OWASP PHP Security Training System (PSeTS)

Timo Pagel (timo.pagel@owasp.org)

Introduction

In web programming languages PHP has 82% market share [1]. Common developer security training systems focus on the attack of vulnerable web applications. PSeTS provides a didactically oriented system consisting of several units. Every unit is divided in an attack and, more importantly, a **defense part**. Knowledge transfer of the system has to be evaluated.

Problem

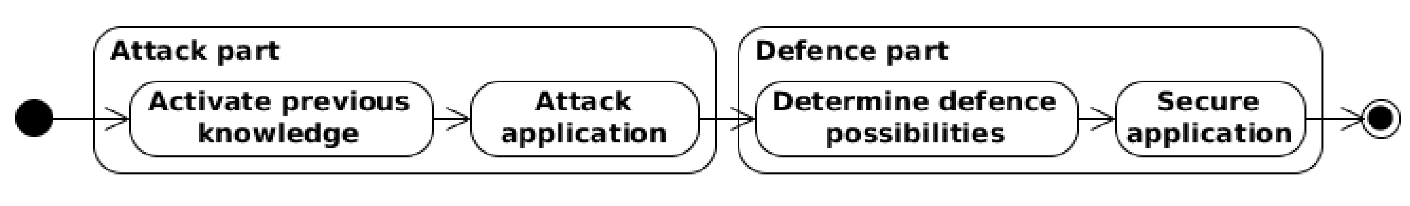
The developer takes the following steps in a unit:

1) Read initial instructions
2) Attack a vulnerable application in the same window
3) Optional: Search for further information in the references

