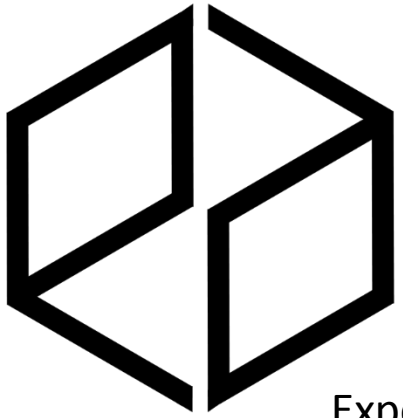

www.pandoralabs.net
PANDORA
SECURITY LABS
Expert Advice. Experience Advantage.
Proactive Security Solutions Through Cutting-Edge Research.
Web App Testing: RECON. MAPPING. ANALYSIS.
By @isaacsabas



PANDORA
SECURITY LABS

Expert Advice. Experience Advantage.
Proactive Security Solutions Through Cutting-Edge Research.
www.pandoralabs.net

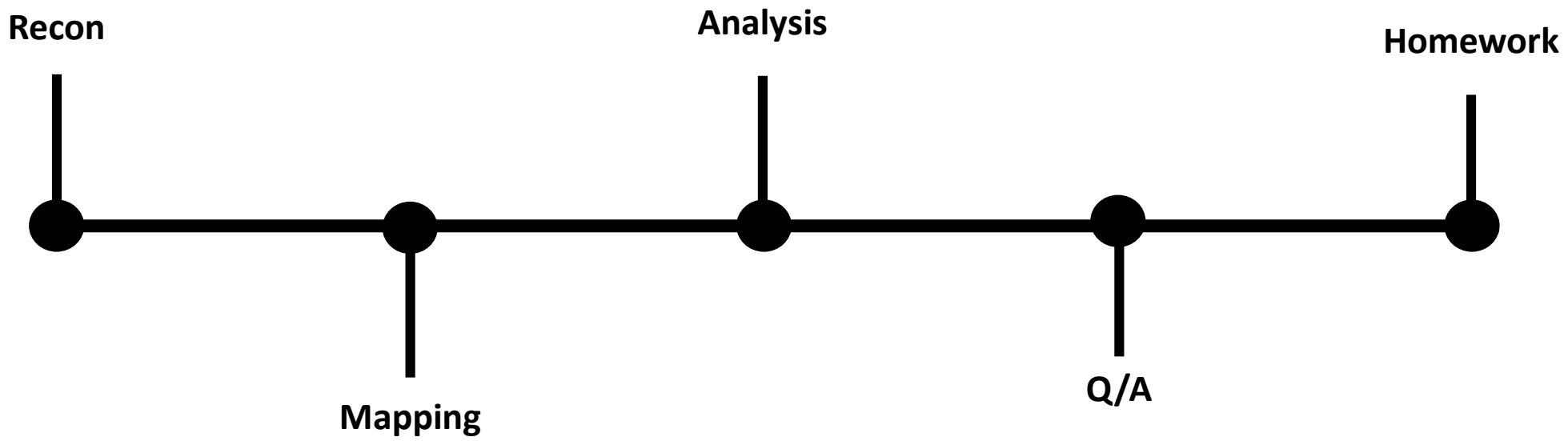
We are a Security-as-a-Service company

Providing businesses with on-demand threat detection & intelligence capabilities to secure their IT infrastructure, 24x7.

We Make IT Secure

WEB APPLICATION TESTING

RECON
MAPPING
ANALYSIS



Discussion Flow

What we will be discussing today

The Attack Surface describes all of the different points where an attacker could get into a system, and where they could get data out.

Recon

What should we check for?

The Attack Surface is:

- All paths for data/commands into and out of the application
  - The code that protects these paths (including resource connection and authentication, authorization, activity logging, data validation and encoding)
- All valuable data used in the application, including secrets and keys, intellectual property, critical business data, personal data and PII, and
  - The code that protects these data (including encryption and checksums, access auditing, and data integrity and operational security controls).

