

SQL injection and ethical hacking: threat analysis and vulnerability detection

Vinnitsia National Technical University

Анотація

Стаття досліджує роль етичного хакінгу в кібербезпеці, підкреслюючи його важливість у виявленні вразливостей до того, як ними скористаються кіберзлочинці; описує структуровані етапи та етичні норми, яких повинні дотримуватися етичні хакери. Однак, виникають занепокоєння щодо можливого зловживання навичками хакінгу. Стаття також виділяє SQL-ін'єкції як серйозну загрозу безпеці та обговорює необхідність впровадження передових заходів безпеки, включаючи рішення на основі штучного інтелекту, такі як нечіткі нейронні мережі, для підвищення ефективності запобігання кібератакам.

Ключові слова: етичний хакінг, SQL-ін'єкція, White-Hat хакери, витік даних

Annotation

The article explores the role of ethical hacking in cybersecurity, emphasizing its importance in identifying vulnerabilities before cybercriminals exploit them. It outlines the structured phases ethical hackers follow and the ethical guidelines they must adhere to. However, concerns are raised about the potential misuse of hacking skills. The article also highlights SQL injection as a major security threat and discusses the need for advanced security measures, including AI-driven solutions like fuzzy neural networks, to enhance cyberattack prevention.

Keywords: ethical hacking, SQL injection, White-Hat Hacker, data leakage

As the number of fraudulent activities increases, organisations face a significant problem, how to protect a public reputation and sensitive information. Fraud has caused financial losses for more than half of financial institutions, with fintech companies and regional banks being the most affected. Moreover, last year, the United States witnessed data breaches. Data leaks have increased by 72% since 2021, affecting over 300 million people and causing financial losses of nearly \$5 million per breach, according to a Forbes report. [1]

With the increasing frequency of fraudulent activities and advancements in technology, the demand for computer security specialists has grown significantly. These professionals, also known as "White-Hat Hackers" or "Ethical Hackers," hack into systems to identify vulnerabilities and fix them, thereby improving the security of an organization. White-hat hackers use their expertise to protect companies before malicious hackers, known as "crackers," can exploit these vulnerabilities.

Ethical hacking also known as "Intrusion Testing", "Penetration Hacking" or "Red Teaming" is the practice of hacking without malicious intent. Ethical hackers use the same techniques and tools as cybercriminals, but they neither damage the systems nor steal sensitive data. Instead, they assess target systems for weaknesses and report their findings to the organization along with recommendations for addressing vulnerabilities. However, ethical hacking should not be mistaken for a guarantee of complete security; rather, it is a method of risk assessment. The result of ethical hackers' work is a detailed report on the assessed system, highlighting discovered vulnerabilities and proving whether a hacker, given a certain level of knowledge and time, could successfully carry out a cyberattack or data breach. Ethical hacking exposes risks within an IT environment and proposes actions to mitigate them. [2, p.7].

The Ethics of Ethical Hacking

Students who study ethical hacking gain comprehensive knowledge of how to breach computer systems or exploit vulnerabilities in order to prevent such attacks. However, how they choose to use these skills remains an ethical concern.

The increasing reliance on technology in business has led to most transactions being conducted electronically. Ethical hackers could potentially misuse their knowledge to bypass payment systems, exploit software vulnerabilities after conducting penetration tests, create and distribute malware, or find ways to avoid paying for services.

White-hat hackers can also contribute to the rise of cyberattacks by using the commercial package Acunetix, which tests vulnerabilities in web applications. This package has many cracks that lead to easy data leakage[3, p. 3759 - 3760]

Therefore, in order to avoid causing harm, the work of ethical hacker involves the following requirements:

Respecting Privacy: Attitude to collected information must be completely respectful. Any data obtained during testing, including log files or plaintext passwords, should remain private.

Working ethically: Employees must have high professional morals and principles. Every action must align with the company's goals and be fully authorized. No hidden agendas or misuse of information are permitted. Trustworthiness is the ultimate goal.

Adherence to the precepts of ethical hacking: Ethical hackers should adhere to fundamental ethical principles, which are often overlooked or ignored during testing.

