Sicurezza nei Browser Moderni: Analisi, Minacce e Soluzioni

Relatore

Prof. Fabio Vitali

Tesi di laurea

Alessandro Frau

Anno accademico
2022-2023

Background

La sicurezza web coinvolge profondamente la vita quotidiana di persone, aziende e istituzioni. Attraverso il browser gli utenti interagiscono con banche, social network, servizi di stato, prenotano voli e treni, danno accesso completo ai propri dati personali.

È facile osservare che la sicurezza per questo tipo di strumenti sia un argomento prioritario, dato che qualsiasi violazione potrebbe portare a delle conseguenze terrificanti, dalle violazioni dei dati personali e truffe, a grossi casi di frodi e furti d’identità.

Risulta quindi fondamentale sensibilizzare gli utenti ad un utilizzo corretto di questo strumento, per limitare i danni che questi possono subire, dato che, come vedremo, anche i browser risultano spesso vulnerabili a dei vettori d’attacco.

Struttura

La trattazione segue un percorso pratico che evidenzia, su base teorica, le problematiche affrontate dai browser.

- In primo luogo vengono analizzate le tecnologie, per creare una base teorica di riferimento, e migliorare la comprensione dell’argomento.
- Tramite la ricerca approfondita su fonti ufficiali come l’issue tracker di Chrome, vengono descritte delle vulnerabilità, con esempi di attacchi reali, per comprendere al meglio il potenziale danno che esse possono causare.
- Infine vengono trattate le strategie adottate dai browser per mitigare o risolvere tali minacce.

Chrome, Firefox, Safari e Edge sono i 4 browser di riferimento di questa tesi, e coprono più del 90% dell’utilizzo di browser alla data corrente.

HTTPS

Tramite il protocollo HTTPS, i browser riescono a garantire una connessione sicura e crittografata tra utente e server web, proteggendo così la privacy e l'integrità dei dati scambiati durante la navigazione.

Gli attacchi a questo protocollo possono portare a danni su larga scala, infatti un attaccante potrebbe leggere e modificare qualsiasi comunicazione web, ad esempio cambiare iban di destinazione di un bonifico, leggere i messaggi di importanti esponenti politici, e scoprire tutti i link che questo ha visitato.

Attacco	Descrizione	Anno uscita
BEAST	TLS downgrade a TLSv1.0	2011
DigiNotar	Rilascio di più di 500 certificati falsi	2011
HeartBleed	Rubate migliaia di chiavi private di certificati	2014
POODLE	TLS downgrade a SSLv3.0	2014
FREAK	Downgrade a RSA export-grade	2015
Logjam	Downgrade a Diffie-Hellman export-grade	2015

Cookies e gestione delle sessioni

I cookie sono piccoli blocchi di dati che vengono salvati dal browser per permettere di gestire lo stato e le interazioni degli utenti con i siti web.

Un grande sforzo viene fatto dai browser per mettere in sicurezza questi dati, visto che se un attaccante ne entra in possesso, tramite attacchi Man In The Middle (MITM) o Cross Site Scripting (XSS), oppure ne sfrutta il contenuto tramite Cross Site Request Forgery (CSRF), potrebbe ottenere accesso completo a tutte le piattaforme web utilizzate dagli utenti, come mail, messaggi, mandare bonifici, vedere le foto salvate nel cloud.

Nome	Scopo	Anno uscita
max-age e expires	Impostano la data di scadenza di un cookie	2011
Secure	Trasmissione solo su canali sicuri (HTTPS)	2011
HttpOnly	Mitiga XSS rendendo il cookie inaccessibile tramite Javascript	2011
Cookie Name Prefixes	Mitigano weak integrity dei cookie prevenendo accessi da domini fratelli	2015
SameSite	Previene CSRF determinando se i cookie possono essere inviati a domini esterni	2016

Oltretutto, vengono utilizzati costantemente per la profilazione, e per questo l’utente dovrebbe decidere con cura quali cookie salvare.

SOP e CORS

La maggior parte delle pagine complesse che vengono utilizzate tutti i giorni richiede di interagire con altre risorse dall’origine differente.

Un esempio è quello di Google maps, che permette a tutte le origini di comunicare con la piattaforma per integrare le mappe.

Queste interazioni pongono un grande rischio per la sicurezza degli utenti, infatti, se configurate in maniera errata, possono causare gravi violazioni della privacy degli utenti, e fare in modo che questi commettano azioni involontariamente.

Se vulnerabili, queste politiche permettono all’attaccante di leggere i dati personali dell’utente, come informazioni bancarie e documenti identificativi, rubare credenziali, ad esempio quelle aziendali, e effettuare delle azioni indesiderate come la cancellazione di un account o l’aggiunta di un post dal contenuto nocivo su social media.

Esecuzione Sicura di Codice

Capita spesso di visitare pagine web di cui non si conosce l'autore, ad esempio quando si effettua una ricerca su un motore di ricerca. In questo caso, l'utente si aspetta che all'apertura della pagina web, anche se questa è stata creata da un malinenzionato, non possa comunque accedere al contenuto del dispositivo.

Molto spesso invece, questo non è il caso, infatti gli strati di isolamento del browser vengono elusi, permettendo all'attaccante di controllare il dispositivo, e quindi poter accedere a tutte le immagini e i file salvati, a tutti i sensori come telecamera e microfono, e potendo anche bloccare l'intero dispositivo.

