WAS Web Application Report

Qualys. Express Lite

Web Application Report

10 Jul 2019

Each targeted web application is listed with the total number of detected vulnerabilities and sensitive content.

Brian Martin
fxzne-tf

Fixzone UK Ltd
420-424 Ewell Road
Surbiton, None KT6 7EH
United Kingdom

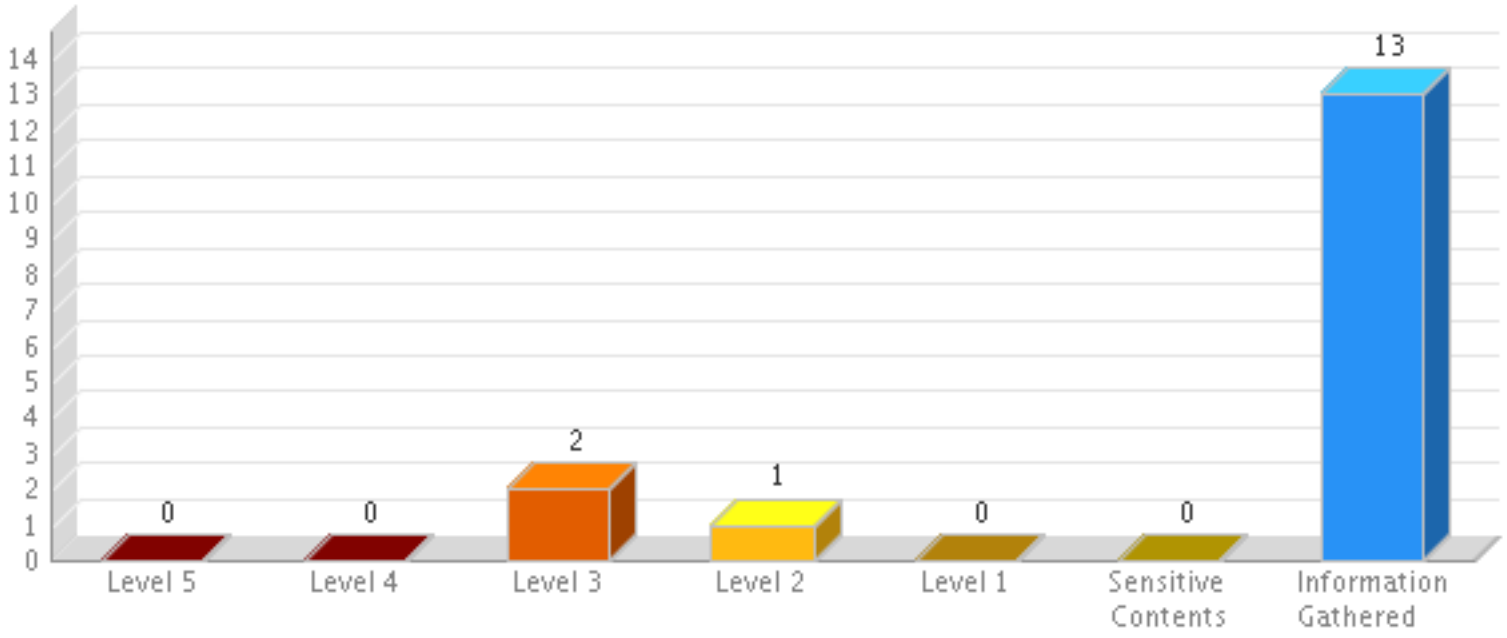
Target and Filters

Web Applications (1)	Very Product Protection
Status	New, Active, Re-Opened
Detection Source	Qualys, Burp, Bugcrowd

Summary

Security Risk	Web Applications	Vulnerabilities	Sensitive Contents	Information Gathered
MED	1	3	0	13

