TECH TALKS

ADVENT COWORKING

- Next event: May 2018 (TBD)
- Application UX and Front-End Design

Brought to you by

RMCSoft

SOFTWARE SECURITY 101

Meet the panel of experts

Srinivasan Vanamali, Olympus Infotech

Ben Wilson, deliverypath

Kate Kliebert, Kliebert Law

Bilal Soylu, Xcobee

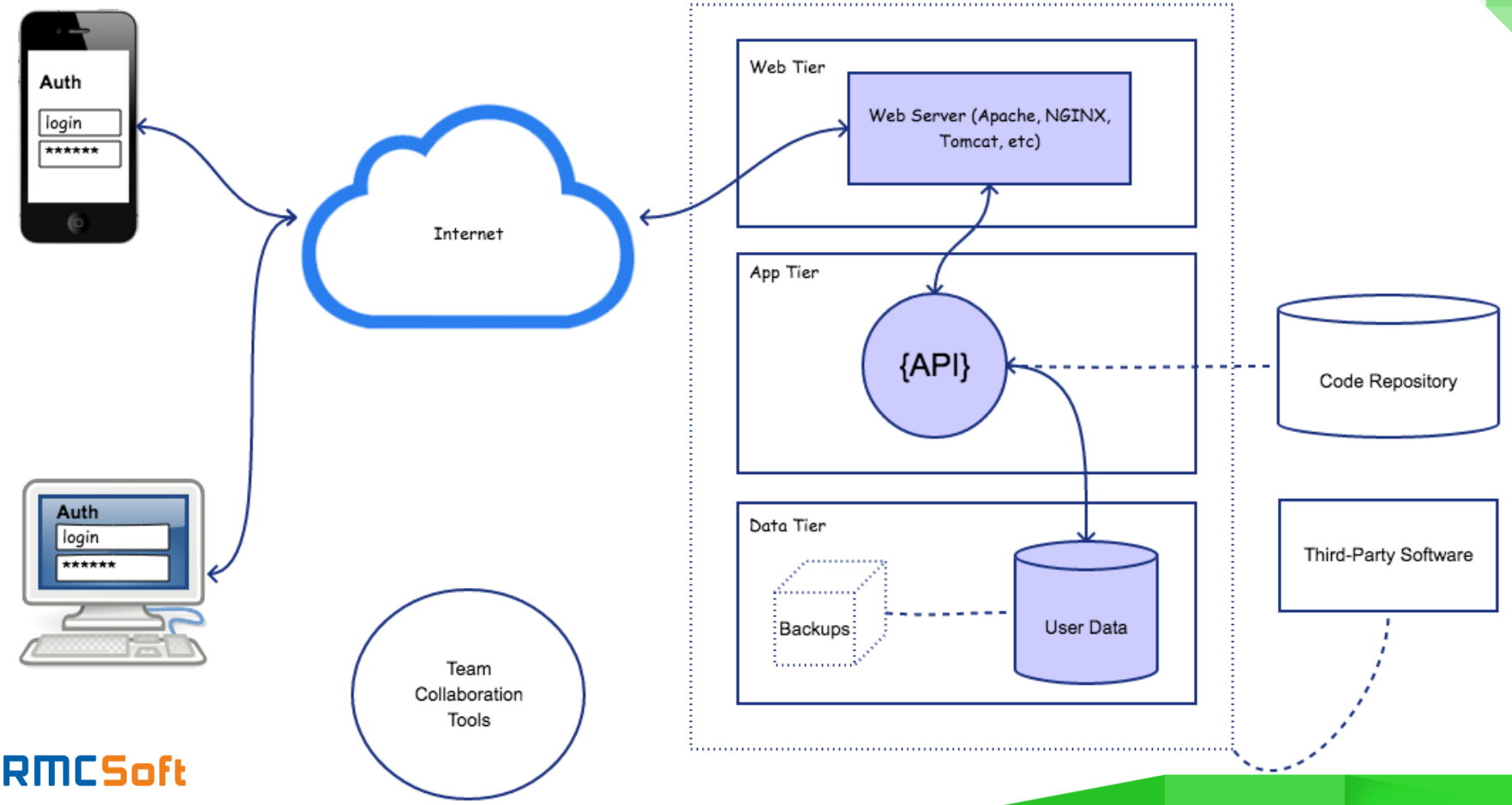
❖ sponsored by: deliverypath OLYMPUS Infotech

From An Idea to The Killer App

- ❖Idea
- ❖Validate it with Business Partners, potential clients, colleagues & friends
- ❖Define the Requirements
- ❖Develop the App
- ❖Ready to go!

