



## Chat History with [WTANZ04 \(#marlena.compton/\\$64b011d3e63bfaea\)](#)

Created on 2010-06-13 18:29:35.

**2010-06-13**

**Marlena Compton:** 16:30:56  
OMG someone found the chat!!

**[Oliver Erlewein:](#)** 16:31:05  
ok in

**[Oliver Erlewein:](#)** 16:31:14  
WTF why did that work now?

**Marlena Compton:** 16:31:20  
This week's mission: Find the WTANZ04 public chat.

**[Keis:](#)** 16:31:22  
Hello, guys :)

**[Oliver Erlewein:](#)** 16:31:33  
I think we should test Skype at one of these sessions

**[Oliver Erlewein:](#)** 16:32:02  
Hi all. Excuse my frustration but as much as I love skype the group chat is....

**[Trish Khoo:](#)** 16:32:10  
ah, winner!

**Marlena Compton:** 16:32:19  
Hey Trish!

**[Trish Khoo:](#)** 16:32:34  
Hey! Finally :)

**[Ajay Balamurugadas:](#)** 16:32:37  
'm in too <ss type="smile">:)</ss> Hi All

**[Ajay Balamurugadas:](#)** 16:32:53  
<quote author="marlena.compton" conversation="#marlena.compton/\$64b011d3e63bfaea" timestamp="1276410679" authorname="Marlena Compton" guid="x3dadd6f4f65b9d508e75410645d420ba47c908d4af7c981faea8ea6e8d2ce0a2"><legacyquote>[12:01:19 PM] Marlena Compton: </legacyquote>This week's mission: Find the WTANZ04 public chat.<legacyquote>

&lt;&lt;&lt; </legacyquote></quote> LOL

**[Oliver Erlewein:](#)** 16:33:03  
LOL!

**[Trish Khoo:](#)** 16:33:09  
lol, nice

**Marlena Compton:** 16:33:48  
Talk amongst yourselves while I make sure everyone else is added and can find us.

**[Ajay Balamurugadas:](#)** 16:34:13

Most time consuming task of a tester?

**Trish Khoo:** 16:34:17

Hi all. where are we all from? I'm in Sydney

**Ajay Balamurugadas:** 16:34:22

Convincing the stakeholders?

**Oliver Erlewein:** 16:34:30

<--- Wellington NZ

**Richard R:** 16:34:34

Hi. Richard, Wellington. Banking. 5yrs. 3rd WT session this weekend ;)

**Ajay Balamurugadas:** 16:34:34

I'm from Bangalore, India

**Trish Khoo:** 16:35:02

Richard, 3rd WT session this weekend, wow! You're on a roll!

**Keis:** 16:35:10

hi! i'm from Manila, Philippines

**Oliver Erlewein:** 16:35:20

@Ajay: Convincing stakeholder's easy....

**Richard R:** 16:35:30

Yeah the 3hr session this morning at 330am was a streeeeetch

**Oliver Erlewein:** 16:35:38

@Ajay: Just don't forget to reload after the 14th shot.

**Trish Khoo:** 16:35:47

Most time consuming task of a tester - finding Skype chatrooms

**Oliver Erlewein:** 16:36:03

@Richard: Can't do WT & WC at the same time.

**Oliver Erlewein:** 16:36:14

@Richard: I'd never sleep

**Oliver Erlewein:** 16:36:36

@Keis: what's the time there?

**Trish Khoo:** 16:36:41

3.30am?!

**Richard R:** 16:36:42

@Oliver, My sleep patterns will be changed for the next 4 weeks, during WC.

**Keis:** 16:36:57

@Oliver, 2:30PM

**Oliver Erlewein:** 16:37:30

@Richard: Tomorrow 6am at FourKings for Ger vs. Aus

**Ajay Balamurugadas:** 16:37:32

Good @Richard, Ashes (Eng vs Aus) wakes me early too.

