Iranian Journal of Medical Informatics (2012) Vol 1, Issue 3

Analysis URIs and Provide a New Security Approach for URLs

بررسی URIs و ارائه راهکار نوین امنیتی جهت ایمن سازی URL ها

Mojtaba Farrokhi Far, Mohsen Soltani

Abstract — *In Present Article Primarily Some Explanation About URIs In Order To Encrypting Of Physical And Virtual Resource With RDF Content Is Presented. Encrypting in the present scheme is in the form of reversible and offline and it also has advantages and disadvantages which in this article will be dealt with. the mentioned scheme is similar to URL, but with due to its disadvantages, the potential of its usage will be decreased . Next, the representation of new method for security of URL will be concerned. in this new method, encrypting of physical and virtual resource which will be presented in the form of irreversible algorithm and offline, can increase the security of URL in high extend, and it makes the host information and the wanted website not allow to hackers*[1].

Keywords — algorithm, encoding reversible, encoding irreversible, URIs, encode, decode, URL.

۱. مقدمه

در ابتدا به معنی واژه RDF می پردازیم، Resource Description Framework یا چارچوب توصیف منابع که به اختصار RDF نامیده می شود ; در شبکه (اینترنت) جهت اشتراک یا نمایش منبع به صورت RDF می بایست از طریق URL ها این کار صورت گیرد، ارائه منابع از طریق URL ها مشکلاتی را ایجاد می نماید، که در ادامه به این موضوع بیشتر خواهیم پرداخت .

وقتی به صورت معمول پیوندی به یک URL داده می شود، در حقیقت اطلاعاتی از فضای میزبانی سایت مورد نظر در اختیار بازدیدکننده قرار می گیرد، که این خود باعث کاهش امنیت وب سایت می گردد . در سال ۱۹۹۸ اولین روش ایمن سازی URL ها ارائه گردید، در این روش که به نام URI معروف می باشد URL ها با محتوای RDF به صورت رمزنگاری شده می باشند، که رمزنگاری می تواند به دو صورت بازگشتی یا غیر بازگشتی باشد .

URI به دلیل معایبی که دارد، می تواند اطلاعات لازم را جهت دسترسی هکر به فضای میزبانی دهد . هدف از طرح پیشنهادی که با مطالعات و تجربیات فراوان به دست آمده است، به حداقل رساندن اطلاعات هکر جهت نفوذ به سایت ها می باشد، که امیدواریم برای خوانندگان محترم این مقاله مفید واقع گردد .

طرح شناسه یکسان منابع یا Uniform Resource Identifier scheme که به اختصار با URIs نام گذاری می شود، روشی برای قرار دادن یا نمایش دادن منابع رمزنگاری شده همچون عکس ها، فایل ها و ... در برنامه ها (بیشتر مرورگرها) می باشد . توسط این روش منبع مورد نظر همچون عکس، فایل و ... رمزنگاری می شود ، Encoding کردن این روش با الگوریتم های متفاوت صورت می پذیرد، که متداول ترین روش Encoding در حال حاضر Base64 می باشد .

برای اولین بار این روش در سال ۱۹۹۸ ارائه گردیده و به علت ضعف های امنیتی کمتر استفاده می گردد، ولی نکته ی جالب در اینجا می باشد که کمپانی های بزرگ جهان جهت رمزنگاری از این روش استفاده می نمایند، برای مثال کمپانی گوگل به تازگی مقداری از تصاویر موتور جست و جو خود را توسط URIs رمزنگاری نموده است . کمپانی Mozilla نیز در نسخه ۱۴.۰.۱ مرورگر محبوب خود (FireFox) که در تاریخ 2012/07/17 ارائه گردید برای Background این مرورگر از روش URIs جهت رمزنگاری تصاویر استفاده نموده است .

URIs را در تمامی زبان های برنامه نویسی تحت وب Dynamic(پویا) و Static (ثابت) همچون PHP، ASP، HTML، CSS، Python، Java Script و ... می توان استفاده نمود .

