БЕЗПЕКА HTTP ЗАГОЛОВКІВ

Синицін Я.С., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

З розвитком веб-технологій питання безпеки веб-додатків стає все більш актуальним [1]. HTTP-заголовки відіграють ключову роль у захисті комунікацій між сервером і клієнтом. Неправильна конфігурація цих заголовків може призвести до серйозних загроз, таких як XSS, Clickjacking, MIME-Sniffing та Man-in-the-Middle атаки [2]. Для забезпечення високого рівня безпеки веб-додатків в процесі розробки додатків та їх експлуатації необхідно здійснювати постійний аналіз та контроль щодо відсутності основних вразливостей, до яких можна віднести: відсутність або неправильне використання HTTP-заголовків безпеки, що може призвести до атак XSS, Clickjacking та MIME-Sniffing; надлишкова інформація у заголовках (наприклад, X-Powered-By), що сприяє роботі зловмисників; неправильна конфігурація політик безпеки, зокрема Content Security Policy (CSP).

Метою доповіді є аналіз основних загроз, пов'язаних із некоректним налаштуванням HTTP-заголовків, оцінка існуючих механізмів безпеки та розгляд ефективних методів захисту.

Серед основних механізмів безпеки можна відзначити елементи заголовків:

- Strict-Transport-Security (HSTS) - примусове використання HTTPS;
- Content-Security-Policy (CSP) - обмеження джерел виконуваного коду;
- X-Frame-Options - захист від Clickjacking;
- X-Content-Type-Options - запобігання MIME-Sniffing;
- Referrer-Policy - контроль передачі реферер-заголовків;
- Permissions-Policy - управління доступом до браузерних API.

Аналіз зазначених механізмів дозволив розробити практичні рекомендації.

1. Використання HTTPS та примусове шифрування через HSTS є обов'язковим та має використовуватись постійно.
2. Впровадження CSP для обмеження виконуваного JavaScript-коду.
3. Автоматичне визначення MIME-типів має бути вимкнено.
4. Сайт не має завантажуватися у фреймі, функціонал має бути недоступний.
5. Політики доступу до API має бути проаналізована та верифікована. Необхідно підтримувати мінімальний рівень, що реалізує потрібний функціонал.
6. Має регулярно проводитись аудит безпеки заголовків.

Дотримання наведених рекомендацій дозволяє суттєво зменшити ризики атак та підвищити рівень безпеки веб-додатків.

Список літератури

1. Д'якова Н.Є., Сєвєрінов О.В. Тестування вразливостей сучасних вебресурсів, НТУ «ХПІ»,. – 2022.
2. OWASP Foundation. "HTTP Security Headers." OWASP Cheat Sheet Series, 2023.