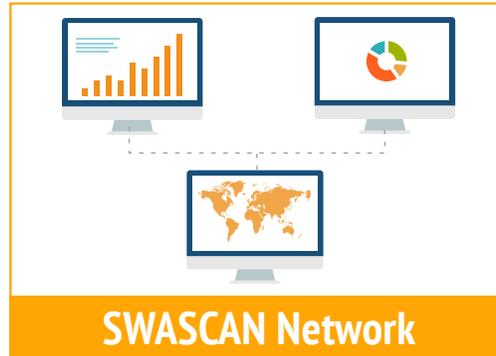




Swascan

The first all-in-one Cloud Security Suite Platform

SWASCAN ALL in ONE



http://www.swascan.com The Unified Cloud Security Suite Pierguido Iezzi

HOME > Dashboard Dashboard Upgrade your account

Web App Scan
Your account type is **Enterprise**
Vulnerabilities per Targets
107 / 8

Network App Scan
Your account type is **Enterprise**
Vulnerabilities per Targets
10 / 9

Code Review
Your account type is **Enterprise**
Issues per Targets
5 / 2

Summary
Tests per Targets
29 / 25
Vulnerabilities per Targets
529 / 25

Last reports

TARGET NAME	DATE	STATUS	VIEW
VPN 10.195.2.3	Oct. 11, 2015, 1:39 p.m.	Success	View
31.193.138.137	Oct. 20, 2015, 9:28 a.m.	Success	View
Test Pippo	Dec. 23, 2015, 3:22 p.m.	Success	View

Your targets

TARGET NAME	REPORTS	RUN TEST
loc test 2	Show Reports	Make New Test
test loc count	Show Reports	Make New Test
31.193.138.137	Show Reports	Make New Test

See whole list

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.

HOME > MY SITES > SCAN A WEB APP > Test Settings

Scan Setting

Web Scan

Scan Strength **i**

Default

Scanner Alert Threshold **i**

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	Severity	Impacts	Likelihood of Exploits	Top Owasp	Method
Application Error Disclosure	Medium	Confidentiality	Medium	True	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 false 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

- <http://www.infrastrutturericriche.it/aiic/index.php?itemid=103>. See request and response
- http://www.infrastrutturericriche.it/aiic/index.php?itemid=42&catid=36&3Aa-soc&format=pdf&id=2363Aaoc-collettivi&option=com_content&view=article. See request and response
- http://www.infrastrutturericriche.it/aiic/index.php?catid=19&3Aprimo-piano&format=pdf&id=2403Ahttpwwinfrastrutturericricheitaicindexpoptioconcomocmanatemid123&option=com_content&view=article. See request and response
- http://www.infrastrutturericriche.it/aiic/index.php?itemid=118&catid=122&3Aconvegni&format=pdf&id=2363Aaic-al-security-submit&option=com_content&view=article. See request and response
- <http://www.infrastrutturericriche.it/aiic/index.php?catid=19&3Aprimo-piano&format=pdf&id=2403Ahttpwwinfrastrutturericricheitaicindexpoptioconcomocmanatemid123&view=article>. See request and response
- <http://www.infrastrutturericriche.it/aiic/index.php?catid=122&convegni&format=pdf&id=2363Aaic-al-security-submit&view=article>. See request and response
- <http://www.infrastrutturericriche.it/aiic/index.php?itemid=111>. See request and response
- <http://www.infrastrutturericriche.it/aiic/index.php?catid=19&3Aprimo-piano&format=pdf&id=191&master-di-il-livello-in-homeland-security&view=article>. See request and response
- <http://www.infrastrutturericriche.it/aiic/index.php?catid=19&3Aprimo-piano&format=pdf&id=175&comunicato-stampa-su-direttiva-ue&view=article>. See request and response
- <http://www.infrastrutturericriche.it/aiic/index.php?catid=19&3Aprimo-piano&format=pdf&id=174&sono-aperte-le-iscrizioni-per-lanno-2009&view=article>. See request and response
- <http://www.infrastrutturericriche.it/aiic/index.php?catid=19&3Aprimo-piano&format=pdf&id=180&direttiva-eu-sulla-identificazione-e-disignazione-delle-infrastrutture-critiche&view=article>. See request and response
- <http://www.infrastrutturericriche.it/aiic/index.php?catid=19&3Aprimo-piano&format=pdf&id=157&aic-linkedin&view=article>. See request and response
- http://www.infrastrutturericriche.it/aiic/index.php?itemid=79&catid=19&3Aprimo-piano&format=pdf&id=24093Ahttpwwinfrastrutturericricheitaicindexpoptioconcomocmanatemid123&option=com_content&view=article. See request and response
- http://www.infrastrutturericriche.it/aiic/index.php?itemid=79&catid=122&3Aconvegni&format=pdf&id=2363Aaic-al-security-submit&option=com_content&view=article. See request and response
- http://www.infrastrutturericriche.it/aiic/index.php?itemid=79&catid=19&3Aprimo-piano&format=pdf&id=174&sono-aperte-le-iscrizioni-per-lanno-2009&temp_url%23. See request and response
- http://www.infrastrutturericriche.it/aiic/index.php?itemid=79&catid=19&3Aprimo-piano&format=pdf&id=180&direttiva-eu-sulla-identificazione-e-disignazione-delle-infrastrutture-critiche&option=com_content&view=article. See request and response
- http://www.infrastrutturericriche.it/aiic/index.php?itemid=79&catid=19&3Aprimo-piano&format=pdf&id=175&3Acomunicato-stampa-su-direttiva-ue&option=com_content&view=article. See request and response

