[20:12:07] *** weeknighttesting added Andy Glover, Sunitha Krishnappa ***

[20:12:24] weeknighttesting: Did that create a new group chat?

[20:12:59] Sunitha Krishnappa: Hello All

[20:13:09] Andy Glover: Hi

[20:13:20] weeknighttesting: aha, that seems to have worked :)

[20:13:28] Sunitha Krishnappa: :)

[20:14:01] *** weeknighttesting added Alan Richardson ***

[20:15:01] *** weeknighttesting added sharath ***

[20:16:46] weeknighttesting: Sharath, can you see that group chat here?

[20:17:00] sharath: Oh yes now I can

[20:17:03] sharath: Hello All

[20:17:09] weeknighttesting: great, the power of drag and drop!

[20:17:17] *** weeknighttesting added Jeremy Marer ***

[20:17:33] *** weeknighttesting added Daniel Prokopiwskyi ***

[20:17:45] sharath: Hi Andy how are you doing?

[20:17:58] *** weeknighttesting added Francis Balfe (SQS) ***

[20:18:48] Andy Glover: Yeah good thanks. and you?

[20:19:06] sharath: Good :)

[20:20:06] sharath: Hey Francis nice to see you here

[20:21:45] Francis Balfe (SQS): nice to be here, on the train home from work :)

[20:22:19] Jeremy Marer: That's dedication!

[20:22:27] *** weeknighttesting added chris rojohn ***

[20:22:27] Francis Balfe (SQS): I've missed too many of these. tonight's topic hooked me

[20:22:42] Andy Glover: What's the topic?

[20:23:00] Francis Balfe (SQS): I'm not sure dedication is the word I'd use

[20:23:20] sharath: The topic is -> Encourage testers to perform exploratory testing, in a security context. In so

doing they will demonstrate to themselves and the group, that they are

capable of performing a level of security related testing.

[20:23:32] sharath: Mark is the facilitator tonight

[20:23:33] Jeremy Marer: Boredom then Francis ;)

[20:23:44] sharath: He will give further details

[20:23:56] Sunitha Krishnappa: Hi all, iam a developer and this is my first weeknight testing session

[20:24:17] Andy Glover: This should be good... not done any security testing.

[20:24:24] Andy Glover: Hi Sunitha

[20:24:34] *** weeknighttesting added krishan.shyam ***

[20:24:44] Sunitha Krishnappa: Hi Andy

[20:25:00] weeknighttesting: (is franticly adding people, not ignoring folks ;)

[20:26:22] Francis Balfe (SQS): hey Sunitha, will be great to get a developer perspective

[20:26:26] sharath: I guess most of us are new to security testing

[20:26:26] Andy Glover: So strange. Spoke to Pradeep this morning and he mentioned Mark. I then checked Testing Hats web site and saw they did a bit of security testing and I thought I should get some practice doing this type of testing... and here I am!

[20:26:51] *** weeknighttesting added Oliver V. ***

[20:26:54] *** weeknighttesting added Rajesh P ***

[20:26:57] *** weeknighttesting added Mohinder Khosla ***

[20:27:15] sharath: @Andy A small world :)

[20:27:24] Andy Glover: Indeed :)

[20:27:29] Oliver V.: Hello Andy

[20:27:35] Andy Glover: Hi Oliver

[20:27:46] *** weeknighttesting added Indrek Kõnnussaar ***

[20:27:48] Mohinder Khosla: Hi everyone

[20:27:52] Andy Glover: I really must get back to you on your test.

[20:27:59] Oliver V.: I brought a friend as well :)

[20:28:02] sharath: Hello Oliver, Mohinder

[20:28:11] Oliver V.: yes, you haven't given me any feedback yet

[20:28:24] Oliver V.: I planned to use it last weekend in Peer Conference

[20:28:33] Andy Glover: @Oliver I know. Did you use it?

[20:28:47] *** weeknighttesting added Thomas Ponnet ***

[20:28:57] Oliver V.: no, we only had some local data and Anne-Marie's perception of the topic

[20:29:14] Oliver V.: it would have been maybe little too boring

[20:29:29] Thomas Ponnet: Good evening

[20:29:38] Andy Glover: Hi Thomas

[20:29:38] sharath: Good evening Thomas

[20:29:53] weeknighttesting: Good evening everyone, I *think* that all who's asked/replied are now in the chat

[20:30:16] Oliver V.: Then let's start?

