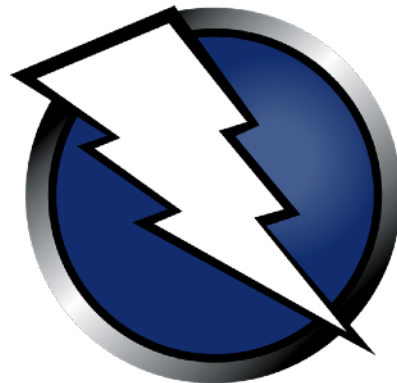


How to use proxy in security testing

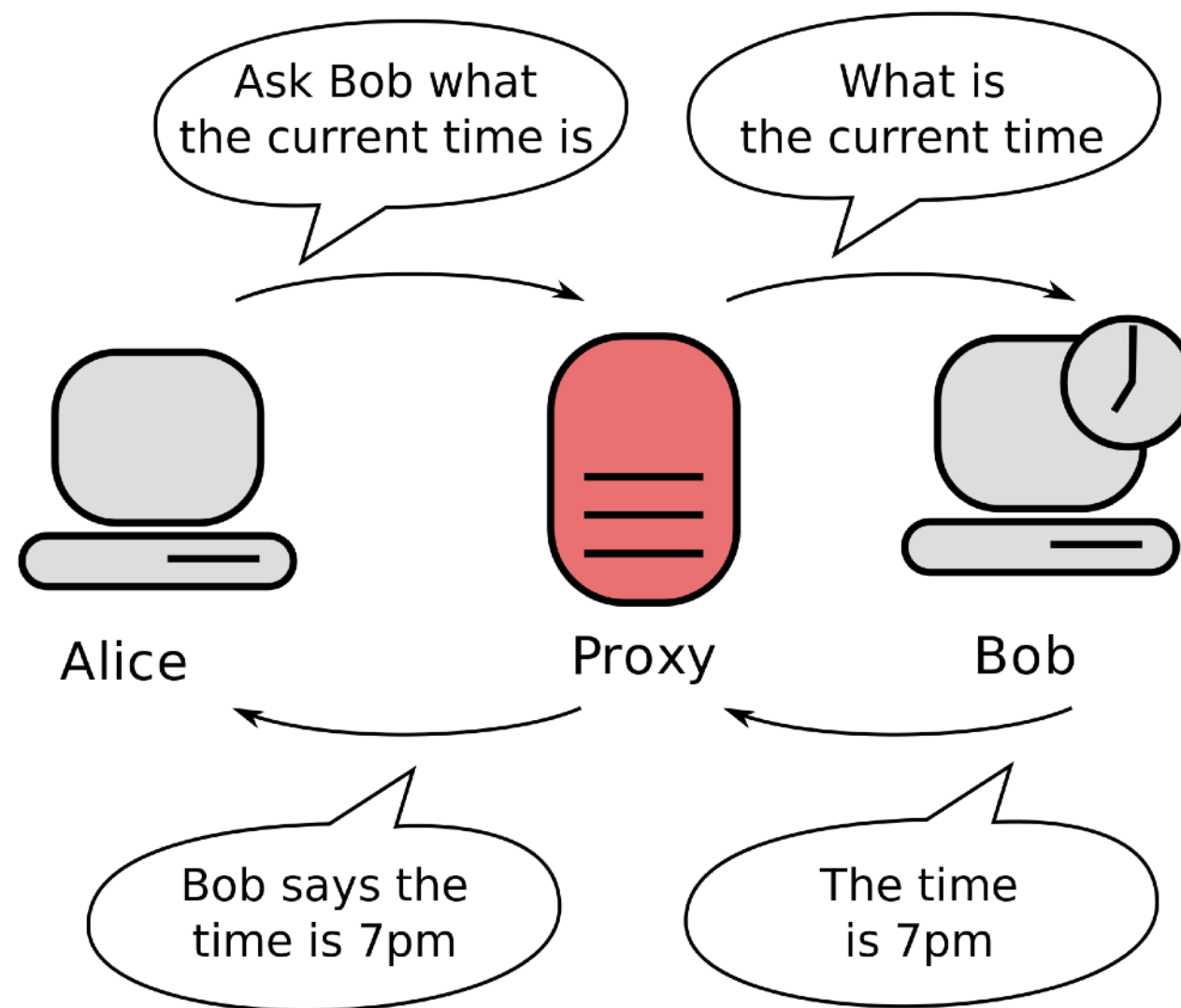
OWASP Zed Attack Proxy (ZAP)



MAKER

ZINC
not another conference

What is Proxy (Server)