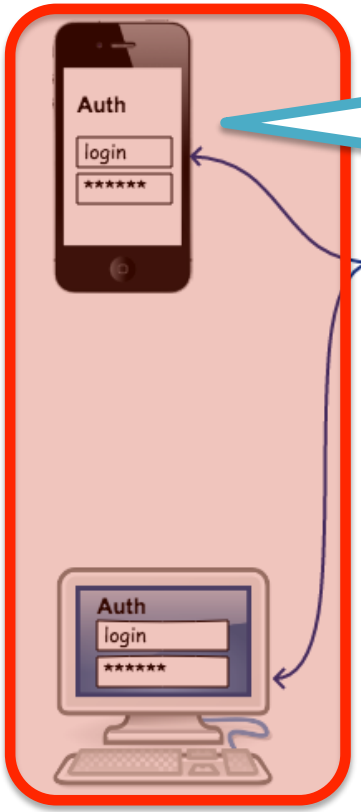
RMCSoft

Typical Application Architectural Components:



RMCSoft

Typical Mistakes: Client Tier

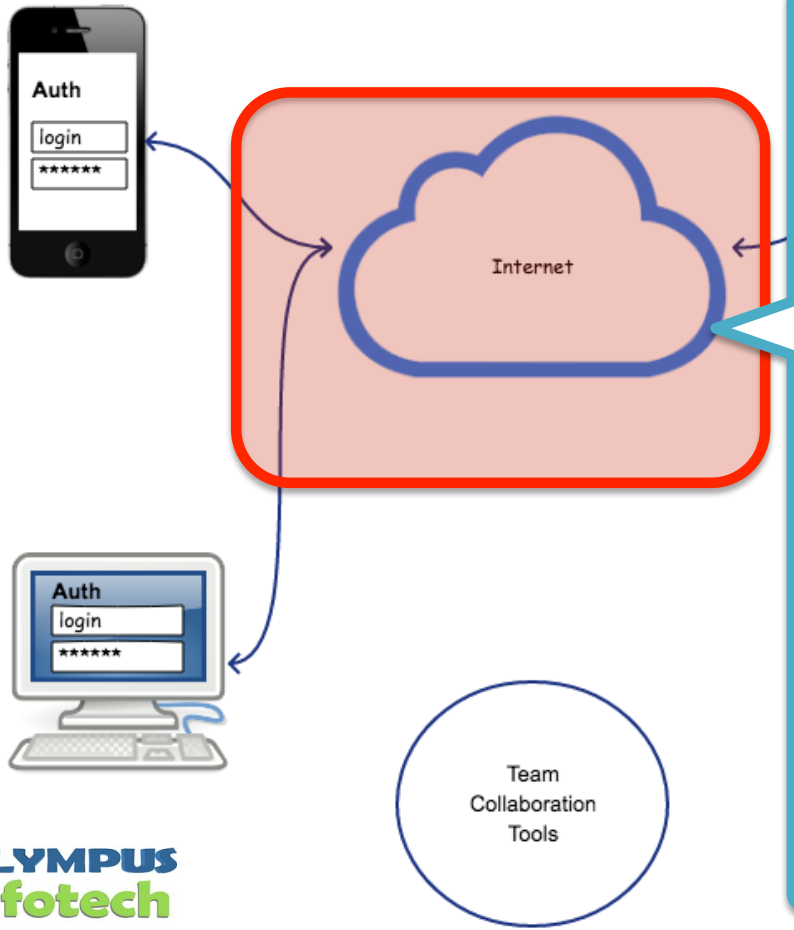


- ❖Issues in separation of Public / Private areas of the application
- ❖Some of the application resources that meant to be private get exposed to the public

- ❖Authorization - issues in user rights
- ❖The user roles get messed up - wrong type of users get access to the resources that they should not to