→ **No practical defense part in other systems**

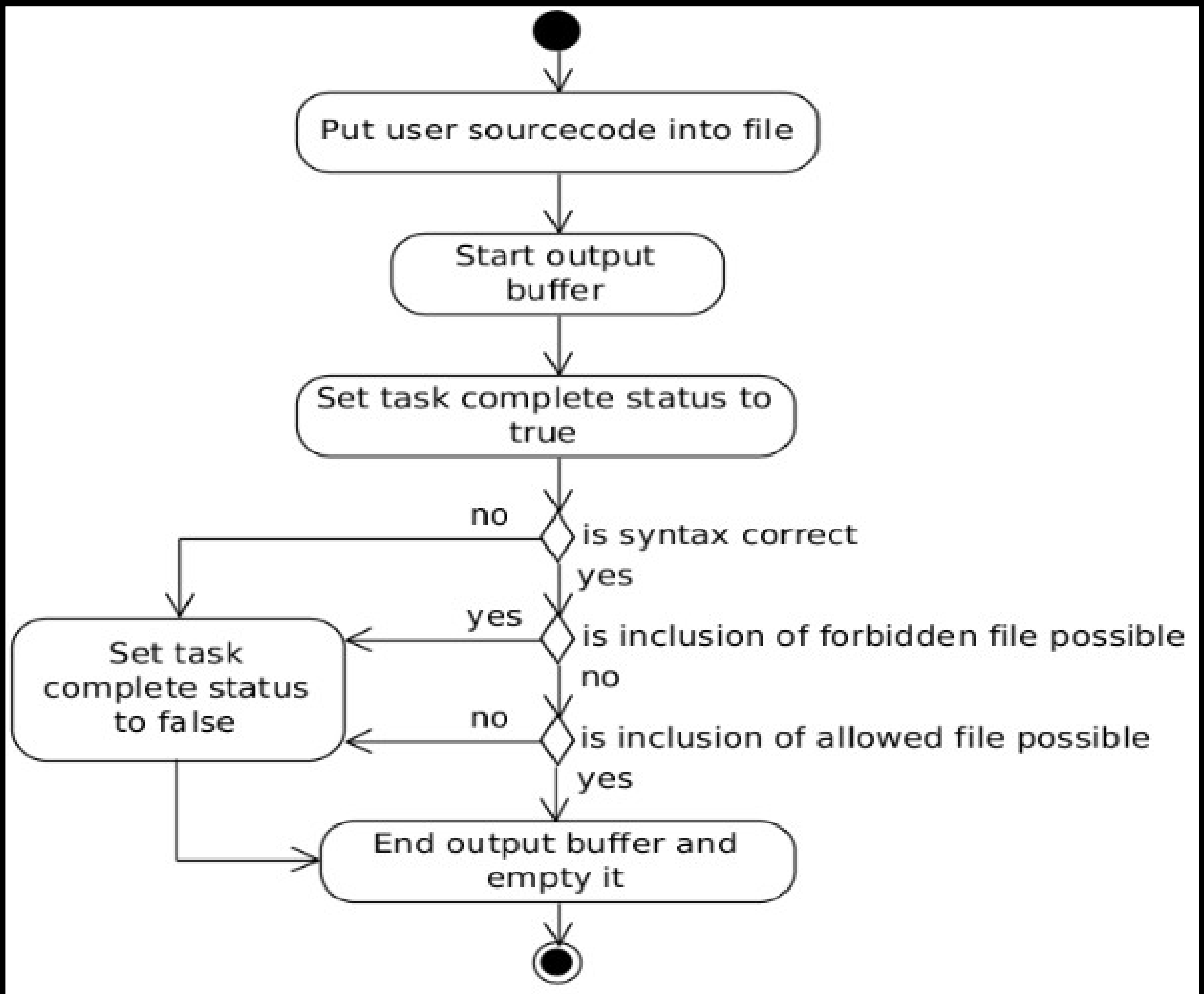
Solution

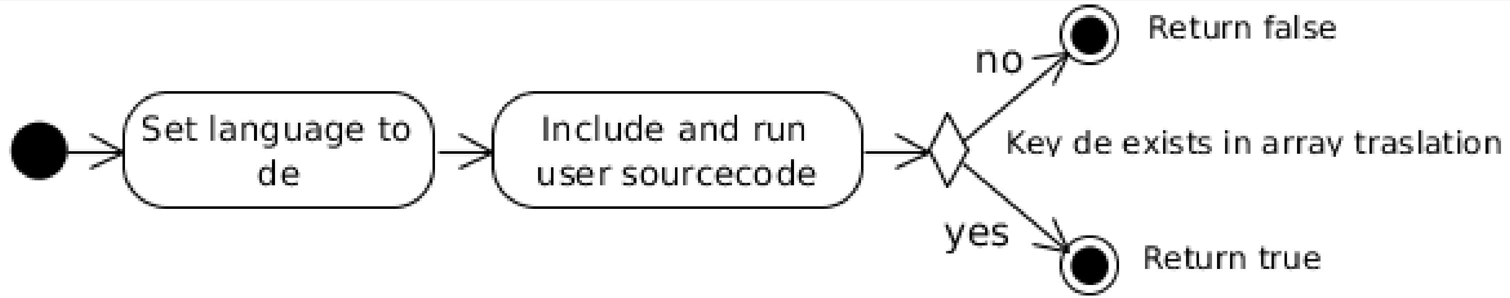
- Developers have to **adopt knowledge** and **apply this knowledge in practical tasks** afterwards
- Use cases
  - Benefit independently at home
  - Used by a teacher in a class room
- Social-learning theories
  - Bundle connected learning content [2, p. 159]
  - Learning content is structured bottom up [3, p. 59]
  - Superfluous learning content is removed [2, p. 159]
- Categories
  - *Authentication and Session Management*
  - *Cross Site Scripting*
  - *Cryptographic Storage*
  - *Direct Object References*
  - *Injections*
- The structure of a unit is shown in the figure below



Technical Implementation

- Guidance Part
  - Leads the developer through the system
  - Category menu, unit menu, information and the task itself
- Unit Part
  - Vulnerable application
  - Validates answers
- Secure the source code
  - **Static checks**: Normalize user's code and compare it
  - **Dynamic checks**: Validates user's code by executing it with different parameters as shown in the figures below


Put user sourcecode into file
Start output buffer
Set task complete status to true
no
is syntax correct
yes
yes
is inclusion of forbidden file possible
no
Set task complete status to false
no
is inclusion of allowed file possible
yes
End output buffer and empty it


Set language to de
Include and run user sourcecode
no
Return false
Key de exists in array traslation
yes
Return true

Evaluation

- *Where*: Interdisciplinary week at the University of Applied Sciences Kiel
- *Who*: A heterogeneous group of 12 developers with different skills in PHP and web security (9 developers left by the end)
- *Target*: Test the skill improvement by PseTS
- *How*: Volunteers have to proof their **knowledge before and after** they use PSeTS
- *Outcome*: Results for the survey category knowledge are shown below
- *Additional Outcome*: The general usage is rated with an arithmetic mean of 2.0, the user interface with 1.74 and the navigation with 2.28

Category	Correct Answer	
	Pre Ø	Post Ø
Input Handling	55.7 %	85.3 %
Output Handling	75.0 %	92.7%
Hashfunction	8.0 %	89.0%

Conclusion

Because a developer has the willingness to learn new things, he will not trick PSeTS to finish a task. Therefore PSeTS is a **perfect addition for a security training** but not usable in a competition. To establish a community, the following tasks have to be done:

Implementation of internationalization to enhance the coverage of PseTS. Introduction of dynamic checks for existing defense tasks. Implementation of unit tests to simplify the introducing phase of PSeTS for developers.

On the other hand, PSeTS could be integrated in a project like OWASP WebGoat, which has a community already.

References

[1] Usage of server-side programming languages for websites. W3Techs, Retrieved December 2014. URL `http://w3techs.com/technologies/overview/programming_language/all`

[2] Michael Kerres. *Multimediale und telemediale Lernumgebungen: Konzeption und Entwicklung*. Oldenbourg Verlag, 2001.

[3] Michael Kerres. *Mediendidaktik: Konzeption und Entwicklung mediengestützter Lernangebote*. Oldenbourg Verlag, 2012.

Keywords

OWASP PSeTS; php security; web application security; e-learning; interactive training system