ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

Securing Web Application from SQL Injection & Session Tracking

[1]Pranjali Gondane, [2]Dinesh. S. Gawande, [3]R. D. Wagh, [4]S.B. Lanjewar, [5]S. Ugale
[1]Lecturer, Department Computer Science & Engineering, Dr. Baba Saheb Ambedkar College of Engineering & Research, .NAGPUR (M.S.), INDIA
[2]Lecturer, Department Computer Science & Engineering, Dr. Baba Saheb Ambedkar College of Engineering & Research, .NAGPUR (M.S.), INDIA
[3]Lecturer, Department Information Technology, Dr. Baba Saheb Ambedkar College of Engineering & Research, NAGPUR (M.S.), INDIA
[4]Lecturer, Department Computer Science & Engineering, Dr. Baba Saheb Ambedkar College of Engineering & Research, .NAGPUR (M.S.), INDIA
[5]Lecturer, Department Computer Science & Engineering, S.B. Jain College of Engineering, NAGPUR (M.S.), INDIA

Abstract: ***Due to the rise and rapid growth of E-Commerce, online purchases have dramatically increased and it caused an explosion in the credit card fraud. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. In the existing system the fraud is detected after the fraud is done that is, the fraud is detected after the complaint of the card holder. And so the card holder faced a lot of trouble before the investigation finish. And also as all the transaction is maintained in a log, we need to maintain a huge data. And also now a day's lot of online purchase are made so we don't know the person how is using the card online, we just capture the IP address for verification purpose. So there need a help from the cyber crime to investigate the fraud. To avoid the entire above disadvantage we propose the system to detect the fraud in a best and easy way. This project presents three modules: Website designing, Hacking techniques like SQL Injection attacks for avoiding these techniques Filters and Session Tracker are added.SQL Injection is a technique used to attack databases i.e. gaining unauthorized access to a database, to view or to manipulate restricted data. A filter is an object that performs filtering tasks on either the request to a resource or on the response from a resource, or both. Filters can perform many different types of functions viz. Authentication and Logging and auditing thus assuring card holder a secured transaction.***

Keywords: **Internet**, **SQL injection, Filters, Session tracking, E-commerce Security, Online shopping.**

I. INTRODUCTION

Web application security is a branch of Information Security that deals specifically with security of websites, web applications and web services. A secure website where your customers, readers, and visitors feel safe is vital to your online success. Cyber crime has impacted the world's largest organizations and it can also damage your business. Why risk damaging your reputation and the trust you've worked so hard to earn from your customers, when maintaining a secure website has never been so simple and effective. Cyber attacks turn hacked websites into launch pads for further hacking assaults that install malicious software or malware on your visitors' computers. Hackers can then steal sensitive customer data like credit card details, destroy your business's search engine optimization (SEO) rankings and propagate illegal content to your users: such as child pornography, or viruses. Now a day the usage of credit cards has dramatically increased. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. In real life, fraudulent transactions are scattered with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. Implementation of efficient fraud detection systems has thus become imperative for all credit card issuing banks to minimize their losses. In this synopsis, we model the sequence of operations in credit card transaction processing by creating database driven website & showing hacking using SQL injection, session tracking and then add filters technique to show how it can be used for the detection of frauds. Aim and objective is to design a system which detects and block fraud transactions using a credit card at an early stage & at same time system which is user friendly.

II LITERATURE REVIEW

There were some of the challenges that are faced by most detection techniques include:

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

Skewed distribution of legitimate and fraudulent data in the database that challenges the detection approaches. Genuine transactions are much higher as compared to fraudulent [1]. Count of transaction which is proliferating swiftly. Mining [6] of such immense amount of data calls efficient techniques.

