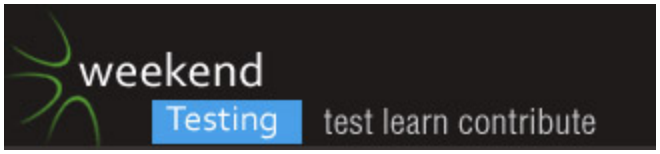

WTEU56 Session Transcript

[19/04/2015 15:45:45] Weekend Testing Europe: Hi everyone
[19/04/2015 15:45:51] Weekend Testing Europe: there are simply too many to add
[19/04/2015 15:46:16] Weekend Testing Europe: so, if additional people want to join in they can
[19/04/2015 15:46:23] Weekend Testing Europe: so lets kick this off
[19/04/2015 15:46:56] Weekend Testing Europe: Weekend Testing Europe set topic to "WTEU-56: INTRODUCTIONS"
[19/04/2015 15:47:08] Weekend Testing Europe: Tell us all a bit about yourselves!
I'm Dan Billing and I'll be facilitating today. I've been testing in the UK since 2001, working on lots of different products for the private, public and defence sectors. I currently work at New Voice Media in Basingstoke as a Test Engineer. I work in a great team of exploratory testers, who use a wide range of tools to solve their problems. I can't wait to find out what sort of tool experiences you have, and even better we get to share those with each other.
[19/04/2015 15:48:33] Teri Charles-@booksrg8: Hi everyone. I'm Teri Charles, a software tester living in Boulder, Colorado (USA). Twitter: @booksrg8
[19/04/2015 15:49:02] Christian Legget: im Christian, contract testing last few years in retail and automotive sectors. newbie to API's .enjoyed the last WTEU session on API and learnt a lot, soaked up a lot of new info..looking forward to more of the same today
[19/04/2015 15:49:19] bhagya gdm: I am Bhagya Mudiyanselage and a Tester for few years now. Working in a company named RBI at Sutton. First day at weekend testing
[19/04/2015 15:49:30] Gagan Talwar: Hi All, I am Gagan Software Tester from India. You can visit me at www.gagantalwar.com . Tw handle :- gagantalwar
[19/04/2015 15:49:35] Kadri-Annagret: I'm Kadri-Annagret Petersen. Testing software since 2005. Originally from Estonia, currently living in Sweden.
[19/04/2015 15:49:39] suma: I'm suma, was working as a UAT analyst 8 yrs back, now want to return back to testing

[19/04/2015 15:49:39] Weekend Testing Europe: Weekend Testing Europe added Elena Toropova to this conversation
[19/04/2015 15:49:43] Christian Kram: Hi, I am Christian from Wolfsburg, Germany. I'm a product owner (for 5 whole days now..) and tester for some time in the automotive area. My twitter handle is @chr_kram
[19/04/2015 15:49:44] Test Analyst: Sandeep Garg from India. Started Testing in 2006. Primarily worked in Banking, Credit Unions and Payment sectors. Twitter:@testanalystat ...This is my First day in Weekend testing
[19/04/2015 15:49:53] Toby Sinclair: I'm Toby Sinclair, @TobyTheTester on Twitter, i blog here http://tobythetesterblog.wordpress.com, Live in London, work for JP Morgan. I'm hiring testers in Glasgow and Bangalore so ping me if your interested. This morning i was lucky enough to buy some Glastonbury tickets which was cool (cool)
[19/04/2015 15:50:42] Sarah Pimentel: I'm Sarah Pimentel. Twitter: @sarahpimentel. Developing/Testing SW since 2003. Originally from Brazil, currently living in Germany.
[19/04/2015 15:51:36] Srinivas Kadiyala: Hi Everyone,
Im Srinivas Kadiyala. Software Test Engineer from India since 2012.Origin from Hyderabad. Currently Working on eCommerce solutions at @Unilog1, Mysore.
Twitter: @srinivasskc
Blog: www.testingeduindia.blogspot.in
[19/04/2015 15:52:05] Amit: Hi all, I am Amit. Testing since 2008 mostly on automation. Currently living in US
[19/04/2015 15:52:15] Weekend Testing Europe: Weekend Testing Europe added Roman Parkin to this conversation
[19/04/2015 15:52:50] Weekend Testing Europe: I also tweet @thetestdoctor and blog at http://thetestdoctor.wordpress.com
[19/04/2015 15:53:49] Roman Parkin: Call started
[19/04/2015 15:54:26] Weekend Testing Europe: If that's the introductions finished, let's talk a bit about today's topic.
[19/04/2015 15:54:38] Weekend Testing Europe: Weekend Testing Europe set topic to "WTEU-56: MISSION STATEMENT"
[19/04/2015 15:54:41] namita jain: Hi I am namita .i am in cleveland us.
[19/04/2015 15:54:56] Weekend Testing Europe: The topic for today's session is "Security Testing for APIs".

We are going to be talking about the issues and implications around security and security testing for APIs. We'll be using a vulnerable application to explore some of the ideas and thinking around it, but first we are going to discuss what we consider the main issues for security and APIs.

There appears to be quite a few of us today, more than usual, so after the initial discussion, we are going to break up into groups to explore the API under test.

After that we will come back together and find out what we discovered and share it with the group.
[19/04/2015 15:55:08] namita jain: Sorry I am getting all message bit late.
[19/04/2015 15:55:13] Weekend Testing Europe: (ignore the bit about groups)
[19/04/2015 15:55:13] Toby Sinclair: is there supposed to be a voice call?
[19/04/2015 15:55:18] Weekend Testing Europe: no, that was my cat
[19/04/2015 15:55:32] Toby Sinclair: ohhhh
[19/04/2015 15:55:34] Toby Sinclair: I've hung up
[19/04/2015 15:55:37] Roman Parkin: Call ended 1 minute 40 seconds
[19/04/2015 15:55:53] Teri Charles-@booksrg8: lol (cat)!
[19/04/2015 15:56:34] Weekend Testing Europe: Firstly, are there any of you here who currently test APIs?
[19/04/2015 15:56:44] Toby Sinclair: (y)
[19/04/2015 15:57:07] Weekend Testing Europe: excellent...would you like to chip in on any experiences Toby?
[19/04/2015 15:57:08] Gagan Talwar: Nope
[19/04/2015 15:57:20] Christian Legget: not knowingly with current project.
[19/04/2015 15:57:31] Teri Charles-@booksrg8: I've only done a little bit of API testing, would like to do a lot more.
[19/04/2015 15:57:44] Weekend Testing Europe: APIs form the back bone of a lot of modern web and mobile applications
[19/04/2015 15:57:48] Toby Sinclair: i work on a web application which uses WebAPI - http://www.asp.net/web-api
[19/04/2015 15:58:04] Toby Sinclair: Its nice, really good to work with and very testable

[19/04/2015 15:58:07] Weekend Testing Europe: we have seen their use when Amy guided us through the Songkick API
[19/04/2015 15:58:10] namita jain: Yeah not currently. But I have used soap ui and parasoft soatest and little bit green hat for api testing
[19/04/2015 15:58:17] Christian Kram: nope. never except for the songkick session.
[19/04/2015 15:58:17] Srinivas Kadiyala: Rather, i call myself test api's, i would call it as check: check the request and response using the tool.

I am new - what to test with API's
[19/04/2015 15:58:53] Weekend Testing Europe: Weekend Testing Europe added Trisha agarwal to this conversation
[19/04/2015 15:59:00] Toby Sinclair: we test a lot of our WebAPI with SpecFlow. Heres the first result from google - http://www.culbertsonexchange.com/wp/?p=293
[19/04/2015 15:59:13] bhagya gdm: The API we have is a basic which give search results. I am using Fiddler to mainly catch the responses
[19/04/2015 15:59:36] Toby Sinclair: SOAP UI and Fiddler are nice tools too
[19/04/2015 15:59:41] Weekend Testing Europe: thanks, Toby, can I share those around the team, the same question to you Teri
[19/04/2015 15:59:49] Weekend Testing Europe: via the blog?
[19/04/2015 16:00:13] Toby Sinclair: sure
[19/04/2015 16:00:23] Teri Charles-@booksrg8: I've not done much with API testing. Would like to do a lot more.
[19/04/2015 16:00:45] Teri Charles-@booksrg8: And I've not used Fiddler yet. Would like to learn that as well.
[19/04/2015 16:01:01] Weekend Testing Europe: API security testing is much like security testing for web applications
[19/04/2015 16:01:41] bhagya gdm: Can you explain a bit more please
[19/04/2015 16:01:49] Trisha agarwal: (y)
[19/04/2015 16:01:53] bhagya gdm: security testing is a bit new area for me
[19/04/2015 16:02:01] Roman Parkin: Roman Parkin has left the conversation
[19/04/2015 16:02:10] Teri Charles-@booksrg8: In what way? Unauthorized access? Login/passwords? Different user types?

