CYBER ATTACKS - TRENDS, PATTERNS, AND SECURITY COUNTERMEASURES

Mohammed Saeed Z Alshahrani[1*], Dr. Amr Ibrahim Mahmoud Ramadan[2]
[1*]Masters student, Faculty of Computing and Information Technology, University of Bisha, Bisha, Saudi Arabia
[2]Faculty of Computing and Information Technology, University of Bisha, Bisha, Saudi Arabia
mohammed.alshahrani2020@gmail.com[1*], aemahmod@ub.edu.sa[2]

In the present world, the rapid growth of technology-enabled public communication for various purposes like cloud computing, social networks, automated processes, and online transactions, etc. Though technological evolution leads to good deeds, still allowed the existence of intruders and cybercrimes seemingly without any interruption which further leads to the evolution of new attack types, techniques, and tools. All those immoral signs of progress allow attackers to get throughmore complicated or well-governedinfrastructures, and developenhancedimpairment and even persistas an untraceable source.There is plenty of techniques that don't demand prior cognition of hacking.These immoral approaches can be executed by any exploiter if there exists an opening for some defenseless code in the system or websites.This research articleintent to traverse through the brief summarization onthe cyber-crime domainthat mostly includes cyber-attack, hacking as it is outlined and exposed by specialized existing work, international statute law, and historical realities.Eventually, the work is focused on analyzing various major attacks accounted throughout the world over the past three years to find outtrends and patterns in the sector of cyber-crime. Later on,different experiments are carried out on several aspects to find out or trace some possible attacks, and to examine countermeasures. Based on the outcomes of the experimental analysis,this research article exhibitsvalid countermeasure strategies that any organization may undertake to ensure improved protection that would affirm in guarding their enterpriseagainstthe attackers. Moreover, the core part of the article aids thesecurity experts, incursion testers, and developers to acquire prior knowledge about countermeasures based onan information security perspective.

Keyword: Cybersecurity, Attacks, Security Countermeasures, Security Assurance

1. INTRODUCTION

In the present era, the world is increasingly moving ontosocial networks, cloud, big data, web servers, and online transactions. Nowadays valuable data is being stored and managed

online via the internet. Most of the automated procedures that are followed and executed through the utilization of standard IT systems, data privacy, and information security are continuously dealing with higher risks. With the unstable and unsaturation of new security systems, cyber-crimes aresystematicallyraising in terms of the number of vulnerabilities to its victims.

About the recent research, it is found that 229,000 attacks against onlineweb systems happened every day and out of these 229,000, it's been evident that around 76% of website attacks [1] are occurring due to vulnerabilities. To evolve some novel modes to attain unauthorized admittance into the secured networks, confidential data, and precise programs, most of the attackers intend to compromisethe integrity, availability, and confidentiality of information. Further, they aim to build up their objectives from individuals to the minor ormid-sized organization and sometimeslarger enterprises. Thus the overall immoral activities lead to the business discontinuity and ultimately losing the customers' faith. The raisingcourse of action has attained new elevations in 2014, cosmicallyrecognized as "the year of cyber-attacks", but the real fact is believed that this would be a non-culmination factor unless fixed with suitable countermeasures at a global reference standard.The overall advancement and evaluation led to a much easier way of dealing with security concerns but on the other aspects, it is gettingvastdispute in ensuring the security standards for any online systems.

1.1. Overview of Web Systems

Penetrations testing of web systems hashugegrandnesssince it impliesbase-level user data and log-in credentials.Testing acts asa criticalpart in ensuring the quality of whateverweb system. Software examiner makesvarioustest suit on whichthey execute testing on all developed web system to further catch up withencountering bugs.This workiterates until every bug is eliminated [2]. Normally, it has been found that the software examinersare not cyberpunks so they can't breach the database and credentialsas hackers do.Thus, the prerequisite of basic knowledge on hacking techniquescan actas a criticalpart in maintaining the quality sureness of any software.

In this research work,the few most recentproficiencies or techniques of hackingfor web-based applicationswith sign-up and sign-in pages are discussed [3]. In such applications, user data plays a key role, therein, various techniques are utilized by the attackers to disfigure thesecurity of entire web systems. Few major techniques include R2L, DoS, Probing, U2R,etc., [4].

Remote to User (R2L): On the utilization of this technique, hackers use to sends a good deal of packets to the machine to determine vulnerability and to make headway for local access.

Denial of Service (DoS): Through these techniques, the perpetrator attempts to make the system or available resource of the network into an unavailable mode to the users, thus disrupts the service indefinitely or temporarily.

