OWASP™

Meeting Starts at 6:05PM

In the meantime, checkout https://zapcon.io

OWASP Sacramento

February 2022

Agenda

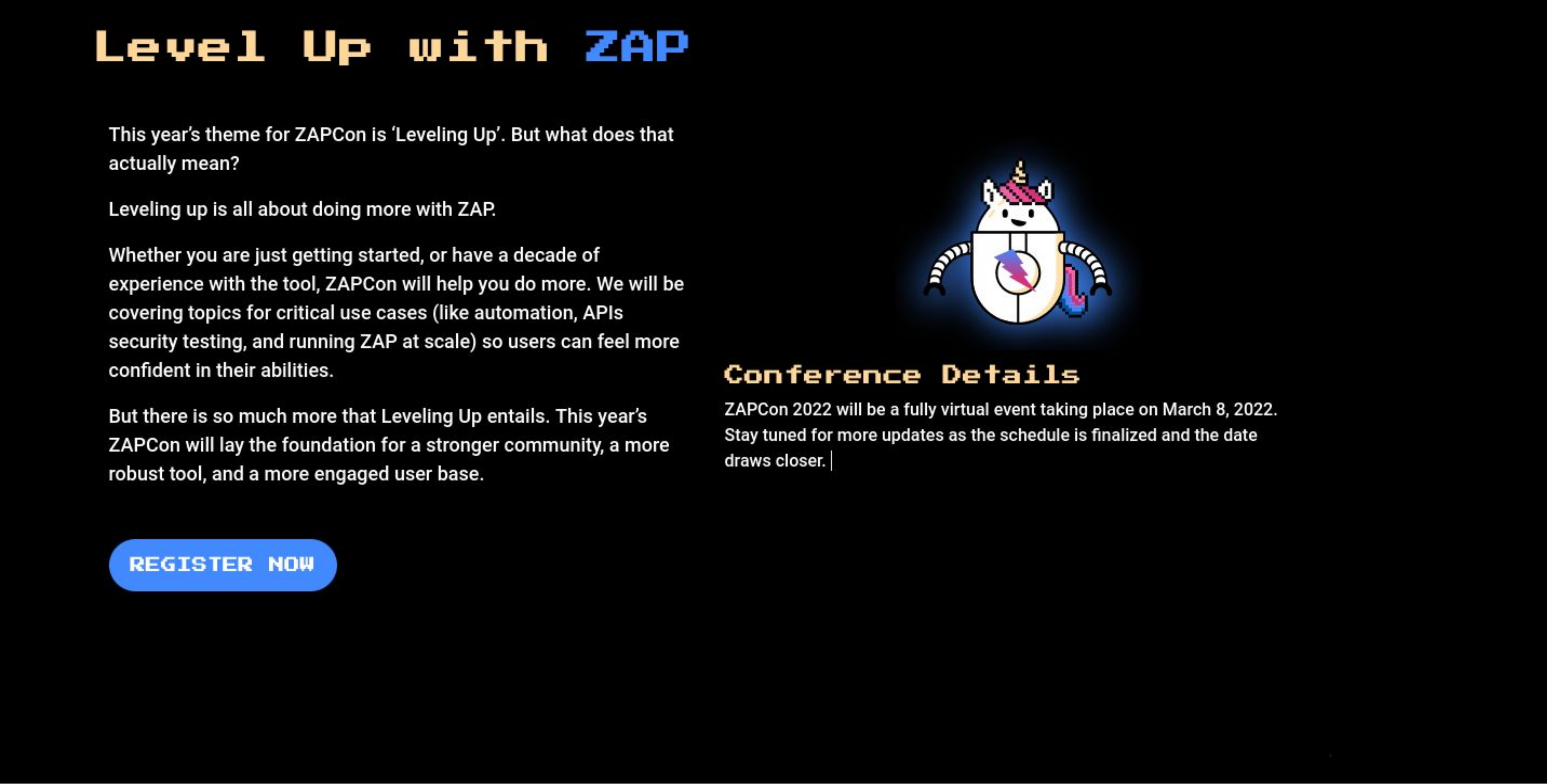
1) Community Topics
   - ○ Welcome to 2022!
   - ○ ZapCon
2) CI/CD and TeamCity in a nutshell.
3) PwnCity Walkthrough

Happy 2022!

