WAS Scan Report

The resource of this report item is not reachable.

Scan Report

08 Apr 2019

Vulnerabilities of all selected scans are consolidated into one report so that you can view their evolution.

Enrico Speranza
gtsr5es

GT50 50 S.r.l.
Viale degli Ammiragli, 67 Scala A, 3° Piano, Interno 6
Roma, None 00136
Italy

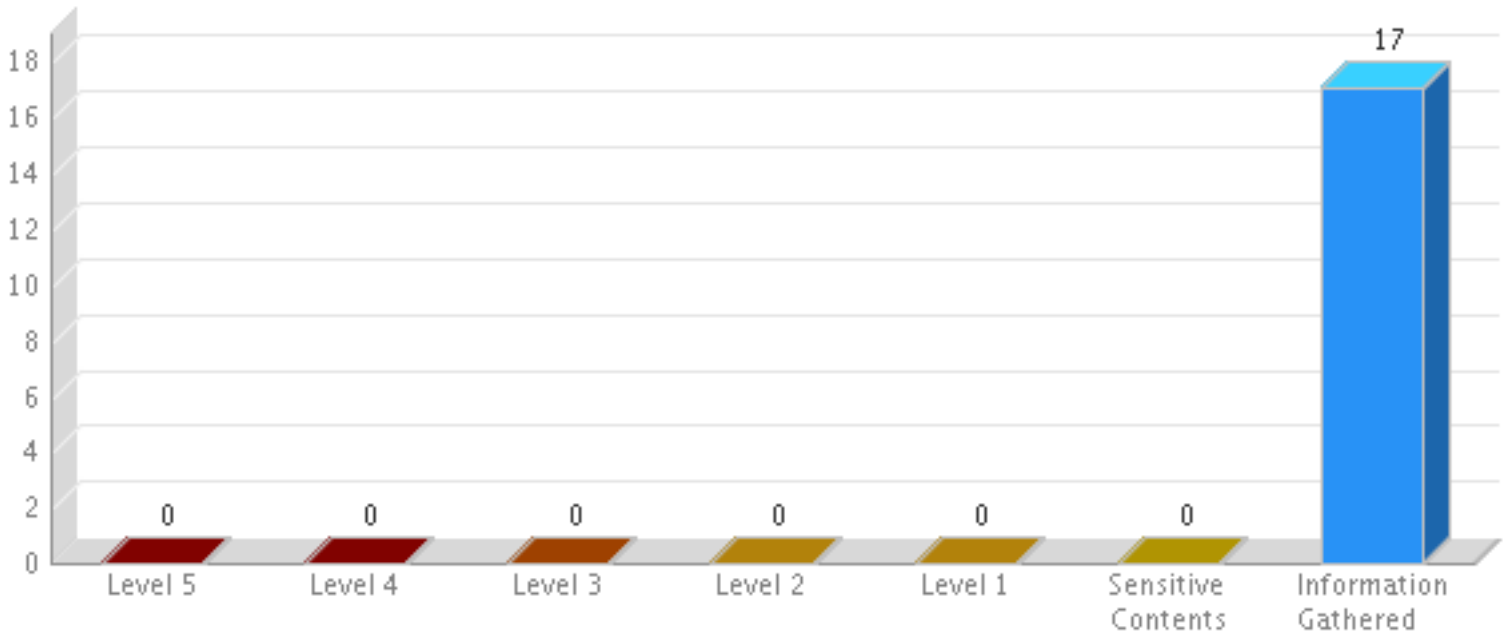
Target and Filters

Scans (1)	**Relaunch [Web Application Vulnerability Scan - 2019-04-03] 2019-04-03 5:15:03PM**
Web Applications (1)	**https://services-aruba.gt50.org/**

Summary

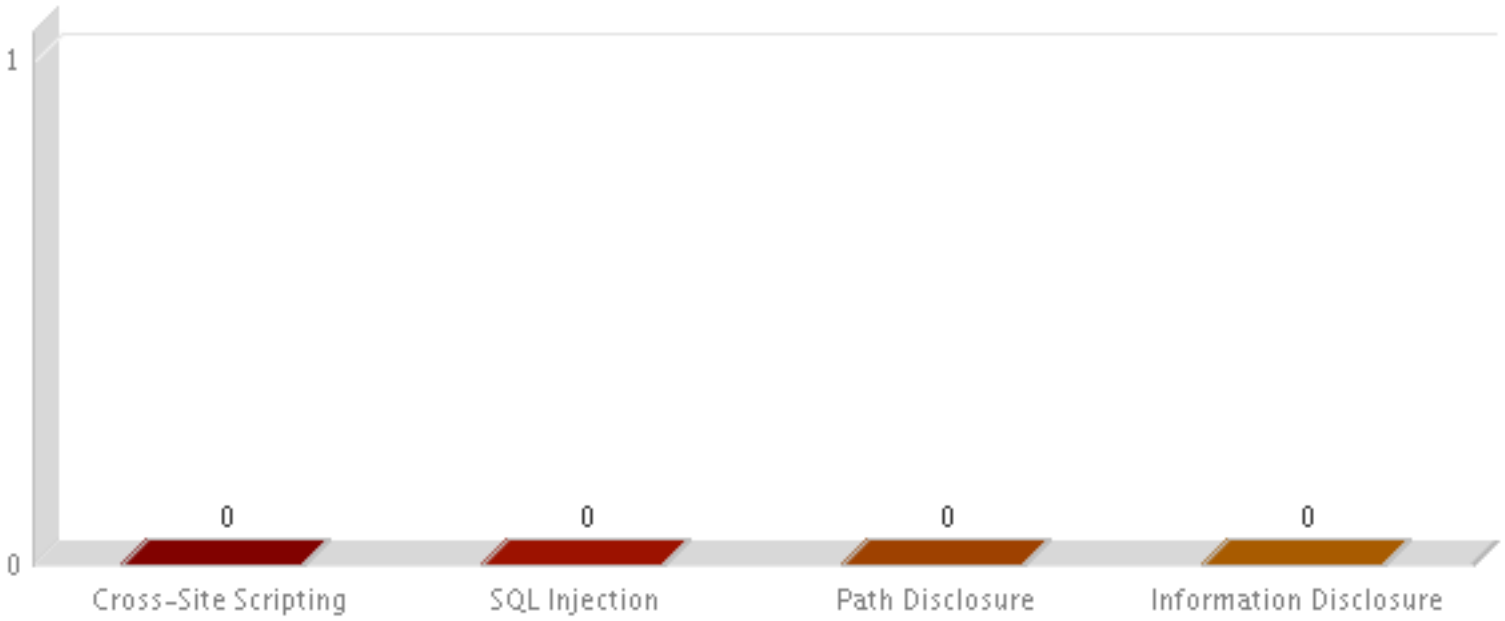
Security Risk	Vulnerabilities	Sensitive Contents	Information Gathered
-	0	0	17