*Probing:*On the utilization of thissurvey type of proficiency, the hackers obtain control over the entire network through the scan and determines the vulnerabilities that further destabilize the network

User to Root (U2R): To attaincontrol over the root of the server, cyberpunksemploymere user credentials then broadcast packets to detectvulnerabilities to arrive atthe root.

All the aforementioned techniques demand a lot of prerequisite knowledge to execute attacks. Though the attacker has multiple choices to opt for a suitable technique, few simple techniques can be utilized to deface the web systems.

1.2. Types of Vulnerabilities

Vulnerability is of various types but for the objective of this research articlevery few vital types of vulnerabilities are considered and they are stated as:

SQL INJECTION: One of the most popularly known vulnerabilities is “SQL Injection” which is based on Input parameters. In SQL Injection malicious exploiters can falsify any SQL Command by injecting their SQL command to access the desired database [5].

Cross-Site Scripting (XXS): It is a well-known kind of vulnerability that is usually detected across web systems. In this type, the attacker mainly induces more or less malicious scripts into the web to attain accessibility over the main server [6].

*Cryptography:*From the perspective of cryptanalyst, this technique is known to be the separate domain for secure communication. Here, the sender is an authorized person to encrypt the data beforesending and the receiver is responsible to decrypt the received data. But most occasions, this form of secure communication is breached by an intruder or middle man who can attain control and possess enough capabilities to deceive the sender (act like receiver [7].

*Cross-Site Request Forgery:*It is a special kind of technique through which a hacker or malicious user could send and perform an unneeded request to user side web application during the login duration [8].

This article has the aim of exposing the elaborated analysis based on existing attack models, trends, patterns, and results observed in the last three years. Further, through the overall obtained reports, the research work tends to confront justifiable countermeasures for aiding the system betterment especially in security build-ups and to reduce worldwide crimes. This article isintegrated with three primary constituents: it commences by exhibiting the most generalized perspective of cyber-crime in terms of specialized existing work, international statute law, and historical realities. Later on, continues to disclose major attacks with their principal resolutionsand interpreting the short study that has prevailed for the past three years.Afterward,a methodology is proposed in which an attack is executed on the selective webpage to detect and examine the vulnerabilities and their following countermeasure strategy. Finally, it concludes by depicting some of theprimary countermeasures strategies that any enterprises may set about to assure the betterment of controls addressing thedata confidentiality, availability, and integrity concerning the reduction of several security breaches.

2. RELATED WORK

In daily reality, cyber-attacks turn nightmare for both giants as well as small scale organizations; but still only a few are aware of this cybercrime. The article from [9],delineate the lack of understanding and gaining knowledge regarding various attacks and their characteristics. Thus, this sense of unawareness possesses some real obstacles in defending the network, and information security.

Respective resolutions on cyber-crime, cyber-attack, etc. can be found amongst the world-wide literature, allbearing in common the intention to compromise the integrity, availability, and confidentiality of information. The technological advancements also contributedto the progress of cybercrime, thus novelmodes to execute attacks, accomplish even more difficult topenetrate objectives or targets, and to stayin untraceable mode are arousedendlessly. Nevertheless, conventional cyber menacespersist as theorigin of the majority of the common attacks. Several types of approaches or attacks have been outlined and examinedacross the standard literature:

*Man-in-the-middle:*Whenever some communicative messages are sent from source to destination, is interrupted and reaches the attackers which are commonly referred to as a man-in-the-middle attack. The consequences of this type of attack compromises by admitted

unauthorized access to a sensible set of information or allows the attackers to modify the information/data before reaching the destination.

Brute force attack: This type of attack comprises recurrentattacks to benefitaccession on the highly protected data/information (e.g. encryption data/ciphertext, passwords, etc.) until the requireddata is breached, and obtained.

Distributed Denial of Service (DDoS): This is a kind of approach that compromises the accessibility of data, decisively that the attacker plans to flood out the host (e.g. server) withnecessary commands, thus goingunserviceable;

*Malware:*Malware is a collective term describing numerous malicious software variants, often preferred by the attacker to compromise the availability, integrity, and confidentiality of data. The most common types of malware areRansomware, Viruses, Trojans, Worms, Adware, Rogware /Scareware, and Spyware.

Phishing: It is a kind of technique targeted to attain some private information without prior authorization from users via masquerading as a faithful resource (e.g. website).

Social Engineering: It is the genericname that delineates theproficiencies used to attain unauthorized accessibilities tosecuredinformation via human interaction.