[19/04/2015 16:02:26] namita jain: Yeah I have never api for security ..would like to know more
[19/04/2015 16:02:33] Weekend Testing Europe: well...the concepts that are used to do security testing are to try to exploit vulnerabilities in order to expose data, or under mine access controls
[19/04/2015 16:02:35] bhagya gdm: SQL injections and scripting
[19/04/2015 16:02:43] Weekend Testing Europe: or escalate privilege
[19/04/2015 16:03:38] Weekend Testing Europe: APIs are used by a lot of web applications to transport data, control logins, and communicate with other applications
[19/04/2015 16:03:52] Weekend Testing Europe: does anyone know who or what Moonpig are?
[19/04/2015 16:04:07] Weekend Testing Europe: the Brits amongst you should
[19/04/2015 16:04:16] bhagya gdm: yup
[19/04/2015 16:04:32] Toby Sinclair: Yup, i use Funky Pigeon though(equally crazy name)
[19/04/2015 16:04:36] Weekend Testing Europe: http://www.developer-tech.com/news/2015/jan/08/moonpigs-api-breach-could-cost-its-business/
[19/04/2015 16:04:39] Teri Charles-@booksrg8: I've heard of Moonpig. :-)
[19/04/2015 16:05:07] Teri Charles-@booksrg8: I remember reading that article.
[19/04/2015 16:05:16] Weekend Testing Europe: The issues depicted in this article were serious enough for Moonpig to shut down their public API that powered their mobile applications
[19/04/2015 16:05:28] Toby Sinclair: classic
[19/04/2015 16:05:33] Teri Charles-@booksrg8: wow
[19/04/2015 16:05:51] Weekend Testing Europe: unsuspecting users data were exposed to all, via simple enumeration of unencrypted and simple user ids
[19/04/2015 16:06:04] Weekend Testing Europe: including contact information and payment data
[19/04/2015 16:06:16] Toby Sinclair: “This fault was left unfixed for 17 months” LOL!
[19/04/2015 16:06:19] Weekend Testing Europe: yes
[19/04/2015 16:06:49] Gagan Talwar: So user data was at risk for 17 months :O
[19/04/2015 16:07:03] Weekend Testing Europe: yeah, the security researcher gave them over a year to get it fixed, and they didn't

[19/04/2015 16:07:24] Teri Charles-@booksrg8: that's crazy!
[19/04/2015 16:07:28] Weekend Testing Europe: leaving the politics and business aside, its a pretty appalling business practice to expose data like that
[19/04/2015 16:07:39] Weekend Testing Europe: and ignore advice to fix it
[19/04/2015 16:07:59] Teri Charles-@booksrg8: Amazing!
[19/04/2015 16:08:04] Trisha agarwal: any example how to test this kind of scenarios ?
[19/04/2015 16:08:08] Weekend Testing Europe: http://www.ifc0nfig.com/moonpig-vulnerability/
[19/04/2015 16:08:16] Weekend Testing Europe: here is more technical detail on the problem
[19/04/2015 16:08:34] Weekend Testing Europe: which will i hope allow us to see what the issues were and how to find them
[19/04/2015 16:09:11] Weekend Testing Europe: examine the GET request here:
[19/04/2015 16:09:22] Weekend Testing Europe: GET /rest/MoonpigRestWebservice.svc/addresses?&customerId=5379382&countryCode=9424 HTTP/1.1
Authorization: Basic aXBjiS5lOk1vb25QHjimvF58DEw
Host: api.moonpig.com
Connection: Keep-Alive
[19/04/2015 16:09:35] Weekend Testing Europe: can anyone see any initial issues with this request?
[19/04/2015 16:09:51] Gagan Talwar: Customer Id is not encrypted
[19/04/2015 16:09:56] bhagya gdm: CustomerId is not encrypted
[19/04/2015 16:10:18] Weekend Testing Europe: things that are encrypted can be decrypted, so that isn't the whole solution
[19/04/2015 16:10:21] Trisha agarwal: Customer Id , Countrycode, Host any user can see with session id (i guess aXBjiS5lOk1vb25QHjimvF58DEw)
[19/04/2015 16:10:33] Amit: Authorization is basic
[19/04/2015 16:10:37] suma: connection keep alive
[19/04/2015 16:10:55] Weekend Testing Europe: Weekend Testing Europe set topic to “WTEU-56: DISCUSSION”
[19/04/2015 16:11:25] Weekend Testing Europe: good spot Amit
[19/04/2015 16:11:49] Weekend Testing Europe: basic authorisation is simple to break....it would be better to use Oauth 1.0 or similar

[19/04/2015 16:12:21] Christian Legget: can you explain more Dan ?
[19/04/2015 16:12:25] Christian Legget: please :)
[19/04/2015 16:12:34] bhagya gdm: But does all API's use Oauth?
[19/04/2015 16:12:40] Srinivas Kadiyala: How can we get to know the GET request ?
[19/04/2015 16:13:16] Weekend Testing Europe: https://developers.google.com/identity/protocols/OAuth2
[19/04/2015 16:13:30] Weekend Testing Europe: oath is deprecated...oauth 2.0 is the right one
[19/04/2015 16:13:49] Weekend Testing Europe: its essentially an authorisation protocol that is more secure than basic authorisation
[19/04/2015 16:14:19] Weekend Testing Europe: it requires a token, which expects a valid response
[19/04/2015 16:14:52] Teri Charles-@booksrg8: Dan, would just changing that have fixed most of their issue?
[19/04/2015 16:15:10] Weekend Testing Europe: there are also methods within it I believe that prevent the use of proxies against them, such as man in the middle attacks
[19/04/2015 16:15:24] Weekend Testing Europe: potentially Teri...nothing is ever 100% secure
[19/04/2015 16:15:27] Toby Sinclair: here is a .NET Token based OAuth framework I've used with API's - http://www.asp.net/aspnet/overview/owin-and-katana/owin-oauth-20-authorization-server
[19/04/2015 16:15:33] Teri Charles-@booksrg8: True! :-)
[19/04/2015 16:16:01] Weekend Testing Europe: lets look at the response to the query that they ran at Moonpig
[19/04/2015 16:16:20] Weekend Testing Europe: GET https://api.moonpig.com/rest/MoonpigRestWebservice.svc/addresses?&customerId=713443990&countryCode=9424


```
[
  {
    "Address": "xxxxxx\r\nxxxxxxxx\r\nxxxxxxxx",
    "AddressBookId": 414628930,
    "AddressType": "CustomerAddress",
    "AddressTypeId": 1,
```

```
  "Anniversary": null,
  "Birthday": null,
  "BuildingName": null,
  "BuildingNumber": null,
  "Company": "Test",
  "Country": "United Kingdom",
  "County": "London",
  "Custom1": null,
  "Custom2": null,
  "Custom3": null,
  "Custom4": null,
  "Custom5": null,
  "CustomerId": 0,
  "Deleted": false,
  "DeliveryInstructions": null,
  "EmailAddress": null,
  "FacebookId": null,
  "FilterChar": null,
  "Firstname": "Test",
  "Greeting": null,
  "LastUpdated": "\/Date(147136045396670+0100)\/",
  "Lastname": "Test",
  "MainAddressBookId": null,
  "OtherDate": null,
  "Postcode": " LN1 3FN",
  "PostcodeSystemUpdated": null,
  "SortByLastName": false,
  "Suffix": null,
  "TelephoneNo": null,
  "Title": "",
  "TitleId": null,
  "Town": "London"
}
```

