

Arachni & OWASP Zed Attack Proxy

Course:

*Sicurezza delle reti e dei
sistemi software*

AA: 2016/2017



Arachni

- ▶ <http://www.arachni-scanner.com/>
- ▶ Multi-Platform (MS Windows, Mac OS X and Linux)
- ▶ Support highly complicated web applications
- ▶ Coded in Ruby
- ▶ Different approach in scanning
- ▶ Key Point:
 - free
 - simple
 - distributed
 - intelligent



Arachni Distributed Architecture

3 | 21

- ▶ Using deployed agents on remote servers
- ▶ Designed to integrate in existing infrastructure
- ▶ REST API
 - interoperability with non-Ruby systems
 - JSON messages
 - polling for progress
- ▶ RPC API
 - MessagePack
 - GridRPC

Arachni Example

```
1 ./bin/arachni http://192.168.1.7/wivet/ --checks trainer \  
2 --audit-links --audit-forms --scope-exclude-pattern=logout \  
3 --scope-exclude-pattern='100\.php' \  
4 --http-cookie-string="PHPSESSID=h4pksk4dte915acu8sa8rnds00"
```

Arachni Web UI

Arachni v1.4 - WebUI v0.5.10

Scans ▾

Profiles ▾

Dispatchers ▾

Users ▾

5 ▾

Administrator ▾

Welcome to Arachni, this is your dashboard.

Issues per scans, 'cause that's the way the cookie crumbles.

Notifications, about things you're involved in.

✓ Mark all read

Scan <http://10.10.30.25:81/dvwa/> (Default profile) completed – Thu, 06 Oct 2016 14:59:09 +0000

(Now deleted) Scan #5 completed – Thu, 06 Oct 2016 14:16:11 +0000

Review your activity, to freshen your memory.

Scan <http://10.10.30.25:81/dvwa/> (Default profile) was aborted – Thu, 06 Oct 2016 16:21:32 +0000

Scan <http://10.10.30.25:81/dvwa/> (Default profile) started – Thu, 06 Oct 2016 15:35:26 +0000

Scan <http://10.10.30.25:81/dvwa/> (Default profile) started – Thu, 06 Oct 2016 15:10:36 +0000

Scan <http://10.10.30.25:81/dvwa/> (Default profile) started – Thu, 06 Oct 2016 15:03:45 +0000

Scan <http://10.10.30.25:81/dvwa/> (Default profile) started – Thu, 06 Oct 2016 15:01:51 +0000

Scan <http://10.10.30.25:81/dvwa/> (Default profile) started – Thu, 06 Oct 2016 14:59:03 +0000

(Now deleted) Scan #5 started – Thu, 06 Oct 2016 14:15:52 +0000

Scan <http://10.10.30.25:81/dvwa/> (Default profile) started – Thu, 06 Oct 2016 10:44:18 +0000

Arachni GitHub

- ▶ <https://github.com/Arachni>
- ▶ Tasos Laskos
- ▶ Wiki
- ▶ Arachni Framework
 - Master (stable)
 - Experimental (alpha)
- ▶ Arachni UI Web

Arachni CLI

- ▶ github.com/Arachni/arachni/wiki/Command-line-user-interface
- ▶ Checks
 - `--checks=*, -csrf`
 - `--checks=xss*`
 - **Default** `--checks=*`
- ▶ Audit
 - `--audit-{audit_name}`
 - *Disabled by default*
 - *Template audit type expects a pattern*

Arachni CLI Customization

- ▶ **Generic**
- ▶ **Scope**
- ▶ **Output**
- ▶ **HTTP**
- ▶ **Input**
- ▶ **Session**
- ▶ **Report**
- ▶ **Plugin**

Arachni CLI Plugin

▶ `arachni --plugins-list`

▶ Login

➤ `arachni http://10.10.30.25:90
--plugin=autologin:url=http://10.10.30.25:90,parameters="name=user&pass=user&form_build_id=form-PW9ju5rKh70XU5uGnk_dGrVGw9AHctDt2TF65yyhHZQ&form_id=user_login_block&op=Log+in",check="My account"`