Looking to have meetings monthly.

- Has been the 4th Thursday of every month @ 6pm.
- May evaluate different time/day of week if members would like.

Virtual for the next couple, but we’ll evaluate the potential to have them in person.



Level Up with ZAP

This year's theme for ZAPCon is 'Leveling Up'. But what does that actually mean?

Leveling up is all about doing more with ZAP.

Whether you are just getting started, or have a decade of experience with the tool, ZAPCon will help you do more. We will be covering topics for critical use cases (like automation, APIs security testing, and running ZAP at scale) so users can feel more confident in their abilities.

But there is so much more that Leveling Up entails. This year's ZAPCon will lay the foundation for a stronger community, a more robust tool, and a more engaged user base.

Conference Details

ZAPCon 2022 will be a fully virtual event taking place on March 8, 2022. Stay tuned for more updates as the schedule is finalized and the date draws closer.

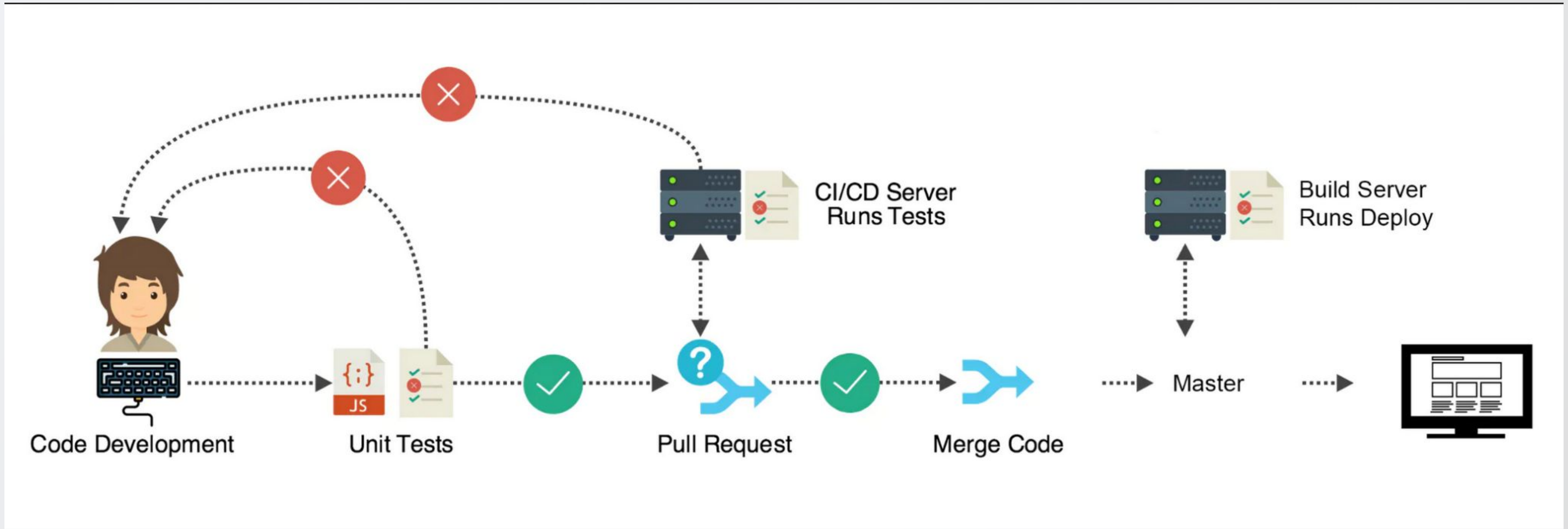
PwnCity

CI/CD

Code changes are made, and automated build-and-test steps are triggered. The code is then delivered automatically as a part of the CD process.

