Timur Abdiukov's Blog

Create Post (/COMP6443/19T1/blogs/create)

27/03/2019 (/COMP6443/19T1/blogs/post/32393)

(/COMP6443/19T1/blogs/32393/edit) (/COMP6443/19T1/blogs/32393/delete)

* Wednesday, 27/03/2019, 11:00 o'clock.

I got my new iPhone, and what do you do when you get a new fast and noice phone? You install apps! And so did I. I installed the UNSW uni-verse app (how original). But what is interesting is that unlike the jailbreak nerds, I went straight up to installing the latest iOS. What is interesting is that on iOS 12 the app, to say the least, doesn't work correctly (constant exceptions etc). Even more so, if you access certain areas on the app, you'd get access to the API which outputs otherwise inaccessible information. I guess similarly to the Elliptic curve encryption, it's the case of 'performance+less mess undermining security'. Still pretty cool!

Unfortunately I can't, and won't disclose much not to undermine UNSW (yet again). I'm not that crazy. On the bright side, I already let know the IT support and they askedc me to come show them what I mean. Will likely do that next week (1->7th of April)

posted by Timur Abdiukov (/users/z5214048) 3 days ago (Saturday 30 March 2019, 01:46:44 AM)

22/03/2019 (/COMP6443/19T1/blogs/post/32392)

* (/COMP6443/19T1/blogs/32392/edit) (/COMP6443/19T1/blogs/32392/delete)

Friday 22/03/2019, around 10 PM

I looked (and actually still do) for the aviation textbooks and a fellow student named **adamt** from Seceduau slack suggested to look into the Bob Tait textbooks (and urged not to crash planes heh). Sure, I looked around and found this guy's online store (http://store.bobtait.com.au/) (http://store.bobtait.com.au/) . What is surprisingly interesting is that the 'search field' was SQL injectable and in fact very trivially SQL injectable (didn't even have to fire up SQLMAP). How did I discover that? Just out of boredon typed in random rubbish in search for books, and boom - an error message! I later emailed Bob Tait, and he had the issue fixed very fact.

Bottom line is, COMP6443 is very well practically useful! I think I would've underestimated the taught content if not it was trivially applicable in practice ☺

* Monday 01/04/2019 (April Fools day)

Adding a meme which surprisingly fits in,

{ ----- M E M E ----- } (https://www.youtube.com/watch?v=I17jhOgrGMU)

posted by Timur Abdiukov (/users/z5214048) 3 days ago (Saturday 30 March 2019, 01:44:56 AM), last modified about a minute ago (Monday 01 April 2019, 07:20:15 PM)

20/03/2019 + memes added slightly later (/COMP6443/19T1/blogs/post/32390)

(/COMP6443/19T1/blogs/32390/edit) (/COMP6443/19T1/blogs/32390/delete)

* Wednesday, 20/03/2019, 7-8 AM:

I received a letter (a physical one, they still exist!) that by lovely car is recalled due to possibly faulty airbag. The letter adviced to check my car out on IsMyAirbagSafe (http://ismyairbagsafe.com.au) . I entered my rego plate, and sure enough, it is eligible for a recall. BUT what is interesting is that the website provided a link to the car make website with the VIN within the link! Crazy! And if one finds out this, and is in the state of mind to go rogue, they can brute the

number plates to get VINs and other leaking misc information.

For number plates: 26+10=36(possible characters)^6(trivial rego length)/ 100 (suppose, 100 requests a second) = in around 251 days one can dump the entire Australian cars database, with regos corresponding to the car make, car model, VINs, year made and other miscellaneous info.

Unlike IsMyAirbagSafe (http://ismyairbagsafe.com.au) , the car makers at least ask for the driver's licence and/or the VIN! Thank God!

Meme time AKA examples: from Ruby Fields' P-plates (starting 1 munite and ~45 seconds (https://youtu.be/t5s1DGjUa68?t=105)), we now know that the guy's Black Subaru is affected and now we know his VIN? Now the question is, what do we do with this information heh?

MORE memes (probably a few days later): On the other hand, at least nationwide favourite ~~trashy~~ ladies who empty Jack Daniels stocks at your local ~~AWS~~ BWS have their Falcon as safe as ever.

[Link to the video. Webcms3 doesn't like IFRAME] (https://www.youtube.com/watch?v=6cDdvFQIAfM)

Still, Commodore or Falcon?

posted by Timur Abdiukov (/users/z5214048) 3 days ago (Saturday 30 March 2019, 01:14:50 AM), last modified 3 days ago (Saturday 30 March 2019, 01:19:38 AM)

15/03/2019-17/03/2019 (/COMP6443/19T1/blogs/post/32389)

~~(/COMP6443/19T1/blogs/32389/edit)~~ ~~(/COMP6443/19T1/blogs/32389/delete)~~

* Friday, 15/03/2019, around 9 o'clock:

Discovered a **CRITICAL** vulnerability of CSE login system. If the range of ASCII characters from 32 to 255 are inputted, the system allows through, bypassing checking.

[Messages on it deleted from Slack to avoid troubles both for myself and UNSW alike]

17/03/2019: Vulnerability fixed up quietly. Bless UNSW

posted by Timur Abdiukov (/users/z5214048) 3 days ago (Saturday 30 March 2019, 01:08:35 AM)

【Something Awesome!】 (/COMP6443/19T1/blogs/post/32388)

(/COMP6443/19T1/blogs/32388/edit) (/COMP6443/19T1/blogs/32388/delete)

Note : This blog is dedicated to storing my Something awesome notes and information. Initially they resided on my WebApp-tools repo, which had to be set to private to avoid unfair use (no worries!). Unfortunately, there does not seem to be a direct way to import my notes here with timestamps (and their markdown syntax), so I will specify dates whereever applicable.

【Something Awesome!】
The idea: with the new COMP6443 knowledge, I will try to passively find vulnerabilities on the everyday websites I use. While the idea seems 'crazy', it may be worthwhile?

Here goes

posted by Timur Abdiukov (/users/z5214048) 3 days ago (Saturday 30 March 2019, 01:03:27 AM)