Websec-Practicum — SS 21

Web Application Security

Fabian Franzen, Ludwig Peuckert,
Fabian Kilger, and Stephan Krusche

Chair for IT Security / I20
Prof. Dr. Claudia Eckert
Technische Universität München

February 3, 2021

What we offer

- Exploiting buggy Web Appplications in CTF style
- Real world application: Artemis

What you should bring

- Java, Javascript, PHP, SQL
- Necessary? You can learn it on the way if you are disceplined
- **Willingness to work and learn a lot**

Process

Phase I (∼10 weeks):

- "Usual" practical course (weekly meetings and assignments)

Phase II (∼4 weeks):

- Final project (short paper and presentation)

Process — Phase I

- **Teams of two**
- Every week: Introduction to a new topic
  - Submission of solutions until the following week **before** the meeting
  - Private explanation of solution during the meeting

Contents

- Injection vulnerabilities
- XSS, CSRF, sandbox escaping
- Include attacks
- Cryptographic attacks
- Upload attacks
- Configuration vulnerabilities
- Advanced bugs
- ... own suggestions?

Process — Phase II

Final project

- **Real world application** of the knowledge gained
- **Specialisation** in one/two topics
- Security analysis of **Artemis**
- Short paper (about 5 pages)
- **Presentation** (about 15 minutes)
- Details follow when the time has come

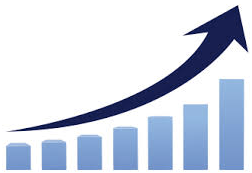
Artemis - interactive learning with individual feedback

Programming exercises

Modeling exercises

Text exercises

Quiz exercises



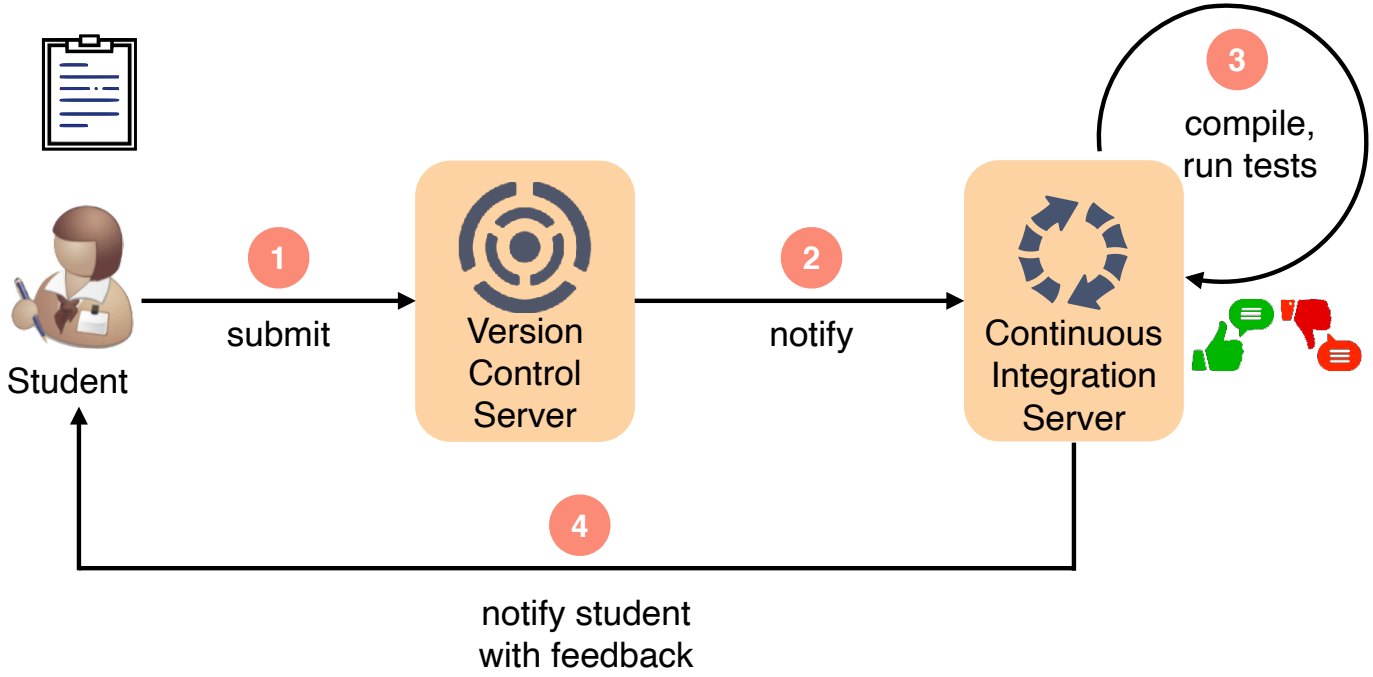
Scalability: handle > 200 submissions per second

