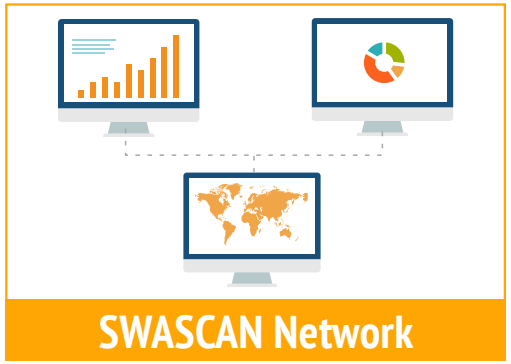
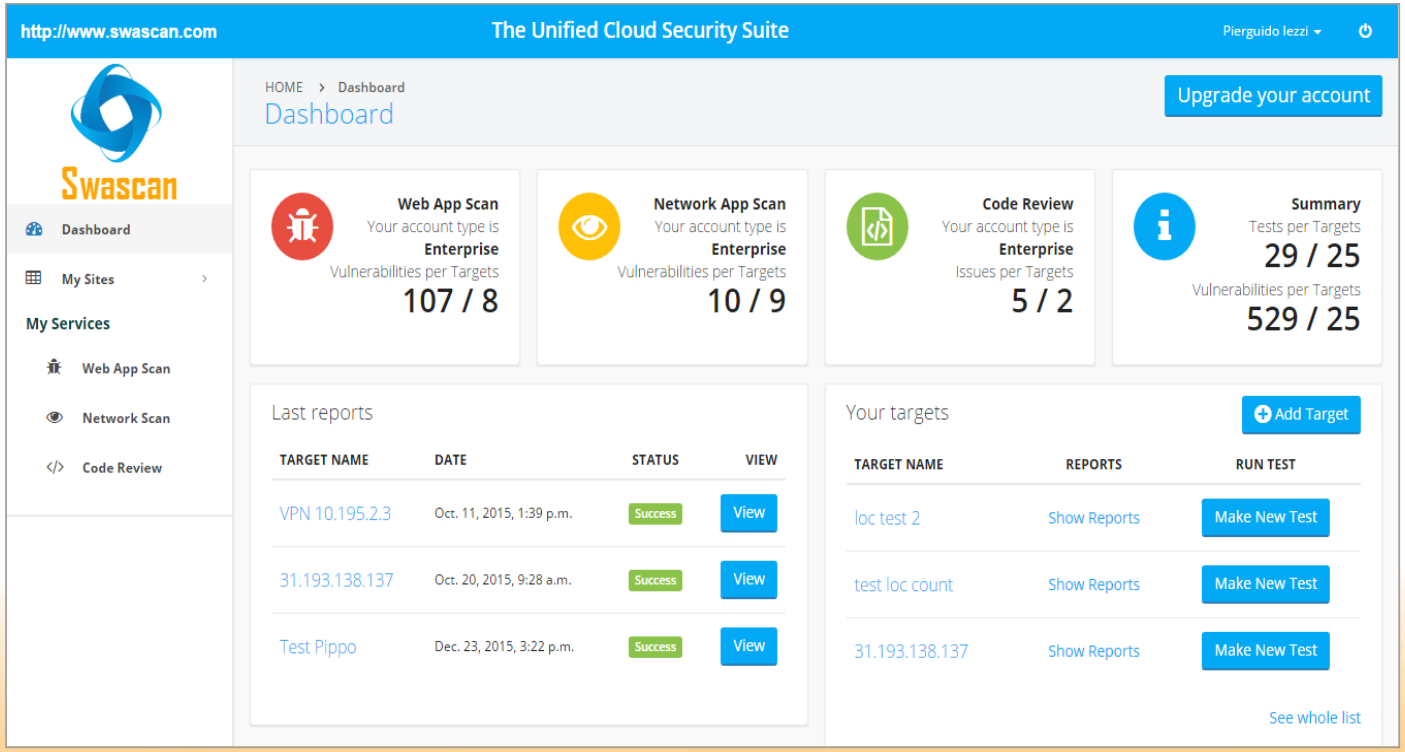
Swascan

The first all-in-one Cloud Security Suite Platform

SWASCAN ALL in ONE





SWASCAN at a Glance

The first Cloud Suite Security Platform

The right way to manage the Security Risk, both for web and mobile applications as well as the overall technological infrastructure

All-in-one SAAS that offers to its users:

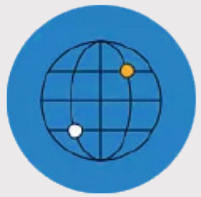
- Flexibility
- Cost cutting
- Scalability
- Accessibility
- Background to audit
- Compliance to regulations and OWASP best practises

Three main products:

- Web Application Scan
- Network Scan
- Code Review

SWASCAN Core Business

- The power and efficiency of Cloud technology is enhanced by a unique platform with a SaaS model, through different integrated and advanced tools.
- SWASCAN key products aim to test and verify the weaknesses of third-parties applications, preventing data-loss, and analyze the quality standards of company's network security, its compliance, internal policies and procedures, overall quality and the security of source code.
- SWASCAN also offers other features that complete the Suite and make it an ideal solution for the full risk management activity.



Scale

Global Scalability, Manageability

Discover

Automated, Dynamic, Deep Scanning

Assess

Scan application everywhere

Prioritize

Identify the highest business risk, and take action

SWASCAN Suite description: WEB APP SCAN

Swascan Web APP SCAN basically allows:

- To provide automated security testing and security scan of web applications to identify vulnerabilities
- To verify the weaknesses of third-parties applications that could generate loss of data or undesired accesses to private data
- To verify and guarantee the compliance to OWASP best practices and current regulations, identifying security issues of the applications
- To customize the length of the service (monthly, per year) and the number of targets to be analyzed

