07.05.2018, Berlin
Sebastian Neef & Tim Philipp Schäfers
Co-Founders
$> \texttt{whoami}$

Sebastian Neef
@gehaxelt

- MSc student CS @TU Berlin
- Freelancer: IT-Sec / Coder
- CTFs <3

Tim Philipp Schäfers
@TimPhSchaefers

- Author of two info-sec Books
- Junior-Fellow @German Informatics Society
Problem / Idea

• Since 2010: During our A-Levels
  • Fascination for info-sec (creative use of computers)
  • Started looking for webapp bugs & reported them
• Often: no reactions or fixes (!)

• Idea (mid-2012): Internetwache.org
  • To be taken more seriously
  • Wanted to create an understanding of „good hackers“
  • Transparent blog about reported security bugs

• Responsible disclosure / ethical hacking

• Positive feedback from affected companies
White hat hacking

Federal court of justice Germany closes SQL injection

After a short analysis we found a critical SQL injection on the website of the federal court of justice.

This SQL injection was located in a python-script under the subdomain “juris”. The script’s function is to manage documents of the court and make them available to the public.
Bug hunting 🪤

Responsible disclosure programs

- Recognition in hall of fame or swag (stickers, t-shirts, etc.)

Bug bounty programs

- Bounties based on severity ($$)
- ~50$ - ~40,000$
- First to find

Main idea: „Hack us!“
Platforms: BugCrowd, HackerOne, etc.
or direct report

Specific scope
No legal repercussions

07.05.2018 - Internetwache.org
Bounty examples

1500 $ from Facebook

"./" => "../"  
"../" => "../../"  
"/" => "//"

15000 $ from Paypal


2000 $ from Yahoo

3133,7 $ from Google

07.05.2018 - Internetwache.org
Our achievements
Security research / internet scanning

• Scanning the Alexa Top 1M websites
  • High traffic sites have security issues

• 2013: DNS / AXFR (CVE-1999-0532)
  • 132.854 NS
    72.401 affected domains
  • US-CERT Alert: TA15-103A

• 2015: Exposed .git-repositories on webservers
  • ~10k affected websites

• 2018: Exposed .DS_Store
  • ~10k affected websites
Internet scanning: 5 waterworks (DE, IT)

HMIs & PLC exposed to the internet
3x 2016, 1x 2017, 1x 2018
HTTP / no authentication

07.05.2018 - Internetwache.org
Internet scanning: smart tower (IL)

2016: Tel Aviv
Internet scanning: mobile traffic light systems (DE)

- 2016: >30 systems
- 0-byte injection to bypass login (VNC, CVE-2006-2369)
- Online via mobile internet connection (GSM of Telekom)
- In one case: Admin session still active
- Reported to the BSI, the Telekom CERT and the vendor
Internet scanning: Gondola ski lift (AT)

2018: Innsbruck
Media and politics

- Talks on conferences about „hacking“ & „IT-Sec“
- Ongoing reporting about our project:
  - Blog (internetwache.org)
  - Twitter (@internetwache)
  - golem.de
- Collaboration with media (ARD, ZDF, WDR, Spiegel, ZEIT, etc.) to educate the public
- Use of our work and results in the state and EU parliament. Also included in the latest BSI report.

07.05.2018 - Internetwache.org
Community work

• Exchange with the info-sec community (social media, Blog, conferences, etc.)

• 2016: Internetwache Jeopardy CTF
  • 30 Challenges (5x Misc, 5x Web, 5x Rev, 5x Crypto, 5x Code, 5x Exploit)
  • 36 hours
  • 650 participating teams (worldwide)
  • 38 teams solved all challenges
  • HTTP Requests: 2,336,957
  • Traffic: ~20 GB
  • Costs: 20$ for hosting on DigitalOcean
  • Challenges and setup is on GitHub

• CTFs are a fun (frustrating?) way to learn new things!
Conclusion

• Hacking is fun! Always wear your white hat ;)
• Keep on hacking or start to learn it 😊

• Responsible disclosure and bug bounty programs are cool
• Share your knowledge / tools with the community
• Join a CTF team and play CTFs!

• Believe in your projects and push them.
Thank you for your attention.

Questions? / Ideas?

Internetwache.org
contact@internetwache.org