]
[19/04/2015 16:16:50] Weekend Testing Europe: So, a user could create an account, and each time the customer id was incremented
[19/04/2015 16:17:06] Weekend Testing Europe: so, an attacker could guess what a whole range of customer ids would be
[19/04/2015 16:17:13] Weekend Testing Europe: look at the content in the response here
[19/04/2015 16:17:44] Weekend Testing Europe: It contained sensitive personal information, which you wouldn't want exposed
[19/04/2015 16:18:09] Weekend Testing Europe: there is no injection, or tampering, just through poor configuration you can access anybodies data
[19/04/2015 16:18:27] Weekend Testing Europe: thankfully, they have turned this off
[19/04/2015 16:19:09] Weekend Testing Europe: In addition they had this method also:
[19/04/2015 16:19:11] Weekend Testing Europe: <ArrayOfCustomerCreditCard

xmlns="http://schemas.datacontract.org/2004/07/Moonpig.Model.CustomerAttributes.Accounting"
   xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
   <CustomerCreditCard>
      <CardType>Credit Card (Unspeci</CardType>
      <CustomerId>11466749</CustomerId>
      <ExpiryDate>12/18</ExpiryDate>
      <LastFourDigits>5993</LastFourDigits>
      <NameOnCard>Mr X XXX</NameOnCard>
      <TransactionId>5983632541-1/TransactionId>
   </CustomerCreditCard>
</ArrayOfCustomerCreditCard>
[19/04/2015 16:19:24] Weekend Testing Europe: which exposed customer payment information
[19/04/2015 16:19:27] Toby Sinclair: lol
[19/04/2015 16:20:17] Teri Charles-@booksrg8: so do these queries just try using random customer id numbers?
[19/04/2015 16:20:25] Weekend Testing Europe: again, no injection or theft of data via hacking, just poor account id management

[19/04/2015 16:20:26] Weekend Testing Europe: yes
[19/04/2015 16:20:30] Teri Charles-@booksrg8: wow!
[19/04/2015 16:20:32] Weekend Testing Europe: exactly teri
[19/04/2015 16:20:48] Weekend Testing Europe: I would think there are more examples out there like this
[19/04/2015 16:20:52] Teri Charles-@booksrg8: and even after knowing about this, they still didn't change it for a while?
[19/04/2015 16:21:04] Weekend Testing Europe: Lets dig a little deeper
[19/04/2015 16:21:31] Weekend Testing Europe: has everyone heard of Troy Hunt? those that attended my earlier security sessions may remember the name
[19/04/2015 16:21:45] Christian Legget: was it down to the communication and approach made by the security researcher Dan? (given the context of yesterdays MEWT3)
[19/04/2015 16:21:54] Trisha agarwal: how a normal user can reach to xml data ? guess from get and post method ?
[19/04/2015 16:21:54] Weekend Testing Europe: Weekend Testing Europe added Ash Winter to this conversation
[19/04/2015 16:22:43] Weekend Testing Europe: Weekend Testing Europe added Prasanna B to this conversation
[19/04/2015 16:22:59] Srinivas Kadiyala: So we can get to know, about API url if its public ?
[19/04/2015 16:23:19] Weekend Testing Europe: yes...exactly that Christian...he gave clear and concise information, a time frame and was respectful
[19/04/2015 16:23:20] Elena Toropova: Elena Toropova has left the conversation
[19/04/2015 16:23:31] Weekend Testing Europe: even after the 12 month gap...
[19/04/2015 16:23:55] Christian Legget: was it perceived as a bounty hunt/reward tho ?
[19/04/2015 16:24:04] Weekend Testing Europe: Trisha, there are a number of methods and tools to expose the xml or json
[19/04/2015 16:24:11] Toby Sinclair: you can sniff the API’s using tools such as Fiddler, Firebug etc. It’s quite interesting to watch the traffic from sites. You can very easily spot problems. Try it out on the next site you go to.
[19/04/2015 16:24:11] Weekend Testing Europe: or what ever type of data is returned
[19/04/2015 16:24:31] Trisha agarwal: Thank you
[19/04/2015 16:24:44] Weekend Testing Europe: I use a tool called The Postman

[19/04/2015 16:25:34] Weekend Testing Europe: which is run in the browser...the requests and responses can then be observed by an attacking proxy such as burp suite or zed attack proxy
[19/04/2015 16:26:33] Sandeep Garg: even if the API using the OAuth 2.0 (say), can proxies be used there as well?
[19/04/2015 16:27:03] Weekend Testing Europe: I can then use the tools inside them, such as fuzzers to submit random data to the API
[19/04/2015 16:27:13] namita jain: I have very slow network .I can't participate actively .
[19/04/2015 16:27:18] Toby Sinclair: whats an example of a fuzzer?
[19/04/2015 16:27:19] bhagya gdm: is OAuth token can be guessed or use the same again? is it random?
[19/04/2015 16:27:25] Toby Sinclair: haven’t heard that before
[19/04/2015 16:27:29] namita jain: I have also used postman
[19/04/2015 16:28:09] Weekend Testing Europe: Fuzzers are great tools
[19/04/2015 16:28:25] Weekend Testing Europe: ZAP has a built in fuzzer, as does burp
[19/04/2015 16:28:41] Weekend Testing Europe: fiddler also has a plugin called X5S, which can do fuzzing
[19/04/2015 16:29:07] Weekend Testing Europe: simply we can submit random data to any input, be it a field in a form, or a request/value in an api
[19/04/2015 16:29:24] Weekend Testing Europe: and repeat the input multiple times to see if errors are reflected back to us
[19/04/2015 16:29:29] Toby Sinclair: http://i.ytimg.com/vi/auqyJ1FisSY/hqdefault.jpg (fuzzy)
[19/04/2015 16:29:32] Toby Sinclair: lol
[19/04/2015 16:29:44] bhagya gdm: :)
[19/04/2015 16:29:46] Toby Sinclair: nice, i might look into that
[19/04/2015 16:29:51] Ash Winter: Or that you can continuously post junk to an API with no error message
[19/04/2015 16:29:54] Weekend Testing Europe: I've used them to great success
[19/04/2015 16:30:05] Ash Winter: You'd be surprised how many have no validation
[19/04/2015 16:30:08] Weekend Testing Europe: yes...with no validation :)
[19/04/2015 16:30:27] Weekend Testing Europe: thanks Ash, you are quite right...server or client side validation is very important

[19/04/2015 16:30:56] Weekend Testing Europe: if the input is invalid, ideally the API should respond with an apporpriate but not overly informative error message
[19/04/2015 16:31:03] Weekend Testing Europe: thanks Mate
[19/04/2015 16:31:13] Ash Winter: Depends how much info you want to give out
[19/04/2015 16:31:19] Ash Winter: If the API says too much
[19/04/2015 16:31:20] Toby Sinclair: “not overly informative error” TRUE!
[19/04/2015 16:31:37] Weekend Testing Europe: so...we have an hour to go, so I'd thought id get you testing one of Troy Hunt's open test applications
[19/04/2015 16:31:50] Toby Sinclair: sounds good
[19/04/2015 16:31:51] bhagya gdm: So show a less descriptive error to the user and add the detailed error to the log?
[19/04/2015 16:31:58] bhagya gdm: for debuggin purpose
[19/04/2015 16:32:16] Weekend Testing Europe: If you have an open browser...go chuck this in there:
[19/04/2015 16:32:17] Weekend Testing Europe: http://hackyourselffirst.troyhunt.com/help
[19/04/2015 16:32:31] Toby Sinclair: “add the detailed error to the log?” Thats one of the school boy errors you need to also watch out for, masking sensitive data in logs
[19/04/2015 16:32:43] Weekend Testing Europe: if you remember from previous sessions, we looked at the hack yourself first application, Supercar Showdown
[19/04/2015 16:32:56] Weekend Testing Europe: which is at hackyourselffirst.troyhunt.com
[19/04/2015 16:33:19] Teri Charles-@booksrg8: Dan, I don't think I attended those sessions.
[19/04/2015 16:33:31] bhagya gdm: hmmm.. so where does the detialed error should be recoded? nowhere?
[19/04/2015 16:33:32] Weekend Testing Europe: thats fine, the transcripts are online if you want to check them out
[19/04/2015 16:34:00] Weekend Testing Europe: there should be some logging for analysts to be able to examine
[19/04/2015 16:34:21] Weekend Testing Europe: want me to send the links later Teri?
[19/04/2015 16:34:33] Trisha agarwal: yes
[19/04/2015 16:34:33] Teri Charles-@booksrg8: Thanks, Dan. That would be great!
[19/04/2015 16:34:45] Weekend Testing Europe: I'll do it tonight or tomorrow
[19/04/2015 16:34:56] Sandeep Garg: Dan, to me too
[19/04/2015 16:34:59] Teri Charles-@booksrg8: Thanks!