Usability: beginners are able to use it

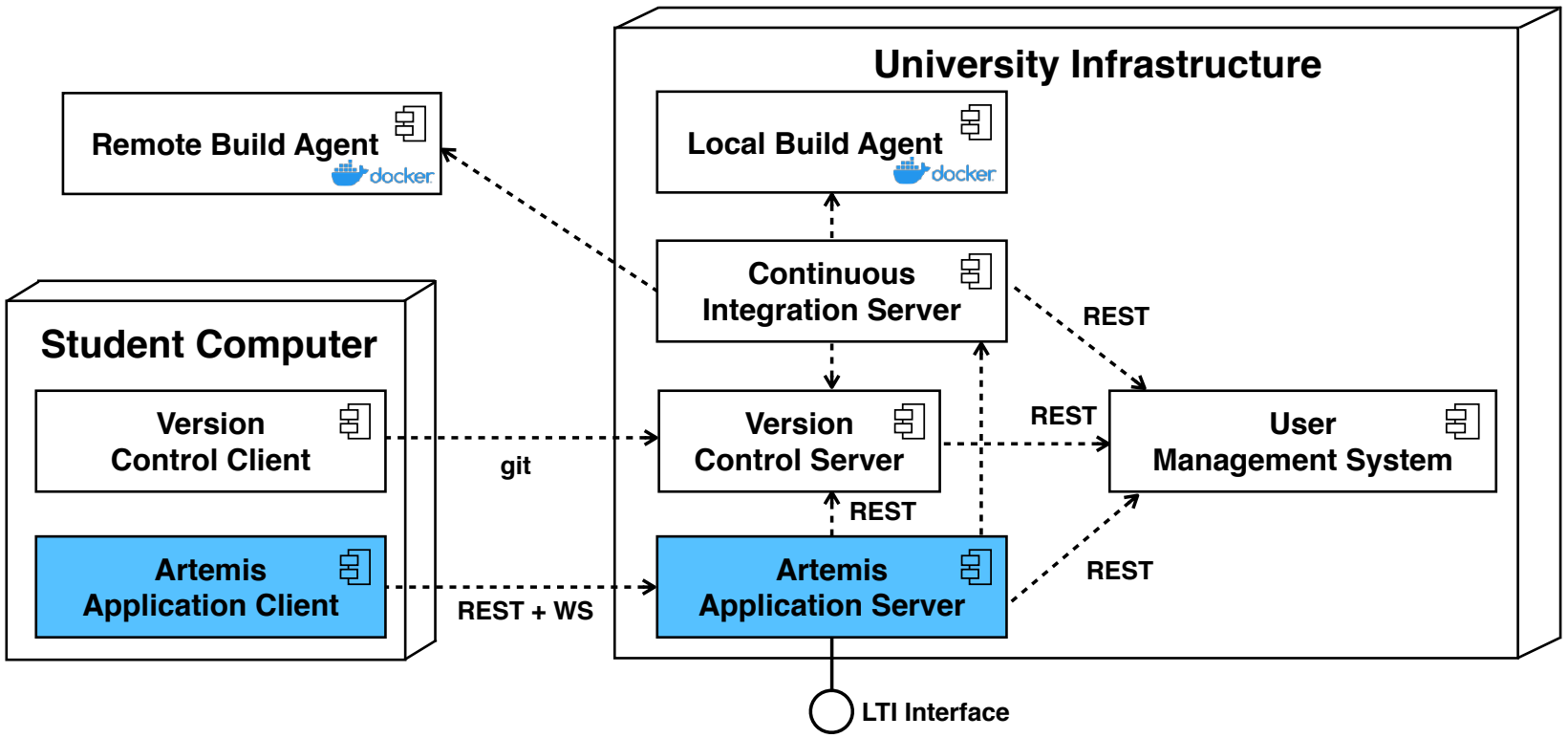
Instant feedback: provide feedback in real-time

Team exercises | Lectures | Presentations | Exam mode | Questions and answers | Learning analytics

Automatic assessment of programming exercises



Artemis architecture



Time and place

When? Montag, 14:00 - 15:30
Where? https://bbb.in.tum.de/lud-r9f-drd

Registration

- Solve the **qualification challenge**
- Visit honeynet.sec.in.tum.de
- Uppon solving you'll receive a flag: **websec{[0-9a-f]*}**
- Submit untill **22.02.2021, 23:59**
- 2^4 slots planned
- **FCFS**, but solving the challange usually is sufficient for joining
- Don't forget to register in the **matching system**!

Why is there a challenge?

- **Option 1: You're already a "l33t" hacker**
  - You will be fast and
  - Will not have problems with this course.
- **Option 2: You are a beginner but determined**
  - You'll probaply take some time, but
  - This will give you a good impression on the course.
- **Option 3: You can't solve the challenge**
  - Tasks in this course may be a fair bit harder then this one, and
  - This course is probably not for you.

Questions?

Questions?