



Web Platform for Comprehensive Penetration Testing

26 April 2022

Willi Lazarov



The need of penetration testing



- The number of users and online services is rapidly increasing.
- With this increase, the number of cyberattacks is also growing.
- A successful cyberattack can cause significant financial losses.
- There is a need to meet compliance (standards, regulations, etc.).
- The world is lacking cybersecurity professionals (approx. 3 million¹).
- The prevention? Penetration testing, but there are issues as well...

¹ According to the latest report by the World Economic Forum (WEF).



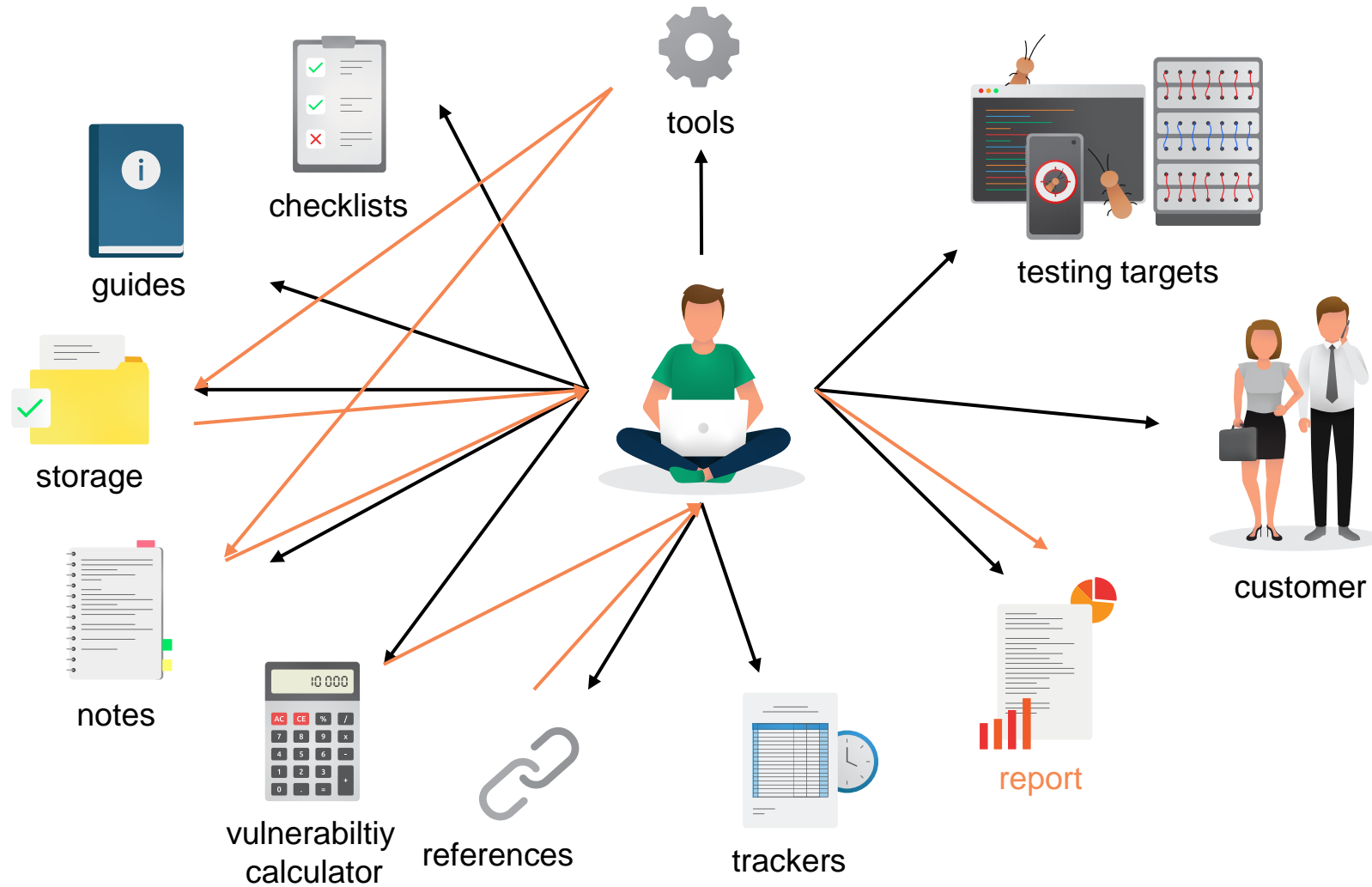
The current state of penetration testing



- Penetration tester needs:
 - advanced knowledge through experience,
 - checklists based on different methodologies,
 - guidelines (tester can't remember everything),
 - (automated) penetration testing tools,
 - software for taking notes and team collaboration,
 - vulnerability scoring system calculator,
 - time (work) tracking software,
 - reporting system.
- All of this makes penetration testing a complex process.

