```
The Spanner
                                            Javascript blog with messed up syntax inside
                                                                RPO
                                                                Friday, 21 March 2014
Q- Search..
                                                                Relative VS Absolute
                                                                RPO (Relative Path Overwrite) is a technique to take advantage of relative URLs by
            Inspiration
                                                                overwriting their target file. To understand the technique we must first look into the differences
                                           Alex Inführ
                                                                between relative and absolute URLs. An absolute URL is basically the full URL for a
                                               Arshan
                                                                destination address including the protocol and domain name whereas a relative URL doesn't
                                               Ascetik
                                                                specify a domain or protocol and uses the existing destination to determine the protocol and
                                               beford
                                                                domain.
                                            Billy Rios
                                         Chris Weber
                                                                Absolute URL
                                          David Ross
                                                                https://hackvertor.co.uk/public
                                       Eric Lawrence
                                         hackademix
                                                                Relative URL
                                           Hackvertor
                                                                public/somedirectory
                                         Halvar Flake
                                     Jesse Ruderman
                                                                The relative URL shown will look for public and automatically include the domain before it
                                          Joe Walker
                                                                based on the current domain name. There are two important variations of a relative URL, the
                                          John Resig
                                                                first is we can use the current path and look for a directory within it such as "xyz" or use
                                              Kuza55
                                                                common directory traversal techniques such as "../xyz". To see how these work within markup
                                     maliciousmarkup
                                                                let's take a look at a common relative URL used within a stylesheet.
                                   Manuel Caballero
                                        Matt Presson
                                            Miscoded
                                                                 <html>
                                              nihilogic
                                                                 <head>
                                              PHPIDS
                                                                <link href="styles.css" rel="stylesheet" type="text/css" />
                                       pro.grammatic
                                                                 </head>
                                              Reiners
                                             rgaucher
                                                                 <body>
                                                                 </body>
                                          Sirdarckcat
                                                                 </html>
                                             sla.ckers
                                        Soroush Dalili
                                                                The link element above references "style.css" using a relative URL, depending where in the
                                         Stefan Esser
                                                                sites directory structure you are it will load the style sheet based on that. For example if you
                                     Stefano Di Paola
                                                                were in a directory called "xyz" then the style sheet would be loaded from "xyz/style.css".
                                         Thornmaker
                                                                 The interesting aspect of this is how the browser knows what a correct path is since it doesn't
                                        tssci-security
                                                                have access to the server's file system. The answer is it doesn't. There is no way to
                                                                determine a valid directory structure from outside the file system you can only make educated
                                      Web Reflection
                                                                 guesses and use http status codes to determine their existence.
                                Yosuke HASEGAWA
                                                                The missing styles
            Recent Comments
Gareth Heyes on Sandboxing and parsing jQuery
                                                                I noticed something interesting with relative styles, manipulating the path of the site could
                                                                result in styles failing to load. It occurred to me this was a flaw in some way but the pieces of
       Ariya on Sandboxing and parsing jQuery in
                                                                the jigsaw didn't make sense yet. How could it be exploited?
Gareth Heyes on Sandboxing and parsing jQuery
                                                                       Relative and absolute URLs
                                                                                                                                                                                      ∴ v C S Coogle
                                                                  ( iii ) ( more webdeveloperanotes.com/design/relative_and_absolute_urls.php)
Rick on Sandboxing and parsing jQuery in 100ms
      Gareth Heyes on MentalJS Sandbox/Parser
                                                                                                                 Developers
                                                                                                             Basics Tutorials Tips & Tricks Articles New Do 17 Web Graphics Design Resting Eps Web Page Design Resources (Blog
                  March 2014
            \mathsf{M} \mathsf{T} \mathsf{W} \mathsf{T} \mathsf{F} \mathsf{S} \mathsf{S}
                                                                                                                              Homecage → Hist, Fage, Design
                                                                                                         Web Page Design Articles
                                                                                                                                                                                      ਤੀ f 🕒 🔊
                                                                                                                              Relative and absolute urls
                                                                                                         What should be the width of a
                                                                                                                              What are relative and absolute URLs and which one should I use for web sites? This
            3 4 5 6 7 8 9
                                                                                                                              question is asked by almost everyone when they make their first web site. Let us first
                                                                                                                               understand what they mean and then I will provide some advice on which one to use and
          10 11 12 13 14 15 16
                                                                                                                               In this article we first discuss absolute URLs followed by relative URLs. A detailed article on
          17 18 19 20 <u>21</u> 22 23
                                                                                                         Test web prowser definition and 
which is the best
                                                                                                                              URLs can be found in the Basics section of this web site. So if you don't know what is a URL.
                                                                                                                               I suggest you first the read this page - LRLs . What is an URL?
                                                                                                                                                                                       Socius Notreal enail Instructions to install physiologis on Windows 7
          24 25 26 27 28 29 30
                                                                                                        Using WYSIWYG HTML, editors 
advantages and disadvantages
          31
                                                                                                                              In addition to several other meanings, the word absolute, in English, means 'not dependent
                                                                                                         Optimizing web pages
                                                                                                                               An Absolute URL is, thus, something that is independent or free from any relationship. When
           <u>« Feb</u>
                                     <u>Apr »</u>
                                                                                                         Variability in web page displays
                                                                                                                              you use an absolute URS, you point directly to a file. Hence, an absolute URS, specifies the
                                                                                                         Relative and absolute urts
                                                                                                                               exact location of a file/directory on the internet. It also follows that each absolute URL is:
                                                                                                        Structuring web sites - Web site 
design and layout
                                                                                                                              unique, which means that if two URLs are identical, they point to the same file.
                                                                                                        Browser compatible fonts - which fonts to use on web pages?
                                                                                                                              http://www.webdevelopersectes.com/mages/email.gif specifies an image file email.gif
                                                                                                                              located in the images directory under www.webdevelopersnotes.com.domain.name.
                                                                                                                              Similarly, the absolute URL of the document you are viewing is
                                                                                                         List of HTML character entitles
                                                                                                                              http://www.webdevelopersectes.com/design/ relative_and_absolute_urls.php3 which is a
                                                                                                                              page in the directory called design on this web site.
                                                                                                         Web safe colors
                                                                                                         Web safe colors list.
                                                                                                         Detailed list of HTML color 
names
                                                                                                                              A relative URL points to a file/directory in relation to the present fleidirectory.
                                                                                                         List of html colour names
                                                                                                                              Let us understand relative URLs through a small exercise.
                                                                                                         Browsers - the complete list
                                                                                                                              Look at the two URL above. We want to include (display) the image file email of stored in the
                                                                                                                               images directory of www.webdevelopersnotes.com domain on this
                                                                                                         Windows web browsers list
                                                                                                                               (relative_and_absolute_uris_php3 stored in the design directory) page.
                                                                                                         Download list of text web-
browsers
                                                                                                                               There are two ways to do this. We can either refer to it using an absolute URL or use a
                                                                                                                              relative URL. The <a>cing></a> tag for this image display will be as follows:
                                                                                                                               Using an Absolute URL in an < Lucy tag
                                                                   Electric III Relative and absolute URLs
                                                                  ( 🛊 🗎 🖰 www.webdeveloperanctes.com/design/relative_and_absolute_arls.php//
                                                                  Homepage Agrow Web Page Design
                                                                  Relative and absolute urls
```