**Richard R:** 16:37:46

Wow, tempting.

**Marlena Compton:** 16:37:55  
I'm glad everyone made it :o)

**Oliver Erlewein:** 16:37:57  
Eng can't play Aus they are in separate divisions

**Marlena Compton:** 16:37:58  
:)

**Ajay Balamurugadas:** 16:38:13  
Ashes - Cricket <ss type="smile">:)</ss>

**Oliver Erlewein:** 16:38:23  
Ahhhh OK.

**Marlena Compton:** 16:38:26  
Y'all ready to start?

**Ajay Balamurugadas:** 16:38:30  
so all set for WTANZ04?

**Ajay Balamurugadas:** 16:38:31  
<ss type="smile">:)</ss>

**Richard R:** 16:38:33  
:)

**Oliver Erlewein:** 16:38:35  
Small round ball. Easy to confuse ;-)

**Ajay Balamurugadas:** 16:38:36  
yes, ready.

**Trish Khoo:** 16:38:40  
yep

**Oliver Erlewein:** 16:38:44  
Ready - Over

**Keis:** 16:38:47  
game :)

**Marlena Compton:** 16:39:02  
I have a special treat for you today. Hope you brought your bread and your wine. Wine and cheese go so well together.  
<http://jarlsberg.appspot.com/part1>

**Trish Khoo:** 16:39:12  
jarlsberg!

**Marlena Compton:** 16:39:31  
We're gonna work through Google's security testing of Jarlsberg, the cheesiest app on the web.

**Trish Khoo:** 16:39:43  
Awesome, I've had that on my to-do list for some time

**Marlena Compton:** 16:40:00  
We've been going through it at work together.

**Marlena Compton:** 16:40:04  
Has WT written all over it.

**Marlena Compton:** 16:40:09  
in cheese, even.

**Trish Khoo:** 16:40:15  
:)

**Marlena Compton:** 16:40:25  
So I thought we'd work through at our own pace for an hour and then trade notes.

**Trish Khoo:** 16:40:56  
sounds good. I need to get some music

**Marlena Compton:** 16:40:56  
Should be good for everyone to work through at their own pace.

**Marlena Compton:** 16:41:16  
So I'm gonna let y'all get started.

**Marlena Compton:** 16:42:47  
just, whatever you do, DoN't UsE a ReAl PasSwOrD

**Ajay Balamurugadas:** 16:43:29  
A session of #learning by #exploring <ss type="smile">:)</ss> Hope it turns out good.

**Ajay Balamurugadas:** 16:56:36  
<ss type="smile">:)</ss> First test completed: Result favorable. File Upload XSS

**Marlena Compton:** 16:57:49  
So everyone's in there and breaking stuff? Excuse me...exposing vulnerabilities?

**Oliver Erlewein:** 16:57:56  
yes

**Trish Khoo:** 16:58:04  
yep

**Marlena Compton:** 16:58:13  
kewl

**Keis:** 16:58:46  
hehe yeah, my room mate and i actually went thru the xss stuff before (when we had nothing else to do... just for fun). I'm revisiting :)

**Trish Khoo:** 17:00:04  
we've been doing some XSS prevention at work lately (and therefore testing of it). so this is good, learning some new tricks

**Marlena Compton:** 17:18:33  
We've got about 12 minutes left

**Marlena Compton:** 17:25:23  
5 minutes everyone.

**Marlena Compton:** 17:25:46  
I've never seen a WT chat this quiet... lol

**Keis:** 17:26:02  
hehe everyone's busy with jarlsberg

**Richard R:** 17:26:06  
shhhhh.....

**[Richard R:](#)** 17:26:19  
keep it down ;)

**Marlena Compton:** 17:26:34  
uh-oh we've got a self-appointed librarian :P

**[Richard R:](#)** 17:27:21  
lol, and there are fines in this library for noise too <ss type="cool">8-)</ss>

**[Ajay Balamurugadas:](#)** 17:27:36  
'm done playing <ss type="smile">:)</ss>

**[Richard R:](#)** 17:27:51  
Im done too. Much to learn on this site.

**[Ajay Balamurugadas:](#)** 17:28:05  
Will play more with office friends on weekdays too

**[Trish Khoo:](#)** 17:28:20  
done as well. I want to continue with it some other time though

**[Richard R:](#)** 17:28:34  
I wonder if there is a neat summary of the attacks that we could use as a reference checklist.