In [13] the author demonstrated a research tool called “VulScan” which is used to create automatic test cases to find vulnerabilities from the web system. These vulnerabilities could be in the form of SQL injection and Cross-Site Scripting (XXS). But the author fails to elaborate on the countermeasure strategies which are highly complex to understanding by the developers.

In [14], the authors provided an in-depth survey and also exhibited lots of mechanisms to find Vulnerabilities caused due to SQL Injection.They also delivered a few techniques and mechanismsto precludethe occurrence of these vulnerabilities while launching the websites. Prerequisite knowledge on Vulnerabilities supports the developer in developing an efficient secure code.

The work from [15] delivers extremely practicablemethodologies to detect the various form of vulnerabilities and they also delineate the categorization of SQL Injection attacks. Here, the prevention strategies or countermeasures are described only in the statement formulation.

The article from [16] demonstrated the idea to preclude CSRF (Cross-Site Request Forgery) which exhibits the additional authentication technique along with browser-based resolution.This technique is found to be hugeutilitarian from the perspective of

architecturalaspects but this is a kind of proficiencies which is not much practicable for the developer's side but it could be a very facilitator segmentespecially for software quality assurersand testers.

The research paper from [17] provided a required and complete study on the open issue of penetration testing which is very critical for Cyber Security. Here, the authors delineated these associated technical issues in a narrower form but fail to elaboratestandard countermeasure and solutions for the same issue.

The researchers from [18] described the state ofthe art review of various types of hacking approaches on the web system.They also delivereda relative study of detection tools in a comparable mode andSuggested several tools for countermeasures as a prevention strategy from these attacks.

From [19], the author presented a various testing methodological analysis for penetration testing of web systems. They also exhibited the conception of abuse cases,which wasnotable for penetration testing, however, such test cases fail to aid the developers to createan accurate system as per the desired outcomes.

3. GENERALIZED PERSPECTIVE OF CYBER-CRIME

The analysisset out with athoughtful follow-up regarding cyber-crimes current status, through thiscritical review ofspecialized existing work, international statute law (legal aspects), and historical realities of the last three years.The goal wasto attain a worldwide overview of the cyber-attacksacross the world, to realize the significances of functioning and possible impact upon business enterprise or individuals, besides the countermeasures to be taken as for dealing thejeopardizes. This research was based on attacks keyed out and tracked among the last three years. With the vastcount ofcyber-attacks set about on a day-to-day basis across the world, besides the boundedselective information companies mostlyexhibitwhenever they found to be the victim of cyber-crime and the conception that some approaches are difficult to be tracked, and it wasinconceivable for the authors to attain a perfect data set for analysis intents. Nevertheless, the analysis was based on thedataensued from combininginformationconcerning detected attacks and trackedfrom the last complete three years. Commonly the data are gathered from the news and attacks account, as well as from previous reports and surveys published by globally major market

participants on anti-malware overhauls and security consulting, thus attaining a targeted round sum of around 15 million attacks or approaches.

3.1. Primary Factors

On concerning the real facts about this study which tends to expose the rootcause of the security breaches. To a lesser extent, 50% of the illegal approaches are purported to intentional criminal attacks. The causes constituting three primary factors: Man-made errors, deliberate attacks, and the overall organization system vulnerabilities. Here, the outcomes delineate the fact that whenever an attack or intentional approaches succeed, it is only due to the partial proficiency skills of the attacker and prior cognition, and also on account of vulnerabilities at the victim's position – such as Man-made errors, defective programs, and deficient level of controls to assure some standard information security guidelines. In the year 2013, Cenzic organization has observed numerous security vulnerabilities in 96% of the analyzed applications coverage. Accordant to the 2014 Application Vulnerability Trends Report, it's been stated that with an average of 14 vulnerabilities for any single application.

3.2. GeneralizedReview on Attacks

All around the analysis, it was difficult to decide the precise count or vital component of the various attack type. However, the majority of these kinds of attacks are:

- Malicious Codes
- Worms
- Trojans
- Malware
- Denial of Service
- Viruses
- Web-Based Attacks
- Stolen Devices, And
- Phishing
- Social Engineering, And
- Malicious Business/Corporate Executive,

The final resolutions could easily besegregated into four classes, which are based on the targeted plan/ultimate goal of the attack, they are;

- Cyber Espionage
- Hacktivism
- Cyber-Crime, And
- Cyber Warfare.