[20:30:34] sharath: I do not see Oliver's friend ;)

[20:30:42] Oliver V.: Indrek is here

[20:30:47] Indrek Kõnnussaar: I'm here. Hi everyone

[20:30:50] *** weeknighttesting added Rakesh Reddy ***

[20:31:06] Andy Glover: Hi

[20:31:23] Rakesh Reddy: Hi all

[20:31:24] Thomas Ponnet: hello

[20:31:30] Alan Richardson: hi

[20:31:37] Daniel Prokopiwskyi: hi there

[20:31:53] chris rojohn: Hi

[20:31:54] krishan.shyam: hi

[20:32:16] weeknighttesting: And the clock strikes half-past!

[20:32:34] weeknighttesting: Good evening all, thanks for coming to this session on "Black Box Security Testing"

[20:33:00] weeknighttesting: With a small tweek of the URL that's been sent out we'll have access to a very insecure web application

[20:33:31] weeknighttesting: The application is on the web already, some of you may recognise it. If so that's just fine.

[20:34:04] weeknighttesting: The goal of tonight is to apply your 'regular' testing techniques to the context of security testing

[20:34:20] weeknighttesting: and then... of course explain to others hwo, what, why you did what you did

[20:34:29] weeknighttesting: Does that make sense before I roll on?

[20:34:36] Alan Richardson: yes

[20:34:37] Thomas Ponnet: yep

[20:34:37] *** weeknighttesting added Ashish Maheshwari ***

[20:34:39] Francis Balfe (SQS): yes

[20:34:44] Daniel Prokopiwskyi: yep

[20:34:50] Jeremy Marer: yup

[20:34:53] weeknighttesting: ok, I take that as a general yes :)

[20:34:53] Rajesh P: Yes

[20:34:56] chris rojohn: yes

[20:35:00] Sunitha Krishnappa: Yes

[20:35:10] weeknighttesting: http://184.175.76.222

[20:35:12] Mohinder Khosla: o far so good

[20:35:25] weeknighttesting: That's the link for where the app will be, I'll update the main link now...

[20:35:59] weeknighttesting: At the above is a document with some 'Support Tickets' in, these are 'hints' to the type of things that are insecure about the app

[20:36:16] weeknighttesting: Your call, hack if you already know how, take some hints if this is all new, it's all good either way!

[20:36:54] weeknighttesting: Just going to make the link live...

[20:37:20] weeknighttesting: http://184.175.76.222:8008/137793173/

[20:37:35] weeknighttesting: Try clicking the above... (he said holding hsi breath)

[20:37:56] Thomas Ponnet: copy paste works

[20:38:00] Daniel Prokopiwskyi: looks good

[20:38:00] Jeremy Marer: Works for me....

[20:38:06] sharath: works for me

[20:38:17] Mohinder Khosla: I am in now

[20:38:23] Ashish Maheshwari: Yes, working

[20:38:41] weeknighttesting: The application allows the following:

* You can create a User account

* Add snippets

* Edit your profile

* upload files

etc... a quick review will show you the functioanlity

[20:38:53] weeknighttesting: The question is - is anything about that insecure?

[20:39:09] weeknighttesting: The *hints* are in the document in the form of Tickets

[20:39:58] Rakesh Reddy: Brilliant "Raport software" provided by my bank for a safer web works right away - Doesn't allow me to carry on till i trust the site :)

[20:40:11] weeknighttesting: lol, good start

[20:40:18] weeknighttesting: You're free to attack the application

[20:40:33] weeknighttesting: If you find the RESET button - please do NOT click it :D

[20:40:40] sharath: The link http://184.175.76.222:8008/137793173/newaccount.gtl -> Oops! Google Chrome could not connect to 184.175.76.222:8008

[20:40:44] weeknighttesting: Please ask any questions!

[20:40:52] Francis Balfe (SQS): will be offline for 10 mins as I get in the door and set up

[20:40:54] weeknighttesting: ooh

[20:41:03] weeknighttesting: kk

[20:41:34] weeknighttesting: Note: This is a single instance, kudos for hacking your colleagues

[20:41:40] Thomas Ponnet: Are there any areas that you're particularly interested in? Is there anything that a potential customer would like to know?

[20:41:50] Rajesh P: Hi I am anot able to access the application.

[20:41:53] Rakesh Reddy: Aweee !! my un & pwd in URL

[20:42:04] Rakesh Reddy: with out any encoding :(

[20:42:14] sharath: The link http://184.175.76.222:8008/137793173/newaccount.gtl returns Oops! Google Chrome could not connect to 184.175.76.222:8008 first instance but then it starts working

[20:42:26] weeknighttesting: Ouch x 2

[20:42:32] Mohinder Khosla: I try to create an account without username/password and I am getting the message the user already exists

[20:43:38] Mohinder Khosla: Can't create an account, keep getting the message the user already exists

[20:44:07] sharath: @Rakesh nice find I see my username and password in the link :)

[20:44:13] sharath: http://184.175.76.222:8008/137793173/saveprofile?action=new&uid=test&pw=test&is_author=True

[20:44:14] Andy Glover: Just logged in as Oliver. Hope that's ok

[20:44:32] Thomas Ponnet: [20:42] weeknighttesting:

<<< Has this site been tested before and are there known bugs that we can look at?