**[Trish Khoo:](#)** 17:28:37  
Ajay, yes me too :)

**[Trish Khoo:](#)** 17:28:47  
Richard: that would be great

**[Keis:](#)** 17:28:59  
if there isn't, we can make one :)

**[Ajay Balamurugadas:](#)** 17:29:10  
I want to pair up with a web developer and then play.

**Marlena Compton:** 17:29:12  
The Jarlsberg cheat sheet

**[Trish Khoo:](#)** 17:29:36  
I want all of my company's web developers to go through these exercises

**Marlena Compton:** 17:29:46  
So are we ready to start discussing?

**[Ajay Balamurugadas:](#)** 17:29:55  
developers or testers too? @Trish

**[Trish Khoo:](#)** 17:30:01  
testers too of course :)

**Marlena Compton:** 17:30:17  
This would be a great way to do some practive dev-test pairing

**[Ajay Balamurugadas:](#)** 17:30:22  
yes Marlena, lets start. Why is Oliver quiet <ss type="smile">:)</ss>

**Marlena Compton:** 17:30:22  
practice

**Marlena Compton:** 17:30:31

Hey Oliver...YO!

**[Trish Khoo:](#)** 17:30:33

lost in the cheese

**[Richard R:](#)** 17:30:43

haha...

**[Oliver Erlewein:](#)** 17:30:46

\*yumm\*yumm\*

**[Oliver Erlewein:](#)** 17:30:49

cheese!

**Marlena Compton:** 17:31:02

In Confluence there is a cheese macro

**[Oliver Erlewein:](#)** 17:31:05

Still chomping through some code

**[Oliver Erlewein:](#)** 17:31:14

ahhhhh cheese

**Marlena Compton:** 17:31:16

You type {cheese} into the wiki editor

**[Trish Khoo:](#)** 17:31:28

really? what does it do

**Marlena Compton:** 17:31:28

and it will display "I like cheese!"

**[Trish Khoo:](#)** 17:31:32

haha

**[Trish Khoo:](#)** 17:31:35

easter egg?

**[Oliver Erlewein:](#)** 17:31:37

@Marlena: geek

**[Oliver Erlewein:](#)** 17:32:02

I like about:robots

**Marlena Compton:** 17:32:04

What can I say. We all like the cheese.

**Marlena Compton:** 17:32:16

Ok gang.

**Marlena Compton:** 17:32:25

Let's see how far people got.

**Marlena Compton:** 17:32:36

Did anyone finish?

**[Keis:](#)** 17:32:45

tried out {cheese} as a snippet maybe there's an easter egg :)

**[Trish Khoo:](#)** 17:32:52

I only got to the end of the XSS page

**[Richard R:](#)** 17:32:59  
Same here

**[Oliver Erlewein:](#)** 17:33:01  
Yes. End of XSS

**[Trish Khoo:](#)** 17:33:15  
some of their things didn't really work for me. Maybe I needed to try in a different browser.

