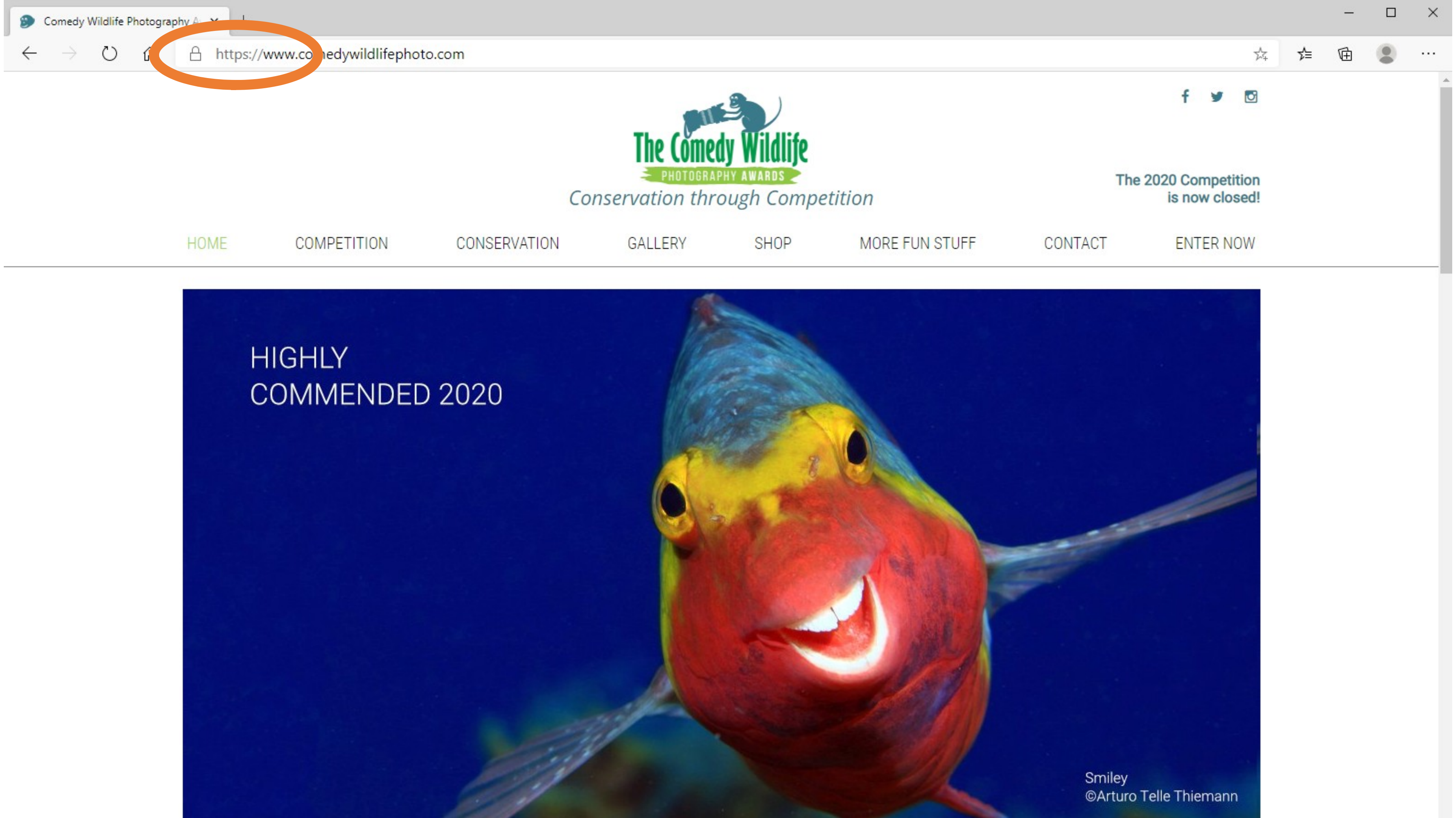
Project Group
TLS Academy

Juraj Somorovsky

Winter Semester 2021/22

Paderborn University

Transport Layer Security (TLS)



The Comedy Wildlife PHOTOGRAPHY AWARDS

Conservation through Competition

The 2020 Competition is now closed!