Findings by Severity

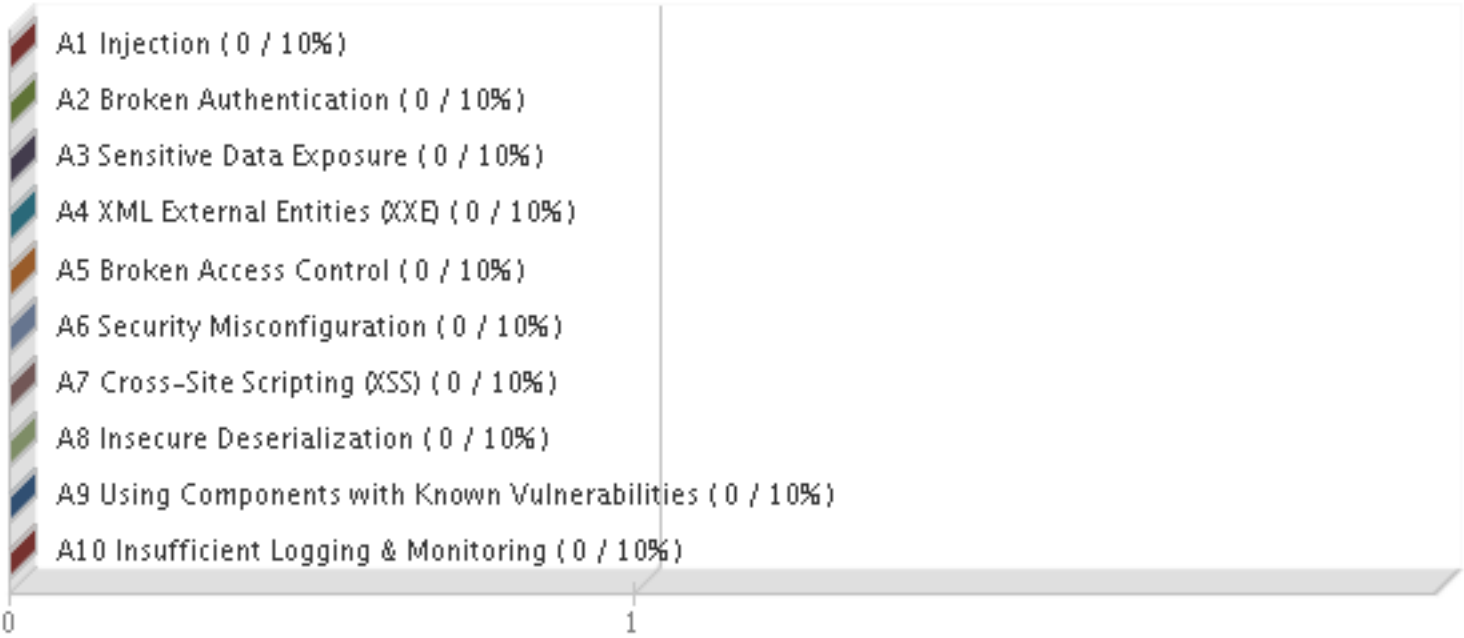


WAS Scan Report

Vulnerabilities by Group



OWASP Top 10 2017 Vulnerabilities



Scan	Date	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
Relaunch [Web Application Vulnerability Scan - 2019-04-03] 2019-04-03 5:15:03PM	03 Apr 2019 17:16 GMT +0100	0	0	0	0	0	0	17

WAS Scan Report

Results(17)

Information Gathered (17)

Information Gathered (17)

150086 Server accepts unnecessarily large POST request body (1)

150086 Server accepts unnecessarily large POST request body

Finding #	**2417380**(78586714)	**Severity**	Information Gathered - Level 3
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Web application scanner successfully sent a POST request with content type of application/x-www-form-urlencoded and 65536 bytes length random text data. Accepting request bodies with unnecessarily large size could help attacker to use less connections to achieve Layer 7 DDoS of web server. More information can be found at the here

Impact

Could result in successful application level (Layer 7) DDoS attack.

Solution

Limit the size of the request body to each form's requirements. For example, a search form with 256-char search field should not accept more than 1KB value. Server-specific details can be found here.

Results

Server responded 200 to unnecessarily large random request body(over 64 KB) for URL https://services-aruba.gt50.org/, significantly increasing attacker's chances to prolong slow HTTP POST attack.

45017 Operating System Detected (1)

WAS Scan Report

45017 Operating System Detected

Finding #	**2417390**(78586724)	**Severity**	Information Gathered - Level 2
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) **TCP/IP Fingerprint**: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

2) **NetBIOS**: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) **PHP Info**: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) **SNMP**: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

Impact

Not applicable.

Solution

Not applicable.

