said it lost $2.7 million. Just a few months before the attack, the company was affected by another security breach. It started at Epsilon,

an email marketing provider for 2,500 large companies including Citigroup. Specialists estimated that the Epsilon breach affected millions of people and produced an overall $4 billion loss.
The US carrier was hacked last year, but said no account information was exposed. They said they warned one million customers about the security breach. Money stolen from the hacked business accounts was used by a group related to Al Qaeda to fund terrorist attacks in Asia. According to reports, refunding costumers cost AT&T almost $2 million.The most impressive numbers come from last year. 40 million employee records were stolen in March 2011, after RSA Security was hacked. Another huge theft of information happened in the summer, when personal data of 35 million South Koreans was exposed after hackers breached the security of software provider ESTsoft.

Other interesting figures include this year's Zappos hack, with 24 million accounts exposed. Because credit cards were not stolen, the shoe store's attack wasn't as damaging as it could have been.
The case, brought by US attorneys in Manhattan and New Jersey, is the largest hacking scheme ever prosecuted in the US, Department of Justice officials said. From 2005 to 2012, the four Russian nationals and a Ukrainian penetrated the private networks of the Nasdaq stock exchange, Citibank, PNC Bank, Heartland Payment Systems,. The hacking gang traded text strings that exploited SQL-injection vulnerabilities in the victim companies' websites to obtain login credentials and other sensitive data, then installed malware that gave them persistent backdoor access to the networks.

European credit card numbers sold for as much as $50, while US ones fetched about $10. Buyers then used the data to create clone cards that, along with stolen PINs, were used to withdraw millions of dollars from ATMs around the world. On May 19, 2007, Kalinin allegedly identified a vulnerability in a password-reminder page of the Nasdaq website. Five days later, prosecutors said, he fashioned a text string that injected SQL programming code that allowed him to obtain cryptographically hashed login credentials from the page. He then shared the string with Gonzalez.The US Department of Justice today announced charges against five individuals who allegedly pulled off the largest hacking and data breach scheme in US history a scheme that ran from 2005 through last year that resulted in 160 million stolen credit card numbers. "Changing root password: As soon as the MySQL server is installed, root user with blank password is created. The MySQL root user will have full access to perform any operation on the MySQL server. It is a good practice to change the root password immediately after installation.Cross-site scripting (XSS) is increasingly common in the cloud computing world, up more than 160% in the fourth quarter of 2012 from the previous three months, a security firm is warning.
Fire Host said that it blocked 64 million cyber attacks in 2012. The company warns that both XSS and SQL injection attacks have become even more prevalent since the third quarter of 2012.

Following are some graphical representation of Cyber Crime:



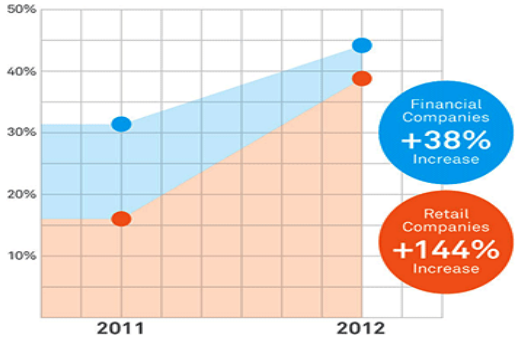


Figure 2 Amount of vulnerability Comparison Chart Figure 3 Comparison Chart of Cyber Crime in AC 2012& 13

Following are some measures :

- 42% increase in targeted attacks in 2012.
- 31% of all targeted attacks aimed at businesses with less than 250 employees.
- One waterhole attack infected 500 organizations in a single day.
- 14 zero-day vulnerabilities.
- 32% of all mobile threats steal information.
- A single threat infected 600,000 Macs in 2012.
- Spam volume continued to decrease, with 69% of all email being spam.
- The number of phishing sites spoofing social networking sites increased 125%.
- Web-based attacks increased 30%.