3.3. Cyber Espionage

Cyber espionage [11] is a type of cyber-attack that grabs the most restricted, sensible information or IP (Intellectual Property) to benefit some vantage over a competitor Organization.

3.2.1 Hacktivism

Hacktivism portrays the act of maltreating a network system for a politically or socially prompted intellect. The person who executes hacktivism is referred to as hacktivists.

3.2.2 Cyber-Crime

Cybercrime [10], sometimes referred to as e-crime which necessitates a web-connected system and a network. The particular system or network will be utilized to equip for crime service into other targeted subjects.

3.2.3 Cyber Warfare [12]

On the utilization of digitalization across the world, the attackers tend to attack anenemy's network infra nation, leading to destruction, thus disables the entire or partial communication system of the targeted nation.

3.4. Dissipation across various sectors

This study disclosed the realism about the organization of versatile sizes and how the business spheres have been influenced and became the primary victims of cyberattacks for the last three years. Irrespective of the entity’s business sector and size, all the fields, right from the public sectors (Government, Education, Enforcement, Healthcare, and Law), and somenon-profit

organizationstill to the private sectors(like media, finance, Tourism,online services, retail, internal security, telco, automotive, food & beverage, and energy & utilities)are targeted by cyberpunks for major attacks. In connection with the geographical split oriented attacks, thiscogitationis prominently focused on two linear perspectives: the geographic origin of the attacks, and their destination. As per the study's outcomes, it's been revealed that the few countries are targeted as the source of the attack, are:

- Canada,
- France,
- Germany,
- Romania and others.
- Russia,
- Netherlands,
- UK,
- Ukraine,
- USA,
- Vietnam,

Concurrently, it is found that the regular frequent victims arelocated in Russia, the USA, and the UK.

3.5. Cyber-attacks Impacts

Concerning the impact that cyber-attacks deliver upon their victims, it is difficult, and sometimes not possible enough to quantitates the precise costs of the organizations which always expect for recovery process for their regular business, customers' faith, and reputation, especially considering that victimized organization do not perpetuallyexpose all the security concerned information to the populace.However, the outcomes depict theimpact of cyber-hackings which normally leads to the loss of selective information, business commotion, and revenue loss, and device or instrumentation damages. Such kind of attacks allows forunauthorizedadmittance of intruders, especially to profile information (meta-source)that comprises data sets likepersonal IDs, full names, surname, Date-of-birth, official and residential addresses, financial and medical

records, mobile numbers, and official mail-ids addresses, important credentials, and insurance policy details.

3.6. Cybersecurity Correlations, Trends and Patterns

This study discloses concerning results, trends, and patterns. Foremost, the consequencesdelineate a proportional correlationamong the business sector and the different types of attacks; thus, cyber espionage is majorly targetingMedia, Law Enforcement sectors, Government, and alsounconvincing targeting other commercial sectors (Online Services, Telco, Retail, etc.). The resultants for the past three years delineate a relatively firm correlation among the types of attacks and manufacturing sectors. The correlation demonstrates the cases of targetingthe public sector (government, lawenforcement, education, etc.) likely by cyber espionage, wherein all business sectors are targeted by hacktivism, cyber-crime, and cyberwartechniques.

The analysis results exhibit that the attacks are not only fromexternal hackers but fragmentationamong them and organization associated factors (current or former employees, partners, management, etc.). These consequences draw a few more trends,attaining the source'strust regardingunauthorizedforcibleaccessionendlessly loses base against unauthorizedlegitimateaccession to secured information. Likewise, it’s beenillustrious that there is anuninterrupted incremental issue through the mobile attacks, from which the sources believedto be instinctivedeliberationon the dissipation of smartphones thatmay evident to be aleisure target. All these effects are illustrated as the forcible forerunner to the unrecognized actions due to the permanentestablishment through the internet, utilization of a social network and other public-oriented applications, besides the realities that they arehardly switched off and comprise/hold back a lot of personal data (from the first name, mobile number and locating to the device to the recently connected network, etc.).