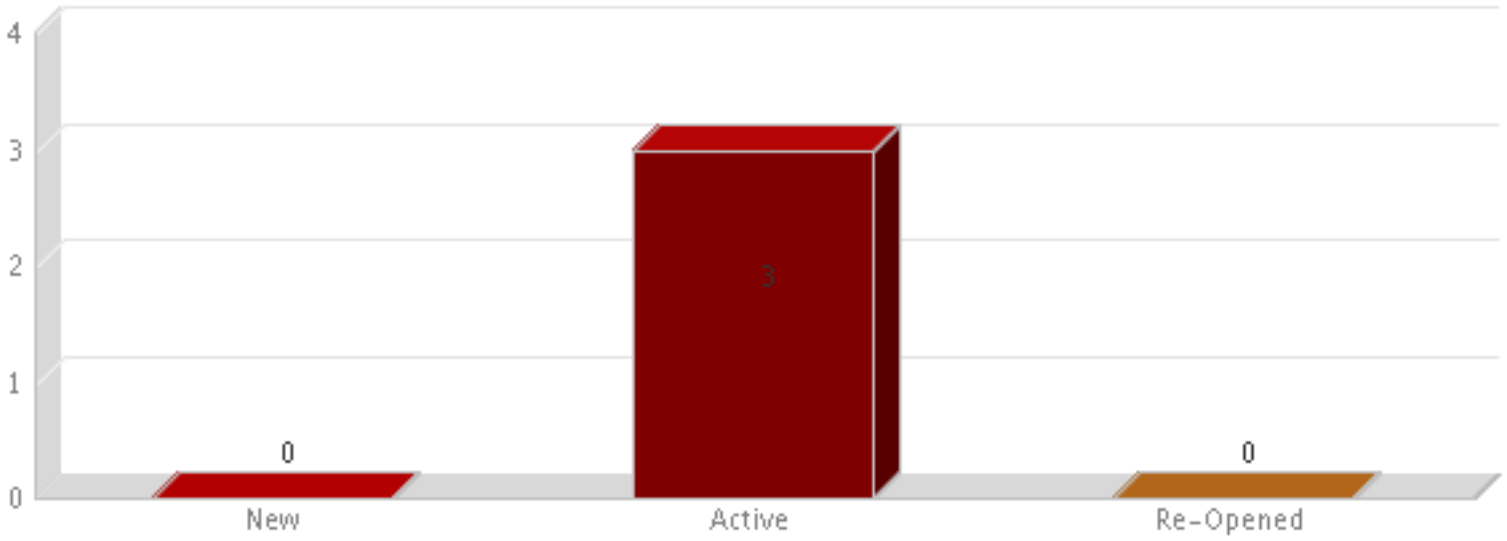
Findings by Severity



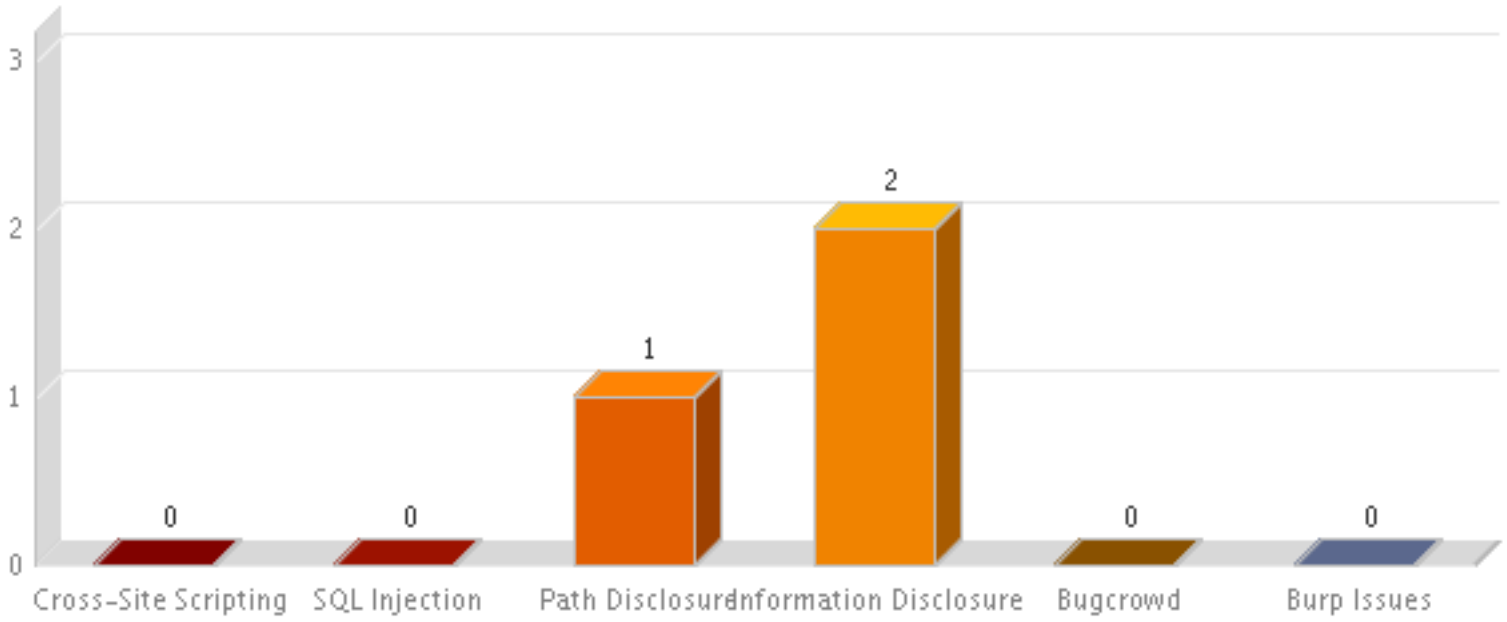
CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