Cancel and delete an AOL email account. Advantages of dedicated serve Can you trust information on the web? Closure of Hotmail account phishing scam example Good security question for your account Popular Articles Hotmail Sign in page Create Omail address ☆ ∀ C S • Google P E- + + -What are relative and absolute URLs and which one should I use for web sites? This question is asked by almost everyone when they make their first web site. Let us first understand what they mean and then I will provide some advice on which one to use In this article we first discuss absolute URLs followed by relative URLs. A detailed article on URLs can be found in the Basics section of this web site. So if you don't know what is a URL, I suggest you first the read this page - URLs - What is an URL? Absolute URL In addition to several other meanings, the word absolute, in English, means "nor dependent on anything else". It also means "free from doubt". An Absolute URL is, thus, something that is independent or free from any relationship. When you use an absolute URL, you point directly to a file. Hence, an absolute URL specifies the exact location of a file-directory on the internet. It also follows that each absolute URL is unique, which means that if two URLs are identical, they point to the same file. http://www.webdevelopersnotes.com/images/email.gif specifies an image file email.gif located in the images directory, under www.webdevelopersnotes.com domain name. Similarly, the absolute URL of the document you are viewing is http://www.webdevelopersnotes.com/design/ relative_and_absolute_urls.php3 which is a page in the directory called design on this web site. Relative URL A relative URL points to a file/directory in relation to the present file/directory. Let us understand relative URLs through a small exercise. Look at the two URL above. We want to include (display) the image file email gif stored in the images directory of www.webdeveloperanotes.com domain on this (relative_and_absolute_aris_php3 stored in the design directory) page. There are two ways to do this. We can either refer to it using an absolute URL or use a relative URL. The tag for this image display will be as follows: Using an Absolute URL in an tag <img src="http://www.webdevelopersnotes.com/images/email.gif"
width="..." height="..." /> Using a Relative URL in an tag <ing src="../images/email.gif" width="..." height="..." /> The absolute URL is straight forward but in the relative URL you'll notice that I have referred to the image with .../images/email.gif. In order to understand the relative URL, let me tell you about the directory structure of this web site. This web site has several sections and the files and web pages for each section have been segregated into different directory. This helps me to keep things organized and unclustered on the web site. Under the document or server root directory (the main directory of the web site), I have a directory called images which stores all common images used on the pages of this web site. The image email gifresides in this directory called design which is at the same level as images i.e. it is also in the document root directory. This design directory contains the files and web pages for the "Web Page Design" section of this web site. Diagramatically, the scenario can be represented as: Now to access entill gif file from relative_and_absolute_and_absolute_and_absolute_and_absolute URL we put _images/email.gif in the SRC attribute. We, thus, instruct the browser to first go one level up (i.e. to the document root) and then move to the images The two screenshots above show a site without manipulating with URL the styles load as expected however in the second screenshot the same site is loaded with an added forward slash and the relative style sheet does not load. Simply adding a forward slash at the end of the URL breaks the styles of the relative style. Looking in Firebug we can see the style wdn.css returns a 404 when we add the forward slash. ☆ ∀ C S - Google

