

Forum:[Hack Forums](#)

Thread: [XSS Challenge - tesco.com - med \(?\)](#)

Cathal - July 6, 2013, 5:17 am

I usually hate these kind of threads, but this one took me fucking ages, even though the end vector was unbelievably simple.

Here's the site: <http://www.tesco.com/>

[img]http://aspectmodding.net/cap/15d1b0853d0a0a7a77cd.png[/img]

And here's the proof:

Spoiler ([Click to View](#)) [img]http://aspectmodding.net/cap/ab5385e608443dd851de.png[/img]

Oh, pm me dem vectors.

Solvers

xXSehgalXx

cheatson

Gee4rce

PuzzuS

EDIT - ._. Easy challenge is easy.

Anarchist001 - July 6, 2013, 6:18 am

Damn, it is a dot.net site I guess..it doesnt allow <s ... hmm..very tricky..how did you solve it, I must know

xXSehgalXx - July 6, 2013, 6:53 am

Easy - Test your basic knowledge

Spoiler ([Click to View](#))

cheatson - July 6, 2013, 7:51 am

This wasn't trivial for me at all although may have reinvented the wheel for it in the end. Good challenge!

Possession - July 6, 2013, 8:01 am

What can you do with with it? Tesco is a one of the largest supermarket in the UK.

Anarchist001 - July 6, 2013, 8:34 am

Did you find it in the search function?

Cathal - July 6, 2013, 8:43 am

(Jul 6, 2013 08:34 AM)Anarchist001 Wrote: ([CITE](#)) Did you find it in the search function?
I'm sorry, didn't you say you were a pentester?

Anarchist001 - July 6, 2013, 8:51 am

yeah, did you bypass the :
dangerous request.form error
There isnt an error, but if there was no custom field.

By the url, I can see that you are in the homepage.. can u XSS the search box...or is it not possible?

Cathal - July 6, 2013, 8:54 am

(Jul 6, 2013 08:51 AM)Anarchist001 Wrote: [\[CITE\]](#) yeah, did you bypass the :
dangerous request.form error
There isnt an error, but if there was no custom field.

By the url, I can see that you are in the homepage.. can u XSS the search box...or is it not possible?

This is a challenge, mister pentester.

Anarchist001 - July 6, 2013, 9:08 am

On what browser did you do the injection?

Orph4n - July 6, 2013, 10:59 am

ah this is irking the sh!t out of me lol, I am close I think.. Im still learning this. Will post results soon as i figure it out

Gee4rce - July 6, 2013, 11:45 am

Done.

Yes i would rate this one as a medium -
finally, a Challenge wich really included some challenging part (after tons of standard
<script>alert(0)</script> search box 'challenges' which have been postet in the past)...



Thanks for the challenge!

PS.:

Ohh, there was also some sort of Redirect problem, here;

(Copy & Paste for demonstration)

Code <http://www.tesco.com/r/?from=HomePageHelp&url=//pwnyc0d3.t.gp/b00bs/>

Greetings, Gee ?

domex27 - July 6, 2013, 11:51 am

(Jul 6, 2013 11:45 AM)Gee4rce Wrote: [\[CITE\]](#) Done.

Yes i would rate this one as a medium -
finally, a Challenge wich really included some challenging part (after tons of standard
<script>alert(0)</script> search box 'challenges' which have been postet in the past)...



Thanks for the challenge!

PS.:

Ohh, there was also some sort of Redirect problem, here;

(Copy & Paste for demonstration)

Code <http://www.tesco.com/r/?from=HomePageHelp&url=//pwnyc0d3.t.gp/b00bs/>

Greetings, Gee ?n00b i dont click on site , you are n00b it a lfi?

Gee4rce - July 6, 2013, 12:06 pm

(Jul 6, 2013 11:51 AM)domex27 Wrote: [\[CITE\]](#) n00b i dont click on site , you are n00b it a lfi? lawl, you call le me a n00b :D ?!

Well if thats an LFI then go and report it - you will get amazingly tons of Ca\$\$\$\$\$h !!!! ?

"you are n00b it a lfi?"

(erm... English?)

MFFS - July 6, 2013, 12:20 pm

(Jul 6, 2013 11:45 AM)Gee4rce Wrote: [\[CITE\]](#) PS.:

Ohh, there was also some sort of Redirect problem, here;

(Copy & Paste for demonstration)

Code <http://www.tesco.com/r/?from=HomePageHelp&url=//pwnyc0d3.t.gp/b00bs/>

Greetings, Gee ?