Results

Operating System	Technique	ID
Ubuntu / Fedora / Tiny Core Linux / Linux 3.x	TCP/IP Fingerprint	U5933:443

150202 Missing header: X-Content-Type-Options (1)

WAS Scan Report

150202 Missing header: X-Content-Type-Options

Finding #	**2417389**(78586723)	**Severity**	Information Gathered - Level 2
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	A6 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-Content-Type-Options response header is not present. WAS reports missing X-Content-Type-Options header on each crawled link with all types of static and dynamic response. The scanner performs the check on 4xx and 5xx responses too. It's possible to see a directory link reported for QID as well.

Impact

All web browsers employ a content-sniffing algorithm that inspects the contents of HTTP responses and also occasionally overrides the MIME type provided by the server. If X-Content-Type-Options header is not present, browsers can potentially be tricked into treating non-HTML response as HTML. An attacker can potentially leverage the functionality to perform a cross-site scripting (XSS) attack. This specific case is known as a Content-Sniffing XSS (CS-XSS) attack.

Solution

It is recommended to disable browser content sniffing by adding the X-Content-Type-Options header to the HTTP response with a value of 'nosniff'. Also ensure that the Content-Type header is set correctly on responses.

Results

X-Content-Type-Options: Header missing
Response headers on link: https://services-aruba.gt50.org/
Date: Wed, 03 Apr 2019 15:16:27 GMT
Server: Klingon_2052_Enterprise_Server
X-Frame-Options: SAMEORIGIN
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Set-Cookie: PHPSESSID=tsb6irsodgdto8f6q5bced4s76; secure; HttpOnly; domain=services-aruba.gt50.org; path=/

Header missing on the following link(s):
https://services-aruba.gt50.org/
https://services-aruba.gt50.org/?
https://services-aruba.gt50.org/favicon.ico
https://services-aruba.gt50.org/css/bootstrap.min.css
https://services-aruba.gt50.org/mycss/loginmodal.css
https://services-aruba.gt50.org/css/jumbotron.css
https://services-aruba.gt50.org/css/strongpass.css
https://services-aruba.gt50.org/index.php
https://services-aruba.gt50.org/demo/index.php
https://services-aruba.gt50.org/changeLanguage.php?lang=IT
https://services-aruba.gt50.org/changeLanguage.php?lang=EN
https://services-aruba.gt50.org/lambdaPage.php
https://services-aruba.gt50.org/js/StrongPass.js
https://services-aruba.gt50.org/demo/favicon.ico
https://services-aruba.gt50.org/demo/js/StrongPass.js
https://services-aruba.gt50.org/demo/index.php?oper=newuser

150206 Content-Security-Policy Not Implemented (1)

WAS Scan Report

150206 Content-Security-Policy Not Implemented

Finding #	**2417393**(78586727)	**Severity**	Information Gathered - Level 2
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	A6 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

No Content-Security-Policy (CSP) is specified for the page. WAS checks for the missing CSP on all static and dynamic pages. It checks for CSP in the response headers (Content-Security-Policy, X-Content-Security-Policy or X-Webkit-CSP) and in response body (http-equiv="Content-Security-Policy" meta tag).

HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security it's important to set appropriate CSP policies on 4xx and 5xx responses as well.

Impact

Content-Security Policy is a defense mechanism that can significantly reduce the risk and impact of XSS attacks in modern browsers. The CSP specification provides a set of content restrictions for web resources and a mechanism for transmitting the policy from a server to a client where the policy is enforced. When a Content Security Policy is specified, a number of default behaviors in user agents are changed; specifically inline content and JavaScript eval constructs are not interpreted without additional directives. In short, CSP allows you to create a whitelist of sources of the trusted content. The CSP policy instructs the browser to only render resources from those whitelisted sources. Even though an attacker can find a security vulnerability in the application through which to inject script, the script won't match the whitelisted sources defined in the CSP policy, and therefore will not be executed.

The absence of Content Security Policy in the response will allow the attacker to exploit vulnerabilities as the protection provided by the browser is not at all leveraged by the Web application. If secure CSP configuration is not implemented, browsers will not be able to block content-injection attacks such as Cross-Site Scripting and Clickjacking.

Solution

Appropriate CSP policies help prevent content-injection attacks such as cross-site scripting (XSS) and clickjacking. It's recommended to add secure CSP policies as a part of a defense-in-depth approach for securing web applications.

References:
- https://www.owasp.org/index.php/Content_Security_Policy_Cheat_Sheet
- https://developers.google.com/web/fundamentals/security/csp/

Results

Content-Security-Policy: Header missing
Response headers on link: https://services-aruba.gt50.org/
Date: Wed, 03 Apr 2019 15:16:27 GMT
Server: Klingon_2052_Enterprise_Server
X-Frame-Options: SAMEORIGIN
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Set-Cookie: PHPSESSID=tsb6irsodgdto8f6q5bced4s76; secure; HttpOnly; domain=services-aruba.gt50.org; path=/

Header missing on the following link(s):
https://services-aruba.gt50.org/
https://services-aruba.gt50.org/?
https://services-aruba.gt50.org/favicon.ico
https://services-aruba.gt50.org/css/bootstrap.min.css
https://services-aruba.gt50.org/mycss/loginmodal.css
https://services-aruba.gt50.org/css/jumbotron.css
https://services-aruba.gt50.org/css/strongpass.css
https://services-aruba.gt50.org/index.php
https://services-aruba.gt50.org/demo/index.php
https://services-aruba.gt50.org/changeLanguage.php?lang=IT
https://services-aruba.gt50.org/changeLanguage.php?lang=EN
https://services-aruba.gt50.org/lambdaPage.php
https://services-aruba.gt50.org/js/StrongPass.js
https://services-aruba.gt50.org/demo/favicon.ico

https://services-aruba.gt50.org/demo/js/StrongPass.js
https://services-aruba.gt50.org/demo/index.php?oper=newuser

6 DNS Host Name (1)

6 DNS Host Name

Finding #	**2417381**(78586715)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

Impact
N/A

Solution
N/A

Results

IP address	Host name
5.249.140.169	host169-140-249-5.serverdedicati.aruba.it

45038 Host Scan Time (1)

WAS Scan Report

45038 Host Scan Time

Finding #	**2417385**(78586719)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

Impact

N/A

Solution

N/A

Results

Scan duration: 1108 seconds

Start time: Wed, Apr 03 2019, 15:16:19 GMT

End time: Wed, Apr 03 2019, 15:34:47 GMT

150009 Links Crawled (1)

WAS Scan Report

150009 Links Crawled

Finding #	**2417392**(78586726)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The list of unique links crawled and HTML forms submitted by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch.