[20:44:34] Oliver V.: I won't mind

[20:44:35] Oliver V.: really

[20:44:51] Thomas Ponnet: If there are support tickets it suggests there may be a tracking system

[20:45:08] weeknighttesting: Known bugs are in the document as Support Tickets (made up for this session to provide hints)

[20:45:23] Thomas Ponnet: ok

[20:45:27] Thomas Ponnet: Are there any others>

[20:45:36] sharath: I guess I am in the admin page now :)

[20:45:44] weeknighttesting: oi! Hacker!

[20:45:56] sharath: add /admin at the end of the link

[20:46:21] weeknighttesting: Can you paste the link?

[20:46:32] sharath: http://184.175.76.222:8008/137793173/saveprofile?action=new&uid=test&pw=test&is_author=True/admin

[20:46:37] Andy Glover: When you sign out it still displays the snippets

[20:47:59] weeknighttesting: Nice find Sharath, I have a smiliar one but not that simple

[20:48:02] Rakesh Reddy: Boom !!! connection to site list...

[20:48:02] krishan.shyam: I am getting it

[20:48:05] krishan.shyam: [Fiddler] Connection to 184.175.76.222 failed.

Exception Text: No connection could be made because the target machine actively refused it 184.175.76.222:8008

[20:48:19] Oliver V.: I think something went bang?

[20:48:23] Indrek Kõnnussaar: that was quick

[20:48:31] weeknighttesting: hehe, is it down?

[20:48:35] Oliver V.: yep

[20:48:36] Jeremy Marer: looks dead

[20:48:37] Thomas Ponnet: same here

[20:48:39] Rakesh Reddy: yep.. looks dead

[20:48:43] weeknighttesting: Ok, checking

[20:48:53] Ashish Maheshwari: yes, it is down

[20:48:56] Jeremy Marer: who dos'd it? ;)

[20:49:03] Oliver V.: now came up

[20:49:07] Oliver V.: at least for me...

[20:49:13] weeknighttesting: hmm, getting calls OK here

[20:49:42] Thomas Ponnet: site's up again

[20:49:58] weeknighttesting: that issues was out of scope :D

[20:50:03] Ashish Maheshwari: did u restart app

[20:50:12] weeknighttesting: nope, so that's interesting

[20:50:16] Jeremy Marer: dead again for me...

[20:50:18] Thomas Ponnet: same here

[20:50:27] Oliver V.: and dead

[20:50:28] krishan.shyam: not up for me

[20:50:29] Mohinder Khosla: The links has connection problems

[20:50:32] weeknighttesting: Has anyone found a file called 'secret'

[20:50:49] Daniel Prokopiwskyi: app still isn't up at this end

[20:50:55] Alan Richardson: site keeps going down

[20:51:06] weeknighttesting: ok, let me restart app

[20:51:13] sharath: The link has connection problems for me

[20:51:34] weeknighttesting: will be down for 2 minutes...

[20:51:47] Thomas Ponnet: ok

[20:52:09] Ashish Maheshwari: in which technology is this application built in?

[20:52:27] Jeremy Marer: toilet paper and blutak....

[20:52:39] weeknighttesting: Python, sat on a Win 2008 server on a VM

[20:53:13] Oliver V.: @Jeremy: and they were all out of toilet paper? :)

[20:53:30] Jeremy Marer: I think Mark used it up after lunch ;)

[20:53:48] weeknighttesting: OK, should be up now

[20:54:11] weeknighttesting: lol, I thknk the cloud needed a bit more resource

[20:54:31] Ashish Maheshwari: yes it is up

[20:55:11] weeknighttesting: So have we cracked how to become an admin then?

[20:55:40] Indrek Kõnnussaar: down for me again..