نحوه استفاده از URI را با ذکر یک مثال توضیح می دهیم. به عنوان مثال تصویری با پسوند png و حجم 116byte را می خواهید به URI تبدیل نمایید که طرح URI آن از قالب زیر تشکیل شده است. قسمت اولیه و ثابت کلمه data که نشان دهنده اجرای طرح URI می باشد، پس از این کلمه کاراکتر : قرار می گیرد که ادامه دهنده ی روند قالب می باشد، در قسمت بعدی نوع فایل مشخص می گردد به عنوان مثال اگر تصویر باشد از کلمه image استفاده یا اگر قلم باشد از کلمه font استفاده می نماییم و ...، سپس کاراکتر / را برای ادامه کار قرار داده و در این قسمت Extention یا پسوند فایل را مشخص می نماییم . به عنوان مثال Png یا jpg و ... (در بعضی مواقع از truetype استفاده می شود) کاراکتر ; را قرارداده، در قسمت بعدی قالب URI نوع Unicode را مشخص می نمایید با قرار

[1] M. Farrokhi Far is with Sama College, Qom Branch, Islamic Azad University, Qom, Iran (e-mail: info@e3tar.ir).
M. Soltani is Research Director of Sama College, Qom Branch, Islamic Azad University, Qom, Iran (e-mail: info@qom-samacollege.ir).

دادن کلمه charset= به صورت ثابت و نوع Unicode این قسمت را تکمیل نمایید به عنوان مثال ASCI یا UTF8 و ... کاراکتر ; را گذاشته و نوع رمزنگاری را قرار می ده ید (به عنوان مثال الگوریتم base64 یا base32 و ...)، کاراکتر , گذاشته و فایل رمز نگاری شده را در ادامه قرار می دهید .

data: MIME/type;charset=encoding;base64, encoded data

یک نمونه تصویر (رمزنگاری شده توسط طرح URI به شرح زیر می باشد:

iVBORw0KGgoAAAANSUhEUgAAAAkAAAANCAY
AAAB7AEQGAAAAO0lEQVQoU2NgGKygeeF/BlwY7
GaQJD4AlkdXBDMRphFDEboCuE0wk7ApwFAEE8B
mPeluwuZLuMkEwgkAspVRMzxb5CAAAAAASUVO
RK5CYII%3D

۲. مزایای URIs

عدم نیاز به معرفی نشانی اینترنتی URL (Uniform Resource Locator) که این خود به امنیت فضای میزبانی کمک می کند .

بالا رفتن سرعت Load شدن صفحات با توجه به کم شدن درخواست های HTTP یا Http Request به مرورگر و شبکه (اینترنت) .

قابلیت استفاده به صورت آفلاین .

معایب: URIs

ضعیف بودن بهینه سازی اطلاعات برای موتورهای جست و جو یا SEO (Search Engine Optimization) زیرا دیگر URL ای در کار نیست که موتور جست و جو آدرس آن را ذخیره نماید و در حقیقت موتور جست و جو باید کل RDF رمزنگاری شده را ذخیره نموده که معمولا به خاطر حجیم نشدن پایگاه داده چنین کاری را انجام نمی دهد .

نیاز به پروسه زمانی برای مرورگر جهت Encoding و Decoding کردن اطلاعات .

استفاده بیشتر از منابع سخت افزاری جهت Decoding کردن فایل ها .

با توجه به اجباری بودن استفاده از الگوریتم های بازگشتی قابلیت Decode سازی توسط هکر جهت دسترسی به اطلاعات رمزنگاری شده می باشد .

افزایش حجم صفحات وب یا Application ها با توجه به مقدار بایت های RDF رمزنگاری شده .

با توجه به معایب روش URI و کاربردی نبودن استفاده از آن، در این مقاله به ارائه شیوه ای کاملا نوین و ابتکاری جهت استفاده از روش رمز نگاری URL ها می پردازیم. قبل از هر چیز به معرفی کوتاه این Method می پردازیم :

توسط رمزنگاری URL ها امنیت سایت را به حد زیادی می توان افزایش داد، بدین صورت که اگر به عنوان مثال ما آدرس به نام www.domain.com/test/test.jpg داشته باشیم، می توانیم آن را به صورت رمز نگاری شده به صورت زیر تبدیل نماییم :

www.domain.com/qdsaciQlxqw2ui591XzjHI2mkN
sAli2uhjydsjH9sD821lhASlx8123saH2kil/j1519juSa9
D2158j12c5j1lMxzco2151kmp15h1lashmAshas.jpg

با استفاده از Encoding کردن URL ها می توان از شناسایی Directory ها، File ها و سایر منابع موجود در سرور جلوگیری و در حقیقت از ارائه هرگونه ایده به هکر جلوگیری نمود .