NOTE: This list also includes - All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled) - All the forms reported in QID 150152 (Forms Crawled), - All the forms in QID 150115 (Authentication Form Found) and - Certain requests from QID 150172 (Requests Crawled)

Impact

N/A

Solution

N/A

Results

Duration of crawl phase (seconds): 119.00
Number of links: 11
(This number excludes form requests and links re-requested during authentication.)

https://services-aruba.gt50.org/
https://services-aruba.gt50.org/?
https://services-aruba.gt50.org/changeLanguage.php?lang=EN
https://services-aruba.gt50.org/changeLanguage.php?lang=IT
https://services-aruba.gt50.org/demo/favicon.ico
https://services-aruba.gt50.org/demo/index.php
https://services-aruba.gt50.org/demo/index.php?oper=newuser
https://services-aruba.gt50.org/demo/js/StrongPass.js
https://services-aruba.gt50.org/favicon.ico
https://services-aruba.gt50.org/index.php
https://services-aruba.gt50.org/lambdaPage.php

150010 External Links Discovered (1)

WAS Scan Report

150010 External Links Discovered

Finding #	**2417388**(78586722)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

Impact

N/A

Solution

N/A

Results

Number of links: 24
https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js
https://cdnjs.cloudflare.com/ajax/libs/tether/1.4.0/js/tether.min.js
https://www.google.com/intl/en/policies/privacy/
https://www.google.com/intl/en/policies/terms/
https://www.google.com/recaptcha/api.js
https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcaazcUAAAAAA_MVG_DN1FWwOLPskOz0TR8GOJR&co=aHR0cHM6Ly9zZXJ2aWNlcy1hcnViYS5ndDUwLm9yZzo0NDM.&hl=en&v=v1552285980763&size=normal&cb=fef3fidpa

https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcaazcUAAAAAA_MVG_DN1FWwOLPskOz0TR8GOJR&co=aHR0cHM6Ly9zZXJ2aWNlcy1hcnViYS5ndDUwLm9yZzo0NDM.&hl=en&v=v1552285980763&size=normal&cb=vzurvafv

https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcaazcUAAAAAA_MVG_DN1FWwOLPskOz0TR8GOJR&co=aHR0cHM6Ly9zZXJ2aWNlcy1hcnViYS5ndDUwLm9yZzo0NDM.&hl=en&v=v1552285980763&size=normal&cb=xjjeta1zz

https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcaazcUAAAAAA_MVG_DN1FWwOLPskOz0TR8GOJR&co=aHR0cHM6Ly9zZXJ2aWNlcy1hcnViYS5ndDUwLm9yZzo0NDM.&hl=en&v=v1552285980763&size=normal&cb=xn64fbez

https://www.google.com/recaptcha/api2/bframe?hl=en&v=v1552285980763&k=6LcaazcUAAAAAA_MVG_DN1FWwOLPskOz0TR8GOJR&cb=90lgv138k76d
https://www.google.com/recaptcha/api2/bframe?hl=en&v=v1552285980763&k=6LcaazcUAAAAAA_MVG_DN1FWwOLPskOz0TR8GOJR&cb=lbf7gixiasnf
https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc-AMP6lQ.woff
https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmYUtfBBc-AMP6lQ.woff
https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxMKTU1Kg.woff
https://code.jquery.com/jquery-3.3.1.slim.min.js
https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js
https://www.gstatic.com/recaptcha/api2/logo_48.png
https://www.gstatic.com/recaptcha/api2/v1552285980763/recaptcha__en.js
https://www.gt50.org/products/digital_seal_sqcode.php
http://www.timbrodigitale.com/
http://www.gt50.org/
http://www.gt50.org/support.php
http://www.q-id.net/
http://www.q-id.net/download_page.html

150021 Scan Diagnostics (1)

WAS Scan Report

150021 Scan Diagnostics

Finding #	**2417382**(78586716)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

Impact

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

Solution

No action is required.

