

الدليل السريع
لموضوع
القبول العالمي



ما الذي يعنيه "القبول العالمي"؟

القبول العالمي (UA) هي الحالة التي يتم فيها قبول جميع أسماء النطاقات وعاوين البريد الإلكتروني الصحيحة، والتحقق من صحتها وتخزينها ومعالجتها وعرضها بشكل صحيح ومتناسق من قبل كافة التطبيقات والأجهزة والنظم التي تدعم خدمة الانترنت.

بسبب التغيرات السريعة في خريطة اسماء النطاقات، فإن العديد من الأنظمة لا تعترف أو تعالج أسماء النطاقات الجديدة بشكل مناسب ، ويعود ذلك في المقام الأول لأنها قد تكون أكثر من ثلاثة أحرف في الطول أو ليست على صيغة ASCII. ونفس الشيء ينطبق على عناوين البريد الإلكتروني التي تتضمن هذه الامتدادات الجديدة.

المجموعة التوجيهية للقبول العالمي (UASG)، والتي أسستها هيئة الإنترنت للأسماء والأرقام المخصصة (ICANN)، هي مبادرة بقيادة المجتمع على النطاق الصناعي تعمل على نشر الوعي وتحديد وحل المشاكل المرتبطة بالقبول العالمي لأسماء النطاقات. والغرض من هذه الجهود هو المساعدة على ضمان تجربة متناسقة وإيجابية لمستخدمي الإنترنت على مستوى العالم.

للحصول على المزيد من المعلومات عن المجموعة التوجيهية للقبول العالمي (UASG) والتطورات الأخيرة، قم بزيارة موقعنا: www.uasg.tech.

القبول



التحقق



التخزين



المعالجة



العرض



تدعم البرمجيات والخدمات عبر الإنترنت
القبول العالمي عندما توفر القدرات المذكورة
أعلاه لكافة أسماء النطاقات وعاوين البريد
الإلكتروني.

القبول



توصيات المجموعة التوجيهية للقبول العالمي UASG

يجب على أي عنصر بواجهة المستخدم يتطلب من المستخدم كتابة اسم نطاق أو عنوان بريد إلكتروني أن يدعم يونيكود سلاسل احرف تصل إلى 256 حرفا.

يجب السماح للمستخدمين، وليس مطالبهم، بإدخال نص مشفر متوافق مع ASCII (ويعرف أيضا باسم "Punycode") بدلا من اليونيكود المكافئ له .
وعلى الرغم من ذلك، يجب إظهار يونيكود بشكل افتراضي مع عرض Punycode للمستخدم فقط عندما يوفر ميزة ما .

القبول هو العملية التي يتم فيها تلقي عنوان البريد الإلكتروني أو اسم النطاق كسلسلة من الأحرف من خلال واجهة المستخدم، ملف أو API (الواجهة البرمجية للتطبيق) المستخدمة من قبل تطبيق أو خدمة عبر الإنترنت.

التحقق



توصيات المجموعة التوجيهية للقبول العالمي UASG

لا يجب أن يتم التحقق من البيانات إلا إذا كان مطلوباً لسلسلة عمل التطبيق أو الخدمة. هذه هي أسهل وسيلة لضمان قبول جميع أسماء النطاقات الصحيحة في النظم.

إذا كان التحقق مطلوباً، يجب مراعاة ما يلي:

التحقق من صحة جزء النطاق العلوي (TLD) لاسم النطاق بالاستعانة بجدول رسمي:

<http://www.internic.net/domain/root.zone>

<http://www.dns.icann.org/services/authoritative-dns/index.html>

<http://data.iana.org/TLD/tlds-alpha-by-domain.txt>

راجع أيضاً SAC070: <https://tinyurl.com/sac070>

استعلم عن اسم النطاق من خلال نظام أسماء النطاقات (DNS).

المطالبة بتكرار إدخال عنوان البريد الإلكتروني لتجنب أخطاء الكتابة.

التحقق من صحة الأحرف في المسميات فقط بالتأكد من أن U-Label لا يحتوي على رموز "غير مسموح بها" أو رموز غير مشمولة في نسخته من اليونيكود.

<https://tools.ietf.org/html/rfc5892>.

اقتصار التحقق من المسميات لعدد قليل من قواعد المسميات الكاملة والتي يتم تحديدها في طلبات التعليقات (RFC). قم بزيارة: <https://tools.ietf.org/html/rfc5894>.

إذا كانت سلسلة من الأحرف تمثل اسم نطاق وكانت تحتوي على حرف الوقف الرسومي '،'، يجب تحويله إلى '!' قبل إجراء التحقق من الصحة.

هي العملية التي يتم من خلالها التحقق من صحة البناء النصي لعنوان البريد الإلكتروني أو اسم النطاق الوارد أو الصادر، وقد تم تدريب العديد من المبرمجين للتحقق من صحة النص بالتحقق من أن النطاق العلوي يحتوي على العدد "الصحيح" من الأحرف، أو أن الأحرف من مجموعة أحرف ASCII. هذه الطريقة للتحقق لم تعد قابلة للتطبيق بسبب طرح أسماء نطاقات تحتوي على أكثر من ثلاثة أحرف، وحروف يونيكود (غير ASCII).