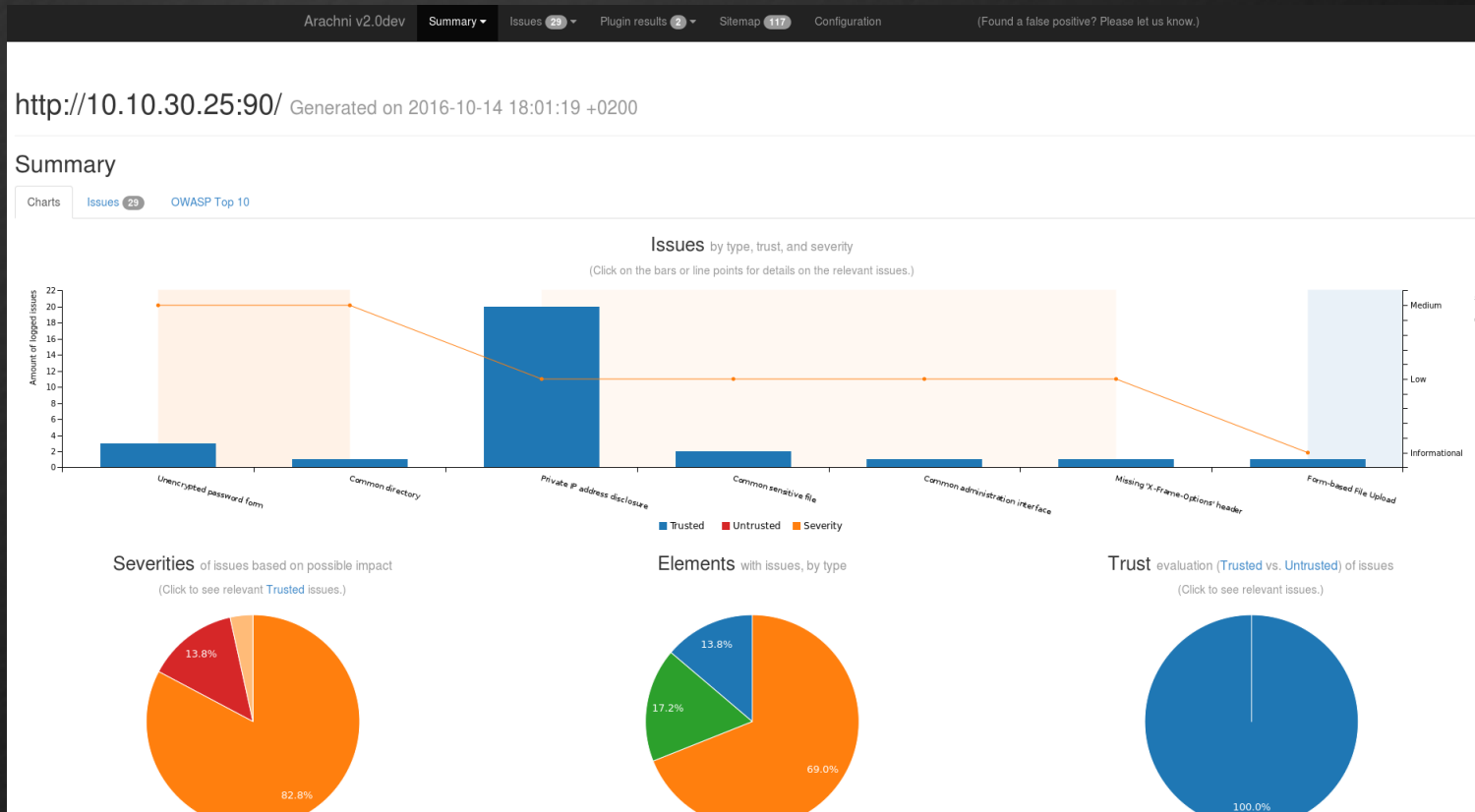
Arachni CLI Messages

- ▶ [*] are status messages
- ▶ [~] are informational messages
- ▶ [+] are success messages
- ▶ [v] are verbose messages
- ▶ [!] are debug messages
- ▶ [-] are error messages

Arachni Report

- ▶ `arachni_reporter reportName.afr --reporter=type:outfile=output.type`
 - XML (*experimental branch*)
 - HTML (zip)
 - Text
 - JSON
 - Stdout
- ▶ `arachni_reporter --reporters-list`

Arachni Report Example



Arachni Report Example (2)

```
function renderCharts() {
  if( window.renderedCharts )
    window.renderedCharts = true;

  c3.generate({
    bindto: '#chart-issues',
    data: {
      columns: [
        ["Trusted", 3, 1, 20, 2, 1, 1, 1],
        ["Untrusted", 0, 0, 0, 0, 0, 0, 0],
        ["Severity", 3, 3, 2, 2, 2, 2, 1]
      ],
      axes: {
        Severity: 'y2'
      },
      type: 'bar',
      groups: [
        ['Trusted', 'Untrusted']
      ]
    }
  });
}
```

OWASP Zed Attack Proxy

- ▶ www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- ▶ Open-Source Web Application Security Scanner
- ▶ Linux, Windows, OS X
- ▶ Fully translated over 25 languages
- ▶ Raspberry Pi! supported
- ▶ Good community
- ▶ ZAP is a fork of Paros Proxy



OWASP Zed Attack Proxy Functionally

15 | 21

- ▶ *Intercepting Proxy*
- ▶ *Traditional and AJAX spiders*
- ▶ *Automated scanner*
- ▶ *Passive scanner*
- ▶ *Forced browsing*
- ▶ *Fuzzer*
- ▶ *Dynamic SSL certificates*
- ▶ *Authentication and session support*

OWASP Zed Attack Proxy User Interface

16 | 21

File Edit View Analyse Report Tools Online Help

Standard Mode

Sites +

Quick Start Request Response +

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack:

Progress: Not started

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.
See the help file for more details.