What is HTTP Proxy Server

The screenshot displays the OWASP ZAP 2.7.0 interface. The main window is titled "Manual Request Editor" and shows a "Request" tab. The request is a POST to `http://192.168.0.24/index.php` with the following headers:

```
POST http://192.168.0.24/index.php HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.0.24/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: 192.168.0.24
```

The body of the request is:

```
inputEmail=test%40test.zinc&inputPassword=test
```

The "Response" tab shows the following headers:

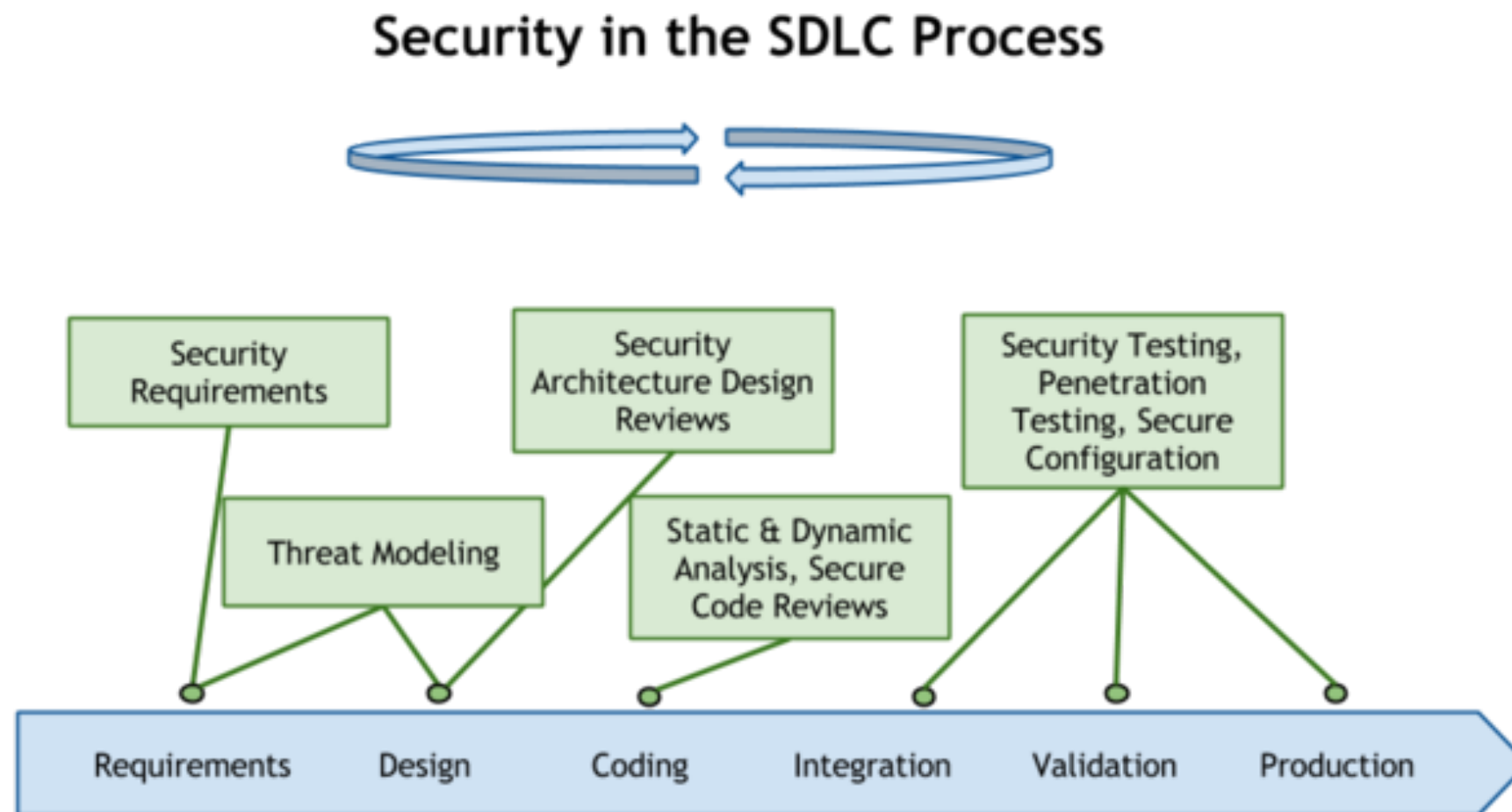
```
HTTP/1.1 200 OK
Date: Tue, 22 May 2018 14:08:03 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1485
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

The body of the response is an HTML document:

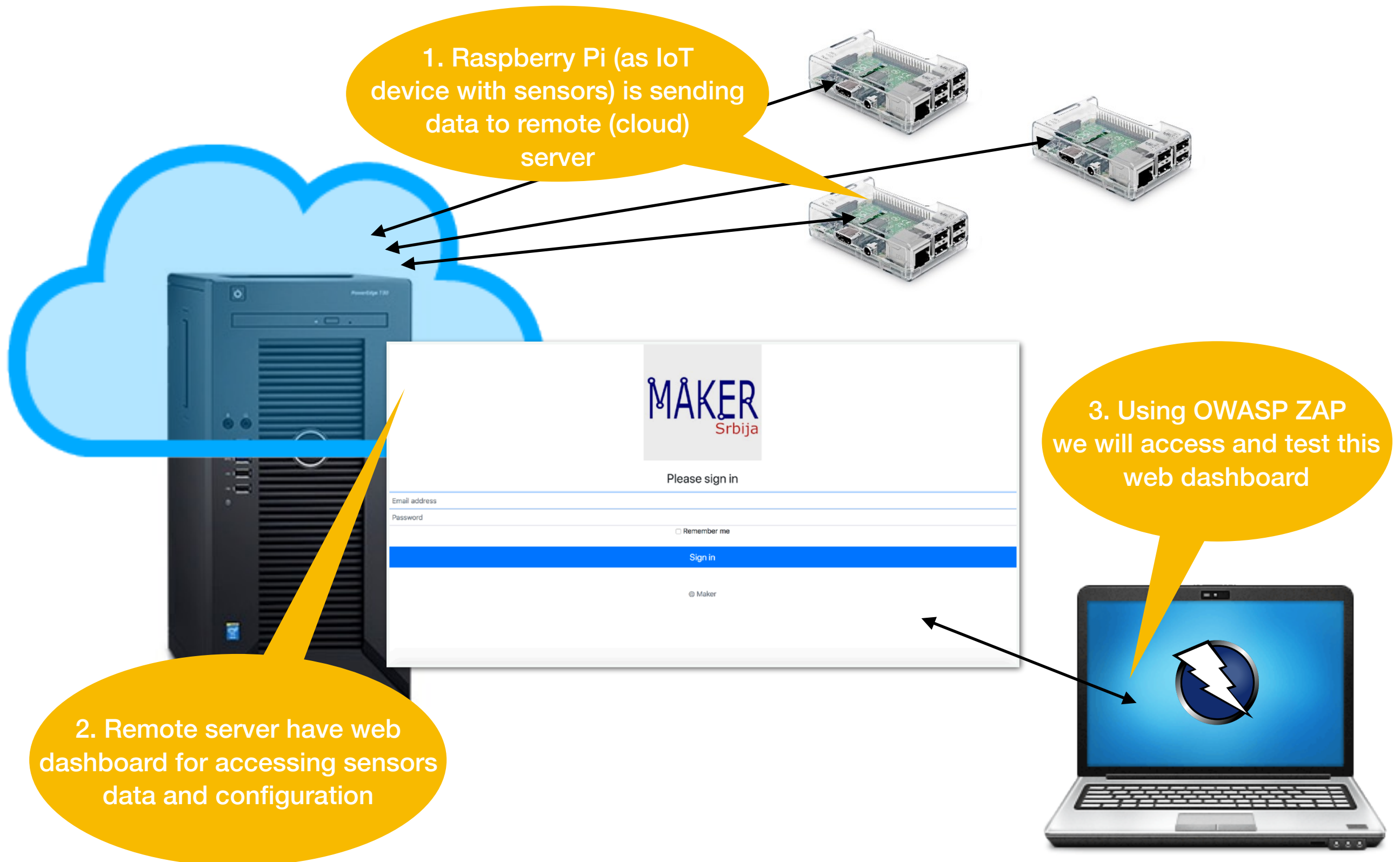
```
<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <meta name="description" content="Maker Vulnerable POC for ZINC">
    <meta name="author" content="Ivan Markovic">
    <link rel="icon" href="favicon.ico">
