



OWASP
Open Web Application
Security Project

Security Awareness - A Hackers Mindset

Martin Knobloch

Email: martin.knobloch@owasp.org

Twitter: <https://twitter.com/knoblochmartin>

/whoami



From developer to security specialist:

- +10 years developer experience

- +10 years information security experience

OWASP:

- OWASP Netherlands, Chapter Leader

- OWASP Global Foundation, Member of the BoD

Micro Focus:

- Global AppSec Strategist at Fortify PM

Contact:

martin.knobloch@microfocus.com

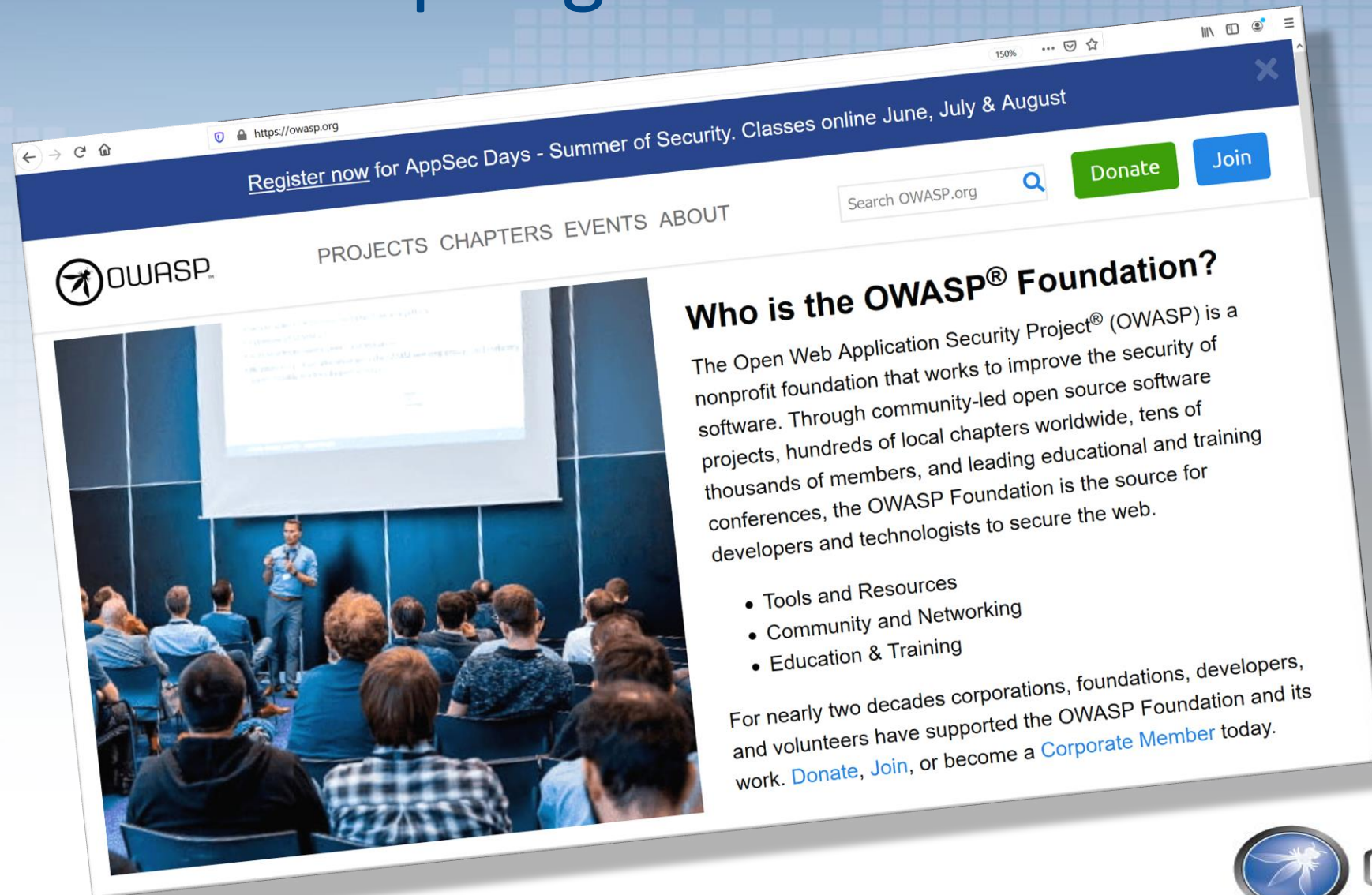
martin.knobloch@owasp.org

<https://twitter.com/knoblochmartin>

<https://www.linkedin.com/in/martin-knobloch>

