Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Кафедра управління інформаційною безпекою

«Допущено до захисту»
Завідувач кафедри управління
інформаційною безпекою
_____Ростислав ТКАЧУК
“____” _____2022 року

БАКАЛАВРСЬКА

КВАЛІФІКАЦІЙНАНА РОБОТА

на тему Проектування та реалізація захисту адмінпанелей сайту від брутфорс-атак

Виконав:
здобувач IV курсу, групи КБ-41
спеціальності (освітньої-професійної програми)
125 “Кібербезпека”_____
(шифр і назва спеціальності)
Ткаченко Артур Мар'янович _____
(прізвище, ім’я, по батькові)

Керівник_____Ящук Валентина_____
(прізвище та ініціали)

Рецензент_____
(прізвище та ініціали)

Львів – 2022

АНОТАЦІЯ

Ткаченко Артур “ Проектування та реалізація захисту адмінпанелей сайту від брутфорс-атак”. Бакалаврська кваліфікаційна робота за спеціальністю 125 "Кібербезпека” складається з текстової частини (пояснювальної записки), що містить 3 розділи, 69 с., 41 рис., 0 табл., 35 джерел. А також - графічної (презентації), що містить 14 слайдів.

Об'єкт дослідження – інформаційна безпека web-сайтів, брутфорс-атаки.

Предмет дослідження – пошук першопричини виникнення брутфорс-атак, реалізація та побудова ефективного захисту від брутфорс-атак.

Мета роботи – написати рекомендації для захисту web-сайтів від кібератак, створити та протестувати в реальних умовах захист адмінпанелей сайту від брутфорс-атак.

У бакалаврській кваліфікаційній роботі описано основні теоретичні та практичні рекомендації для ефективного захисту веб-ресурсів від кібератак.

Описано рекомендації щодо безпечного проектування адмінпанелей веб-сайтів.

Зроблено аналіз загроз інформаційної безпеки web-сайтів, а також аналіз переваг та недоліків відомих методів захисту від брутфорс-атак.

Розроблено надійний та ефективний захист веб-ресурсів від брутфорс-атак.

ABSTRACT

Tkachenko Artur "Design and implementation of protection of site administration panels from brute force attacks." Bachelor's thesis on the specialty 125 "Cybersecurity" consists of a text part (explanatory note), containing 3 chapters, 67 pages, 41 pictures, 0 tables, 35 sources, as well as a graphic (presentation) containing O slides.

The object of study - information security of web-sites, brute force attacks.

The subject of research is the search for the root cause of brute force attacks, implementation and construction of effective protection against brute force attacks.

The purpose of the work is to write recommendations for protection of web-sites from cyberattacks, to create and test in real conditions own protection of administrative panels of a site against brute force attacks.

The bachelor's thesis describes the basic theoretical and practical recommendations for effective protection of web resources from cyber attacks.

Recommendations for safe design of web admin panels are described.

An analysis of threats to information security of web-sites, as well as an analysis of the advantages and disadvantages of known methods of protection against brute force attacks.

Reliable and effective protection of web resources from brute force attacks has been developed.

ЗМІСТ

ВИСНОВКИ

У кваліфікаційній роботі вирішено важливе науково-практичне питання щодо проектування та реалізації захисту адмінпанелей сайту від брутфорс-атак, зокрема:

- Описано основні теоретичні та практичні рекомендації для ефективного захисту веб-ресурсів від кібератак, досліджено сучасні підходи до класифікації веб-ресурсів, визначено особливості визначення загроз інформаційної безпеки веб-ресурсів, досліджено способи виконання брутфорс-атак та концепцію управління процесом захисту веб-ресурсів.
- Описано рекомендації щодо безпечного проектування адмінпанелей веб-сайтів. Зроблено аналіз загроз інформаційної безпеки web-сайтів, а також аналіз переваг та недоліків відомих методів захисту від брутфорс-атак.
- Ефективне рішення по запобіганню бутфорс-атак на адмінпанелі сайтів було отримано за допомогою: криптографії, власних досліджень, HTML та JavaScript. Це рішення полягає в наступному: якщо зловмисник не зможе отримати доступ до веб форми входу в адмінпанель сайту, то він не зможе визначити куди і яким чином треба звертись до сайту для авторизації, а значить не зможе здійснити брутфорс-атаку та отримати доступ до адмінпанелі сайту.
- Це можливо завдяки парольній перевірці за допомогою згенерованої html веб-форми та обробником подій на JS. Справжня веб-форма шифрується алгоритмом AES128 і паролем є не той пароль який ви вводиться в поле вводу, а його sha256 хеш. Тобто у форму, яка генерується вставляється зашифрована справжня html вебформа адмінпанелі і щоб її розшифрувати зловмиснику треба спочатку зламати 64-ьох символьний пароль, при цьому не використовуючи жодних HTTP/HTTPS запитів, оскільки JS на них ніяк не реагує.
- Зловмисник в такому випадку може проаналізувати JS код, спробувати провести брутфорс-атаку за допомогою JS. Щоб цього не сталося було прийнято рішення реалізувати функцію подвійного дна. Скоріше за все, зловмисник відмовиться від брутфорс атак та й в цілому інших атак, оскільки для цього потрібно потратити багато зусиль, а будь-яких результатів ця атака у більшості

випадків просто не принесе. Результат у вигляді лістингу всієї програми наведено у додатку А.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 13 кроків, щоб захистити панель адміністратора WordPress [Електронний ресурс] – Режим доступу до ресурсу: https://gretathemes.com/protect-wordpress-admin-area/

2. 14 життєво важливих порад щодо захисту вашої адміністративної області WordPress [Електронний ресурс] – Режим доступу до ресурсу: https://www.wpbeginner.com/wp-tutorials/11-vital-tips-and-hacks-to-protect-your-wordpress-admin-area/

3. 15 методів запобігання атак грубою силою, які ви повинні знати. [Електронний ресурс] – Режим доступу до ресурсу: https://www.thesslstore.com/blog/15-brute-force-attack-prevention-techniques-you-should-know/

4. Балацька В.С., Ящук В.І., Полотай О.І. Вразливість комп'ютерної мережі як проблема закладів вищої освіти. Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи: збірник тез доповідей VI Міжнародній науково-практичній конференції (м. Київ - м. Львів, 4-5 листопада 2021 р.). Львів: ЛДУ БЖД, 2021. С. 66–68.

5. Блокування брутфорс-атак. [Електронний ресурс] – Режим доступу до ресурсу: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

6. Брутфорс атаки. [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Brute-force_attack

7. Драб Ю. Основні підходи до побудови системи управління інформаційною безпекою / Ю. Драб, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.29-32).

8. Захист від парольних атак [Електронний ресурс] – Режим доступу до ресурсу: https://www.ibm.com/docs/en/rational-clearquest/9.1?topic=model-protecting-from-password-attacks

9. Захист панелі адміністратора. [Електронний ресурс] – Режим доступу до ресурсу: https://processwire.com/docs/security/admin/

10. Кленик О., Ткачук Р. Особливості побудови захищеної мережі підприємства. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 52–54.

11. Колядич І., Ткачук Р. Системи автоматичного керування програмним забезпеченням. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2021 р.). Львів : ЛДУБЖД, 2021. С. 55–57.

12. Купріков М. Методи тестування системи на проникнення для забезпечення кібернетичної безпеки / Н. Купріков, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.80-83).

13. Мельцов В. В., Ткачук Р. Л. Організація захисту сайту створеного за технологіями: MONGODB, ANGULAR 12, HTML5, CSS3, JAVASCRIPT, NESTJS. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції “Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України” (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М.П. Драгоманова, 2022. С. 84–85.

14. Н.Думич, О.Полотай Особливості захисту Proxy-сервера, як один із способів забезпечення безпеки розподілених інформаційних систем. Захист інформації в інформаційно-комунікаційних системах: збірник тез доповідей II Міжвузівської науково-практичної конференції студентів і курсантів. – Львів: ЛДУ БЖД, 2017. – С. 18-19.