[19/04/2015 16:35:12] bhagya gdm: please send those linkes to me as well Dan. Thanks!
[19/04/2015 16:35:18] Weekend Testing Europe: don't worry, they'll be on the link to this transcript and in the mailing
[19/04/2015 16:35:25] Trisha agarwal: please give us a little context as to futher move ahead in testing
[19/04/2015 16:35:36] Trisha agarwal: http://hackyourselffirst.troyhunt.com/help
[19/04/2015 16:35:37] Weekend Testing Europe: Weekend Testing Europe set topic to “WTEU-56: EXERCISE”
[19/04/2015 16:36:02] Weekend Testing Europe: SO...Troys app allows us to search for and research a number of excellent high performance vehicles
[19/04/2015 16:36:17] Weekend Testing Europe: nothing complicated, no payments or anything like that
[19/04/2015 16:37:03] Weekend Testing Europe: his app has a web front end, with a REST API in the background processing data and requests to the application
[19/04/2015 16:37:37] Weekend Testing Europe: if you look at the API schema help page, it has details of 4 api calls it can make
[19/04/2015 16:37:38] Teri Charles-@booksrg8: Dan, just to be sure I understand this site...is this for people to practice on?
[19/04/2015 16:37:40] Weekend Testing Europe: yes
[19/04/2015 16:37:45] Teri Charles-@booksrg8: :-)
[19/04/2015 16:38:21] Weekend Testing Europe: Troy cleans it up regularly, so unless you are going to try to run a Denial of Service on it, he has no objection to people accessing it
[19/04/2015 16:38:35] Teri Charles-@booksrg8: Cool
[19/04/2015 16:38:38] Weekend Testing Europe: it is linked to a Pluralsight training course which i highly recommend
[19/04/2015 16:38:42] Toby Sinclair: if you have a plurasight account you can do his course, http://www.pluralsight.com/courses/hack-your-api-first - Plurasight is a great place for learning this kind of stuff, pricey but great content
[19/04/2015 16:38:43] Weekend Testing Europe: Hack yourself first
[19/04/2015 16:38:47] Weekend Testing Europe: and hack your api first
[19/04/2015 16:38:49] Toby Sinclair: ditto
[19/04/2015 16:38:50] Weekend Testing Europe: thanks Toby
[19/04/2015 16:39:05] Weekend Testing Europe: legndary Toby, i shall also link to this

[19/04/2015 16:39:37] bhagya gdm: Thanks Tobi. Just got mydelf a account last Friday.
[19/04/2015 16:39:38] Weekend Testing Europe: it has a free trial period, and the courses only take about 4-10 hours to complete...it is TOTALLY worth it
[19/04/2015 16:40:09] Weekend Testing Europe: lets look at the first one on the list
[19/04/2015 16:40:17] Toby Sinclair: our manager just got us a load of accounts, its deifntley worth asking your work if they'll pay. I think there are corporate discounts
[19/04/2015 16:40:33] Toby Sinclair: £250 a year
[19/04/2015 16:41:09] Weekend Testing Europe: http://hackyourselffirst.troyhunt.com/api/supercar/leaderboard
[19/04/2015 16:41:48] Weekend Testing Europe: its pretty simple, it returns a list of car specs for each vehicle in the application database
[19/04/2015 16:42:40] Weekend Testing Europe: nothing especially problematic...and there is nothing especially sensitive in this request and response...but what if there was
[19/04/2015 16:42:57] Weekend Testing Europe: what would you want from an API transmitting sensitive info, that this API does not have?
[19/04/2015 16:43:18] Ash Winter: An SSL certificate?
[19/04/2015 16:43:24] Weekend Testing Europe: swee
[19/04/2015 16:43:27] Weekend Testing Europe: t
[19/04/2015 16:43:33] Weekend Testing Europe: thanks Ash...anything else?
[19/04/2015 16:43:49] Weekend Testing Europe: minimum, your apis should be using HTTPS
[19/04/2015 16:43:55] Trisha agarwal: cookies containing user login info
[19/04/2015 16:43:59] Toby Sinclair: token based authentication
[19/04/2015 16:44:07] Weekend Testing Europe: great stuff, keep it coming
[19/04/2015 16:44:19] Aleksandar Simic: http://hackyourselffirst.troyhunt.com/api/admin/users
[19/04/2015 16:44:27] Christian Legget: Dan, I ve just tweaked your url...to this...
some interesting response
http://hackyourselffirst.troyhunt.com/api/supercar/Car?=1
[19/04/2015 16:44:50] Trisha agarwal: (y)
[19/04/2015 16:44:58] Toby Sinclair: LOL!
[19/04/2015 16:45:08] Weekend Testing Europe: thanks Christian...yeah!
[19/04/2015 16:45:12] Weekend Testing Europe: the next step...

[19/04/2015 16:45:39] Weekend Testing Europe: we can see here, that not only do we get the car spec, but we can see the username, password and other sensitive info for the people that voted for the car
[19/04/2015 16:45:54] Weekend Testing Europe: bad bad BAD BAD BAD
[19/04/2015 16:45:58] Trisha agarwal: :)
[19/04/2015 16:47:15] Ash Winter: Also shows some fields are nullable, reveals metadata about your storage structure
[19/04/2015 16:47:33] Weekend Testing Europe: yep...would you like to explain that Ash? for the group
[19/04/2015 16:48:36] Ash Winter: So, you can have either empty as in ""
[19/04/2015 16:48:56] Ash Winter: or null, as in takes up no space in memory
[19/04/2015 16:49:24] Toby Sinclair: http://hackyourselffirst.troyhunt.com/api/supercar/Car?=
[19/04/2015 16:49:25] Toby Sinclair: {"Message":"The request is invalid.","MessageDetail":"The parameters dictionary contains a null entry for parameter 'id' of non-nullable type 'System.Int32' for method 'Web.ViewModels.Leaderboard Get(Int32)' in 'Web.Controllers.SupercarApiController'. An optional parameter must be a reference type, a nullable type, or be declared as an optional parameter."}
[19/04/2015 16:49:33] Ash Winter: At lot of storage is set to NULL or NOT NULL
[19/04/2015 16:49:48] Ash Winter: What he said
[19/04/2015 16:49:53] Weekend Testing Europe: I got the same message or one similar when I did this
[19/04/2015 16:50:11] Weekend Testing Europe: http://hackyourselffirst.troyhunt.com/api/supercar/Car?=2%27%20or%201=1--%27
[19/04/2015 16:50:21] Weekend Testing Europe: by attempting to sql inject the request
[19/04/2015 16:50:23] Christian Legget: would this error not be better wrapped Dan ? http://hackyourselffirst.troyhunt.com/api/supercar/Model=PLOP
[19/04/2015 16:50:31] Weekend Testing Europe: to try to expose all results
[19/04/2015 16:50:39] Christian Legget: as in not very insightful or user friendly?
[19/04/2015 16:50:52] Weekend Testing Europe: indeed...
[19/04/2015 16:51:17] Christian Legget: can you explain how this was sql request injection ?
[19/04/2015 16:51:23] Weekend Testing Europe: the id is simple to enumerate, so we could theoretically get all the user information out of requests to example the detail of each individual car