**[Oliver Erlewein:](#)** 17:33:22  
Started on elevation of privilege...

**Marlena Compton:** 17:33:54  
I had problems initially because I was using Chrome. Once I restarted it, I kind of got some errors

**[Ajay Balamurugadas:](#)** 17:33:54  
I did not fix any issue. just went thru each attack, tried it out.

**[Ajay Balamurugadas:](#)** 17:34:03  
Came till the privilege part.

**[Oliver Erlewein:](#)** 17:34:05  
It was all very interesting but I need about 10hrs to get through this stuff.

**[Oliver Erlewein:](#)** 17:34:09  
but very useful.

**[Trish Khoo:](#)** 17:34:12  
I would have liked it if they'd had more examples of scripts that would have actually done something evil

**[Oliver Erlewein:](#)** 17:34:18  
might just hack my project tomorrow

**Marlena Compton:** 17:34:36  
So ping if you've tested for XSS before

**[Trish Khoo:](#)** 17:34:38  
not because I want to h4x0r anything, but just because the excuse I hear a lot from devs is "yeah but that's an alert box, big deal"

**[Ajay Balamurugadas:](#)** 17:34:54  
Chrome which version Marlena. i have 5.0 and the attacks were straight forward - reproducible

**Marlena Compton:** 17:35:19  
I'm not sure, but once I re-started with the flag they suggested I started getting alerts.

**[Ajay Balamurugadas:](#)** 17:35:26  
ok

**Marlena Compton:** 17:35:31  
So no one's tested for XSS at work before?

**[Trish Khoo:](#)** 17:35:34  
I have

**[Trish Khoo:](#)** 17:35:42  
doing more or less the same thing

**[Trish Khoo:](#)** 17:35:49  
alert boxes, stealing cookies

**Oliver Erlewein:** 17:35:54  
I haven't done XSS on project but devs have. Made all the images fly across the browser

**Richard R:** 17:35:57  
I have done some at work, but not according to the plan ;)

**Oliver Erlewein:** 17:35:59  
was very funny

**Richard R:** 17:35:59  
Just out of interest

**Ajay Balamurugadas:** 17:36:07  
I did but was restricted by scripts - more of confirmation that a particular issue is fixed.

**Marlena Compton:** 17:36:14  
"not according to the plan" hahaha

**Oliver Erlewein:** 17:36:22  
and they did a successful escalation of privilege to admin

**Trish Khoo:** 17:37:02  
we had a security breach of our product last year, so I had to learn some of this stuff

**Oliver Erlewein:** 17:37:05  
We usually have external companies come in and verify.

**Trish Khoo:** 17:37:24  
we have external companies audit us as well

**Marlena Compton:** 17:37:26  
Regarding Trish's comment about devs not taking it seriously, I have a co-worker who would use cornify to piss off the devs about their stuff being vulnerable.

**Ajay Balamurugadas:** 17:37:28  
We had to look into these once security audit failed at customer end `<ss type="speechless">:|</ss>`

**Oliver Erlewein:** 17:37:30  
Need to do that because of govt. They need to be independent

**Richard R:** 17:37:31  
At the bank, we have external Pen testers

**Marlena Compton:** 17:37:45  
@Ajay ouch

**Keis:** 17:37:52  
Not officially... just played around some of the internal sites we had in the office just to try to make alerts or text pop up