3.7. GeneralizedOutcomes

The cogitation was based on a targeted round sum of around 15 million attacks or approaches, that werecompiledacrosspast news and events, as well as accounted records set bykey players in the industry sectors concerning security. Some primary key players are the Federal Bureau of Investigations (FBI), Kaspersky Cenzic, CISCO, Mandiant, Sophos, Verizon,

hackmageddon.com, McAfee, PriceWaterhouseCoopers, Symantec, and FireEye.The“Threats Predictions 2015 reported by McAffee Labs, expose the estimate that cyber-attack will engage a raisingtrend, sketching the anticipation of heightened espionage and cyber-warfare, also toughened by cyberpunks /hackers’ improvedschemes and tools for concealing their individuality/emplacement and finally, receivesensibleinformation. As per the report, ‘Attacks on IoT (Internet of Things) devices and its peripherals will enhance speedilybecause ofoveractivegrowth in the count of associated objects, haplesssecurity hygienic, and the high-pitchedmeasure of information on the devices associated with IoT domain, also estimating an approximatedcount of 50 billiondevices to be linked to the cyberspace by 2019. The outcomesdelineate the reality that attackers seemingly without any interruptionevolve newmodes to exploit the secured programs, Information, and networks. On the other hand, on yearly basis, a trend that has been observed is the uninterruptedincrement ofhand-helddevice based attacks or approaches.

4. VULNERABILITY DETECTION METHODOLOGY

In this research article,a novel vulnerability detection methodology has been proposed, in which well-framed attacking scenarios are performed on a sample webpage. This page hasa vulnerable code to test out the proposed attacking scheme. On the detection of vulnerabilities, a standard and suitable countermeasure have been suggested. The entire process has been depicted in Figure1.

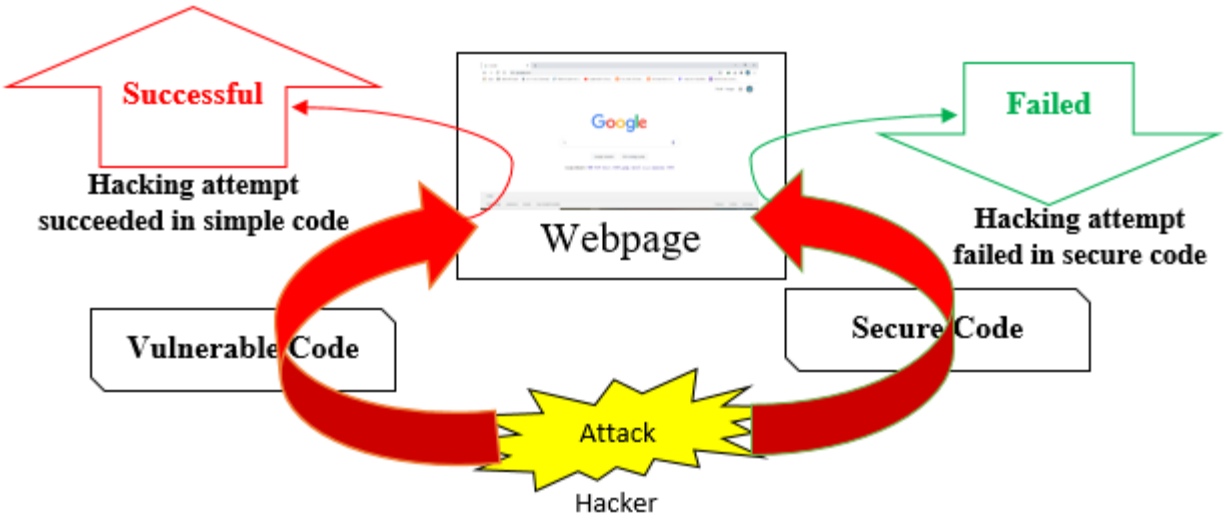

Figure 1. Vulnerability Detection Methodology

In this article, two major types of vulnerabilities have opted for experiments analysis, which is already discussed in section 2. They are

- SQL injection-based experiment
- Cryptography

Based on the aforementioned experimental results, suitable countermeasures are suggested to tackle different types of vulnerabilities in section V.

4.1. SQL injection-based experiment

Normally SQLstatements are text-only statements, which makesit the hackers easy to alter the Statement.Here come the concepts of “tautology”. Tautology-based SQL injection s a process of bypassing the authentication and derives partial or complete information/data through the WHERE clause of any query.Example: Valid data to be enteredin the field of username & password is given aswhich is based on "or"=" string.Figure 1and 2 depicts anHTML login page and a relevant PHP code in which data is given through the user and standard authentication procedures are followed.