WAS Web Application Report

Vulnerabilities by Status



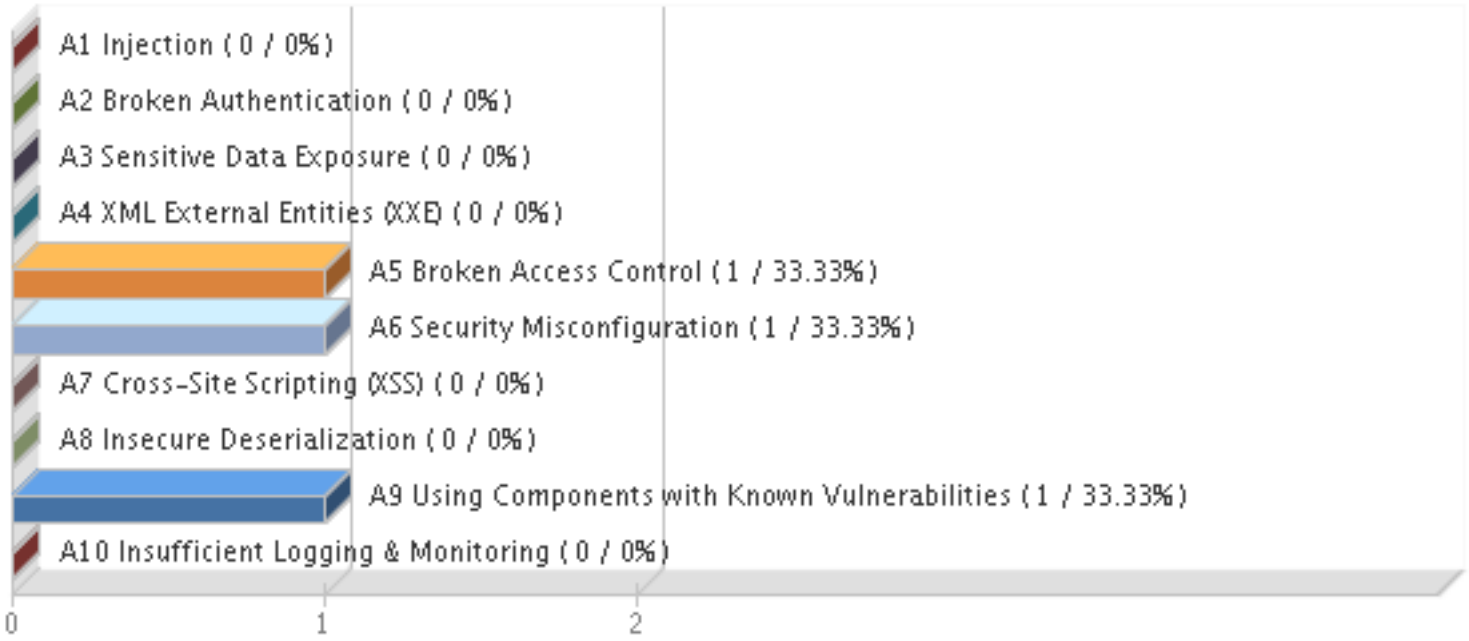
Vulnerabilities by Group



CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

WAS Web Application Report

OWASP Top 10 2017 Vulnerabilities



Web Application	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
Very Product Protection	0	0	2	1	0	0	13

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

WAS Web Application Report

Results(16)

Vulnerability (3)

Path Disclosure (1)

150004 Path-Based Vulnerability (1)

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

WAS Web Application Report

150004 Path-Based Vulnerability

Very Product Protection **Active**

URL: https://www.productprotection.very.co.uk/js/

Finding #	4574517	**Severity**	Confirmed Vulnerability - Level 2
Group	Path Disclosure	**First Time Detected**	26 Oct 2017 11:47 GMT
CWE	CWE-22	**Last Time Detected**	08 May 2019 09:31 GMT
OWASP	A5 Broken Access Control	**Last Time Tested**	08 May 2019 09:31 GMT
WASC	WASC-15 APPLICATION MISCONFIGURATION WASC-16 DIRECTORY INDEXING WASC-17 IMPROPER FILESYSTEM PERMISSIONS	**Times Detected**	10
CVSS Base	2.1	**CVSS Temporal**	1.9

Details

Threat
A potentially sensitive file, directory, or directory listing was discovered on the Web server.

Impact
The contents of this file or directory may disclose sensitive information.

Solution
Verify that access to this file or directory is permitted. If necessary, remove it or apply access controls to it.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

Payload	https://www.productprotection.very.co.uk/js/
Request	GET https://www.productprotection.very.co.uk/js/

#1 Referer: https://www.productprotection.very.co.uk/
#2 Cookie: __RequestVerificationToken=qG01TjbC2EFv4c5JxYCyZ02HtykRNuJbRAKK9oBwwzsuAHYPAwP8Rr5II8w6hOfcdUx9gp-X2stJeSk-3GJekLQtEZoX-bFPYaLH0BlQaeO4AdNnMC2AxEKB0TyV799wygaLzWKWgHByxPRJ1l-28Q2; ASP.NET_SessionId=3bvegkjjralp04a1ardolx4s;

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

comment: The server redirected and 3XX response has message body.