Availability of labeled data for the purpose of training, as genuine or cheat is not readily available [4]. Tracking user's behavior is tough as it changes quite often for all type of users (good users, business and fraudsters) [2].Dealing with old as well as new intellectual is a challenging task [3]. They are artificial neural-network models which are based upon artificial intelligence and machine learning approach [8] [9], distributed data mining systems [7] [5], sequence alignment algorithm which is based upon the spending profile of the cardholder [1] [6]. The other technologies involved in credit card fraud detection are Web Services-Based Collaborative Scheme for Credit Card Fraud Detection in which participant banks can Share the knowledge about fraud patterns in a heterogeneous and distributed environment to enhance their fraud detection capability and reduce financial loss [10] [11], Credit Card Fraud Detection with Artificial Immune System [11]. Most of the credit card fraud detection systems mentioned above are based on artificial intelligence, Meta learning and pattern matching. SQL injection attacks happen because of badly implemented Web Application filters, meaning that the web application will often fail to properly sanitize malicious user input. We can usually find this type of badly implemented SQL injection filters in outsourced web applications to India, Asia or other possibly third world countries, that developers are not aware of what SQL injection proper filtering is. Most of the time well known large organizations from the financial sector will create a large team of functional and security testers and then outsource the project in order to reduce the development cost, at the same time they would try to maintain and increase the control of the web application development progress and quality assurance process. Unfortunately this is not easy to happen or even possible due to bad management procedures or lack of security awareness from the side of the developers.

The proposed system compares and analyzes some of the good techniques that have been used in detecting credit card fraud. It focuses on sql injection technique and session tracking.

III PROPOSED SYSTEM

A. Website Designing

In this project we are designing a database driven website. A database-driven Web site is a Web site that uses a database to gather, display, or manipulate information as shown in fig 1. The website has two users that are admin & members. Each one has their separate menus.

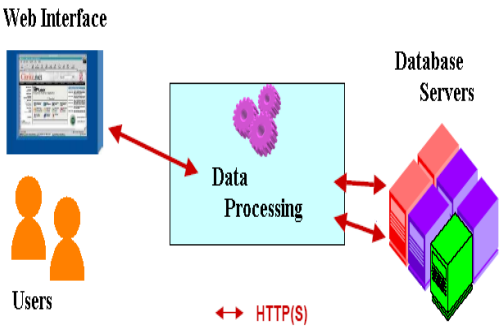


Fig 1: Database Driven Website

B. Advantages of database driven websites

Users can do their own maintenance via a set of Web-based data entry forms. For Example, A user can change his address, other information of his account by himself. The site visitor can do a search on the items in the database. It is easy for Administrator to maintain the Website Web pages of database-driven Web sites are created dynamically (in real time) thus giving a Web site visitor an up-to-date view of information stored in the database.

C. SQL injection attacks

A SQL injection attack consists of insertion or "injection" of SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify data(Insert/Update/Delete),execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands as shown in fig 2.SQL Injection has become a common issue with database-driven web sites. The vulnerability is easily detected, and easily exploited, and as such, any site or software package with even a minimal user base is likely to be subject to an attempted attack of this kind. SQL Injection is a type of vulnerability in applications that use an SQL database. The vulnerability arises when a user input is used in a SQL Statement.

Like Below:

```
$name = $_GET['username'];
$query = "SELECT password FROM tbl_user WHERE name = '$name' ";
```

As you can see the value the user enters into the URL variable *username* will get assigned to the variable *$name* and then placed directly into the SQL statement. This means that is possible for the user to edit the SQL statement.

```
$name = "frank' OR 1=1 -- ";
$query = "SELECT password FROM tbl_user WHERE name = '$name' ";
```

The SQL database will then receive the SQL statement as the following:

```
SELECT password FROM tbl_users WHERE name = 'frank' OR 1=1 -- '
```

Which is valid SQL, and instead of returning one password for the user, the statement would return all the passwords in the table. This is not something anyone wants in their web applications. Now the attacker enters the following in the username field in the above statement. If the web application is vulnerable to the SQL injection attack, the above input is validated normally and an existing user's account is displayed to the attacker in random. The attacker can then alter and enjoy the privileges of the legitimate user, resulting in hacking the account. In severe cases the attackers input query inputs in a vulnerable web application and tries to find the table names and other important database information and exploit them.