Results

Loaded 0 blacklist entries.
Loaded 0 whitelist entries.
HTML form authentication unavailable, no WEBAPP entry found
Batch #0 VirtualHostDiscovery: estimated time < 1 minute (70 tests, 0 inputs)
VirtualHostDiscovery: 70 vulnsigs tests, completed 70 requests, 12 seconds. Completed 70 requests of 70 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found. Aborting the CMS Detection phaseCMSDetection: 1 vulnsigs tests, completed 38 requests, 1 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
Collected 16 links overall in 0 hours 1 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 9) + files:(0 x 9) + directories:(9 x 6) + paths:(0 x 15) = total (54)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 15 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 45 requests, 1 seconds. Completed 45 requests of 54 estimated requests (83.3333%). All tests completed.
Batch #0 WS enumeration: estimated time < 1 minute (11 tests, 13 inputs)
WS enumeration: 11 vulnsigs tests, completed 40 requests, 0 seconds. Completed 40 requests of 143 estimated requests (27.972%). All tests completed.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (58 tests, 1 inputs)
Batch #1 URI parameter manipulation (no auth): 58 vulnsigs tests, completed 70 requests, 1 seconds. Completed 70 requests of 58 estimated requests (120.69%). All tests completed.
Batch #1 Form parameter manipulation (no auth): estimated time < 1 minute (58 tests, 5 inputs)
Batch #1 Form parameter manipulation (no auth): 58 vulnsigs tests, completed 285 requests, 5 seconds. Completed 285 requests of 290 estimated requests (98.2759%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 1 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 16 requests, 0 seconds. Completed 16 requests of 24 estimated requests (66.6667%). All tests completed.
Batch #1 Form blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 5 inputs)
Batch #1 Form blind SQL manipulation (no auth): 8 vulnsigs tests, completed 80 requests, 2 seconds. Completed 80 requests of 120 estimated requests (66.6667%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (12 tests, 1 inputs)
Batch #1 URI parameter time-based tests (no auth): 12 vulnsigs tests, completed 12 requests, 0 seconds. Completed 12 requests of 12 estimated requests (100%). All tests completed.
Batch #1 Form field time-based tests (no auth): estimated time < 1 minute (12 tests, 5 inputs)
Batch #1 Form field time-based tests (no auth): 12 vulnsigs tests, completed 60 requests, 1 seconds. Completed 60 requests of 60 estimated requests (100%). All tests completed.
Batch #1 URI parameter time-based tests for CVE-2011-3923 (no auth): estimated time < 1 minute (1 tests, 1 inputs)
Batch #1 URI parameter time-based tests for CVE-2011-3923 (no auth): 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Batch #1 Form field time-based tests for CVE-2011-3923 (no auth): estimated time < 1 minute (1 tests, 5 inputs)
Batch #1 Form field time-based tests for CVE-2011-3923 (no auth): 1 vulnsigs tests, completed 5 requests, 0 seconds. Completed 5 requests of 5 estimated requests (100%). All tests completed.
Batch #2 URI parameter manipulation (no auth): estimated time < 1 minute (58 tests, 2 inputs)
Batch #2 URI parameter manipulation (no auth): 58 vulnsigs tests, completed 70 requests, 1 seconds. Completed 70 requests of 116 estimated requests (60.3448%). All tests completed.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 2 inputs)
Batch #2 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 16 requests, 0 seconds. Completed 16 requests of 48 estimated requests (33.3333%). All tests completed.
Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (12 tests, 2 inputs)
Batch #2 URI parameter time-based tests (no auth): 12 vulnsigs tests, completed 12 requests, 1 seconds. Completed 12 requests of 24 estimated requests (50%). All tests completed.
Batch #2 URI parameter time-based tests for CVE-2011-3923 (no auth): estimated time < 1 minute (1 tests, 2 inputs)
Batch #2 URI parameter time-based tests for CVE-2011-3923 (no auth): 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 2 estimated requests (50%). All tests completed.
Batch #3 URI parameter manipulation (no auth): estimated time < 1 minute (58 tests, 1 inputs)
Batch #3 URI parameter manipulation (no auth): 58 vulnsigs tests, completed 57 requests, 1 seconds. Completed 57 requests of 58 estimated requests (98.2759%). All tests completed.
Batch #3 Form parameter manipulation (no auth): estimated time < 1 minute (58 tests, 11 inputs)
Batch #3 Form parameter manipulation (no auth): 58 vulnsigs tests, completed 627 requests, 22 seconds. Completed 627 requests of 638 estimated requests (98.2759%). All tests completed.
Batch #3 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 1 inputs)
Batch #3 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 16 requests, 0 seconds. Completed 16 requests of 24 estimated requests (66.6667%). All tests completed.
Batch #3 Form blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 11 inputs)
Batch #3 Form blind SQL manipulation (no auth): 8 vulnsigs tests, completed 176 requests, 3 seconds. Completed 176 requests of 264 estimated requests (66.6667%). All tests completed.
Batch #3 URI parameter time-based tests (no auth): estimated time < 1 minute (12 tests, 1 inputs)
Batch #3 URI parameter time-based tests (no auth): 12 vulnsigs tests, completed 12 requests, 0 seconds. Completed 12 requests of 12 estimated requests (100%). All tests completed.
Batch #3 Form field time-based tests (no auth): estimated time < 1 minute (12 tests, 11 inputs)
Batch #3 Form field time-based tests (no auth): 12 vulnsigs tests, completed 132 requests, 3 seconds. Completed 132 requests of 132 estimated requests (100%). All tests completed.

