



Introduction To Cross Site Scripting

Presented By:
Joe McCray

joe@strategicsec.com

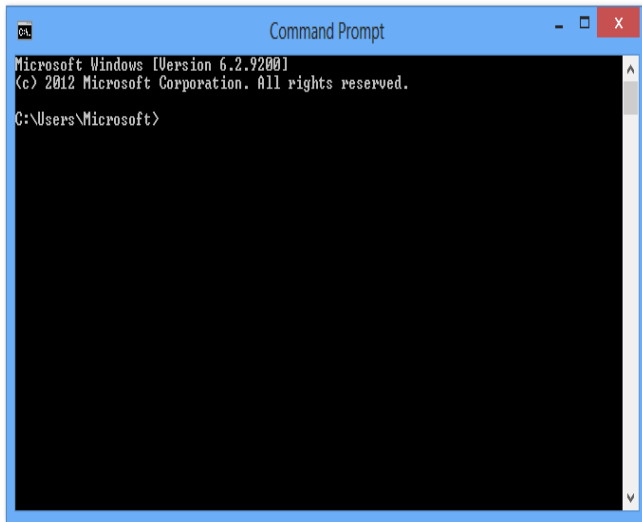
<http://twitter.com/j0emccray>

<http://www.linkedin.com/in/joemccray>

The Basics

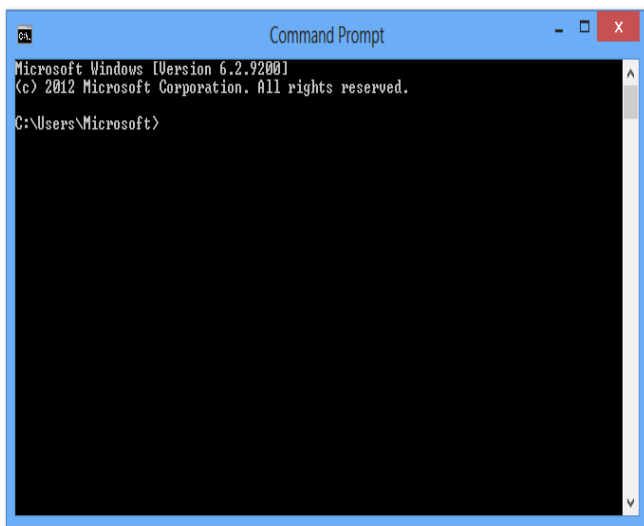
How does IE differ from CMD.EXE?

- Access/Modify Files
- Execute Programs



Here Drive My Box

Surfing the web is like giving every website you go to a shell on your box!



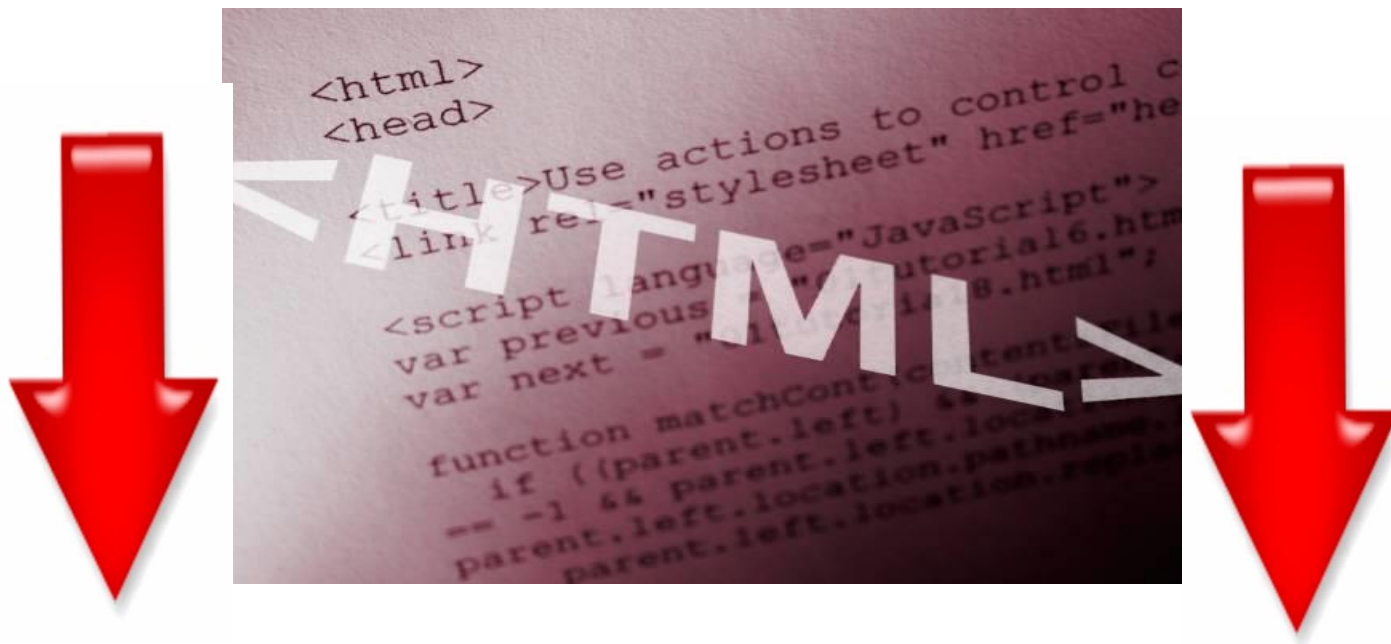
Sh!t just got real!