5,291 new vulnerabilities discovered in 2012, 415 of them on mobile operating systems

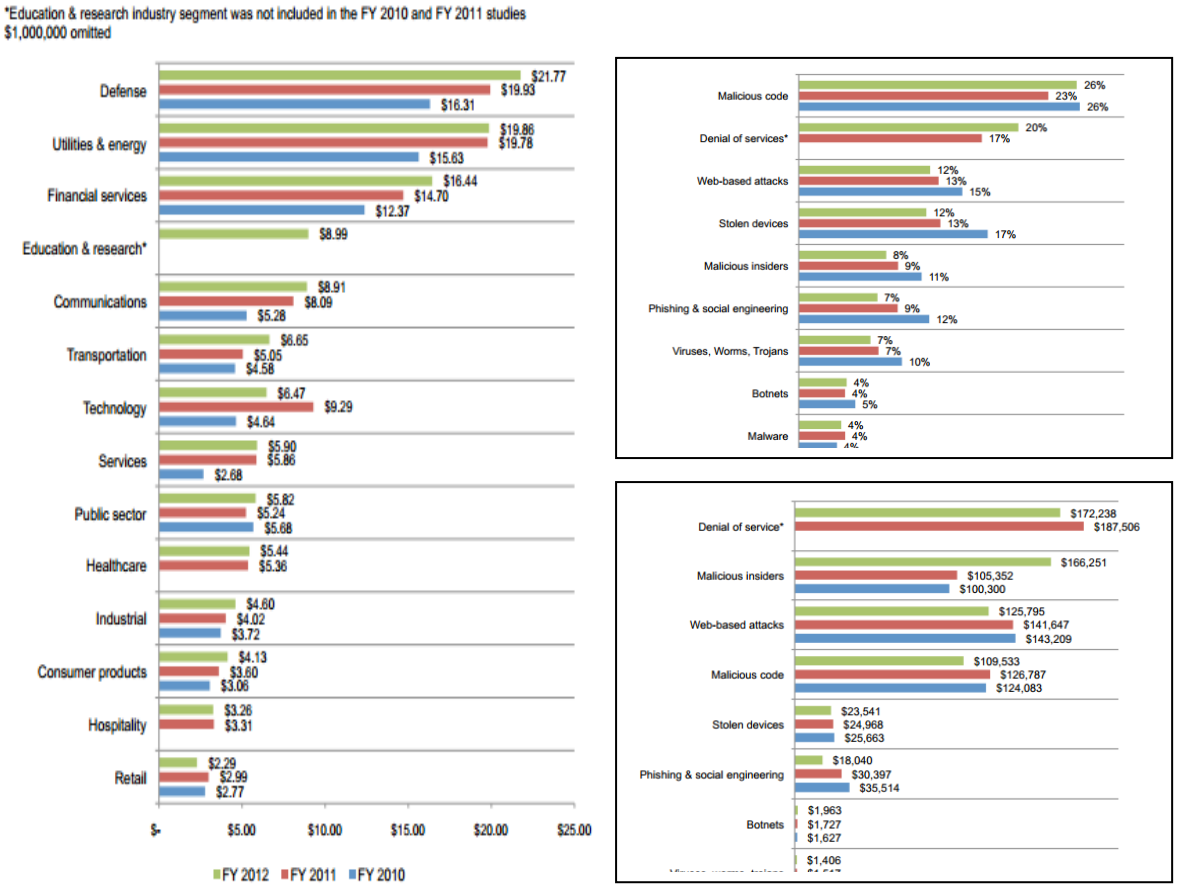


Fig. 4 Financial harm in different sectors

From the above survey we can say that we are now in dangerous zone. We save our internet world we should proposed solution to stop such a malicious things.[7]

IV. Proposed Preventive Measures

This solution will definitely useful for future software security engineers to secure our e-world.

1. In this attack, attackers inject client side script code. The script code embeds itself in the response data, which is send back to an unscripting user. The user's browser then runs the script code. Because the browser downloads the script code from a trusted site, the browser has no way of recognizing that code is not valid.

Protection Mechanism

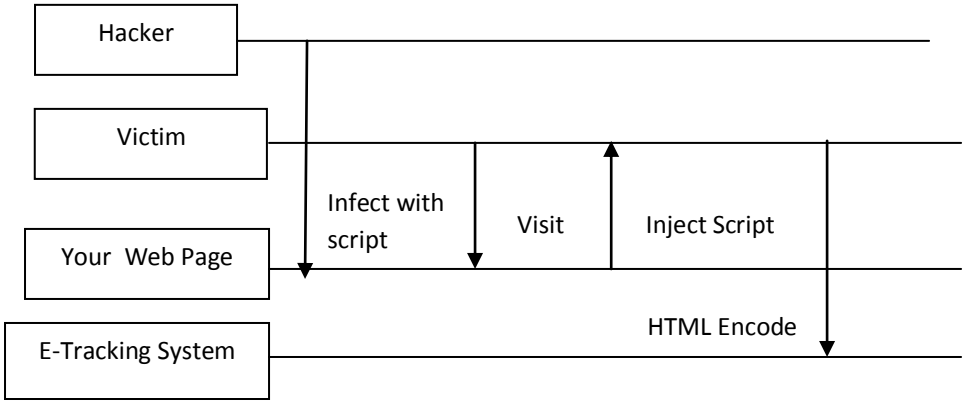


Fig. 5 Protection against XSS attack

1. DOS Attack :

In this hacker sends continuous request to down the server by making it busy by sending the continuous, hacker tries to crash the server