**Marlena Compton:** 17:38:19  
Cornify: <http://www.cornify.com/>

**Oliver Erlewein:** 17:38:40  
i think i'll grt fluent with j=cheeses here and then start teaching my testers

**Trish Khoo:** 17:38:46  
Marlena: how did he use that?

**Trish Khoo:** 17:38:57  
oh he cornified their site :)

**Marlena Compton:** 17:39:02  
He would insert the js for cornify instead of an alert.

**Trish Khoo:** 17:39:10  
hahah nice

**Trish Khoo:** 17:39:14  
I will have to use that :D

**Ajay Balamurugadas:** 17:39:19  
so the site wud be full of images?

**Marlena Compton:** 17:39:42  
Yes, pretty unicorns and rainbows.

**Marlena Compton:** 17:39:55  
Embarrasing for some devs.

**Trish Khoo:** 17:40:22  
the excuse I then hear is "yeah but that user is only affecting their own session / account"

**Marlena Compton:** 17:40:44  
I've heard that too at my office.

**Trish Khoo:** 17:40:48  
So my mission is to find a way to affect someone else's, but in an insidious way

**Trish Khoo:** 17:40:56  
rather than just annoying alerts etc

**Ajay Balamurugadas:** 17:41:20  
can we make the other user aces the site or click the cornify button?

**Oliver Erlewein:** 17:41:29  
SQL injection is useful to show stuff that really hurts but i'm no expert

**Ajay Balamurugadas:** 17:41:29  
Then the purpose would be solved?

**Trish Khoo:** 17:41:44  
I find SQL injection is taken more seriously yes

**Keis:** 17:41:50  
not really... in a forum, the display of posts could get altered if someone posted something not properly escaped

**Marlena Compton:** 17:41:55  
@Ajay I guess that depends on the vulnerability.

**Trish Khoo:** 17:41:58  
but it's a different vulnerability

**Ajay Balamurugadas:** 17:42:40  
yes. When the customers become more aware, then the dev would take these things seriously.

**Trish Khoo:** 17:43:02  
Ajay: I imagine in that instance it would be addressed, but maybe only treated as a low priority because it doesn't look evil enough

**Marlena Compton:** 17:43:14  
Another way to look at is that the vulnerability may only exist for the user to do it to themselves, but what if their account is hacked?

**Trish Khoo:** 17:43:16  
(with my people anyway :)

**Trish Khoo:** 17:43:42  
Marlena: good point, if their account is silently hacked and these things are set up

**Marlena Compton:** 17:43:52  
So which browsers was everyone using?

**Trish Khoo:** 17:43:59  
I was using Chrome

**Ajay Balamurugadas:** 17:44:04  
Chrome 5.0 on Win XP SP3

**Richard R:** 17:44:05  
Is the jarslberg site regularly updated with new attacks? Or is it now dated?

**Richard R:** 17:44:09  
Chrome

**Oliver Erlewein:** 17:44:14  
Firefox 3.6 Mac

**Keis:** 17:44:14  
Firefox

**Marlena Compton:** 17:44:19  
It came out a few months ago

**Oliver Erlewein:** 17:44:23  
Safari 4.0.2

**Keis:** 17:44:31  
Firefox 3.6.3 on Windows

**Ajay Balamurugadas:** 17:44:43  
maybe we can have multiple sessions with someone leading the group

**Marlena Compton:** 17:44:45  
So as much as we all bitch about devs not using IE, we didn't use it either ;)

**Marlena Compton:** 17:44:58  
or, I know I complain at work about devs not using IE

**Trish Khoo:** 17:45:02  
hahaha, in retrospect I think I should have used IE

**Trish Khoo:** 17:45:07  
since it tends to be a web bug magnet ;)

**Oliver Erlewein:** 17:45:15  
Try installing IE on my mac ;-)

**Trish Khoo:** 17:45:16  
especially for client-side scripting

**Keis:** 17:45:19  
i haven't opened my IE in this laptop in ages

**Keis:** 17:45:24

:D

**Richard R:** 17:45:59  
Can any of these attacks be used outside of a web browser?

**Oliver Erlewein:** 17:46:05  
no

**Trish Khoo:** 17:46:14  
Marlena: I used to complain about them not using IE as well, then they got sick of all the IE bugs raised and started using it