۳.روش های ENCODING آدرس های اینترنتی

به ۲ روش می توان این کار را انجام داد .

رمزنگاری به صورت بازگشتی

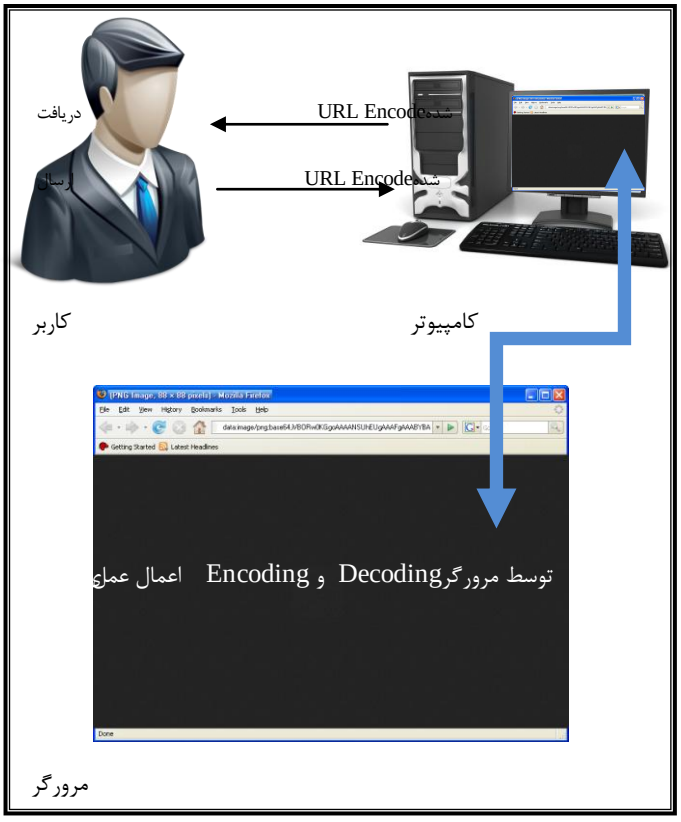
رمز نگاری به صورت غیر بازگشتی

أ. روش اول (رمز نگاری به صورت بازگشتی - آفلاین)

بدین صورت که ما الگوریتمی را طراحی نموده و توسط این الگوریتم که به مرورگر یا Application قبلا شناخته شده، در زمان مورد نیاز رمزنگاری و رمزگشایی نمایید . (شکل ۱)

ویژگی این نوع رمز نگاری، قابلیت رمزگشایی کردن آن می باشد که مدیر سایت می تواند در صورت نیاز به رمزگشایی اقدام به استفاده از URL استاندارد یا Encode نشده نماید .

عیب این نوع رمز نگاری این می باشد، که در صورت کشف الگوریتم هکر می تواند اقدام به رمزگشایی URL ها نماید . الگوریتم های Base64، Base32 نمونه هایی از این روش رمز نگاری می باشند.



شکل (۱) : نقشه (رمز نگاری به صورت بازگشتی – آفلاین)

ب.روش دوم (رمز نگاری به صورت غیر بازگشتی)(روشی کاملا ابداعی)

در این روش RDF ها را به علت حجیم بودن آن ها رمزنگاری نمی کنیم، بلکه

URL ها را به پایگاه داده ارسال نموده و توسط الگوریتم های غیر بازگشتی (به عنوان مثال sha1 یا MD5) آن ها را رمزنگاری و ذخیره می نماییم .

URL رمزنگاری شده توسط Referrer (ارجاع دهنده،معرف) که می تواند وب سایت، Application و ... باشد به کاربر معرفی می شود سپس درخواست مشاهده URL مورد نظر توسط کاربر به مرورگر ارسال می گردد، مرورگر نوع رمز نگاری را تشخیص داده و با توجه به نوع رمزنگاری اقدام به ارسال درخواست جهت رمزگشایی به سرور موجود در شبکه (اینترنت) می نماید، مرورگر پس از تشخیص و بررسی اطلاعات اولیه به Data Base ای که URL ها Encode شده در آن ذخیره می باشد، متصل می گردد . پس از اتصال URL را بررسی نموده و درخواست کاربر در دیتابیس URL ها را جست و جو کرده و به شبکه ارسال می نماید و پس از ارسال URL به شبکه و دریافت پاسخ، صفحه مورد نظر را به کاربر نمایش می دهد . (شکل ۲)

نحوه شناسایی و ارسال درخواست URL به مرورگر بدین صورت می باشد که Data Base ای از قبل تعیین شده و در صورت ارسال درخواست URL Encode شده، مرورگر با تشخیص نوع Encoding به Data Base رمزنگاری URL ها متصل می گردد .