<https://xing.to/knoblochmartin>

www.owasp.org



<https://owasp.org/>

OWASP Mission

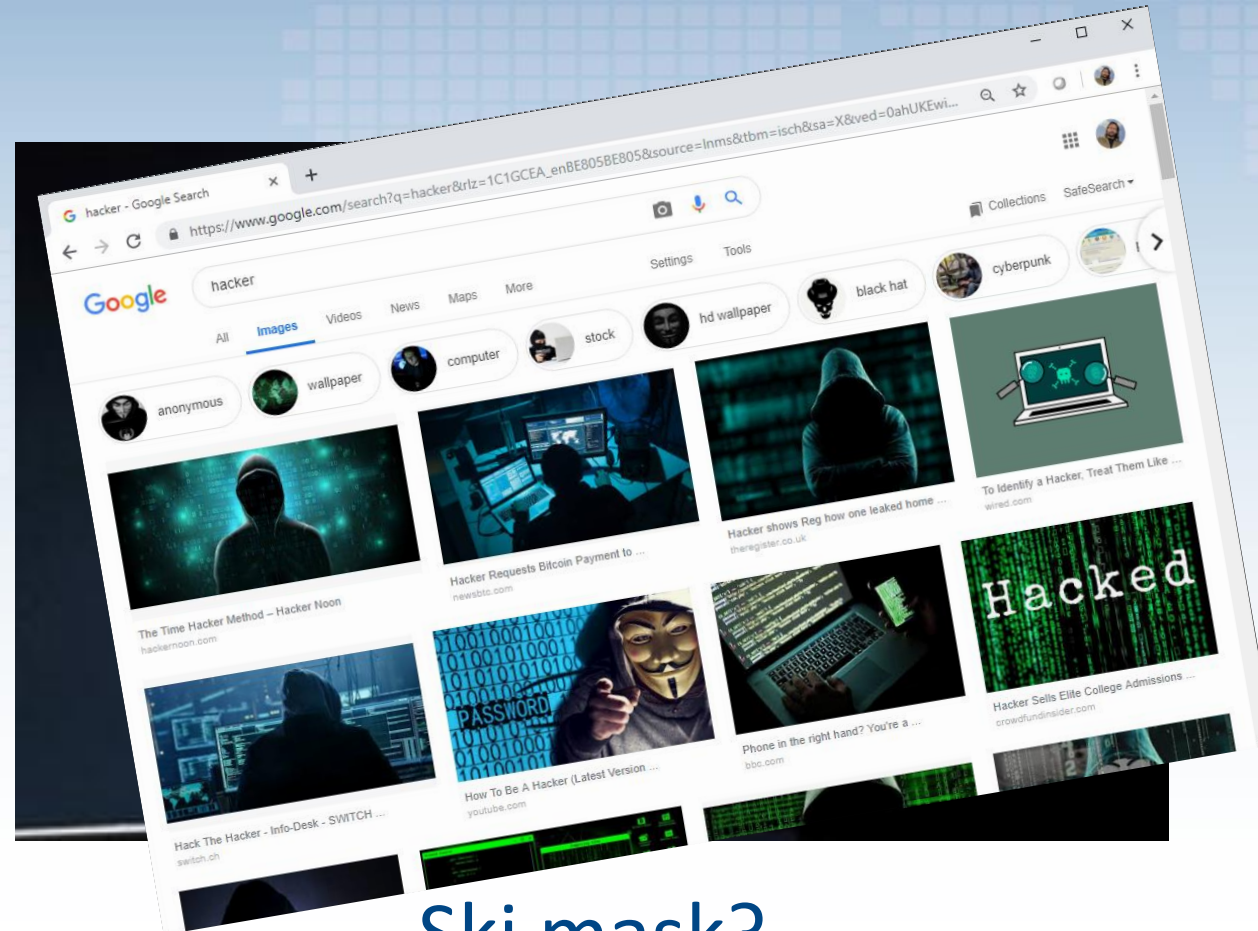
- to make application security "visible," so that people and organizations can make informed decisions about application security risks



OWASP Top 10 - 2013	➔	OWASP Top 10 - 2017
A1 – Injection	➔	A1:2017-Injection
A2 – Broken Authentication and Session Management	➔	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	➡	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	➡	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	➔	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]



What (not) is a hacker



Ski mask?