The “CI/CD pipeline” refers to the automation that enables incremental code changes from developers’ desktops to be delivered quickly and reliably to production.

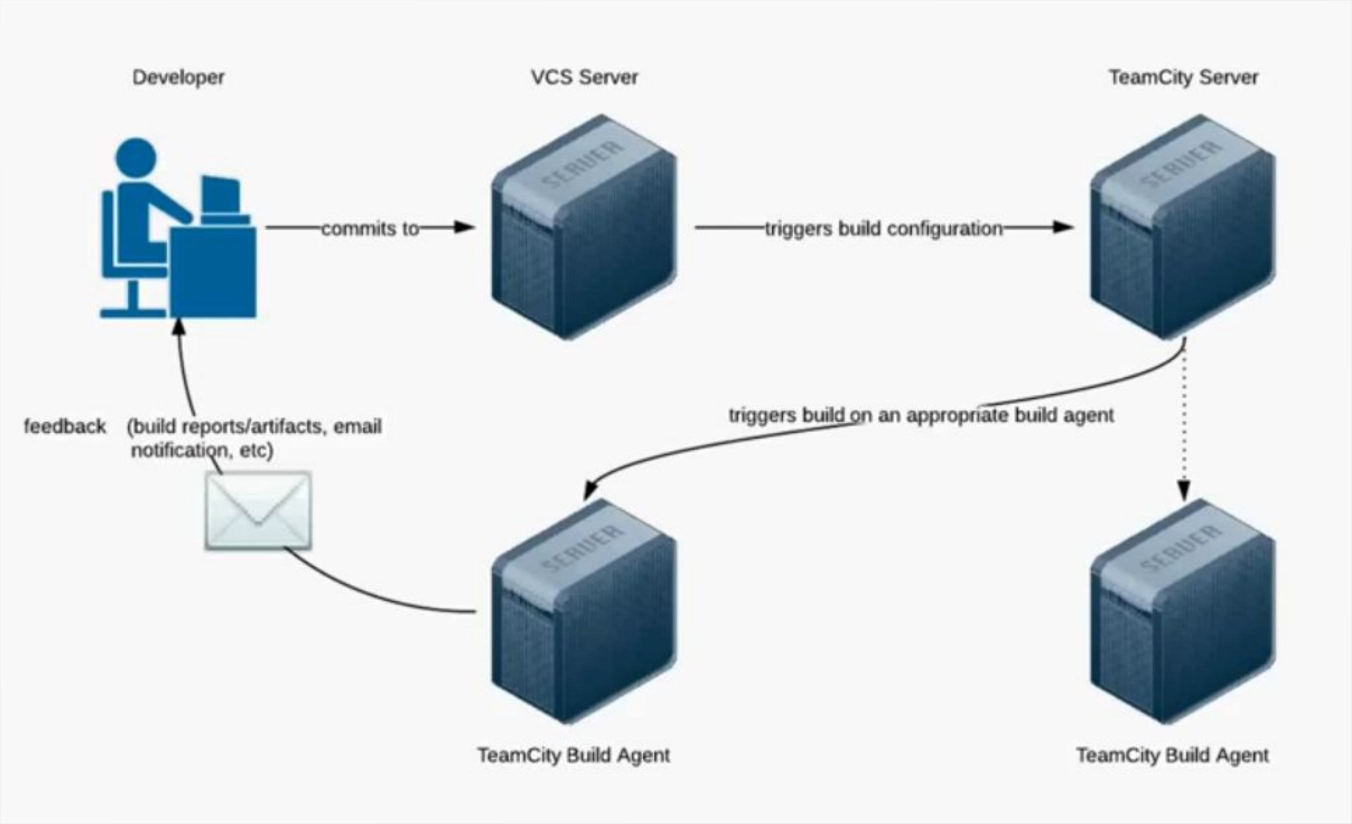
-Synopsys



CI and CD stand for continuous integration & continuous delivery.