VULNERABILITY SCANNING

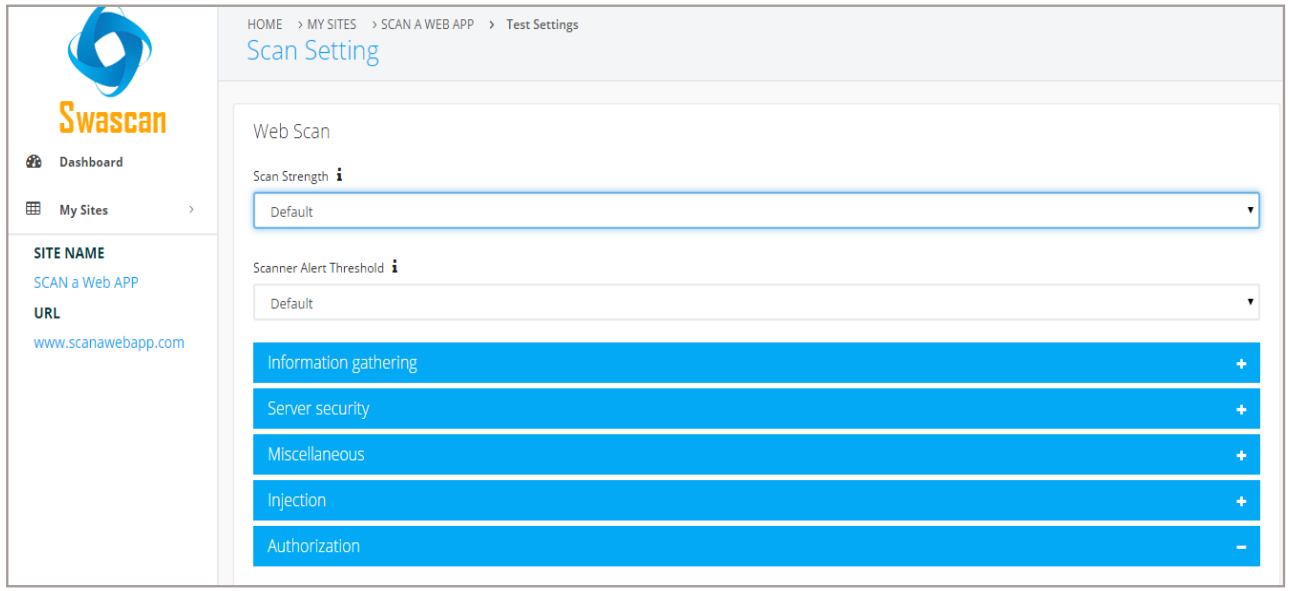
Provides a Web Application Scan. Identifies more than 200 different web application security flaws and vulnerabilities, including SQL injection, Cross-Site Scripting and many others

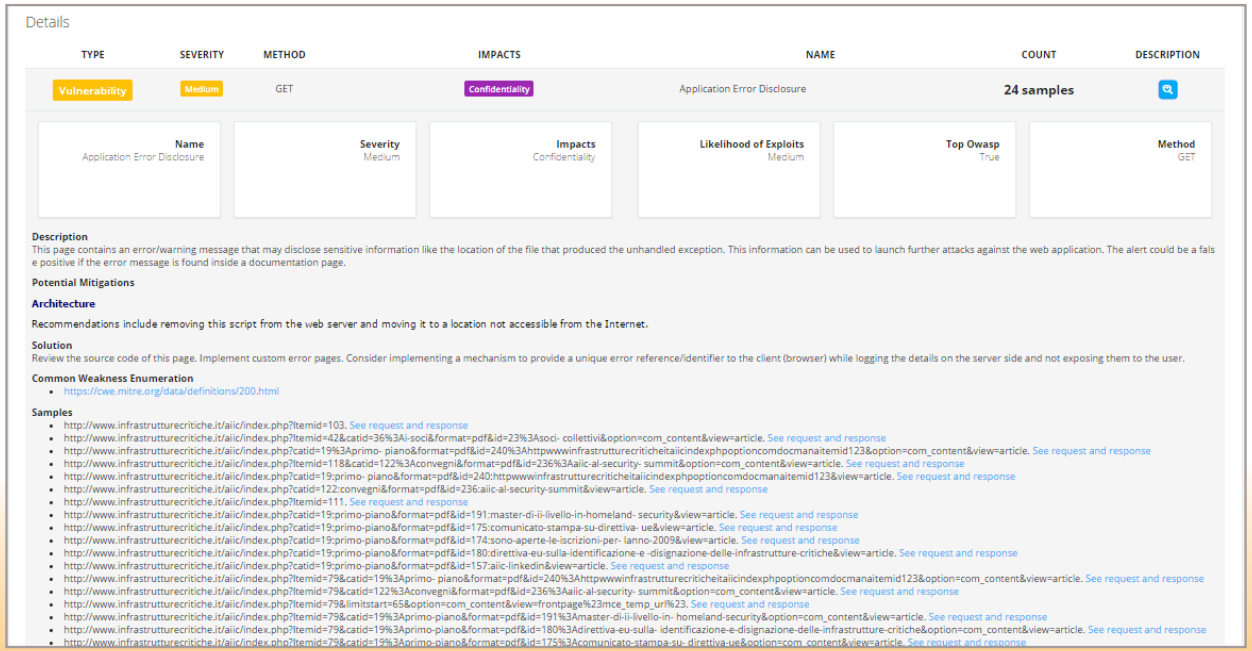
COMPLIANCE

Failure to comply with strict regulations can be costly for companies.
Swascan is an essential tool to help ensuring you to meet mandatory standards and avoid penalties.

AUDIT FRAMEWORK

Automatic generation of reports giving you a complete and detailed overview of your network inventory, status, and security risks.


