PROVOCĂRI DE SECURITATE CIBERNETICĂ ÎN PROTOCOLUL HTTP

Ana TURCAN

Departamentul Informatică și Ingineria Sistemelor, Facultatea Calculatoare, Informatică și Microelectronică, Universitatea Tehnică a Moldovei, Chișinău, Moldova

Autorul corespondent: Ana TURCAN, e-mail: ana.turcan@fcim.utm.md

Coordonator: **Dumitru CIORBĂ**, dr., Universitatea Tehnică a Moldovei

Rezumat. *Hypertext Transfer Protocol este un protocol fundamental pentru comunicarea în Web, definind semantica și sintaxa interacțiunilor. Avantajele protocolului pe lângă accesul rapid și flexibil la conținuturi cuprind simplitatea, interoperabilitatea și versatilitatea. Evoluția protocolului a fost determinată de necesitatea de a îmbunătăți performanța: transfer date mai rapid, mai sigur și mai eficient. În prezent aplicarea versiunilor de protocol fluctuează în funcție de procesele tehnologice și de adoptarea acestora la cerințele actuale. Deși noile specificații determină noi parametri de performanță și securitate, rămân a fi susceptibile la anumite vulnerabilități, care pot compromite atât integritatea, cât și confidențialitatea datelor. Ultimele vulnerabilități atestate în protocolul HTTP/2 confirmă necesitatea conștientizării faptului că orice protocol, indiferent de statutul său, proiect propus sau standard recunoscut, fiind expus noilor amenințări pot induce vulnerabilități neidentificate. Pentru a diminua din vulnerabilitățile protocolului și implementările acestuia este crucial de a fi adoptate măsuri de securitate adecvate, nu doar utilizarea TLS, dar și utilizarea unor practici de dezvoltare sigure și implementarea unor politici de securitate bine definite. Acestea se pot augmenta prin implementarea antetelor de securitate potrivite, beneficiind în continuare de avantajele oferite de protocolul HTTP, asigurând în același timp o experiență online sigură și protejată pentru toți utilizatorii.*

Cuvinte cheie: *protocol HTTP, antete de securitate, politica de securitate, vulnerabilități de tip man-in-the-middle, handshake, injection, Rapid Reset, zero-day.*

Domeniul de cercetare

Odată cu dezvoltarea mediului Web a evaluat și protocolul HTTP fiind ajustat la cerințele noilor tehnologii pentru a oferi livrări rapide, fiabile și securizate de conținut. Evoluția versiunilor HTTP/1.1, HTTP/2 cât și HTTP/3 denotă focusarea pe extinderea performanței: transfer date mai rapid, mai sigur și mai eficient [1-3].

În prezent utilizarea versiunilor protocolului fluctuează în funcție de adoptarea proceselor tehnologice la cerințele actuale, de implementarea și suportul browserelor și serverelor Web. În Figura 1 este prezentată distribuția utilizării versiunilor protocolului HTTP, la nivel global și separat pentru Republica Moldova [4].

Versiunea dominantă rămâne a fi HTTP/2, deși există încă o cantitate semnificativă de trafic web care rulează pe HTTP/1.1 fie datorită ritmului lent de actualizare a serverelor și site-urilor web fie compatibilității limitate a browserelor mai vechi. Actualizarea și optimizarea continue a infrastructurii web vor accelera probabil migrarea către HTTP/2. HTTP/3 deși se află în faza de dezvoltare prezintă o tendință ascendentă clară datorită avantajelor sale precum reducerea semnificativă a latenței și îmbunătățirea eficienței rețelei, ce îl fac o alegere atractivă pentru viitorul web [5,6].

Motivarea cercetării

Deși specificațiile implementate în protocolul HTTP au determinat noi parametri de performanță și un grad de securitate ridicat niciuna dintre ele nu rămâne imună la vulnerabilități, fapt ce poate compromite atât integritatea, cât și confidențialitatea datelor. Protocolul HTTP rămâne de a fi susceptibil inclusiv la vulnerabilitățile zero-day sau DDoS [7-10].

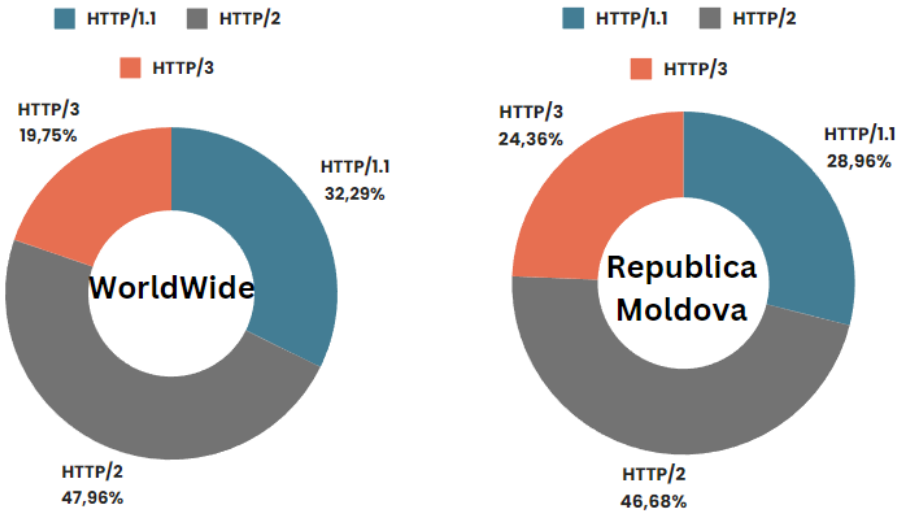

Figura 1. Utilizarea versiunilor protocolului HTTP [4]

