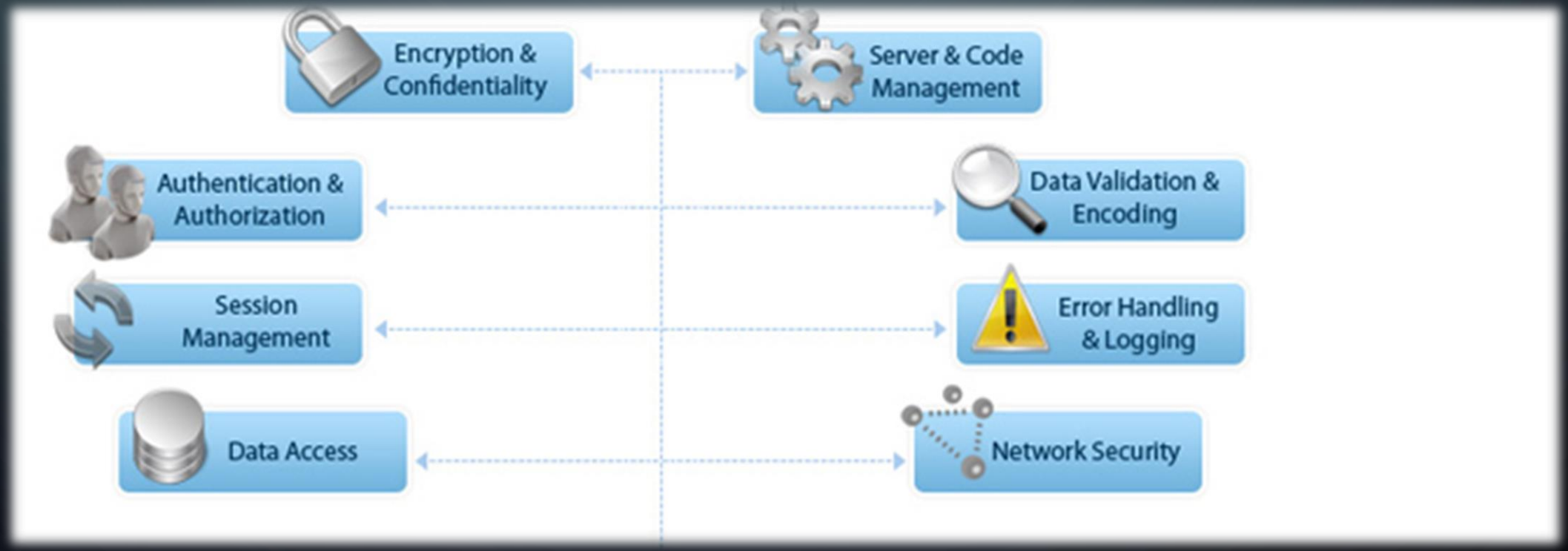
AUTOMATED SECURITY TESTING

AGENDA

- What is Security Testing ?
- Why we Testers need to worry about it ?
- Why Automated Security Testing?
- How can we Automate this?
- Demo
- Resources

WHAT IS SECURITY TESTING

- Part of Software Testing
- Process intended to reveal flaws in the security mechanism.

