



Mentoring talent in IT security – A case study

Gábor Pék

Laboratory of Cryptography and System Security (CrySyS Lab)

Budapest University of Technology and Economics

www.crysys.hu

this is joint work with **Levente Buttyán** and **Márk Félegyházi**

The story began



Talent management in IT security



Identification of ***a few students*** with
increased field interest

Careful ***assessment***
(of skill levels)

Understanding ***individual needs***
(for development)

Personalized training
(that unfolds their potential)

Designed for a ***large number of average***
students

(and not for the few outstanding ones)

Insufficient number of hands-on exercises

Lack of personalization

Our talent mentoring program

Based on two key elements



1. CrySyS Student Core
2. avatao platform

Invite-only group of selected students



How to get invited?

1. top performers of CrySyS Security Challenge or
2. having impressive results in semester projects

Core members meet once every week



Discussion of various topics in IT sec.

- presentations of interesting hacks,
- preparation for CTFs – Founding **!SpamAndHex**
- watch talks

The CrySyS Student Core operates as a
community of practice (CoP)



A group of people who
share a concern or passion

Domain

(identity of the community: IT security)

Community

(joint activities and discussions to help each other)

Practice

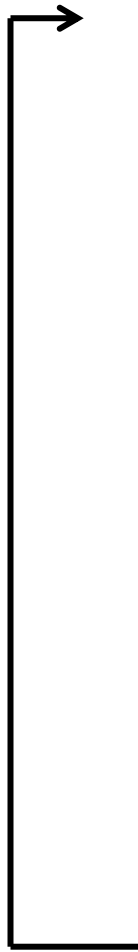
(develop a shared "repertoire of resources": CTFs, tricks, tools)

Initially, the Core was driven by the enthusiasm
of founding members



Later, it became a strategic asset of the
CrySyS Lab

Conditions for Sustainability



Visibility

Bootstrapping

Speeding up

Admission

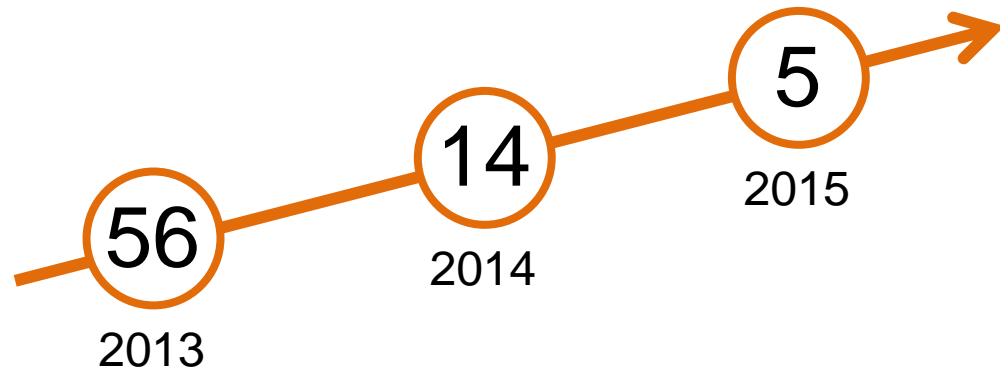
Inclusion

Giving back

Measuring success



DefCon CTF finalist (2015, 2016)



!SpamAndHex after winning iCTF



Challenge: Better inclusion of new members

Newcomers have to catch up



New members should follow a self-directed learning process

dependent → interested → involved → self-directed

Your First Path at avatao

[Path description](#)

[Challenge list](#)

Challenges

Tutorial

[Getting Started](#)

SQL Injection

[Sadness 1](#)

[Sorting Fruits](#)

XSS

[Fancy Tech 1](#)

LFI

[Company Homepage](#)

Secure coding

[Prepare Statements!](#)

Network & Web

[Cookie in PCAP](#)

Buffer Overflow

[FlagSafe](#)

Access Control

[Password Recovery](#)

Puzzle

[Coffee Shop Routers](#)

Challenge details

Sadness 1

by Gábor Szarka

57 100

Skill tags

[Web Security](#)

[PHP](#)

[Offensive](#)

Description

Brainy and his smart friends wrote an "intranet portal",... and then deployed it on the Internet. They did not trust any professional web developers, but developed the whole thing themselves. Well, the result is questionable at best. Although it is a "secure" portal (with password authentication, encrypted passwords, encrypted data storage) it contains a number of amateur mistakes.

In this challenge, you will meet the first version of the portal.

Goal:

Hack the login screen! There is a MySQL database behind the website and the login function is vulnerable to SQL Injection - that means, you can login without password. Check out the recommended readings, it will help you solve the challenge!

Recommended readings

- [OWASP top10](#)
- [PHP Sadness](#)
- [SQLi](#)
- [SQLi Cheat Sheet](#)

Start your environment

Hey there! To start your environment, please click on the button below.

[Start!](#)

High-quality challenges



- originally CTF challenges, now secure coding and more...
- experiment with security tools
- built-in hints and recommended readings
- instant feedback on solutions

Comparison with existing platforms



more help and customization



avatao™

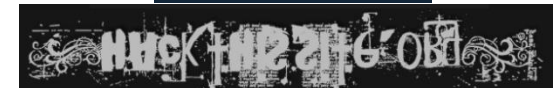


*more difficult
setup/access*



easy setup/access

HACK-ME



less help and customization

Support talent mentoring in the Student Core



- CrySyS Security Bootcamp
- CrySyS Security Challenge

CrySyS Student Core

- Improve sustainability → better inclusion of new members
- Increase value given back to traditional education
- Measure the impact of avatao on learning

avatao

- Easier content creation in avatao
- Introduce tools experimentation and security adventures

(DEFCON 2016) Finals – Thank you