Swascan
Dashboard
My Sites
SITE NAME
SCAN a Web APP
URL
www.scanawebapp.com
HOME › MY SITES › SCAN A WEB APP › Test Settings
Scan Setting
Web Scan
Scan Strength
Default
Scanner Alert Threshold
Default
Information gathering
Server security
Miscellaneous
Injection
Authorization


Details
TYPE
SEVERITY
METHOD
IMPACTS
NAME
COUNT
DESCRIPTION
Vulnerability
Medium
GET
Confidentiality
Application Error Disclosure
24 samples
Name
Application Error Disclosure
Severity
Medium
Impacts
Confidentiality
Likelihood of Exploits
Medium
Top Owasp
True
Method
GET
Description
This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a fals e positive if the error message is found inside a documentation page.
Potential Mitigations
Architecture
Recommendations include removing this script from the web server and moving it to a location not accessible from the Internet.
Solution
Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Common Weakness Enumeration
https://cwe.mitre.org/data/definitions/200.html
Samples


Swascan
Dashboard
My Sites
My Services
Web App
Network
Code
Target
Scan Type test
Web Scan
Date
July 24, 2015, 8:38 a.m.
New Test
Pages with victims
1946
Low Severity
4
(19827 samples)
Medium Severity
2
(5002 samples)
High Severity
0
(0 samples)
Vulnerabilities By Risk in %
Vulnerability Impacts
Likelihood of Exploits
Historical Diagram
TYPE
SEVERITY
METHOD
IMPACTS
NAME
COUNT
DESCRIPTION
Vulnerability
Medium
GET
Confidentiality
Application Error Disclosure
24 samples
Vulnerability
Medium
GET
Integrity, Confidentiality
X-Frame-Options Header Not Set
4978 samples
Vulnerability
Low
GET
Confidentiality
Cookie set without HttpOnly flag
5656 samples
Vulnerability
Low
GET
Confidentiality
Password Autocomplete in browser
4215 samples
Vulnerability
Low
GET
Integrity, Confidentiality, Availability, Access Control
Web Browser XSS Protection Not Enabled
4978 samples
Vulnerability
Low
GET
Confidentiality
X-Content-Type-Options Header Missing
4978 samples
Started at: July 24, 2015, 6:58 a.m.
Finished at: July 24, 2015, 8:38 a.m.
Export to PDF
Export List of Transactions to PDF
Export to CSV

SWASCAN Suite description: Network SCAN

Network Scan aims to Scan networks and devices and suggests you how they can be fixed.

- To Analyse the security level of company networks
- To Verify the compliance to current regulations
- To Check the company policies and internal procedures framework
- To Offer a security service customizable by number of targets

VULNERABILITY SCANNING

Successfully meet compliance regulations
Perform full vulnerability and port scanning
Manage organization-wide software deployment
Solve bring your own device (BYOD) headaches
Provide IT reports to your managers