What (not) is a hacker



Hoodie? ..only if functional!

Disclaimer



Disclaimer



Physics



(Defying) Physics?



Bending the reality



Expectation management



Obvious?



(Barbra) Streisand Effect



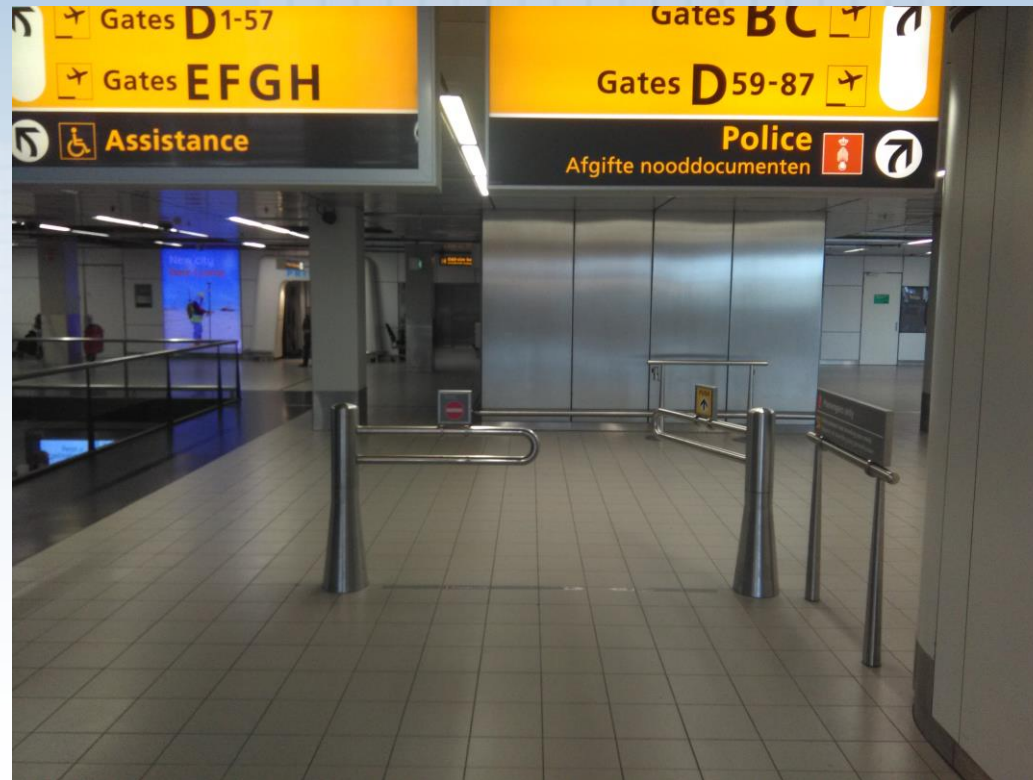
Intention?



