УДК 004.05

Ювковецький О.С.
Войтович О.П.

НАВІСНИЙ ЗАХИСТВІД SQL-ІН'ЄКЦІЙ

Вінницький національний технічний університет

Анотація: *існуючі вразливості web-ресурсів ставлять під загрозу нормальну роботу інформаційно-комунікаційних систем. Найбільш поширеними загрозами web-ресурсів є sql-ін'єкції. У даній статті описані відомі підходи для захисту від sql-ін'єкцій, а також запропоновано навісний захист для фільтрації вхідних даних.*

Ключові слова: *Вразливість Web-ресурсів, Web-додатки, класифікація вразливостей Web-ресурсів, SQL-ін'єкція.*

Abstract: *Existing vulnerabilities of Web-resources threaten the regular work of information systems. The most common Web-resource vulnerability is SQL Injection. This article describes the known approaches to protect Web-applications against SQL Injection attacks and offers SQL Injection prevention system for filtrating incoming data.*

Keywords: *Web-resources vulnerabilities, Web-applications, classification of Web-resources vulnerabilities, SQL Injection.*

Більшість Web-ресурсів не відповідають сучасним вимогам безпеки. Вразливості Web-ресурсів можуть поставити під загрозу імідж, фінанси, активи, персональні дані та інші цінні ресурси організацій, а отже як підсумок можливе банкрутство або повна ліквідація компанії.

На сьогоднішній день існує велика кількість класифікацій [1], які систематизують різні види вразливостей та атак, що на них базуються, за різноманітними параметрами. Розглянуто такі класифікації як OWASP [2], систематику Маркова [3], реєстр вразливостей CAPEC, класифікацію загроз WASC [4], модель загроз Microsoft STRIDE та класифікацію лабораторії Касперського [5]. У цих та інших джерелах описані основні вразливості Web-ресурсів та атаки на них [6].

Найбільш поширеними загрозами web-ресурсів, які виділені в усіх класифікаціях як найнебезпечніші, є SQL-ін'єкції. SQL - ін'єкція - це вразливість, яка виникає при зверненні Web-додатку до бази даних. Це один з поширених способів злому сайтів і програм, які працюють з базами даних.

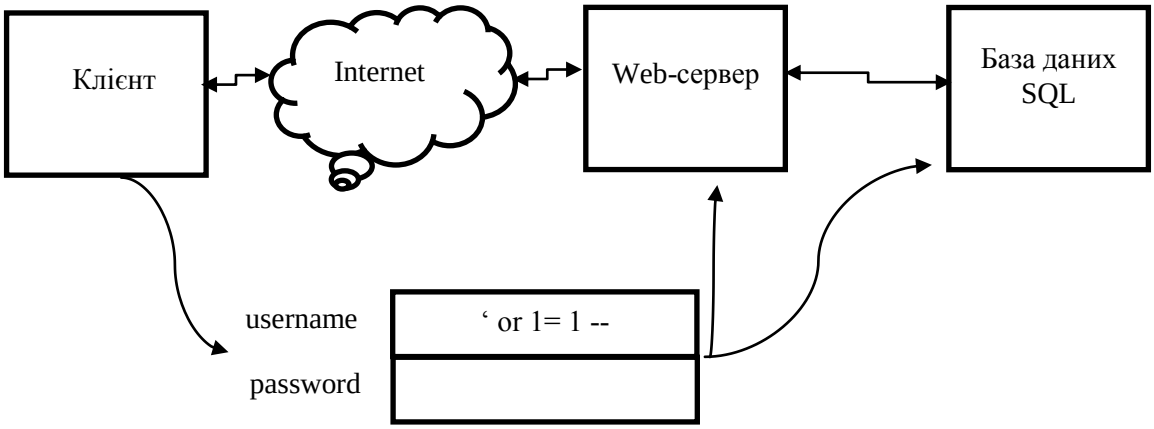

Рисунок 1 – Реалізація SQL-ін'єкції

SQL-ін'єкція, в залежності від типу використовуваної СУБД і умов впровадження, може дати можливість атакуючому виконати довільний запит до бази даних (наприклад, прочитати вміст будь-яких таблиць, видалити, змінити або додати дані), отримати можливість читання і / або запису локальних файлів і виконання довільних команд на сервері [7].

Атака за допомогою використання SQL-ін'єкцій стає можливою через некоректну обробку вхідних даних, що використовуються в SQL-запитах.

Для захисту від SQL-ін'єкцій запропоновано навісний захист, який виконує три функції:

1. Екранування одинарних і подвійних лапок.

