STUDY OF STENOGRAPHY AND FORENSIC ANALYSIS OF CYBER CRIMES USING SQL INJECTION ATTACK

VIRAL RAJENDRAKUMAR DAGLI, SURENDRANAGAR

DR. H. B. BHADKA, C U SHAH UNIVERSITY

DR. K. H. WANDRA

ABSTRACT

Cyber Crime is normally comprehended to comprise of getting to a PC without the proprietor's consent, surpassing the extent of one's endorsement to get to a PC framework, changing or annihilating PC information or utilizing PC time and assets without appropriate approval. Cyber fear mongering comprises basically of undertaking these equivalent exercises to propel one's political or ideological closures. Psychological oppressor activities in the internet should be possible by confined people or fear monger gatherings, yet one state against another. By that, digital psychological warfare doesn't vary from other sort of fear mongering in any capacity. The particular idea of the risk can extend from forswearing of administration to listening in, extortion, damage, and robbery of licensed innovation and restrictive data. This paper expects to give a wide review of the difficulties looked by the world in digital wrongdoing and issues looked by law implementation organizations and Information and Communication Technology security masters in digital examinations and the advantages that might be picked up by the worldwide network and obviously the open private associations (PPP) to the anticipation, location and arraignment of digital violations and how underdeveloped nations need to keep pace with the consistently changing innovations and the control of this innovation by what we may term digital crooks so as to make benefit.

Keywords: Cyber Crime, online frauds, SQL Injection

INTRODUCTION

Cybercrime is any crime that includes a PC, organized gadget or a system. While most cybercrimes are done so as to create benefit for the cybercriminals, a few cybercrimes are completed against PCs or gadgets straightforwardly to harm or cripple them, while others use PCs or systems to spread malware, unlawful data, pictures or different materials. A few cybercrimes do both - i.e., target PCs to contaminate them with a PC infection, which is then spread to different machines and, once in a while, whole systems. An essential impact of cybercrime is money related; cybercrime can incorporate various kinds of benefit driven

crime, including ransom ware assaults, email and web misrepresentation, and character extortion, just as endeavors to take budgetary record, charge card or other instalment card data. Cybercriminals may likewise focus on a person's private data, just as corporate information for burglary and resale.

WORKING OF CYBER CRIME

Cybercrime assaults can start any place there is advanced information, opportunity and thought process. Cybercriminals incorporate everybody from the solitary client occupied with cyberbullying to state-supported entertainers, similar to China's knowledge administrations.

Cybercrimes for the most part don't happen in a vacuum; they are, from multiple points of view, dispersed in nature. That is, cybercriminals commonly depend on different entertainers to finish the wrongdoing, regardless of whether it's the maker of malware utilizing the dull web to sell code, the merchant of unlawful pharmaceuticals utilizing digital money dealers to hold virtual cash retained or state danger on-screen characters depending on innovation subcontractors to take licensed innovation (IP).

Cybercriminals utilize different assault vectors to complete their cyber attacks and are always looking for new strategies and systems for accomplishing their objectives, while dodging discovery and capture. Cybercriminals regularly complete their exercises utilizing malware and different sorts of programming, however social building is frequently a significant segment for executing most kinds of cybercrime. Phishing messages are another significant segment to numerous sorts of cybercrime however particularly so for focused assaults, similar to business email bargain (BEC), in which the aggressor endeavors to imitate, by means of email, an entrepreneur so as to persuade representatives to pay out sham solicitations.

TYPES OF CYBER CRIME

- **Cyber extortion:** A wrongdoing including an assault or danger of an assault combined with an interest for cash to stop the assault. One type of cyber extortion is the ransom ware assault, in which the aggressor accesses an association's frameworks and scrambles its archives and documents - anything of potential worth - making the information out of reach until a payoff is paid, ordinarily in some type of digital currency, for example, bit coin.

- **Credit Card Fraud:** An assault that happens when programmers penetrate retailers' frameworks to get the MasterCard as well as banking data of their clients. Taken installment cards can be purchased and sold in mass on dark net markets, where hacking bunches that have taken mass amounts of MasterCard benefit by offering to bring down level cybercriminals who benefit through MasterCard extortion against singular records.
- **Exit Scam:** The dim web, of course, has offered ascend to the advanced adaptation of an old wrongdoing known as the leave trick. In the present structure, dull web heads redirect virtual money held in commercial center escrow records to their very own records - basically, lawbreakers taking from different hoodlums.