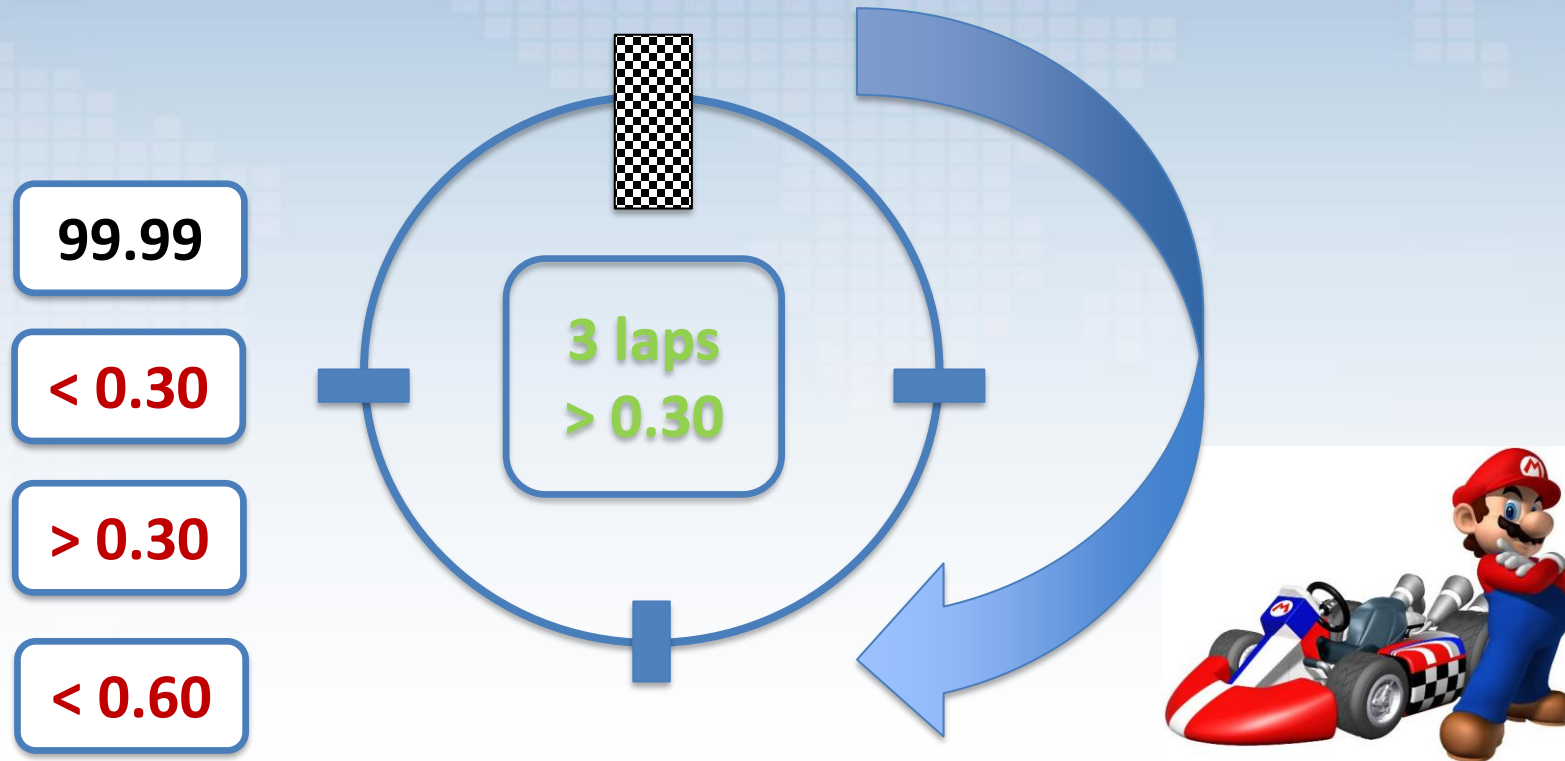
Intention?



Intuitive



Flaw vs Bug



Reward



The gain, doesn't has to be money!

The victim



Crime scene investigation board



Treasure trail



How to achieve the goal?

