МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ
КАФЕДРА КОМП’ЮТЕРНИХ НАУК

ШУТКО БОГДАН ЮРІЙОВИЧ

УДК 004.73

ДОСЛІДЖЕННЯ ПОШИРЕНИХ ВРАЗЛИВОСТЕЙ ВЕБ-САЙТІВ ТА МЕТОДИКИ ЇХ УСУНЕННЯ

124 «Системний аналіз»

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2019

Роботу виконано на кафедрі комп'ютерних наук Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат технічних наук, доцент кафедри комп'ютерних наук
Назаревич Олег Богданович,
Тернопільський національний технічний університет імені Івана Пулюя

Рецензент: доктор технічних наук, професор кафедри комп'ютирних систем та мереж
Лупенко Сергій Анатолійович,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 24 грудня 2019 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії №29 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 46, навчальний корпус №1, ауд.702.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Веб-сервери постійно піддаються безлічі самих різноманітних небезпек. Причому найсерйознішу загрозу становлять для них хакери і віруси. Перші можуть отримати доступ до конфіденційної інформації, розміщеної на сервері, зламати сайти і підмінити їх вміст, а також вивести з ладу сервер за допомогою розподіленої атаки (DDoS-атака). Віруси ж, заражаючи веб-сервери, перетворюють їх самих у розсадник інфекції. Крім того, вони істотно сповільнюють його роботу, а також займають Інтернет-канал. На перший погляд здається, що ці загрози за принципом роботи дуже сильно відрізняються один від одного. Але насправді це не зовсім так. Виявляється, багато вірусів, особливо Інтернет-черв'яки, використовують для поширення уразливості в програмному забезпеченні. Так і хакери теж воліють застосовувати атаки, спрямовані на відомі «дірки» в ПЗ. І в цьому немає абсолютно нічого дивного.

Мета роботи: розробка система підвищення рівня безпеки веб-сайтів ТНТУ.

Об’єкт, методи та джерела дослідження. Вразливості веб-сайтів.

Наукова новизна отриманих результатів:

Використання сканера вразливостей Nikto-Online в поєднанні із використанням методики збільшення захищеності веб-сайтів інформаційного порталу ТНТУ.

Практичне значення отриманих результатів.

Розроблено систему, що дозволить убезпечити від несанкціонованого доступу веб-сайти.

Апробація. Окремі результати роботи доповідались на VIII Міжнародній науково-технічній конференції молодих учених та студентів „Актуальні задачі сучасних технологій“, Тернопіль, ТНТУ, 27-28 листопада 2019. — Т. : ТНТУ, 2019. — С. 53-54. — (Том 2).

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 8 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 119 арк. формату А4.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі наведено актуальність забезпечення надійності роботи різних веб сайтів.

В першому розділі проаналізовано вразливості веб-серверів. Таким чином розглянуто компіляцію відомих класів атак, які представляють загрозу для веб-додатків в минулому і представляють зараз. Кожному класу атак присвоєно стандартну назву і описані його ключові особливості. Класи організовані в ієрархічну структуру.

В другому розділі В розділі проведено аналіз статистики вразливостей веб-додатків. Поширені вразливості веб-додатків організовані в структурований список, що складається із дев'яти класів (WSTCv2): аутентифікація (Authentication); авторизація (Authorization); атаки на клієнтів (Client-side Attacks); виконання коду

(Command Execution); розголошення інформації (Information Disclosure); логічні недоліки (Logical Flaws); небезпечні конфігурації (Misconfiguration); недоліки протоколу (Protocol Abuse); інші (Miscellaneous).

Для кожного із класів наведено детальний опис різновидів атак. Описи містять приклади вразливостей, що призводять до можливості реалізації атаки, а так само посилання на додаткові матеріали.

У наведеній статистиці враховуються тільки уразливості веб-додатків. Такі поширені проблеми інформаційної безпеки, як недоліки процесу управління оновленнями ПЗ не розглядалися.

Критичність уразливості, яка оцінювалася згідно CVSSv2 (Common Vulnerability Scoring System version 2), наводилася до класичної "світлофорної" оцінки шляхом ділення на 3.

