clarified security
- we break security to bring clarity -

Hope management

in web applications from pentester's point of view

Elar Lang
linkedin.com/in/elarlang
25th October 2014 / Agile Saturday

Elar Lang

- Work
  - 2002 – 2011 – web app developer (LAMP)
  - 2012 - .... - Clarified Security OÜ
    - Lector and author of web application security trainings
      - This year ~600h trainings, total ~1100h
    - GWAPT (GIAC Web Application Penetration Tester)

- Education
  - Diploma: „PHP Application Layer Attacks – mechanisms and protection“
  - Masters thesis: „Web Application Security – hands-on training“

Why and what

- Why
  - As pen-tester, lecturer, ex-developer
  - I see a lot of
    - expectations (without reason)
    - assumptions (wihtout reason)
    - blind trust (people, systems, … especially systems)

- „Hope management”
  - It's just „let's hope nothing bad will happen”

Previously…

- September
  - „Fappening" - celebrity pictures leaked, at least 4 times (iCloud)
  - ShellShock – how many systems use bash?
- October
  - „Snappening" - another picture/video leakage
  - Nearly 7 Million Dropbox Account Passwords Leaked (3rd party)
  - Drupal SQLi

Pa$$w0rd5

Where are your passwords stored?

- Do you trust those servers?


ONE DOES NOT SIMPLY
REMEMBER PASSWORDS TO ALL THE SERVERS
quickmeme.com

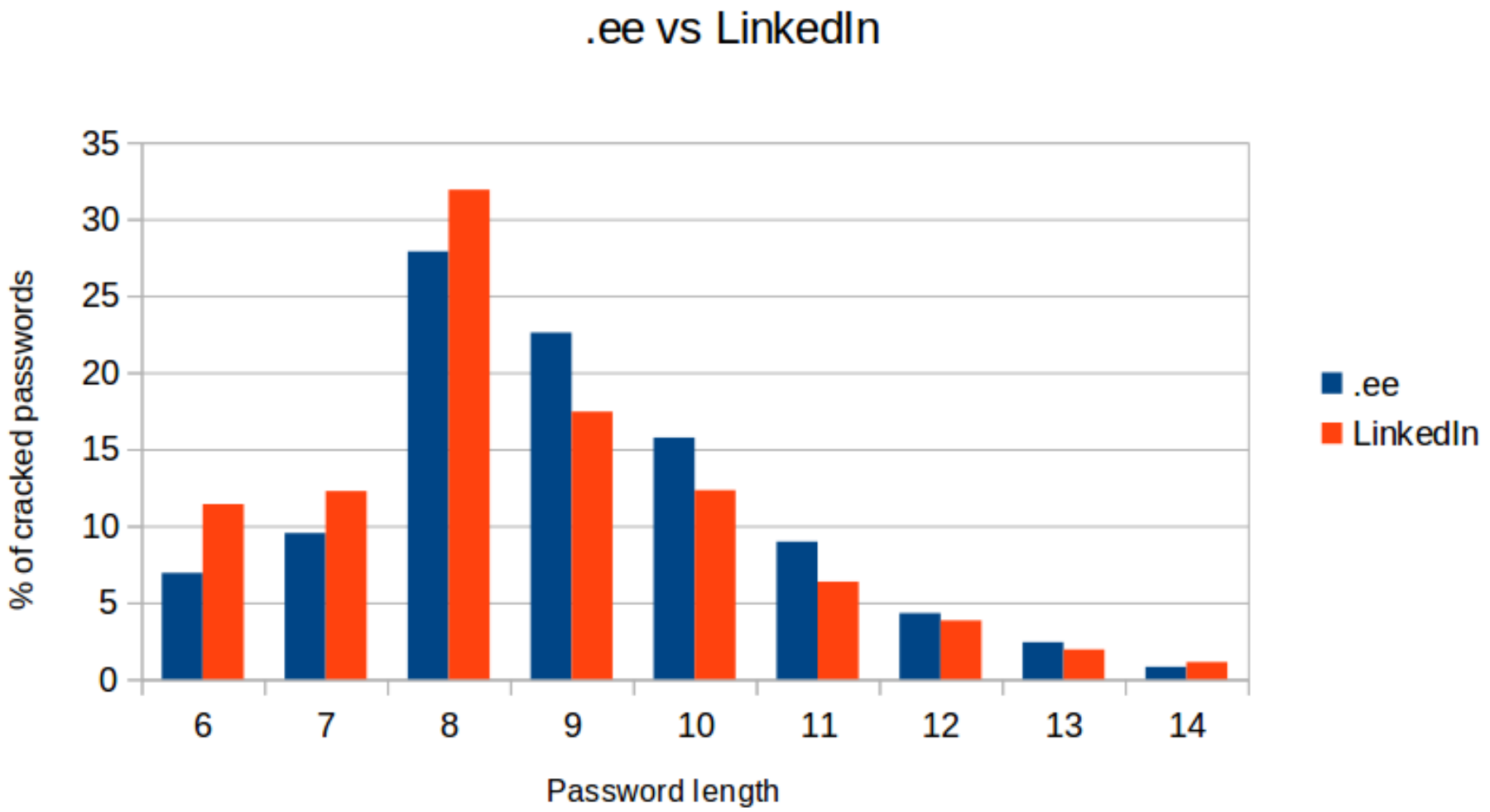
Those passwords...

