

Part 1. Scan Information

Scan Customer Company:	Safenames Ltd	ASV Company:	Comodo CA Limited
Date scan was completed:	10-01-2018	Scan expiration date:	12-30-2018






















Part 2. Component Compliance Summary






Component (IP Address, domain, etc.):217.19.248.70	Pass <input type="checkbox"/>	Fail <input checked="" type="checkbox"/>
--	-------------------------------	--

Part 3a. Vulnerabilities Noted for each Component

ASV may choose to omit vulnerabilities that do not impact compliance from this section, however, failing vulnerabilities that have been changed to "pass" via exceptions or after remediation / rescan must always be listed

Component	Vulnerabilities Noted per Component	Severity level	CVSS Score	Compliance Status		Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
				Pass	Fail	
217.19.248.70	JQuery 1.x < 1.12.0 / 2.x < 2.2.0 XSS 443 / tcp / www	Medium	4.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Automatic Failures
217.19.248.70	CVE-2015-9251 HTTP Server Type and Version 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	HyperText Transfer Protocol (HTTP) Redirect Information 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	HyperText Transfer Protocol (HTTP) Redirect Information 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Web Application Sitemap 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Nessus SYN scanner 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Nessus SYN scanner 80 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	HSTS Missing From HTTPS Server 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	JQuery Detection 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	SSL Cipher Block Chaining Cipher Suites Supported 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Web Server Directory Enumeration 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Web Application Potentially Sensitive CGI Parameter Detection 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Device Type 0 / tcp /	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	SSL Cipher Suites Supported 443 / tcp / www	Low	0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The vulnerability is not included in the NVD

Component	Vulnerabilities Noted per Component	Severity level	CVSS Score	Compliance Status		Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
				Pass	Fail	
217.19.248.70	Common Platform Enumeration (CPE) 0 / tcp /	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	HTTP Methods Allowed (per directory) 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	HTTP Methods Allowed (per directory) 80 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	SSL Root Certification Authority Certificate Information 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Service Detection 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Service Detection 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Service Detection 80 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	HyperText Transfer Protocol (HTTP) Information 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	HyperText Transfer Protocol (HTTP) Information 80 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Web Server Harvested Email Addresses 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	HTTP X-Content-Security-Policy Response Header Usage 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	SSL Certificate Information 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Web Server Office File Inventory 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	SSL / TLS Versions Supported 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	HTTP X-Frame-Options Response Header Usage 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	TCP/IP Timestamps Supported 0 / tcp /	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	SSL Perfect Forward Secrecy Cipher Suites Supported 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	OS Identification 0 / tcp /	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Additional DNS Hostnames 0 / tcp /	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Web Server No 404 Error Code Check 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	Web Server No 404 Error Code Check 80 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD

Component	Vulnerabilities Noted per Component	Severity level	CVSS Score	Compliance Status		Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
				Pass	Fail	
217.19.248.70	CGI Generic Tests Load Estimation (all tests) 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	CGI Generic Tests Load Estimation (all tests) 80 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	CGI Generic Injectable Parameter 443 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	HTTP Server Type and Version 80 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD
217.19.248.70	CGI Generic Injectable Parameter 80 / tcp / www	Low	0.0		<input type="checkbox"/>	The vulnerability is not included in the NVD

Consolidated Solution/Correction Plan for above IP address:
Upgrade to JQuery version 1.12.0 or later.
Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.
Protect your target with an IP filter.
Configure the remote web server to use HSTS.
Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.
Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.
Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.
Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Set a properly configured X-Frame-Options header for all requested resources.
If you want to test them, re-scan using the special vhost syntax, such as :

www.example.com[192.0.32.10]

Part 3b. Special Notes by Component

Component	Special Note	Item Noted	Scan customer`s description of action taken and declaration that software is either implemented securely or removed

Part 3c. Special notes -- Full Text
Note

Part 4a. Scope Submitted by Scan Customer for Discovery
IP Addresses/ranges/subnets, domains, URLs, etc.

IP_ADDRESS:217.19.248.70

Part 4b. Scan Customer Designated “In-Scope” Components (Scanned)

IP Addresses/ranges/subnets, domains, URLs, etc.

217.19.248.70

Part 4c. Scan Customer Designated “Out-of-Scope” Components (Not Scanned)

Requires description for each IP Address/range/subnet, domain, URL