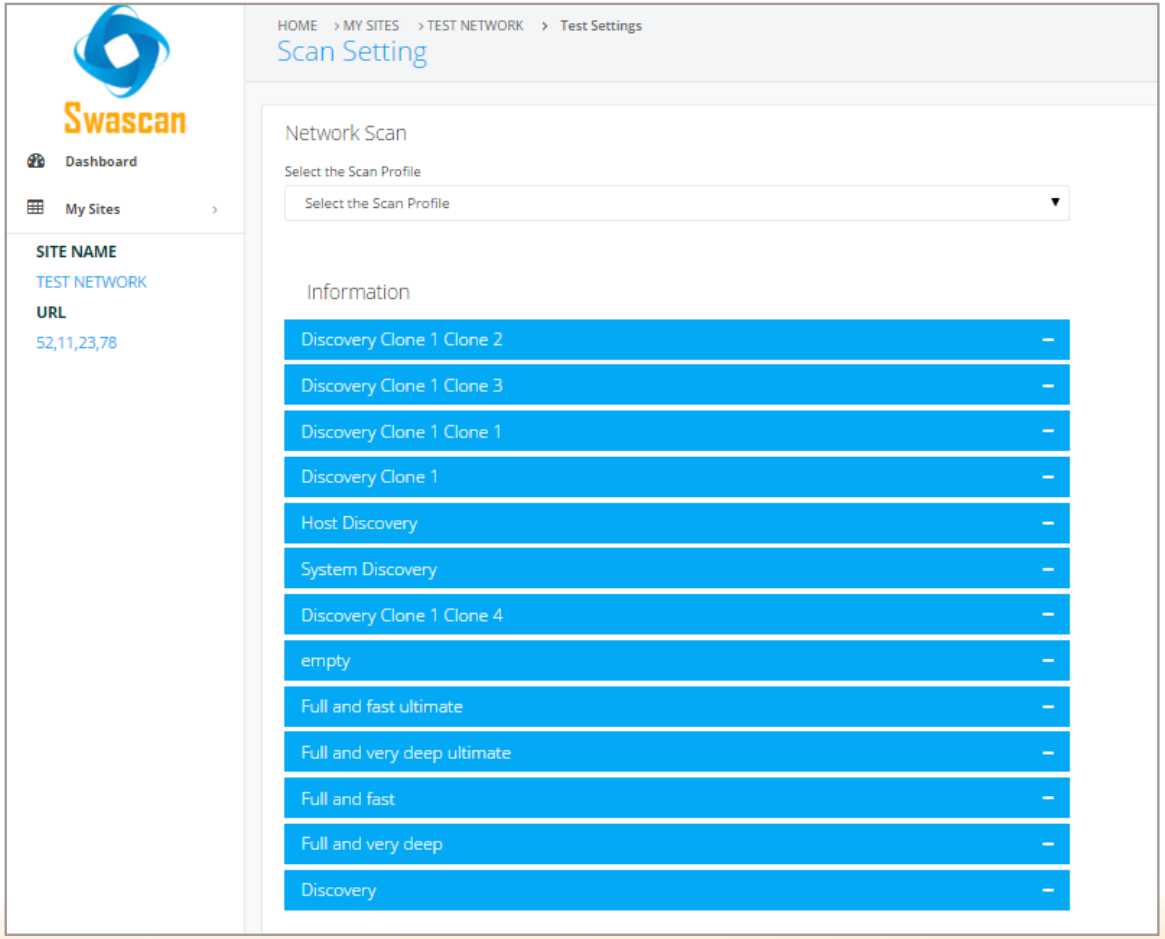
COMPLIANCE

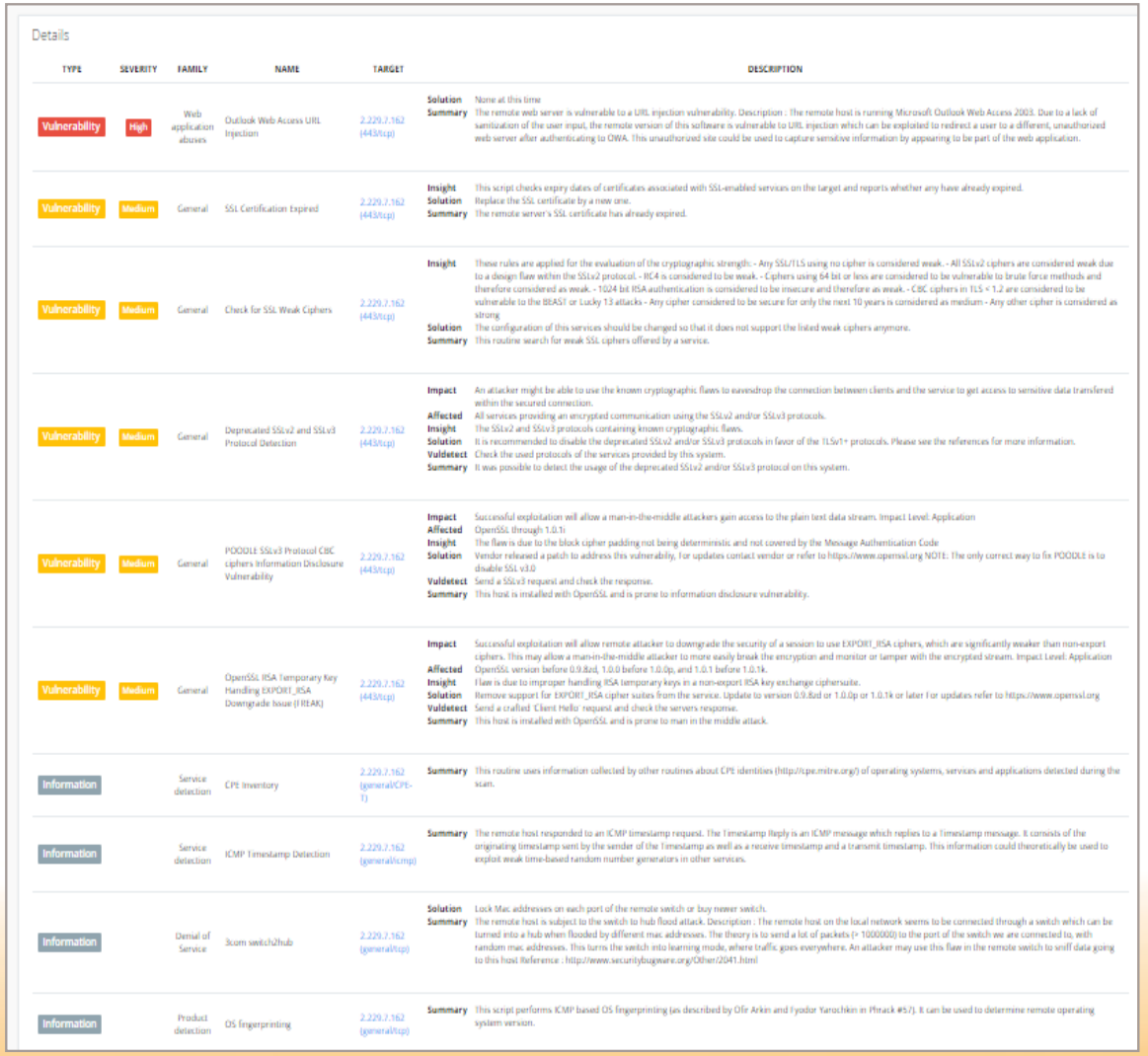
Generate reports of devices, computers, software
and applications installed in your network automatically, giving you a complete and
detailed overview of your network inventory, status, and security risks.

AUDIT FRAMEWORK

Automatically scan for and deploy missing security and non-security patches issued by Windows®, Mac OS®, Linux® and many third-party applications.

SWASCAN Suite description: Network SCAN





SWASCAN Suite description: Code Review

Code Review has been created to provide a source code analysis to identify and resolve security weaknesses and vulnerabilities

- To Test the vulnerability of source codes
- To Assess leaks and inefficiencies of source codes
- To Highlight the areas to intervene on