- ❖Securing Credentials
- ❖User credentials are stored & passed as CLEAR TEXT

Typical Mistakes: Web Tier



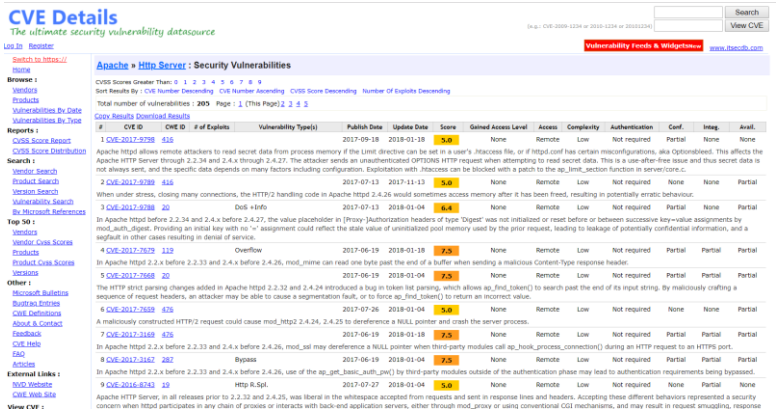
❖Data gets transferred through the INTERNET - unprotected area

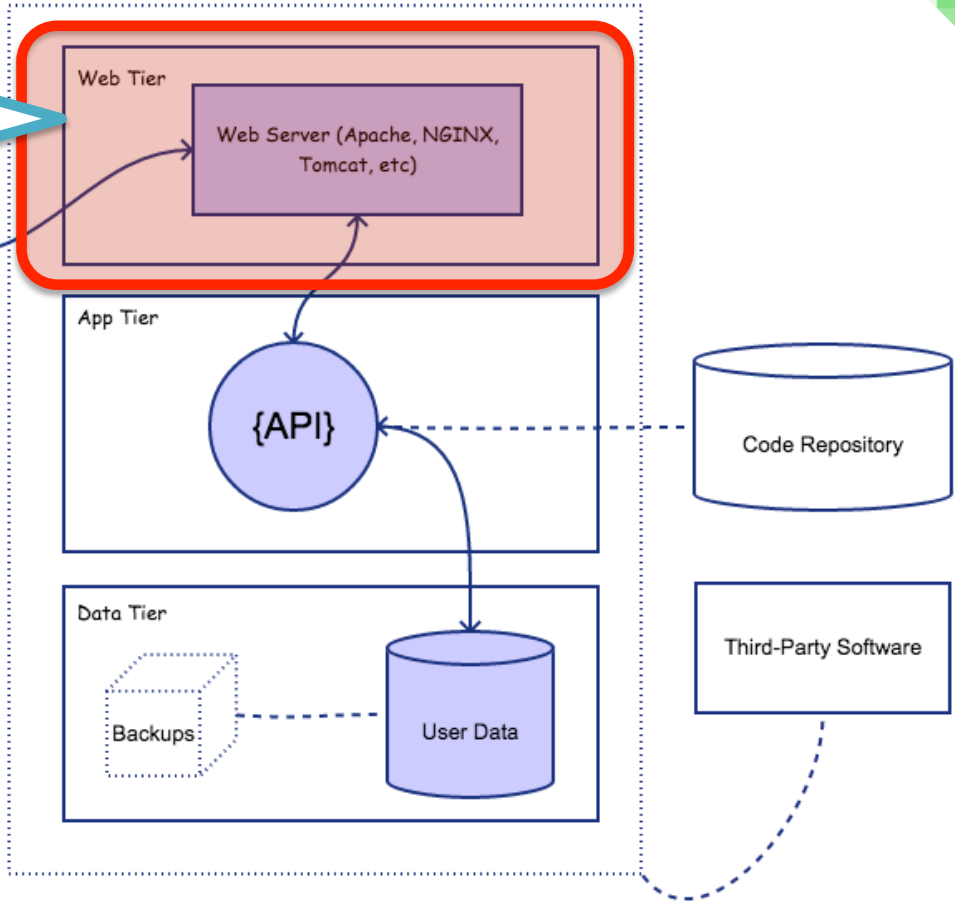
❖The connection is not encrypted
➢HTTP instead of HTTPS is used
➢Old and vulnerable versions of SSL/TLS are used

❖Other Vulnerabilities

Typical Mistakes: Web Tier

- ❖No breaches monitoring for the software installed on the servers
- ❖Common Software Vulnerabilities get overlooked
- ❖The Server Software is not updated promptly after the vulnerabilities get discovered
- ❖I.e. 9 pages of vulnerabilities for Apache on the screenshot:

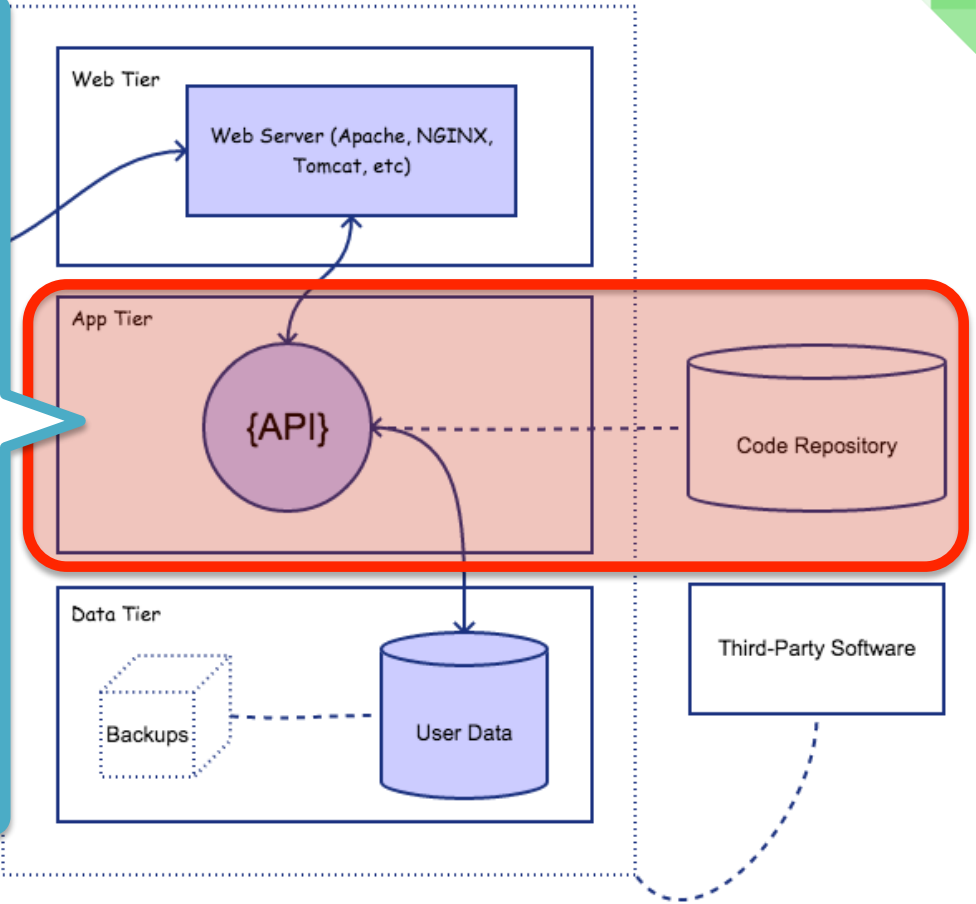




OLYMPUS Infotech

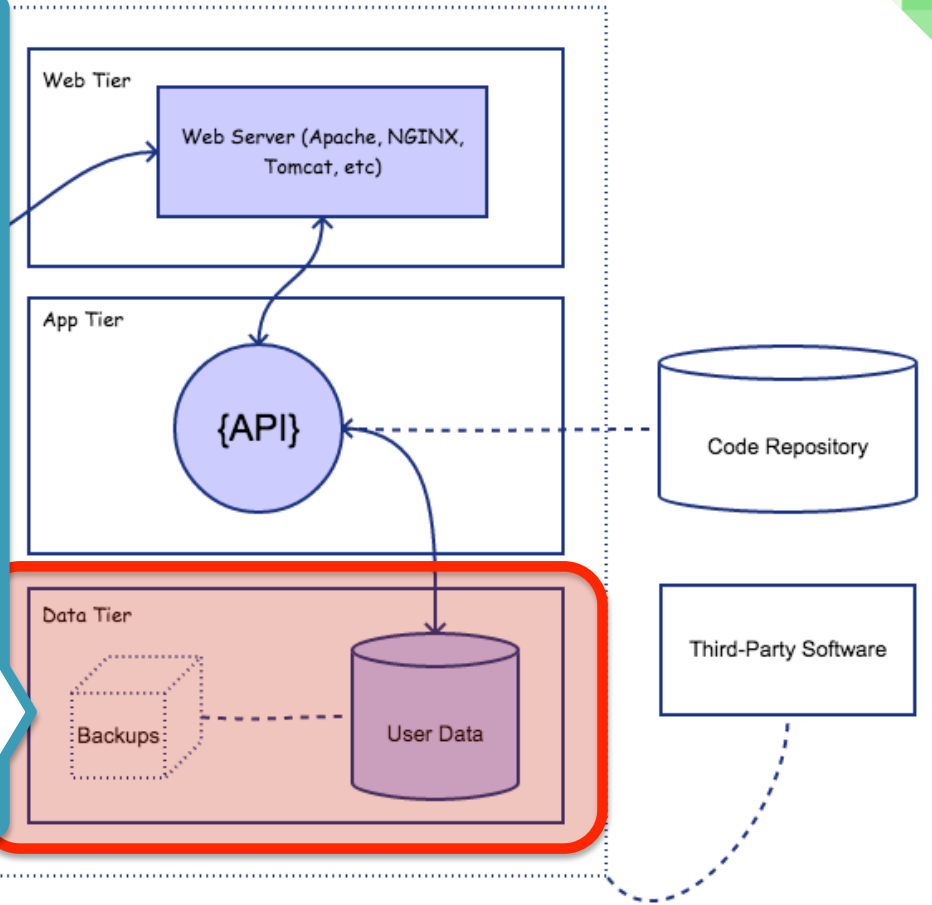
Typical Mistakes: App Tier

- Source Code Management
- Public repositories instead of private
- Access rights to the source code are not managed
- Developers do not have clear understanding on what project they are working on
- Vulnerability in the code
- Not following the best practices
- Not following “Security by design” pattern
- Not storing API keys securely
- Breaches in the third-party components and libraries