Original URL is: https://www.productprotection.very.co.uk/

HTTP/1.1 302 Redirect

Information Disclosure (2)

150085 Slow HTTP POST vulnerability (1)

150085 Slow HTTP POST vulnerability

Very Product Protection **Active**

URL: https://www.productprotection.very.co.uk/Account/IsUniqueMail?Email=%26urn=

Finding #	4574453	**Severity**	Potential Vulnerability - Level 3
Group	Information Disclosure	**First Time Detected**	26 Oct 2017 11:47 GMT
CWE	CWE-772	**Last Time Detected**	10 Jul 2019 09:32 GMT
OWASP		**Last Time Tested**	

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

WAS Web Application Report

	A6 Security Misconfiguration		10 Jul 2019 09:32 GMT
WASC	WASC-10 DENIAL OF SERVICE	Times Detected	65
CVSS Base	6.1	CVSS Temporal	5.5

Details

Threat

The web application is possibly vulnerable to a "slow HTTP POST" Denial of Service (DoS) attack. This is an application-level DoS that consumes server resources by maintaining open connections for an extended period of time by slowly sending traffic to the server. If the server maintains too many connections open at once, then it may not be able to respond to new, legitimate connections. Unlike bandwidth-consumption DoS attacks, the "slow" attack does not require a large amount of traffic to be sent to the server -- only that the client is able to maintain open connections for several minutes at a time.

The attack holds server connections open by sending properly crafted HTTP POST headers that contain a Content-Length header with a large value to inform the web server how much of data to expect. After the HTTP POST headers are fully sent, the HTTP POST message body is sent at slow speeds to prolong the completion of the connection and lock up server resources. By waiting for the complete request body, the server is helping clients with slow or intermittent connections to complete requests, but is also exposing itself to abuse.

Further information can be found under BlackHat_DC_2011_Brennan_Denial_Service-Slides.pdf.

Impact

All other services remain intact but the web server itself becomes inaccessible.

Solution

Solution would be server-specific, but general recommendations are: - to limit the size of the acceptable request to each form requirements - establish minimal acceptable speed rate - establish absolute request timeout for connection with POST request Server-specific details can be found here. A tool that demonstrates this vulnerability in a more intrusive manner is available here.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

Payload	N/A
Request	POST https://www.productprotection.very.co.uk/Account/IsUniqueMail?Email=&urn=

#1 Host: www.productprotection.very.co.uk
#2 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_3) AppleWebKit/601.4.4 (KHTML, like Gecko) Version/9.0.3 Safari/601.4.4
#3 Accept: */*
#4 Content-Type: application/x-www-form-urlencoded

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Vulnerable to slow HTTP POST attack
Connection with partial POST body remained open for: 129050 milliseconds

150162 Use of JavaScript Library with Known Vulnerability (1)

150162 Use of JavaScript Library with Known Vulnerability

Very Product Protection **Active**

URL: https://www.productprotection.very.co.uk/Account/SignIn

Finding #	4938163	Severity	Confirmed Vulnerability - Level 3

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

WAS Web Application Report

Group	Information Disclosure	**First Time Detected**	11 Jan 2018 12:54 GMT
CWE	CWE-937	**Last Time Detected**	10 Jul 2019 09:32 GMT
OWASP	A9 Using Components with Known Vulnerabilities	**Last Time Tested**	10 Jul 2019 09:32 GMT
WASC	-	**Times Detected**	65
CVSS Base	6.4	**CVSS Temporal**	4.9

Details

Threat

The web application is using a JavaScript library that is known to contain at least one vulnerability.

Impact

Attackers could potentially exploit the vulnerability in the JavaScript library. The impact of a successful exploit depends on the nature of the vulnerability and how the web application makes use of the library.

Solution

Please refer to the information provided in the response section. Also check the vendor's security advisories related to the vulnerable version of the library.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

#1 Request

Payload -

Request GET https://www.productprotection.very.co.uk/Account/SignIn

#1 Host: www.productprotection.very.co.uk
#2 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_3) AppleWebKit/601.4.4 (KHTML, like Gecko) Version/9.0.3 Safari/601.4.4
#3 Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Vulnerable javascript library: jQuery
version: 1.8.2
script uri: https://www.productprotection.very.co.uk/Scripts/jquery-1.8.2.js

Details:
In jQuery version before 1.9.0b1 selector interpreted as HTML. This could lead to potential vulnerabilities (https://bugs.jquery.com/ticket/11290).
Solution: jQuery version 1.9.0b1 has been released to address the issue. Please refer to vendor documentation (https://blog.jquery.com/) for the latest security updates.

CVE-2015-9251: jQuery versions on or above 1.4.0 and below 1.12.0 (version 1.12.3 and above but below 3.0.0-beta1 as well) are vulnerable to XSS via 3rd party text/javascript responses(3rd party CORS request may execute). (https://github.com/jquery/jquery/issues/2432).
Solution: jQuery version 1.12.0 has been released to address the issue (http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/). NOTE: Fix was reverted back in 1.12.2, so version 1.12.3 and above but below 3.0.0-beta1 are vulnerable as well. Please refer to vendor documentation (https://blog.jquery.com/) for the latest security updates.

In jQuery versions on or above 1.8.0 and below 1.12.0 $.parseHTML has (lots of) XSS. In these versions parseHTML() executes scripts in event handlers. Please refer following resource for more details: https://bugs.jquery.com/ticket/11974, http://research.insecurelabs.org/jquery/test/

CVE-2019-11358: jQuery versions below 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. An unsanitized source object containing an enumerable __proto__ property could extend the native Object.prototype. Please refer following resources for more details: https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/, https://nvd.nist.gov/vuln/detail/CVE-2019-11358, https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b, https://nvd.nist.gov/vuln/detail/CVE-2019-11358.