- Blind trust – system vs human
  - Behind every system there is a human
- System owner, developers can get your password
  - Even if it's stored in secure way
- Blind trust to big systems – „they are secure!”
  - 2012 – LinkedIn, 6.5 million sha1 hashes
  - 2013 – Adobe, ~150 million users' data
  - 2014 – Ebay, ~110 million users' data

.ee vs LinkedIn

- *anonymous*.ee
  - Year 2014
  - Rules
    - Capital + lower + min 6
  - Cracked 75%
  - Average length 8.95
  - Length >= 9 56%
  - Patterns
    - Aa1 81%
    - *1 86%
- LinkedIn
  - Year 2012
  - Rules
    - Min 6
  - Cracked x%
  - Average length 8.62
  - Length >= 9 44%
  - Patterns
    - Aa1 7%
    - *1 52%

.ee vs LinkedIn

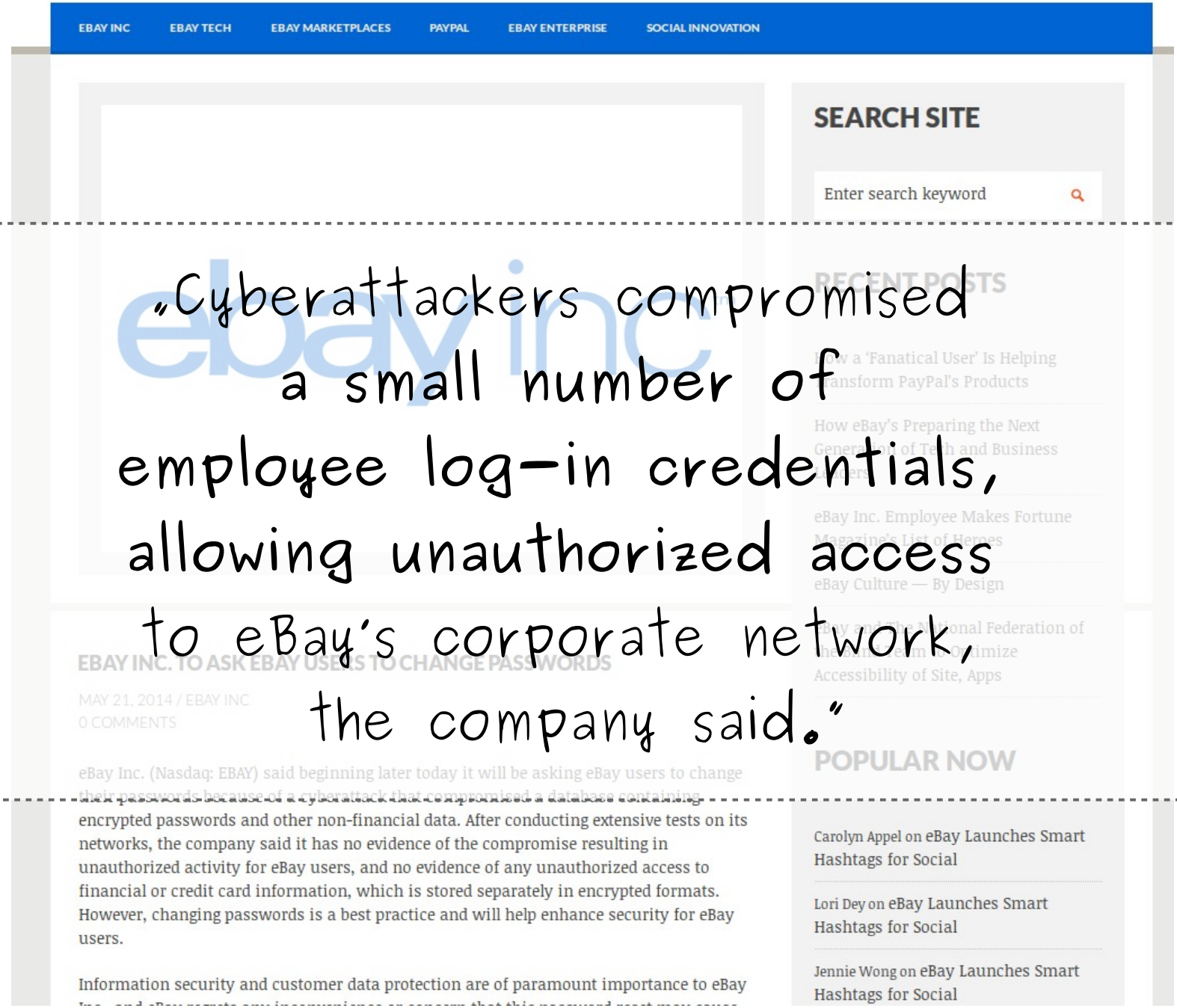


Typical .ee password

- Passwords in one .ee site
  - 30% of passwords on my laptop in 3min
    - Is your password in first 3min?
  - 75% cracked
    - Name + Digit (year)
      - Names – Schools, sport events, names stat
    - Dictionary word + digit
      - Language instutute
    - Already hacked passwords from other sites
      - LinkedIn, ***

Typical password

- Rules
  - At least 6-8 symbols long
  - At least one uppercase letter
  - At least one lower case letter
    - At least one number
      - At least one symbol
- Based on rules they are strong:
  - „Firstname2010”
  - „Parool123” (Password123)
  - „Kalamaja666” (fish house)



„Cyberattackers compromised a small number of employee log-in credentials, allowing unauthorized access to eBay's corporate network, the company said."

Hope

- You hope that
  - No one will guess your password
    - What if it's stored as plain-text and site got hacked?
  - Other users (your employees) use strong password
    - Why should they? It's hard to remember ...
    - Even if they do, it's enough when one of those sites got hacked


DEVELOPERS
memegenerator.net

Are developers guilty?

- Typical reaction when security problem appears
  - „Developers are stupid, idiots, …”
    - Because they wrote the code
- Team management problem
  - Were security tests planned?
  - Was analysis done?
  - Were developers trained?
    - Do they have time to learn something?
    - How experienced are they?
    - Too much expectations on juniors

Training developers is expencive?

Testing your own code

Developers

- „XSS, SQLi, CSRF, session hijacking, cookies”
  - Still typical 10 year old problems
- „I know it all!”
  - Some knoledge make you feel like you know it... but you don't
  - How developer can say to his boss, that he doesn't know something?
- „It's not something critical, just alert box”
  - Manager also trusts this
- “I have never thought that way”
  - Mindset for builing, not breaking
- „My framework is secure and do security for me”