4.2.1 Unsecure Code

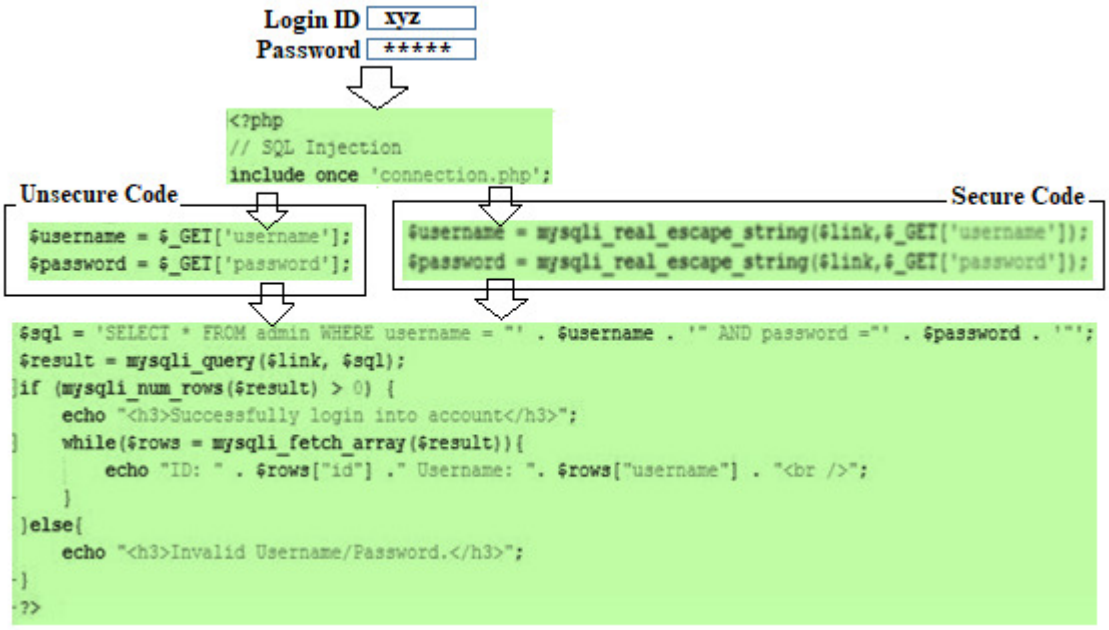

Figure 2. Unsafe and safe PHP code

Here, the tautology process ofcasting an erroneousness to make the application to certify the string that is not encapsulating quotes correctly.This way of attacking the SQL query statement, where it constantly conceived to be true on account of "has row" logicin the codification part as illustrated in Figure. This SQL injection attack is primarily employed by the hackers intothe query part of the "WHERE" clause. Since the statement is made as a tautology (i.e.: 1=1); queryaffirmation consequence will always be true. In this way,the hacker obtains all the tuples/records of the table in this case hacker getall rows from the table as depicted in Figure 3.

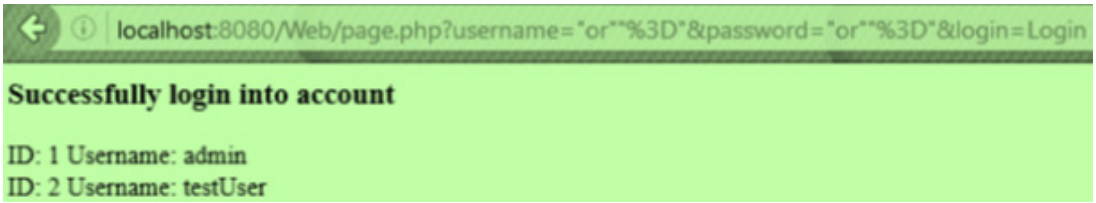

Figure 3: Outcomes of the SQL Injection Attack

4.2.2 Secure Code: Countermeasure

To tackle the vulnerability caused by SQL injection, code developers are supposed to validate credential data as“mysqli_real_escape_String”, where v1 and v2 are escaping special characters required to be utilized for constructing the SQL statements for security reasons. Normally,in the secure PHP code depicted in the figure, the credential data are validated and filtered before stored in the database. Whenever a user feeds string data like"or" "="into fields of username and password respectively, the coded function automatically creates a legal query statement by escaping the special character from the input, later then, which are usually converted as "\or\" and "\=\". Thus, a suitable countermeasure has been suggested.

4.2.3 Cryptography

Cryptography is a special domain in the field of computer science in which original data is encrypted (ciphered) and as of requirement of the user, the ciphered data is decrypted. Both the encryption and decryption are handled through Mathematics logic to enable secure communication. To transfer and receive the most sensitive information acrossthe network (internet), cryptography techniques play a vital role. Figure 4 depicts the basic working mechanism of the cryptography technique.