**Oliver Erlewein:** 17:46:20  
i.e. only if JS & HTML gets executed

**Richard R:** 17:46:38  
what about URLs

**Richard R:** 17:46:43  
we have curl commands at work

**Oliver Erlewein:** 17:46:43  
which can be the case in Air apps or other like products

**Richard R:** 17:46:51  
can these be exploited?

**Marlena Compton:** 17:46:51  
ooo you mean using something like curl

**Marlena Compton:** 17:47:13  
Now that would be interesting.

**Oliver Erlewein:** 17:47:23  
curl cannot be used because it does not interpret code

**Trish Khoo:** 17:47:26  
that sounds pretty 1337

**Oliver Erlewein:** 17:47:41  
it only loads html.

**Oliver Erlewein:** 17:47:56  
you could use Watir though to script these things

**Oliver Erlewein:** 17:48:11  
/automate them \*note\_to\_self\_for\_monday\*

**Trish Khoo:** 17:48:35  
would Watir have an advantage over doing in manually?

**Oliver Erlewein:** 17:48:50  
with a little intelligence yes

**Oliver Erlewein:** 17:49:10  
you could tell watir to get every field off a page and start attacking each one.

**Oliver Erlewein:** 17:49:17  
would take ages manually

**Oliver Erlewein:** 17:49:24

or even crawl whole sites

**Trish Khoo:** 17:49:33  
true, how would it know if it had succeeded?

**Oliver Erlewein:** 17:49:45  
but I wouldn't suggest doing that on stuff on the internet...you leave a trail.

**Trish Khoo:** 17:49:49  
I guess it could try and save some data

**Trish Khoo:** 17:50:04  
alert box would be a pain

**Oliver Erlewein:** 17:50:07  
@Trish: Very good comment. any suggestions?

**Trish Khoo:** 17:50:39  
It could try and get session cookies

**Oliver Erlewein:** 17:50:39  
Our Watir API called H2O automagcally screenshots everything and records cookies.

**Oliver Erlewein:** 17:50:43  
(devil)

**Trish Khoo:** 17:51:06  
but that would only exploit vulnerabilities to do with session cookies

**Oliver Erlewein:** 17:51:15  
We have used Watir to try and break sessioncookies by getting it to pattern match. Didnt succeed though

**Trish Khoo:** 17:51:43  
trying to verify that every output looks as expected would be ridiculously tedious

**Oliver Erlewein:** 17:52:09  
No but e.g. if you take the pop-up you could check for that.

**Trish Khoo:** 17:52:20  
true. I don't know how good Watir's pop up handling is though

**Oliver Erlewein:** 17:52:21  
or a text on page. like "hello hacked"

**Trish Khoo:** 17:52:37  
a lot of automation tools have pretty horrible pop up handling

**Oliver Erlewein:** 17:52:39  
Popup handling is ok

**Oliver Erlewein:** 17:52:54  
...finally. Took them a while to get it though

**Trish Khoo:** 17:53:07  
yeah. I know for WatiN it was a bit flakey

**Oliver Erlewein:** 17:53:11  
Anyway back to XSS

**Marlena Compton:** 17:53:14  
yeah

**Trish Khoo:** 17:53:22  
I like your idea though Oliver

**Oliver Erlewein:** 17:53:27  
So is this part of what we usuall do

**Oliver Erlewein:** 17:53:31  
or should do?

**Marlena Compton:** 17:53:32  
so I want to hear from each person about some way they broke jarlsberg

**Marlena Compton:** 17:53:59  
@Keis let's start off with you.

**Oliver Erlewein:** 17:54:11  
I wason my way to hack the cookie that gave admin rights in the end. failed at trying to edit my own cookie :(

**Oliver Erlewein:** 17:54:20  
sorry jumped the gun

**Marlena Compton:** 17:54:35  
Hey Keis, you still there?

**Keis:** 17:54:36  
some of the usual stuff i try is i tinker with the URL to try to make it display the text i entered in the URL

**Keis:** 17:54:53  
i also try to put some alert() as my inputs

**Keis:** 17:55:05  
to try to make them appear when i load the page

**Keis:** 17:55:28  
both were part of the XSS items in jarlsberg

**Keis:** 17:55:51  
i also tried {{text}} enclosed in double braces

**Keis:** 17:56:03  
and noticed they disappeared

**Keis:** 17:56:15  
maybe that was a python thing

**Keis:** 17:56:34  
:D

**Marlena Compton:** 17:57:04  
Ajay? Anything you are particularly proud of breaking in Jarlsberg?

**Ajay Balamurugadas:** 17:57:22  
This was new. I followed each line right from <a href="http://jarlsberg.appspot.com/#0\_\_hackers">http://jarlsberg.appspot.com/#0\_\_hackers</a> to changing the privilege.

