

Forum:[Hack Forums](#)

Thread: [\[TUT\] HTMLi](#) [\[TUT\]](#)

Germans - March 29, 2012, 6:24 pm

A simple tutorial brought to you by Team Ultra Alternative with more to come

CODES

Spoiler ([Click to View](#))

This displays nothing on the screen, makes it blank:

```
<style>
body
(
display:none;
)
</style>
```

This makes the screen white, (or any other color of your choice):

```
<style>
body
(
background-color:white;
)
</style>
```

This shows a pop-up on the page and makes the background white, (you can edit Hello World but keep the quotation marks around it):

```
<script>
document.body.style.backgroundColor = "white";
alert("Hello World");
</script>
```

This redirects the page to any URL of your choice:

```
<script>
windows.location = "http://google.com";
</script>
```

You can use all these codes together, to make effects like a pop-up coming and then the redirect happening, or etc...

Credits to Unloaded and Ammar23 (Team Ultra Alternative)

Ariana Grande - March 29, 2012, 6:25 pm

The reason that it's a dead topic on HF is because most, if not all guestbooks have been patched and/or hacked. HTMLi is a very hard vulnerability to come by nowadays.

Germans - March 29, 2012, 6:29 pm

(Mar 29, 2012 06:25 PM)Ariana Grande Wrote: [\[CITE\]](#) The reason that it's a dead topic on HF is because most, if not all guestbooks have been patched and/or hacked. HTMLi is a very hard vulnerability to come by nowadays. This is true, but many websites if you have hacked the admin account, supply a place to enter data, or something and can be exploited. You are right, and finding HTMLi vulns also very often involves other hacking also. I just found an HTMLi vulnerable area the other day in the admin panel of a site.

FastFive - March 29, 2012, 6:42 pm

so what exactly is the difference between persistent xss and htmli? xss is not limited to javascript you know
if you ask me it is the same thing

good tutorial though, and these are still around but mostly as random finds. i found one of these on a chinese government site....

Germans - March 29, 2012, 7:03 pm

(Mar 29, 2012 06:42 PM)FastFive Wrote: [\[CITE\]](#) so what exactly is the difference between persistent xss and htmli? xss is not limited to javascript you know
if you ask me it is the same thing

good tutorial though, and these are still around but mostly as random finds. i found one of these on a chinese government site.... Lol, Chinese government site, well they are very similar to persistent XSS, you're right.

zer0pwn - March 29, 2012, 7:24 pm

It's unseen because people can't even tell the difference between Persistent XSS and HTMLi. People like you -facepalm-. HTMLi is injecting HTML not javascript. Using an alert would be javascript. HTML would be more like:

Code <h1> OHAIDER! </h1>

Germans - March 29, 2012, 7:29 pm

(Mar 29, 2012 07:24 PM)Zer0Pwn Wrote: [\[CITE\]](#) It's unseen because people can't even tell the difference between Persistent XSS and HTMLi. People like you -facepalm-. HTMLi is injecting HTML not javascript. Using an alert would be javascript. HTML would be more like:

Code <h1> OHAIDER! </h1> I know, with HTMLi you can also edit smaller things like adding your mark to the footer, or something else. It can be used to make smaller or insignificant changes.

live fast - March 29, 2012, 8:31 pm

(Mar 29, 2012 07:24 PM)Zer0Pwn Wrote: [\[CITE\]](#) It's unseen because people can't even tell the difference between Persistent XSS and HTMLi. People like you -facepalm-. HTMLi is injecting HTML

not javascript. Using an alert would be javascript. HTML would be more like:

Code <h1> OHAIDER! </h1>

So, if you exploit a vulnerability to use JavaScript to redirect a page, it is an XSS, but if you use HTML to redirect a page, it is considered an HTMLi?

Weird. As far as I'm concerned, the only difference between "HTMLi" and XSS is the name.

RRRoooRRR - March 29, 2012, 9:14 pm

You made a Mistake on the first box, its XSS not XXS, nice, and your not bringing HTMLi back, its always been around.

EDIT: Ooh never mind you keep referring to it as XXS, noob ?

-Chosen-

The Ion - March 29, 2012, 9:24 pm

i did only one site for html injection thats a famous actor site

Techie??? - March 29, 2012, 10:20 pm

Wow. So many noobs on HF.

http://en.wikipedia.org/wiki/Code_injection

Quote:HTML-script injection (cross-site scripting)

HTML/Script injection is a popular subject, commonly termed "Cross-Site Scripting", or "XSS". XSS refers to an injection flaw whereby user input to a web script or something along such lines is placed into the output HTML, without being checked for HTML code or scripting.

The two basic types are as follows:

Active (Type 1)

This type of XSS flaw is less dangerous, as the user input is placed into a dynamically generated page. No changes are made on the server.

Passive (Type 2)

This type is more dangerous, as the input is written to a static page, and as such, is persistent.

BeggFoMercy - March 30, 2012, 12:38 am

Dude , I seen the same pics in the same name TUT on the Web Tutorials Section , Did you copy it ?

Great Prosperity - March 30, 2012, 1:57 am

Actually a site vulnerable to HTML has the potential to be vulnerable to xss by using different vectors like <img SRC to execute JavaScript.

MaX0xf - March 30, 2012, 4:49 am

What the fuck is XXS?

Dude, seriously.

Btw, just like Techy said.

Germans - March 30, 2012, 8:53 am

(Mar 29, 2012 09:14 PM)-Chosen- Wrote: [\[CITE\]](#) You made a Mistake on the first box, its XSS not XXS, nice, and your not bringing HTMLi back, its always been around.

EDIT: Ooh never mind you keep referring to it as XXS, noob ?

-Chosen-OK, sorry it was an accident, I know what it stands for just typed it wrong. Cross (X) Site (S) Scripting (S)

Nerv - *March 30, 2012, 9:00 am*

? Good hakings freind