[19/04/2015 16:51:47] Weekend Testing Europe: I typed ' OR 1=1--' at the end of the request
[19/04/2015 16:51:56] Weekend Testing Europe: the browser encoded it
[19/04/2015 16:52:10] Ash Winter: Yes, use of GUIDs is quite common now
[19/04/2015 16:52:25] Ash Winter: for randomness rather than ints
[19/04/2015 16:52:41] Weekend Testing Europe: yeah...guids are long, pretty random strings used to indentify stuff
[19/04/2015 16:53:02] Weekend Testing Europe: they are hard to copy and reuse
[19/04/2015 16:53:16] Trisha agarwal: please explain a little more in brief about injections ,guids
[19/04/2015 16:53:55] Trisha agarwal: i have heard about guids for the 1st time .
[19/04/2015 16:53:59] Weekend Testing Europe: injection is just a way to pass ANY untrusted data into a system
[19/04/2015 16:54:00] Ash Winter: GUIDs are pretty universal
[19/04/2015 16:54:04] Ash Winter: something like this
[19/04/2015 16:54:06] Ash Winter: f0182227-df6d-488e-8dcc-609aee2c3b4f
[19/04/2015 16:54:17] Ash Winter: I will often use
[19/04/2015 16:54:18] Ash Winter: https://www.guidgenerator.com/online-guid-generator.aspx
[19/04/2015 16:54:22] Trisha agarwal: Thank you
[19/04/2015 16:54:27] Ash Winter: to grab a list
[19/04/2015 16:54:32] Weekend Testing Europe: everything before the car id is trusted in the request
[19/04/2015 16:54:48] Weekend Testing Europe: everything including the car id is untrusted
[19/04/2015 16:55:07] Weekend Testing Europe: if it allows untrusted data to be submitted to the request, then that is 'injection'
[19/04/2015 16:55:35] Weekend Testing Europe: If you check out the OWASP documentation on this Trisha, the explanation has more detail and is more comprehensive
[19/04/2015 16:55:45] Weekend Testing Europe: i can link to it in the transcript
[19/04/2015 16:56:03] Trisha agarwal: Sure, i will do that :) Thank you a brief explaination
[19/04/2015 16:56:41] Toby Sinclair: i need to drop, will catch up later
[19/04/2015 16:57:03] Christian Legget: dan...when you says everything is strutted in the request before the cardId ..what is the significance of this?
[19/04/2015 16:57:08] Christian Legget: *trusted
[19/04/2015 16:57:11] Weekend Testing Europe: bye Toby, thanks for your input

[19/04/2015 16:57:27] Ash Winter: There are very sneaky types of SQL injection like blind injection
[19/04/2015 16:57:30] Weekend Testing Europe: that is what the server knows and understands when it makes the request
[19/04/2015 16:57:38] Ash Winter: where you get a blank response
[19/04/2015 16:57:42] Ash Winter: but no error
[19/04/2015 16:57:48] Weekend Testing Europe: the car id could be anything...you put PLOP
[19/04/2015 16:58:11] Ash Winter: so you can guess that your able to change data in storage
[19/04/2015 16:58:50] Ash Winter: Ooo
[19/04/2015 16:58:51] Ash Winter: http://hackyourselffirst.troyhunt.com/api/supercar/Model=%22Select%20*%20from%20users%22
[19/04/2015 16:59:09] Trisha agarwal: i thought we are validating with the response of data , not changing the data in database
[19/04/2015 16:59:31] Weekend Testing Europe: You can change data with injection...
[19/04/2015 16:59:36] Weekend Testing Europe: or steal it
[19/04/2015 16:59:40] Weekend Testing Europe: or just expose it
[19/04/2015 16:59:55] Trisha agarwal: okay! That wow
[19/04/2015 17:00:05] Srinivas Kadiyala: Can we perform these on real time API's ?
[19/04/2015 17:00:13] Weekend Testing Europe: this is why as testers...we i feel
[19/04/2015 17:00:17] Srinivas Kadiyala: which are used in solutions - INJECTIONS
[19/04/2015 17:00:27] Weekend Testing Europe: need to raise our game when it comes to security
[19/04/2015 17:00:35] Weekend Testing Europe: I am not talking about penetration testing here...
[19/04/2015 17:01:00] Weekend Testing Europe: this is where a tester or hacker takes an app they don't know and tries to undermine it
[19/04/2015 17:01:09] Weekend Testing Europe: we are testers, and we know our applications intimately
[19/04/2015 17:01:35] Weekend Testing Europe: we can use that knowledge to help us with testing for security as well as functionality, performance etc
[19/04/2015 17:01:41] Trisha agarwal: exciting!

[19/04/2015 17:02:08] Weekend Testing Europe: its just that a lot of us don't do that...or that's what my perception is..
[19/04/2015 17:02:16] Sandeep Garg: Dan...our application?
[19/04/2015 17:02:27] Weekend Testing Europe: sure..whats up sandeep?
[19/04/2015 17:02:56] Sandeep Garg: the APIs are not always ours
[19/04/2015 17:03:08] bhagya gdm: Is there guide for a newbie in security testing to get the basic understanding?
[19/04/2015 17:03:13] Weekend Testing Europe: like google apis, twitter apis etc?
[19/04/2015 17:03:23] Sandeep Garg: yes
[19/04/2015 17:03:34] Weekend Testing Europe: I can share information on the basics in the transcript later :)
[19/04/2015 17:03:45] Christian Legget: (y)
[19/04/2015 17:03:52] bhagya gdm: (y)
[19/04/2015 17:03:56] Weekend Testing Europe: this is where we need to be careful...we just can't go hacking other peoples APIs
[19/04/2015 17:03:59] Trisha agarwal: that great
[19/04/2015 17:04:10] Srinivas Kadiyala: (y)
[19/04/2015 17:04:12] Weekend Testing Europe: you need to make a judgement call on each case...
[19/04/2015 17:04:18] Trisha agarwal: useful information
[19/04/2015 17:04:43] Sandeep Garg: poor or no Documentation at all have been a concern for APIs..so third party APIs integrated with your aapplication in a way
[19/04/2015 17:04:45] Weekend Testing Europe: where you are reusing openly available services, you can check up with those orgs to see what measures they take to protect data
[19/04/2015 17:04:51] Weekend Testing Europe: they would have documentation on this
[19/04/2015 17:04:55] Sandeep Garg: will also present same challenge of not knowing API very well
[19/04/2015 17:04:56] Sandeep Garg: no?
[19/04/2015 17:05:41] Weekend Testing Europe: often the API itself is documentation enough for some people
[19/04/2015 17:06:08] Trisha agarwal: one question , as mentioned i cannot perform security testing on 3rd party application , what if there is a bug which is hampering our application data too

[19/04/2015 17:06:11] Sandeep Garg: okay
[19/04/2015 17:06:44] Srinivas Kadiyala: Can we get API documentation online or we need ask for team members?
[19/04/2015 17:07:07] Weekend Testing Europe: everyone's systems are different, I can't advise on every case...BUT...I feel it is the responsibility of a business to ensure that its data is transported and managed in a secure way, and not always to rely on the work of others...
[19/04/2015 17:07:36] Weekend Testing Europe: if you use a third party, then you must do your own due diligence on that third party, their reputation and products/services
[19/04/2015 17:07:55] Trisha agarwal: Thank you
[19/04/2015 17:08:01] Ash Winter: Facebooks Graph API is a good example of API docs
[19/04/2015 17:08:04] Ash Winter: https://developers.facebook.com/docs/graph-api
[19/04/2015 17:08:18] Sandeep Garg: well said Dan about business responsibility
[19/04/2015 17:08:21] Weekend Testing Europe: Lets look at Alexander's comment earlier...
[19/04/2015 17:08:27] Weekend Testing Europe: before we wrap up
[19/04/2015 17:08:28] Weekend Testing Europe: http://hackyourselffirst.troyhunt.com/api/admin/users
[19/04/2015 17:08:36] Sandeep Garg: A good exaqmple could be https://www.youtube.com/watch?v=hdSrT4yjS1g
[19/04/2015 17:08:58] Trisha agarwal: Thank you
[19/04/2015 17:09:16] Trisha agarwal: On 19/04/2015, at 17:08, Weekend Testing Europe wrote:
> http://hackyourselffirst.troyhunt.com/api/admin/users

