

P7

Sun, Jul 21, 2024 2:13AM • 21:15

SUMMARY KEYWORDS

testing, security, test, software, pci dss, test cases, good, database, api, important, team, release, trainings, logging, pipeline, quality, manual testing, running, launch, ports

00:00

Yeah, I am back.

00:02

Sounds perfect.

00:03

I started recording, and we can continue. So for that, I did not expect that.

00:11

No worries, I had the tiebreak. So it was good action.

00:17

Sounds perfect.

00:20

Worry about the, let's say,

00:24

what impacts do you see

00:28

while prioritizing software quality

00:32

over the future rolling?

00:36

Like how it affects the villas still near future delivery, is it affecting or it's just me.

00:56

That's interesting,

00:57

in my opinion testing actually,

01:01

in short term testing takes more time and resources.

01:09

While in long term,

01:12

it helps to,

01:15

to basically win, as you mentioned, time and human resources, because basically, the more bugs you found during development, prototyping, and design plays before the release, the better mean basically, over time, like your customers will enjoy a good product. And over time, you will, you will have more more customers. And basically, there will be less bugs over time. So it helps to eliminate future future bugs. And over time, it helps to basically over the good quality software is important. But also launch time in Agile is important as well. So in Asia, you're doing horizontal launching, and you need to launch as fast as possible, especially for startups, it's important to launch as fast as possible. So there is some some ratio, Golden Ratio, where your software should be good enough for a customer's there should be less political box. And there can be a minor box, maybe some medium box that found after some time, and you have time to patch it to release patches. That's why you need good release management system, you need CI CD, you need to have automation testing, in order to to do faster regression testings, when you do patch releases by quarter fixes and patch releases. So yeah,

03:24

correctly, like before having automations and CI CD in place, it takes more time, but after you have them already saves you some time.

03:38

Well, basically, you need C ICD unit testing framework.

03:46

In order to win,

03:48

basically your idea, you definitely need the ICD cert unit to have different tests, you'd smoke tests which run build and regression test testing pipelines separately, in order to test as often as possible. So first term, it's huge investment of resources. PJM investment of time, different servers. A lot of developers involved, helping as that to build test framework, but in long term you're winning, because increase quality means more satisfied customers. more satisfied customers at some point will be organic, and it will increase your brand awareness. So in one long term, you're winning, but there it should be right to you. You should not launch late before of tests because of testing. Yeah, like were late. So basically, the

strategy To find the golden ratio, you can enough quality like good enough to launch. And like also not to have a lot of critical bugs. So if you launch, a lot of customers are going to use your buggy software and they will decide not to use and brought to your computers. So they should you need to find a good way to you need to build test framework and have a pipeline in order to do testing as often as possible.

05:30

Good. By the way, you also mentioned that you have like different pipelines, for example, you said smoke tests should run in every, let's say, delivery basically, every commit. But in vice versa. There are some test cases that are too costly to run, how it's working, how you strategize, like what to run and whatnot around how often you are running them. Can you tell me a bit about it?

06:01

Yeah, so basically,

06:03

why don't we have some branch created when developer creates a branch. And developer is developer needs to create a merge request domain or pull request in some companies. So before doing that, you need to run your branch in in CI CD pipeline. So you're running your branch and usually unit tests, integration tests, and some entrance smoke tests are running in our in our case, and how I design usually I put at least one pass test, which is critical. One or two have the bestest, and one or two negative case scenarios, which are also critical for all the features. In in, let's say in the product. If we are using API, then it's API if it is a web application and web application. So basically, in regression, I can have, let's say, again, we are given an example of login page, let's say for testing login page, some small login page, I have like 20 test cases or the case test cases for regression, like automated test cases. But for smoke in smoked Su, there are only three or four test cases by two positive and two negative. They are the most critical ones. And they are running each time in main pipeline. So I have separate pipeline developed for only for testing, which is regression testing, and it's running, scheduled running, but also in a main pipeline of development in there are like unit tests, integration tests, and Atlantis, some smoke tests.

08:16

Good, good.

08:19

It turns around understandable.

08:21

I have one more question left regarding the compliance. Like in the banking industry in the finance industry. There are like tons of regulations as we discussed earlier. What about like,

08:36

how it affects the software quality?

08:38

And how organization ensure the compliance with these regulations?

08:47

Yeah, that's good question. I think I touched this question in like previously. So basically the main.

08:57

So I will say like that there are two main

09:01

compliance regulations that are important for finance. It's GDPR and PCI DSS, and in my opinion, PCI DSS, if not mistaken, is a part of GDPR. So it's basically GDPR for finance. There is also HIPAA, but it's for health stake. So not bad, but it's basically HIPAA. If you are, there are some software's that touch healthcare and fintech. It might be like you need to be compliant with Bas PCI DSS and HIPAA.

09:48

This GDPR is Europe related. We're about here in the US. Have you seen the compliance like regulations? Or

09:58

you didn't touch the By now. Well,

10:04

I definitely know that we need to follow PCI DSS. And I think PCI DSS is a part of GDPR. Maybe I'm mistaken. But in my opinion, it's part of GDPR is basically like, like how you mentioned how company ensures that. Like, we follow PCI DSS so basically, we have a lot of training. First of all, we have trainings. For

10:37

my second question, by the way.