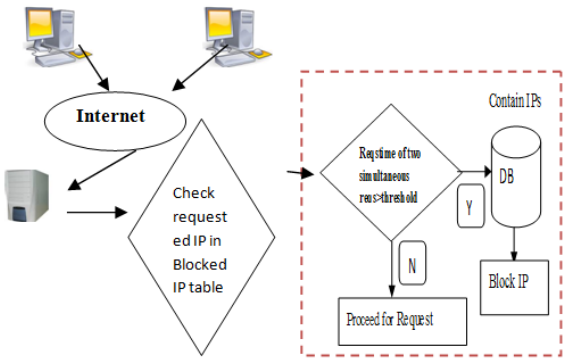


Fig. 6 Protection against DOS attack

2. SQL Injection : In this attack sql queries are inserted through input medium like text box to hamper the database

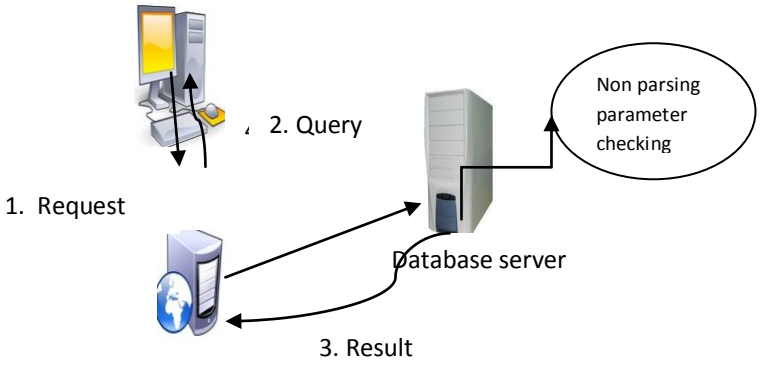


Fig. 7 Protection against SQLI attack

4. Request Encoding

In this type of attack, the attacker tries to decode the request which is traversed between client and server. After decoding the request he may track the sensitive data from the application.

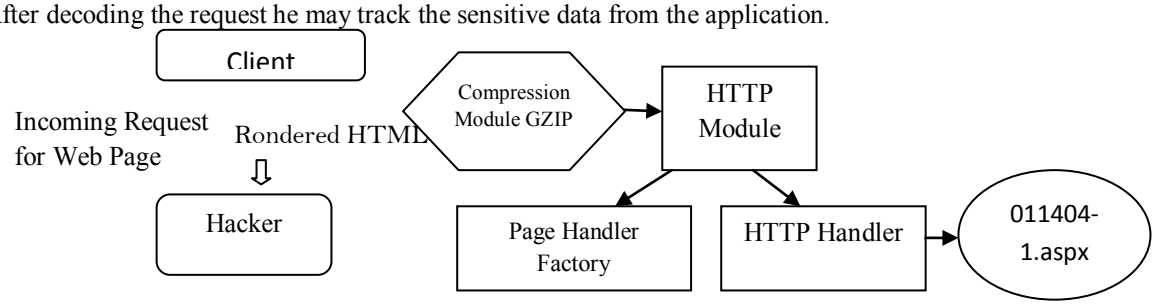


Fig. 8. Protection against RE attack

V. CONCLUSION

The proposed solution will definitely help for building rich & secured web application. We can remove used good best designing/modeling practices while building a web application to crate great design and can protect our web application from different web attacks like DOS,SQL Injection, XSS and Request encoding. By using all said solutions/methods we can make our application very secured & efficient which definitely save our business world.