[19/04/2015 17:09:27] Christian Legget: Dan...http://hackyourselffirst.troyhunt.com/api/supercar/weight?=5 seems to return different results than expecting?
[19/04/2015 17:09:28] Trisha agarwal: i can see all the user senstive information
[19/04/2015 17:09:30] Weekend Testing Europe: Thanks, can I share that on the transcript please Sandeep
[19/04/2015 17:09:42] Sandeep Garg: sure
[19/04/2015 17:09:53] Weekend Testing Europe: yeah, for each one you can get a numeric user id...
[19/04/2015 17:09:58] Weekend Testing Europe: easy to guess and enumerate

[19/04/2015 17:10:10] Weekend Testing Europe: all the email addresses and passwords
[19/04/2015 17:10:19] Weekend Testing Europe: again, its a basic error
[19/04/2015 17:10:38] Weekend Testing Europe: this is simple stuff to explore before even a pen tester gets their hands on your products
[19/04/2015 17:11:10] Christian Legget: the api doesn't allow searching for 2 parameters? or is my badly constructed call?
http://hackyourselffirst.troyhunt.com/api/supercar/weight=5&Power=2
[19/04/2015 17:11:43] Weekend Testing Europe: IT DOESN'T ALLOW IT
[19/04/2015 17:11:44] Weekend Testing Europe: OOPS
[19/04/2015 17:11:46] Weekend Testing Europe: caps off
[19/04/2015 17:11:49] Weekend Testing Europe: sorry
[19/04/2015 17:11:59] Sandeep Garg: :)
[19/04/2015 17:12:10] Weekend Testing Europe: slight comms error there Christian, sorry
[19/04/2015 17:12:18] Weekend Testing Europe: :)
[19/04/2015 17:12:41] Christian Legget: ok..I've not read the documentation for the api ..so just exploring
[19/04/2015 17:12:46] Weekend Testing Europe: thats great...
[19/04/2015 17:12:54] Weekend Testing Europe: no need to apologise...were here to explore
[19/04/2015 17:13:19] Weekend Testing Europe: this is just a primer for your own learning guys, so please go forward and do other learning from this...
[19/04/2015 17:13:38] Weekend Testing Europe: do the course we recommended, or explore public api's safely
[19/04/2015 17:13:54] Weekend Testing Europe: or practise on work ones you have permission to test on
[19/04/2015 17:14:13] Sandeep Garg: right Dan
[19/04/2015 17:14:39] Srinivas Kadiyala: is there any place to get public api's ?
[19/04/2015 17:14:43] Weekend Testing Europe: can anyone spot an nice easy thing that might cause a problem...?
[19/04/2015 17:14:51] Weekend Testing Europe: in this users request?
[19/04/2015 17:15:46] Sandeep Garg: Dan I would like to share one more link which is very concisely written by Ole Lensmar http://tinyurl.com/kycdthz
[19/04/2015 17:16:01] Weekend Testing Europe: there have been a few shared already Srinivas, I'll collate and circulate them

[19/04/2015 17:16:03] Sandeep Garg: You can use it on TRanscript if you wishh to
[19/04/2015 17:16:39] Srinivas Kadiyala: Thanks
[19/04/2015 17:16:40] Weekend Testing Europe: yes, i have started a Pinterest board...and this is on it...
[19/04/2015 17:16:44] Weekend Testing Europe: hold on, someone at the door
[19/04/2015 17:16:55] Amit: Srinivas, you can a get a plenty through google - http://www.programmableweb.com/apis/directory
[19/04/2015 17:16:56] Amit: http://www.publicapis.com/
[19/04/2015 17:17:04] Trisha agarwal: On 19/04/2015, at 17:14, Weekend Testing Europe wrote:
> can anyone spot an nice easy thing that might cause a problem...?
in this users request?
I didnt got after changing the url with different param
[19/04/2015 17:17:59] Sandeep Garg: hmm
[19/04/2015 17:18:24] Srinivas Kadiyala: Thanks Amit.
[19/04/2015 17:18:56] Aleksandar Simic: passwords are not protected?
[19/04/2015 17:19:06] Trisha agarwal: This message has been removed.
[19/04/2015 17:19:36] Trisha agarwal: Admin information
[19/04/2015 17:20:43] Sandeep Garg: Trisha...share the link pls
[19/04/2015 17:21:52] Christian Legget: Dan, when it comes back with this message.. off this call...is it a prompt or just a standard message? http://hackyourselffirst.troyhunt.com/api/vote
[19/04/2015 17:22:35] Sandeep Garg: okay got it
[19/04/2015 17:23:07] Ash Winter: Vote is a POST, your browser does a GET
[19/04/2015 17:23:17] Ash Winter: http request wise I mean
[19/04/2015 17:23:28] Ash Winter: Is Dan OK?
[19/04/2015 17:23:39] Ash Winter: I wonder who's at the door?
[19/04/2015 17:23:42] Christian Legget: ah..makes sense ..thanks Ash...
[19/04/2015 17:24:00] Sandeep Garg: paassword is not encrypted - yes, Admin Informatiion @ Trisha - can u explain
[19/04/2015 17:24:00] Sandeep Garg: ?
[19/04/2015 17:24:14] Weekend Testing Europe: hi there
[19/04/2015 17:24:16] Weekend Testing Europe: sorry
[19/04/2015 17:24:21] Trisha agarwal: IsAdmin =null

[19/04/2015 17:24:27] Weekend Testing Europe: my neighbour was at the door
[19/04/2015 17:24:32] Trisha agarwal: i meant , sorry if i confused
[19/04/2015 17:24:50] Ash Winter: Cup of sugar? :)
[19/04/2015 17:25:00] Weekend Testing Europe: no, he's doing some gardening for us
[19/04/2015 17:25:08] Weekend Testing Europe: anyway...someone spotted it
[19/04/2015 17:25:19] Weekend Testing Europe: it also suggested if the user was an admin or not
[19/04/2015 17:25:28] Trisha agarwal: yes
[19/04/2015 17:25:48] Weekend Testing Europe: we could then, craft a user admin login with the login request to say IsAdmin: true or whatever
[19/04/2015 17:25:54] Weekend Testing Europe: to create our own admin users
[19/04/2015 17:26:09] Weekend Testing Europe: that is an example of escalation of privilege
[19/04/2015 17:26:37] Sandeep Garg: cool
[19/04/2015 17:26:38] Teri Charles-@booksrg8: It's amazing all of the bad stuff people can do!
[19/04/2015 17:26:47] Weekend Testing Europe: the VOTE request is a POST, not a GET
[19/04/2015 17:26:53] Sandeep Garg: @trisha - good one :)
[19/04/2015 17:27:02] Trisha agarwal: Thank you
[19/04/2015 17:27:13] Christian Legget: Dan..can you recap this isAdmin thing...not following it 100%
[19/04/2015 17:27:42] Weekend Testing Europe: so, here you can use a tool like Fiddler, firebug, or the Postman to pass in multiple votes for a car, but the UI only allows one vote per user per car
[19/04/2015 17:27:52] Weekend Testing Europe: ok, Chris...
[19/04/2015 17:27:52] Weekend Testing Europe: here goes
[19/04/2015 17:28:40] Weekend Testing Europe: when you create a standard user, it gets created here http://hackyourselffirst.troyhunt.com/Account/Register
[19/04/2015 17:29:12] Weekend Testing Europe: as you can see, it does not allow you to set if they are an admin user or not at this point
[19/04/2015 17:30:47] Weekend Testing Europe: you can monitor the traffic using dev tools or fiddler
[19/04/2015 17:30:52] Sandeep Garg: right...i just created with userid 59084