HIGHLY COMMENDED 2020

Smiley
©Arturo Telle Thiemann

TLS is complex

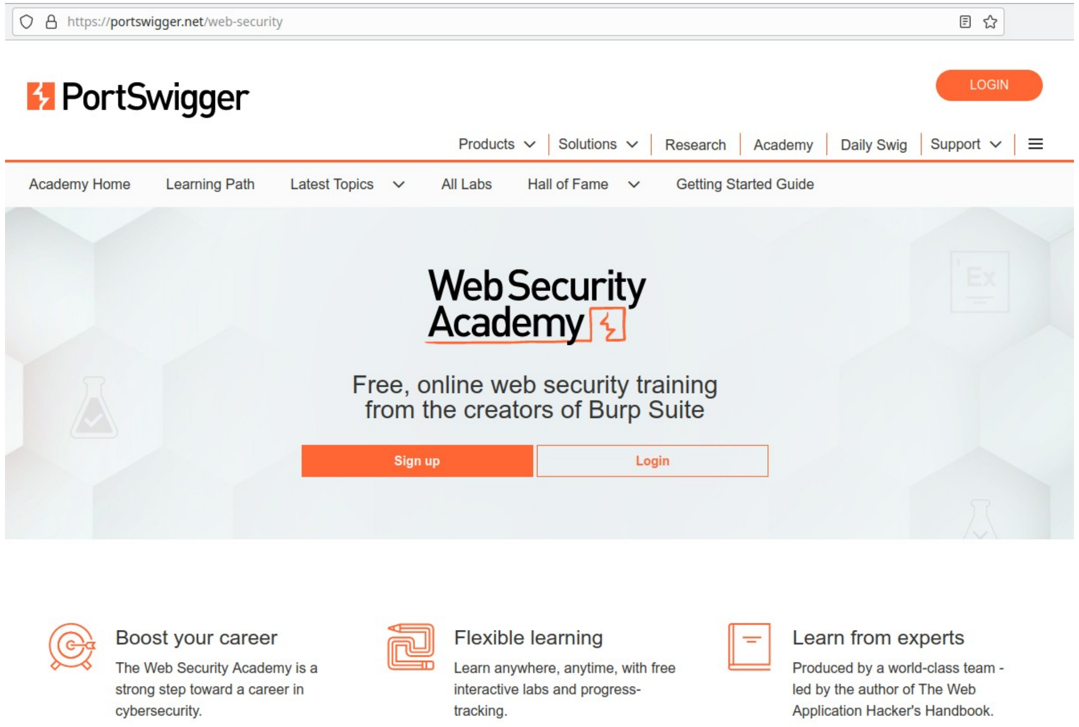
- Many versions, many algorithms, many **attacks** …