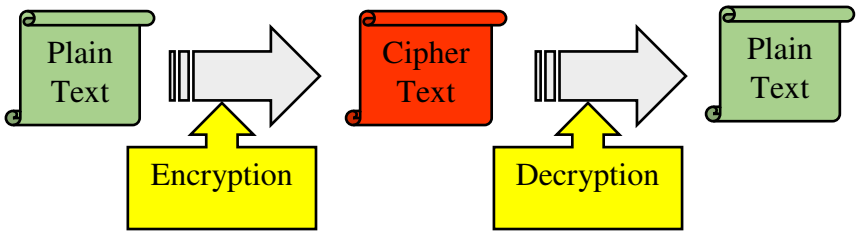

Figure 4. Simple Cryptography Process

Allsensitiveinformation should be stored and transmitted securelyon the internet. The cryptography technique ensures that the data transferred between source and destinations are highly secured and prevents any intrusion by hackers to the maximum extent. Suppose a string like "WELCOME" is needed to be encrypted. Then a specified schema is framed as per the user choice, Example:

A B C D E F G H I J K L M N O P Q R S T U V W X YZ

A schema for encryption and decryption.

e f g h i j k l m n o p q r s t u v w x y z a b c d

Where W=a, E=i, L=p, and so on. On utilizing this, plain text "WELL" encrypt as "aipp".

5. CYBERSECURITY COUNTERMEASURES

Most of the unauthorized accession is seemly growing in a sophisticated and broader way, with even many organization secure schemes that were once conceived secure enough versus various menaces now being opened to dangerous cyber-attacks. Thus, this study exposes the suitable countermeasures against various cyber-attacks in association with different sectors like the secure status of industrial bodies, Certification (authentication).

Relying upon the risks to be dealt with, various control conditions and periodic checks may be enforced to assure theintegrity, confidentiality, and availability of primary information. Controls may vary from one organization to another, and maybeclassified as:

5.1 Secure Status of Industrial Bodies

Organizations are supposed to ensure that all their deployed instrumentation (hardware and software), including security software like antivirus, is unremittingly updated as per the current requirement, the most recent set of commands (patches) are installed with the total exclusion of errors. Also, industries need to guarantee the upgrade services and maintenance coverage through third party agreement provided software.

5.2 Certification

Relying upon the endangerment assessment, admittance to the company’s schematic codes and data must be always saved solely by an encrypted instruction or password. Nevertheless, particularly for web-based applications or remote access, to ensure the safeness, it is encouraged to employ morecomplex authentication entails like in leastways, aggregating any two of the following: “something you generate” (e.g. known password),“something you have chosen” (e.g. stochastic PIN generating device), and “something you provide” (e.g. biological identity verification).

5.3 Grant to Access Information

Top stakeholders of any organization should frame the regulation which assures the automated accessibility conditions through appropriate restrictions and timely terminations for

departers, declarers,comptroller and all third parties those who have the previous association to the business network. A wide range ofverification may dealwith these risks, from manual verification (e.g. occasionalfollow-upon all exploiter access rights) to automatedverification will assure tight security enhancements. (e.g. automated removal of inactive domain records that have no relation to the network).

5.4 Enhancing the level of informationretentiveness

Removing all information isconsidered to be of no use for routine business activities. But retrieval and storage of vital and primal information in advanced back-up servers always assures safer environs. Limiting the control of vital data minimizes the risk factors associated with unauthorized access. (Particularly 20% data stored on the network server of any organization to which most of the victims have no prior knowledge).

5.5 Additional security checks

Detective checks – this kind of checks driven to detect any menace to the data security (e.g. even ifthe unauthorized approach was contacted, IDS (Intrusion Detection System) supervises the network traffic and distinguishes thedefendant access from the right one);

Preventive checks – Thesesecurity checkare commonly utilized to forestall the rise of any threat (e.g. constrainingthe illegal access to the organization information, programs, and network systems which autonomously restricts any unauthorized access).

Corrective Checks – Here, the security checksdeal to counterbalancethe keyed out irregularities (e.g. recovery ofregular business routineto the Subsequent of any attack).

6. CONCLUSIONS

There is a broad space for advancement in the globalcombat against cyber-crime activities. This article aids to enhance the cybersecurity of network systems at the organization level (small, mid, or large), and also created better awareness against the keyed out vulnerabilities in various sectors. This composition theory also presents variouscountermeasures and it is also found that after choosing the suitable countermeasures, the selected web page was secured and the preferred set of instructions fails to accomplish the vulnerable input strings.