P E + + + -

Relative and absolute URLs P □ + + + -(iii) (www.webdevelopernotes.com/design/relative_and_absolute_urls.php?) Homepage Agrow Web Page Design Relative and absolute urls What are relative and absolute URLs and which one should I use for web sites? This question is asked by almost everyone when they make their first web site. Let us first understand what they mean and then I will provide some advice on which one to use In this article we first discuss absolute URLs followed by relative URLs. A detailed article on URLs can be found in the Basics section of this web site. So if you don't know what is a URL, I suggest you first the read this page - URLs - What is an URL. Absolute URL In addition to several other meanings, the word absolute, in English, means "nor dependent on anything else". It also means "free from doubt". An Absolute URL is, thus, something that is independent or free from any relationship. When you use an absolute URL, you point directly to a file. Hence, an absolute URL specifies the exact location of a file/directory on the internet. It also follows that each absolute URL is unique, which means that if two URLs are identical, they point to the same file. http://www.webdevelopersnotes.com/images/email.gif specifies an image file email.gif located in the images directory, under www.webdevelopersnotes.com domain name. Similarly, the absolute URL of the document you are viewing is http://www.webdevelopersnotes.com/design/ relative_and_absolute_urls.php3 which is a page in the directory called design on this web site. Relative URL A relative URL points to a file/directory in relation to the present file/directory. Let us understand relative URLs through a small exercise Look at the two URL above. We want to include (display) the image file email gif stored in the images directory of www.webdeveloperanotes.com domain on this (relative_and_absolute_arls.php3 stored in the design directory) page. There are two ways to do this. We can either refer to it using an absolute URL or use a relative URL. The tag for this image display will be as follows: Using an Absolute URL in an tag <img src="http://www.webdevelopersnotes.com/images/email.gif"
width="..." height="..." /> # 😪 🔾 ▷ 🗏 + Console HTML CSS Script DOM Net • Cookies [6] Clear Persist All HTML CSS JavaScript XHR Images Plugins Media Fonts UEL Status Domain