Found on the following pages (only first 10 pages are reported):
https://www.productprotection.very.co.uk/Account/SignIn
https://www.productprotection.very.co.uk/Account/IsUniqueMail?Email=&urn=
https://www.productprotection.very.co.uk/Error/Unhandled
https://www.productprotection.very.co.uk/Error/http404
https://www.productprotection.very.co.uk/Home/FAQ
https://www.productprotection.very.co.uk/Home/ContactUs
https://www.productprotection.very.co.uk/Account/InputUserId?returnurl=NewEnrole
https://www.productprotection.very.co.uk/Account/IsUniqueMail?Email=was%40qualys.com&urn=1
https://www.productprotection.very.co.uk/Account/InputUserId

Information Gathered (13)

Information Gathered (13)

45017 Operating System Detected (1)

45017 Operating System Detected *Very Product Protection*

Finding #	1475410	**Severity**	Information Gathered - Level 2
Group	Information Gathered		
CWE	-	**Detection Date**	10 Jul 2019 09:32 GMT
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.

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

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

Windows_Vista_/_Windows_2008_/_Windows_7_/_Windows_2012_/_Windows_8_/_Windows_10 TCP/IP_Fingerprint U3414:443

150009 Links Crawled (1)

150009 Links Crawled

Very Product Protection

Finding #	1475412	**Severity**	Information Gathered - Level 1
Group	Information Gathered		
CWE	-	**Detection Date**	10 Jul 2019 09:32 GMT
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

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

Results

Duration of crawl phase (seconds): 221.00
Number of links: 17
(This number excludes form requests and links re-requested during authentication.)

https://www.productprotection.very.co.uk/
https://www.productprotection.very.co.uk/Account/InputUserId
https://www.productprotection.very.co.uk/Account/InputUserId?returnurl=NewEnrole
https://www.productprotection.very.co.uk/Account/IsUniqueMail
https://www.productprotection.very.co.uk/Account/IsUniqueMail?Email=&urn=
https://www.productprotection.very.co.uk/Account/IsUniqueMail?Email=was%40qualys.com&urn=1
https://www.productprotection.very.co.uk/Account/SignIn
https://www.productprotection.very.co.uk/BookNewService/JobPage
https://www.productprotection.very.co.uk/Content/css/iconfont/fontello.svg?56441710
https://www.productprotection.very.co.uk/Content/css/iconfont/fontello.ttf?56441710
https://www.productprotection.very.co.uk/Error/Unhandled
https://www.productprotection.very.co.uk/Error/http404
https://www.productprotection.very.co.uk/Home/ContactUs
https://www.productprotection.very.co.uk/Home/FAQ
https://www.productprotection.very.co.uk/Process/Go/10
https://www.productprotection.very.co.uk/Process/Go/15
https://www.productprotection.very.co.uk/Process/PreviousStep

150010 External Links Discovered (1)

150010 External Links Discovered — *Very Product Protection*

Finding #	1475409	**Severity**	Information Gathered - Level 1
Group	Information Gathered		
CWE	-	**Detection Date**	10 Jul 2019 09:32 GMT
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: 1
https://www.google-analytics.com/analytics.js

150021 Scan Diagnostics (1)

150021 Scan Diagnostics — *Very Product Protection*

Finding #	1475401	**Severity**	Information Gathered - Level 1
Group	Information Gathered		
CWE	-	**Detection Date**	10 Jul 2019 09:32 GMT
OWASP	-		
WASC	-		