    <title>Maker Vulnerable POC for ZINC</title>
```

The bottom status bar shows the request details: "Time: 67 ms | Body Length: 1485 bytes | Total Length: 1714 bytes". The bottom left shows "Alerts" with 0 critical, 2 high, 6 medium, and 1 low alerts. The bottom right shows "Current Scans" with 0 active scans.

What is Security Testing (and why it is important)



Our lab for today



What is OWASP



OWASP

Open Web Application
Security Project

What is OWASP Top Ten

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	⊗	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	⊗	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Cloud Top 10 Risks
R1: Accountability & Data Risk
R2: User Identity Federation
R3: Regulatory Compliance
R4: Business Continuity & Resiliency
R5: User Privacy & Secondary Usage of Data
R6: Service & Data Integration
R7: Multi-tenancy & Physical Security
R8: Incidence Analysis & Forensics
R9: Infrastructure Security
R10: Non-production Environment Exposure

OWASP IoT Top10 2014

OWASP
The Open Web Application Security Project

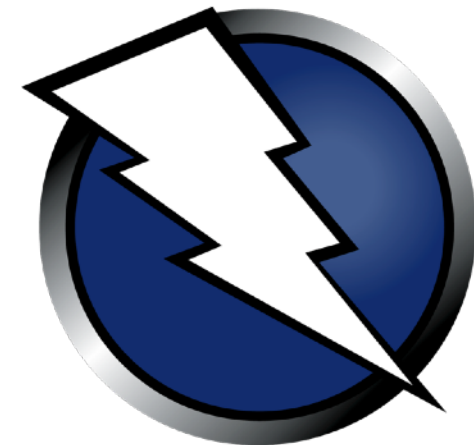