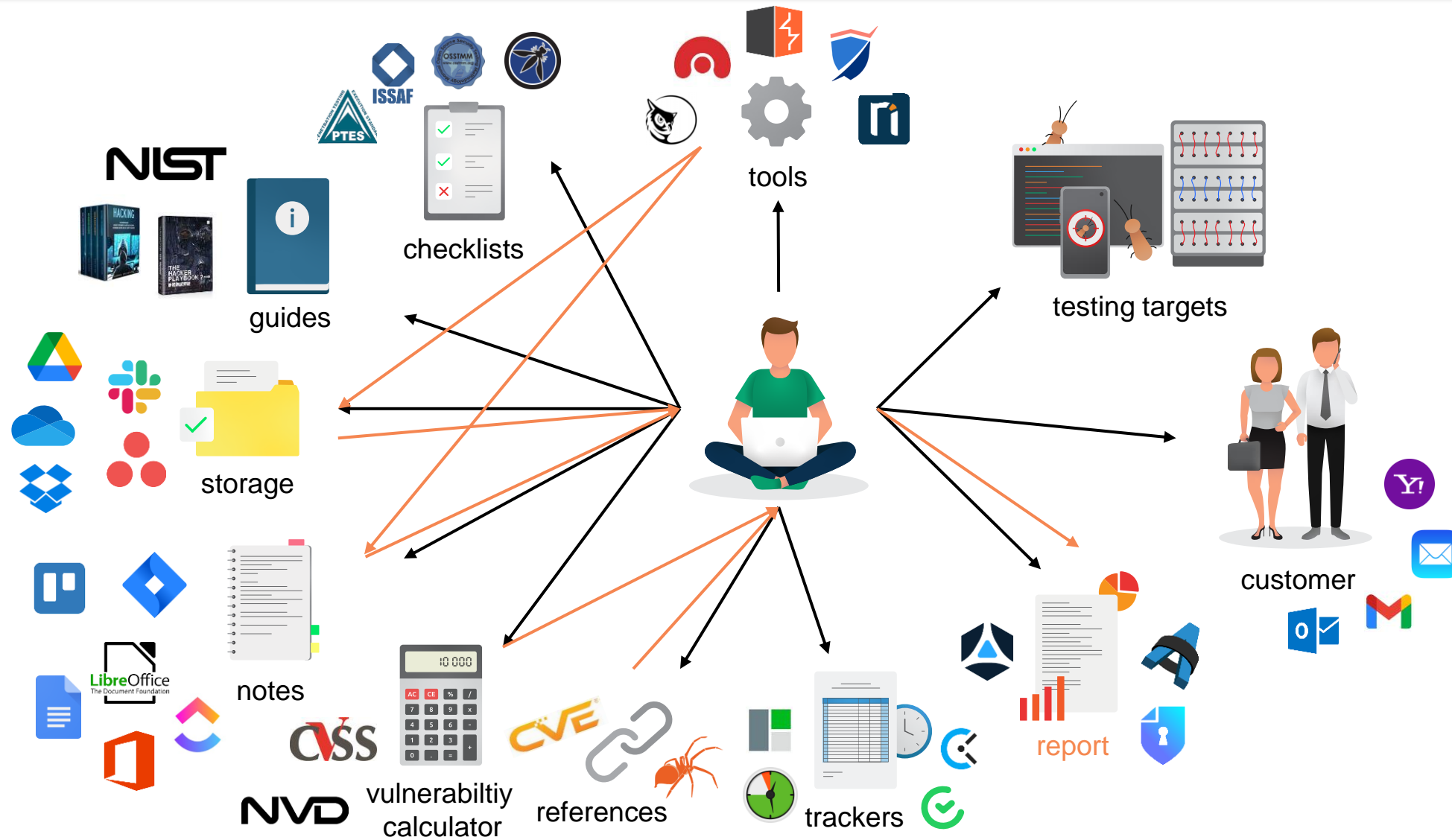


The current state of penetration testing



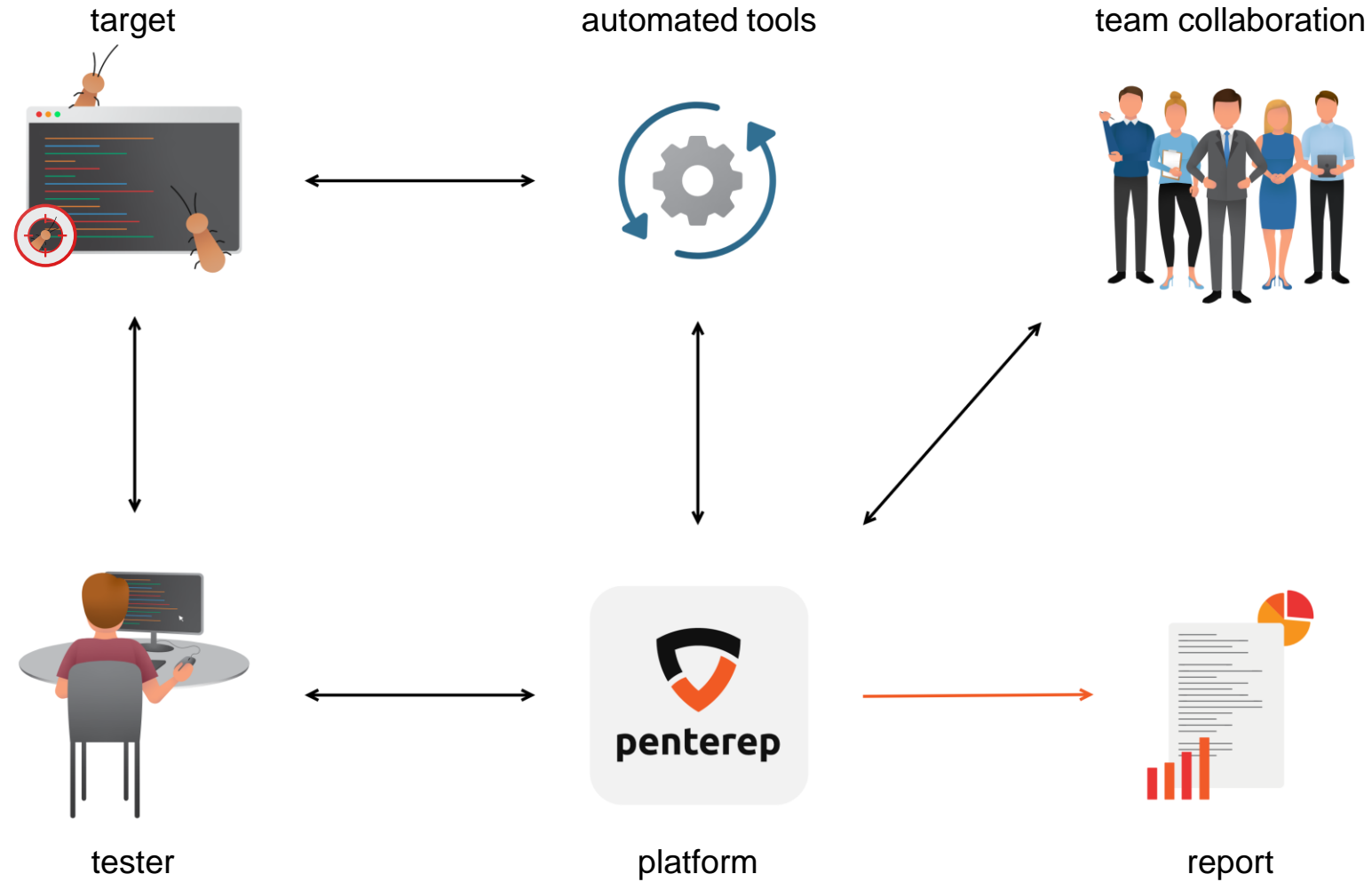


The current state of penetration testing



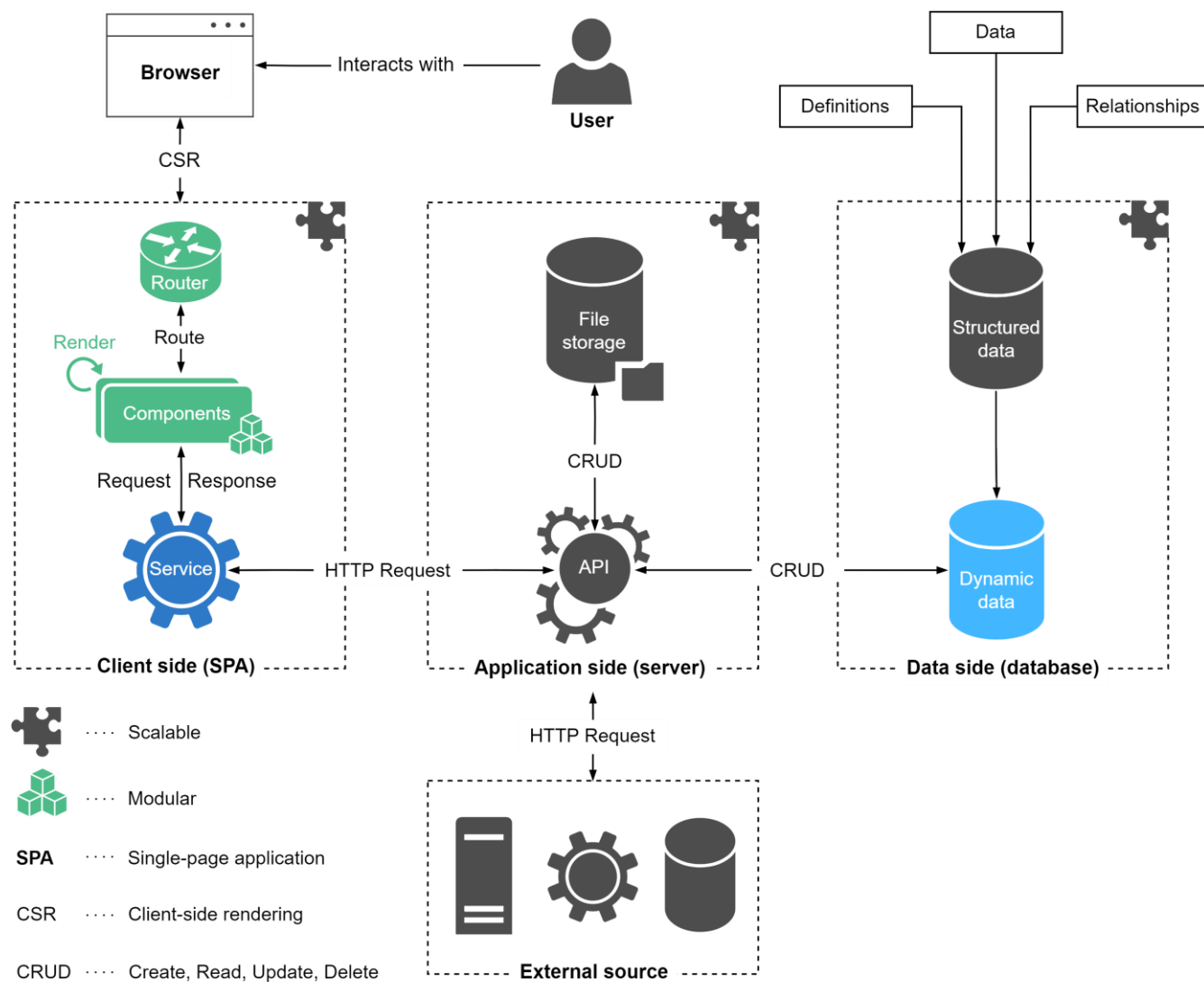


The proposed solution



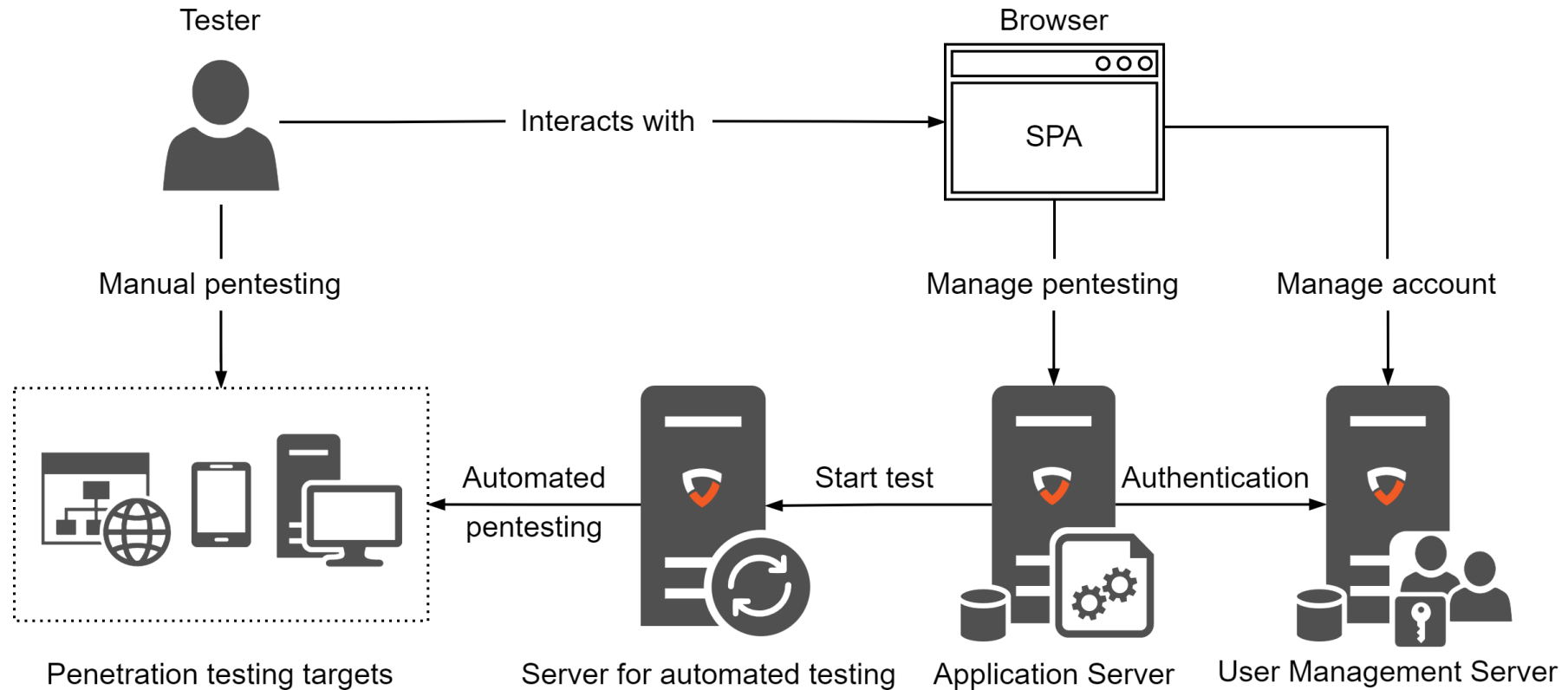


Highly Scalable Model





Production environment





The work behind the solution

Part of the platform	Size
Source code of all parts	14 000 lines
Project repository (GitHub)	1 000 commits
Implemented functions	433 functions
Database – static + dynamic	50 tables