[20:55:42] Jeremy Marer: dead again... :/

[20:55:42] Ashish Maheshwari: oh no

[20:55:45] weeknighttesting: lol

[20:55:46] Ashish Maheshwari: it is down again

[20:55:52] krishan.shyam: down again yeah

[20:56:10] weeknighttesting: revert to plan B

[20:56:19] Oliver V.: current web application is not meant to handle 24 users :P

[20:56:20] Sunitha Krishnappa: down again

[20:56:22] weeknighttesting: http://google-gruyere.appspot.com/231664200656/

[20:56:26] Mohinder Khosla: Got corrupt page set up by Mark Crowther

[20:56:27] Jeremy Marer: maybe this should have been tested beforehand ;)

[20:56:39] weeknighttesting: Go to the original app - some modifications are missing but it's essentially the same

[20:57:54] Mohinder Khosla: Account created with username and password on http://google-gruyere.appspot.com/231664200656/. This sould not be allowed

[20:58:49] weeknighttesting: So anyone who HAS used Gruyere before, you'll need to be super inventive now

[20:59:42] Mohinder Khosla: Why Gruyere allow blank username created?

[21:00:32] weeknighttesting: Didn't know it did, good find

[21:01:19] Mohinder Khosla: But you can't sign in with blak username/password and no error message displayed either

[21:04:13] weeknighttesting: Currently playing with file upload

[21:04:24] Andy Glover: I can sign out and then press back and I'm automatically signed in, prob should ask me to sign back in.

[21:04:49] Rajesh P: Hi, I want to tell one point here, while creating new account there is no validation that human is trying to create account or any automated program. If any automated program attacks then there are chances whole site will be down.

[21:05:47] Francis Balfe (SQS): no validation to stop a user creating an account as "admin" which could then accidently be given priveleges

[21:06:06] Sunitha Krishnappa: i got exception when i click on upload. Then i try to reload the page its automatically signed in

[21:06:56] Alan Richardson: I think I just changed ashis's name to bob

[21:07:03] weeknighttesting: :)

[21:07:07] Francis Balfe (SQS): Just uploading a 56MB file

[21:08:55] Thomas Ponnet: I'm interested to know about the name change

[21:09:16] Alan Richardson: do a profile change yourself, it is done through a get

[21:09:26] Alan Richardson: notice that the uid is missing from the url list

[21:09:28] krishan.shyam: url input gave me admin access

[21:09:29] krishan.shyam: Referer: http://google-gruyere.appspot.com/231664200656/saveprofile?action=new&uid=shyam&pw=china&is_admin=True

Cookie: GRUYERE=75915593|shyam||admin

[21:09:31] Alan Richardson: add someone elses uid

[21:09:35] Thomas Ponnet: ah

[21:09:36] Andy Glover: I can add snippets and upload files without signing in

[21:09:36] Alan Richardson: then you are amending their account

[21:09:39] Alan Richardson: GET http://google-gruyere.appspot.com/231664200656/saveprofile?action=update&uid=ashish&name=bob&oldpw=&pw=&icon=&web_site=http%3A%2F%2Fwww.google.com&color=&private_snippet=

[21:10:34] Thomas Ponnet: Just showed that we can have two bob's, changed my username to his

[21:11:02] Thomas Ponnet: Interesting to see if bob can still log in and what snippet's they'll see then

[21:11:11] Thomas Ponnet: who's bob at the moment?

[21:12:31] Mohinder Khosla: It can let be upload and add snipplets while logged in from the previous session.

[21:13:40] weeknighttesting: I'm having a brain glitch, what's wrong with this: <script>alert('test')</script>

[21:14:07] sharath: I found this -> http://google-gruyere.appspot.com/resetbutton/123

[21:14:14] Indrek Kõnnussaar: what do you mean wrong?

[21:14:34] weeknighttesting: is it syntactically correct?

[21:14:40] Indrek Kõnnussaar: yes

[21:14:40] weeknighttesting: Trying to get it to pop

[21:14:44] weeknighttesting: hmm...

[21:15:09] Indrek Kõnnussaar: I'm guessing there are a bunch of filters there, which take out stuff like <script> etc

[21:16:04] Indrek Kõnnussaar: they probably don't work 100%. Maybe some simple obfuscation like <SCR IPT> or smth might work

[21:16:59] Thomas Ponnet: No appreciation for Shakespear: 413. That’s an error.

[21:17:09] Thomas Ponnet: Couldn't upload Hamlet as one word

[21:17:17] Thomas Ponnet: (that's good)

[21:17:50] Francis Balfe (SQS): Error: Request Entity Too Large

Your client issued a request that was too large.

[21:18:43] weeknighttesting: Ooh, poppage: http://google-gruyere.appspot.com/231664200656/%3Cscript%3Ealert%28%27test%27%29%3C/script%3E

[21:19:06] weeknighttesting: Well suggested Indrek

[21:19:26] krishan.shyam: upload got hanged after inputing many char !

[21:20:47] Thomas Ponnet: No resetting or quitting?

[21:21:29] weeknighttesting: have you found a button?