I will never ever again click on any your link. I think i am dead.

Gee4rce - July 6, 2013, 12:25 pm

(Jul 6, 2013 12:20 PM)M4rk096 Wrote: [\[CITE\]](#) I will never ever again click on any your link. I think i am dead.

I know, it's hard - i faced "it" on the same way... i was thinking for many months allready if i should put it somewhere or not... but finally i thought my self; yes, i should - others should see it, too :D

But anyways, the redirect seems to work, it first goes to tesco.com and then to target file (no local ones).

P.S.: Sorry : 3

Cathal - July 6, 2013, 12:46 pm

(Jul 6, 2013 12:25 PM)Gee4rce Wrote: [\[CITE\]](#) I know, it's hard - i faced it on the same way... i was thinking for many months allready if i should put it somewhere or not... but finally i thought my self; yes, i should - others should see it, too :D

But anyways, the redirect seems to work, it first goes to tesco.com and then to target file (no local ones).

P.S.: Sorry : 3

Not a problem, thanks for posting :) And you wouldn't get money out of these cunts if you held them at gunpoint :'(

Gee4rce - July 6, 2013, 1:00 pm

(Jul 6, 2013 12:46 PM)MrCathal09 Wrote: [\[CITE\]](#) you wouldn't get money out of these cunts if you held them at gunpoint :'(

I know, it was just a sarcastic answer to they guy who stated that me is a noob, but at the same time stated that the redirection is an LFI ?

Milf - July 6, 2013, 1:01 pm

XSS is the most meaningless exploit you can ever find.

(Jul 6, 2013 11:45 AM)Gee4rce Wrote: [\[CITE\]](#) (Copy & Paste for demonstration)
Code <http://www.tesco.com/r/?from=HomePageHelp&url=//pwnyc0d3.t.gp/b00bs/>
Greetings, Gee ?
That wasn't funny, kid.
Low Quality Post.

Gee4rce - July 6, 2013, 1:05 pm

(Jul 6, 2013 01:01 PM)Milf Wrote: [\[CITE\]](#) XSS is the most meaningless exploit you can ever find.
False, the impact of XSS is only limited to the exploiters knowledge...

(Jul 6, 2013 01:01 PM)Milf Wrote: [\[CITE\]](#) That wasn't funny, kid.
Low Quality Post.
Common man dont be that stuffily, it was only a joke ?

Cathal - July 6, 2013, 1:09 pm

(Jul 6, 2013 01:01 PM)Milf Wrote: [\[CITE\]](#) XSS is the most meaningless exploit you can ever find.

That wasn't funny, kid.
Low Quality Post.
[img]<http://aspectmodding.net/cap/a71461fed38582fd6e26.png>[/img]
You should have expected the unexpected :)

Gee4rce - July 6, 2013, 2:45 pm

(Jul 6, 2013 01:09 PM)MrCathal09 Wrote: [\[CITE\]](#)
[img]<http://aspectmodding.net/cap/a71461fed38582fd6e26.png>[/img]
Come on bro, it's only a few years off your lifespan anyway :p
lawl, it seems Milf didn't expect the unexpected at this one ?

urez - July 6, 2013, 7:19 pm

(Jul 6, 2013 01:01 PM)Milf Wrote: [\[CITE\]](#) XSS is the most meaningless exploit you can ever find.

That wasn't funny, kid.
Low Quality Post.<http://www.securitytube.net/video/7915>
not really meaningless

Gee4rce - July 6, 2013, 7:45 pm

(Jul 6, 2013 07:19 PM)urez Wrote: [\[CITE\]](#) <http://www.securitytube.net/video/7915>
not really meaningless
Another dangerous possibility!

Nice Post
[img]<http://img856.imageshack.us/img856/6551/iyqg.png>[/img]

Greetings, Gee.

EDIT: Any more solvers? Only 3 have done it till now : 3

Mattus - July 6, 2013, 8:36 pm

God dang Gee4rce..
I just registered here and already had the shit scared out of me.. lol.

OP: I would have absolutely no idea how to even begin hacking anything lol... but goodluck to everyone in the challenge... maybe one day I will be able to give it a go :)

Gee4rce - July 6, 2013, 9:16 pm

Yes you will, just dont give up...