Batch #3 URI parameter time-based tests for CVE-2011-3923 (no auth): estimated time < 1 minute (1 tests, 1 inputs)
Batch #3 URI parameter time-based tests for CVE-2011-3923 (no auth): 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Batch #3 Form field time-based tests for CVE-2011-3923 (no auth): estimated time < 1 minute (1 tests, 11 inputs)
Batch #3 Form field time-based tests for CVE-2011-3923 (no auth): 1 vulnsigs tests, completed 11 requests, 1 seconds. Completed 11 requests of 11 estimated requests (100%). All tests completed.
No XML requests found. Skipping XXE tests.
Batch #4 DOM XSS exploitation: estimated time < 1 minute (4 tests, 0 inputs)
Batch #4 DOM XSS exploitation: 4 vulnsigs tests, completed 0 requests, 1 seconds. No tests to execute.
Batch #4 HTTP call manipulation: estimated time < 1 minute (33 tests, 0 inputs)
Batch #4 HTTP call manipulation: 33 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Open Redirect analysis: estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 Open Redirect analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
CSRF tests will not be launched because the scan is not successfully authenticated.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 15 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 15 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (37 tests, 1 inputs)
Batch #4 Cookie manipulation: 37 vulnsigs tests, completed 148 requests, 3 seconds. Completed 148 requests of 130 estimated requests (113.846%). XSS optimization removed 240 links. All tests completed.
Batch #4 Header manipulation: estimated time < 1 minute (37 tests, 10 inputs)
Batch #4 Header manipulation: 37 vulnsigs tests, completed 220 requests, 3 seconds. Completed 220 requests of 500 estimated requests (44%). XSS optimization removed 240 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 10 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 10 requests, 1 seconds. Completed 10 requests of 10 estimated requests (100%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 3 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 3 requests, 0 seconds. Completed 3 requests of 3 estimated requests (100%). All tests completed.
Batch #4 httpoxy detector: estimated time < 1 minute (1 tests, 10 inputs)
Batch #4 httpoxy detector: 1 vulnsigs tests, completed 10 requests, 0 seconds. Completed 10 requests of 10 estimated requests (100%). All tests completed.
Batch #4 httpoxy detector(form): estimated time < 1 minute (1 tests, 3 inputs)
Batch #4 httpoxy detector(form): 1 vulnsigs tests, completed 3 requests, 0 seconds. Completed 3 requests of 3 estimated requests (100%). All tests completed.
Batch #4 Struts timebased detector: estimated time < 1 minute (1 tests, 10 inputs)
Batch #4 Struts timebased detector: 1 vulnsigs tests, completed 10 requests, 1 seconds. Completed 10 requests of 10 estimated requests (100%). All tests completed.
Batch #4 Login Brute Force manipulation: estimated time < 1 minute (176 tests, 1 inputs)
Batch #4 Login Brute Force manipulation: 176 vulnsigs tests, completed 176 requests, 248 seconds. Completed 176 requests of 176 estimated requests (100%). All tests completed.
Batch #4 insecurely served cred forms detector (no auth): estimated time < 1 minute (1 tests, 6 inputs)
Batch #4 insecurely served cred forms detector (no auth): 1 vulnsigs tests, completed 6 requests, 1 seconds. Completed 6 requests of 6 estimated requests (100%). All tests completed.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 9) + files:(0 x 9) + directories:(4 x 6) + paths:(11 x 15) = total (189)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 15 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 151 requests, 2 seconds. Completed 151 requests of 189 estimated requests (79.8942%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 9) + files:(0 x 9) + directories:(1 x 6) + paths:(0 x 15) = total (6)
Batch #5 Tomcat Vuln manipulation: estimated time < 1 minute (1 tests, 15 inputs)
Batch #5 Tomcat Vuln manipulation: 1 vulnsigs tests, completed 5 requests, 0 seconds. Completed 5 requests of 6 estimated requests (83.3333%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 9) + files:(0 x 9) + directories:(16 x 6) + paths:(0 x 15) = total (96)
Batch #5 Time based path manipulation: estimated time < 1 minute (16 tests, 17 inputs)
Batch #5 Time based path manipulation: 16 vulnsigs tests, completed 64 requests, 660 seconds. Completed 64 requests of 96 estimated requests (66.6667%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(4 x 9) + files:(18 x 9) + directories:(102 x 6) + paths:(14 x 15) = total (1020)
Batch #5 Path manipulation: estimated time < 1 minute (138 tests, 15 inputs)
Batch #5 Path manipulation: 138 vulnsigs tests, completed 748 requests, 7 seconds. Completed 748 requests of 1020 estimated requests (73.3333%). All tests completed.
Generic WebCgi Test no test enabled
Total requests made: 3439
Average server response time: 0.10 seconds

150028 Cookies Collected (1)

WAS Scan Report

150028 Cookies Collected

Finding #	**2417384**(78586718)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
The cookies listed in the Results section were received from the web application during the crawl phase.

Impact
Cookies may contain sensitive information about the user. Cookies sent via HTTP may be sniffed.

Solution
Review cookie values to ensure that sensitive information such as passwords are not present within them.

Results

Total cookies: 1
PHPSESSID=tsb6irsodgdto8f6q5bced4s76; secure; HttpOnly; path=/ First set at URL: https://services-aruba.gt50.org/

150082 Protection against Clickjacking vulnerability (1)

150082 Protection against Clickjacking vulnerability

Finding #	**2432398**(78586712)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
The URIs listed have a protection against Clickjacking. The protection is implemented by use of X-Frame-Options header.

Impact
X-Frame-Options header is used to prevent framing of the page.

Solution
Another technique of prevention against Clickjacking is the "framekiller" JavaScript.

Results

https://services-aruba.gt50.org/
https://services-aruba.gt50.org/?
https://services-aruba.gt50.org/demo/index.php
https://services-aruba.gt50.org/demo/index.php?oper=newuser
https://services-aruba.gt50.org/index.php
https://services-aruba.gt50.org/lambdaPage.php

150099 Cookies Issued Without User Consent (1)

WAS Scan Report

150099 Cookies Issued Without User Consent

Finding #	**2417386**(78586720)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
The cookies listed in the Results section were issued from the web application during the crawl without accepting any opt-in dialogs.

Impact
Cookies may be set without user explicitly agreeing to accept them.

Solution
Review the application to ensure that all cookies listed are supposed to be issued without user opt-in. If the EU Cookie law is applicable for this web application, ensure these cookies require user opt-in or have been classified as exempt by your organization.

Results

Total cookies: 1
PHPSESSID=ajbjqgqf2r3rmmfmgk31fjacu3; secure; HttpOnly; path=/ First set at URL: https://services-aruba.gt50.org/

150104 Form Contains Email Address Field (1)

150104 Form Contains Email Address Field

Finding #	**2417391**(78586725)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
The HTML form contains a field that collects an email address.

Impact
In some web apps, forms that collect email addresses also generate messages to back-end systems whenever the form is submitted. If no rate limiting or CAPTCHA is applied to form submissions, then vulnerability tests against this form may produce a significant amount of messages. If too many messages are generated, then it may produce a Denial of Service situation.

Solution
Review the form to determine if it produces an email message each time it is submitted. If so, consider blacklisting this form from being tested or disable the messaging during the web application scan. Forms that generate messages can be abused by malicious users to create Denial of Service attacks. Apply rate limiting to the form in order to throttle the number of times it may be submitted by a user or by an IP address; or apply a CAPTCHA to it to reduce the chance of automated tools being used against the form.