[21:21:37] Thomas Ponnet: two

[21:22:03] Thomas Ponnet: reset and quit the server

[21:22:34] weeknighttesting: nice :)

[21:23:03] sharath: uploading this as html -> <script>

alert(document.cookie);

</script>

[21:23:27] weeknighttesting: "You are not an author" - has someone hacked my account o_O

[21:23:32] Thomas Ponnet: Oy, who just stole my user?

[21:24:06] Indrek Kõnnussaar: someone reset the app I guess

[21:24:48] weeknighttesting: aha, looks like it

[21:25:03] Daniel Prokopiwskyi: really sorry guys.....

[21:25:15] weeknighttesting: Yet I'm still signed in, where is that stored then...

[21:25:27] Thomas Ponnet: xss vulnerability on snippets: <b onmouseover=alert('Wufff!')>click me! </b>

[21:25:30] Daniel Prokopiwskyi: didn't mean to click that...

[21:26:14] sharath: http://google-gruyere.appspot.com/123/<script>alert(1)</script> -> I can rest again

[21:26:21] sharath: ;)

[21:28:01] weeknighttesting: --- 5 minute warning ---

[21:28:21] sharath: adding this <a onmouseover="alert(1)" href="#">read this!</a> gives me an interesting popup

[21:31:54] weeknighttesting: Darn it, jsut as I find cookie goodness

[21:31:54] weeknighttesting: GRUYERE=131011245|MarkCrowther||author;

[21:31:57] Thomas Ponnet: Don't upload 4MB+ files. Takes ages to upload on a slow connection, worse, it works, and it then takes ages to open "My page"

[21:32:02] sharath: Found manage this server page

[21:32:08] sharath: http://google-gruyere.appspot.com/236723285654/manage.gtl

[21:32:25] sharath: Am I now the Admin ? ;)

[21:32:54] weeknighttesting: I reckon! you can now click those ebil buttons all you like!

[21:33:37] weeknighttesting: Well folks, we're at the 1 hour point and I believe it's pencils down and time to discuss

[21:35:57] weeknighttesting: First off, thanks for taking part tonight - the team and I over here at Test Hats have been looking forward to facilitating this and (allowing for the lowly VM server) it's been fun

[21:36:27] Thomas Ponnet: Was a good performance test for the server ;)

[21:36:33] weeknighttesting: AS some of you may know we're a team of 5 specialist testers out here in London and Spain, we're always looking for ways to support the community so if you have any other ideas be sure to shout!

[21:36:35] weeknighttesting: hehe true

[21:37:00] weeknighttesting: Head over to www.TestHats.com for the rest of the sales / info type stuff :)

[21:37:38] weeknighttesting: To kcik off the discussion - let me as some questions

[21:38:13] Francis Balfe (SQS): The contact Name, email address, subject input boxes extend over the About Us in FF on Ubuntu

[21:38:43] weeknighttesting: What were your thoughts going into the session?

How were you thinking of applying your 'regular' testing skills to a security contect

What did you find most challenging?

What resources did you draw on and what was your strategy?

[21:38:58] weeknighttesting: (back over to you all)

[21:40:27] Alan Richardson: I normally test web sites with a proxy server like fiddler between me and the server so I thought I'd be able to use proxy observation for seeing what was going on. That helped. Sadly I used a new proxy (ZED) which I'm not as familiar with so I found it harder to replay and amend messages than I'm used to.

[21:41:18] Alan Richardson: I should have stuck to Fiddler or Burpsuite. I wasn't expecting so many of the requests to be GETs, so I had to find a url encoder to amend the data.

[21:42:28] sharath: What were your thoughts going into the session?

I am new to security testing and though I knew some of the terminologies like sql injection, cross site scripting. Never studied or exercised them much

How were you thinking of applying your 'regular' testing skills to a security contect

I used my exploratory test approach to start with. Found a lot of bugs. But going my the session's mission. I was not sure if the stake holder would be interested in it. Started looking for resources which can help me break into the system. I did find a blue print of the web page under test

• gruyere.py is the main Gruyere web server

• data.py stores the default data in the database. There is an administrator account and two default users.

• gtl.py is the Gruyere template language

• sanitize.py is the Gruyere module used for sanitizing HTML to protect the application from security holes.

• resources/... holds all template files, images, CSS, etc.

[21:43:12] Thomas Ponnet: I started writing an ET session sheet but abandoned that as I found that the original server wasn't working and because there were just too many issues to be found. It was just plain more fun to explore than to keep track of all the bugs!

What were your thoughts going into the session?

Scared, daunting as I didn't do a lot of security testing before.

How were you thinking of applying your 'regular' testing skills to a security contect

ET approach, using the tools at my disposal, i.e. Xenu Sleuth for spidering the site and finding broken links or just any links, running Fiddler2 in the background

What did you find most challenging?