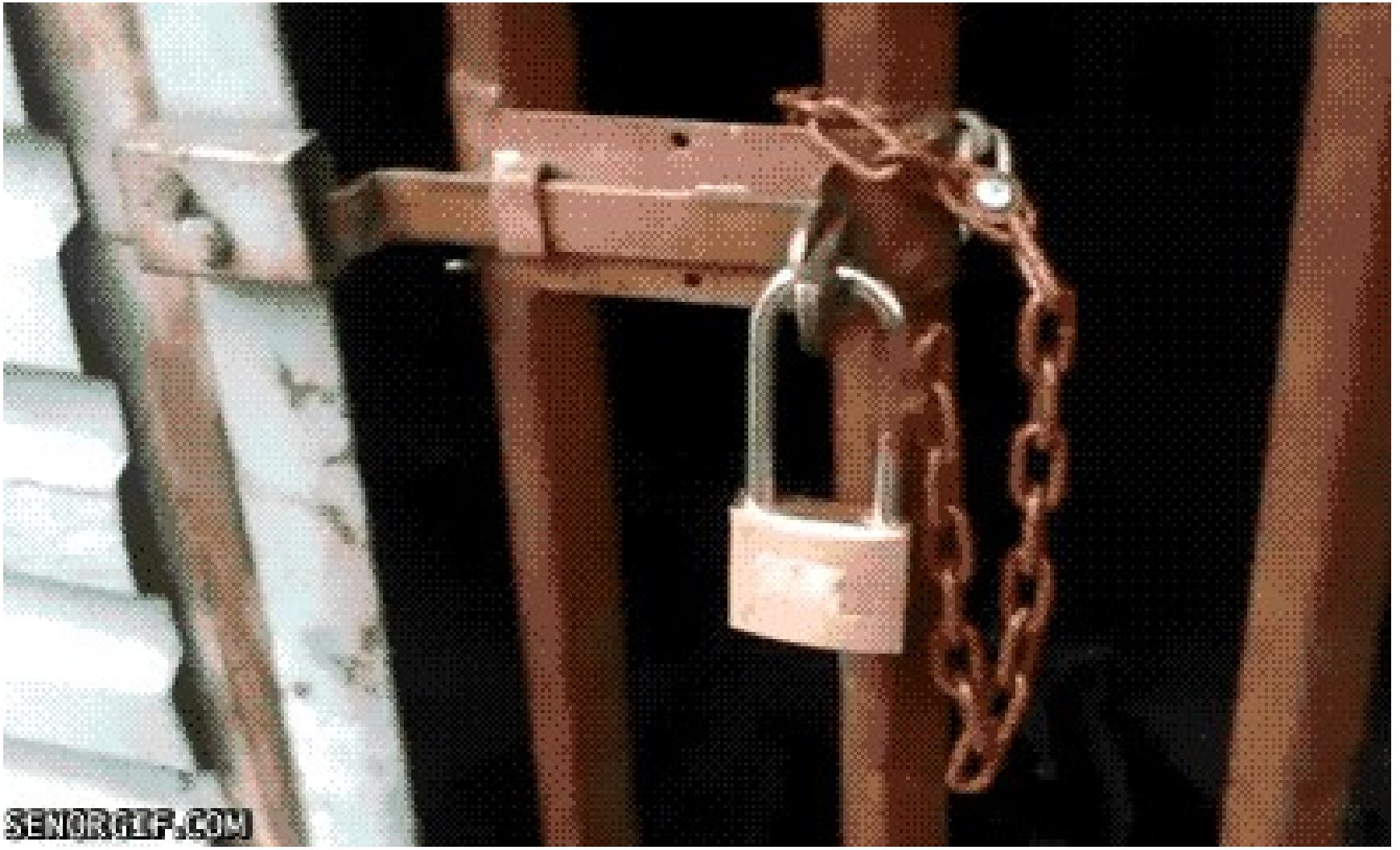
What you order is what you get

- The only or the main criteria is the price
  - Cheapest offer wins
  - Softare owner hopes and expects that security is there by default
- Developer-company
  - Security wasn't ordered
  - Security is expensive!
- Who is guilty?
  - Both!
  - Security ABC is MUST HAVE

What you order is what you get

- „After putting OWASP ASVS to tender, offer increased more than 50%”
  - By default … you get really non-secure solution (?)
  - … or it was nice trick to ask extra-money

Seems secure



Seems secure

- As a customer you should know
  - Who really developed your software before putting your critical data and business there
  - What (3rd party) components are there
    - What problems they have had? Are those fixed?
  - Does anyone else have keys to your doors?

- Widespread systems in use
  - It should be secure, because SO many sites use it

Keeping it up and secure

Known vulnerabilities

- Old software in use
  - With known vulnerabilities
  - Just with Google query…
  - Exploit-scripts are ready to use
    - No technical knowledge needed
    - Youtube and „Monkey see, monkey do”
- Just a week ago I reported to cert.ee about „few sites” with SQLi
  - Few == ?

The Scope

- „System”
  - Operation system +all services
    - *ShellShock*
  - Web Server +all modules/services
  - Programming language +all modules
  - Framework +all components/modules
    - *Drupal SQLi*
  - Application

- For attacker… one security hole is enough

ShellShock

- „Since September 1989”
- CVE-2014-6271 (initial)