Was happy on seeing the XSS, different ways it failed.  
I also browsed through the files - the different .py files.  
In near future, I&apos;ll download the zip files and try to fix the issues on my own.

**Ajay Balamurugadas:** 17:58:03

It was a learning session for me. I plan to go through the similar session with an expert some day.

**Ajay Balamurugadas:** 17:58:37

That's it from my side. I'm happy that i did not back off but tried what I could learn today.

**Marlena Compton:** 17:59:19

Richard, what type of stuff were you able to break in Jarlsberg?

**Richard R:** 17:59:35

I worked my way through the examples.

Although i felt as though the site was controlling me, instead of the other way around.

**Richard R:** 17:59:44

So I would like to practise the examples and become confident with their meaning.

**Ajay Balamurugadas:** 18:00:10

Richard, remember me when you are practicing. We can pair-practice <ss type="smile">:)</ss>

**Richard R:** 18:00:22

True Ajay. Good idea.

**Richard R:** 18:00:23

I am most proud of getting the popup to show on mouseover and onload, although I am still uncertain about exactly what this could lead to, so have more work to do there.

**Oliver Erlewein:** 18:00:32

we could also do it at the bank.

**Richard R:** 18:00:43

Overall, it was enlightening. I have wanted to do these exercises for a few years now, but kept forgetting the name.

**Trish Khoo:** 18:00:48

I liked the mouseover one too, hadn't seen it before

**Ajay Balamurugadas:** 18:00:50

yes, forgot. The onmouseover brought a big smile on my face <ss type="smile">:)</ss>

**Marlena Compton:** 18:00:56

huh

**Marlena Compton:** 18:01:10

someone please explain the mouseover

**Richard R:** 18:01:10

Well, maybe it was another site.

**Richard R:** 18:01:17

As you said this one is new

**Richard R:** 18:01:31

The popup script is executed when the mouse passes over the link

**Oliver Erlewein:** 18:01:36

I think FF 3.6 blocked the onmouseover

**Ajay Balamurugadas:** 18:01:45

<a onmouseover="alert(1)" href="#">read this!</a>

**Trish Khoo:** 18:02:21

it's pretty cool, but does rely on someone moving their mouse over the link (rather than on page load)

**Marlena Compton:** 18:02:32

ok...I clearly have some more work to do with Jarlsberg. Probably in IE.

**Trish Khoo:** 18:02:48

but if like in the example the way of doing it on page load is blocked, it's a creative alternative

**Marlena Compton:** 18:02:52

Let's hear from Trish next. Anything you enjoyed breaking in Jarlsberg?

**Trish Khoo:** 18:03:22

I just went through the exercises too. The mouseover thing was cool, and it was interesting to see from the code why the things were breaking.

**Trish Khoo:** 18:03:30

It made it easier to think up new attacks

**Trish Khoo:** 18:04:05

But I wonder if it's a better approach to try it black-box first, then look at the code to explain the black-box results, then use the code to inspire new ideas from there

**Trish Khoo:** 18:04:15

rather than white-box all the way

**Trish Khoo:** 18:04:31

the advantage of ignorance

**Marlena Compton:** 18:04:43

Ping if you looked at the code before doing the exercises?

**Trish Khoo:** 18:04:55

I only looked at the code when the exercises told me to

**Richard R:** 18:05:09

@Marlena - what do you mean 'ping'?

**Ajay Balamurugadas:** 18:05:10

&lt;No Ping&gt; <ss type="wink">)</ss>

**Oliver Erlewein:** 18:05:23

Chuck Norris does not look at code.