ix GET /design/relative such the such pha 200 CK webdevelopersruites.com

ix GET webs.cvs 40-13ct Found webdevelopersruites.com

ix GET enterior yelshoot 40-13ct Found webdevelopersruites.com

ix GET relative_absolute_units_0f 200 CK webdevelopersruites.com

ix GET websyte_absolute_units_0f 200 CK webdevelopersruites.com

ix GET websyte_absolute_units_0f 200 CK webdevelopersruites.com 31,418 64,50,169,109.80 7128 64.50,109,109:80 GET widget,php?v=10 still additive com-2.8 KB 185.31.19.185.60 35 8 173.194.66.101.00 SET _utm.pf?utmev=1.48utm_Cutmond% 200 00 geogle-analytics.com SET_challenge,ju?k+,-cl.twe,.ep+0.1805562 ≥00 00 1018 82087880 # GET pixel*a.1+p-16-mFEk4344..a.1+type.pol 200 OC pixel quantaerve.com 35 8 95.172.94.56:80 10.618 173.194.34.134.443 apis google.com 52 8 72.251.243.38.80

The screenshot shows the style sheet returning a 404 for a style that previously loaded fine without manipulating the path. If the style returns 404 maybe we can manipulate the relative URL further by changing the path. This is in essence what RPO is about, we try to change the relative URL to something we control although this post is about XSS it's worth noting that manipulating relative URLs can be done for any such URL and isn't restricted to XSS.

Quick CSS lesson

Since we are looking at manipulating a style sheet to something we control we must first understand CSS parsing in order to take advantage of it. There is an interesting piece of the CSS 2 specification that we are very interested in. "In some cases, user agents must ignore part of an illegal style sheet. This specification defines ignore to mean that the user agent parses the illegal part (in order to find its beginning and end), but otherwise acts as if it had not been there." CSS 2 specification. Another piece of the jigsaw is added, CSS2 ignores illegal syntax which we can use by supplying a file that contains mixed content of CSS and something else. If we can fool the CSS parsing into ignoring the illegal syntax before our intended code we can get the CSS parser to load our code. CSS selectors offer the best way to do this since an invalid selector can be ignored and all the previous illegal syntax.

Invalid code

* {

}*{color:#ccc;}

There are two tricks to ignore illegal code both involve selectors, depending on the CSS parser a single } will work or {}. We shall look at IE compat since the parser is quite loose and supports CSS expressions. A CSS expression looks like the following:

xss:expression(alert(1)); The first part is a global selector "*" and the { opens the selector a custom property xss is

used and then the expression contains JavaScript that executes alert(1). Self-referencing

If we can make the style sheet self-reference for the page it's on then we can use the CSS

parsing to ignore the HTML and execute our custom CSS in IE compat. When a site includes

a style sheet like the following: <link href="styles.css" rel="stylesheet" type="text/css" />

We simply need to include a forward slash at the end of the URL and the style sheet will end up (if rewriting is available) loading the original page via what the browser thinks is a directory but is in fact the current page. E.g somepage.php/. Now that our style sheet is loading the web page we need to supply it with some CSS to execute, we can do this by mixing persistent data such as a first name or address think of this as both a reflective attack and a persistent attack but the persistent data contains CSS code. To understand this it's better to show the actual structure of the page and you to see the vector itself. Imagine we have a web page with some data we control such as "first name" the web page would look like the following.