References

[1] Monika Sachdeva, Krishan Kumar Gurvinder Singh Kuldip Singh SBS College of Engg. & Technology, Guru Nanak Dev University Indian Institute of Technology Ferozepur, Punjab, India Amritsar, Punjab, India Roorkee, Uttarakhand, Indiamonika.sal(kediffmail.com gzsbawa7 1(yahoo.om kds56fec(&riitr.ernetmin) Performance Analysis of Web Service under DDoS Attacks 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009

[2] Diallo Abdoulaye Kindy1,2 and Al-Sakib Khan Pathan2, A Detailed Survey on Various Aspects of SQL Injection in Web Applications: Vulnerabilities, Innovative Attacks, and Remedies, 1CustomWare, Kuala Lumpur, Malaysia 2Department of

Computer Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia diallo14@gmail.com and sakib@iium.edu.my , 2012
[3] DDoS Attacks in the United Kingdom: 2012 Annual Trends and Impact Survey
[4] Joaquin Garcia-Alfaro1 and Guillermo Navarro-Arribas2, Prevention of Cross-Site Scripting Attacks on Current Web Applications_,1 Universitat Oberta de Catalunya,Rambla Poble Nou 156, 08018 Barcelona - Spain, joaquin.garcia-alfaro@acm.org 2 Universitat Autònoma de Barcelona, Edifici Q, Campus de Bellaterra, 08193, Bellaterra - Spain, gnavarro@deic.uab.es
[5] William G.J. Halfond, Jeremy Viegas, and Alessandro Orso College of Computing Georgia Institute of Technology {whalfond|jeremyv|orso}@cc.gatech.edu, A Classification of SQL Injection Attacks and Countermeasures, College of ComputingGeorgia Institute of Technology {whalfond|jeremyv|orso}@cc.gatech.edu,
[6] Mark Curphey The Open Web Application Security Project David Endler iDefense William Hau Steve Taylor Predictive Solutions Tim Smith The Open Web Application Security Project Alex Russell OWASP Filters project Secure Pipe Inc. netWindows.org Gene McKenna Richard Parke Kevin McLaughlin," A Guide to Building Secure Web Applications The Open Web Application Security Project"
[7] Security Threat Report 2013-New Platforms and Changing Threats,SOPHOS
[8] Uzi Ben-Artzi Landsmann and Donald Str¨omberg, Web Application Security: A Survey of Prevention Techniques Against SQL Injection, Department of Computer and Systems Sciences Stockholm University / Royal Institute of Technology
[9] Sonam Panda, 1 Ramani S2," Protection of Web Application against Sql Injection Attacks", International Journal of Modern Engineering Research (IJMER)www.ijmer.com Vol.3, Issue.1, Jan-Feb. 2013 pp-166-168 ISSN: 2249-6645
[10] Mihir Gandhi, JwalantBaria," SQL INJECTION Attacks in Web Application", International Journal of Soft Computing and Engineering (IJSCE)ISSN: 2231-2307, Volume-2, Issue-6, January 2013
[11] Asha. N M. Varun Kumar Vaidhyanathan. G, **Preventing SQL Injection Attacks** nternational Journal of Computer Applications© 2012 by IJCA JournalVolume 52 - Number 13 Year of Publication: 2012
[12] Zhang Chao-yang," DOS Attack Analysis and Study of New Measures to Prevent", Intelligence Science and Information Engineering (ISIE), 2011 International Conference on Date of Conference**:** 20-21 Aug. 2011
[13] Adam Kie˙zun MIT akiezun@csail.mit.eduPhilip J. Guo Stanford University pg@cs.stanford.edu Karthick Jayaraman Syracuse University kjayaram@syr.edu Michael D. Ernst University of Washington mernst@cs.washington.edu
[14] Y. Song, S. J. Stolfo, and A. D. Keromytis, "Spectrogram: A mixtureof-markov-chains model for anomaly detection in web traffic," in Proc.of the 16th Annual Network & Distributed System Security Symposium,San Diego, CA, USA, February 2009.
[15] C. Criscione, G. Salvaneschi, F. Maggi, S. Zanero Dipartimento di Elettronica e Informazione — Politecnico di Milano 2009 European Conference on Computer Network Defense Integrated Detection of Attacks Against Browsers,Web Applications and Databases.
[16] Vipul Patel, Radhesh Mohandas and Alwyn R. Pais Information Security Research Lab, National Institute of Technology Karnataka, Surathkal, India {vip04pat, radhesh, alwyn.pais}@gmail.com ATTACKS ON WEB SERVICES AND MITIGATION SCHEMES
[17] Forewords by Mark Curphey, Joel Scambray, and Erik Olson Improving Web Application Security Threats and Countermeasures
[18] Encription limited The Stables White Lodge Bevere Worcester WR3 7RQ www.encription.co.uk Campbell Murray encryption limited "The need for secured web development"
[19] http://www.linuxtoday.com/infrastructure/2008091100735OSSV