Security Awareness

- A Hackers Mindset

Martin Knobloch
Email: martin.Knobloch@owasp.org
Twitter: https://twitter.com/knoblochmartin
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

Who is the OWASP® Foundation?

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software. Through community-led open source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

- Tools and Resources
- Community and Networking
- Education & Training

For nearly two decades corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. Donate, Join, or become a Corporate Member today.

https://owasp.org/
OWASP Mission

• to make application security "visible," so that people and organizations can make informed decisions about application security risks
<table>
<thead>
<tr>
<th>OWASP Top 10 - 2013</th>
<th>OWASP Top 10 - 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2 – Broken Authentication and Session Management</td>
<td>A2:2017-Broken Authentication</td>
</tr>
<tr>
<td>A3 – Cross-Site Scripting (XSS)</td>
<td>A3:2017-Sensitive Data Exposure</td>
</tr>
<tr>
<td>A6 – Sensitive Data Exposure</td>
<td>A6:2017-Security Misconfiguration</td>
</tr>
<tr>
<td>A8 – Cross-Site Request Forgery (CSRF)</td>
<td>A8:2017-Insecure Deserialization [NEW, Community]</td>
</tr>
<tr>
<td>A9 – Using Components with Known Vulnerabilities</td>
<td>A9:2017-Using Components with Known Vulnerabilities</td>
</tr>
</tbody>
</table>

https://owasp.org/www-project-top-ten/
What (not) is a hacker

Ski mask?
What (not) is a hacker

Hoodie? ..only if functional!
Disclaimer
Physics
(Defying) Physics?
Bending the reality
Expectation management
Obvious?
(Barbra) Streisand Effect

The Streisand effect is a phenomenon in which an attempt to hide, remove, or censor a piece of information has the reverse consequences of publishing the information more widely, usually facilitated by the Internet. It is an example of psychological backlash, wherein once people are aware that some information is being kept from them, their motivation to access and spread it is increased. It is named after American entertainer Barbra Streisand, whose 2003 attempt to suppress photographs of her residence in Beverly, California (which had been turned public over a dispute) backfired. Similar attempts have been made, for example, in cases alleging the suppression of free, online media such as videos and soundtracks, often being widely circulated on the Internet or distributed on file-sharing networks.
Intention?
Intention?
Intuitive
Flaw vs Bug

99.99
< 0.30
> 0.30
< 0.60

3 laps
> 0.30

3 laps
> 0.30

OWASP
Open Web Application
Security Project
Reward

The gain, doesn’t have 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
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?

Username
Password

password forgotten link
Create account
Authentication process

Username

User exists?

NO
Exit

YES

Password

Password Correct?

NO
Exit

YES

Grant Access

User user = getUser(String un)

String hashPwd = hash(String pwd)

Boolean match = compare(hashPwd, User.getPwd())
Ever seen this?

Username

Password

password forgotten link

Create account
Security Questions

The Curse of the Secret Question

It's happened to all of us. We sign up for an online account, it's easy to remember and hard to guess password, and are then presented with a "secret question" to answer. Sounds like a hedge against us remembering our password... but it's not. It's your mother's maiden name? Today, there are more "What's the name of your first pet?" "What's your lucky color?" And so on.

The point of all these questions is the same: a backup password. If you forget your password, the secret question can verify your identity so you can choose another password. If you have the site e-mail your current password to you, it's a great idea from a usability perspective — it makes it less likely you'll forget the first piece of information that someone needs to identify you. The secret question is much easier to guess than a good password, and the information is much more public. (It's hard to come up with fully made-up passwords that even remotely sound like the same series of actual questions.

The result is a normal disaster protocol (phishing) fail back into an insecure secret protocol (questions). And the security of the entire system suffers.

What can one do? His usual technique is to type in a completely random answer. I mostly check my real life. 

OWASP
Open Web Application
Security Project
Ever seen this?

Username

Password

password forgotten link

Create account
Implicit vs explicit binding

From the template

User:
Username
Password
Address
Role

To business object

User:
Username
Password
Address
Role
(Dis-) Connection
Replay (playback) attack
Identity Theft
Baby-Duck Authentication
Claiming the bounty
Detection