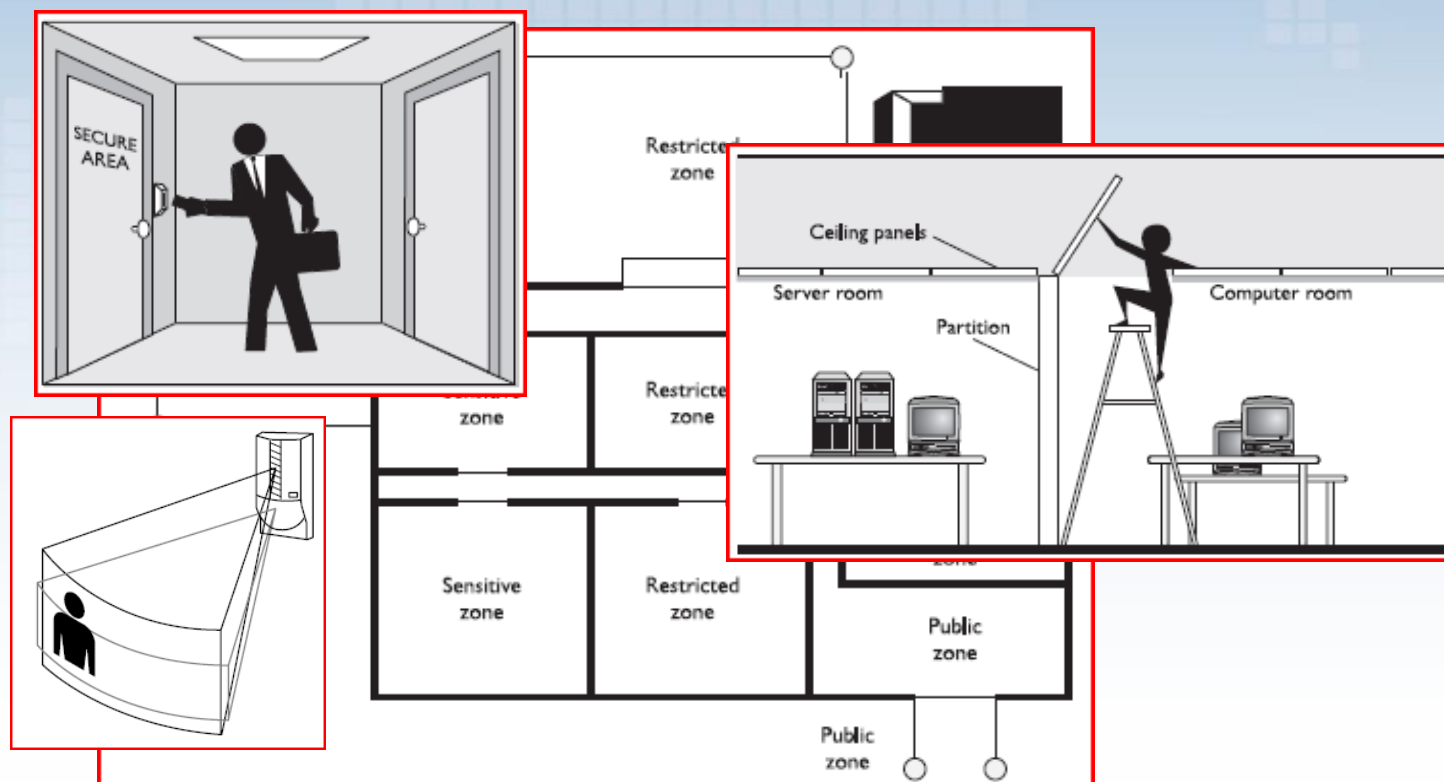
The team



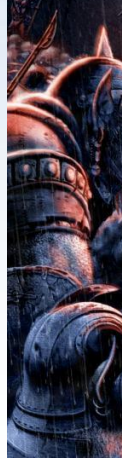
The plan



Imagine a building...