CODE REVIEW

- Easy to use
- Scans uncompiled code
- Highly accurate
  On-Premise & On-Demand

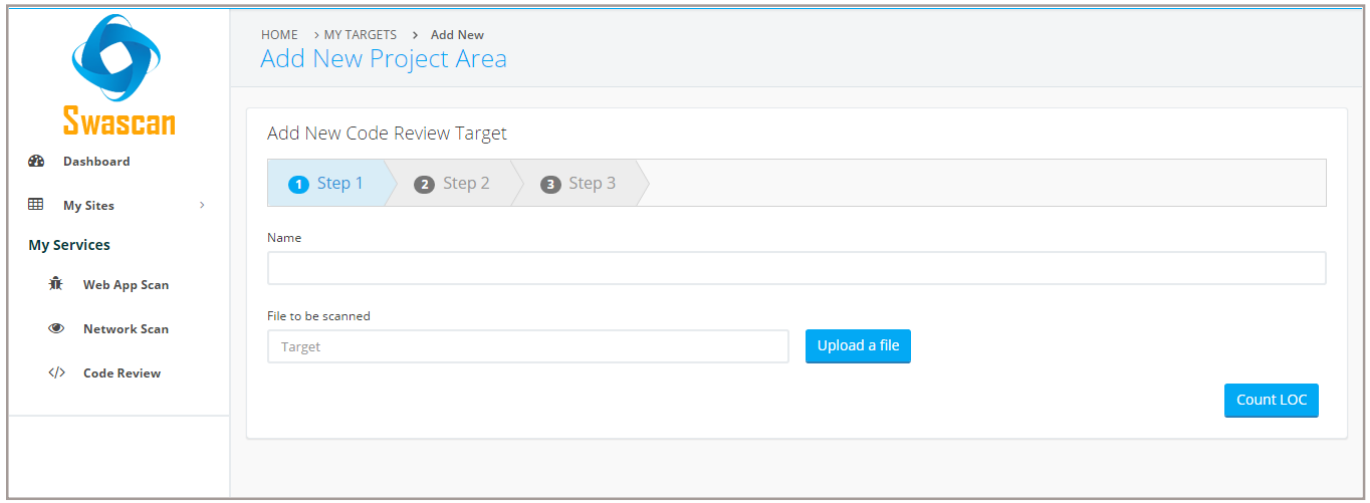
CODING LANGUAGES & FRAMEWORKS

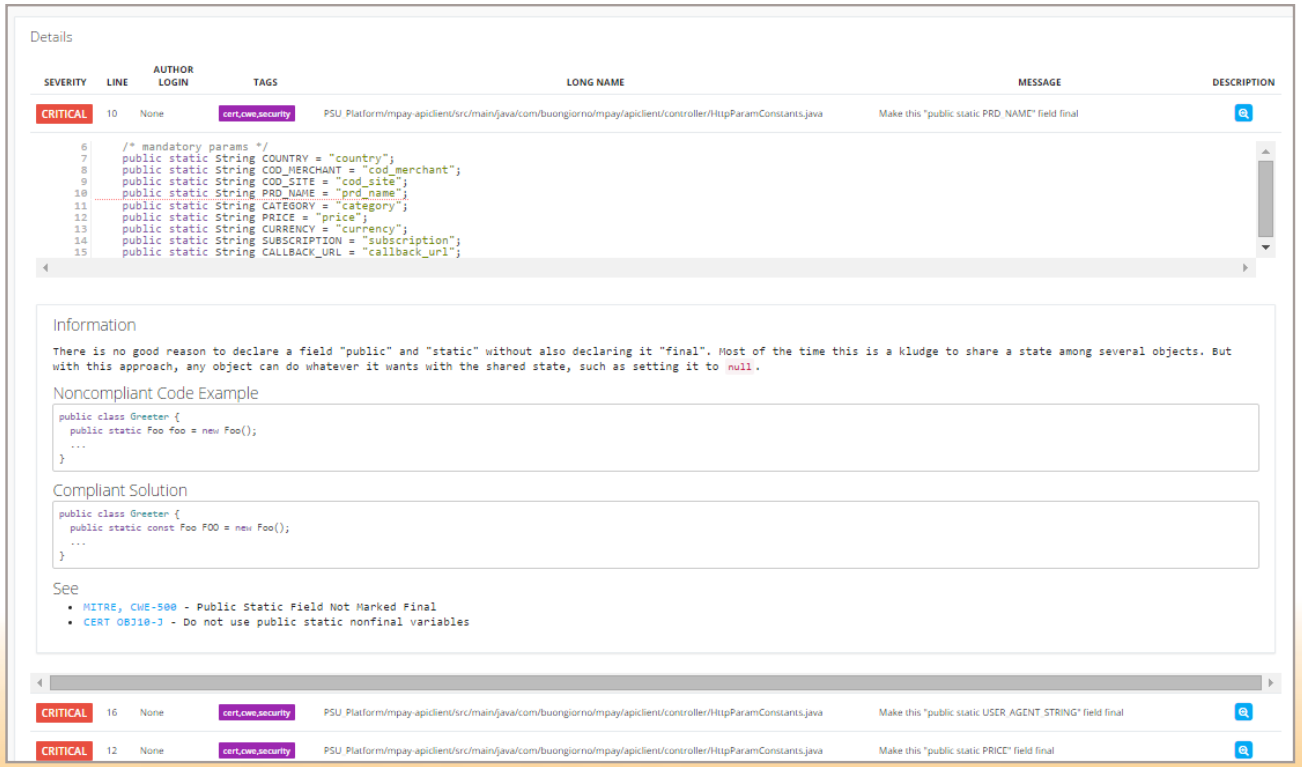
AUDITING AND COMPLIANCE

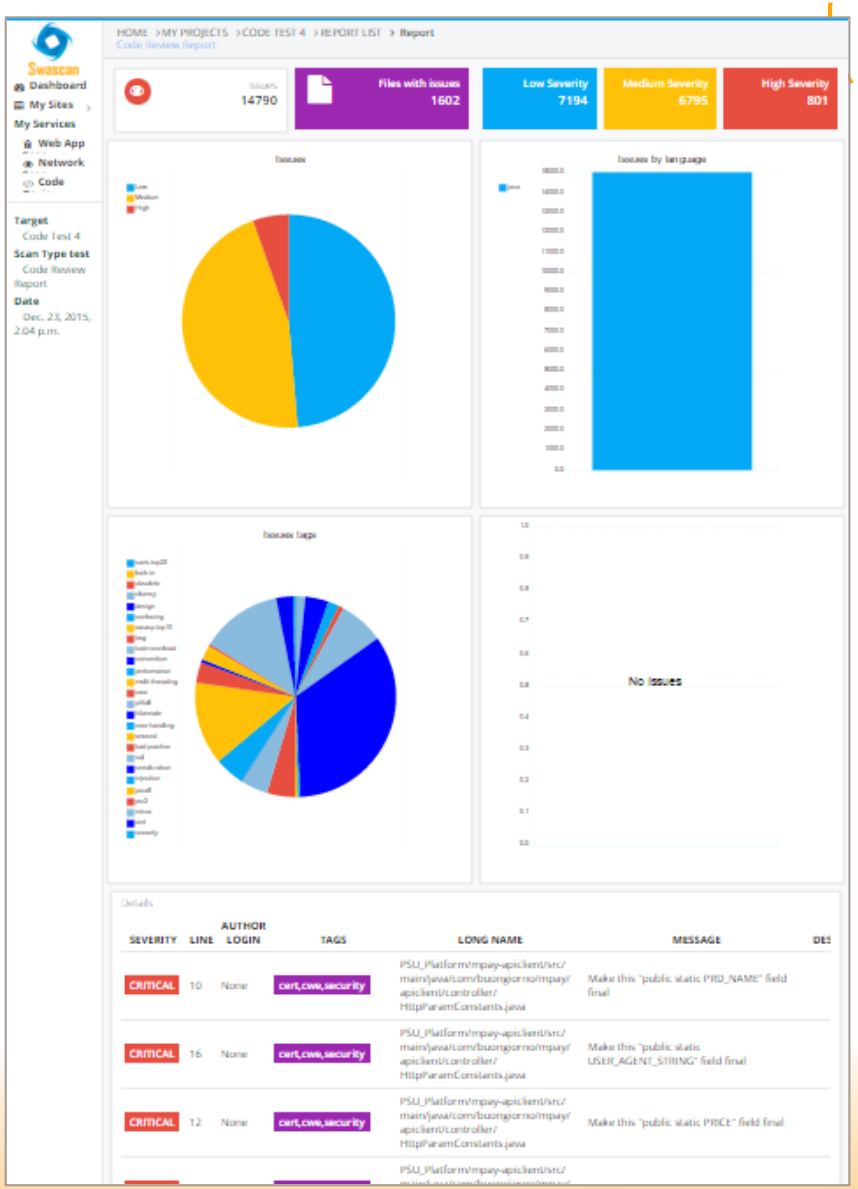
Security code review is the process of auditing the source code for an application to verify that the proper security controls are in place, that they work as intended and that they have been invoked in all the right places. Code review is a way of ensuring that the application has been developed to be “self-defended” in its given environment.