Obiectivele și metodologia cercetării

Pentru a diminua din vulnerabilitățile protocolului HTTP, inclusiv și implementările acestuia este crucial de a fi adoptate măsuri de securitate adecvate, nu doar utilizarea protocolului TLS, dar și utilizarea unor practici de dezvoltare sigure, precum și implementarea unor politici de securitate bine definite. Acestea se pot augmenta prin implementarea antetelor de securitate potrivite [2,11].

Rezultatele analizei exploratorii a literaturii de specialitate, a rapoartelor de incidente, portalurilor de tehnologii și cercetare denotă creșterea interesului pentru securitatea în protocolul HTTP.

Pentru a proteja sistemele bazate pe protocolul HTTP de vulnerabilitățile curente, este esențial de a se propune politici de securitate prin intermediul antetelor specializate, deoarece modificări în construcția sau structura HTTP sunt eventuale decât în versiunile ulterioare. Deși importanța antetelor de securitate este evidentă adopția lor nu este la nivelul necesar. Utilizarea exclusivă a setărilor implicite sau neglijarea totală a antetelor de securitate expune site-urile web la un spectru larg de atacuri cibernetice [12,13].

Concluzii

Protocolul HTTP va continua a fi piatra de temelie în comunicarea Web. În pofida faptului că a progresat semnificativ, totuși rămâne susceptibil la diverse vulnerabilități care pot compromite atât integritatea, cât și confidențialitatea datelor. Analiza standardelor HTTP este relevantă pentru menținerea unui nivel adecvat de securitate și protecție a datelor chiar și după publicare, acceptare și standardizarea acestora. Antetele de securitate HTTP joacă un rol important în atenuarea amenințărilor și vulnerabilităților. Implementate corect cu o configurare corespunzătoare, ținându-se cont de vulnerabilitățile deja depistate și remediate, în combinație cu alte mecanisme de securitate, acestea vor contribui semnificativ la protecția datelor și a infrastructurii web. Beneficiind astfel în continuare de avantajele oferite de protocolul HTTP, de o comunicare sigură și protejată în mediul Web.

Referințe

[1] Bishop, Mike. *HTTP/3*. Request for Comments, RFC 9114, Internet Engineering Task Force, June 2022, https://datatracker.ietf.org/doc/rfc9114/.

[2] "HTTP/1 vs HTTP/2 vs HTTP/3." *DEV Community*, 5 May 2023, https://dev.to/accreditly/http1-vs-http2-vs-http3-2k1c.

[3] *NVD - CVE-2023-44487*. https://nvd.nist.gov/vuln/detail/CVE-2023-44487. Accessed 13 Mar. 2024.

[4] "Cloudflare Radar" [Online]. Available: https://radar.cloudflare.com/year-in-review/2023/#http-versions, 2024

[5] Ortiz, Bob. "What Security Risks Are Involved in Using Older HTTP Protocols Such as HTTP/1.x That Would Justify Upgrading to HTTP/2 or HTTP/3?" *Information Security Stack Exchange*, 30 Oct. 2023, https://security.stackexchange.com/q/272878.

[6] Sjoerd. "Answer to 'What Security Risks Are Involved in Using Older HTTP Protocols Such as HTTP/1.x That Would Justify Upgrading to HTTP/2 or HTTP/3?'" *Information Security Stack Exchange*, 1 Nov. 2023, https://security.stackexchange.com/a/272917.

[7] "Built-in Weakness in HTTP/2 Protocol Exploited for Massive DDoS Attacks." *CSO Online*, https://www.csoonline.com/article/655106/built-in-weakness-in-http-2-protocol-exploited-for-massive-ddos-attacks.html. Accessed 13 Mar. 2024.

[8] *CRITICAL: Vulnerable HTTP Report | The Shadowserver Foundation*. https://www.shadowserver.org/what-we-do/network-reporting/vulnerable-http-report/. Accessed 25 Mar. 2024

[9] Newman, Lily Hay. "A New Protocol Vulnerability Will Haunt the Web for Years." *Wired*, https://www.wired.com/story/http-2-rapid-reset-flaw/. Accessed 13 Mar. 2024.

[10] "HTTP/2 Rapid Reset: Deconstructing the Record-Breaking Attack." *The Cloudflare Blog*, 10 Oct. 2023, https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack.

[11] *HTTP Headers - OWASP Cheat Sheet Series*. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html. Accessed 19 Mar. 2024.

[12] Buchanan, William J., et al. "Analysis of the Adoption of Security Headers in HTTP." *IET Information Security*, vol. 12, no. 2, 2018, pp. 118–26, https://doi.org/10.1049/iet-ifs.2016.0621

[13] *OWASP Secure Headers Project | OWASP Foundation*. https://owasp.org/www-project-secure-headers/. Accessed 19 Mar. 2024.