ویژگی این نوع رمزنگاری، غیر قابل هک شدن توسط هکر می باشد، بدلیل اینکه الگوریتم در Data Base ای اختصاصی می باشد و هکر اجازه دسترسی به این Data Base را نداشته و امکان هک شدن الگوریتم این نوع رمزنگاری به صفر می رسد .

عیب این نوع رمزنگاری نیاز داشتن به سروری اختصاصی جهت ارسال درخواست های Encode شده می باشد، همچنین نیاز به Data Base ای حجیم جهت Encode و Decode کردن URL ها می باشد .

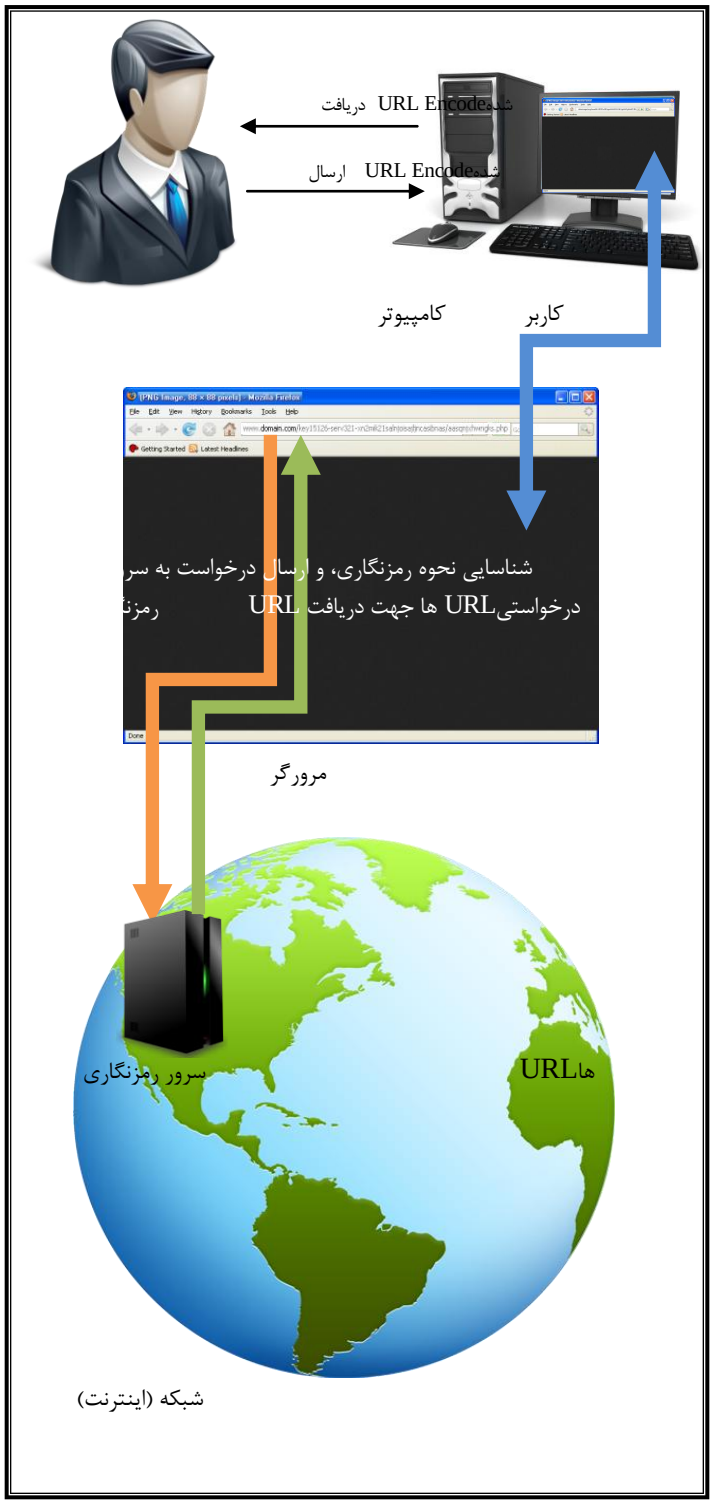
در حقیقت این روش شبیه SSL یا Secure Sockets Layer بوده، ولی دقیقا Invert یا معکوس آن انجام می شود که در ادامه توضیحاتی در این رابطه داده می شود .