Cookies, don't know enough about them to change them effectively. The bit that Mark found I had after 5 minutes but didn't know what to do with it. That's the most common problem, missing problems due to lack of knowledge. Pairing in a future session may help here

What resources did you draw on and what was your strategy?

Resources: Previouus experience and tools mentioned above. Strategy: Explore and look what's interesting. There were too many bugs for me to go deep so I went for a shallow and wide approach.

[21:43:57] sharath: What resources did you draw on and what was your strategy?

The bible to break the webpage under test http://google-gruyere.appspot.com/part1

[21:44:04] sharath: :)

[21:44:09] Mohinder Khosla: I ran a scan with Xenu to find out the links within the website to vulenability of the links. I did not have to logon to browser the accounts. These are one available: http://google-gruyere.appspot.com/231664200656/

http://google-gruyere.appspot.com/231664200656/snippets.gtl?uid=cheddar

http://google-gruyere.appspot.com/231664200656/snippets.gtl?uid=brie

http://google-gruyere.appspot.com/231664200656/snippets.gtl?uid=MarkCrowther

http://google-gruyere.appspot.com/231664200656/lib.js

[21:44:12] Andy Glover: I haven't done any seriuos security testing befor hadnd was unsure how this was going to play out. I 'played' around with the web site, not using any tools, and found a few obvious issues, after that I was stock. Did  a bit of research and downloaded a couple of tools but not got round to understanding how to use them properly (TamperData and Cookies Manager)

[21:45:32] Oliver V.: @Andy - pretty much the same thing that happened with me...

[21:45:41] Thomas Ponnet: Mohinder: Interesting, I used Xenu as the first thing before I did anything else just to get the lay of the land

[21:46:16] Oliver V.: haven't done almost any security testing and thus got stuck pretty fast, spent most of the remaining time reading tutorial and familiarizing myself about the topic

[21:46:23] Francis Balfe (SQS): I'm in a similar boat to Andy. I used to Hotlink quite a bit back in college so I spent most of my time trying to use the url to gain access to other user's profile edit pages etc.

[21:46:49] Francis Balfe (SQS): Was able to create an accoutn called "admin". There was no Captcha (which someone had mentioned)

[21:46:59] weeknighttesting: Really good work all round- this was hard for a first time!

[21:47:13] Thomas Ponnet: If someone could explain how to use the Cookies Manager to edit the cookies, for example change "65097335|abc||author" to "65097335|abc||admin" I'd appreciate it

[21:47:25] Andy Glover: In fact, I have no idea how to launch TamperData! The Dev tools menu doesn't list it

[21:47:27] Francis Balfe (SQS): I was going to use Fiddler (using it in work for hitting REST/Web services) but using ubuntu and don't have it installed

[21:47:47] weeknighttesting: We've spent time modifiying the code and have a our own version yet 'where to begin' is the big question and you did it, Mapping the Application / Assessing Attack Surface

[21:47:49] krishan.shyam: Thanks for session ! I am running late .... see you next time ! Thanks ...

[21:48:01] weeknighttesting: Ok Krishan!

[21:48:21] Thomas Ponnet: Had Fiddler running but didn't use it much which surprised me a bit, not going with it was fine for this app imo

[21:48:26] Mohinder Khosla: The interesting thing was that you can use blank username and password to create an account but you can't sign in with those details

[21:48:33] Indrek Kõnnussaar: I've done some security before so I usually know where to look and can spot warning signs that point to something being broken. So far, the main issues with apps have been authentication and XSS, which are actually easy to test even if you're just getting started with security.

It was mostly the same here, as in, authentication issues (such as, it's possible to create an admin account with just a GET request) and some slightly more difficult XSS.

[21:49:06] weeknighttesting: How did you find that Indrek? Via the URL?

[21:49:07] Alan Richardson: Thomas - in cookie list, right click and choose edit to edit the cookie

[21:49:26] Thomas Ponnet: Indrek, agree, it was scary to see how easy it was to amend the url

[21:49:46] Thomas Ponnet: Alan, tried then but the app didn't take that and overwrote the cookie on reload

[21:50:02] Indrek Kõnnussaar: well yeah, if you create an account the url contains all the info.. the first thing to try is to replace is_author with is_admin :)

[21:50:23] Andy Glover: I can't see Indrek's comments :^)

[21:50:51] Thomas Ponnet: [21:48] Indrek Kõnnussaar:

<<< I've done some security before so I usually know where to look and can spot warning signs that point to something being broken. So far, the main issues with apps have been authentication and XSS, which are actually easy to test even if you're just getting started with security.