توصيات المجموعة التوجيهية للقبول العالمي UASG

التطبيقات والخدمات يجب أن تدعم معايير يونيكود مناسبة.

يجب أن يتم تخزين المعلومات بتنسيق UTF-8 (تنسيق يونيكود-8) كلما كان ذلك ممكناً. قد تتطلب بعض الأنظمة دعم UTF-16 أيضاً، ولكن بشكل عام يفضل UTF-8. وينبغي تجنب UTF-7 و UTF-32.

راعي جميع السيناريوهات المتكاملة قبل تحويل مسميات-A الى مسميات-U والعكس بالعكس عند التخزين. قد يكون من المرغوب فيه ابقاء مسميات-U فقط في الملف أو قاعدة البيانات، لأنه يسهل البحث والفرز. ومع ذلك، قد يكون للتحويل تأثيرات عند التشغيل البيئي مع التطبيقات والخدمات الأقدم والتي لا تدعم يونيكود. يفضل مراعاة التخزين بالتنسيقين معاً.

ميز عناوين البريد الإلكتروني وأسماء النطاقات بوضوح أثناء التخزين لتسهيل الوصول إليها. وقد أدت حالات تم فيها ملئ عناوين البريد الإلكتروني وأسماء النطاقات تحت حقل "المؤلف" للوثيقة أو "معلومات الاتصال" في ملف السجل إلى فقدان المصدر كعنوان.

التخزين يشير إلى تخزين طويل الأجل و/أو مؤقت لأسماء النطاقات وعناوين البريد الإلكتروني. بغض النظر عن عمر البيانات، فإنه يجب أن يتم تخزينها في تنسيقات معرفة من قبل طلبات التعليقات RFC (يفضل) أو غيرها من الأشكال التي يمكن أن تحول بين التنسيقات المعرفة في وثائق طلبات التعليقات (RFC).



توصيات المجموعة التوجيهية للقبول العالمي UASG

حيث أن معيار يونيكود يتوسع باستمرار، فإن الرموز التي لم تكن معرفة عندما تم إنشاء التطبيق أو الخدمة يجب أن يتم التحقق منها للتأكد من أنها لن "تخل" بتجربة المستخدم. نقص الخطوط في نظام التشغيل الأساسي قد يؤدي إلى أحرف غير قابلة للعرض (في كثير من الأحيان يتم استخدام "□" لتمثيل هذه)، ولكن يجب ألا يؤدي هذا الوضع إلى فشل كارثي.

استخدم واجهات برمجة التطبيقات التي تدعم يونيكود.

استخدم أحدث بروتوكول لأسماء النطاقات المدوّلة في التطبيقات (IDNA)

[<http://tools.ietf.org/html/rfc5891>]

وثائق الجداول [http://tools.ietf.org/html/rfc5892] لأسماء النطاقات المدوّلة (IDNs).

قم بالمعالجة بتنسيق UTF-8 حيثما كان ذلك ممكناً.

تأكد من أن المنتج أو الميزة يعالج الأرقام كما هو متوقع. على سبيل المثال، أرقام ASCII والأرقام الأيديولوجية الآسيوية يجب أن تعامل كأرقام. [RFC5892، الرابط اعلاه]

قم بتحديث التطبيقات والخوادم/الخدمات معاً. إذا كان الخادم يدعم Unicode والعمل لا يدعم Unicode أو العكس، فسوف يتوجب تحويل البيانات إلى صفحة الرموز المناظرة في كل مرة تنتقل فيها البيانات بين الخادم والعمل.

قم بمراجعة برامج التطبيقات لتجنب الهجوم بإغراق ذاكرة التخزين المؤقت. عند القيام بتحويل الأحرف، قد تنمو أو تنكمش السلاسل النصية بشكل كبير.

تحدث المعالجة كلما تم استخدام عنوان البريد الإلكتروني أو اسم النطاق من قبل تطبيق أو خدمة لتنفيذ عملية (على سبيل المثال، البحث أو فرز قائمة)، أو تحويلها (إلى تنسيق بديل (على سبيل المثال، تخزين ASCII كيونيكود). قد يحدث أيضاً تحقق إضافي من صحة البيانات أثناء المعالجة.

أسماء النطاقات وعناوين البريد الإلكتروني يمكن معالجتها بعدد غير محدود من الطرق*، الأمر الذي يعزز الحاجة إلى اتفاقات لضمان فهم البيانات وتصنيفها بشكل منسق.



توصيات المجموعة التوجيهية لقبول العالمي UASG

عرض كل رموز اليونيكود التي يدعمها نظام التشغيل الأساسي. إذا كان التطبيق يحتفظ بمجموعات الخط الخاصة به، ينبغي أن يقدم دعماً شاملاً لليونيكود لمجموعة الخطوط المتوفرة من نظام التشغيل.

عند تطوير تطبيق أو خدمة، أو عند تشغيل سجل، خذ بعين الاعتبار اللغات المدعومة والتأكد من أن نظام التشغيل والتطبيقات تغطي تلك اللغات.