  - At least 5 similar problems found (also from patches)

- Demo
  - Writing PoC file to the system

Drupal SQLi

- CVE-2014-3704
- Drupal core 7.0 – 7.31

- Demo
  - How to add „Admin user”

http://seclists.org/fulldisclosure/2014/Oct/75

„If we have not been hacked so far, why to check those old systems…."

Need for security test?

- I don't need!
  - „This is not critical system”
  - „This have been in internet 10 years, no-one have hacked it”
- I used scanner, it didn't find any vulnerabilities
  - „So, it's secure!”
- How to validate security testers?
  - Automated, manual

Conclusions

- We hope that passwords are safe
  - But they are not
- We hope that developers are security specialists
  - But (usually) they are not
- We hope that no one will hack us
  - If it's not done already, it's just a question of time
- We hope nothing bad will happen…
  - But…
- Hope less (otherwise you are hopeless), check more!

Workplace for you?

Thank you!

(Questions?)

Clarified Security OÜ
http://www.clarifiedsecurity.com/

Elar Lang
elar@clarifiedsecurity.com
https://linkedin.com/in/elarlang

clarified security
- we break security to bring clarity -

„What we can break for you?"

http://www.linkedin.com/company/clarified-security-o-/webapp-security-was-training-from-the-attacker-s-viewpoint-hands-on-4-days-1609978/product?trk=biz_product

https://www.facebook.com/pages/Clarified-Security/301801776551016

Clarified Security OÜ - trainings

- Hands-On Hacking
- Web Application Security
  - Client-Side Module
  - Server-Side Module
- Secure Logging

http://clarifiedsecurity.com/trainings/