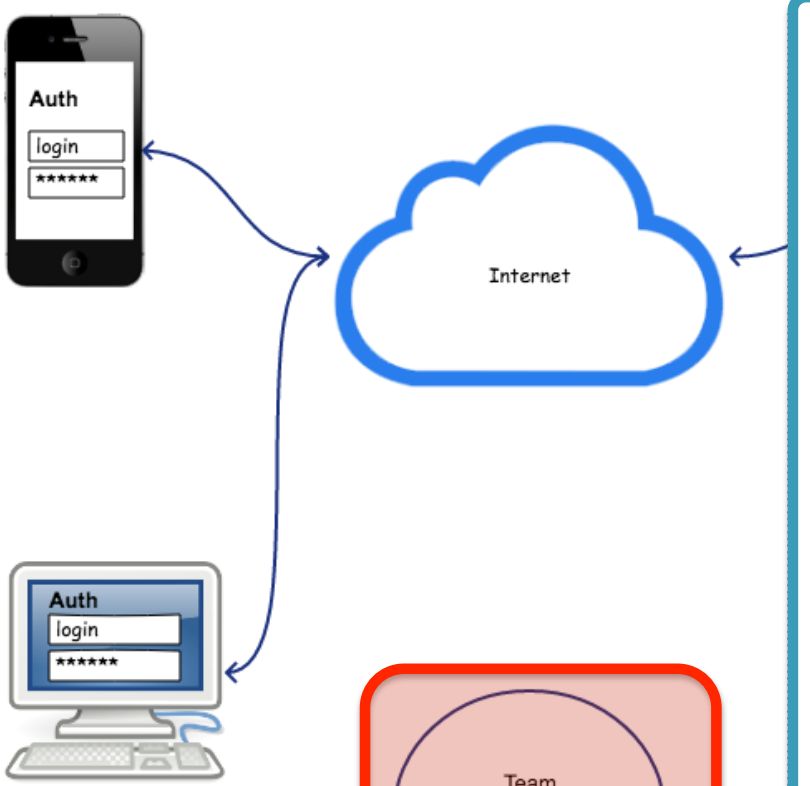


Typical Mistakes: Data Tier

- ❖Non-securing sensitive data (PII - personal identifiable information: Name, Address, Date of Birth, SSN, etc)
- ❖Storing data when you do not need to (i.e. credit card data - very often!)
- ❖Not following the Regulatory Compliance when needed:
- ❖PCI (credit card data)
- ❖HIPAA (medical data)
- ❖GDPR (when operating in EU)
- ❖etc
- ❖Not following right coding standards when communicating with database
- ❖SQL injections possibility
- ❖Physical Server Security
- ❖Other vulnerabilities