TeamCity

by JetBrains


Developer
VCS Server
TeamCity Server
commits to
triggers build configuration
feedback (build reports/artifacts, email notification, etc)
triggers build on an appropriate build agent
SERVER
TeamCity Build Agent
TeamCity Build Agent

TeamCity is a general-purpose CI/CD solution that allows the most flexibility for all sorts of workflows and development practices.

-JetBrains

Consists of

- Version Control Repo(s)
- Build Server(s)
- Build Agent(s)

Disclaimer

This presentation neither advocates for or against the use of TeamCity by JetBrains.

TeamCity is the chosen CI/CD tool for this demonstration of an insecurely configured environment.

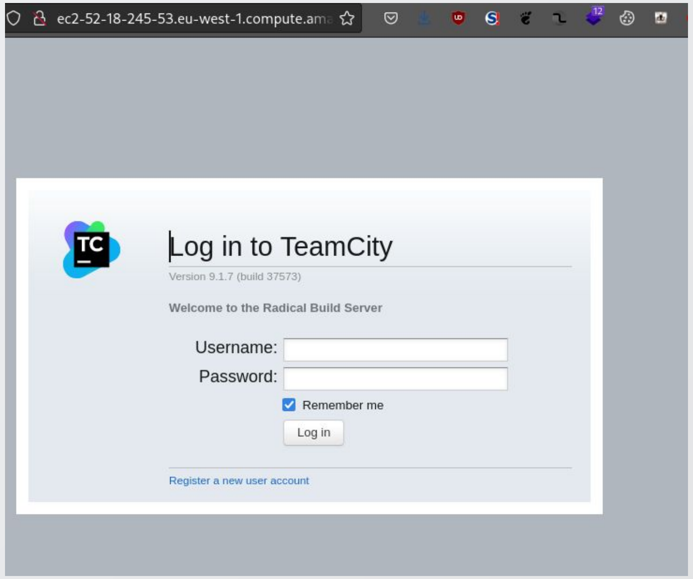
This presentation **does not** imply any security shortcomings in TeamCity as a product.

Begin

Background

http.title:"Log in to TeamCity &mdash;”

- Shodan reveals thousands of exposed TeamCity panels.
- Registration and Guest login is enabled in the wild for many.
- PwnCity is a compilation of misconfigurations I’ve come across during engagements.
- Chains of misconfigurations can and has lead to complete compromise of a network.



ec2-52-18-245-53.eu-west-1.compute.ama

Log in to TeamCity

Version 9.1.7 (build 37573)

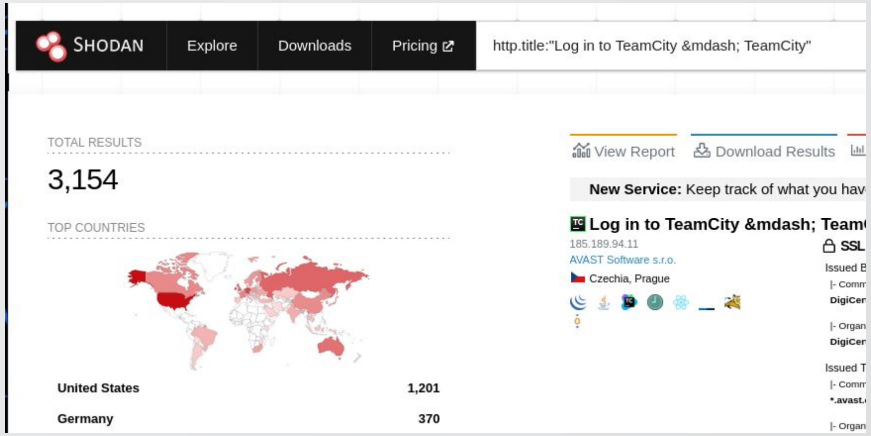
Welcome to the Radical Build Server

Username:

Password:

☑ Remember me

Register a new user account



http.title:"Log in to TeamCity &mdash; TeamCity"

TOTAL RESULTS

3,154

TOP COUNTRIES

United States	1,201
Germany	370

New Service: Keep track of what you hav

Log in to TeamCity &mdash; Team

185.189.94.11

AVAST Software s.r.o.