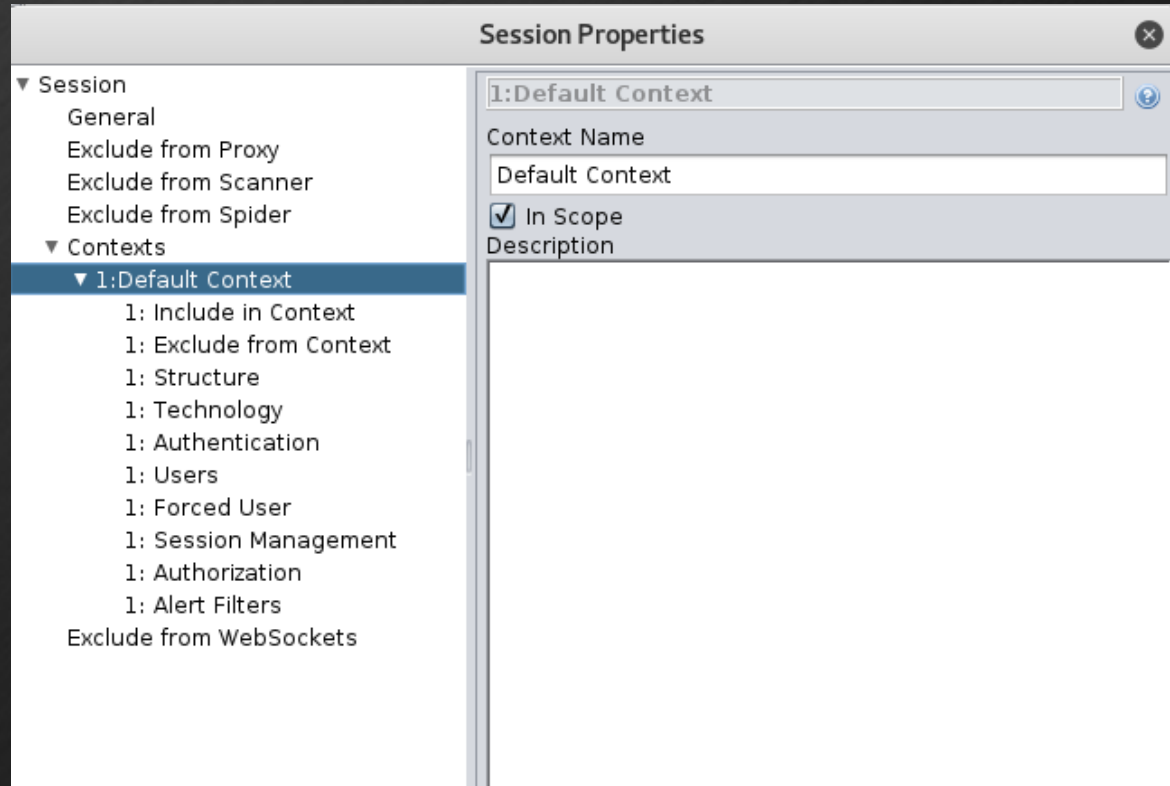
History Search Alerts Output Spider +

New Scan Progress: --Select Scan-- 0% Current Scans: 0 URIs Found: 0 Show Messages