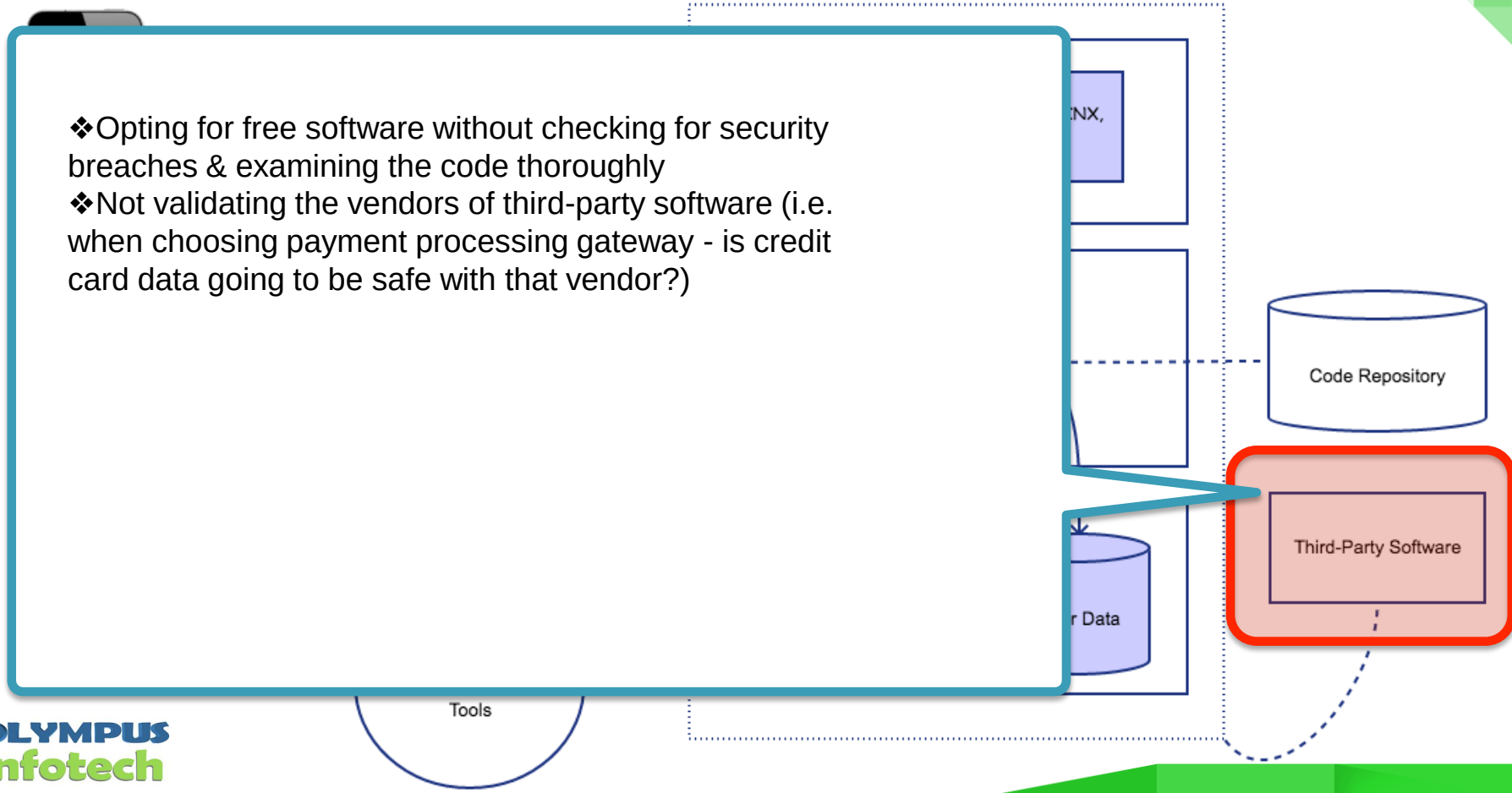
Typical Mistakes: Team Collaboration Tools



- ❖Use of public team collaboration tools by unexperienced users
- ❖Not enough training for the employees
- ❖Accidentally sharing information that is not supposed to (i.e. everyone with the link can open the google doc or DropBox document)
- ❖The users who are not employees any more still have access
- ❖etc

Typical Mistakes: Third-Party Software

❖Opting for free software without checking for security breaches & examining the code thoroughly
❖Not validating the vendors of third-party software (i.e. when choosing payment processing gateway - is credit card data going to be safe with that vendor?)



OLYMPUS Infotech

Resources

❖Common Vulnerabilities and Exposures
➢https://cve.mitre.org/
➢https://nvd.nist.gov/

❖https://www.us-cert.gov/
❖https://www.xcoobee.com/breach-cost-calculator/
❖https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html