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

WAS Web Application Report

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 69 requests, 11 seconds. Completed 69 requests of 70 estimated requests (98.5714%). 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, 2 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
Collected 39 links overall in 0 hours 3 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 2) + files:(0 x 16) + directories:(9 x 11) + paths:(0 x 27) = total (99)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 27 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 99 requests, 1 seconds. Completed 99 requests of 99 estimated requests (100%). All tests completed.
Batch #0 WS enumeration: estimated time < 1 minute (11 tests, 26 inputs)
WS enumeration: 11 vulnsigs tests, completed 123 requests, 4 seconds. Completed 123 requests of 286 estimated requests (43.007%). All tests completed.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (58 tests, 0 inputs)
Batch #1 URI parameter manipulation (no auth): 58 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #1 Form parameter manipulation (no auth): estimated time < 1 minute (58 tests, 6 inputs)
Batch #1 Form parameter manipulation (no auth): 58 vulnsigs tests, completed 356 requests, 19 seconds. Completed 356 requests of 348 estimated requests (102.299%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 0 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #1 Form blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 6 inputs)
Batch #1 Form blind SQL manipulation (no auth): 8 vulnsigs tests, completed 144 requests, 11 seconds. Completed 144 requests of 144 estimated requests (100%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 0 inputs)
Batch #1 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #1 Form field time-based tests (no auth): estimated time < 1 minute (14 tests, 6 inputs)
Batch #1 Form field time-based tests (no auth): 14 vulnsigs tests, completed 70 requests, 6 seconds. Completed 70 requests of 84 estimated requests (83.3333%). All tests completed.
Batch #1 URI parameter time-based tests for CVE-2011-3923 (no auth): estimated time < 1 minute (1 tests, 0 inputs)
Batch #1 URI parameter time-based tests for CVE-2011-3923 (no auth): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #1 Form field time-based tests for CVE-2011-3923 (no auth): estimated time < 1 minute (1 tests, 6 inputs)
Batch #1 Form field time-based tests for CVE-2011-3923 (no auth): 1 vulnsigs tests, completed 5 requests, 1 seconds. Completed 5 requests of 6 estimated requests (83.3333%). All tests completed.
Batch #2 URI parameter manipulation (no auth): estimated time < 1 minute (58 tests, 5 inputs)
Batch #2 URI parameter manipulation (no auth): 58 vulnsigs tests, completed 222 requests, 14 seconds. Completed 222 requests of 290 estimated requests (76.5517%). All tests completed.
Batch #2 Form parameter manipulation (no auth): estimated time < 1 minute (58 tests, 5 inputs)
Batch #2 Form parameter manipulation (no auth): 58 vulnsigs tests, completed 299 requests, 41 seconds. Completed 299 requests of 290 estimated requests (103.103%). All tests completed.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 5 inputs)
Batch #2 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 80 requests, 11 seconds. Completed 80 requests of 120 estimated requests (66.6667%). All tests completed.
Batch #2 Form blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 5 inputs)
Batch #2 Form blind SQL manipulation (no auth): 8 vulnsigs tests, completed 112 requests, 22 seconds. Completed 112 requests of 120 estimated requests (93.3333%). All tests completed.
Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 5 inputs)
Batch #2 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 42 requests, 5 seconds. Completed 42 requests of 70 estimated requests (60%). All tests completed.
Batch #2 Form field time-based tests (no auth): estimated time < 1 minute (14 tests, 5 inputs)
Batch #2 Form field time-based tests (no auth): 14 vulnsigs tests, completed 56 requests, 11 seconds. Completed 56 requests of 70 estimated requests (80%). All tests completed.
Batch #2 URI parameter time-based tests for CVE-2011-3923 (no auth): estimated time < 1 minute (1 tests, 5 inputs)
Batch #2 URI parameter time-based tests for CVE-2011-3923 (no auth): 1 vulnsigs tests, completed 3 requests, 1 seconds. Completed 3 requests of 5 estimated requests (60%). All tests completed.
Batch #2 Form field time-based tests for CVE-2011-3923 (no auth): estimated time < 1 minute (1 tests, 5 inputs)
Batch #2 Form field time-based tests for CVE-2011-3923 (no auth): 1 vulnsigs tests, completed 4 requests, 1 seconds. Completed 4 requests of 5 estimated requests (80%). All tests completed.
Batch #3 URI parameter manipulation (no auth): estimated time < 1 minute (58 tests, 2 inputs)
Batch #3 URI parameter manipulation (no auth): 58 vulnsigs tests, completed 148 requests, 22 seconds. Completed 148 requests of 116 estimated requests (127.586%). All tests completed.
Batch #3 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 2 inputs)
Batch #3 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 64 requests, 22 seconds. Completed 64 requests of 48 estimated requests (133.333%). All tests completed.
Batch #3 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 2 inputs)
Batch #3 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 28 requests, 9 seconds. Completed 28 requests of 28 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, 2 inputs)
Batch #3 URI parameter time-based tests for CVE-2011-3923 (no auth): 1 vulnsigs tests, completed 2 requests, 1 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
No XML requests found. Skipping XXE tests.
Batch #4 DOM XSS exploitation: estimated time < 1 minute (4 tests, 8 inputs)
Batch #4 DOM XSS exploitation: 4 vulnsigs tests, completed 64 requests, 57 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)

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

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, 20 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 20 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (37 tests, 2 inputs)
Batch #4 Cookie manipulation: 37 vulnsigs tests, completed 664 requests, 21 seconds. Completed 664 requests of 534 estimated requests (124.345%). XSS optimization removed 288 links. All tests completed.
Batch #4 Header manipulation: estimated time < 10 minutes (37 tests, 15 inputs)
Batch #4 Header manipulation: 37 vulnsigs tests, completed 440 requests, 21 seconds. Completed 440 requests of 750 estimated requests (58.6667%). XSS optimization removed 360 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 17 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 22 requests, 1 seconds. Completed 22 requests of 17 estimated requests (129.412%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 2 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 2 requests, 1 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #4 httpoxy detector: estimated time < 1 minute (1 tests, 17 inputs)
Batch #4 httpoxy detector: 1 vulnsigs tests, completed 17 requests, 1 seconds. Completed 17 requests of 17 estimated requests (100%). All tests completed.
Batch #4 httpoxy detector(form): estimated time < 1 minute (1 tests, 2 inputs)
Batch #4 httpoxy detector(form): 1 vulnsigs tests, completed 2 requests, 1 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.
Batch #4 Struts timebased detector: estimated time < 1 minute (1 tests, 17 inputs)
Batch #4 Struts timebased detector: 1 vulnsigs tests, completed 17 requests, 2 seconds. Completed 17 requests of 17 estimated requests (100%). All tests completed.
Login Brute Force manipulation estimated time: no tests enabled
Login Brute Force manipulation estimated time: no tests enabled
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 200 requests, 8 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 2) + files:(0 x 16) + directories:(4 x 11) + paths:(11 x 27) = total (341)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 27 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 307 requests, 8 seconds. Completed 307 requests of 341 estimated requests (90.0293%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 2) + files:(0 x 16) + directories:(1 x 11) + paths:(0 x 27) = total (11)
Batch #5 Tomcat Vuln manipulation: estimated time < 1 minute (1 tests, 27 inputs)
Batch #5 Tomcat Vuln manipulation: 1 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 11 estimated requests (81.8182%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 2) + files:(0 x 16) + directories:(16 x 11) + paths:(0 x 27) = total (176)
Batch #5 Time based path manipulation: estimated time < 1 minute (16 tests, 21 inputs)
Batch #5 Time based path manipulation: 16 vulnsigs tests, completed 48 requests, 960 seconds. Completed 48 requests of 176 estimated requests (27.2727%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(4 x 2) + files:(18 x 16) + directories:(102 x 11) + paths:(15 x 27) = total (1823)
Batch #5 Path manipulation: estimated time < 10 minutes (139 tests, 27 inputs)
Batch #5 Path manipulation: 139 vulnsigs tests, completed 1432 requests, 30 seconds. Completed 1432 requests of 1823 estimated requests (78.5518%). All tests completed.
Generic WebCgi Test no test enabled
Total requests made: 5278
Average server response time: 0.18 seconds

