


Automating Security Testing

Eric Therond ✉ contact@designsecurity.org

 Eric Therond <http://www.designsecurity.org>

What kinds of security tests can be automated ?

- ▶ Part of security tests is subjective
 - ▶ Acquire confidence about a service
 - ▶ Measure robustness of a service against experimented hackers
- ▶ Security tests coverage should include measure of
 - ▶ The legitimacy to collect and process personal data
 - ▶ The eligibility for access to a system
- ▶ It's difficult to test stakeholders expectatives.
- ▶ So detection of known vulnerabilities is our first goal.

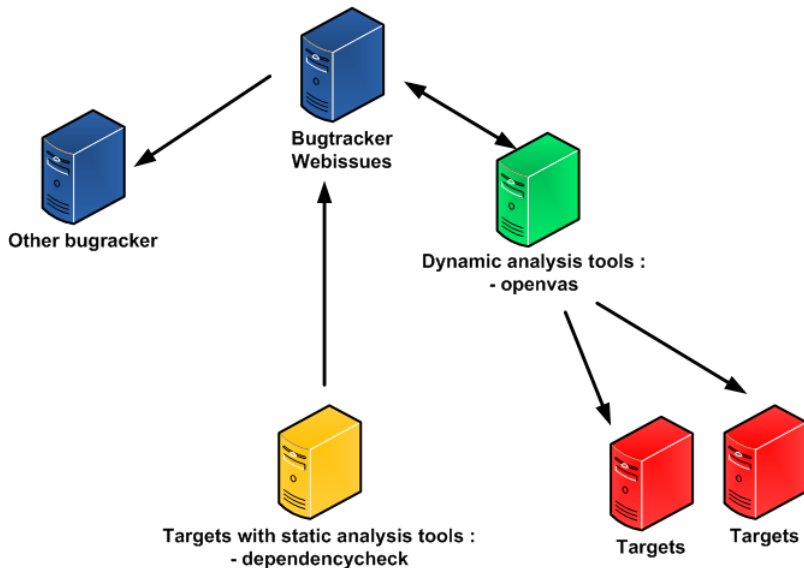
How security tests can be automated ?

- ▶ Automating security testing is a **cost project** : you need skilled and experimented QA for developing process, tools and documentation.
- ▶ An exploit which could be used to test the presence of heartbleed openssl vulnerability is about 700 lines of low level code : <https://www.exploit-db.com/exploits/32791/>
- ▶ More than 5000 new vulnerabilities are referenced each year : <http://www.cvedetails.com/browse-by-date.php>
- ▶ We are going to use open-source tools to test the exposure of organizations against those common vulnerabilities.
- ▶ It's a necessary step but for reasons invoked earlier it's not sufficient :
 - ▶ Each organization has his own known, specifics and legacies vulnerabilities which must be tested regularly.
 - ▶ Deeper analysis like intensive codes reviews and penetrations tests are the basics for critical systems.

What are the benefits of automated security tests ?




- ▶ Improve the coverage of systems under testing.
- ▶ Security experts are forsaken of manuals and repetitives tasks.
- ▶ You need a process for automating tests (developers and administrators are directly impliqued in the running of tests and remediations of detected defaults, SOC are correlated with security testing) and so the maturity of organizations increases quickly.
- ▶ Automated security tests are the first attacks that a hacker will doing against your organization, your knowledge of these techniques will help you to identify and block your attackers.


Illustrated Solution





Add servers

Servers

 Ajouter une demande |  Tout marquer comme lue |  Tout marquer comme non lue |

Vue : Toutes les demandes ▼  Ajouter une vue

ID ▼	Nom	ips address
#2372	 eric-pc	127.0.0.1,10.0.2.15
#2819	 box	192.168.1.1

Detailed Solution

- ▶ Project servers are added with the HIM or WebService.
- ▶ Each server can have multiple ips.
- ▶ These servers will be scan by dynamic analysis tools.
- ▶ By default the tool is OpenVas.

Add codes

Codes

Ajouter une demande | Tout marquer comme lue | Tout marquer comme non lue | Gérer les v

Vue : Ajouter une vue

ID ▼	Nom	code
#2229	java test	/home/eric/test/libs-java

Detailed Solution

- ▶ Project codes are added with the HIM or Webservice.
- ▶ Each code has a path.
- ▶ These paths will be scan by static analysis tools.
- ▶ By default the tool is DependencyCheck.

Run a scan

Nom	severity	tool
✉ scan_dependency-check_88	medium	dependency-check
✔ scan_openvas_88	medium	openvas
✉ test scan soap ui	medium	openvas

Detailed Solution

- ▶ Run scan with the HIM or WebService.
- ▶ All ips address in the folder servers will be scan.
- ▶ All paths codes in the folder codes will be scan.
- ▶ Filter as severity of bugs can be specified.
- ▶ When OpenVas finish a scan an alert is sent to the bugtracker and detected bugs are recorded in the associated folder.

View bugs

Nom	Date de modification	Modifié par	Assigné à	État	Sévérité
 known vulnerabilities in javax.servlet.jsp.jstl-1.2.1.jar	15/12/2015 13:01	dependency-check	Administrateur	Actif	2
 MySQL Authentication Error Message User Enumeration Vulne...	15/12/2015 13:28	openvas	Administrateur	Actif	2
 Check for SSL Weak Ciphers	15/12/2015 13:28	openvas	Administrateur	Actif	2
 Deprecated SSLV2 and SSLV3 Protocol Detection	15/12/2015 13:28	openvas	Administrateur	Actif	2
 DCShop exposes sensitive files	15/12/2015 13:28	openvas	Administrateur	Actif	2
 http TRACE XSS attack	15/12/2015 13:28	openvas	Administrateur	Actif	2
 MySQL weak password	15/12/2015 13:28	openvas	Administrateur	Actif	3
 Proxy accepts CONNECT requests to itself	15/12/2015 13:28	openvas	Administrateur	Actif	3

Detailed Solution

- ▶ View bugs with the HIM or WebService.
- ▶ The creator of the bug is the analysis tool.
- ▶ By default the bug is assigned to an administrator of the project.

Continuous Integration

- ▶ Other analysis tools can be used.
- ▶ All the methods can be used via Web Service.
- ▶ Duplicated bugs are handled.
- ▶ Bugs can be move to another bugtracker.
- ▶ Jobs in link with configuration management can be used :
- ▶ With Jenkins FSTrigger plugin you can Monitor file system when a server is added for example and run dynamic analysis scan (jobs/run_openvas.php).

Automating Security Testing

26/02/2016

Webinar build security - DesignSecurity