It was mostly the same here, as in, authentication issues (such as, it's possible to create an admin account with just a GET request) and some slightly more difficult XSS.

[21:50:53] Thomas Ponnet: [21:49] Indrek Kõnnussaar:

<<< well yeah, if you create an account the url contains all the info.. the first thing to try is to replace is_author with is_admin :)

[21:51:17] sharath: @Inder noted it. Will chk it every time from now on

[21:51:53] weeknighttesting: In every form field and at the end of urls it's stunning how often "> and ' indicate issues

[21:52:26] Indrek Kõnnussaar: But usually, all these things are sent with a POST request. For example, tested an app today where a user could change between roles and the role ID was sent with a post request, so anyone could actually modify it with Tamper Data and become an admin

[21:52:56] weeknighttesting: What other tools have we mentioned: Tamper Data, ...?

[21:53:01] Indrek Kõnnussaar: Fiddler

[21:53:13] Rakesh Reddy: Apologies for not actively participating in the session, had to take breaks in between. Firstly, I've spent sometime on Security Testing before but was long back (excuse) and as Test Hat's team mentioned most of us knowingly/unknowingly have used few of the hacking tricks (ex: testing with characters like <, % etc) during exploratory testing of web applications

Most challenging aspect for me was setting up environment with right tool like Fiddler, Tamper data, Paros or Webscraber etc can be very helpful and keeping focus on the mission Security Testing as opposed to functional testing

I've refered Owasp site (https://www.owasp.org/index.php/Main_Page) really useful

@Sharath http://google-gruyere.appspot.com/part1 - site added to bookmark

[21:53:20] Mohinder Khosla: Has anyone used Brute Force?

[21:53:54] Alan Richardson: For tools I was using ZED
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

[21:54:07] Alan Richardson: Firebug, with Firecookie

[21:54:11] Rakesh Reddy: Paros (open source) tool can also be used to tamper data

[21:54:28] Alan Richardson: although all I did with firecookie was see that an invalid session id got me logged out

[21:54:32] Thomas Ponnet: I found that TamperData or Fiddler weren't really necessary as data could be changed by amending the URL

[21:54:56] Alan Richardson: I mainly used ZED as a history so I could cut and paste urls and amend in the browser url bar

[21:55:23] Thomas Ponnet: Firebug was constantly on the page here as well, I checked some of the page elements for names and uids

[21:55:45] sharath: Is it a good idea to always get a new cookie after one tampers with the URL

[21:56:13] Indrek Kõnnussaar: what exactly do you mean?

[21:56:50] sharath: After visiting this URL http://google-gruyere.appspot.com/236723285654/saveprofile?action=update&is_admin=True&uid=username

[21:57:08] sharath: the cookies still said i was not an admin

[21:57:31] sharath: when i logged back in it logged me as an admin

[21:57:48] sharath: uid=test -> in my case

[21:57:51] Alan Richardson: I think the cookie was only set on the login get

[21:57:54] Alan Richardson: and cleared on logout

[21:58:05] Indrek Kõnnussaar: Yes.

[21:58:14] Alan Richardson: I didn't see a set cookie header on the other responses

[21:58:43] Alan Richardson: I think the cookie was mainly used in teh app for checking your session

[21:59:00] sharath: okie got it

[21:59:20] Indrek Kõnnussaar: Since the cookie contained the username too I'd assume the username was used somewhere.. but couldn't figure out where exactly.

[21:59:52] weeknighttesting: Is it how we could see our own snippets maybe

[22:01:14] Alan Richardson: I think we could have highjacked a session as the cookie was not set to httponly so if you had injected javascript as a xss that sent you the session id from the cookie then you could have used someone else's session

[22:01:46] Thomas Ponnet: Alan, I tried changing the cookie, then navigating to the Edit profile page and the app logged me out

[22:01:58] Thomas Ponnet: which is good

[22:02:33] Alan Richardson: did you amend the session id? I was trying that to see if I could get lucky with someone else's sessioni id, but they didn't come through sequentially that I could tell

[22:02:42] Indrek Kõnnussaar: no, it was a hash of something

[22:02:48] Indrek Kõnnussaar: the cookie ID

[22:02:50] Thomas Ponnet: Ah, no I didn't, see that was the part I was missing

[22:04:04] Rakesh Reddy: Alan, when cookie is hijack could cookie expiry time play any role in this context

[22:04:40] Alan Richardson: it was session based so until the person logged out, you would have their sesion

[22:04:59] Alan Richardson: the expiry time is for the browsers use

[22:07:26] Alan Richardson: seems like people are typing a lot, but I can't see any of the things being written, I think I may have encountered a skype display error

[22:07:43] Rakesh Reddy: Any one had a chance to get database name/table etc details... I tried using few SQL Injections couldn't manage to get one...