Czechia, Prague

SSL

Issued B

|- Comm

DigiCer

|- Organ

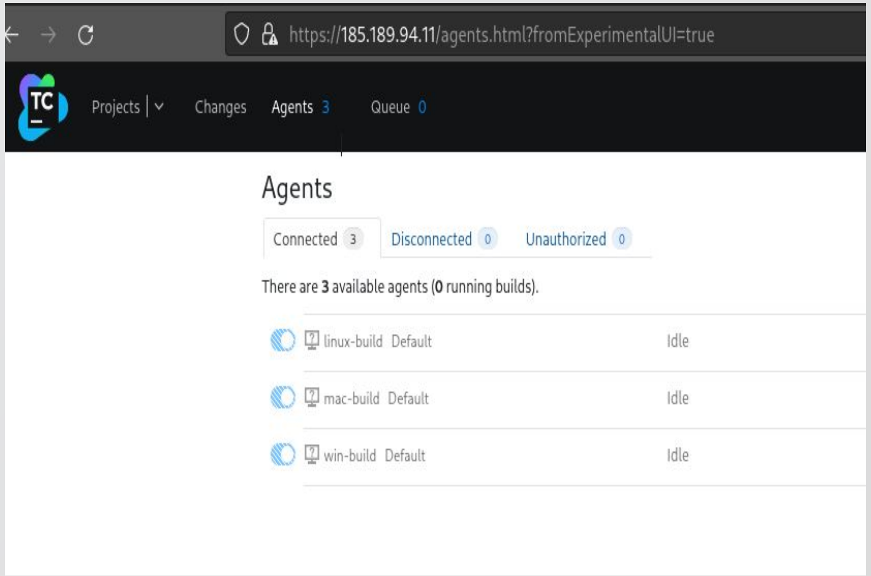
DigiCer

Issued T

|- Comm

*.avast.

|- Organ



https://185.189.94.11/agents.html?fromExperimentalUI=true

Agents

There are 3 available agents (0 running builds).

```
linux-build  Default    Idle
mac-build    Default    Idle
win-build    Default    Idle
```

Premise

We’ve been asked to evaluate the security posture of a small software development shop.

Objective: Determine if we can gain access to sensitive information.

Our recon has determined that they own the assets behind the public IP address `52.234.0.18`

Demo

Duration – 30 min(ish)

Conclusion

1. These misconfigurations are common because…?
   a. Of ignorance.
   b. Environments are/were built quickly to achieve business goals,so no one ever looked back.
   c. The impact of multiple misconfigurations combined isn’t clear enough to owners.
   d. All of the above.
2. A hardening guide for admins, is a cheat sheet guide to attackers.
3. Common security practices are all important for good reason.
4. TeamCity is an example in this case for any CI/CD tools/server.

References

- https://blog.jetbrains.com/teamcity/2021/02/hardening-your-teamcity-server/
- https://www.jetbrains.com/help/teamcity/super-user.html
- https://github.com/kacperszurek/pentest_teamcity
- https://github.com/d0n601/PwnCity/

OWASP Community

Call for Presentations: **March** and **April** (likely virtual events)

If you'd like to present (or know someone else who would) at the OWASP Sacramento Chapter's upcoming meetings, please email us your topic.

You don't need to be an expert!

Joubin: joubin.jabbari@owasp.org
Ryan: ryan.kozak@owasp.org