How to educate researchers/developers about …

- Vulnerabilities
- Their impact
- Practical exploits
- Secure configuration

© Txema Garcia Laseca / Comedy Wildlife Photography Awards 2019

There is a lot in the are of Web security

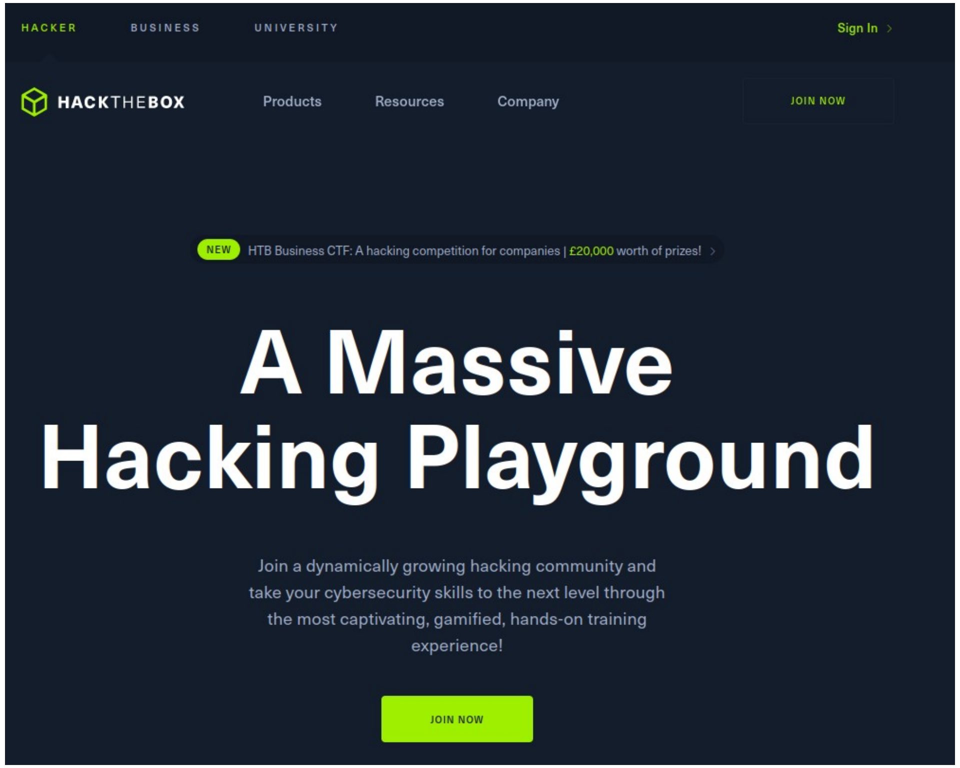


Free, online web security training from the creators of Burp Suite

Boost your career
The Web Security Academy is a strong step toward a career in cybersecurity.

Flexible learning
Learn anywhere, anytime, with free interactive labs and progress-tracking.

Learn from experts
Produced by a world-class team - led by the author of The Web Application Hacker's Handbook.



HTB Business CTF: A hacking competition for companies | £20,000 worth of prizes!

A Massive Hacking Playground

Join a dynamically growing hacking community and take your cybersecurity skills to the next level through the most captivating, gamified, hands-on training experience!

Unfortunately, there is nothing for TLS.