قم بتحويل البيانات غير يونيكود إلى يونيكود قبل عرضها. على سبيل المثال، يجب ان يرى المستخدم النهائي "نطاق-علوي.الجميع" بدلاً من "xn--mgbk3b2bg4a.xn----ymc1ck7boiws". (هذا التحويل هو مثال على جاهزية معالجة UA).

عرض يونيكود افتراضياً. استخدام النص على هيئة Punycode للمستخدم فقط عندما يقدم ميزة. اضع نص حوام على هيئة Punycode عند عرض يونيكود كتخفيف.

راعي أن العناوين ذات النصوص المختلطة سوف تصبح أكثر شيوعاً. بعض رموز يونيكود قد تبدو متشابهة للعين البشرية، ولكن مختلفة لأجهزة الحاسوب. لا تفترض أن السلاسل ذات النصوص المختلطة المراد بها أعراض خبيثة، مثل التصيد، وإذا كانت واجهة المستخدم تلقت انتباه المستخدمين إلى سلاسل الرموز، تأكد من أنها تفعل ذلك بطريقة لا تضر بمستخدمي النصوص غير اللاتينية.

تعلم المزيد عن الاعتبارات الأمان لليونيكود في: <http://unicode.org/reports/tr36>

استخدم معالجة التوافق لأسماء النطاقات المدوّلة في التطبيقات (IDNA) لتتماشى مع توقعات المستخدمين. لمعرفة المزيد، انتقل إلى: <http://unicode.org/reports/tr46>.

كن حذراً من الرموز غير المخصصة والغير مسموح بها. لمعرفة المزيد: RFC 5892: <https://tools.ietf.org/rfc/rfc5892.txt>

يحدث العرض كلما تم تقديم عنوان بريد إلكتروني أو اسم نطاق ضمن واجهة المستخدم. عرض أسماء النطاقات وعناوين البريد الإلكتروني عادة ما تكون بسيطة عندما يدعم نظام التشغيل الأساسي الأحرف المستخدمة وتكون سلاسل الأحرف مخزنة على شكل يونيكود. وعلى الرغم من ذلك، فإن عمليات تحويلات خاصة بالتطبيقات قد تكون مطلوبة خلافاً لذلك.

كن مستعد للقبول العالمي

مراجعة أصل برامج التطبيقات واختبار الوحدات

عملية فحص برامج التطبيقات والتحقق من أن أساليب البرمجة الصحيحة ومكتبات البرمجيات وواجهاتها (يعرف أيضا ب API) هي فقط التي قد استخدمت. بعد الانتهاء من هذا، يمكن للمسؤول التحقق من عمل التطبيق أو الخدمة عن طريق اختبار إمكانيات محددة (قبول والتحقق، ..الخ) المذكورة أعلاه. تستخدم هذه الطريقة عادة فقط من قبل مطوري التطبيقات ومزودي خدمات الإنترنت.

وكجزء من جهود التوعية التي تقوم بها المجموعة التوجيهية للقبول العالمي، فإن المجموعة تتواصل مباشرة بمطوري التطبيقات وأكبر موفري خدمات الإنترنت لتشجيعهم على مراجعة واختبار مصدر شفرة البرامج لصالحيتها للقبول العالمي، ونشر قائمة من المعايير التي يمكن استخدامها لتطوير سيناريوهات الاختبار.

الاختبار اليدوي

يتطلب تشغيل عدد من الاختبارات على نطاقات جديدة والنطاقات غير ASCII، مثل إدخال عنوان البريد الإلكتروني عند التسجيل لخدمة ما عبر الإنترنت، والتحقق من أنه قد تم قبولها. بما أنه يوجد عدد لا يحصى من الخدمات عبر الإنترنت المحتملة للأشترك، فضلا عن توليفات عناوين البريد الإلكتروني الجديدة المحتملة، يتطلب هذا الأسلوب تجربة توليفات مختلفة من التطبيقات، والخدمات، وعناوين البريد الإلكتروني و/أو أسماء النطاقات لتوفير مجموعة واسعة من حالات الاستخدام. يمكن استخدام هذا الأسلوب من قبل أي شخص، ولكنه الأكثر جهدا.

وتساعد المجموعة التوجيهية للقبول العالمي أيضا ترويج هذه الطريقة من خلال إنشاء قائمة للمواقع الأكثر زيارةً على الإنترنت، والتطبيقات وعناوين البريد الإلكتروني وأسماء النطاقات المناسبة للاختبار.

الاختبار التلقائي

استخدام النصوص او المشتقات التلقائية لاختبار مجموعة متنوعة من عناوين المواقع. يتطلب هذا الأسلوب المزيد من العمل الفني، ولكنه الأكثر قابلية للتوسع للجهد المبذول للقياس والرصد.

مثال واقعي هو التحريات الأخيرة عن النطاقات العلوية العامة التي يقوم بها APNIC نيابة عن الأيكان

<https://tinyurl.com/new-gtld-ua>

وتتحرى المجموعة التوجيهية للقبول العالمي عن أساليب الاختبار الآلي للقبول عالمي وسوف تنشر النتائج متى كانت متوفرة.