Samples of Attack Points

- User interface (UI) forms and fields
- HTTP headers and cookies
- APIs
- Files
- Databases
- Other local storage
- Email or other kinds of messages
- Run-time arguments

Attack Surface Recon allows you to:

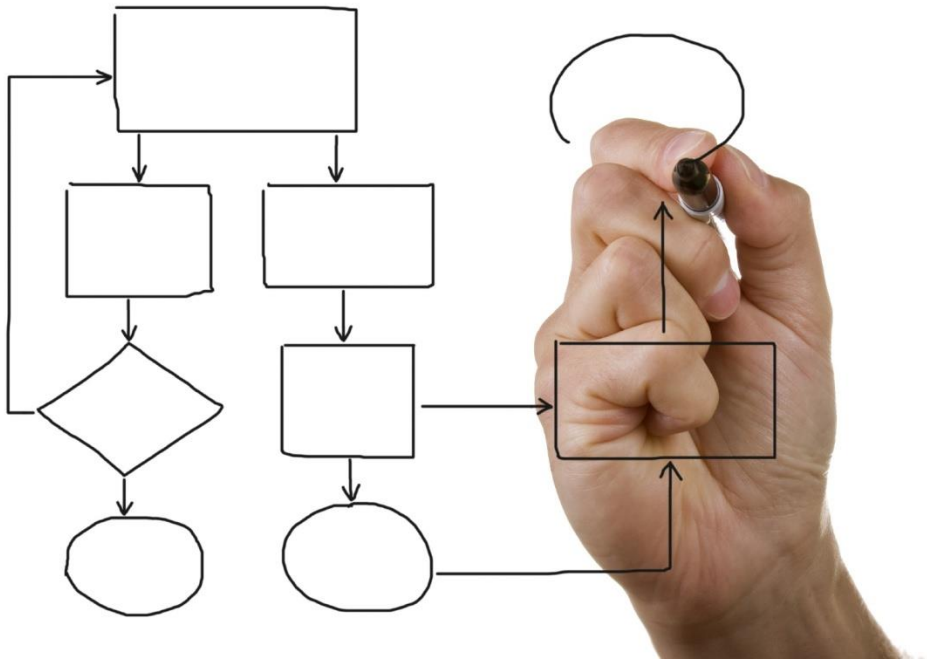
- Identify what functions and what parts of the system you need to review/test for security vulnerabilities
- Identify high risk areas of code that require defense-in-depth protection (what parts of the system that you need to defend)
- Identify when you have changed the attack surface and need to do some kind of threat assessment

Tools we can use to RECON

Builtwith.com

OWASP ZAP

OWASP ZAP DEMO



Attack Surface mapping is to map out and prioritze what parts of a system need to be reviewed and tested for security vulnerabilities.

Mapping

Mapping out the Attack Surface with Potential Use Cases

Mapping Attack Surface/Point to:

- Types of users/roles, and its privilege levels
- External-facing or internal-facing
- Purpose (function, storage, informational, etc.)
- Implementation (server-side, client-side)
- Technology

Attack Point	User/Role	External/ Internal	Purpose	Implementation	Technology
User Search Form	Member	Internal	Function	Server-side	PHP, AJAX
Contact Us Form	Anonymous	External	Function	Server-side	PHP, AJAX

Prioritization & Focus

- By grouping attack surface or attack points:
  - You don't need to understand every endpoint in order to understand the total Attack Surface and the potential risk profile of a system.
  - You can budget what it will take to assess risk at scale, and you can tell the risk profile of an application based on a certain criteria or parameter.

Attack Surface Analysis is about identifying which parts of the system need to be fixed given the risk score and how it affects the overall system.

Analysis

Based on the mapped out Attack Surface and identified risks, what now?

What Now?

- Prioritize what is the most important attack surface to address
- As modification and adjustments are made, use the baseline to test:
  - What has changed?
  - What are you doing different? (technology, new approach, etc.)
  - What holes could you have opened?
- Helps in the SDLC to build the application securely

TIME FOR

Q&A

RECON. MAPPING. ANALYSIS.

Homework

- Install OWASP ZAP on your system

  https://github.com/zaproxy/zaproxy/wiki/Downloads

- Conduct the recon, mapping, and analysis procedures on your web application and identify the following:
  - Attack Surface/Points
  - Map and

WEB APPLICATION TESTING

RECON
MAPPING
ANALYSIS


www.pandoralabs.net
PANDORA
SECURITY LABS
Expert Advice. Experience Advantage.
Proactive Security Solutions Through Cutting-Edge Research.
Web App Testing: RECON. MAPPING. ANALYSIS.
By @isaacsabas