В третьому розділі проаналізовано основні засоби захисту сайтів та веб-проектів.

В четвертому розділі роботи проаналізовано поширені вразливості веб-сайтів. Вказано на основні слабкі місця веб-додатків.

В спеціальній частині проведено аналіз альтернативних сканерів вразливостей веб-сайтів.

В розділі "Обґрунтування економічної ефективності" проведено економічні розрахунки, спрямовані на визначення економічної ефективності від дослідження систем захисту веб-сайтів, а також прийнято рішення щодо подальшого розвитку розробки. Розраховане значення економічної ефективності становить 0,559, що є високим значенням. Так само нормальним є термін окупності. Для даного дослідження він становить 1.78 року.

В розділі "Охорона праці та безпека в надзвичайних ситуаціях" розглянуто такі питання: дії роботодавця за результатами атестації робочих місць за умовами праці, організація робочого місця: природне та штучне освітлення, Забезпечення захисту працівників суб'єктів господарювання та населення від впливу іонізуючих випромінювань та Оцінка стійкості роботи промислового підприємства до впливу вторинних вражаючих факторів.

В розділі "Екологія" наведено етапи та техніка збору та опрацювання екологічної інформації та індексний метод в екології.

У загальних висновках щодо дипломної роботи описано прийняті в роботі технічні рішення.

В графічній частині приведено вразливості веб-серверів, атаки при аутентифікації та авторизації, атаки на клієнтів та сервер СУБД, атаки внаслідок виконання коду, розголошення інформації та логічні атаки, статистика критичних вразливостей, статистика вразливостей (детальний аналіз), процес сканування веб-сайтів.

ВИСНОВКИ

Згідно поставленої мети вирішено наступні задачі:

1. Проаналізовано вразливості веб-серверів.
2. Проведено аналіз статистики вразливостей веб-додатків.
3. Проаналізовано поширені вразливості веб-сайтів. Вказано на основні слабкі місця веб-додатків;
4. Проведено аналіз сканерів вразливостей веб-застосувань.
5. Розроблено рекомендації щодо підвищення захищеності веб-сайтів.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Шутко Б.Ю. Методи оптимізації програми / Б.Ю. Шутко // Матеріали VIII Міжнародної науково-технічної конференції молодих учених та студентів „Актуальні задачі сучасних технологій“, 27-28 листопада 2019. — Т. : ТНТУ, 2019. — С. 53-54. — (Том 2).

АНОТАЦІЯ

Дипломна робота присвячена питанням дослідження систем захисту веб-сайтів.

В першому розділі проведено аналіз вразливостей веб-серверів, зокрема звернуто увагу на аутентифікацію, авторизацію, атаки на клієнтів, атаки типу виконання коду, розголошення інформації, логічні атаки. В другому розділі наведено статистику вразливостей веб-додатків. В третьому розділі описаний захист веб-сайтів та веб-проектів. В четвертому розділі наведено аналіз поширених вразливостей веб-сайтів та створено методику їх усунення. В п’ятому розділі описано практичне використання проведених досліджень, а саме описано процедуру модифікації під власні потреби сканера вразливостей Nikto-online.

Ключові слова: АУТЕНТИФІКАЦІЯ, ВРАЗЛИВОСТІ, ВЕБ-САЙТ, ВЕБ-ДОДАТОК, АВТОРИЗАЦІЯ, МЕТОДИКА, ЗАХИСТ, ПОШИРЕНИЙ, СКАНЕР ВРАЗЛИВОСТЕЙ.

ANNOTATION

The first section analyzes vulnerabilities Web servers, in particular referred to the authentication, authorization, attacks on customers, such as attack code execution, information disclosure, logical attack. The second section provides statistics vulnerabilities Web applications. In the third section describes the protection of sites and web projects. In the fourth section, the analysis of common vulnerabilities sites and established methods to address them. In the fifth chapter describes the practical use of the research and describes how to modify it to your needs vulnerabilities scanner Nikto-online.

Key words: AUTHENTICATION VULNERABILITY WEBSITE, WEB APPLICATION, AUTHORIZATION, METHODS, PROTECTION, HARBOR, SCANNER VULNERABILITY.