[19/04/2015 17:32:46] Weekend Testing Europe: it creates a whole load of stuff, including some juicy cookies
[19/04/2015 17:33:07] Weekend Testing Europe: that straying into web security, not api...so not relevant here
[19/04/2015 17:33:14] Aleksandar Simic: @dan would you intercept and modify request?
[19/04/2015 17:34:06] Weekend Testing Europe: you could, but that's not my focus here
[19/04/2015 17:34:07] Christian Legget: ok, so can see the user.. I hadn't twigged the api showed these ...discretely..http://hackyourselffirst.troyhunt.com/api/admin/users
[19/04/2015 17:35:41] Weekend Testing Europe: when you login, it makes a call to the Login part of the API
[19/04/2015 17:36:30] Weekend Testing Europe: My user is isAdmin: Null
[19/04/2015 17:36:35] Weekend Testing Europe: can anyone verify that
[19/04/2015 17:36:36] Weekend Testing Europe: ?
[19/04/2015 17:37:28] Trisha agarwal: yes , sandeep have created a new login as userid "UserId":59086,
[19/04/2015 17:37:35] Sandeep Garg: yes
[19/04/2015 17:37:35] Trisha agarwal: and its null
[19/04/2015 17:37:36] Sandeep Garg: "UserId": 59085,
"Email": "dan.test@test.com",
"FirstName": "Dan",
"LastName": "Test",
"IsAdmin": null,
"Password": "test1234"
[19/04/2015 17:37:41] Weekend Testing Europe: yeah...
[19/04/2015 17:37:44] Weekend Testing Europe: thanks Sandeep
[19/04/2015 17:39:28] Sandeep Garg: but when you created user, Request didn't contaain that isAdmin param at all..and you are not intercepting it...
[19/04/2015 17:39:59] Sandeep Garg: then in order to exploit the Escalation Privilege vulnarability
[19/04/2015 17:40:05] Sandeep Garg: what is the catch?
[19/04/2015 17:40:21] Weekend Testing Europe: I am going to try to modify my login post
[19/04/2015 17:40:26] Weekend Testing Europe: using The Postman
[19/04/2015 17:40:34] Weekend Testing Europe: to login as an admin, with a standard user

[19/04/2015 17:41:23] Weekend Testing Europe: I am just crafting the request now, I should have done it sooner...I apologise
[19/04/2015 17:41:31] Sandeep Garg: okay
[19/04/2015 17:41:46] Weekend Testing Europe: try it out yourself if you want
[19/04/2015 17:42:07] Trisha agarwal: okay , will create a new onces
[19/04/2015 17:43:12] Weekend Testing Europe: The Postman is great ...it can be used for testing for functionality and security
[19/04/2015 17:43:26] Weekend Testing Europe: but it does not store requests across machines :(
[19/04/2015 17:44:00] Trisha agarwal: yes , that will be a problem for us too create a new account as admin user
[19/04/2015 17:47:36] Weekend Testing Europe: I am having some difficulty with this at the moment, so I suggest trying yourself at some point
[19/04/2015 17:47:38] Weekend Testing Europe: BUT
[19/04/2015 17:47:43] Weekend Testing Europe: I can do this...
[19/04/2015 17:47:51] Weekend Testing Europe: if you go to the website and select a car
[19/04/2015 17:48:03] Trisha agarwal: Okay
[19/04/2015 17:48:04] Weekend Testing Europe: find me a car id for a car you really like
[19/04/2015 17:48:15] Christian Legget: i voted for the LFa for you..
http://hackyourselffirst.troyhunt.com/api/supercar/weight?=10
[19/04/2015 17:48:18] Weekend Testing Europe: and vote for it, if you have created a user
[19/04/2015 17:48:35] Weekend Testing Europe: do you notice that you cannot vote for that again via the UI
[19/04/2015 17:49:44] Trisha agarwal:
http://hackyourselffirst.troyhunt.com/api/supercar/SupercarId?=1
[19/04/2015 17:50:41] Christian Legget: yes, can vote for other cars but see what you mean dan...how does one get crafty through the api?
[19/04/2015 17:51:29] Teri Charles-@booksrg8: Dan, I have to leave. Thanks for this. You have given me much to think about and learn!
[19/04/2015 17:51:34] Weekend Testing Europe: ok, so i have examined the request
[19/04/2015 17:51:37] Weekend Testing Europe: via firebug
[19/04/2015 17:51:40] Weekend Testing Europe: or chrome tools
[19/04/2015 17:51:51] Weekend Testing Europe: Bye Teri..thanks for your input as always :)

[19/04/2015 17:52:01] Teri Charles-@booksrg8: Awesome session!
[19/04/2015 17:52:08] Trisha agarwal: can you explain , how to examine using firebug as i too have
[19/04/2015 17:52:26] Trisha agarwal: Yes intresting session to learn !
[19/04/2015 17:52:34] Weekend Testing Europe: in the Network tab, you can see the traffic of the vote request
[19/04/2015 17:52:39] namita jain: Thanks a lot ...
[19/04/2015 17:52:45] Trisha agarwal: okay
[19/04/2015 17:53:09] Sandeep Garg: yeah...
[19/04/2015 17:53:44] Sandeep Garg: I need to work on Fiddler
[19/04/2015 17:54:32] Trisha agarwal: muntiple get request are there , i guess we should consider the first one ?
[19/04/2015 17:54:50] Sandeep Garg: scroll up a bit
[19/04/2015 17:55:02] Sandeep Garg: you should be able to see the vote
[19/04/2015 17:55:12] Weekend Testing Europe: it is easier in Fiddler by a mile
[19/04/2015 17:55:36] Weekend Testing Europe: inside fiddler, you can circumvent the UI
[19/04/2015 17:55:46] Weekend Testing Europe: find the request for api/vote
[19/04/2015 17:55:59] Weekend Testing Europe: amend the comment, or the supercar id, or even the user id
[19/04/2015 17:56:05] Weekend Testing Europe: so you could do
[19/04/2015 17:56:12] Weekend Testing Europe: 1) pretend to be someone you are not
[19/04/2015 17:56:21] Weekend Testing Europe: and vote using their id
[19/04/2015 17:56:35] Weekend Testing Europe: 2) vote for as many cars as you like
[19/04/2015 17:56:36] Gagan Talwar: Sorry Guys need to leave. Have a good day
[19/04/2015 17:56:44] Weekend Testing Europe: 3) vote as many times as you want
[19/04/2015 17:56:48] Gagan Talwar: Gagan Talwar has left the conversation
[19/04/2015 17:56:50] Weekend Testing Europe: take care Gagan
[19/04/2015 17:57:34] Weekend Testing Europe: look at the Agera
[19/04/2015 17:57:39] Weekend Testing Europe: supercar number 5
[19/04/2015 17:57:45] Weekend Testing Europe: how many times have i voted for it?
[19/04/2015 17:57:51] Trisha agarwal: which URL we need to have in address bar as you mentioned we can do for car id , i am using the URL http://hackyourselffirst.troyhunt.com/api/supercar/SupercarId?=1

[19/04/2015 17:58:15] Weekend Testing Europe: thats the one!
[19/04/2015 17:58:21] Weekend Testing Europe: try it for 5 trisha
[19/04/2015 17:58:28] Weekend Testing Europe: how many times have I voted
[19/04/2015 17:58:29] Weekend Testing Europe: ?
[19/04/2015 17:58:55] Trisha agarwal: 5 times i can see your votes(al votes)
[19/04/2015 17:58:56] Sandeep Garg: 2
[19/04/2015 17:59:02] Weekend Testing Europe: right sandeep
[19/04/2015 17:59:04] Weekend Testing Europe: :)
[19/04/2015 18:00:19] Christian Legget: two comments.. Test and test1 :)
[19/04/2015 18:00:29] Trisha agarwal: ii still didnt get using get in network tab how can i change my previliges in firebug (as you mentioned fiddler is easy but i have to download it my computer)
[19/04/2015 18:01:26] Weekend Testing Europe: don't worry Trisha
[19/04/2015 18:01:36] Weekend Testing Europe: look at supercar 5 via the website
[19/04/2015 18:01:49] Trisha agarwal: http://hackyourselffirst.troyhunt.com/api/supercar/SupercarId?=5
[19/04/2015 18:01:56] Weekend Testing Europe: how many times has 'testing days' voted for the Agera?
[19/04/2015 18:01:57] Trisha agarwal: yes, i am there
[19/04/2015 18:02:34] Weekend Testing Europe: Anyone found it?
[19/04/2015 18:02:40] bhagya gdm: 3
[19/04/2015 18:02:43] Sandeep Garg: 3
[19/04/2015 18:02:43] Weekend Testing Europe: great stuff
[19/04/2015 18:03:03] Christian Legget: Dan, in fiddler ..newb question..how do you post..?!
[19/04/2015 18:03:10] Weekend Testing Europe: so, this proves that the API both allows the API to circumvent the UI validation against multiple votes
[19/04/2015 18:03:14] Trisha agarwal: 4
[19/04/2015 18:03:17] bhagya gdm: Go to composer
[19/04/2015 18:03:19] bhagya gdm: and select post
[19/04/2015 18:03:22] bhagya gdm: from the drop down
[19/04/2015 18:03:30] Weekend Testing Europe: by or right click Reissue and edit requests
[19/04/2015 18:03:36] Weekend Testing Europe: composer is very easy too
[19/04/2015 18:03:44] Weekend Testing Europe: we can do a session sometime if you like