In our lectures …

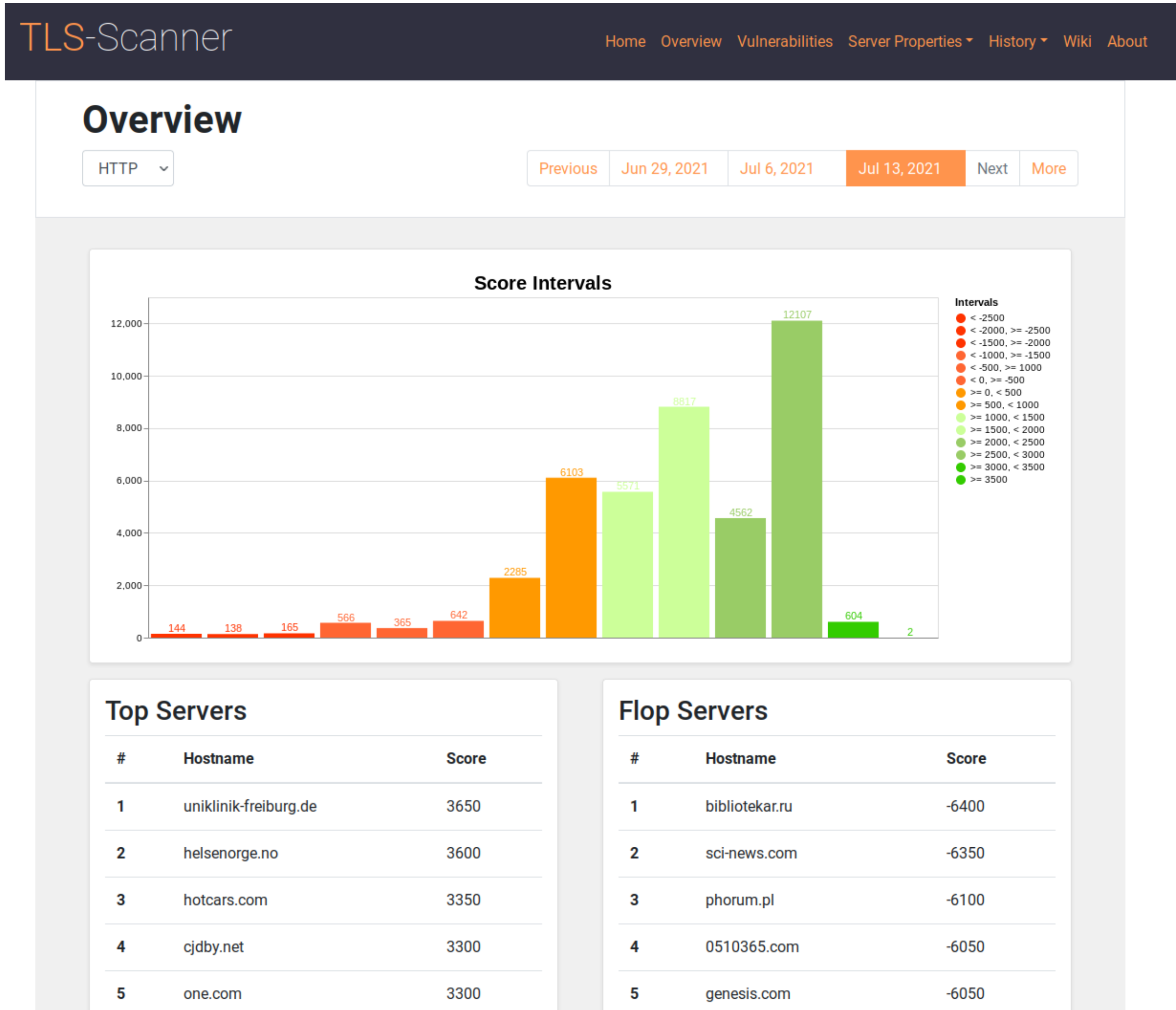
- We provide you some challenges
  - Bleichenbacher's attack
  - DROWN
  - Invalid curve attack

- But there is a lot more …
- Needs to be consolidated and provided to a wider audience

Synergies with our TLS-Attacker PG

- Scan of the TLS ecosystem
- Reports on misconfigurations
- Cool statistics

- Based on TLS-Attacker
  - Open source
  - Flexible attacks and scans
  - https://github.com/tls-attacker/TLS-Attacker



Top Servers

#	Hostname	Score
1	uniklinik-freiburg.de	3650
2	helsenorge.no	3600
3	hotcars.com	3350
4	cjdby.net	3300
5	one.com	3300

Flop Servers

#	Hostname	Score
1	bibliotekar.ru	-6400
2	sci-news.com	-6350
3	phorum.pl	-6100
4	0510365.com	-6050
5	genesis.com	-6050

Goal: Shiny TLS attack education platform

- Collect & write vulnerable clients/servers
  - See https://github.com/tls-attacker/DamnVulnerableOpenSSL
  - Dockerize!
- New attacks
  - Improve TLS-Attacker
  - Write new practical exploits
  - Handbook / tutorials
  - Kali Linux integration
- Develop a website
  - Educate students / developers / researchers
  - Provide comprehensive information
- Provide configuration improvements for the developers

There is more…

What do we offer …

- Deep understanding of cryptographic attacks
- Work on a well-established open source TLS tool
- Implement your ideas
- Be part of the 'competent' and friendly TLS team