Executing the plan: Time and patience are important in ethical hacking.

System crashing by ethical hackers is prohibited: Running too many tests simultaneously may overload and crash a system. There are a lot of security assessment tools that can control the number of tests running at once [4, p.7576].

Ethical hacking follows structured phases to identify vulnerabilities, mirroring cybercriminal techniques to gain a deeper understanding of system weaknesses.

Hacking phases:

Phase 1: Reconnaissance (active or passive): Passive reconnaissance involves gathering data about a target without the organization's knowledge. This can be achieved through bribing employees or searching public online sources. This step is also known as "information gathering". In this approach, a hacker doesn't need to attack the network or system of the company for gathering the data .

Phase 2: Scanning: Collected information used to examine the network. Tools such as port scanners and dialers help hackers detect system vulnerabilities.

Phase 3: Owning the system: Hackers use the gathered data to penetrate Local Area Network (LAN, Wireless or Wired), Local PC Access.

Phase 4: Zombie system: After gaining access, hackers attempt to preserve their control over the system by making modifications that prevent security personnel from detecting their presence.

Phase 5: Evidence Removal: Hackers erase all log files and intrusion detection system (IDS) alerts to avoid detection. This process helps cybercriminals evade prosecution [5, p. 3391].

The main threats to information security are attacks aimed at modifying data. SQL Cracking (cracking SQL passwords) are the most common methods of unauthorized access to data. This process involves the use of various techniques to expose or bypass authentication mechanisms, which lead to the leakage of sensitive information.

Researches have proved that query injection can be applied without double dashes(--), space or single quotes. Bypass authentication conducted by passing the query in such a way, which accesses the unauthorized information.

For example SQL statement:

```
SELECT CREDIT_CARD_INFO FROM client
WHERE username=' or 1=1 -- 'AND password=';
```

This SQL injection will be executed because $1 = 1$ is always true. Additionally " - -" is used for comments, causes ignoring statements after the comment marker.

Unauthorized Knowledge of Database can also be used for authentication evasion. This attack method relies on the injection of a query which causes a logical, or syntax error into the database. Resulting from incorrect querying is a form of error message generated by database, which contains information regarding database and intruder can use these details.

An error message generated by a database due to a logical, or syntax error, can contain sensitive information about the database, which an intruder can exploit.

This method of SQLIA:

```
SELECT CREDIT_CARD_INFO FROM client
WHERE username = 'rahul' AND password = CONVERT (SELECT host FROM host);
```

The error message of this logically and syntactically incorrect query will contain some information regarding database (even some error messages display the table name also)

Unauthorized Remote Execution of Procedure allows attackers to perform tasks and execute the procedure for which they are not authorized.

For example:

```
SELECT CREDIT_CARD_INFO FROM client
WHERE username='' ; SHUTDOWN; AND password ='';
```

Only SHUTDOWN operation is performed, which shuts down the database.

If an additional query is injected into the main query and main query generates Null value, the second query will still be executed. The additional query can harm databases and technique is known as Injected Additional Query.

Example:

```
SELECT CREDIT_CARD_INFO FROM client
WHERE username='rahul' AND password=''; DROP TABLE user';
```

In numerous systems, a blank password is either not permitted or hashed and stored as a different value. Consequently, as a result the first part of the query, which contains password='' generates Null. The system executes the second part and the table will be dropped, provided this table exists in the database.

Injected Union Query involves injecting a query using set operators, where the main query returns Null value but the attached set operator retrieves data from the database.

For example SQL injection:

```
SELECT CREDIT_CARD_INFO FROM client
WHERE username='' AND password=''
UNION SELECT CREDIT_CARD_INFO FROM client
WHERE client_id='10125';
```

In the above query, the first part (which contains WHERE username='' AND password='') generates a Null value but the injected query allows retrieving credit card information of a user with id 10125.[6, p. 2008 - 2009]

Conclusion

SQL injection is the most common attack vector, which is used by intruders and white-hat hackers. Nevertheless, classic tools are not enough to counteract data leaks, underscoring the necessity to employ the fuzzy neural networks model to analyse SQL queries.

