ForceHTTPS: Protecting High-Security Web Sites from Network Attacks

✧ Summary

本篇旨在透過強制 https 的方式，以提供更安全地瀏覽體驗。作者製作了 Firefox 的 extension prototype，利用設置 ForceHTTPS cookie 的方式，改變瀏覽器對一些不安全網站或環境所採取的行為。

如將未受保護的 http 連線導向至 https；若是自簽憑證或一些其他 server 端設置的錯誤，ForceHTTPS 會逕行中斷該 session；而攻擊者亦無法對網站注入不安全的內容。因此可**防止被動攻擊者**利用一些 sniffing tools 竊取 session cookie，從而保護使用者的機敏資料。因 ForceHTTPS 對憑證規範嚴格，故同時也可**防止主動攻擊者**藉由如 DNS poisoning 等方式破壞使用者的隱私安全。此外，在網站開發階段所殘留的一些程式碼或檔案，可能會令攻擊者有其他途徑得以破壞網站安全性，因而對一些不安全、非 https 的 mixed content，ForceHTTPS 也會予以阻擋。不僅如此，ForceHTTPS 也提供 developer mode，令網頁開發者能方便 debug，可以得知哪些原始碼可能是不安全的，讓開發者能予以修正。

✧ Strengths

ForceHTTPS 有一重要使命便是要達到 anti-pharming，保護使用者不會因惡意網頁程式碼或 DNS 伺服器遭受攻擊而導向至攻擊者網站。相較於其他 paper 的做法，ForceHTTPS 僅需要設置 cookie 容易部署，除了可行性較高以外同時也能保持網頁原本的功能性。

一般 http 連線因未加密，若網站將使用者的一些登入帳號密碼資訊儲存於 cookie 中，則當面臨 session hijacking 時，使用者資訊便會暴露於危險之中。因此 ForceHTTPS 能將 session cookie 升級為 secure cookie，防止被動竊聽者與主動攻擊者。而在網站開發方面，因多為由眾多開發者共同進行，因此在整合時可能會有一些漏洞或是有其他考慮不夠周全之處，致使網站遭受 script injection，ForceHTTPS 也能協助阻擋非安全內容。

ForceHTTPS 對使用者而言，能更安全地瀏覽某些可能具潛在漏洞的網站，同時也能確保不安全網路環境的瀏覽體驗。而對網站而言，除了可保護機敏 cookie 不會遭受被動或主動攻擊者的竊聽或盜取外，也能對一些開發者疏忽嵌入於網站的不安全內容予以濾除。

✧ Weaknesses

然而 ForceHTTPS 也有一些無法防禦的攻擊，如 XSS、CSRF 等從**其他角度攻擊網站或瀏覽器**，而其他惡意程式若從使用者系統而來者，也無法防範。另外，諸如**釣魚網站**吸引使用者點擊，令使用者被導向至其他假網站騙取敏感資料，縱使為 https 連線，也不再 ForceHTTPS 的保護範疇中。

尚有其他情況，如使用者若從未連過某 server，則可能會於**初始化連線請求**時遭受攻擊，因該階段仍無法設置 ForceHTTPS cookie，因此可能會遭受如 SSL striping attack 等，因此或許可搭配 HSTS 機制。此外，部分使用者也可能會對 ForceHTTPS 存有隱私疑慮，認為可能會被利用為 super cookie 方式追蹤一部分隱私，甚至某些使用者可能會有**清空 cookie** 的習慣，致使下次初始連線時又會有初始化風險存在。另一方面，攻擊者也可能對 http response header 進行注入而造成 http response attack，進而操控 ForceHTTPS cookie。

在使用者端，若瀏覽器插件未遵守 ForceHTTPS 的 policy，plug-in 便有可能使用 raw socket 而未使用 https，令攻擊者有機會可以繞過安全機制。在網站端，網頁的一些規則也需要被更新，但更新後也有一定可能會令原先網頁功能異常。

✧ Reflection

不容置喙地，ForceHTTPS 在當時可謂相當**簡單**但**實用**的機制，能夠阻擋一定的被動竊聽者與主動攻擊者，且可以抵抗上述作者所述之 attack model。但除了此作法有些限制外，時至今日攻擊手法不斷推陳出新，已不能僅單靠此做法來達到瀏覽安全性。

此外，本篇論文提到在當時有 63%網站的憑證是有問題，瀏覽器會跳出相關警告的，而若 ForceHTTPS 對這些有問題的網站皆逕行阻擋，會令當時使用者無法瀏覽諸多網站，對網站擊使用者都造成損失，那麼方便性與安全性便值得思考該如何權衡了。