DON’T PANIC!

Security’s here to assess your project.

// todo

- The assessment
- Threat modelling
- App hardening
- Vulnerability scanning
- Wrapping up

10 The Assessment

What can you expect?

What can you expect?

- Naturally, OWASP-related attacks.
- Infrastructural tests, if applicable.
- Scans for known vulnerabilities in dependencies, hosts, ...
- Attempts to break out of user’s privileges.
- Tests to see if the presented data doesn’t go out of bounds.
- All presented in a report.

Demo: a sample report

20 Threat Modelling

Know your application

STRIDE / DREAD

Know your application

- Hosting platform
- Technologies & frameworks used
- Interactions with third-party systems
- Network topology, firewall settings, ...

STRIDE / DREAD

STRIDE

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege

DREAD

- Damage potential
- Reproducibility
- Exploitability
- Affected users
- Discoverability

Demo: threat modelling

https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

30 App Hardening

Web security

Data security

Cloud security

Container security

Web security

- Connection security
- HTTP features
- OWASP
- Robots.txt

Web security - The Connection

- HTTPS all the way
  - Even locally while developing!
- TLS 1.2, or 1.3 if you can
- No mixed content!

Web security - HTTP Features

- Headers
  - Strict-Transport-Security
  - Content-Security-Policy
  - Server, X-Powered-By
- Cookies
  - HttpOnly, Secure, SameSite
  - Fingerprinting
- Redirects
- <a rel=“noopener”>

Web security - OWASP

- Cross-site request forgery
  - Attempts to post form data across domain boundaries
  - Use combination of cookies, HTTP headers and form fields as preventive measure

- Server-side request forgery
  - Attempts to abuse endpoints to gain information

Web security - OWASP

```
POST /product/stock HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 118

stockApi=http://localhost/admin
```

Web security - robots.txt

- Tells crawlers where to look for indexing content
- Can also tell crawlers which paths are off limits
- These last paths can be very interesting for potential attackers to focus on!

Data security

- OWASP, continued
- Leaking data
- File transfers
- Encryption

Data security - Return of the OWASP

- Injection
  - SQL
  - API
  - LDAP
  - OS

- XML documents
  - External Entities
  - file:///etc/passwd

Data security - Leaking data

- Inconsistent credential checking
- Error pages / responses
- Search or data retrieval endpoints

Data security - File transfers

- Limit upload size
- Check file types
  - Not just file extension or MIME type
  - Try to open the file as intended in a sandbox
- Scan for malware
- Rename uploads
- Use direct download streams

Data security - Encryption

- Use well-known, proven algorithms
  - Do NOT implement encryption by yourself!

- Use HMAC signatures
  - Encrypt + verify

Cloud security

- IAM
  - Least-privilege principle

- Use the tools given to you
  - Short lived access tokens rather than access keys/credentials
  - Store secrets in vaults
  - Set up virtual networks and limit access on a network level
  - Add services to stop invalid requests, like firewalls or API management services
  - Use monitoring and threat detection

Container security

- Secrets

- Be careful with tutorials

- Don’t be root

40 Vulnerability scanning

Dependencies

Dependencies

And ... dependencies

Dependencies everywhere

- NPM, Nuget, Maven, ...
- Docker
- Dependabot

Demo: vulnerability scanning

50 Wrapping up

GOTO 10

Thank You!

Links

- https://www.google.com/search?q=security+assessment+report+type%3Apdf
- https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
- https://owasp.org/www-project-top-ten/
- https://developer.mozilla.org/en-US/docs/Web/Security
- https://blog.aquasec.com/docker-security-best-practices
- https://cheatsheetseries.owasp.org/cheatsheets/Docker_Security_Cheat_Sheet.html