Передаючи разом із значенням будь-якого строкового параметра одинарні або подвійні лапки (в залежності від їх використання в додатку), хакер може внести зміни в структуру формованого SQL-запиту. Якщо параметр, який передається, в рядку запиту обрамляється в одинарні лапки, то отримавши в запиті разом із значенням параметра одинарні лапки 'і символ коментаря - (або / *), додаток обробить такий запит без помилок.

```
$name = $db->real_escape_string($_POST["name"]);
$query = "SELECT * FROM `users` WHERE `login` = "".$name."""";
```

2. Перевірка типу або примусове задавання типу даних.

Необхідно перевіряти усі дані, що вводяться користувачем, виконуючи перевірку типу, довжини, формату і діапазону даних. При реалізації запобіжних заходів, спрямованих проти зловмисного введення даних, враховується архітектура і сценарії виконання програми. Наприклад, якщо за задумом в змінній, яка згодом вставляється в запит, повинні зберігатися числові дані, необхідно використовувати примусове приведення отриманого типу до числового.

```
$id = settype($_GET["id"],"integer");
$email = settype($_GET["id"],"varchar");
```

3. Перевірка структури вхідних даних за допомогою регулярних виразів.

Якщо за задумом передбачається, що вхідні дані мають певну структуру, наприклад це e-mail клієнтів, телефон або дата - то є сенс "прогнати" такі значення через регулярні вирази. Тим самим, перевіряється точність введених даних і одночасно відсікаються усі небажані символи і неприпустимі модифікації переданих вхідних даних. Однак, регулярні вирази можна використовувати і в разі простих запитів. Наприклад, за допомогою можна переконатись,що вхідний параметр це чотирьохзначне число, або що це тільки рядкові латинські літери, кількістю від 5 до 10 символів.

```
$email = $_POST["mail"];
if (preg_match("/^\w @[a-zA-Z_] ?\.[a-zA-Z]{2,6}$/",$email)) {
  // формуємо запит до бази даних
} else {
  // виводимо помилку або формуємо строку запиту за замовченням
}
```

Таким чином, запропоновано навісний захист, який виконано у вигляді набору скриптів, які підключаються на сторінки Web-ресурсів. Це дозволяє запобігти виконанню атак за допомогою SQL-ін'єкцій. Необхідно розуміти, що зловмисники використовують різні методи, які для різних баз даних працюють по-різному, тому одна і та сама атака на сайт з використанням СУБД MySQLі на сайт з використанням СУБД PostgreSQLбуде мати різні наслідки. Даний навісний захист в основному розрахований на роботу з MySQL, так як за статистикою саме ця система управління баз даних використовується на 56% сайтах у мережі Internet.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] СТАТИСТИКА УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ 2012 [Електронний ресурс]. – Режим доступу:URL: http://ptsecurity.ru/download/analitika_web.pdf - Назва з екрану.

[2] 2013 Top 10 Vulnerabilities List [Електронний ресурс]. – Режим доступу:URL: https://www.owasp.org/index.php/Top_10_2013-Top_10 - Назва з екрану.

[3] Марков А. С. Систематика уязвимостей и дефектов безопасности программных ресурсов / А. С. Марков, А. А. Фадин [Електронний ресурс]. – Режим доступу:URL: http://www.npo-echelon.ru/doc/is_taxonomy.pdf- Назва з екрану.

[4] Common Web Application Vulnerabilities [Електронний ресурс]. – Режим доступу:URL: https://cve.mitre.org/- Назва з екрану.

[5] Защита от эксплойтов в Антивирусе Касперского [Електронний ресурс]. – Режим доступу: URL: http://www.kaspersky.ru/downloads/pdf/technology_auto_protection_from_exploit.pdf/ - Назва за екрану.

[6] Класифікація вразливостей Web-ресурсів [Електронний ресурс]. – Режим доступу: URL:http://itce.pu.if.ua/files/topics/Voytovych-Yuvkovetskyi.pdf

[7] SQL Injection Attacks and Defense, Second Edition, Justin Clarke , Syngress, 576 ст. - 2012

Ювковецький Олександр Сергійович факультет інформаційних технологій так комп'ютерної інженерії, студент групи БС-12б, Вінницький національний технічний університет, Вінниця, hockenhaim@gmail.com.

Войтович Олеся Петрівнакандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, voytovych.op@gmail.com.

Yuvkovetskyi OleksandrInformation Technologies and Computer Engineering department, BS-12b student, Vinnytsia National Technical University, Vinnytsia, hockenhaim@gmail.com.

Voytovych O.P *Ph.D*, Vinnytsia National Technical University, Vinnytsia, voytovych.op@gmail.com.