ج. تفاوت پروتکل SSL با روش ابداعی رمزنگاری URL ها به صورت غیر بازگشتی

در SSL پروتکل ایمن می شود، اطلاعاتی که توسط کاربر به سرور ارسال و دریافت می شود به صورت رمزنگاری شده تبدیل می گردد و از حملات Interception (شنود داده ها) و Modification (دستکاری داده ها) جلوگیری می شود در صورتی که URL ها ایمن نمی شوند، ولی در این روش URL ها را ایمن سازی نموده و به هکر اجازه شناسایی اطلاعات فضای میزبانی و منابع، داده نمی شود . در روش ابداعی رمزنگاری URL ها اطلاعات ارسالی توسط کاربر رمزنگاری نمی شود، بلکه اطلاعات دسترسی به منابع برای معرفی به کاربر رمزنگاری می شود .

د. شباهت پروتکل SSL با روش ابداعی رمزنگاری URL ها به صورت غیر بازگشتی

در SSL تمامی عملیات رمزنگاری و رمزگشایی داده های ارسالی و دریافتی به صورت آنلاین توسط گواهینامه های ارائه شده توسط کمپانی های معتبر صورت می پذیرد . در روش ابداعی رمزنگاری URL ها نیز عملیات رمزنگاری و رمزگشایی URL ها به صورت آنلاین و توسط سروری معتبر صورت می پذیرد .



شکل شماره (۲) : نقشه (رمز نگاری به صورت غیر بازگشتی – آنلاین)

۴. مزایا

افزایش بیش از ۵۰٪ امنیت وب سایت، دسترسی جهت مشاهده Directory ها و File ها و منابع سایت محدود می گردد و از ارائه ایده به هکر جلوگیری

می شود .

جلوگیری از حملات Injection (تزریق) و XSS (Cross Site Scripting) .

قابلیت استفاده از این Method با سایر پروتکل های همچون HTTP، HTTPS، FTP، FTPS و MMS و ... .

۵. معایب

Seo سازی ضعیف: در موتور های جست و جو به علت رمز نگاری شدن URL ها غیر قابل تشخیص می باشد . به همین دلیل سایتی که از Encoding کردن URL ها استفاده می نماید در موتور های جست و جو به خوبی شناخته نمی شود .

پایین بودن سرعت: با توجه به نیاز جهت ارسال درخواست به سرور Encoding جهت مقایسه URL رمزنگاری شده توسط مروگر و تشخیص URL اصلی، مرورگر زمانی را جهت دریافت اطلاعات صرف می نماید که باعث پایین آمدن سرعت مشاهده صفحات می گردد .

بالا بودن هزینه ها جهت راه اندازی این سرویس .

نیاز به سروری ۱۰۰٪ آنلاین، در صورتی که سرور رمزنگاری URL ها با Down Time مواجه شود باعث عدم مشاهده URL ها توسط کاربران می گردد .

۶. موارد مورد نیاز جهت رمز نگاری به صورت غیر بازگشتی

طراحی یک مرورگر جدید جهت اجرای Method های لازم، یا طراحی Plugin برای سایر مرورگر ها جهت اجرای Method های لازم.

انتخاب یک سرور به جهت نگهداری پایگاه داده URL های Encode شده.

طراحی الگوریتم ای در سطح Hashing برای Encoding آدرس ها.

طراحی پایگاه داده (Data Base) جهت ذخیره سازی اطلاعات رمزنگاری شده و اطلاعات درخواستی از طرف مرورگر.

۷. نحوه ی کار

نحوه ارسال اطلاعات از کاربر به مرورگر و مروگر به سرور رمزنگاری:

کاربر وارد سایت (صفحه اصلی یا index) مورد نظر خود می شود، هم اکنون فرض نموده این سایت را به روش رمزنگاری ابداعی ایمن سازی نموده ایم . به عنوان مثال مسیر را جهت مشاهده آرشیو مطالب به کاربر می خواهیم معرفی نماییم .