150028 Cookies Collected (1)

150028 Cookies Collected

Very Product Protection

Finding #	1475404	**Severity**	Information Gathered - Level 1
Group	Information Gathered		
CWE	-	**Detection Date**	10 Jul 2019 09:32 GMT
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: 2
ASP.NET_SessionId=0rkyigjzfl2okkeejtzvr3b3; secure; HttpOnly; path=/ First set at URL: https://www.productprotection.very.co.uk/
__RequestVerificationToken=iMEr8wmLS3XVdWDwH29oBrrX5ytqHzop3lL1yw7qXFwi4_euDESxPxZcsYDoN4RP7GH8xQa-tvhqcGGK7WK7-miDosFlFLfkyiVnGq9N_wP0tz86mL42_QepQ2pwsksVhRZA47yVMMbE8Efnvhy7wA2; secure; HttpOnly; path=/ First set at URL: https://www.productprotection.very.co.uk/Account/SignIn

150082 Protection against Clickjacking vulnerability (1)

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

WAS Web Application Report

150082 Protection against Clickjacking vulnerability

Very Product Protection

Finding #	1550926	**Severity**	Information Gathered - Level 1
Group	Information Gathered		
CWE	-	**Detection Date**	10 Jul 2019 09:32 GMT
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://www.productprotection.very.co.uk/Account/InputUserId
https://www.productprotection.very.co.uk/Account/InputUserId?returnurl=NewEnrole
https://www.productprotection.very.co.uk/Error/Unhandled
https://www.productprotection.very.co.uk/Error/http404
https://www.productprotection.very.co.uk/Home/ContactUs
https://www.productprotection.very.co.uk/Home/FAQ

150099 Cookies Issued Without User Consent (1)

150099 Cookies Issued Without User Consent

Very Product Protection

Finding #	1475407	**Severity**	Information Gathered - Level 1
Group	Information Gathered		
CWE	-	**Detection Date**	10 Jul 2019 09:32 GMT
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: 2
ASP.NET_SessionId=1usdzlertlhsaxix21qegjz0; secure; HttpOnly; path=/ First set at URL: https://www.productprotection.very.co.uk/
__RequestVerificationToken=MUGb3YBH60hnMrbYuC7Mbyu-udmF80VVGC3djmYMk2nsO1O-oYejJLaSVTnC_zYV3JZFu7VVLnRw5fszxZ7bce-jNO0299Tg1pt2uEW0X2jeSPN3tdwTBiu1duaTZCZCAgsN3DX6CAqsQVX2mecIBw2; secure; HttpOnly; path=/ First set at URL: https://www.productprotection.very.co.uk/Account/SignIn

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

WAS Web Application Report

150104 Form Contains Email Address Field (1)

150104 Form Contains Email Address Field *Very Product Protection*

Finding #	1475411	**Severity**	Information Gathered - Level 1
Group	Information Gathered		
CWE	-	**Detection Date**	10 Jul 2019 09:32 GMT
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://www.productprotection.very.co.uk/Account/InputUserId?returnurl=NewEnrole

150126 Links With High Resource Consumption (1)

150126 Links With High Resource Consumption *Very Product Protection*

Finding #	1475403	**Severity**	Information Gathered - Level 1
Group	Information Gathered		
CWE	-	**Detection Date**	10 Jul 2019 09:32 GMT
OWASP	-		
WASC	-		

Details

Threat

The list of links with lowest bytes/sec which are assumed to be resources with highest resource consumption. The links in the list have slower transfer times speeds to an average resource on the server. This may indicate that the links are more CPU or DB intensive than majority of links.

The latency of the network and file size have no effect on calculations.

Impact

The links with high resource consumption could be used to perform DOS on the server by just performing GET Flooding. Attackers could more easily take the server down if there are huge resource hogs on it, performing less request.