Results

https://services-aruba.gt50.org/demo/index.php
https://services-aruba.gt50.org/demo/index.php?oper=newuser

WAS Scan Report

150115 Authentication Form found (1)

150115 Authentication Form found

Finding #	**2417379**(78586713)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Authentication Form was found during the web application crawling.

Impact

N/A

Solution

N/A

Results

Authentication form found at: https://services-aruba.gt50.org/
Action uri: https://services-aruba.gt50.org/index.php
Fields: user_name, login, user_password

150135 HTTP Strict Transport Security (HSTS) header missing/misconfigured. (1)

WAS Scan Report

150135 HTTP Strict Transport Security (HSTS) header missing/ misconfigured.

Finding #	**2417387**(78586721)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

HTTP Strict Transport Security (HSTS) header found to be missing or misconfigured. HSTS header dictates to a conforming browser that the current and all subsequent connections (for a configurable amount of time) to the subject website should only be performed over a secure transport layer. Additionally, users are not permitted to bypass SSL/TLS certificate errors; preventing browser click-throughs in the event of expired or otherwise untrusted certificates.

Impact

If HSTS header is not set by Web applications using TLS, users are potentially vulnerable to active Man-in-the-middle(MITM), SSL Striping and passive eavesdropper attacks.

Solution

1. The strongest protection is to ensure that all requested resources use only TLS with well-formed HSTS header. Add the Strict-Transport-Security HTTPS header to all responses from the target domains 2. Add 'includeSubDomains' directive to all Strict-Transport-Security headers. 3. Ensure that the max-age directive is included and set to an acceptable value equal to or greater than 10,368,000 seconds (120 days) with every Strict-Transport-Security header. If the max-age directive is not included, it must be added. If the value is set to less than 10,368,000 seconds, it must be increased to the minimum value.

Results

Strict Transport Security header missing for
https://services-aruba.gt50.org/

150152 Forms Crawled (1)

WAS Scan Report

150152 Forms Crawled

Finding #	**2417383**(78586717)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Results section consists of the unique forms submitted by the Web Application Scanner. Reported list of forms in this QID does not contain authentication forms (i.e. login forms) which are reported separately in QID 150115. There is redundancy checks done on forms based on form fields. Forms determined to be similar will be considered redundant and not tested.

NOTE: The regular expression specified under 'Redundant Links' are not applied to forms. Forms (unique or redundant) are not reported under QID 150140.

Impact

N/A

Solution

N/A

Results

Total internal forms seen (this count includes duplicate forms): 20

Crawled forms (Total: 5)
NOTE: This does not include authentication forms. Authentication forms are reported separately in QID 150115
Form #:1 Action URI:https://services-aruba.gt50.org/
Form #:2 Action URI:https://services-aruba.gt50.org/?
Form Fields:

Form #:3 Action URI:https://services-aruba.gt50.org/index.php
Form Fields: user_otp, login

Form #:4 Action URI:https://services-aruba.gt50.org/demo/index.php?oper=newuser
Form Fields: user_name, user_email, g-recaptcha-response, user_password_new, user_password_repeat, register

Form #:5 Action URI:https://services-aruba.gt50.org/demo/index.php?oper=newuser
Form Fields: user_name, user_email, user_password_new, user_password_repeat, register

NOTE: Forms with exactly the same form fields were considered identical even if they had different action URI. Only one such form is crawled, the other forms with exactly the same form fields are considered duplicate and are not crawled. If they are different forms and each of them should be crawled then change the scan settings accordingly.

The following forms were not crawled as their fields matched Form #1 above:
Form action: https://services-aruba.gt50.org/index.php
Form action: https://services-aruba.gt50.org/?
Form action: https://services-aruba.gt50.org/lambdaPage.php
Form action: https://services-aruba.gt50.org/demo/index.php
Form action: https://services-aruba.gt50.org/demo/index.php?oper=newuser

The following forms were not crawled as their fields matched Form #2 above:
Form action: https://services-aruba.gt50.org/demo/index.php
Form action: https://services-aruba.gt50.org/RecoverPassword.php
Form action: https://services-aruba.gt50.org/SyncOTP.php
Form action: https://services-aruba.gt50.org/
Form action: https://services-aruba.gt50.org/index.php
Form action: https://services-aruba.gt50.org/lambdaPage.php
Form action: https://services-aruba.gt50.org/demo/index.php?oper=newuser
Form action: https://services-aruba.gt50.org/demo/demo/index.php
Form action: https://services-aruba.gt50.org/demo/RecoverPassword.php
Form action: https://services-aruba.gt50.org/demo/SyncOTP.php

150204 Missing header: X-XSS-Protection (1)

WAS Scan Report

150204 Missing header: X-XSS-Protection

Finding #	**2417394**(78586728)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	03 Apr 2019 17:16 GMT+0100
CWE	-		
OWASP	A6 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-XSS-Protection response header is not present.

Impact

The X-XSS-Protection response header provides a layer of protection against reflected cross-site scripting (XSS) attacks by instructing browsers to abort rendering a page in which a reflected XSS attack has been detected. This is a best-effort second line of defense measure which helps prevent an attacker from using evasion techniques to avoid the neutralization mechanisms that the filters use by default. When configured appropriately, browser-level XSS filters can provide additional layers of defense against web application attacks.

Note that HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security the X-XSS-Protection header should be set on 4xx and 5xx responses as well.

Solution

It is recommend to set X-XSS-Protection header with value set to '1; mode=block' on all the relevant responses to activate browser's XSS filter.

NOTE: The X-XSS-Protection header is not supported by all browsers. Google Chrome and Safari are some of the browsers which support it, Firefox on the other hand does not support the header. X-XSS-Protection header does not guarantee a complete protection against XSS. For better protection against XSS attacks, the web application should use secure coding principles. Also, consider leveraging the Content-Security-Policy (CSP) header, which is supported by all browsers.

