слайд 1

Шановний голово та члени екзаменаційної комісії!

До вашої уваги представляю результати кваліфікаційної роботи магістра на тему:

«АВТОМАТИЗАЦІЯ ПРОЦЕСІВ ПЕНТЕСТУ ВЕБ-ЗАСТОСУНКІВ З ВИКОРИСТАННЯМ СУЧАСНИХ ФРЕЙМВОРКІВ».

Студент: Щербаненко Г.О.

Науковий керівник: канд. техн. наук, доцент Рабчун Д.І.

слайд 2

АКТУАЛЬНІСТЬ ДОСЛІДЖЕННЯ

Сучасні веб-застосунки (особливо fintech) часто мають HMAC-підписування та інші механізми контролю цілісності.

Через це стандартна автоматизація (сканери/фазинг) не проходить перевірки підпису та не досягає вразливої логіки.

слайд 3

МЕТА ДОСЛІДЖЕННЯ.

Розробка підходів до автоматизації пентесту веб-застосунків із нестандартною/ускладненою логікою обробки запитів.

ЗАВДАННЯ ДОСЛІДЖЕННЯ

• Дослідити обмеження стандартних підходів автоматизації;

• Обґрунтувати вибір Burp Suite та Burp Suite Extensions як базового фреймворку;

• Розробити тестовий вразливий веб-застосунок «Raf Demo Bank» (NoSQL Injection + підписування);

• Створити та експериментально перевірити розширення Burp Suite для автоматизованого перепідписування HTTP-запитів.

слайд 4

ОБ’ЄКТ ДОСЛІДЖЕННЯ

Процес тестування на проникнення веб-застосунків як складова забезпечення їх інформаційної безпеки.

ПРЕДМЕТ ДОСЛІДЖЕННЯ

Методи та програмні засоби автоматизації пентесту для систем з ускладненою логікою роботи.

слайд 5

ПЕРШИЙ РОЗДІЛ

Коротко розглянуто типові етапи пентесту та формати тестування (black/gray/white box) у контексті вимог ІБ.

слайд 6

ДРУГИЙ РОЗДІЛ

Проаналізовано інструменти автоматизації та показано, що без адаптації під бізнес-логіку вони обмежені.

Обґрунтовано підхід: Burp Suite + кастомні Burp Extensions як «проміжний шар» для відтворення легітимного клієнта.

слайд 7

ТРЕТІЙ РОЗДІЛ

Створено лабораторний стенд «Raf Demo Bank» з HMAC-підписаним API та вразливістю NoSQL Injection.

Розроблено розширення Burp Suite для автоматизованого перепідписування запитів та роботи з Repeater/Intruder.

слайд 8

АРХІТЕКТУРА РОЗРОБЛЕНОГО ДОДАТКУ

Node.js/Express + MongoDB; модулі auth/profile/admin та API переказу коштів із перевіркою HMAC-підпису.

Валідація параметра IBAN отримувача містить навмисну помилку, що імітує NoSQL Injection у реальній бізнес-логіці.

слайд 9

ІНТЕРФЕЙС РОЗШИРЕННЯ ДЛЯ BURP SUITE

Налаштовується HMAC secret, фільтр URL та порядок параметрів для канонізації.

Після цього Burp може змінювати параметри запиту (Intruder/Repeater), а розширення коректно перепідписує запити.

слайд 10

ПРАКТИЧНИЙ РЕЗУЛЬТАТ

Продемонстровано, що без перепідписування фазинг не працює: змінені запити відсікаються перевіркою підпису.

З використанням розширення виконано фазинг параметрів API та підтверджено NoSQL Injection із отриманням доступу до admin-панелі.

слайд 11

ВИСНОВКИ

• Досліджено обмеження стандартної автоматизації для веб-застосунків з ускладненою логікою;

• Обґрунтовано Burp Suite + Burp Extensions як практичну основу адаптивної автоматизації;

• Реалізовано «Raf Demo Bank» та показано експлуатацію NoSQL Injection в умовах HMAC-підписування;

• Створено та перевірено розширення для автоматизованого перепідписування HTTP-запитів; сформовано рекомендації застосування.

Апробація: конференція «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу», 27.02.2025.

слайд 12

Доповідь закінчено. Дякую за увагу!