Besides this, the study comprises the evolution and trends of cyber-crime along with their suitable countermeasuresespecially concentrating on the global awareness concerning cyber-crime and regulativedeterminations. Finally, all these facts entailed defending the cyber-security domain. For future enhancementdiversified approaches to the rise of novel vulnerabilities cases are considered tohave experimented for the advanced build-up of the security system (at the domain level and organization level).

REFERENCES

[1]. Security. I, and Report. T., "Symantec, Internet Security ThreatReport," Vol. 22, No. 04, 2017.

[2]. Tomanek, M, and Klima, T.,2015. "Penetration Testing in Agile SoftwareDevelopment Projects",International Journal on Cryptography and Information Security, Vol. 5, No. 1,pp. 01-07.

[3]. Bendovschi, A.,2015. "Cyber-Attacks-Trends, Patterns and SecurityCountermeasures", Procedia Economics and Finance, Vol. 28, No. 04, pp.24-31.

[4]. Bertoglio, D.D, and Zorzo, A. F., 2017."Overview and open issueson a penetration test," Journal of Brazilian Computer Society, Vol. 23, No. 1, pp.1-16.

[5]. Qian, L, Zhu, Z, Hu, J, and Liu, S., 2015. "Research of SQL injectionattack and prevention technology",Proceedings of International Conference on Estimation, Detection and Information Fusion, (ICEDIF 2015), No.123456, pp. 303-306.

[6]. Yan, F, and Qiao, T., 2016. "Study on the Detection of Cross-Site ScriptingVulnerabilities Based on Reverse Code Audit",International Conference on Intelligent Data Engineering and Automated Learning, pp. 154-163.

[7]. Al-Abiachi, A. M.,Ahmad,F, and Ruhana,K., 2011. "A competitive studyof cryptography techniques over block cipher," 13th International Conference on Computer Modelling and Simulation, UKSim 2011, pp. 415-419.

[8]. Zeng, H., 2014. "Research on developing a lab environment for cross-siterequest forgery: Attack and defense education in higher vocationalcolleges," 3rd International Conference on Computer Science and Network Technology, (ICCSNT 2013), pp. 56-60.

[9]. Uma, M., and Padmavathi, G., 2013. “A survey on various cyber-attacks and their classification”, International Journal of Network Security, Vol. 15, No. 5, pp. 390-396.

[10]. Alshaikh, M., 2020. “Developing cybersecurity culture to influence employee behavior: A practice perspective”, Computers & Security,Vol. 98, pp. 1-10.

[11]. Jean-Paul A. Yaacoub, Ola Salman, Hassan N. Noura, Nesrine Kaaniche, Ali Chehab, and Mohamad Malli, 2020. “Cyber-physical systems security: Limitations, issues and future trends”, Vol. 77, pp. 1-40.

[12]. Robinson, M, Jones, K, Janicke, H, and Maglaras, L., 2018. “An introduction to cyber peacekeeping”, Journal of Network and Computer Applications, Vol. 114, pp. 70-87.

[13]. Huang, H.C, Zhang,Z.K., Cheng,H.W., and Shieh, S.W., 2017. "Web Application Security: Threats, Countermeasures, and Pitfalls", Computer (Long. Beach. Calif), Vol. 50, No. 6, pp. 81-85.

[14]. Elshazly, K, Fouad, Y, Saleh, M, and Sewisy, A.,2014. "A Survey of SQL Injection Attack Detection and Prevention", J. Computer Communication, Vol. 2, No. 8, pp. 1-9.

[15]. Singh, J. P., 2017. "Analysis of SQL Injection Detection Techniques”, Theoretical and Applied Informatics, Vol. 28, No. 1 & 2, pp. 37-55.

[16]. Nagpal, B,Naresh, C, and Singh, N., 2016. "Articles Additional Authentication Technique: An Efficient Approach to Prevent Cross-Site Request Forgery Attack”, I-manager’s Journal on Information Technology, Vol. 5, No. 2, pp. 14-18.

[17]. P. S. Shinde and S. B. Ardhapurkar, "Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing," 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare, pp. 1-5, 2016.

[18]. Shabut, A. M., Lwin, K. T., and Hossain, M. A., 2016. "Cyber-attacks, countermeasures, and protection schemes - A state of the art survey,"10thInternational Conference on Software, Knowledge, Information Management & Applications (SKIMA), pp. 37-44.

[19]. Dawson J., and McDonald, J. T., 2017. "Improving Penetration Testing Methodologies for Security-Based Risk Assessment", Cybersecurity Symposium(CYBERSEC 2016), pp. 51-58.