Using X-XSS-Protection could have unintended side effects, please understand the implications carefully before using it.

References:
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection
- https://blog.innerht.ml/the-misunderstood-x-xss-protection/
- https://www.mbsd.jp/blog/20160407.html
- https://www.chromium.org/developers/design-documents/xss-auditor

Results

X-Xss-Protection: Header missing
Response headers on link: https://services-aruba.gt50.org/
Date: Wed, 03 Apr 2019 15:16:27 GMT
Server: Klingon_2052_Enterprise_Server
X-Frame-Options: SAMEORIGIN
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Set-Cookie: PHPSESSID=tsb6irsodgdto8f6q5bced4s76; secure; HttpOnly; domain=services-aruba.gt50.org; path=/

Header missing on the following link(s):
https://services-aruba.gt50.org/
https://services-aruba.gt50.org/?
https://services-aruba.gt50.org/index.php
https://services-aruba.gt50.org/demo/index.php
https://services-aruba.gt50.org/changeLanguage.php?lang=IT
https://services-aruba.gt50.org/changeLanguage.php?lang=EN
https://services-aruba.gt50.org/lambdaPage.php
https://services-aruba.gt50.org/demo/favicon.ico

WAS Scan Report

https://services-aruba.gt50.org/demo/js/StrongPass.js
https://services-aruba.gt50.org/demo/index.php?oper=newuser

WAS Scan Report

Appendix

Scan Details

Relaunch [Web Application Vulnerability Scan - 2019-04-03] 2019-04-03 5:15:03PM

Reference	was/1554304514728.803448
Date	03 Apr 2019 17:16 GMT+0100
Mode	On-Demand
Type	Vulnerability
Authentication	None
Scanner Appliance	External (IP: 64.39.106.40, Scanner: 11.1.24-1, WAS: 6.5.47-1, Signatures: 2.4.573-2)
Profile	Initial WAS Options
DNS Override	-
Duration	00:18:28
Status	Finished
Authentication Status	None

Option Profile Details

Form Submission	BOTH
Form Crawl Scope	Do not include form action URI in uniqueness calculation
Maximum links to test in scope	300
User Agent	-
Request Parameter Set	Initial Parameters
Document Type	Ignore common binary files
SmartScan Support	Disabled
Timeout Error Threshold	100
Unexpected Error Threshold	300
Performance Settings	Pre-defined
Scan Intensity	Low
Bruteforce Option	Minimal
Detection Scope	Core
Credit Card Numbers Search	Off
Social Security Numbers (US) Search	Off

Web Application Details: https://services-aruba.gt50.org/

Name	https://services-aruba.gt50.org/
URL	https://services-aruba.gt50.org/
Owner	Enrico Speranza (gtsr5es)
Scope	Limit to URL hostname
Operating System	Ubuntu / Fedora / Tiny Core Linux / Linux 3.x

Severity Levels

Confirmed Vulnerabilities

Vulnerabilities (QIDs) are design flaws, programming errors, or mis-configurations that make your web application and web application platform susceptible to malicious attacks. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the

disclosure of information to a complete compromise of the web application and/or the web application platform. Even if the web application isn't fully compromised, an exploited vulnerability could still lead to the web application being used to launch attacks against users of the site.

Minimal	**Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.**
Medium	**Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.**
Serious	**Vulnerabilities at this level typically disclose security-related information that could result in misuse or an exploit. Examples include source code disclosure or transmitting authentication credentials over non-encrypted channels.**
Critical	**Intruders can exploit the vulnerability to gain highly sensitive content or affect other users of the web application. Examples include certain types of cross-site scripting and SQL injection attacks.**
Urgent	**Intruders can exploit the vulnerability to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture.**

Potential Vulnerabilities

Potential Vulnerabilities indicate that the scanner observed a weakness or error that is commonly used to attack a web application, and the scanner was unable to confirm if the weakness or error could be exploited. Where possible, the QID's description and results section include information and hints for following-up with manual analysis. For example, the exploitability of a QID may be influenced by characteristics that the scanner cannot confirm, such as the web application's network architecture, or the test to confirm exploitability requires more intrusive testing than the scanner is designed to conduct.

Minimal	**Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example in this scenario, information such as web server type, programming language, passwords or file path references can be disclosed.**
Medium	**Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example version of software or session data can be disclosed, which could be used to exploit.**
Serious	**Presence of this vulnerability might give access to security-related information to intruders who are bound to misuse or exploit. Examples of what could happen if this vulnerability was exploited include bringing down the server or causing hindrance to the regular service.**
Critical	**Presence of this vulnerability might give intruders the ability to gain highly sensitive content or affect other users of the web application.**
Urgent	**Presence of this vulnerability might enable intruders to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture. For example in this scenario, the web application users can potentially be targeted if the application is exploited.**

Sensitive Content

Sensitive content may be detected based on known patterns (credit card numbers, social security numbers) or custom patterns (strings, regular expressions), depending on the option profile used. Intruders may gain access to sensitive content that could result in misuse or other exploits.

Minimal	**Sensitive content was found in the web server response. During our scan of the site form(s) were found with field(s) for credit card number or social security number. This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.**
Medium	**Sensitive content was found in the web server response. Specifically our service found a certain sensitive content pattern (defined in the option profile). This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.**
Serious	**Sensitive content was found in the web server response - a valid social security number or credit card information. This infomation disclosure could result in a confidentiality breach, and it gives intruders access to valid sensitive content that could be misused.**

Information Gathered

WAS Scan Report

Information Gathered issues (QIDs) include visible information about the web application's platform, code, or architecture. It may also include information about users of the web application.

Minimal	**Intruders may be able to retrieve sensitive information related to the web application platform.**
Medium	**Intruders may be able to retrieve sensitive information related to internal functionality or business logic of the web application.**
Serious	**Intruders may be able to detect highly sensitive data, such as personally identifiable information (PII) about other users of the web application.**