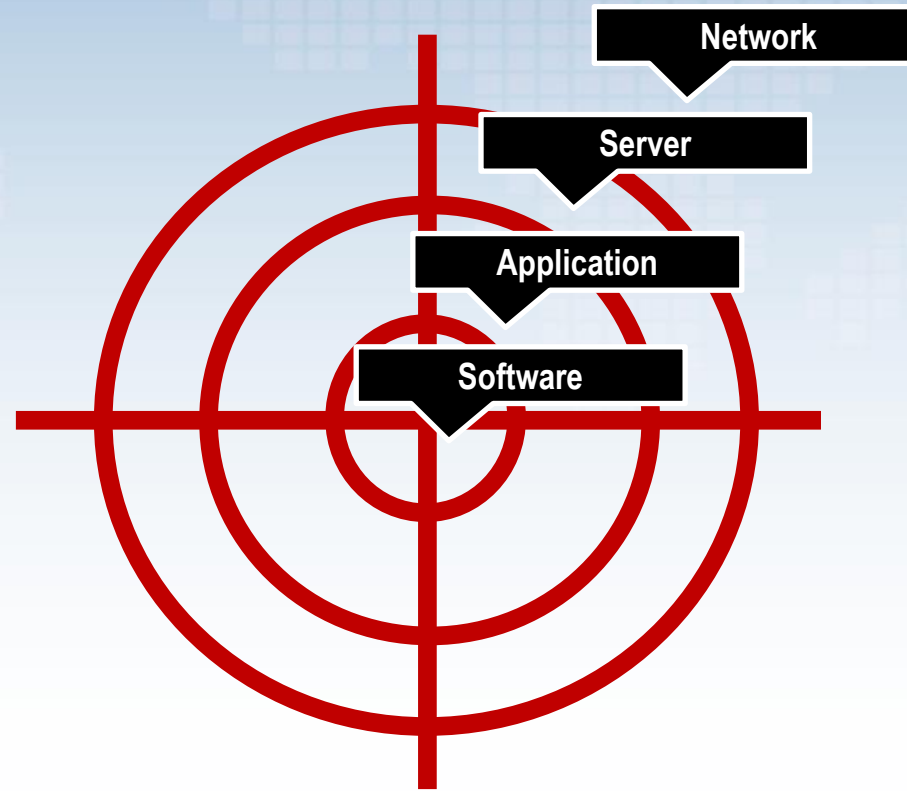


Front door / Back door

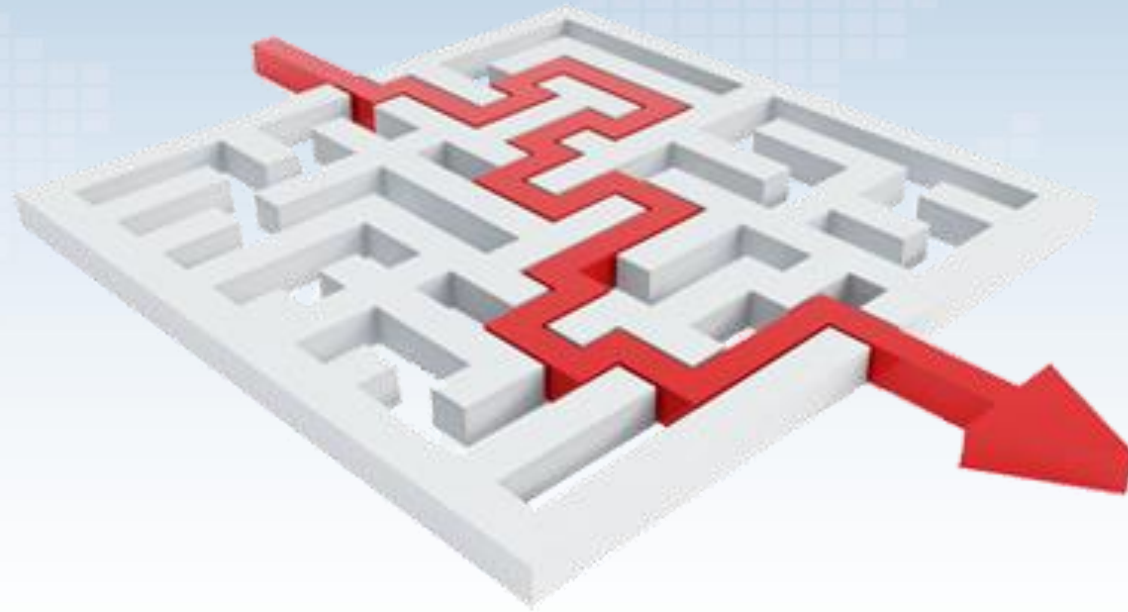


OWASP
Open Web Application
Security Project

scope = scope + 1



Path



Basics

Input validation



Output handling

What could go wrong



Ever seen this?

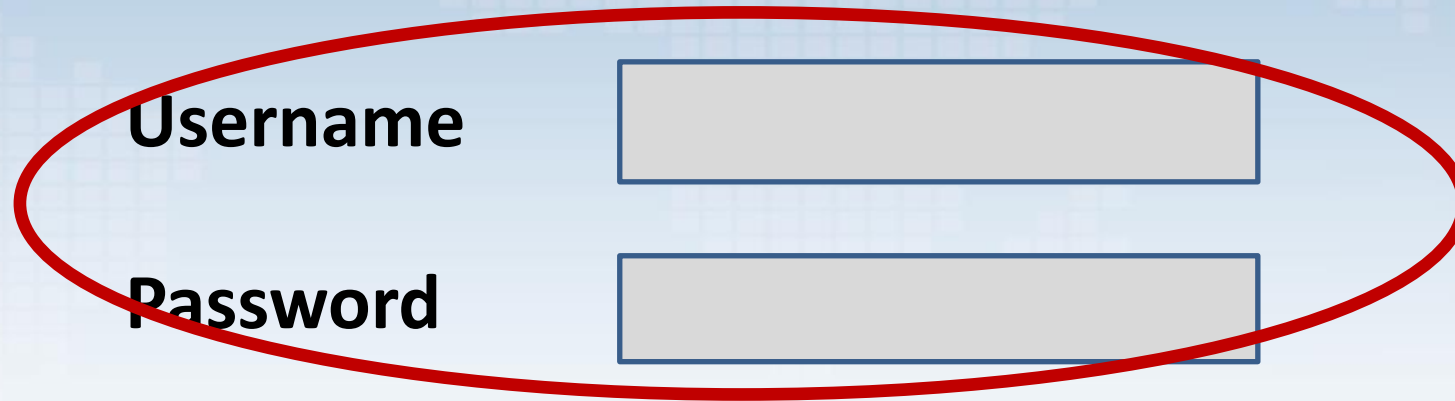
Username

Password

password forgotten link

Create account

Ever seen this?

