Do AppSec Better

My experience from OWASP SnowFROC
<table>
<thead>
<tr>
<th>Jay Simmons</th>
<th>Senior AppSec Analyst @ Great American</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Previous Roles</strong></td>
<td><strong>Developer</strong></td>
</tr>
<tr>
<td></td>
<td><strong>IT Consultant</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Server Admin</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Support Analyst</strong></td>
</tr>
<tr>
<td><strong>Hobbies</strong></td>
<td><strong>Legos</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Homelab Administration</strong></td>
</tr>
<tr>
<td></td>
<td><strong>IT Consulting</strong></td>
</tr>
<tr>
<td><strong>Family</strong></td>
<td><strong>Married for 10 years</strong></td>
</tr>
<tr>
<td></td>
<td><strong>7 year old daughter</strong></td>
</tr>
<tr>
<td></td>
<td><strong>3 year old son</strong></td>
</tr>
</tbody>
</table>
Let’s talk about clickjacking

What is it?
- User is presented with a false interface, where their input is applied to something they cannot see.

Brief History
- Exploit was discovered in 2002 but remained largely ignored (no name given)
- In 2008 clickjacking exploit discovered in flash player by Jeremiah Grossman & Robert Hansen. (name coined)
Kevin Johnson (Secure Ideas)

- Problems in AppSec
  - Heavily focused on identifying vulnerabilities
  - Largely motivated by fame
  - Incentivized based on findings not remediations

- Solutions
  - Understand business use
  - Create concise action plans
  - Assist in the remediation effort
Risk Identification

Identify Risks
- Reputation
- Data Breach
- Contractual Obligations
- Industry Regulations

Categorize Risk
- Confidentiality
- Integrity
- Availability
Prioritize Your Work

Quantify Risk
- Will our business recover
- How much money will we lose
- Are we insured for this type risk

Identify Exposure
- How could this bad thing happen
  - Applications
  - Databases
  - Accounts
  - Networks
## Identify The Problems

**Inside out**
- Perform AST Scans (SAST, SCA, DAST, etc)
- Spend time in the repos
- Talk to developers and QA teams

**Outside in**
- Perform penetration testing
- Spend time using the apps
- Talk to app users
Plan your remediation

Culture
- Does your team enable other teams or is it a wall?
- Is security part of the design phase?
- Do the developers understand the importance?

Training
- Can developers identify security issues?
- Are developers able to resolve the security issues?
- Do developers know what OWASP is?

Partnership
- Can we support the developers?
- Can we support the QA Team?
- Can we prioritize the remediation workload?
Other interesting things

- Automated Remediation
- SCA Exploitable Path
- Mobile AppSec
- SnowFROC 2023 Presentations
  https://www.snowfroc.com/#2023presentations