• Computer Engineer

• System Analyst

• Application and Communications Security Researcher

• I might know how to hack. Emphasis on *might*
→ Outline

◆ Background to OWASP Top 10
◆ Trends and Observations
◆ Analysis
◆ Recommendations
- The OWASP Top 10 has become the standard security awareness document for developers.
- It represents a broad consensus about the most critical security risks to web applications.
- Original Top 10 released in 2003 and then roughly every 3 years since.
- The product is focused on observed security vulnerabilities in applications based off testing and survey by App-Sec-Dev community members.
## Top 10: Trends

<table>
<thead>
<tr>
<th>2013</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Injection</td>
<td>Injection</td>
</tr>
<tr>
<td>Broken Authentication &amp; Session Mgmt</td>
<td>Broken Authentication</td>
</tr>
<tr>
<td>Cross-Site Scripting (XSS)</td>
<td>Sensitive Data Exposure</td>
</tr>
</tbody>
</table>
Top 10: Trends 2021

<table>
<thead>
<tr>
<th>Broken Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic Failures</td>
</tr>
<tr>
<td>Injection</td>
</tr>
<tr>
<td>Insecure Design</td>
</tr>
<tr>
<td>Security Misconfigurations</td>
</tr>
</tbody>
</table>
Top 10: Core Trends

- Data is the new oil (not gold). IMO!
- Data is the most valuable and vulnerable resource

- Cyber incidents have a concentric target. All the hackers want your data and escalated privileges

- Most exploits are escalating to unauthorised access, confidentiality breaches and privacy attacks
Opportunities: Who f’ed up?

• The developers. As usual
• Re/use of **vulnerable components**
• Weak package inspection
• **Flawed design logic** on custom modules (esp. authentication and access control)
Opportunities: What Do We Do?

- Code Audit and Inspection

- Encourage use of SDLCs that enable **flexible & frequent testing**

- Utilise **enhanced data security controls** (e.g. Access & authorisation controls)

- Ensuring **strict or best-possible compliance with cyberspace standards**
• Architecture and Resource allocation have improved esp. with flexible cloud services.

• Availability Attacks are less attractive for the typical threat actor

• Data has infinite upward value

• Confidentiality Attacks are gaining notoriety

• Attackers have many advantages
• Don’t drop the soap! Defenders must keep defending.

• Privacy and data protections are the crux of future security developments, problems and solutions

• Application security is everyone’s job. Devs screw up but so do users

• We may not win, but we lose if we stop fighting
THANK YOU

This work is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License.
It makes use of the works of OWASP community and others discovered during desk research.

This production does not represent the opinions of any specific organisation, regardless of any known affiliations of the author.