**Marlena Compton:** 18:05:26

just say if you looked at the code. I can't really ask for show of hands.

**Richard R:** 18:05:50

Ah, I thought it was a special Skype thingie-ma-jingy

**Oliver Erlewein:** 18:05:56

(wave)

**Trish Khoo:** 18:05:59

someone told me "ping" is a Microsoftie term :)

**Oliver Erlewein:** 18:06:03

<--yes you can

**Marlena Compton:** 18:06:08

uh-huh

**Ajay Balamurugadas:** 18:06:14

he he <ss type="smile">:)</ss>

**Oliver Erlewein:** 18:06:17

@Trish: Ping is a command

**Oliver Erlewein:** 18:06:29

ping 192.168.1.1 <--- remember that?

**Richard R:** 18:06:34

<ss type="lipssealed">:x</ss> or <ss type="hi">(wave)</ss>

**Trish Khoo:** 18:06:34

Oliver: I mean when used in the context of "send me a text message on IM"

**Trish Khoo:** 18:06:57

"ping me with those details later"

**Marlena Compton:** 18:07:02

ok and we're back to Jarlsberg

**Marlena Compton:** 18:07:09

did you look at code: yes/no

**Marlena Compton:** 18:07:13

no

**Keis:** 18:07:14

no

**Ajay Balamurugadas:** 18:07:17

no

**Oliver Erlewein:** 18:07:17

no

**Richard R:** 18:07:18

no

**Trish Khoo:** 18:07:21

yes

**Marlena Compton:** 18:07:35

I think Trish gets a cookie for being original

**Trish Khoo:** 18:07:42

is it a cheese cookie?

**Ajay Balamurugadas:** 18:07:49

she is the expert here <ss type="smile">:)</ss>

**Trish Khoo:** 18:07:50

or a session cookie

**Marlena Compton:** 18:07:58

it's an xsrf cookie

**Trish Khoo:** 18:07:59

mmm session cookie

**Richard R:** 18:08:15

lol

**Trish Khoo:** 18:08:17  
mmm xsrf cookie

**Ajay Balamurugadas:** 18:08:35  
any similar tutorial kind of sites?

**Marlena Compton:** 18:08:46  
There's web goat, it's a bit older

**Ajay Balamurugadas:** 18:08:51  
ok.

**Marlena Compton:** 18:09:06  
Let's hear what Oliver broke :D

**Marlena Compton:** 18:09:16  
oh that didn't work :)

**Oliver Erlewein:** 18:09:27  
Well I certainly had a feeling of "Who moved my cheese".

**Marlena Compton:** 18:09:42  
Did we rock your cheese?

**Richard R:** 18:09:42  
webgoat.org???

**Oliver Erlewein:** 18:10:09  
Basically followed XSS stuff and the higher functions wouldn't do it for me

**Oliver Erlewein:** 18:10:22  
had the suspicion my browser was blocking

**Oliver Erlewein:** 18:10:30  
so i need to trial some of that.

**Oliver Erlewein:** 18:10:43  
I had Live HTTP headers running alongside

**Marlena Compton:** 18:10:50  
I found myself confused about when I was getting the right message.

**Oliver Erlewein:** 18:10:55  
and that showed a lot of interesting stuff

**Richard R:** 18:11:03  
[http://www.owasp.org/index.php/Category:OWASP\\_WebGoat\\_Project](http://www.owasp.org/index.php/Category:OWASP_WebGoat_Project)

**Ajay Balamurugadas:** 18:11:04  
nice.

**Oliver Erlewein:** 18:11:37  
I was more into the getting admin rights thing but time was up when I was trying to change my cookies

**Oliver Erlewein:** 18:11:47  
<--- now that sounded just wrong

**Marlena Compton:** 18:11:56  
well, I wasn't gonna say anything but...

**Oliver Erlewein:** 18:12:17