SWASCAN Code Review Languages

SUPPORTED LANGUAGES	STANDARD	ON DEMAND
ABAP		X
Android	X	
C/C++		X
C#	X	
COBOL		X
Groovy	X	
Java	X	
Javascript	X	
IOS		X
Objective-C		X
PHP	X	
PL/SQL		X
Python	X	
RPG		X
VB.NET		X
Visual Basic 6		X
Web	X	
XML	X	

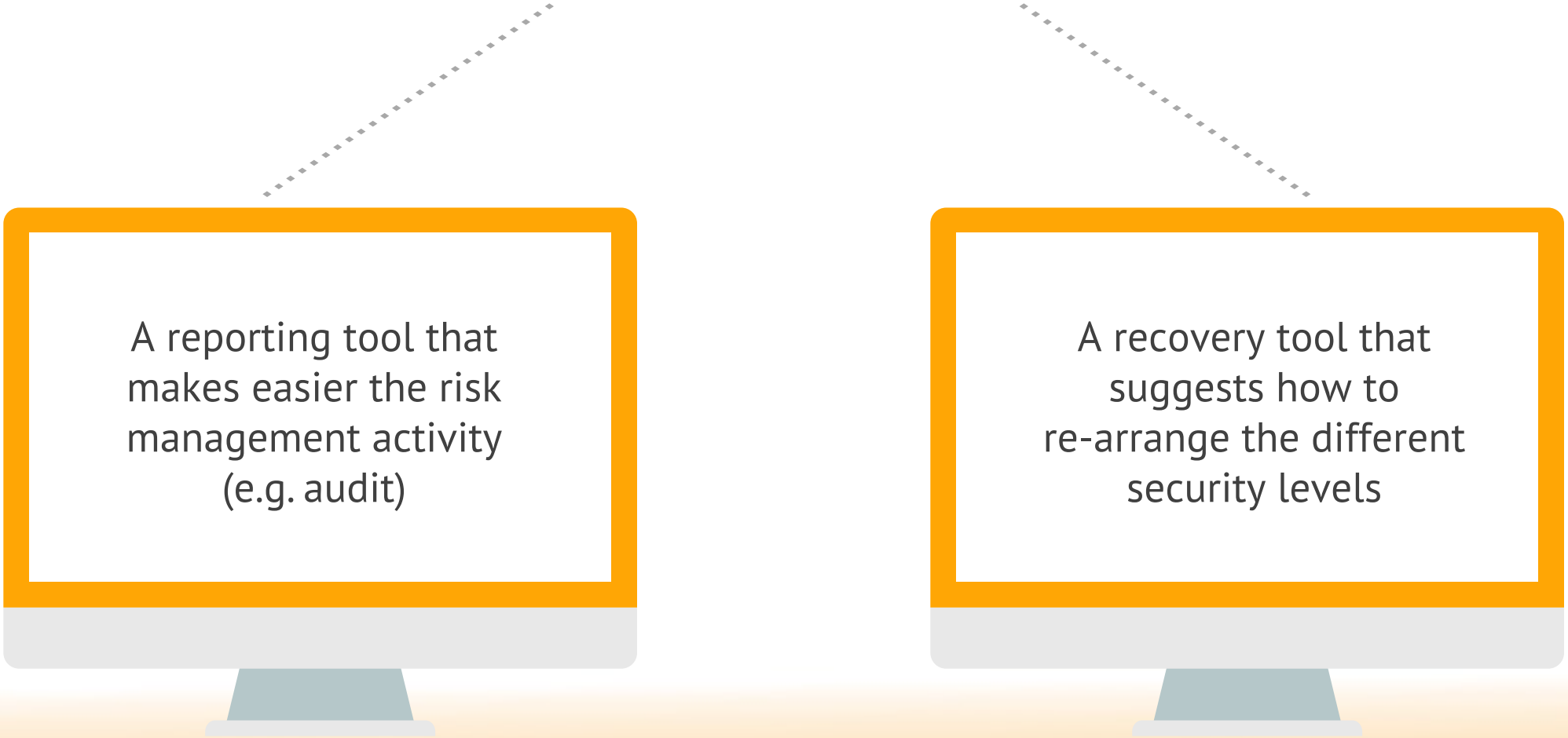

Swascan
Dashboard
My Sites
My Services
Web App Scan
Network Scan
Code Review
HOME › MY TARGETS › Add New
Add New Project Area
Add New Code Review Target
1 Step 1
2 Step 2
3 Step 3
Name
File to be scanned
Target
Upload a file
Count LOC