Reality Check

What's Actually Happening

Your browser just starts at the top of a page and reads until it hits the bottom



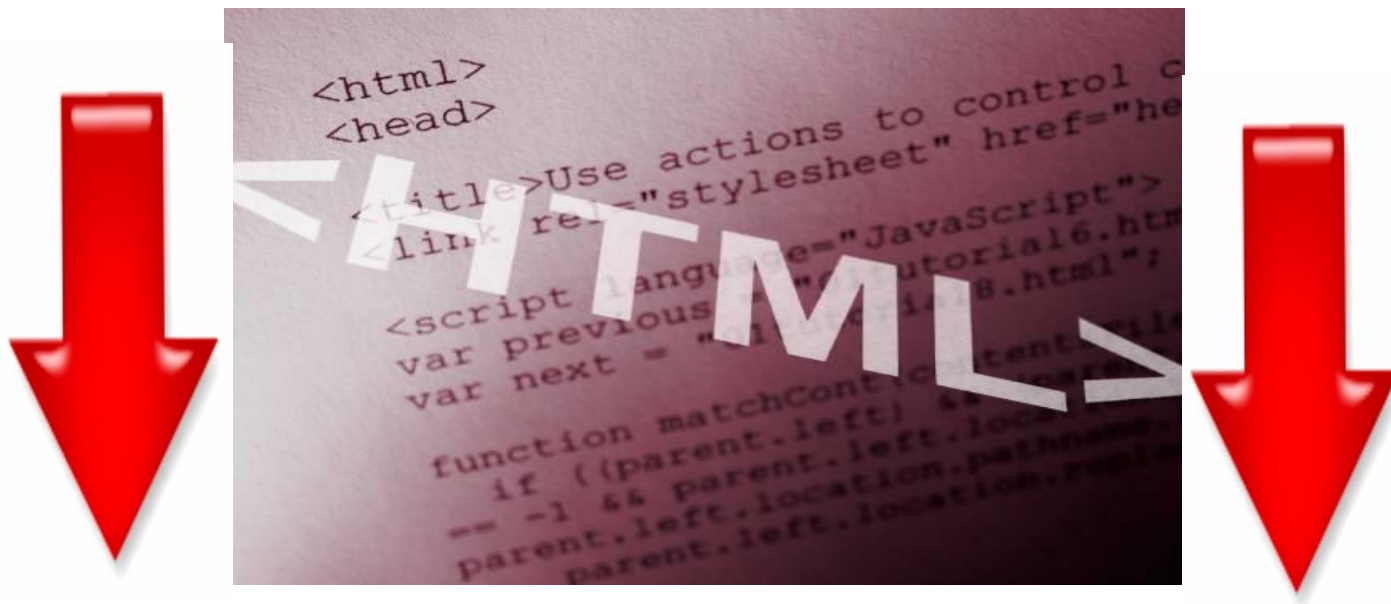


Reality Check

What's Actually Happening

With user generated content webpages your browser thinks the data is from one source