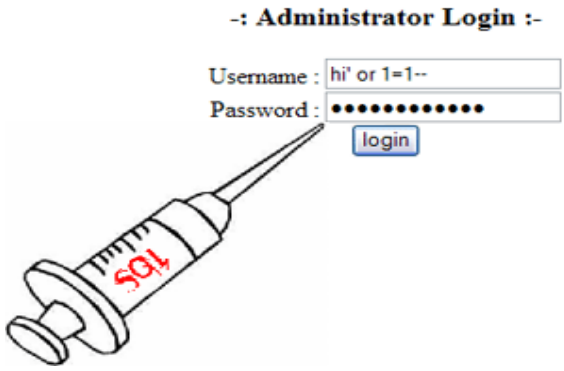


Fig 2: SQL Injection Attack

D. Hacking Prevention Adding Filters

A filter is an object that performs filtering tasks on either the request to a resource (a servlet or static content), or on the response from a resource, or both as shown in fig 3. Filters perform filtering in the doFilter method. Every Filter has access to a FilterConfig object from which it can obtain its initialization parameters, a reference to the ServletContext which it can use, for example, to load resources needed for filtering tasks. Filters are configured in the deployment descriptor of a web application.

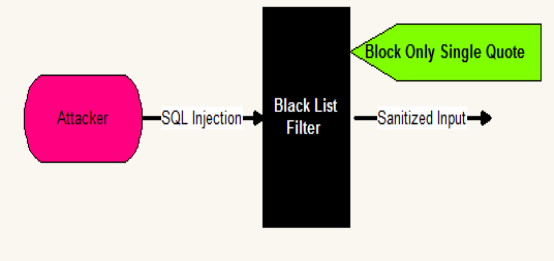


Fig 3: Filters to SQL Injection Attacks

E. Session Tracking

A Session refers to the entire request that a single client makes to a server. A session is specific to the user and for each user a new session is created to track the entire request from that user. Every user has a separate session and separate session variable is associated with that session. In case of web applications the default time-out

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

value for session variable is 20 minutes, which can be changed as per the requirement as shown in fig 4. A session ID is an unique identification string usually a long, random and alpha-numeric string, that is transmitted between the client and the server. Session IDs are usually stored in the cookies, URLs (in case url rewriting) and hidden fields of Web pages. HTTP is stateless protocol and it does not maintain the client state. But there exist a mechanism called "Session Tracking" which helps the servers to maintain the state to track the series of requests from the same user across some period of time.

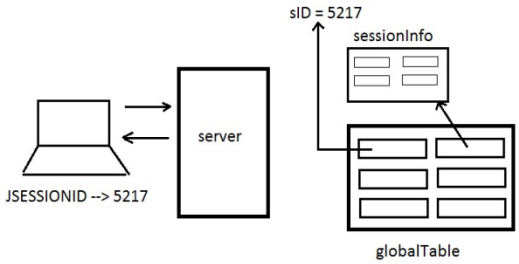
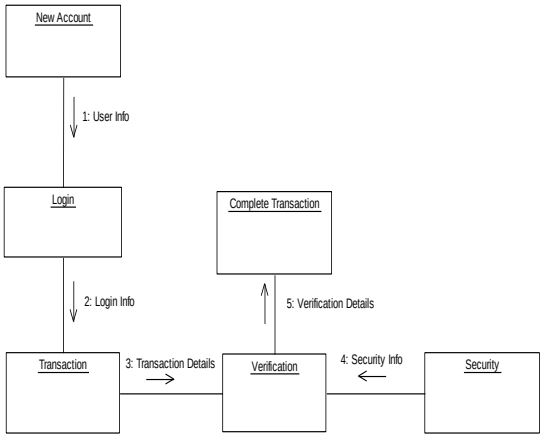


Fig 4: Session Tracking

IV. PROJECT FLOW DIAGRAM

A. Collaboration diagram



Description: this figure shows how the network security is achieved.

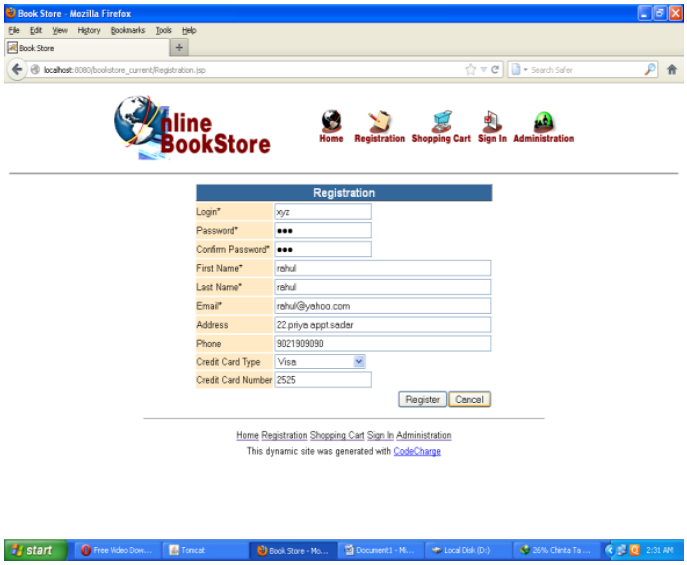
V. OUTPUT

Website Designing

Description: Above screenshot is the home page of website created. Which is a Online BookStore.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