The first two layers of the model are considered a fuzzy inference system, with capacity to extract knowledge from the transforming them into fuzzy rules. The third layer consists of a simple neuron, which can activate the methodology leaky ReLU. First layer is constituted by fuzzy neurons, which activate a Gaussian membership function. The values of bias and synaptic weights for neurons in the first layer are defined at random within the interval [0, 1].

The second layer consists of fuzzy logic neurons Lc, among which a unineuron is distinguished. Each neuron performs a weighted aggregation of outputs of the first layer along with randomly determined weights and biases.

Logical neurons combine the logical aspects of processing with learning through a system of fuzzy rules. They can be explored as multi-variable nonlinear transformations.

Unineurons employ uninorms, a generalisation of t-norms and s-norms, for permitting flexible alterations in the manner of input data processing, ranging from pure conjunction (t-norm) to disjunction (s-norm). This facilitates effective adaptation to different tasks by combining inputs according to their importance.

The aggregation of values in neurons occurs in two stages: firstly, inputs are combined with weights, and secondly, the global aggregation of the obtained results is performed. Logical neurons can be understood as a selection of the most significant rules describing the input space. The LARS method is used to determine the optimal selection of neurons, which allows to highlight the most significant variables while avoiding overtraining. Furthermore, the Bolasso method is employed to enhance the stability of neuron selection through bootstrapping. The final stage of processing involves the utilisation of a neural aggregation network that classifies cyberattacks using the leaky ReLU activation function [7, p. 13 - 17].

The proposed fuzzy neural network model offers a more adaptive approach to analyze SQL queries. Integration of function Leaky ReLU activation improves cyber classification.

The future research works need to be focused on improving fuzzy network model and optimizing the training process. Additionally further inspection of the model on large-scale data sets will ensure its effectiveness in ethical hacking

REFERENCES

1. "Cybersecurity Stats: Facts And Figures You Should Know", [Online]. Available: <https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/>
2. B. Sahare, A. Naik, and S. Khandey, "Study of ethical hacking," International Journal of Computer Science Trends and Technology (IJCTST), vol. 2, no. 6, p. 6, Nov.-Dec. 2014. [Online]. Available: www.ijcstjournal.org
3. J. Danish and A. N. Muhammad, "Is Ethical Hacking Ethical? ", International journal of Engineering Science and Technology, Vol 3 No. 5, pp. 3758-3763, May 2011.
4. Juneja, Gurpreet K. "Ethical hacking: A technique to enhance information security." International Journal of Innovative Research in Science, Engineering and Technology 2.12 (2013): 7575-7580.
5. K.Bala Chowdappa et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3389-3393
6. Mehdi Kiani, Andrew Clark and George , "Evaluation e Detection of SQL Injection Attacks".The Third International Conference on Availability, Reliability and Security,0-7695-3102-4/08, 2008 IEEE.
7. Lucas Oliveira Batista, Gabriel Adriano de Silva, Vanessa Souza Araújo, Vinícius Jonathan Silva Araújo, Thiago Silva Rezende, Augusto Junio Guimarães, Paulo Vitor de Campos Souza. "Fuzzy neural networks to create an expert system for detecting attacks by SQL Injection." arXiv preprint arXiv:1901.02868 (2019).

Базилюк Анастасія Дмитрівна – студентка групи 1 АКІТР-23б, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, e-mail: nastyabaz434@gmail.com

Науковий керівник: Крютченко Олена Олександрівна, викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, e-mail: olena.kriut@gmail.com

Anastasiia Bazyliuk Dmytrivna – student of group 1 AKITR-23b, Faculty of Intelligent Information Technologies and Automation, Vinnytsia National Technical University, e-mail: nastyabaz434@gmail.com

Scientific supervisor Kriutchenko Olena Oleksandrivna – a teacher of English, a Department of the Foreign Languages, Vinnytsia National Technical University, e-mail: olena.kriut@gmail.com