For the start you should check out 'google hacking', its also helps for basic understanding how the web worx

make shure that you understand HTML and a bit of JavaScript... With that then, you can start with XSS, as it varys from very easy to extrem hard..

Then comes PHP & SQLi, the next step,- theese are the most common techniques used for webh4x,
besides LFI/RFI and command execution...

This is one of HF's best Tutorial collections on Webh4x:

<https://hackforums.net/showthread.php?tid=2008347>

Greets, Gee.

Anarchist001 - July 6, 2013, 11:21 pm

I havent got the time to sit on that site a lot of time.. could someone pm me the solution

xXSehgalXx - July 7, 2013, 12:03 am

(Jul 6, 2013 11:21 PM)Anarchist001 Wrote: [\[CITE\]](#) I havent got the time to sit on that site a lot of time.. could someone pm me the solution

Check your message. Sent you a hint.

Mattus - July 7, 2013, 1:07 am

(Jul 6, 2013 09:16 PM)Gee4rce Wrote: [\[CITE\]](#) Yes you will, just dont give up...

For the start you should check out 'google hacking', its also helps for basic understanding how the web worx

make shure that you understand HTML and a bit of JavaScript... With that then, you can start with XSS, as it varys from very easy to extrem hard..

Then comes PHP & SQLi, the next step,- theese are the most common techniques used for webh4x,
besides LFI/RFI and command execution...

This is one of HF's best Tutorial collections on Webh4x:

<https://hackforums.net/showthread.php?tid=2008347>

Greets, Gee.Thank you for the support and for pointing me in the right direction mate, I'll be sure to stick to it... I'm sure when I learn a few things and get the rewarding feeling of accomplishment when something goes right it'll motivate me to hang around and learn more. :)

StarCraft 2 - July 7, 2013, 1:11 am

(Jul 6, 2013 11:45 AM)Gee4rce Wrote: [\[CITE\]](#) PS.:

Ohh, there was also some sort of Redirect problem, here;

(Copy & Paste for demonstration)

Code <http://www.tesco.com/r/?from=HomePageHelp&url=//pwnyc0d3.t.gp/b00bs/>

Greetings, Gee ?
I'll kill you man. I had on max volume...

PuzzuS - July 7, 2013, 2:27 am

Thanks a lot :3

[img]http://www.anonmgur.com/up/d710fc70d3b78eaffc7bf66c98f9b068.png[/img]

Gee4rce - July 7, 2013, 2:40 pm

(Jul 7, 2013 02:27 AM)PuzzuS Wrote: [\[CITE\]](#) Thanks a lot :3

Spoiler ([Click to View](#))

[img]http://www.anonmgur.com/up/d710fc70d3b78eaffc7bf66c98f9b068.png[/img]

Nice to see you have found the solution for it! ?

And:

(Jul 7, 2013 01:11 AM)Terran Wrote: [\[CITE\]](#) I'll kill you man. I had on max volume...

Sorry, my bad : 3

Will 033 - July 7, 2013, 4:08 pm

(Jul 7, 2013 02:27 AM)PuzzuS Wrote: [\[CITE\]](#) Thanks a lot :3

[img]http://www.anonmgur.com/up/d710fc70d3b78eaffc7bf66c98f9b068.png[/img]

Could you PM me the browser, theme and addons you're using?

Thanks :)

I might try this, I've never tried XSS before because I thought it was useless.

Gee4rce - July 7, 2013, 4:34 pm

The plugin is called "hackbar"...

And yes, XSS can be very usefull but since it's more complex to exploit, many people just rely on PoC and thats it for them... thus, they will never understand XSS above & beyond `<script>alert(1)</script>` ...

So it's good you allready took notice about the possibilities! :)

Greetings, Gee.

Will 033 - July 7, 2013, 4:52 pm

(Jul 7, 2013 04:34 PM)Gee4rce Wrote: [\[CITE\]](#) The plugin is called "hackbar"...

And yes, XSS can be very usefull but since it's more complex to exploit, many people just rely on PoC and thats it for them... thus, they will neve understand XSS above & beyond `<script>alert(1)</script>` ...

So it's good you allready took notice about the possibilities! :)

Greetings, Gee.

Ah, thanks for the name of the addon :)

Now I need to learn XSS...