VARIOUS TECHNIQUES OF CYBER CRIME

1. **SQL INJECTION:** SQL injection is a code injection method, used to assault information driven applications, in which malignant SQL articulations are embedded into a passage field for execution (for example to dump the database substance to the attacker).[1] SQL injection must adventure a security weakness in an application's product, for instance, when client input is either erroneously sifted for string exacting break characters installed in SQL proclamations or client input isn't specifically and out of the blue executed. SQL injection is generally known as an assault vector for sites yet can be utilized to assault any kind of SQL database. SQL injection assaults enable assailants to parody character, mess with existing information, cause revocation issues, for example, voiding exchanges or evolving balances, permit the total divulgence of all information on the framework, decimate the information or make it generally inaccessible, and become heads of the database server.
2. **OPHCRACK:** Ophcrack is a free Windows secret word saltine dependent on rainbow tables. It is an effective execution of rainbow tables done by the designers of the technique. It accompanies a Graphical User Interface and runs on various stages.
3. **Denial of Services:** In this cyber-attack, the cyber-criminal uses the bandwidth of the victim's network or fills their e-mail box with spammy mail. Here, the intention is to disrupt their regular services.

4. **Phishing:** Phishing is a procedure of separating classified data from the bank/money related institutional record holders by unlawful ways.

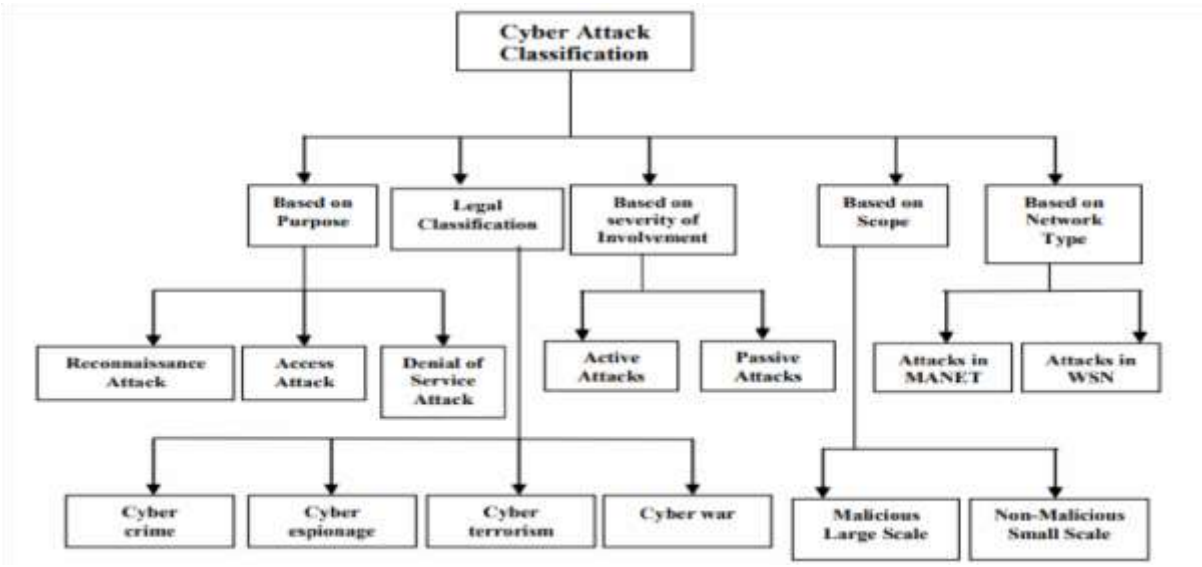

Fig 1: Cyber Attack Classification diagram

TECHNIQUES USED FOR PREVENTION OF CYBER CRIME

Fig 2: Conceptual model – The relationship between the key elements of cyber security education

Along these lines, a lot of suggestions and great practices have come about because of the dissected examines:

-neighbourhood ventures (for the most part IT&C organizations or the financial division) ought to be associated with supporting instructive activities, for example, paid temporary jobs and mentors arrangement;

-government structures ought to and the scholarly condition should work in a cozy relationship, by advancing transient expert trade of data and great practices so as to advance security's job in the internet;

-worldwide associations and accomplices can be a decent wellspring of data in this field;

-accessibility of progressively virtual preparing situations so as to associate more experts from around the globe;

-building quality research after existing abilities and structure, including experienced examiners, subsidizing, look into focuses and plausible task

SOURCES OF SQL INJECTION

1. Injection through client input: Malignant strings are presented in web shapes through client inputs.
2. Injection through treats: Changed treat fields contain assault strings.
3. Injection through server factors: Headers are controlled to contain assault strings.

Frauds can likewise be described dependent on the objective, or intent, of the aggressor. In this manner, we can define[4] a few plans as follows:

1. **Recognizing injectable parameters:** The aggressor needs to test a Web application to find which parameters and client input fields are helpless against SQLIA.
2. **Performing database finger-printing:** The aggressor needs to find the sort and form of database that a Web application is utilizing. Specific sorts of databases react diversely to various inquiries and assaults, and this data can be utilized to "unique mark" the database. Knowing the sort and form of the database utilized by a Web application enables an aggressor to create database specific frauds.
3. **Deciding database pattern:** To accurately remove information from a database, the attacker frequently has to know database construction data, for example, table names, section names, what's more, segment information types. Assaults with this expectation are made to gather or induce this sort of data.
4. **Removing information:** These kinds of frauds utilize strategies that will remove information esteems from the database. Depending on the kind of the Web application, this data could be delicate and exceptionally attractive to the assailant. Frauds with this aim are the most widely recognized kind of SQLIA.
5. **Including or adjusting information:** The objective of these assaults is to include or change data in a database.