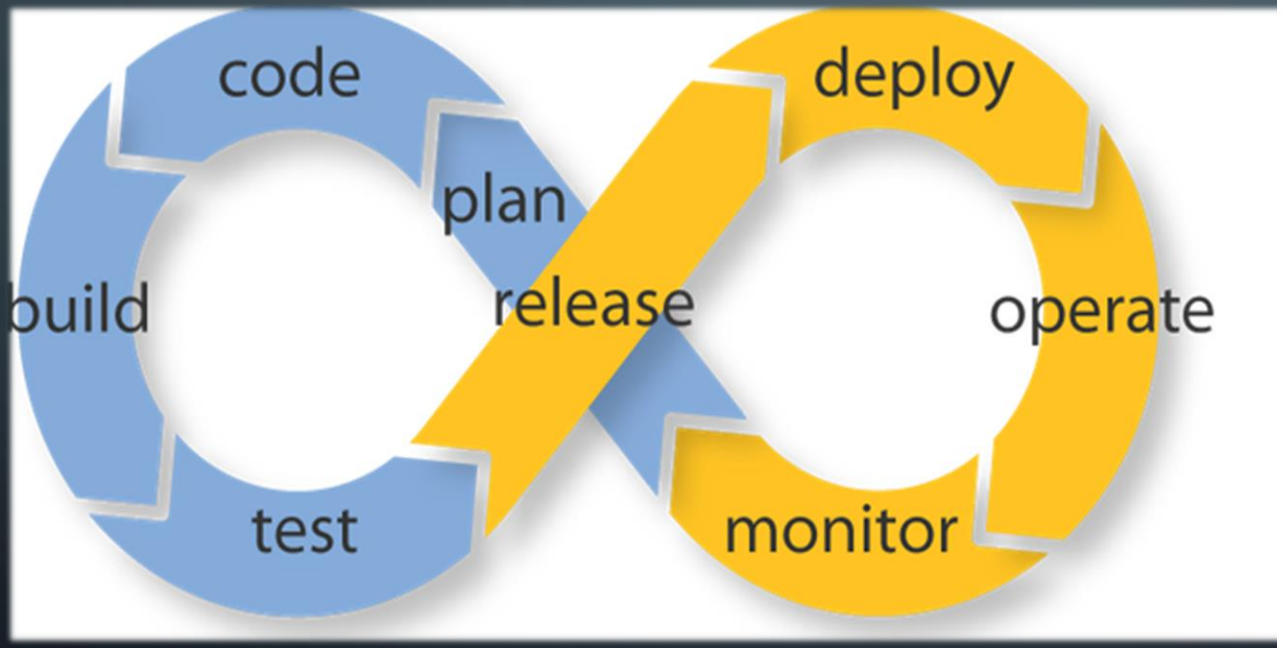


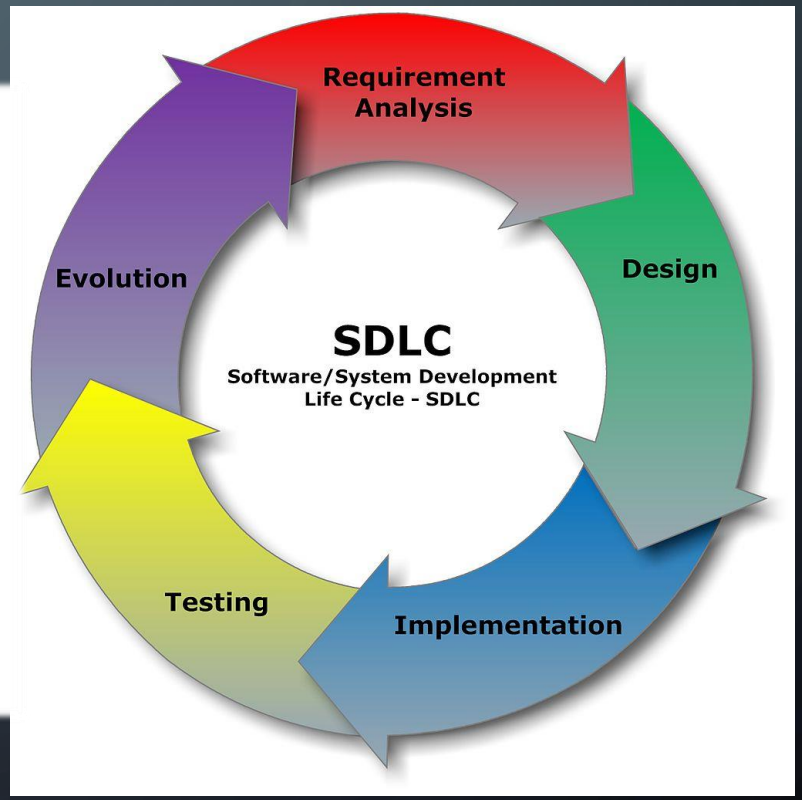
I AM NOT A SECURITY TESTER !

- Why do we, Testers need to worry about security testing ? Isn't there a Security Team to handle this ?

- Tester = { Functional testing + Non Functional (Performance, Security..)}

WHY AUTOMATED SECURITY TESTING?