Details
SEVERITY
LINE
AUTHOR LOGIN
TAGS
LONG NAME
MESSAGE
DESCRIPTION
CRITICAL
10
None
cert,cwe,security
PSU_Platform/mpay-apiclient/src/main/java/com/buongiorno/mpay/apiclient/controller/HttpParamConstants.java
Make this "public static PRD_NAME" field final
/* mandatory params */
public static String COUNTRY = "country";
public static String COD_MERCHANT = "cod_merchant";
public static String COD_SITE = "cod_site";
public static String PRD_NAME = "prd_name";
public static String CATEGORY = "category";
public static String PRICE = "price";
public static String CURRENCY = "currency";
public static String SUBSCRIPTION = "subscription";
public static String CALLBACK_URL = "callback_url";
Information
There is no good reason to declare a field "public" and "static" without also declaring it "final". Most of the time this is a kludge to share a state among several objects. But with this approach, any object can do whatever it wants with the shared state, such as setting it to null.
Noncompliant Code Example
public class Greeter {
public static Foo foo = new Foo();
...
}
Compliant Solution
public class Greeter {
public static const Foo FOO = new Foo();
...
}
See
MITRE, CWE-500 - Public Static Field Not Marked Final
CERT OBJ10-J - Do not use public static nonfinal variables
CRITICAL
16
None
cert,cwe,security
PSU_Platform/mpay-apiclient/src/main/java/com/buongiorno/mpay/apiclient/controller/HttpParamConstants.java
Make this "public static USER_AGENT_STRING" field final
CRITICAL
12
None
cert,cwe,security
PSU_Platform/mpay-apiclient/src/main/java/com/buongiorno/mpay/apiclient/controller/HttpParamConstants.java
Make this "public static PRICE" field final

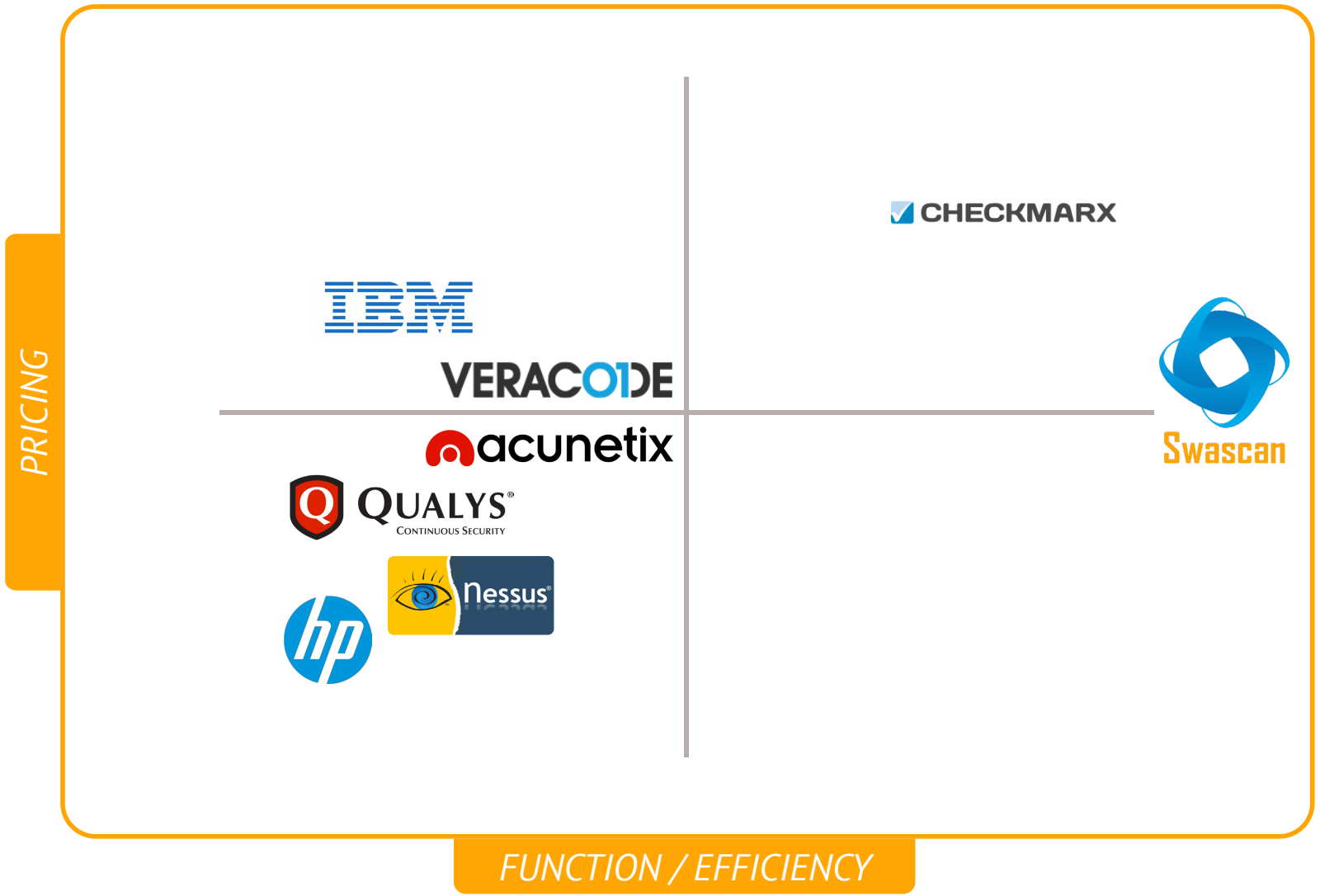

Swascan
Dashboard
My Sites
My Services
Web App
Network
Code
Target
Code Test 4
Scan Type test
Code Review Report
Date
Dec. 23, 2015, 2:04 p.m.
HOME › MY PROJECTS › CODE TEST 4 › REPORT LIST › Report
Code Review Report
14790
Files with issues
1602
Low Severity
7194
Medium Severity
6795
High Severity
801
Issues
Issues by language
Issues tags
No issues
Details
SEVERITY
LINE
AUTHOR LOGIN
TAGS
LONG NAME
MESSAGE
CRITICAL
10
None
cert,cwe,security
Make this "public static PRD_NAME" field final
CRITICAL
16
None
cert,cwe,security
Make this "public static USER_AGENT_STRING" field final
CRITICAL
12
None
cert,cwe,security
Make this "public static PRICE" field final

SWASCAN Suite description: other Services

The Suite has been enriched of other ancillary tools, that complete the platform:



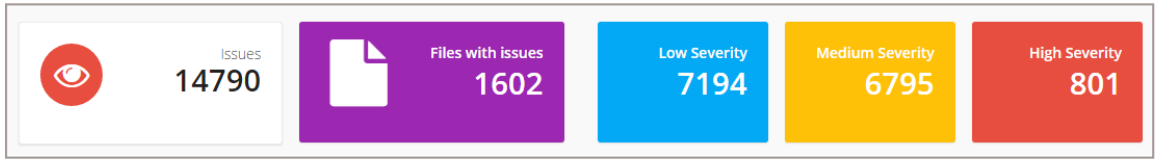
PRODUCT Positioning



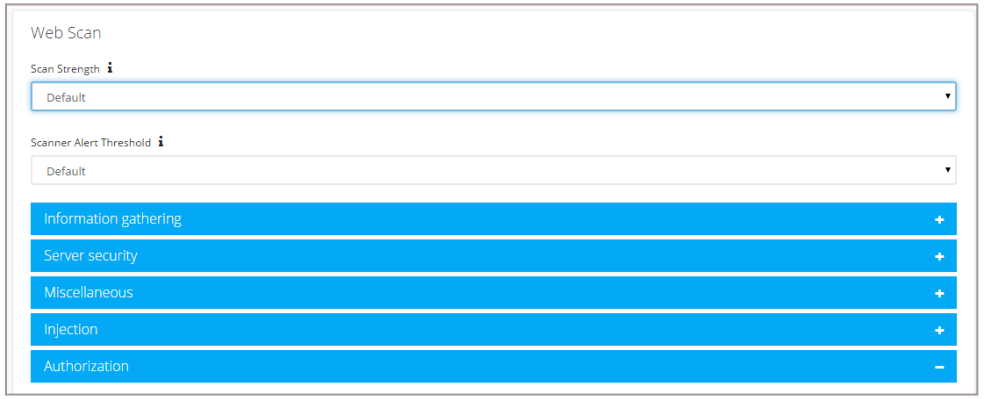
BATTLE Card

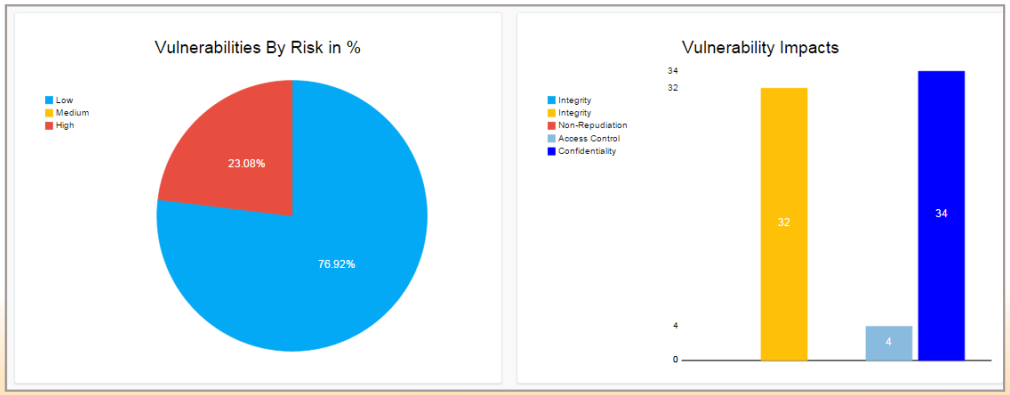
	CLOUD TECHNOLOGY	WEB SCAN	VPN SCAN	NETWORK SCAN	CODE REVIEW	ANNUAL LICENSE (NOT PERPETUAL)
Swascan	OK	OK	OK	OK	OK	OK
CHECKMARX	OK	NO	NO	NO	OK	NO
QUALYS® CONTINUOUS SECURITY	OK	OK	NO	OK	NO	NO
IBM	NO	OK	NO	OK	NO	NO
acunetix	NO	OK	OK	OK	NO	OK
hp	NO	NO	OK	OK	NO	OK
Nessus®	NO	OK	OK	OK	NO	OK

SWASCAN Screenshot



TYPE	SEVERITY	METHOD	IMPACTS	NAME	COUNT	DESCRIPTION
Vulnerability	Medium	GET	Integrity, Confidentiality	X-Frame-Options Header Not Set	107 samples	
Vulnerability	Low	GET	Confidentiality	Cookie set without secure flag	85 samples	
Vulnerability	Low	GET	Confidentiality	Incomplete or No Cache-control and Pragma HTTP Header Set	100 samples	
Vulnerability	Low	GET	Integrity, Confidentiality, Availability, Access Control	Web Browser XSS Protection Not Enabled	107 samples	
Vulnerability	Low	GET	Confidentiality	X-Content-Type-Options Header Missing	107 samples	





Details

TYPE	SEVERITY	METHOD	IMPACTS	NAME	COUNT	DESCRIPTION
Vulnerability	Medium	GET	Integrity, Confidentiality	X-Frame-Options Header Not Set	107 samples	

Name	Severity	Impacts	Likelihood of Exploits	Top Owasp	Method
X-Frame-Options Header Not Set	Medium	Integrity, Confidentiality	High	None	GET

Description
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

Potential Mitigations

Implementation

This Vulnerability identifies the pages for X-Frame-Options header and so for possible ClickJacking attack against URL.

There are two main ways to prevent clickjacking:

1. Sending the proper X-Frame-Options HTTP response headers that instruct the browser to not allow framing from other domains
2. Employing defensive code in the UI to ensure that the current frame is the most top level window

Solution
Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).

References
- http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

SWASCAN Competence: Security Management

Policy and Compliance

Adaptation to the regulatory and legislative law/body in the field of security Personal Data Protection and Privacy...

Risk Management

Analysis and assessment of the level of maturity of the security system in order to define a correct security strategy

ICT Security

Management of activities of ethical hacking to verify the security of the systems and infrastructures

Information Security

Development of the ISMS System for the support of the international security certification ISO 27001

SWASCAN Team

The right mix to achieve extraordinary results:

business competence
Turn Risk Into Opportunity

an established
software developer
(**Business Competence**)

- Software development and updates
- Business development
- Monitoring of innovation related to the Security field

KEYCAPITAL

a “digital”
Venture Incubator
(**Key Capital**)

- Business development
- Administration and legal issues
- Corporate strategy

a Security
Expert
(**Raoul Chiesa**)

- Business development
- Networking
- Strong expertise on cyber-security, hacking, cyber-crime

  Member of several Security agencies, associations, European groups, domestic and International governments task forces

Swascan

The first all-in-one Cloud Security Suite Platform

info@swascan.com