[19/04/2015 18:03:46] Christian Legget: thanks both..
[19/04/2015 18:03:58] Christian Legget: yes, sounds a nice idea Dan :)
[19/04/2015 18:04:09] Weekend Testing Europe: if the API was secured to prevent
[19/04/2015 18:04:10] Srinivas Kadiyala: 6 ?
[19/04/2015 18:04:15] Ash Winter: Good heuristic there, comparing client and server side validation rules
[19/04/2015 18:04:23] Weekend Testing Europe: a) multiple votes
[19/04/2015 18:04:24] Trisha agarwal: yes
[19/04/2015 18:04:35] Weekend Testing Europe: b) user id tampering
[19/04/2015 18:04:43] Weekend Testing Europe: then this would be preventable
[19/04/2015 18:05:01] Weekend Testing Europe: Troy's course is really for developers to learn how to protect applications
[19/04/2015 18:05:17] Weekend Testing Europe: BUT it is Ace in showing testers what to look for when finding problems...
[19/04/2015 18:05:22] Trisha agarwal: great stuff to learn
[19/04/2015 18:05:26] Weekend Testing Europe: yeah, it is a great heuristic
[19/04/2015 18:05:36] Weekend Testing Europe: I am afraid our time is drawing to a close
[19/04/2015 18:05:38] Srinivas Kadiyala: http://codebeautify.org/jsonviewer

I use this to beautify the results.
[19/04/2015 18:05:39] bhagya gdm: seems like need to play with that bit more
[19/04/2015 18:06:00] Weekend Testing Europe: Weekend Testing Europe set topic to “WTEU-56: SUMMARY”
[19/04/2015 18:06:14] Weekend Testing Europe: so...a quick recap
[19/04/2015 18:06:19] Trisha agarwal: http://www.culbertsonexchange.com/wp/?p=293
http://www.developer-tech.com/news/2015/jan/08/moonpigs-api-breach-could-cost-its-business/
http://www.ifc0nfig.com/moonpig-vulnerability/
https://developers.google.com/identity/protocols/OAuth2
oath is deprecated...oauth 2.0 is the right one its essentially an authorisation protocol that is more secure than basic authorisation
it requires a token, which expects a valid response
http://www.asp.net/aspnet/overview/owin-and-katana/owin-oauth-20-authorization-server

Postman- which is run in the browser...the requests and responses can then be observed by an attacking proxy such as burp suite or zed attack proxy
Fuzzer - Fuzzers are great tools, ZAP has a built in fuzzer, as does burp
fiddler also has a plugin called X5S, which can do fuzzing
http://www.pluralsight.com/courses/hack-your-api-first -
https://www.guidgenerator.com/online-guid-generator.aspx
https://developers.facebook.com/docs/graph-api
https://www.youtube.com/watch?v=hdSrT4yjS1g
http://blog.smartbear.com/readyapi/api-security-testing-how-to-hack-an-api-and-get-away-with-it-part-1-of-3/
http://www.programmableweb.com/apis/directory
http://www.publicapis.com/
http://codebeautify.org/jsonviewer
[19/04/2015 18:06:30] Weekend Testing Europe: :)
[19/04/2015 18:06:35] Weekend Testing Europe: lovely Trisha :)
[19/04/2015 18:06:35] Trisha agarwal: my notes from the today session
[19/04/2015 18:06:37] Weekend Testing Europe: thankyou
[19/04/2015 18:06:37] bhagya gdm: :)
[19/04/2015 18:07:08] Weekend Testing Europe: we have looked at an example of poor API security in the real world, and its potential impacts
[19/04/2015 18:07:15] Weekend Testing Europe: the Moonpig problem
[19/04/2015 18:07:29] Srinivas Kadiyala: yes. It was a good example..
[19/04/2015 18:07:31] Weekend Testing Europe: I hope that was a great example of what NOT to do :)
[19/04/2015 18:07:42] Sandeep Garg: :)
[19/04/2015 18:08:03] Weekend Testing Europe: We have seen that APIs are really useful and powerful...they can provide a range of data
[19/04/2015 18:08:05] Trisha agarwal: yes :) be aware when testing the application real time
[19/04/2015 18:08:11] Weekend Testing Europe: so...it is important to protect that data
[19/04/2015 18:08:32] Weekend Testing Europe: we have had some ideas for further reading and training, from lots of good folks
[19/04/2015 18:09:04] bhagya gdm: And use sense when you use the public apis when testing

[19/04/2015 18:09:08] Trisha agarwal: yes :)
http://www.pluralsight.com/courses/hack-your-api-first -
[19/04/2015 18:09:11] Srinivas Kadiyala: Thanks a lot,thinking to do the troyhunts course soon. and apply on it.
[19/04/2015 18:09:13] Weekend Testing Europe: and we did some exploration of a known vulnerable API
[19/04/2015 18:09:30] Weekend Testing Europe: and that course, which It would be great if you could do sometime
[19/04/2015 18:09:40] Weekend Testing Europe: do it with the other course...hackyourself first
[19/04/2015 18:09:52] Sandeep Garg: (y)
[19/04/2015 18:09:52] Weekend Testing Europe: they come as a pair really...complement each other
[19/04/2015 18:10:10] Christian Legget: just got a vote in via fiddler Dan for car 4 (the la rouge donkey)
[19/04/2015 18:10:14] Weekend Testing Europe: some useful tools, fiddler, firebug, zap, etc
[19/04/2015 18:10:34] Weekend Testing Europe: I might do a mini blog post on Fuzzing via my The Test Doctor blog
[19/04/2015 18:10:48] Trisha agarwal: (y)
[19/04/2015 18:11:03] Weekend Testing Europe: but i have to be careful saying too much in public about what tools and stuff I use...as anyone can read that
[19/04/2015 18:11:11] bhagya gdm: (y)
[19/04/2015 18:11:54] Sandeep Garg: yes, do that as a Security Research Analyst :)
[19/04/2015 18:11:58] Srinivas Kadiyala: Thanks for the session.
[19/04/2015 18:12:16] Weekend Testing Europe: Remember...hacking is usually bad...if done at the wrong time/place etc....including testing for security in your work will help your teams, but seek permission first...!!!!
[19/04/2015 18:12:36] bhagya gdm: Thanks Dan and others. was very useful
[19/04/2015 18:12:56] Christian Legget: i mis read the fuzzing for fogging Dan ;)
[19/04/2015 18:13:18] Christian Legget: thanks for todays session..enjoyed the hands on element..
[19/04/2015 18:13:56] Weekend Testing Europe: No date is set yet for the next session...but there will be news coming up soon.

[19/04/2015 18:14:16] Sandeep Garg: this session helped me in looking at APIs, API Testing and API Security Testing from a new angle - Food for thought :)
[19/04/2015 18:14:19] Christian Kram: thanks, Dan. I had to tune out and never got back into topic, so I will have to read the transcribed afterwards. But what I got, was really interesting :)
[19/04/2015 18:14:26] Trisha agarwal: great session to learn ! lot of learning on the unkown area ! Thank you . Will seek for a next session very soon on May
[19/04/2015 18:14:42] Weekend Testing Europe: Weekend Testing Europe set topic to “WTEU-56: END”
[19/04/2015 18:15:03] Weekend Testing Europe: It only goes to say thank you for joining me today, and sharing your learning