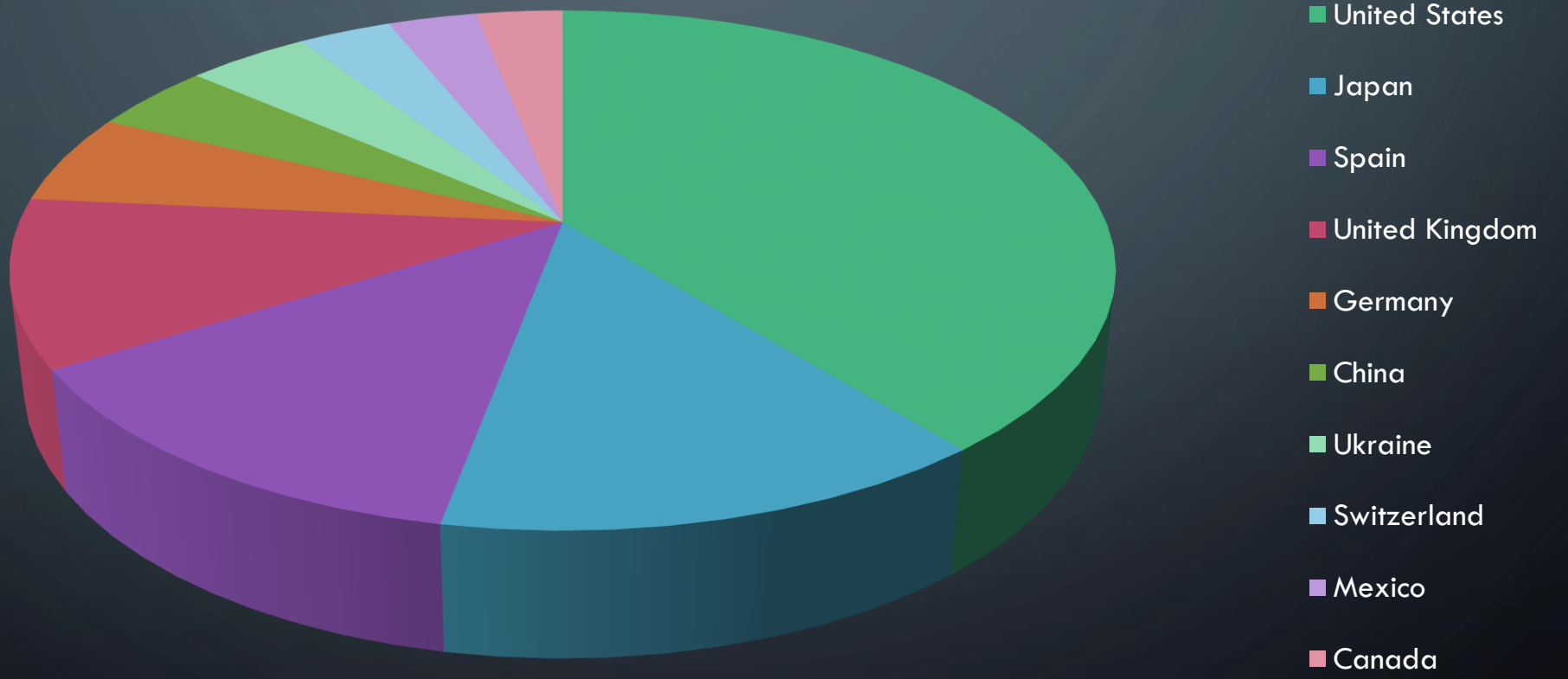




- Detect known vulnerabilities early in the cycle

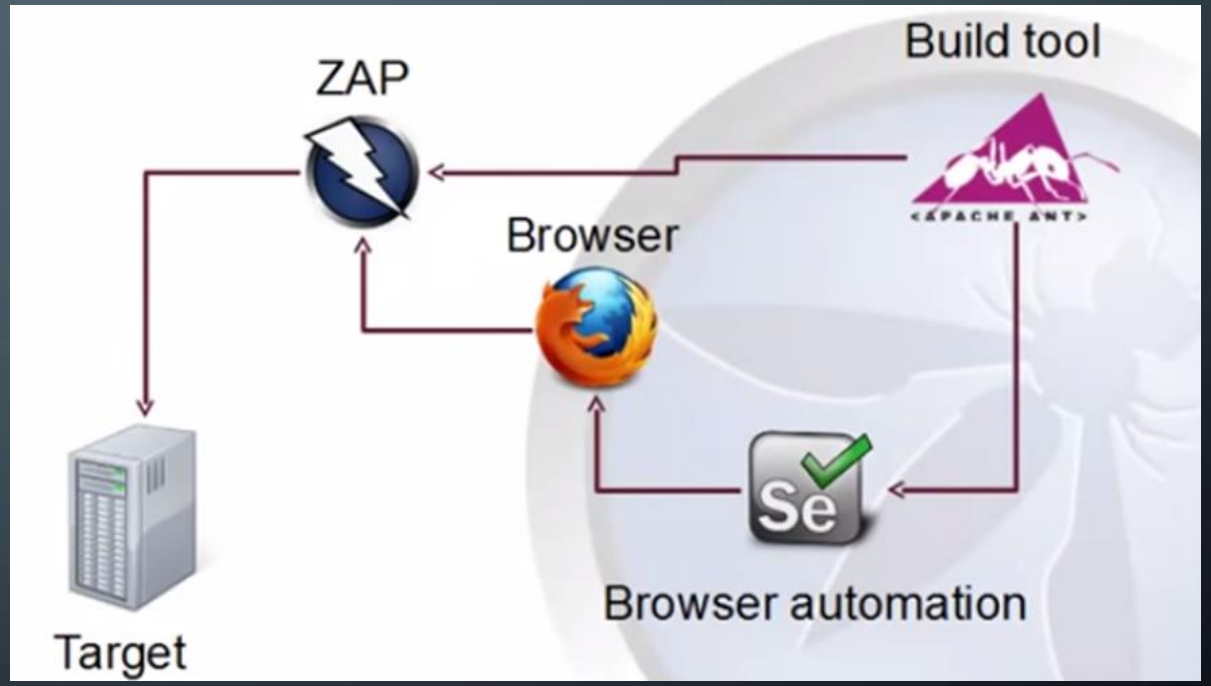
- Reduce Costs – Amount of time you need to hire Security professional
- 10 min to get you started with your first Attack proxy and scan
- Can use your existing automated functional tests to generate HTTP traffic, no need to write special security tests.

WHERE ARE WE ? *AS ON 2014*



HOW DID WE DO? “ATTACK PROXIES”

- Sit between Target and Tester
  - Search for http traffic patterns
  - Manipulate headers
  - Scan for vulnerabilities
  - Fuzzing