CVE	Descrizione	Anno uscita
CVE-2021-3052	Use-After-Free che sfrutta l'autocompletamento delle carte di credito su Chrome per android	2021
CVE-2022-1529	Vulnerabilita Javascript su Firefox che sfrutta una prototype pollution nel processo con esecuzione privilegiata per eseguire codice arbitrario	2022
CVE-2023-36719	Buffer Overflow tramite la Web Speech API dei Chromium	2023

DOM Encapsulation

Capita spesso che delle pagine vogliano integrare altre pagine all'interno della propria schermata. Un esempio comune sono i video dalle piattaforme streaming, che vengono integrati costantemente in altre pagine web.

Queste integrazioni, se non controllate dal browser in maniera corretta, possono essere sfruttate dagli attaccanti, ad esempio facendo seguire all'utente una pagina ingannandolo tramite un pulsante invisibile, oppure permettendo attacchi Cross-Site Scripting e Cross-Site Request Forgery, che possono causare enormi danni alla privacy dell'utente.

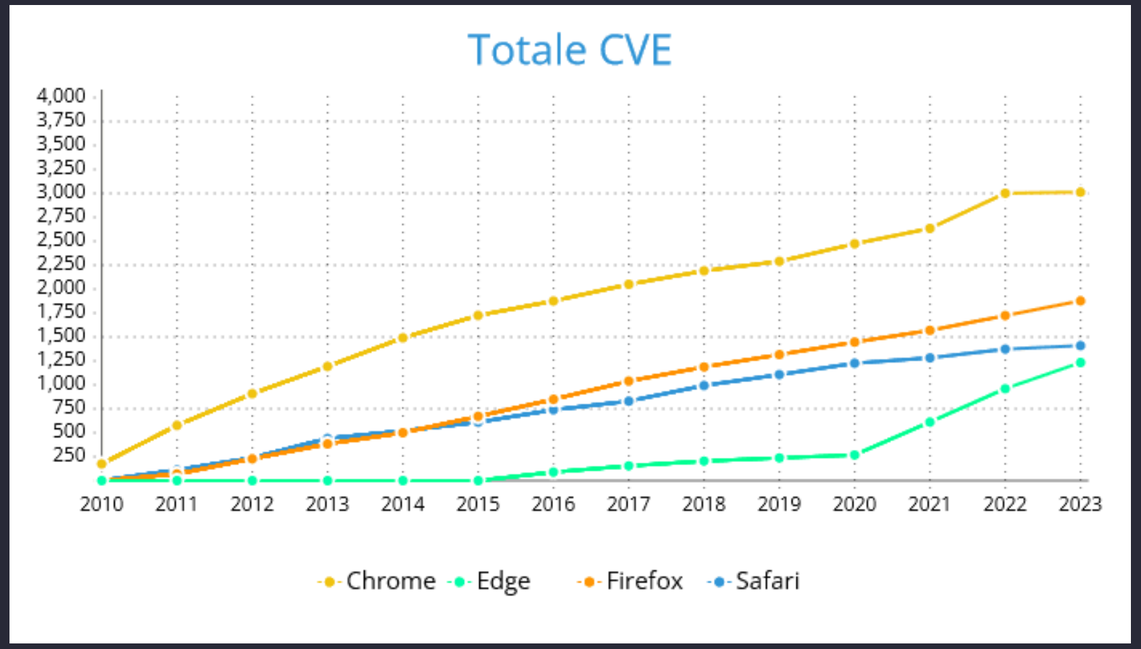
CVE	Descrizione	Anno uscita
CVE-2011-2382	Cookiejacking su Internet Explorer che permette di ottenere i cookie dell'utente tramite IFRAME	2011
CVE-2015-0810	Cursorjacking su Firefox per MacOS che rende il cursore invisibile tramite un oggetto di Flash e un div trasparente, per far eseguire azioni non autorizzate	2015
CVE-2019-5861	Clickjacking in cui Chrome non rileva che due elementi sono sovrapposti se la sovrapposizione avviene tramite la trasformazione di CSS scale.	2019

Dati analizzati

A differenza di quanto si possa pensare, vengono scoperte nuove vulnerabilità ad un ritmo più o meno costante, tant'è che Chrome ha superato le 3000 Common Vulnerability Exposure (CVE)du, e anche Firefox, Edge e Safari sono sull'ordine delle migliaia.

Anche vulnerabilita che hanno impatti importanti sul dispositivo, vengono scoperte piuttosto spesso, Chrome ha superato le 100 Sandbox Escape quest'anno, vulnerabilita che permettono di eseguire codice arbitrario.

Infine in alcuni casi le patch delle vulnerabilita tardano ad arrivare, ad esempio Safari ha rilasciato una patch della vulnerabilita BEAST 3 anni dopo la prima pubblicazione dell'attacco, e inoltre supporta ancora versioni di TLS precedenti alla 1.2, ormai deprecate.



Conclusioni e Sviluppi futuri

Vista l’interazione giornaliera dalle persone con i browser, e la mole di dati sensibili che vengono condivisi tramite questa tecnologia, è molto importante migliorare la comprensione generale delle minacce che questi devono affrontare. Le osservazioni raccolte approfondiscono e raggruppano alcuni attacchi, evidenziando come durante gli anni ci sia stato un costante sforzo di messa in sicurezza da parte degli sviluppatori.

Tuttavia, emerge la necessità di un monitoraggio costante, dato il continuo evolversi degli attacchi, e la risposta a volte tardiva dei fornitori. In futuro, ci si potrebbe concentrare sull’integrazione di tecnologie che ultimamente stanno ricevendo tanto supporto, come quelle di intelligenza artificiale, per riconoscere i pattern di attacco e migliorare i meccanismi di prevenzione lato client.

Potrebbero anche venire proposte delle implementazione di politiche di sicurezza più robuste, per migliorare ad esempio la gestione della revoca dei certificati.