<head>

<html>

<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" /> <link href="styles.css" rel="stylesheet" type="text/css" /> </head> <body> Hello {}*{xss:expression(open(alert(1)))} </body>

</html> PoC (IE ONLY): RPO example

The Meta element forces IE's document mode into IE7 compat which is required to execute expressions. Our persistent text {}*{xss:expression(open(alert(1)))is included on the page and

in a realistic scenario it would be a profile page or maybe a shared status update which is viewable by other users. We use "open" to prevent client side DoS with repeated executions of alert. A simple request of "rpo.php/" makes the relative style load the page itself as a style sheet. The actual request is "/labs/xss_horror_show/chapter7/rpo.php/styles.css" the browser thinks there's another directory but the actual request is being sent to the document and that in essence is how an RPO attack works. Further RPO attacks

You might wonder if the RPO attack is restricted to just relative URLs like "styles.css" the answer is no, it's possible to attack URLs such as "../../styles.css" but in this case we need to

provide levels of fake directories until the styles are loaded from the current document. "../" means look above the current directory; we need three levels of fake directories.

<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" /> <link href="../../styles.css" rel="stylesheet" type="text/css"</pre>

/> </head> <body>

Hello {}*{xss:expression(open(alert(1)))} </body>

<html>

<head>

</html> PoC: RPO example 2

we make a request of "/labs/xss_horror_show/chapter7/rpo2.php/styles.css" this means that you could also target a file in a different directory but in this case we pointed it back to the original html file. Note we could have done just rpo2.php/// but I provided the text of fake directory for clarity. There are other variants such as using the @import command which is useful if length or characters are limited. Using the "}" to ignore the HTML again followed by an @import statement works perfectly fine on IE even though technically it's invalid syntax to use an import statement in this way.

This time because the relative URL is looking for a directory twice above the current directory

RPO isn't restricted to IE, we can use the technique on other browsers but JavaScript isn't supported in CSS on Chrome, Firefox, Opera or Safari. Another restriction is that a doctype cannot be included on the target document since this causes the CSS's parsers to stop parsing the HTML file on non-IE browsers. <html>

<head> <link href="../../styles.css" rel="stylesheet" type="text/css"</pre> />

</head> <body> Hello {}*{color:#ccc;}

</body> </html>

PoC: RPO example 3 The document above changes the colour of the text to grey and works on every browser. It works in the same way as the previous PoC but this time uses pure CSS and no expressions.

If a doctype was included in the document it would fail on every browser except if IE was in compat mode. RPO attacks work on any type of document, it's possible to change the target of image files for example but because the image files look for specific strings at the start of the file and the end result is only an image it makes RPO attacks less useful in these circumstances.

PHP example shows the URL being outputted on the page.

Reflected RPO If the URL is outputted on the page we can send the XSS vector via the path. The following

<html> <head> <meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" /> <link href="styles.css" rel="stylesheet" type="text/css" /> </head> <body> Hello <?php echo \$_SERVER['PHP_SELF']?> </body> </html>

There is a relative URL here and "echo \$_SERVER['PHP_SELF']" outputs the current URL of the page requested. We can exploit this by providing some CSS as part of the path since the relative URL will be loaded with our injection and then the CSS will be loaded from the HTML. On some configurations PHP_SELF will truncate the path information, in this instance PATH_INFO can be used.

PoC: RPO example 4 Summary I consider relative URLs harmful since you cannot rely on the browser to correctly determine the correct directory and when used with so called "pretty URLs". Pretty much everyone who

has used relative URLs will be open to this type of attack if the path information is outputted or there is some persistent data that an attacker can manipulate. I recommend absolute URLs should be used throughout a site or relative URLs that begin with a forward slash since this is the only type of relative URL that isn't vulnerable to a RPO attack because it starts at the document root.

Update.. It's worth noting that a relative root url isn't vulnerable to this sort of attack since the directory

« Sandboxed jQuery

is take from the highest point in the structure and I think can't be influenced the way a normal relative url can.

The entry 'RPO' was posted on March 21st, 2014 at 9:09 pm and last modified on September 18th, 2014

at 8:46 pm, and is filed under <u>Uncategorized</u>. You can follow any responses to this entry through the <u>RSS</u> 2.0 feed. Both comments and pings are currently closed.

Bypassing the XSS filter using function reassignment »