Registration Menu

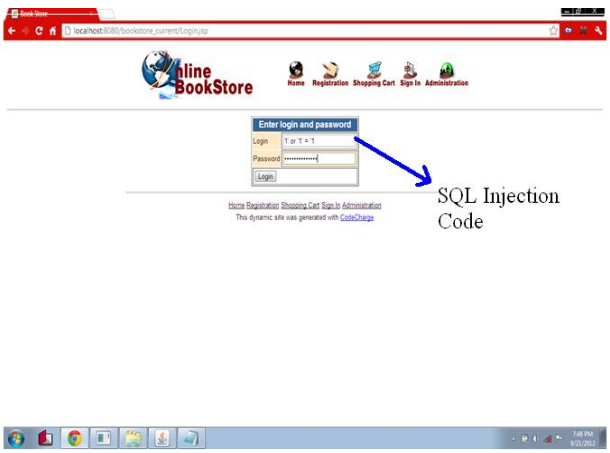


Description: This is the registration form for the new users where fills all his necessary details.

Log-in menu

Description: This is log-in page for getting access to user account in here the authorized user fills his log-in id & password and the unauthorized user injects SQL injection.

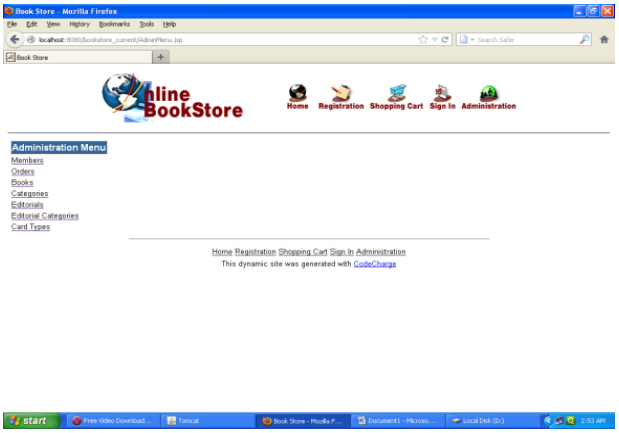
SQL injection attack



Description: This figure shows how the SQL Injection is used to hack the user account.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

Hacker gets access



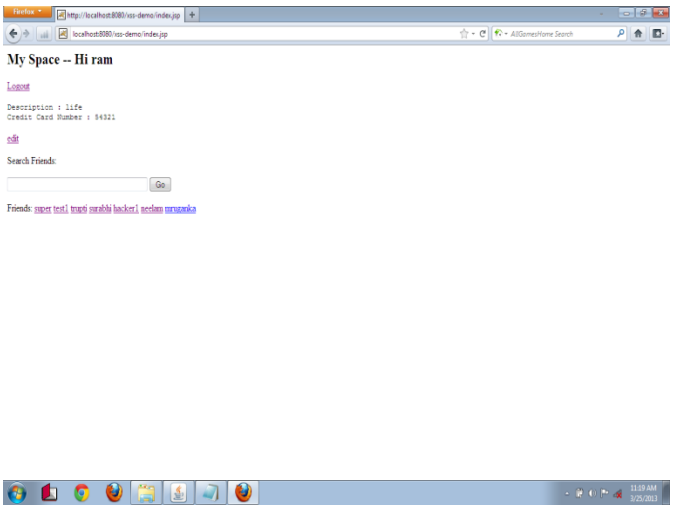
Description: As the site was not secured the hacker gets access to the admin account from where he gets all necessary information of the user which he can use for his own benefit.

After Adding Filters

Description: This figure shows that hacker is blocked and access is not permitted as filters are activated.

