OWASP TOP TEN

What is the state of practice among start-ups?
WHAT: Project and time management solution

Store sensitive information about employees, customers and financial info

Background: Business and management. Outsourced development

⚠️ Biggest fear: Authentication and Access Control. Sensitive information leakage.
WHAT: Crowdsourcing educational material

Each user is assigned privileges based on trust by contributing to the site.

Background: Students at computer science programs

⚠️ Biggest fear: Destruction and privilege escalation.
WHAT: Laundry booking site

Does not store user information, except e-mail addresses as usernames

Background: Experienced developers. Hobby project beside full time jobs

⚠️ Biggest fear: stolen email-addresses, spamming, destruction
WHAT: Communication platform for medical personnel and patients.

Store personal and sensitive information about patients

Background: Computer science fields among others

⚠️ Biggest fear: Information leakage
WHAT: Tutoring service

Store information about grades and diplomas.

Background: Computer science fields and related studies

⚠️ Biggest fear: Ransomware. Being blackmailed in bitcoins
SQL INJECTION

Tool: Burp Suite
MISSING FUNCTION LEVEL ACCESS CONTROL

Tool: Burp Suite
MISSING FUNCTION LEVEL ACCESS CONTROL

Tool: Burp Suite
HTTPs://application.firebaseapp.com/__/auth/handler?apiKey=AIZaSyAUCJL0LMU-iDI3TC2DodURB_A-uptzmPE&appName=%5BDEFAULT%5D&authType=signInViaRedirect&providerId=Google.com&scopes=profile&redirectUrl=HTTPs%3A%2F%2FFacebook.com%2F%23%2F&v=3.9.0

**UNVALIDATED REDIRECT**

Tool: Burp Suite
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>A2</td>
<td>A3</td>
<td>A4</td>
<td>A5</td>
</tr>
<tr>
<td>Injection</td>
<td>Broken Authentication</td>
<td>Cross-Site Scripting (XSS)</td>
<td>Insecure Direct Object References</td>
<td>Security Misconfiguration</td>
</tr>
<tr>
<td>A6</td>
<td>A7</td>
<td>A8</td>
<td>A9</td>
<td>A10</td>
</tr>
<tr>
<td>Sensitive Data Exposure</td>
<td>Missing Function Level Access Control</td>
<td>Cross-Site Request Forgery (CSRF)</td>
<td>Using Components with Known Vulnerabilities</td>
<td>Unvalidated Redirects and Forwards</td>
</tr>
</tbody>
</table>
LESSONS

- Consider security from the start
- Start-ups make more secure applications because they are motivated
- Secure third-party code and samples