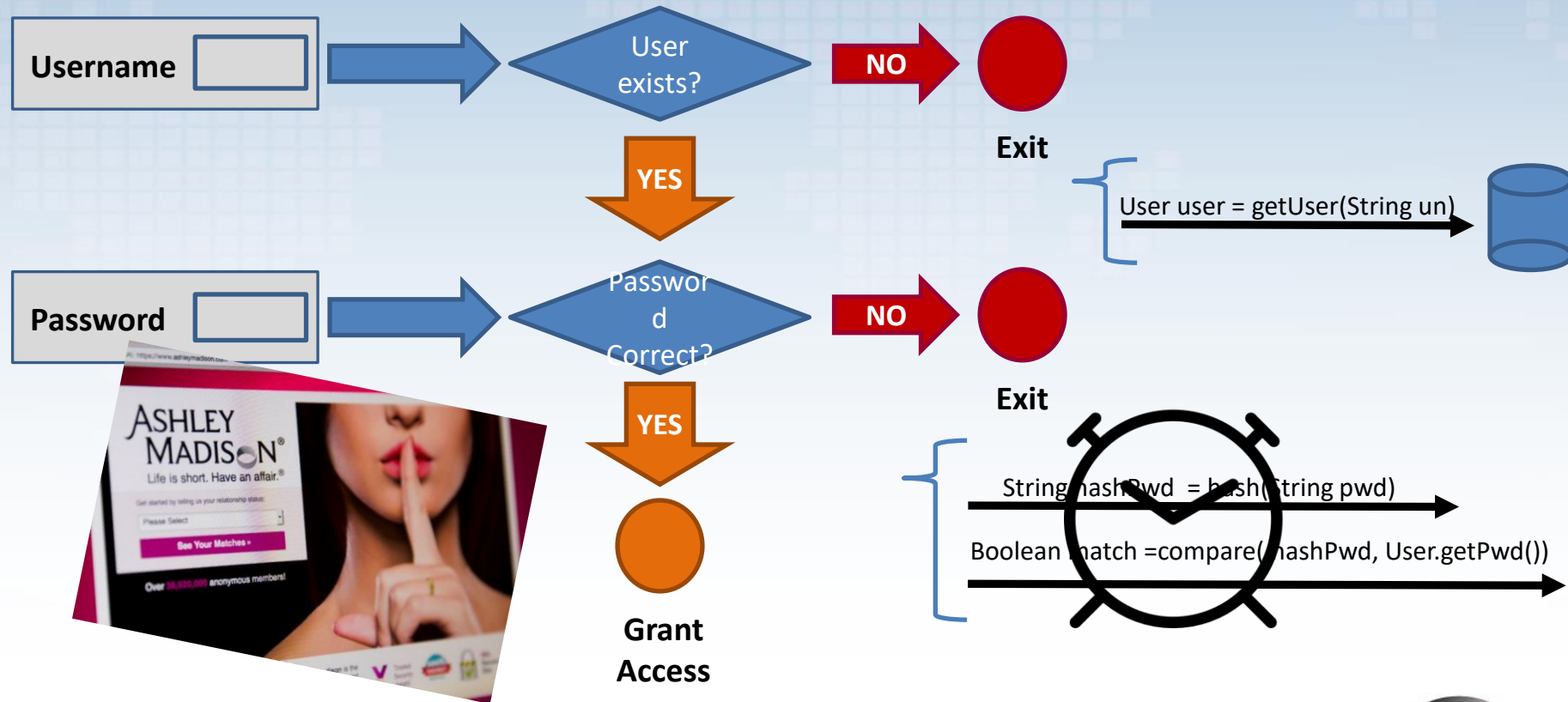


A login form consisting of two rows. The first row has the label 'Username' followed by a light gray rectangular input field. The second row has the label 'Password' followed by a light gray rectangular input field. A thick red oval is drawn around both the labels and their corresponding input fields.

password forgotten link

Create account

Authentication process



Ever seen this?

Username

Password

[password forgotten link](#)

[Create account](#)

Security Questions



2005



2018

Ever seen this?