Database – static	14 000 records
Database – dynamic	4 800 000 records

Note: The values in the table have been rounded down.



Live demonstration of the platform

penterep

Willi Lazarov

Brno University of Technology > cyberarena.utko.feec.vutbr.cz

cyberarena.feec.vutbr.cz

Information

Tests

Code↑↓	Task↑↓	State↑↓	Vulnerable↑↓
PTL-WEB-INFO-WSPAT	Check if it is possible to identify the Apache web serve...	✓	✗
PTL-WEB-INFO-LNGEX	Check if it is possible to identify the programming lang...	✓	✗
PTL-WEB-INFO-LNGHP	Check if it is possible to identify the programming lang...	—	□
PTL-WEB-INFO-LNGSE	Check if it is possible to identify the programming lang...	—	□
PTL-WEB-INFO-LNG...	Check if it is possible to identify the PHP programming ...	✓	✗
PTL-WEB-INFO-ANMET	Check if the author of the application can be identified...	✓	□
PTL-WEB-INFO-ANC...	Check if the author of the application can be identified...	✓	□
PTL-WEB-INFO-ANW...	Check if the author of the application can be identified...	✓	✗
PTL-WEB-INFO-DEFLT	Check if the application is set as default on the server	□	□
PTL-WEB-INFO-REDIR	Check if the application redirects the user to another d...	□	□

Brno University of Technology

cyberarena.feec.vutbr.cz

API Endpoint

Authentication

Username and password

SMS code (2FA)

Local storage

PHPSESSID

lang

Session management

Software

Laravel

Vue.js

Ubuntu

Sources

/robots.txt

/index.php

query

/images/

WebSockets

Questions?

Brno University of Technology
Faculty of Electrical Engineering and Communication
Department of Telecommunications

xlazar15@vut.cz