آدرس آن به صورت زیر می باشد :

www.domain.com/key15126-serv321-xN2mik21salNjoisAjljncasiBnas/Aasqnjxhwn Gks.php

در آدرس بالا key15126 آدرس کلیدی است که مدیر سایت آن را جهت رمزنگاری URL های خود استفاده نموده است .

همچنین serv321 سروری می باشد که اطلاعات سایت فوق به صورت Encrypt شده در دیتابیس آن وجود دارد. توسط این ۲ شناسه مرورگر تشخیص می دهد که باید توسط چه کلیدی و توسط چه سروری به اطلاعات رمزنگاری شده دسترسی پیدا نماید و پس از دسترسی مقایسه نمودن اطلاعات در صورتی که آدرس رمزنگاری شده صحیح باشد مرورگر را به صفحه درخواستی کاربر ارجاع می دهد .

به کاربر Encrypt) و Irreversible به صورت غیر بازگشتی (URLدر ادامه نمایش داده می شود . همچنین کاربر می بایست در مرورگر خود کلیدی را جهت شده ثبت نماید .Encrypt های URLاستفاده از این

شایان به ذکر می باشد که طرح فوق به صورت آزمایشی در شبکه ای کوچک مورد آزمایش و ارزیابی قرار گرفته و با موفقیت انجام شده است .

۸. نتیجه گیری

با توجه به بررسی روش URI جهت رمزنگاری URL ها و مشاهده نقاط ضعف این طرح راه کاری را جهت رمزنگاری URL ها ارائه نموده ایم در راهکار ارائه شده که به صورت آنلاین ارائه می گردد از حملات Injection که باعث ارسال Value های غیر مجاز به پایگاه داده سایت می شود جلوگیری می گردد، همچنین مانع از حملات XSS که هکر توسط این Method به مخزن موقت اطلاعات (Cache یا Temp) کاربران سرور دسترسی پیدا می کند، می شود .

در این روش همچنین از دسترسی به Directory ها و منابع سرور جلوگیری می شود . یکی دیگر از ویژگی های روش فوق قابلیت استفاده از آن بر روی پروتکل های مختلف می باشد .

از این روش برای طراحی سایت ها با قابلیت های یک Application می توان استفاده نمود، همچنین با طراحی نرم افزار هایی تحت سیستم عامل و قرار دادن کدهای API در این برنامه ها می توان سایتی را به صورت Application طراحی نمود که دارای امنیتی بسیار بالایی بوده و مناسب برای کاربران حرفه ای و آماتور می باشد.

قابلیت های استفاده از این روش رمزنگاری برای سایت های مراکز دولتی و خصوصی مهم کشور به جهت اهمیت اطلاعات آن ها به شدت احساس می شود.

سپاسگزاری

مجتبی فرخی فر : با تشکر از خانواده ی دلسوزم ، اساتید گرامی مهندس مرتضوی و صفایی که مرا در ارائه این مقاله یاری نموده اند .

محسن سلطانی : با تشکر از زحمات مادر و همسرم که همیشه مشوق اصلی من بوده اند و از جناب آقای شریفی معاونت محترم سما قم که پشتیبان همیشگی ما در فعالیت های پژوهشی می باشند .

REFERENCES

1 Mivald E. Essential Network Security. Sharif University. 2006, IsIran: Tehran.
2 Modiri N, Jangjoo, M. Computer Networks Security Engineering. 2010, Mehregan Ghalam: Tehran.
3 Davari Dolatabadi M. Reference for security based on CompTIA Security+. 2010, Pendar Pars: Tehran.
4 Cormen L, Rivest S. Introduction to Algorithms. 3rd Ed. 2009.
5 Berners-Lee T. Uniform Resource Identifiers (URI): Generic Syntax, Available at: http://www.ietf.org/rfc/rfc2396.
6 Gregorio. URI Template.
7 Masinter L. The data URL scheme.
8 Hansen T. Guidelines and Registration Procedures for New URI Schemes. 2006.
9 Berners-Lee T. Uniform Resource Identifier (URI): Generic Syntax.Available at: http://www.ietf.org/rfc/rfc3986#section-1.1.1