Session Tracking

User account Menu



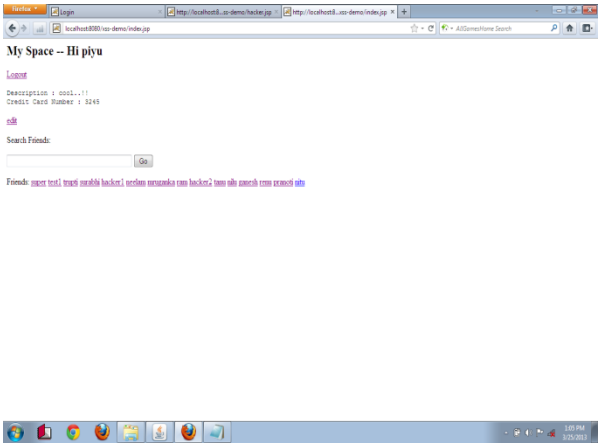
Description: This snap shot shows the user account with all user menus. One of the menus is "friend" where hacker account is also displayed.

Hacker account

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

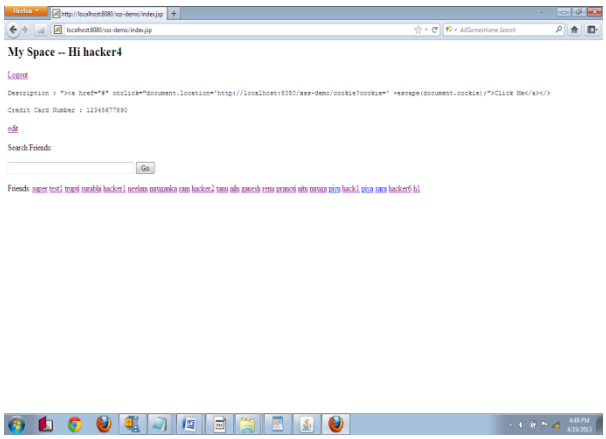
Description: This snap shows the hacker account, and the tab created by the hacker which on being clicked by user stores his session id.

After Hacking



Description: This snap shows the view hacker gets when he uses the session id gained by him from session tracking.

After Adding Filters



Description: This figure shows how after adding filters the hacker is not able to create his tab which stores the session.

VI CONCLUSION

Efficient fraud detection system is an utmost requirement for any card issuing bank. Fraud detection has drawn quite a lot of interest from the research community and a number of techniques have been proposed to counter credit fraud. Many people often overlook the benefits of database driven website and yet even the smallest

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

website will develop over time and could benefit from being database driven. Databases add a new dynamic angle to your website giving- Provide useful information & good presentation. This system can be implemented for avoiding cyber crimes. The system works efficiently in any field where authentication is provided to user. The session which is maintained with the help of session tracking will also be a proof for the bank for the transaction made. This system can be implemented for military purpose.

REFERENCES

[1] S. Benson Edwin Raj, analysis on Credit Card Fraud Detection Methods Paper presented at:- International Conference on Computer, Communication and Electrical Technology –ICCCET2011, 18th & 19th March, 2011.

[2] Short paper presented at:-International Journal of Recent Trends in Engineering, Vol 2, No. 3, November 2009.

[3] Database-driven Web Sites http://www.crendo.com/database-driven- websites.html.

[4] "Stopping Card Fraud in its Tracks" paper presented by an Industry Guide from ACI. Martin Nystrom, "SQL Injection *Defences"*.

[5] Francisca nonyelum ogwueleka, Data mining application in Credit card fraud detection system.

[6] Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws.

[7] R. Brause, T. Langsdorf, M. Hepp, "Neural Data Mining for Credit Card Fraud Detection, "International Conference on Tools with Artificial Intelligence, pp.103-106, 1999".

[8] Ghosh, D.L. Reilly, "Credit Card Fraud Detection with a Neural-Network," Proceedings of the International Conference on System Science, pp.621-630, 1994.

[9] A. Chiu, C. Tsai, "A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection," Proceedings of the IEEE International Conference on e-Technology, e-Commerce and e-Service, pp.177-181, 2004.

[10] Manoel Fernando Alonso Gadi, Xidi Wang, Alair Pereira do Lago, "Credit Card Fraud Detection with Artificial Immune System," Lecture Notes in Computer Science, Vol. 5132/2008, pp.119-131, 2008.