15. Найкращі методи зміни сторінки входу в адмінпанель Wodpress. [Електронний ресурс] – Режим доступу до ресурсу: https://xtemos.com/change-wordpress-login-page-best-methods/

16. Найпопулярніші види кібератак у 2021. [Електронний ресурс] – Режим доступу до ресурсу: https://10guards.com/ua/articles/the-most-common-types-of-cyber-attacks-in-2021/

17. Пароль повинен містити літери різних регістрів - як його придумати і

створити. [Електронний ресурс] – Режим доступу до ресурсу: https://multipassword.com/uk/articles/password-must-contain-letters-of-different-cases

18. Парольний захист панелі адміністратора веб-сайту. URL: https://ostraining.com/blog/coding/how-to-password-protect-your-website/

19. Приховування WP-Admin: популярно, складно і не дуже ефективно. [Електронний ресурс] – Режим доступу до ресурсу: https://raidboxes.io/en/blog/security/wp-admin-verstecken-sinnvoll-oder-nicht/

20. Смик Д. Управління інформаційною безпекою IT – проектів з використанням методики DevSecOps / Д.Смик, В. Ящук // Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с. (С.83-86).

21. Шахуб С. М., Ткачук Р. Л. Дослідження методів і засобів при запроваджені концепції BYOD на підприємстві. Збірник тез доповідей VIII Всеукраїнської заочної науково – практичної конференції “Проблеми цивільного захисту населення та безпеки життєдіяльності: сучасні реалії України” (м. Київ, 28 квітня 2022 р.). Київ, НПУ імені М.П. Драгоманова, 2022. С. 149–150.

22. Що таке брутфорс-атаки і як захистити свою організацію від них. [Електронний ресурс] – Режим доступу до ресурсу: https://expertinsights.com/insights/what-are-brute-force-attacks-and-how-can-you-protect-your-organization-against-them/

23. Як запобігти брутфорс-атакам за допомогою 8 простих стратегій. [Електронний ресурс] – Режим доступу до ресурсу: https://phoenixnap.com/kb/prevent-brute-force-attacks

24. Як захистити панель адміністратора від хакерів. [Електронний ресурс] – Режим доступу до ресурсу: https://www.orainfotech.com/protect-admin-panel-from-hackers/

25. Як захистити сайт від злому та зберегти безпеку особистих даних в Інтернеті. URL: https://group-fs.com/en/how-to-protect-site-from-hacking-and-keep-the-security-of-personal-data-on-the-internet/

26. Як захистити свій сайт від атак методом грубої сили (Brute-force).

[Електронний ресурс] – Режим доступу до ресурсу: https://sebweo.com/yak-zahistiti-svij-sajt-vid-atak-metodom-gruboyi-sili-brute-force/

27. Як змінити URL-адресу адміністратора WordPress, щоб запобігти бутфорс-аткам. [Електронний ресурс] – Режим доступу до ресурсу:\: https://geekflare.com/change-wordpress-admin-url/

28. Як змінити адресу авторизації (wp-login) у WordPress. [Електронний ресурс] – Режим доступу до ресурсу: https://web-programming.com.ua/kak-izmenit-adres-avtorizacii-wp-login-v-wordpress/

29. Як правило, два з п'яти менеджерів паролів легко зламати. Дослідження. [Електронний ресурс] – Режим доступу до ресурсу: https://cybercalm.org/novyny/yak-pravylo-dva-z-p-yaty-menedzheriv-paroliv-legko-zlamaty-doslidzhennya/

30. Як правило, два з п'яти менеджерів паролів легко зламати. Як захистити свій сайт від злому. [Електронний ресурс] – Режим доступу до ресурсу: https://fondy.ua/uk/blog/how-to-protect-website/

31. Britvin A., Alrawashdeh J. H., Tkachuk R. Client-Server System for Parsing Data from Web Pages. Advances in Cyber-Physical Systems Volume 7, Number 1, 2022. P. 8–13.

32. O.Polotai, O. Belej, N. Nestor. Developing a local positioning algorithm based on the identification of objects in a wireless Wi-Fi network of the mall. IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.

33. O.Polotai, O. Belej., N. Nestor, S. Panchak Developing a Model of Cloud Computing Protection System for the Internet of Things. 2020 IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58.

34. O.Polotai, O.Belej, K.Kolesnyk Application of neural networks in intrusion monitoring system for wireless sensor networks. Conference on computer science and information technologies. CSIT 2020: advances in intelligent systems and computing, vol 1293, Springer, Cham. – pp.1101-1115.

35. Zachko O., Kovalchuk O., Kobylkin D., Yashchuk V.. Information

technologies of HR management in safety-oriented systems. Materials of 2021 IEEE 16th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT 2021). V. 2. Lviv, 2021. (Scopus Q2)