

اعتماد (HTTPS) وحده في المواقع الحكومية: ضرورة تأخرت

جاكوب هوفمان أندروز



المخلص:

يعرض المقال تأييد اعتماد (HTTPS) وحده في المواقع الحكومية، بوصفه حدًا أساسيًا لحماية سرية التصفح والبيانات المتبادلة، ويشرح الفرق بين الاتصال المشفر وغير المشفر، ويناقش مخاطر كشف ما يقرأه الناس أو يرفعونه، خاصة عند استخدام الخدمات الحساسة. ويتناول تأخر بعض الجهات في التطبيق وإمكان تحسينه مع انخفاض كلفة الإعداد، ويدعو إلى استجابة حكومية وتعاون عام. كما يوضح هامش المقال حدود البروتوكول، إذ لا يمنع جميع ثغرات المواقع أو التتبع أو استنتاج المعلومات من حركة الشبكة. ويقدم الدعوة وإجراءات التعليق في سياقها التاريخي، دون اعتبارها طلب مشاركة حاليًا. ويؤكد أن حماية الوصول إلى المعلومات تتطلب التشفير مع سياسات وإجراءات وأدوات أخرى مناسبة للمخاطر.

الكلمات المفتاحية: (HTTPS)، المواقع الحكومية، الخصوصية، تشفير الاتصال، أمن الويب

مقدمة:

نشر مكتب الإدارة والميزانية في البيت الأبيض معيارًا جديدًا يوصي بتطبيق (HTTPS) تطبيقًا كاملاً في جميع المواقع والخدمات الحكومية الفدرالية. ويستقبل تعليقات الجمهور عبر (<https://cio.gov>) حتى 14 أبريل؛ فإن كنت تهتم بالخصوصية والأمن، فأدل برأيك.

هذه التدوينة هي تعليقنا العام: نؤيد بكل قوة تبني الحكومة الفدرالية هذا المعيار الأساسي للأمن السيبراني. ونحث الحكومات المحلية والإقليمية والوطنية في جميع أنحاء العالم على الاقتداء به في أقرب وقت ممكن.

(HTTPS)، النسخة الآمنة من (HTTP)، يحمي التصفح بتشفير كل ما يُرسل بين الفرد وخادم الويب والتحقق من أصالته. وهو يحل سريعًا محل (HTTP) غير الآمن، ويخطط خبراء الأمن لإظهار تحذيرات عند زيارة صفحات (HTTP).

من دون (HTTPS)، يستطيع أي شخص يتحكم في الشبكة، أو يستخدم شبكة (Wi-Fi) نفسها فحسب بتقنية تسميم (ARP)، مراقبة نشاط التصفح. وقد يكون من المتطفلين المحتملين صاحب العمل أو المدرسة أو مزود الإنترنت أو أجهزة التجسس الوطنية أو الوالدين أو الزوج أو غيرهم من رواد المكتبة. وليس (HTTPS) علاجًا سحريًا لكل مشكلات الأمن والخصوصية، لكن لا موقع يستطيع أن يكون آمنًا أو يحفظ الخصوصية من دونه.

للأسف، تخلت المواقع الفدرالية كثيرًا عن القطاع الخاص في تطبيقه. فالمواقع التجارية الأشهر، مثل (Google) و(Facebook) و(Twitter)، تعتمد (HTTPS) وحده منذ سنوات، بينما لا تدعمه مواقع فدرالية كثيرة أصلًا، فيستحيل الوصول إليها عبر اتصال آمن. وبعضها يدعمه ولا يجعله افتراضيًا، وبعضها يقدمه ببرمجيات وإعدادات قديمة غير آمنة.

تستقبل المواقع الحكومية أنواعًا كثيرة من المعلومات السرية التي يجب حمايتها من التنصت. لكن (HTTPS) لا يحمي فقط المعلومات المرفوعة، مثل أرقام الضمان الاجتماعي، بل سرية ما يقرأه الناس أيضًا. ومن أمثلة المخاطر الناجمة عن عدم تطبيقه:

قد يتجسس صاحب العمل على عاملة تنزل معلومات عن حقها في التنظيم النقابي، ثم ينتقم منها. وقد يتعرض موظف في شؤون المحاربين القدامى يريد الإبلاغ عن احتيال دون كشف هويته لتجسس غير قانوني من جهة حكومية أخرى، فتُكشف هويته للانتقام.

وقد تُكشف هوية مواطن أمريكي في الخارج يبحث في موقع وزارة الخارجية عن معلومات عن تغيير الجنس بواسطة متطفلين على الشبكة المحلية، فيُسجن أو يُقتل. وقد يتجسس مسؤولون محليون على أمريكي من أصل إفريقي حُرّم حق التصويت ويريد تقديم شكوى إلى وزارة العدل، فيهددونه.

هذه عينة فقط من الفئات المحمية الكثيرة التي تحتاج إلى وصول سري حقيقي إلى الخدمات الحكومية وتستحقه. لحسن الحظ، أصبح تطبيق (HTTPS) أسهل وأرخص من أي وقت. وندعو الحكومة الفدرالية إلى تنفيذ معيار (HTTPS) وحده بأسرع ما يمكن، وعلى الحكومات الأخرى في العالم أن تفعل الشيء نفسه.

إذا وافقت، فشارك الحكومة رأيك بتقديم تعليق عام إلى مكتب الإدارة والميزانية، عبر البريد (https@cio.gov) أو (GitHub). ونشجعك أيضًا على مطالبة حاكم ولايتك ومدير معلوماتها بتطبيق المعيار.

وبالمناسبة، لك أن تستخدم أي جزء من هذه الوثيقة أو كلها في تعليقك العام. فهي، مثل محتوى موقع (EFF)، متاحة بترخيص المشاع الإبداعي؛ وهذه الصفحة تحديدًا تحت (CC0).

حدود الحماية:

لا يضمن (HTTPS) مثلًا خلو الموقع من ثغرات (CSRF) أو (XSS). ومن دون حماية إضافية مثل (Tor)، قد تبقى هوية المستخدم عرضة للخطر، لأن عنوان (IP) لحاسوبه والخوادم التي يتصل بها يظلان مكشوفين لمراقبي الشبكة. ومن دون أدوات مثل (Privacy Badger) قد يبقى المستخدم عرضة لتتبع الأطراف الثالثة بأشكاله. والأقل وضوحًا أن المراقب قد يستنتج أحيانًا المحتوى الذي ينزله المستخدم أو خصائص الموقع التي يستعملها، بتحليل حركة المرور وأحجام الحزم المرسلات والمتلقاة.