HOME > MY SITES > HTTP://WWW.INFRASTRUTTURECRITICHE.IT > REPORT LIST > Report

Vulnerability Web Scan Report

6 Vulnerabilities (24820 samples) | 1946 Pages with victims | 4 Low Severity (19827 samples) | 2 Medium Severity (5002 samples) | 0 High Severity (0 samples)

Target: http://www.infrastrutturericriche.it
Scan Type: Web Scan
Date: July 24, 2015, 8:38 a.m.

Vulnerability by Risk in %

Low	70.0%
Medium	29.9%
High	0.0%

Vulnerability Impacts

Availability	1000
Integrity	2000
Non-Repudiation	1000
Privacy Control	1000
Confidentiality	7000

Likelihood of Exploits

Low	32.0%
Medium	40.7%
High	27.3%

Historical Diagram

Details

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

Powered by Business Competence | info@swascan.com



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





[HOME](#) > [MY SITES](#) > [TEST NETWORK](#) > [Test Settings](#)

Scan Setting

Network Scan

Select the Scan Profile

Select the Scan Profile

Information

Discovery Clone 1 Clone 2	-
Discovery Clone 1 Clone 3	-
Discovery Clone 1 Clone 1	-
Discovery Clone 1	-
Host Discovery	-
System Discovery	-
Discovery Clone 1 Clone 4	-
empty	-
Full and fast ultimate	-
Full and very deep ultimate	-
Full and fast	-
Full and very deep	-
Discovery	-

