Секція 1

КОМПЛЕКСНІ ЗАСОБИ ЗАХИСТУ ВЕБРЕСУРСІВ ВІД ПОШИРЕНИХ АТАК

Гребньов Д.О.
Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ»
Науковий керівник: Тецький А.Г.

Актуальність. У сучасному світі веб ресурси займають якщо не найважливіше місце у різних сферах нашого повсякденного життя, то хоча б одне з найпопулярніших місць, вони охоплюють такі сфери життя як бізнес, освіта, соціальні мережі, розваги та й багато інших аспектів повсякденного життя. Вебресурси в наш час набувають неабиякої популярності та розповсюдження в побутовому житті користувачів, що своєю чергою призводить до збільшення інформації, котра зберігається або передається вебресурсами в інтернеті. Дане зростання кількості інформації, котра зберігається або передається вебресурсами, спонукає зловмисників до все більш витончених та складних атак для отримання даної інформації або до примусу звичайного користувача виконати зловмисні дії.

Метою роботи є аналіз сучасних поширених атак на вебресурси та вибір комплексних засобів захисту веб ресурсів від розглянутих атак.

Основні положення. Сучасні зловмисники використовують дедалі складніші методи реалізації своїх атак, комбінуючи їх для досягнення своєї мети, що й ускладнює захист вебресурсів. Виділяють такі найпопулярніші види атак на вебресурси, як атаки на основі паролей, атаки на порушення автентифікації, обхід каталогів, людина посередині, атаки на відмову в обслуговуванні, міжсайтовий скріптинг та міжсайтова підробка запитів [1]. Хоч дані атаки і є поширеними, але захиститися одним методом не вдасться, для цього і потрібно впроваджувати комплексну систему захисту, навіть від одного типу атаки. Наприклад для захисту від атак на відмову в обслуговуванні можна використовувати брандмауери, адаптивний моніторинг, кешування та обмеження швидкості [2]. Якщо розглядати атаки людина посередині, то захистом може слугувати оновлення програмного забезпечення, використання VPN (Virtual Private Network), постійний моніторинг мережі, використовувати двофакторну автентифікацію, перевіряти справжність сертифікати веб ресурсів та шифрувати дані [3]. Переходячи до атаки міжсайтової підробки запитів, то захистом може бути

використання CSRF-токенів, SameSite у файлах cookie, використовувати принцип найменших привілеїв [4].

Висновки. Враховуючи стрімке зростання попиту вебресурсів у повсякденному житті, захист інформації є першочерговим завданням. Водночас неможливо захистити веб ресурс, використовуючи лише один метод захисту, наразі потрібно використовувати комплексні засоби захисту веб ресурсів, щоб знизити рівень загрози самому веб ресурсу та забезпечити безперебійність його роботи для звичайного користувача.

Список літератури

1. The 10 Most Common Website Security Attacks (and How to Protect Yourself). *Tripwire | Security and Integrity Management Solutions*. URL: https://www.tripwire.com/state-of-security/most-common-website-security-attacks-and-how-to-protect-yourself (дата звернення: 01.11.2024).
2. How to prevent ddos attacks. *Cloudflare*. URL – https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks (дата звернення: 01.11.2024).
3. Malik F. 10 Ways to Prevent Man-in-the-Middle (MITM) Attacks | StrongDM. *StrongDM: Your Partner in Zero Trust Privileged Access*. URL: https://www.strongdm.com/blog/man-in-the-middle-attack-prevention (дата звернення: 06.11.2024).
4. Cross-Site Request Forgery (CSRF) Protection-Synchronizer Token Pattern. *Medium*. URL – https://medium.com/@bhathz222/cross-site-request-forgery-csrf-protection-synchronizer-token-pattern-610032ff8f20 (дата звернення: 07.11.2024).

Відомості про авторів

Гребньов Данило Олександрович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.o.grebnjov@student.csn.khai.edu

Тецький Артем Григорович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., a.tetskiy@csn.khai.edu