Abertay University

Angry {} Birding

Tolga Ünlü, Lynsay A. Shepherd, Natalie Coull, and Colin McLean

"Can we utilize the trial-and-error process of attackers for defence?"

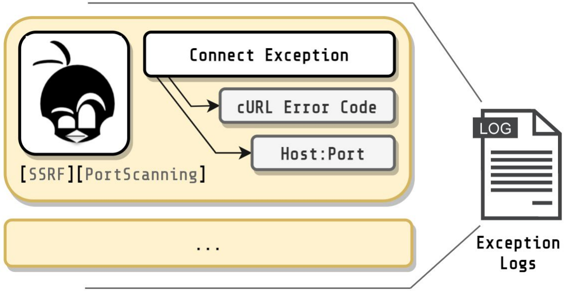
Evaluating Application Exceptions as Attack Canaries

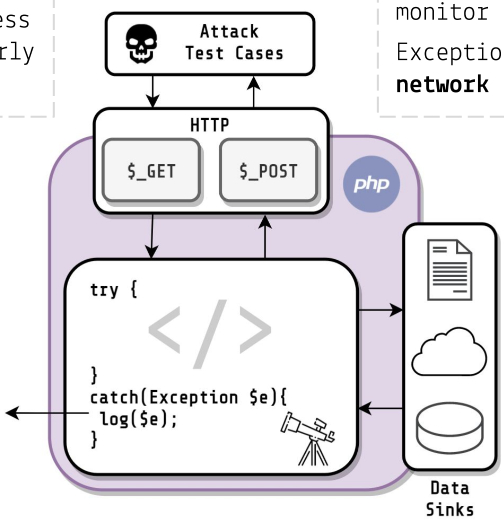
Motivation

Successful attacks require multiple **failed attempts.** Exceptions generated in this process could play the role of an **attack canary**, an early warning system.

Analysis

Observe how a set of exception combinations maps to specific **attacks** or **attack payloads**:





```
try {
</>
}
catch(Exception $e){
 log($e);
}
```

Evaluate the approach based on the following criteria:

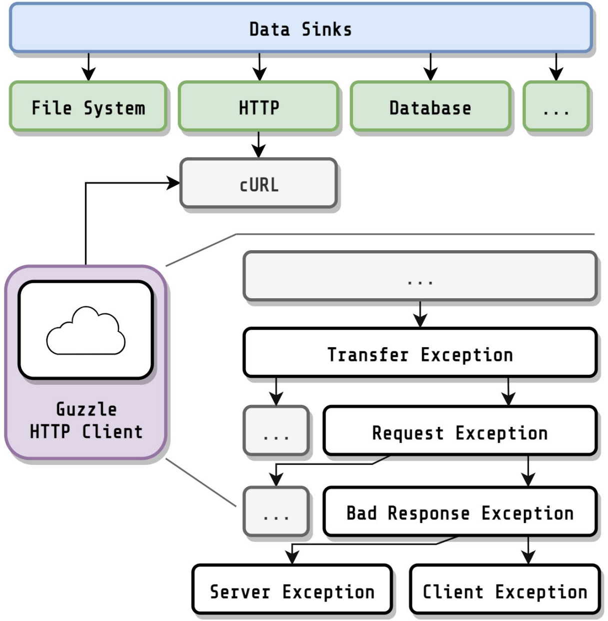
Accuracy
- Exception Payload
- Additional Data Requirement

Effectivity
- Attack Resistance
- Attack and Attack Payload Coverage

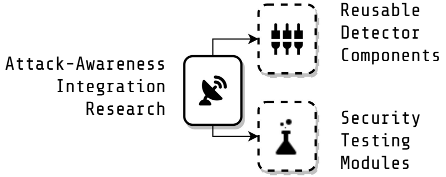
Proposed Approach

Instrument test application in a controlled environment to monitor and log attacker-induced exceptions.

Exceptions generated by **data sinks** such as **filesystem**, **network** and **database APIs**.



Outlook


Attack-Awareness Integration Research
Reusable Detector Components
Security Testing Modules