SITE NAME

TEST NETWORK

URL

52,11,23,78

TYPE	SEVERITY	FAMILY	NAME	TARGET	DESCRIPTION
Vulnerability	High	Web application abuses	Outlook Web Access URL Injection	2.229.7.162 (443/tcp)	Solution Summary None at this time. The remote web server is vulnerable to a URL injection vulnerability. Description : The remote host is running Microsoft Outlook Web Access 2003. Due to a lack of sanitization of the user input, the remote version of this software is vulnerable to URL injection which can be exploited to redirect a user to a different, unauthorized web server after authenticating to OWA. This unauthorized site could be used to capture sensitive information by appearing to be part of the web application.
Vulnerability	Medium	General	SSL Certification Expired	2.229.7.162 (443/tcp)	Insight This script checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired. Solution Summary Replace the SSL certificate by a new one. The remote server's SSL certificate has already expired.
Vulnerability	Medium	General	Check for SSL Weak Ciphers	2.229.7.162 (443/tcp)	Insight These rules are applied for the evaluation of the cryptographic strength: - Any SSL/TLS using no cipher is considered weak. - All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol. - RC4 is considered to be weak. - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak. - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - CBC ciphers in TLS v 1.2 are considered to be vulnerable to the BREAST or Lucky 13 attacks. - Any cipher considered to be secure for only the next 10 years is considered as medium. - Any other cipher is considered as strong. Solution Summary The configuration of this services should be changed so that it does not support the listed weak ciphers anymore. This routine search for weak SSL ciphers offered by a service.
Vulnerability	Medium	General	Deprecated SSLv2 and SSLv3 Protocol Detection	2.229.7.162 (443/tcp)	Impact An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Affected All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols. Insight The SSLv2 and SSLv3 protocols containing known cryptographic flaws. Solution It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information. Validated Check the used protocols of the services provided by this system. Summary It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.
Vulnerability	Medium	General	POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	2.229.7.162 (443/tcp)	Impact Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data streams. Impact Level: Application Affected OpenSSL, through 1.0.1i Insight The flaw is due to the block cipher padding not being deterministic, and not covered by the Message Authentication Code Solution Vendor released a patch to address this vulnerability. For updates contact vendor or refer to https://www.openssl.org/NOTICE. The only correct way to fix POODLE is to disable SSL v3.0 Validated Send a SSLv3 request and check the response. Summary This host is installed with OpenSSL, and is prone to information disclosure vulnerability.
Vulnerability	Medium	General	OpenSSL RSA Temporary Key Handling EXPORT_RSA Downgrade Issue (1 REAK)	2.229.7.162 (443/tcp)	Impact Successful exploitation will allow remote attacker to downgrade the security of a session to use EXPORT_RSA ciphers, which are significantly weaker than non-export ciphers. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream. Impact Level: Application Affected OpenSSL, version before 0.9.8a, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k. Insight Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite. Solution Remove support for EXPORT_RSA cipher suites from the service. Update to version 0.9.8a or 1.0.0p or 1.0.1k or later. For updates refer to https://www.openssl.org Validated Send a crafted Client Hello request and check the servers response. Summary This host is installed with OpenSSL, and is prone to man in the middle attack.
Information		Service detection	CPE Inventory	2.229.7.162 (general/CPE-1)	Summary This routine uses information collected by other routines about CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.
Information		Service detection	ICMP Timestamp Detection	2.229.7.162 (general/icmp)	Summary The remote host responded to an ICMP timestamp request. The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.
Information		Denial of Service	3com switch2hub	2.229.7.162 (general/tcp)	Solution Summary Lock Mac addresses on each port of the remote switch or buy newer switch. The remote host is subject to the switch to hub flood attack. Description : The remote host on the local network seems to be connected through a switch which can be turned into a hub when flooded by different mac addresses. The theory is to send a lot of packets (> 1000000) to the port of the switch we are connected to, with random mac addresses. This turns the switch into learning mode, where traffic goes everywhere. An attacker may use this flaw in the remote switch to sniff data going to this host. Reference : http://www.securitybugzone.org/Other/2041.html
Information		Product detection	OS Fingerprinting	2.229.7.162 (general/tcp)	Summary This script performs ICMP based OS fingerprinting (as described by Ofer Arkin and Yzador Yanochkin in Phrack #57). It can be used to determine remote operating system version.

SWASCAN Suite description: Code Review



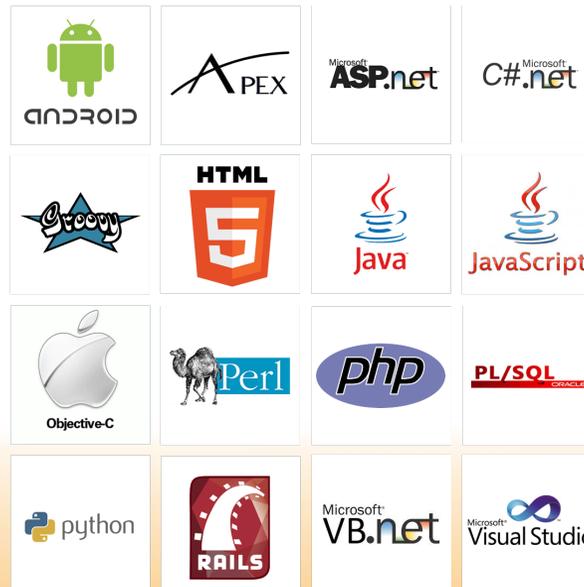
Code Review has been created to provide a source code analysis to identify and resolve security weaknesses and vulnerabilities

- 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

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	
<pre> 6 /* mandatory params */ 7 public static String COUNTRY = "country"; 8 public static String COD_MERCHANT = "cod_merchant"; 9 public static String COD_SITE = "cod_site"; 10 public static String PRD_NAME = "prd_name"; 11 public static String CATEGORY = "category"; 12 public static String PRICE = "price"; 13 public static String CURRENCY = "currency"; 14 public static String SUBSCRIPTION = "subscription"; 15 public static String CALLBACK_URL = "callback_url"; </pre>						

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-588 - Public Static Field Not Marked Final
- CERT OB310-3 - 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	