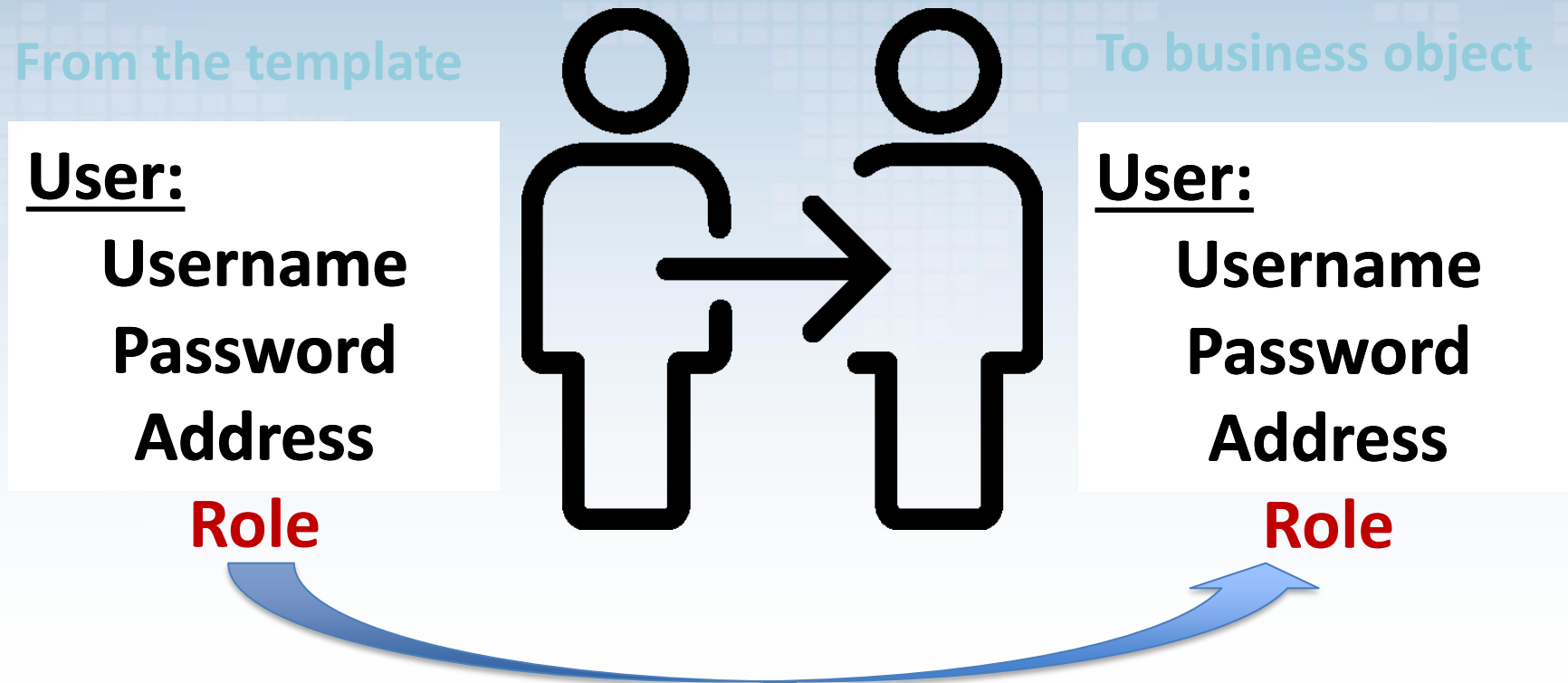
Username

Password

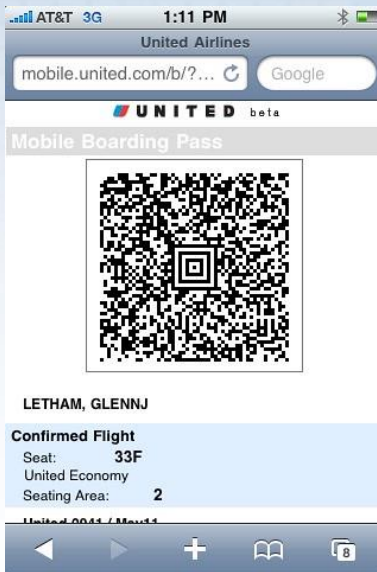
password forgotten link

Create account

Implicit vs explicit binding



(Dis-) Connection



HOTEL 料金表			
* REST	平日・祝祭日	金・土・祝前日	
6:00~18:00		¥2,800	
18:00~6:00	¥2,800		¥3,300
* STAY	¥9,000		¥12,000
* Week Day サービス	(日~木曜日・限定)		
25:00~11:00	お一人様	¥3,800	
(AM 1:00)	お二人様	¥6,000	
* 延長料金 (30分毎)	¥700		(税込)

Replay (playback) attack



OWASP
Open Web Application
Security Project

Identity Theft



Baby-Duck Authentication



Claiming the bounty



Detection