Processed	Method	URI	Flags
-----------	--------	-----	-------

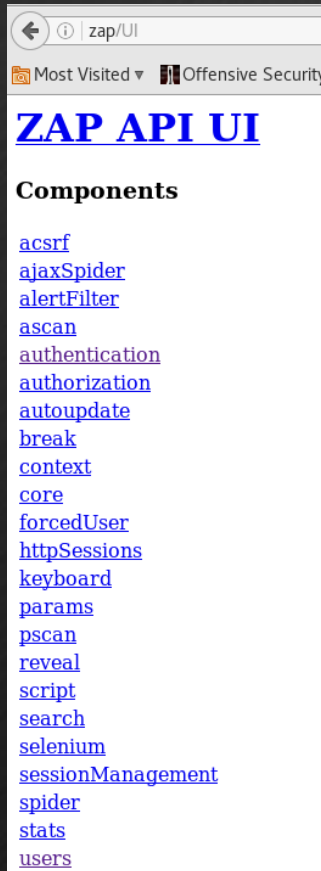
OWASP Zed Attack Proxy Context

17 | 21

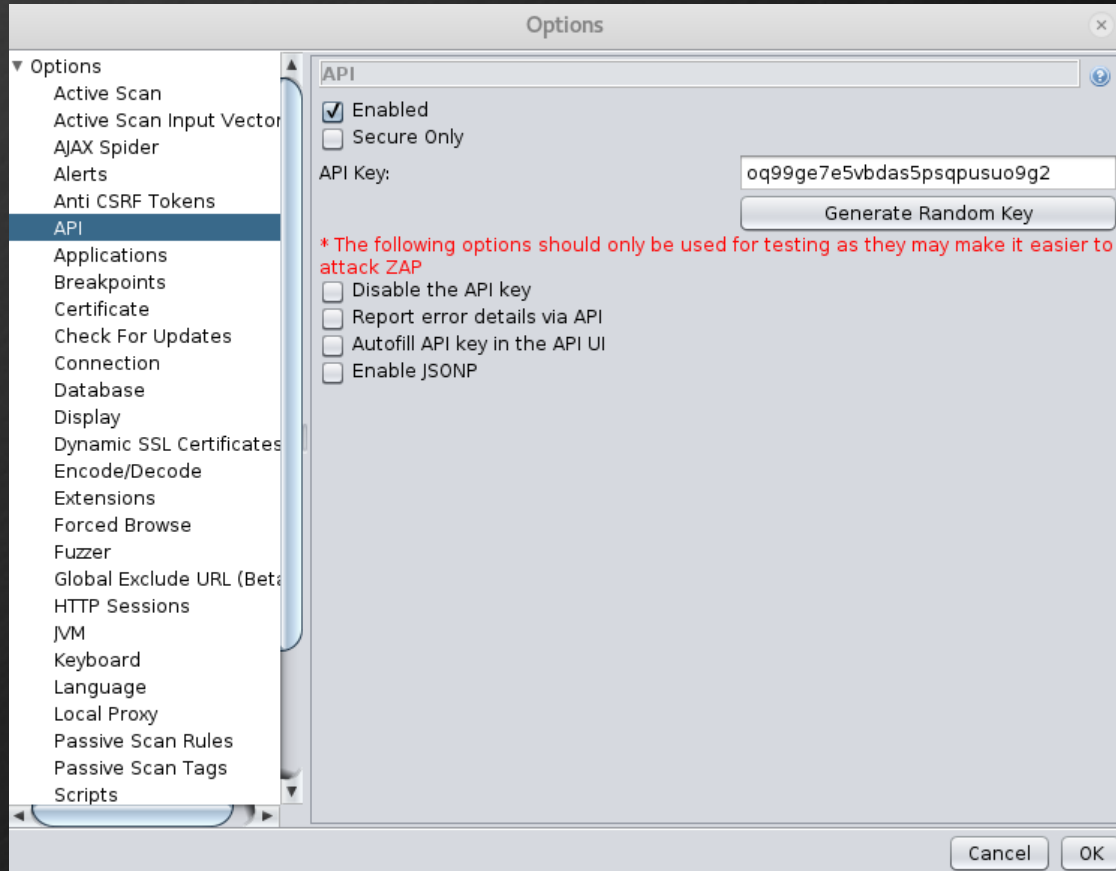


OWASP Zed Attack Proxy API

18 | 21



The screenshot shows the ZAP API UI web page. The browser address bar displays 'zap/UI'. The page title is 'ZAP API UI'. Under the 'Components' section, there is a list of links: [acsrif](#), [ajaxSpider](#), [alertFilter](#), [ascan](#), [authentication](#), [authorization](#), [autoupdate](#), [break](#), [context](#), [core](#), [forcedUser](#), [httpSessions](#), [keyboard](#), [params](#), [pscan](#), [reveal](#), [script](#), [search](#), [selenium](#), [sessionManagement](#), [spider](#), [stats](#), and [users](#).



The screenshot shows the 'Options' dialog box in OWASP ZAP. The 'API' option is selected in the left-hand menu. The 'API' section in the main pane has the following settings:

- Enabled
- Secure Only
- API Key:
-

A red warning message states: *** The following options should only be used for testing as they may make it easier to attack ZAP**

- Disable the API key
- Report error details via API
- Autofill API key in the API UI
- Enable JSONP

At the bottom right, there are 'Cancel' and 'OK' buttons.

OWASP Zed Attack Proxy API Programming Language

19 | 21

- ▶ <https://github.com/zaproxy/zaproxy/wiki/ApiDetails>
- ▶ Java (official)
- ▶ Python (official)
- ▶ Node.js (in progress)
- ▶ PHP (in progress)
- ▶ Ruby (no information)

Paros

- ▶ <https://sourceforge.net/projects/paros/>
- ▶ Java based HTTP/HTTPS proxy
- ▶ Assessing web application vulnerability
- ▶ Tampering request
- ▶ Spider
- ▶ Intelligent scanning for XSS and SQL injections
- ▶ Client certificate

Any Questions?