Dashboard

My Sites

My Services

Web App Scan

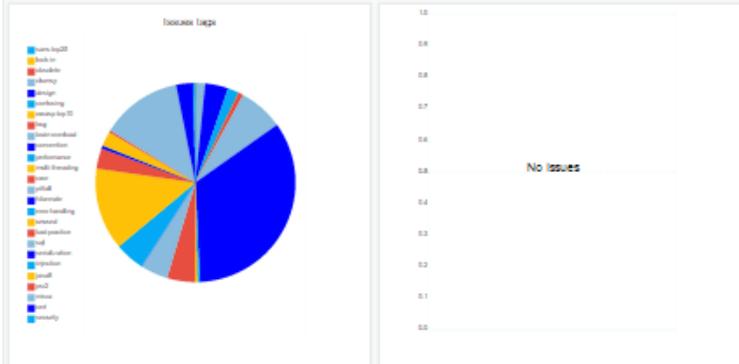
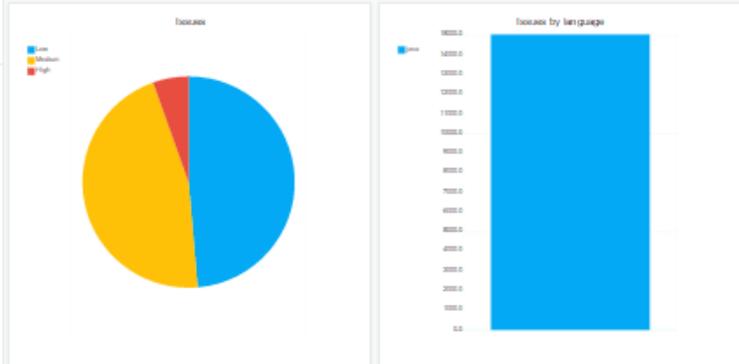
Network Scan

Code Review

HOME > MY PROJECTS > CODE TEST 4 > REPORT LIST > Report

Code Review Report

Issues: 14790
 Files with Issues: 1602
 Low Severity: 7194
 Medium Severity: 6795
 High Severity: 801



Details

SEVERITY	LINE	AUTHOR LOGIN	TAGS	LONG NAME	MESSAGE	DES
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	
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 Suite description: other Services