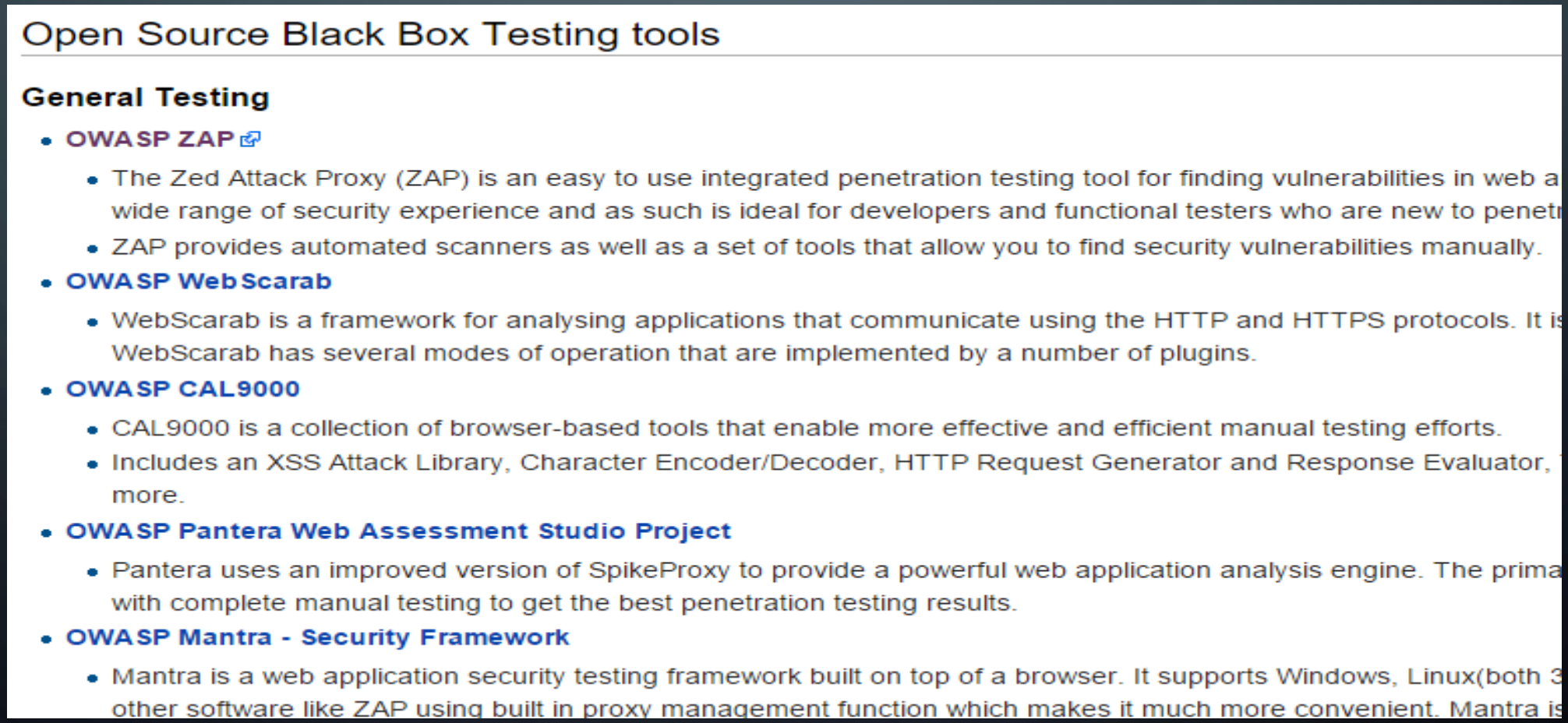
ALWAYS REMEMBER

- Never run any Security Tests on sites that you aren’t authorised to do so.

IN ACTION…

RESOURCES – SO MANY OPTIONS TO EXPLORE!

- https://www.owasp.org/index.php/Appendix_A:_Testing_Tools



Open Source Black Box Testing tools

General Testing

- **OWASP ZAP**
  - The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web a wide range of security experience and as such is ideal for developers and functional testers who are new to penetr
  - ZAP provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.
- **OWASP WebScarab**
  - WebScarab is a framework for analysing applications that communicate using the HTTP and HTTPS protocols. It is WebScarab has several modes of operation that are implemented by a number of plugins.
- **OWASP CAL9000**
  - CAL9000 is a collection of browser-based tools that enable more effective and efficient manual testing efforts.
  - Includes an XSS Attack Library, Character Encoder/Decoder, HTTP Request Generator and Response Evaluator, more.
- **OWASP Pantera Web Assessment Studio Project**
  - Pantera uses an improved version of SpikeProxy to provide a powerful web application analysis engine. The prima with complete manual testing to get the best penetration testing results.
- **OWASP Mantra - Security Framework**
  - Mantra is a web application security testing framework built on top of a browser. It supports Windows, Linux(both 3 other software like ZAP using built in proxy management function which makes it much more convenient. Mantra is