Your browser just starts at the top of a page and reads until it hits the bottom

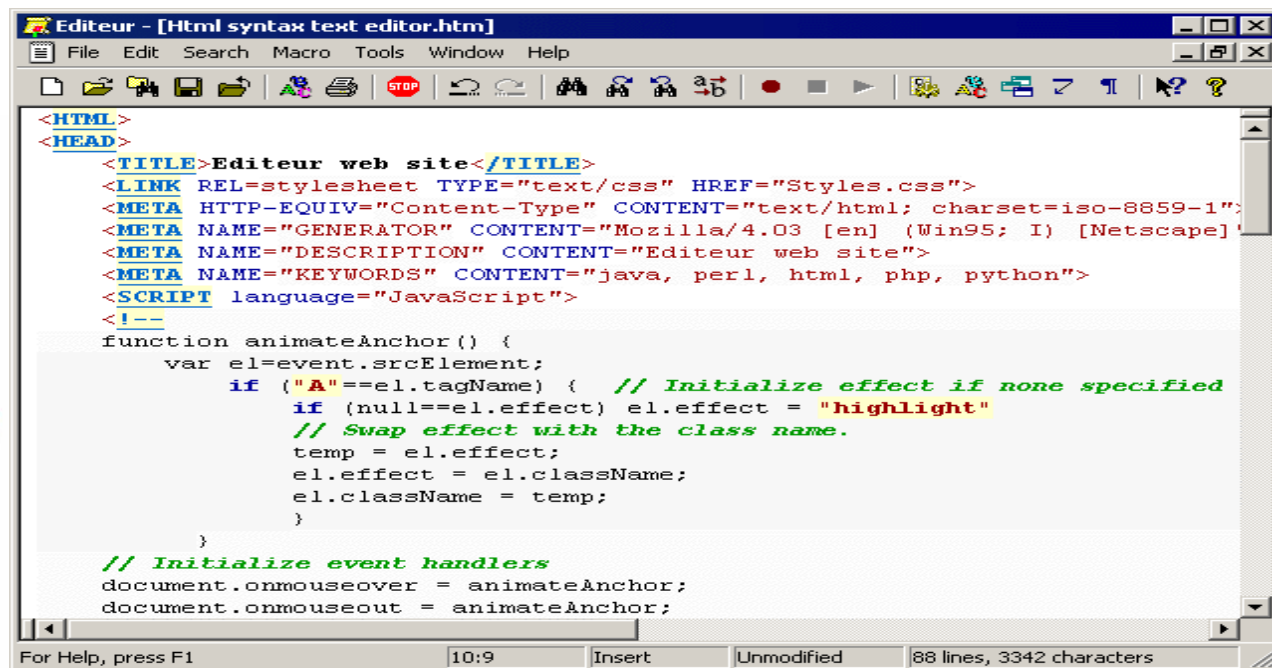


Reality Check

What's Actually Happening

Your browser doesn't know if a particular line of code originated from the site or a user

It doesn't know if the code is good or bad – it just starts at the top and reads to the bottom



```
<HTML>
<HEAD>
  <TITLE>Editeur web site</TITLE>
  <LINK REL=stylesheet TYPE="text/css" HREF="Styles.css">
  <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
  <META NAME="GENERATOR" CONTENT="Mozilla/4.03 [en] (Win95; I) [Netscape]">
  <META NAME="DESCRIPTION" CONTENT="Editeur web site">
  <META NAME="KEYWORDS" CONTENT="java, perl, html, php, python">
  <SCRIPT language="JavaScript">
    <!--
    function animateAnchor() {
      var el=event.srcElement;
      if ("A"==el.tagName) { // Initialize effect if none specified
        if (null==el.effect) el.effect = "highlight"
        // Swap effect with the class name.
        temp = el.effect;
        el.effect = el.className;
        el.className = temp;
      }
    }
    // Initialize event handlers
    document.onmouseover = animateAnchor;
    document.onmouseout = animateAnchor;
  </SCRIPT>
</HEAD>
<BODY>
  <A HREF="#">Editeur web site</A>
</BODY>
</HTML>
```



Think About Places That Let You Write

Where Can I Write On The Web?

- Search box
- Blog
- Forum
- Guest Book
- Contact Us Form
- Feedback Form
- Chat/Instant Messenger

If what you write can be rendered by a browser as executable.....



Here A Script There A Script

```
<html>
```

```
<script>good </script>
```

```
<script>good </script>
```

```
<script>bad</script>           // inserted into the site from a user
```

```
<script>good </script>
```

```
</html>
```

With user contributed content the browser doesn't know what is good or bad

It just starts at the top and runs the code on the screen until it gets to the end of the page

Who Am I??? Shonuf!!

HTTP IS STATELESS

Without URL Parameter passing and/or sessionIDs

The webserver has no idea who you are from one packet to the next



- ASPSessionID
- PHPSessionID
- JSPSessionID
- CFID/CFTOKEN



The Generic Goal of XSS

Where Can I Write On The Web?

1. The attacker will usually try to capture your sessionid
2. Send the sessionid to another server 'cross site'
3. Then use the stolen sessionid to login to a website as you

If what you write can be rendered by a browser as executable.....



Holla @ Me....

You want the presentation?????

Buy me a rum and coke or email me....

You can contact me at:

Email: joe@securitysec.com

Twitter: <http://twitter.com/j0emccray>

LinkedIn: <http://www.linkedin.com/in/joemccray>