[22:08:08] Indrek Kõnnussaar: I'm slow with sql injections so I didn't even try given the time limit

[22:08:11] Francis Balfe (SQS): No, I didn't try

[22:08:25] sharath: Nope Even I tried few SQL injections could not break in :(

[22:08:42] Mohinder Khosla: Did anyone tried buffer overflow if you knew how to do it?

[22:09:00] weeknighttesting: Hmm, good points - didn't try either of thoss

[22:09:25] Indrek Kõnnussaar: python apparently isn't vulnerable to these, typically

[22:09:42] Indrek Kõnnussaar: buffer overflows, I mean.

[22:09:58] weeknighttesting: (Re - SQL Injection just been advised data is in "stored-data.txt")

[22:11:05] Thomas Ponnet: Does anyone know when an error 413 is thrown if the data is actually transmitted to the server? If it is then this is another vulnerability, you could stream the server to death

[22:12:46] Alan Richardson: :) the data is being transmitted

[22:13:04] Francis Balfe (SQS): Gotta go. I'll have a good read over the http://google-gruyere.appspot.com/part1 tomorrow and any further Skype chat when it's uploaded. Thanks

[22:13:10] Thomas Ponnet: Ah, nice! Death by Shakespear!

[22:13:15] *** Francis Balfe (SQS) has left ***

[22:13:17] Thomas Ponnet: Bye

[22:13:27] sharath: See ya

[22:13:41] weeknighttesting: OK, let me jump in with some points I wanted to share

[22:13:56] Thomas Ponnet: *Shakespeare even...

[22:15:03] weeknighttesting: What was hoped is that it could be seen competent testers can take a step towards security testing, clearly a cautious step... but as was mentioned, testing aagainst OWASP and simialr standards is not impossible with some training

[22:15:28] weeknighttesting: If you think about what's been discussed you've (collectively) followed the steps of hacking / vulnerability assessments

[22:15:56] weeknighttesting: Footprinting - what are we dealing with, Scanning / Review - learn about the system

[22:16:10] weeknighttesting: Gain access - escalate privileges

[22:16:21] weeknighttesting: then attack / demonstrate vulnerabilities

[22:16:52] weeknighttesting: so, well done! yes there's a lot to learn and that's why security is a beast unto itself but you'r half way there!

[22:17:13] Thomas Ponnet: :)

[22:17:37] Oliver V.: thanks for the evening, I understood a little bit more about this area of testing.

[22:18:01] Mohinder Khosla: Thanks for the company. Bye for now!

[22:18:10] sharath: (clap) Half way thru

[22:18:13] Thomas Ponnet: Mark, thanks a lot for setting up and hosting this evening, it was a good experience in great company!

[22:18:28] weeknighttesting: Thanks! Was good fun

[22:18:40] Andy Glover: Mark, Thanks for leading/hosting

[22:18:43] Alan Richardson: thanks Mark, g'night all

[22:18:54] sharath: Thank you so much Mark for hosting such a great session

[22:19:01] Andy Glover: Did some learning... but realised there's a lot more to learn :)

[22:19:06] Sunitha Krishnappa: Thank you all

[22:19:09] Rakesh Reddy: Thanks for organizing Mark. Very interactive session, was fun

[22:19:11] Rajesh P: Thank you all

[22:19:12] weeknighttesting: The server will stay up the rest of the week (maybe...!) so feel free to use it or Google's version of course. We ahve a few other modifications on ours but can;t distribute due to copyright

[22:19:13] Indrek Kõnnussaar: Thanks, was fun :)

[22:19:44] Thomas Ponnet: May direct my team towards that server, see what they can find, a bit disappointing that none of them showed up. Oh, well.

[22:20:01] sharath: ya thts a good idea

[22:20:05] weeknighttesting: Not to worry, was a great session - thanks for everyone coming and having a go!

[22:20:27] sharath: Thanks again MArk and every one who made it to the session. GN

[22:20:56] Rakesh Reddy: bye (wave)

[22:21:05] Mohinder Khosla: bye!

[22:21:08] Oliver V.: good evening and night to everyone, hopefully another time again

[22:21:08 | Removed 22:21:16] Andy Glover: This message has been removed.

[22:21:11] Andy Glover: bye

[22:21:15] weeknighttesting: Bye!

[22:21:20] weeknighttesting: Last plug: http://www.softwaretestingclub.com/group/securitytesting

[22:21:31] Thomas Ponnet: bye

[22:26:47] *** Rakesh Reddy has left ***

---- SESSION END ----