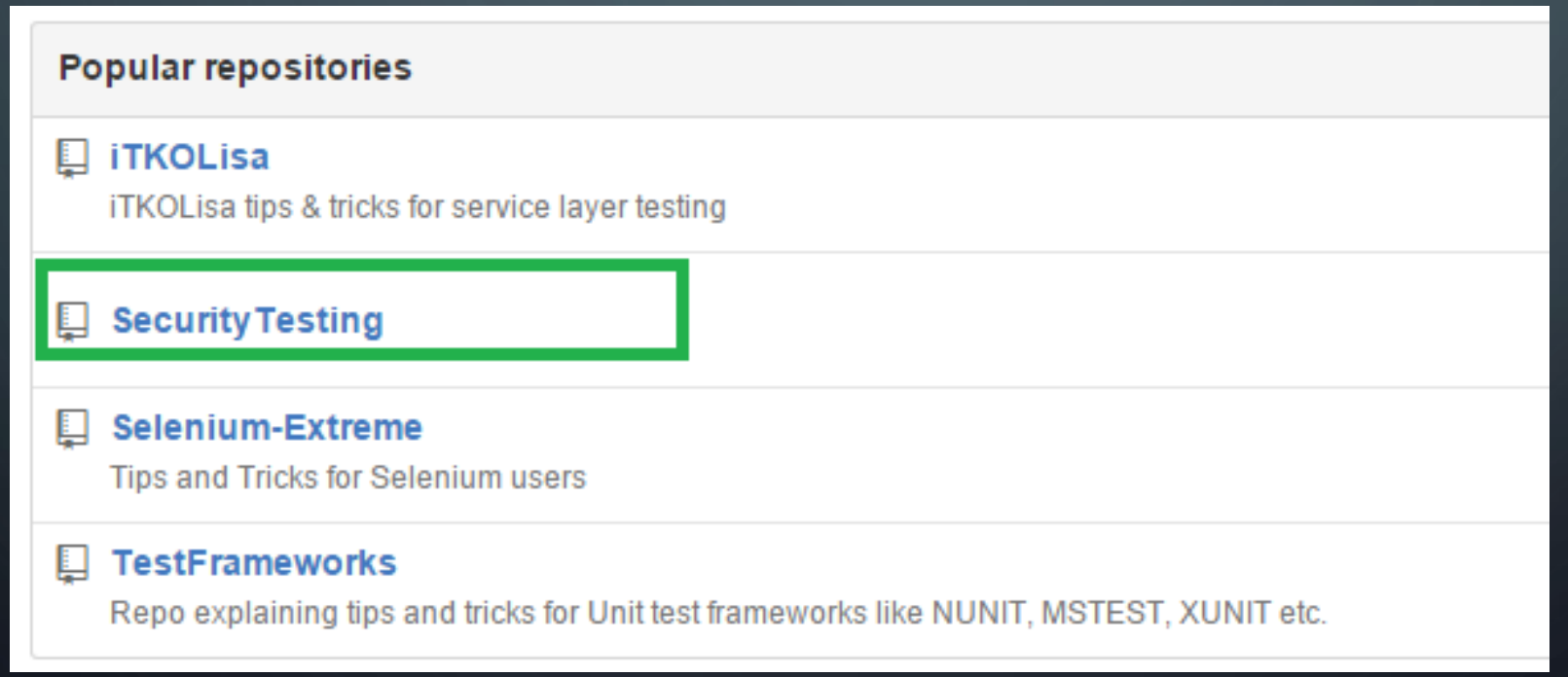
BDD IN SECURITY TESTING. IS IT POSSIBLE?

```
Scenario: The application should not contain SQL Injection vulnerabilities
Meta: @id scan_sql_injection
Given a scanner with all policies disabled
And the URL regular expressions listed in the file: tables/exclude_urls.table are excluded from the scanner
And the SQL-Injection policy is enabled
And the attack strength is set to High
And the alert threshold is set to Medium
When the scanner is run
And false positives described in: tables/false_positives.table are removed
Then no Medium or higher risk vulnerabilities should be present
```

Test Name	Duration	Age
data_security.story.Prevent browser caching of sensitive data {method=viewProfileForBob, username=bob, password=password, sensitiveData=Robert}	0 ms	1
data_security.story.Prevent browser caching of sensitive data {method=viewProfileForBob, username=admin, password=password, sensitiveData=Robert}	0 ms	1
data_security.story.Prevent browser caching of sensitive data {method=viewProfileForAlice, username=alice, password=password, sensitiveData=alice@continuumsecurity.net}	0 ms	1
data_security.story.Prevent browser caching of sensitive data {method=viewProfileForAlice, username=admin, password=password, sensitiveData=alice@continuumsecurity.net}	0 ms	1
data_security.story.Prevent browser caching of sensitive data {method=viewUserList, username=admin, password=password, sensitiveData=User List}	0 ms	1
authentication.story.Passwords should be case sensitive	0 ms	1
authentication.story.Present the login form itself over an HTTPS connection	0 ms	1
authentication.story.Transmit authentication credentials over HTTPS	0 ms	1

ON GITHUB

- https://github.com/impeccable-tester/SecurityTesting



I AM NOW A SECURITY TESTER ☺