6. **Performing refusal of administration:** These assaults are performed to close down the database of a Web application, therefore refusing assistance to different clients. Assaults including locking or dropping database tables likewise fall under this classification.
7. **Sidestepping location:** This class alludes to certain fraud systems that are utilized to abstain from examining and location by framework assurance instruments.
8. **Bypassing validation:** The objective of these kinds of frauds is to enable the assailant to sidestep database and application verification instruments. Bypassing such components could enable the aggressor to accept the rights also, benefits related with another application client.
9. **Executing remote directions:** These kinds of frauds endeavor to execute subjective directions on the database. These directions can be put away methodology or capacities accessible to database clients.
10. **Performing benefit acceleration:** These assaults take advantage of usage blunders or sensible defects in the database so as to raise the benefits of the assailant. Instead of bypassing verification frauds, these fraud center around abusing the database client benefits.

PROPOSED SYSTEM OF SQL INJECTION ATTACK

IndraniBalasundaram, E.Ramaraj [1] proposed an confirmation instrument to forestall SQL infusion fraud utilizing Advance Encryption Standard (AES). In this strategy, scrambled username and secret phrase are utilized to improve the confirmation process with least overhead. The technique has proposed three stages, in the main stage for example enlistment stage, server sends an enlistment compliance. In the second stage for example login stage, client can get to the database from server. The username and secret phrase is scrambled by utilizing Advance Encryption Standard (AES) calculation by applying client discharge key and the SQL inquiry is produced utilizing scrambled username and secret word. At that point the question will be sent to server. In the third stage for example confirmation stage, server gets the login inquiry and confirms the relating clients discharge key. In the event that they coordinates, at that point the decoded username and secret word is checked from client account table. On the off chance that it matches, at that point client is acknowledged generally dismissed.

MayankNamdev, FehreenHasan, Gaurav Shrivastav [2] have given a model to square SQL injection which is based on check data. They have joined two approaches and made another mixture calculation which works by applying the hash code with encryption for greater security. In this methodology, two additional sections are required, one for putting away the hash estimations of username and another for putting away the hash estimations of secret key. At the point when the record of clients is made just because, the hash values are determined and put away in client table. The hash esteems are determined at runtime utilizing put away technique when client logs into the database. The qualities which are determined at runtime are coordinated with put away hash esteems in database table. In this way, on the off chance that client attempts to infuse to the question, the proposed technique will naturally recognize the infusions as noxious substance and rejects the qualities. In this manner, it can't sidestep the confirmation process. Its bit of leeway is that programmers don't think about the hash values idea.

CONCLUSION

In view of the above outcome, in which four distinctive SQL injection recognition instruments are utilized, on various sites have a place with various kinds (like creation based, entrance, social site and so on), to recognize helplessness for sql injection assaults, it is discovered that Netsparker can distinguish Cross-site scripting and Boolean SQL injection. Sqlmap can recognize Boolean based and Union inquiry. Web cruiser can distinguish Cross-site scripting and urlsql injection. What's more, Havij can't distinguish any talked about assault. Furthermore, it is likewise discovered that sites which have a place with item based are increasingly powerless against SQL injection assault. So based on above outcome it very well may be inferred that no instrument can recognize all vulnerabilities for SQL injection frauds. The paper introduced a novel and relevant method for shielding web applications from SQLIAs. The methodology comprises of permitting single word client inputs just, that will consequently wipe out all wellsprings of assault vulnerabilities. The following methodology utilized is Rc4 and blowfish encryption techniques which will improve execution due to their less time multifaceted nature. AES is mind boggling encryption standard while RC4 is old and straightforward. Both RC4 and Blowfish are quicker in execution when contrasted with AES procedure. Since, the strategy is created at application level, it requires no changes in the current runtime framework and forces less execution overhead to diminish SQL injection fraud nearly inside and out.

REFERENCES:

1. BalasundaramIndrani and E. Ramaraj, "An Authentication Mechanism to prevent SQL injection Attacks," International Journal of Computer Applications, vol. 19, no. 1, pp. 30-33, April 2011.
2. MayankNamdev, FehreenHasan, and Gaurav Shrivastav, "Review of SQL Injection Attack and Proposed method for detection and Prevention of SQLIA," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 7, pp. 24-28, July 2012.
3. Sonakshi, Rakesh Kumar and GirdharGopal "Prevention of SQL Injection Attacks using RC4 and Blowfish Encryption Techniques" International Journal of Engineering Research & Technology (IJERT), Vol. 5 Issue 06, June-2016
4. Uma and Padmavati, 2013
5. Source: Cybersecurity Educational Programs: Costs And Benefits, BASIQ-2019CONFERENCE PROCEEDINGS
6. Premveer, Ankur Srivastava, Anuragjain "Vulnerability Detection For SQL Injection Attacks: An Experimental Survey", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 6, June - 2013