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

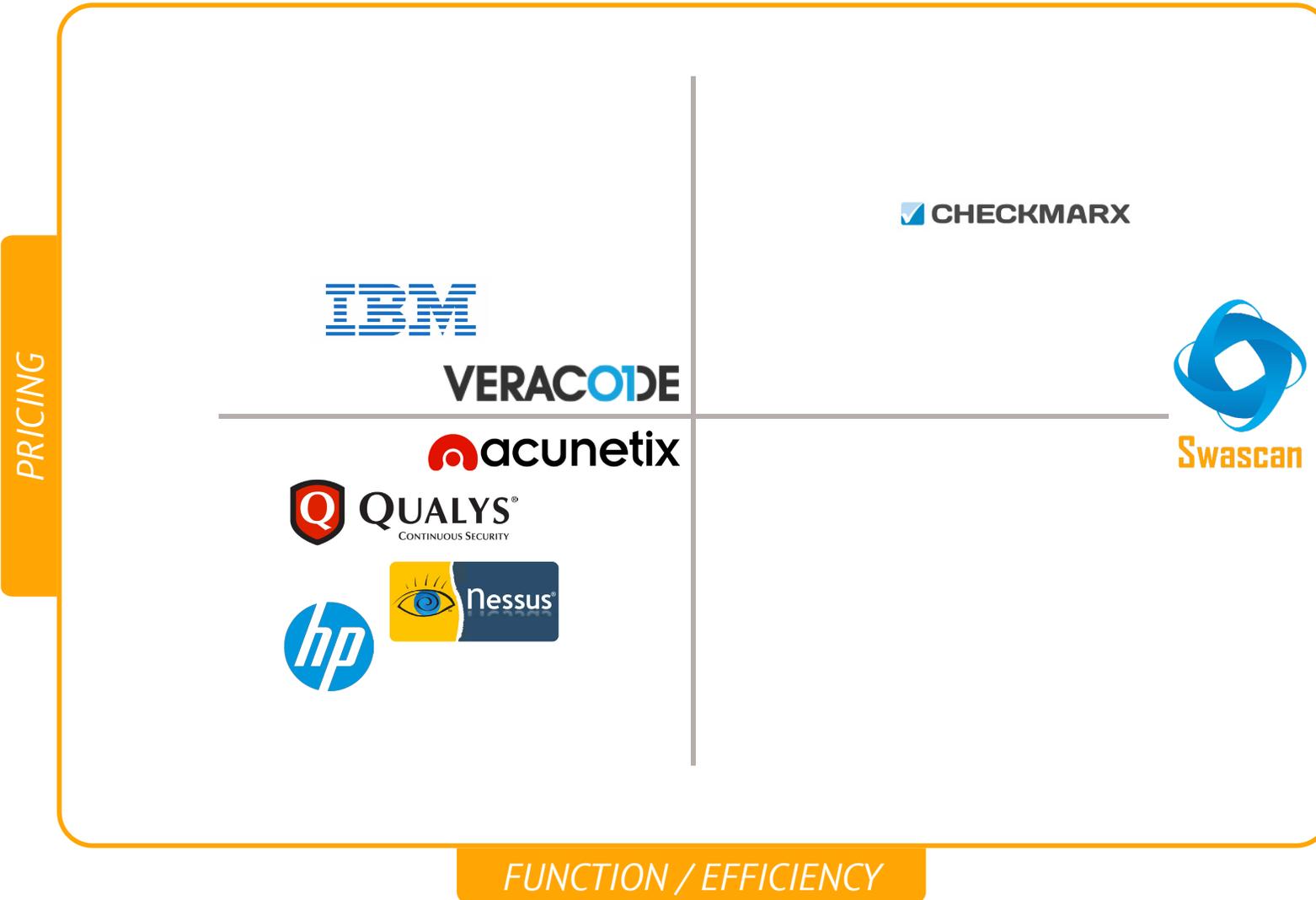


A reporting tool that makes easier the risk management activity (e.g. audit)



A recovery tool that suggests how to re-arrange the different security levels

PRODUCT Positioning



BATTLE Card

	CLOUD TECHNOLOGY	WEB SCAN	VPN SCAN	NETWORK SCAN	CODE REVIEW	ANNUAL LICENSE (NOT PERPETUAL)
	OK	OK	OK	OK	OK	OK
	OK	NO	NO	NO	OK	NO
	OK	OK	NO	OK	NO	NO
	NO	OK	NO	OK	NO	NO
	NO	OK	OK	OK	NO	OK
	NO	NO	OK	OK	NO	OK
	NO	OK	OK	OK	NO	OK

SWASCAN Screenshot





Issues
14790



Files with issues
1602

Low Severity
7194

Medium Severity
6795

High Severity
801

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	

Web Scan

Scan Strength *i*

Scanner Alert Threshold *i*

- Information gathering +
- Server security +
- Miscellaneous +
- Injection +
- Authorization -

Details

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

Name

X-Frame-Options Header Not Set

Severity

Medium

Impacts

Integrity, Confidentiality

Likelihood of Exploits

High

Top Owasp

None

Method

GET

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

Potential Mitigations

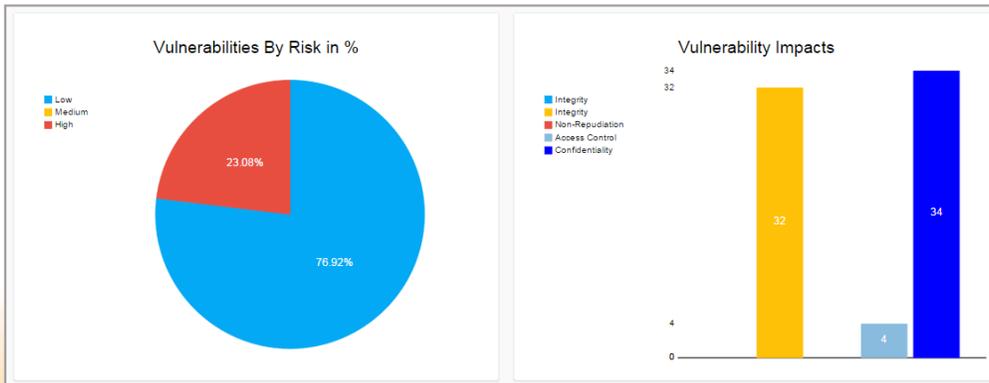
Implementation
 This Vulnerability identifies the pages for X-Frame-Options header and so for possible ClickJacking attack against URL.
 There are two main ways to prevent clickjacking:

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

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