A1: Insecure Web Interface	A2: Insufficient Authentication/Auto rization	A3: Insecure Network Services	A4:Lack of Transport Encryption
A5: Privacy Concern	A6 : Insecure Cloud Interface	A7: Insecure Mobile Interface	A8: Insecure Security Configurability
	A9: Insecure Software / Firmware	A10: Poor Physical Security	

12

OWASP Top 10 Mobile Risk - Final List 2016	
M1	Improper Platform Usage
M2	Insecure Data Storage
M3	Insecure Communication
M4	Insecure Authentication
M5	Insufficient Cryptography
M6	Insecure Authorization
M7	Client code Quality
M8	Code Tampering
M9	Reverse Engineering
M10	Extraneous Functionality

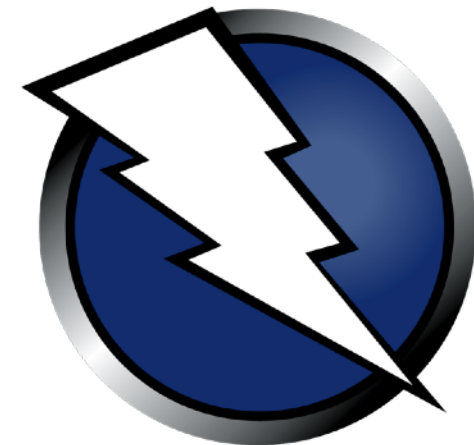
What is OWASP Zed Attack Proxy (ZAP)

- Web application penetration testing tool
- Free and open source
- An OWASP flagship project
- Ideal for beginners but also used by professionals
- Interesting for developers and automated security testing



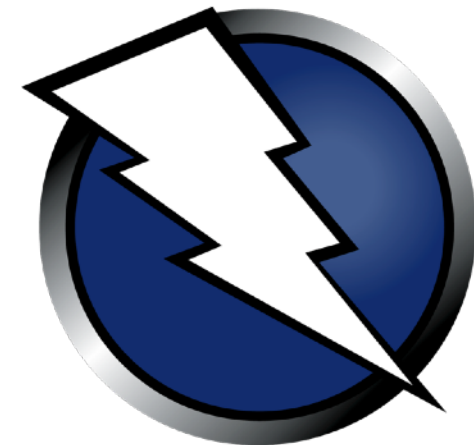
ZAP Principles

- Free, open source
- Cross platform
- Easy to use and easy to install
- Internationalized
- Fully documented