10:41

Yeah, so it's at once. So basically, we have internal trainings, like video materials, and not only, like, let's say, we have, like I am learning OWASP security recommendations for API's, there are different security laboratories. We're passionate to is hackable. And we have a paths, different paths. And I need to break in, like, do SQL injection or cross site scripting, and somehow breaking without authorization and doing different labs. So it's basically teach me security vulnerabilities in API's. And this is a part one part of compliance with PCI DSS and I have examination then, like not only laboratory but also quizzes, like multiple choice. And also, I need to create a documentation and report what I have learned during this trainings. And this is one part. And other part is basically I need to add, like I adding, like, I'm learning this things, and I am applying it in my testing in my manual testing. And also, I'll tell almost this thing, I'm adding it, as I mentioned, the login example. So like I'm using different CSV files with different variations of inputs for user name and password, which includes SQL injections as well. And different scripts inside it, as well. So basically, oh, and also, I'm doing manual testing, I am checking database structure. And to be sure that it's compliant with PCI DSS, the encryption, as I mentioned, that

encryption should have not only some algorithm, which is not traceable, which is not known. But also that algorithm need to have some random data at its basically need to be hash. So that hacker cannot create a rainbow table and match encrypted passwords with some string. No. Yeah, those are the same. So I'm doing my own testing, observing database. And also recently, but sorry, recently, I have done internal audit, we have our security team. Exactly.

13:35

I was trying to ask like,

13:39

regulators doing the audit is normal thing I know that they are doing but what about the internally like how organization issue this like you keep with this rules?

13:52

It's very strict. We have our security team, and security team. All the time trying to test employees, they send phishing emails.

14:06

To trick you like fake phishing emails.

14:10

In addition to that, when we release some product security team gives you recommendations, for instance, like in spring boots, for Spring Boot application, right? So when I'm running some service, there are different I was testing what kinds of Port ports are running in my Linux machine, to be sure that all ports are related to service that I'm using to be sure that there are no other services running in test machines. And to be sure that all my services are documented internally. So we I got a lot of recommendations from security team when launching our products, and we were doing our internal testing. And later, they will do user acceptance testing by their own and check our test reports. So what I'm testing, I'm testing database encryption tables structure, like foreign keys, private keys, like database normalization, me and other team members as well. And then Linux tests, I am verifying that all our libraries in Java, they are up to date, there are no security vulnerabilities, we are using sonar cube, which shows all of that. And also, I am testing Linux file permissions that our file permissions are correct. Like they are, there are more executable for basically we have our own recommendation. So I'm checking directory chmod, malice and to G on values, like who's the owner of application, which should be app user only. And also like, also, and testing like ports, like which ports are listening, which ports are opened. That's important.

16:27

And also logging, logging is also important.

16:32

So meaning,

16:34

meaning like, let's say somebody tried to call our API's, right, I need to assure that in logs, we have IP address, and endpoint and also request body that was sent to endpoint. So we have a huge logging where, like, everything is tracked, all API's that use, like all API endpoints that use and basically.

17:11

So we are doing internal

17:14

testing, based on security recommended teams, conditions as well.

17:19

So the basically security team,

17:23

not only part of the security of the application, but also security of the compliance with the global regulations that we have locally. Here.

17:37

Yeah, where we have trainings.

17:41

And like we're all employees increasing, like studying and increasing our knowledge in this domain. But our there is also security team, who test everything like including employees. They check cameras like physical security test rolling, and like, who tries to, to enter without access rights, and logging, like logs to database different. So everything is traceable, and long. an hour. This is.

18:23

Sounds perfect.

18:26

Well, I got all the answers that I needed for the questions. And right now, I don't have any other question. Do you want to add something?

18:37

Well, in terms of security, we have a network security team as well. Like we have firewalls definitely

18:47

also f5 security

18:51

that basically configures SSL certificates and configures different rules

19:03

for

19:05

for our endpoints and internal software. So yeah, the Yeah, security team is doing their job. And it's it's definitely a different area. And it's running in parallel with software testing. But it

19:26

has four answers. I got everything covered. Who's the really good to talk to you about, like you covered every aspect of the software quality and how it's happening inside of the financial industry. And it seems that it's a bit different from the general tech programs. But it's understandable why it's different. And what's the point there?

19:57

Yeah. Thank you. I accept it as a compliment. I would say that I have that much experience in mobile testing. It's a bit different area, both in terms of web testing, I have tested, like different kinds of web applications and database testing. And API testing as well, both manually and doing automation scripts. So, but yeah, it was, it was nice to talk to you. I really liked the questions too. They are very, very, very broad. And worry interesting. So I wish you good luck in your thesis. Thank you. Yeah. And graduates. Thank you.

20:50

Thank you for answers and for having time for me. It really was perfect session.

20:58

Hello, good evening smile.

21:02

Used to come out. Thank you. And yeah, good luck to you again and enjoy your evening.

21:06

Take care. Take care.

21:09

Bye bye.