Solution

Find the root cause of resources slow download speed.

If the cause is a real CPU strain or complex DB queries performed, there may be a need for re-engineering of the web application or defense measures should be in place. Examples of defense against DOS that is targeted towards high resource consumption links are Load Balancers and Rate Limiters.

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

Results

1015.400000 bytes/sec https://www.productprotection.very.co.uk/Account/IsUniqueMail?Email=&urn=
5178.000000 bytes/sec https://www.productprotection.very.co.uk/Scripts/visibility.js
8813.500000 bytes/sec https://www.productprotection.very.co.uk/Scripts/authenticatedInfo.js
45780.800000 bytes/sec https://www.productprotection.very.co.uk/Scripts/buttons.js
54256.100000 bytes/sec https://www.productprotection.very.co.uk/Scripts/ResponsiveHeightCaption.js
54638.100000 bytes/sec https://www.productprotection.very.co.uk/Scripts/addresses.js
65133.400000 bytes/sec https://www.productprotection.very.co.uk/Scripts/jquery.bgiframe.js
82720.000000 bytes/sec https://www.productprotection.very.co.uk/Content/css/iconfont/fontello.svg?56441710
118889.400000 bytes/sec https://www.productprotection.very.co.uk/Content/css/iconfont/fontello.woff?56441710
206620.000000 bytes/sec https://www.productprotection.very.co.uk/Content/css/iconfont/fontello.ttf?56441710

150152 Forms Crawled (1)

150152 Forms Crawled

Very Product Protection

Finding #	1475402	**Severity**	Information Gathered - Level 1
Group	Information Gathered		
CWE	-	**Detection Date**	10 Jul 2019 09:32 GMT
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): 3

Crawled forms (Total: 3)
NOTE: This does not include authentication forms. Authentication forms are reported separately in QID 150115
Form #:1 Action URI:https://www.productprotection.very.co.uk/Account/IsUniqueMail?Email=&urn=
Form Fields: __RequestVerificationToken, Email, Password, ClientCustRef, password and 1 field(s) without name.

Form #:2 Action URI:https://www.productprotection.very.co.uk/Account/IsUniqueMail?Email=was%40qualys.com&urn=1
Form Fields: __RequestVerificationToken, ReturnUrl, Email, ClientCustRef

Form #:3 Action URI:https://www.productprotection.very.co.uk/BookNewService/JobPage

150176 JavaScript Libraries Detected (1)

150176 JavaScript Libraries Detected

Very Product Protection

Finding #	1475397	**Severity**	Information Gathered - Level 1
Group	Information Gathered		
CWE	-	**Detection Date**	10 Jul 2019 09:32 GMT
OWASP	-		
WASC	-		

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

Details

Threat
The JavaScript libraries discovered by the Web Application Scanning engine are provided in the Results section. The discovered libraries are reported only once based on the page of the web application on which they were first detected. These libraries are reported along with other information such as: the page on which they were first found and their version and script uri.

Impact
N/A

Solution
N/A

Results

Number of unique JS libraries: 4
Javascript library : jQuery
Version : 1.8.2
Script uri : https://www.productprotection.very.co.uk/Scripts/jquery-1.8.2.js
Found on the following page(only first page is reported):
https://www.productprotection.very.co.uk/Account/SignIn

==========

Javascript library : jQuery.ui.autocomplete
Version : 1.9.0
Script uri : https://www.productprotection.very.co.uk/Scripts/jquery-ui-1.9.0.js
Found on the following page(only first page is reported):
https://www.productprotection.very.co.uk/Account/SignIn

==========

Javascript library : jQuery.ui.dialog
Version : 1.9.0
Script uri : https://www.productprotection.very.co.uk/Scripts/jquery-ui-1.9.0.js
Found on the following page(only first page is reported):
https://www.productprotection.very.co.uk/Account/SignIn

==========

Javascript library : jQuery.ui.tooltip
Version : 1.9.0
Script uri : https://www.productprotection.very.co.uk/Scripts/jquery-ui-1.9.0.js
Found on the following page(only first page is reported):
https://www.productprotection.very.co.uk/Account/SignIn

==========

45038 Host Scan Time (1)

45038 Host Scan Time

Very Product Protection

Finding #	1475405	**Severity**	Information Gathered - Level 1
Group	Information Gathered		
CWE	-	**Detection Date**	19 Jun 2019 09:31 GMT
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.

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

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: 1632 seconds

Start time: Wed, Jun 19 2019, 09:31:36 GMT

End time: Wed, Jun 19 2019, 09:58:48 GMT

6 DNS Host Name (1)

6 DNS Host Name

Very Product Protection

Finding #	1475400	**Severity**	Information Gathered - Level 1
Group	Information Gathered		
CWE	-	**Detection Date**	19 Jun 2019 09:31 GMT
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
109.69.232.193	No registered hostname

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.

WAS Web Application Report

Appendix

Web Application Details
Very Product Protection

Name	Very Product Protection
URL	https://www.productprotection.very.co.uk
Owner	Brian Martin (fxzne-tf)
Scope	Limit to URL hostname
Operating System	Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2019, Qualys, Inc.