- Work well with other tools
- Reuse well regarded components
- Involvement is actively encouraged



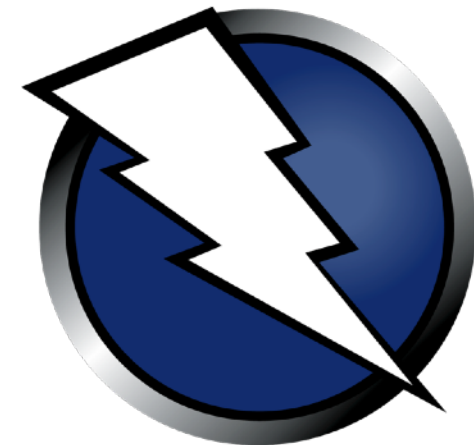
ZAP main features

- Intercepting proxy
- Active and passive scanners
- Spider
- Report generation
- Brute-forcing
- Fuzzing
- Extensibility



ZAP additional features

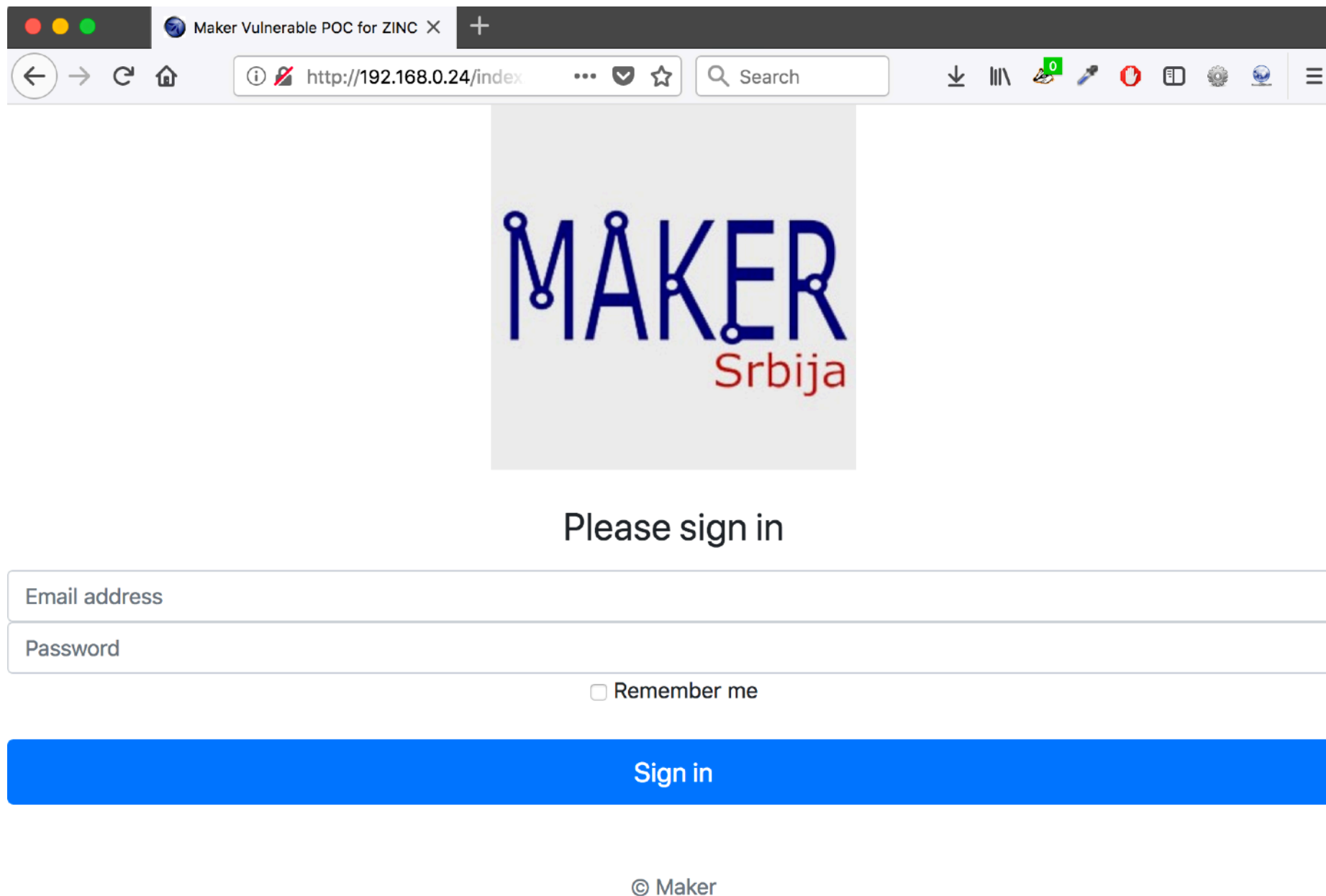
- Auto Tagging
- Port scanner
- Parameter analysis
- Smart card support
- Session comparison
- Invoke external applications and tools
- API + headless mode
- Dynamic SSL certificates



Hand's on time

- Install ZAP
- Configure ZAP
- Configure Mozilla Firefox to use ZAP as proxy server
- Learn ZAP interface
- Explore vulnerable web application via ZAP

Capture The Flag using ZAP



Maker Vulnerable POC for ZINC X

http://192.168.0.24/index

MAKER
Srbija

Please sign in

Email address

Password

☐ Remember me

Sign in

© Maker

Questions



Thank you for your time!

You can contact me via e-mail:

ivanm@security-net.biz

“If you think you are too small to make a difference, try sleeping with a mosquito.” - Dalai Lama XIV