GDPR report for iGDPR following the Portugal's specific rules

Lawfulness, fairness and transparency

In compliance with:

- Does your software ask and record for consent
- Does the processing has an appropriate ground?
- Does the consent inform the Inviduals about the processing method?
- Have you performed any audit to map data flows?

Not in compliance with:

- Does your application provide any informatation regarding the Individual's rights

  ##### Suggestions to be in compliance

  - TODO

Purpose limitation

No principles defined

Data minimisation

In compliance with:

Not in compliance with:

- The data being collected is sufficient to fulfill the consent purposes

  ##### Suggestions to be in compliance

  - TODO
- Is your application holding more data than the what is being used?

  ##### Suggestions to be in compliance

  - TODO
- Is it possible to demonstrate your data minimization practices?

  ##### Suggestions to be in compliance

  - TODO

Accuracy

No principles defined

Storage limitation

In compliance with:

Not in compliance with:

- Is it possible to justify the time frame for the retained data?

  ##### Suggestions to be in compliance

  - TODO
- Does your application automatically deletes the data after the time frame expires?

Suggestions to be in compliance

  - TODO

- Does your application provides a way, so the individual can erease his data(right to erasure)?

  #### Suggestions to be in compliance

  - TODO

Integrity and confidentiality (security)

No principles defined

Accountability

No principles defined

Rules Specific for the selected country

In compliance with:

Not in compliance with:

- x

  #### Suggestions to be in compliance

  - TODO

- y

  #### Suggestions to be in compliance

  - TODO

- z

  #### Suggestions to be in compliance

  - TODO

Nmap Scan Report - Scanned at Sat Apr 25 01:46:51 2020

Scan Summary | **localhost (127.0.0.1)**

Scan Summary

Nmap 7.60 was initiated at Sat Apr 25 01:46:51 2020 with these arguments:
nmap -oX - -sV --script=nmap-vulners/vulners.nse 127.0.0.1

Verbosity: 0; Debug level 0

Nmap done at Sat Apr 25 01:49:30 2020; 1 IP address (1 host up) scanned in 158.35 seconds

127.0.0.1 / localhost

Address

- 127.0.0.1 (ipv4)

Hostnames

- localhost (PTR)

Ports

The 994 ports scanned but not shown below are in state: **closed**

- 994 ports replied with: **conn-refused**

<table>
<tr><th colspan="2">Port</th><th>State (toggle closed [0] | filtered [0])</th><th>Service</th><th>Reason</th><th>Product</th><th>Version</th><th>Extra info</th></tr>
<tr><td>631</td><td>tcp</td><td>open</td><td>ipp</td><td>syn-ack</td><td>CUPS</td><td>2.2</td><td></td></tr>
<tr><td></td><td>http-server-header</td><td colspan="6">CUPS/2.2 IPP/2.1</td></tr>
<tr><td>5000</td><td>tcp</td><td>open</td><td>http</td><td>syn-ack</td><td>Werkzeug httpd</td><td>0.14.1</td><td>Python 3.8.0</td></tr>
<tr><td></td><td>http-server-header</td><td colspan="6">Werkzeug/0.14.1 Python/3.8.0</td></tr>
<tr><td></td><td>vulners</td><td colspan="6">cpe:/a:python:python:3.8.0:
CVE-2020-8492 7.1 https://vulners.com/cve/CVE-2020-8492
CVE-2019-17514 5.0 https://vulners.com/cve/CVE-2019-17514
CVE-2020-8315 4.3 https://vulners.com/cve/CVE-2020-8315
CVE-2019-18348 4.3 https://vulners.com/cve/CVE-2019-18348</td></tr>
<tr><td>5432</td><td>tcp</td><td>open</td><td>postgresql</td><td>syn-ack</td><td>PostgreSQL DB</td><td>9.6.0 or later</td><td></td></tr>
<tr><td></td><td>fingerprint-strings</td><td colspan="6">SMBProgNeg:
SFATAL
VFATAL
C0A000
Munsupported frontend protocol 65363.19778: server supports 2.0 to 3.0
Fpostmaster.c
L2065
RProcessStartupPacket</td></tr>
<tr><td>8000</td><td>tcp</td><td>open</td><td>nagios-nsca</td><td>syn-ack</td><td>Nagios NSCA</td><td></td><td></td></tr>
<tr><td>8090</td><td>tcp</td><td>open</td><td>opsmessaging</td><td>syn-ack</td><td></td><td></td><td></td></tr>
<tr><td></td><td>fingerprint-strings</td><td colspan="6">GetRequest, HTTPOptions:
HTTP/1.1 502 Bad Gateway
Content-Type: text/plain; charset=UTF-8
Content-Length: 1679
Error [java.net.UnknownHostException]: null
Stack Trace:
java.net.UnknownHostException: null
java.net.AbstractPlainSocketImpl.connect(AbstractPlainSocketImpl.java:184)
java.net.SocksSocketImpl.connect(SocksSocketImpl.java:392)
java.net.Socket.connect(Socket.java:607)
sun.security.ssl.SSLSocketImpl.connect(SSLSocketImpl.java:666)
org.parosproxy.paros.network.SSLConnector.createSocket(SSLConnector.java:450)
org.apache.commons.httpclient.HttpConnection.open(HttpConnection.java:728)
org.apache.commons.httpclient.MultiThreadedHttpConnectionManager$HttpConnectionAdapter.open(MultiThreadedHttpConnectionManager.java:1361)
org.apache.commons.httpclient.HttpMethodDirector.executeWithRetry(HttpMethodDirector.java:449)
org.apache.commons.httpclient.HttpMethodDirector.e</td></tr>
<tr><td>9000</td><td>tcp</td><td>open</td><td>cslistener</td><td>syn-ack</td><td></td><td></td><td></td></tr>
</table>

[redacted]

	fingerprint-strings	GenericLines:
		  HTTP/1.1 400 Bad Request
		  Content-Type: text/plain; charset=utf-8
		  Connection: close
		  Request
		GetRequest, HTTPOptions:
		  HTTP/1.0 200 OK
		  Accept-Ranges: bytes
		  Cache-Control: max-age=31536000
		  Content-Length: 23032
		  Content-Type: text/html; charset=utf-8
		  Last-Modified: Thu, 19 Mar 2020 22:46:17 GMT
		  X-Content-Type-Options: nosniff
		  X-Xss-Protection: 1; mode=block
		  Date: Sat, 25 Apr 2020 00:46:58 GMT
		  <!DOCTYPE html><html lang="en" ng-app="portainer">
		  <head>
		  <meta charset="utf-8">
		  <title>Portainer</title>
		  <meta name="description" content="">
		  <meta name="author" content="Portainer.io">
		  <!-- HTML5 shim, for IE6-8 support of HTML5 elements -->
		  <!--[if lt IE 9]>
		  <script src="//html5shim.googlecode.com/svn/trunk/html5.js"></script>
		  <![endif]-->
		  <!-- Fav and touch icons -->
		  <link rel="apple-touch-icon" sizes="180x180" href="dc4d092847be46242d8c013d1bc7c494.png">
		  <link rel="icon" type="image/png" sizes="32x32" href="5ba13dcb526292ae707310a54e103cd1.png">
		  <link rel="icon" type="image/

Go to top

Toggle Closed Ports

Toggle Filtered Ports

Misc Metrics (click to expand)

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	10
Informational	1

Alert Detail

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://public-firing-range.appspot.com/escape/serverside/escapeHtml/js_quoted_string?q=a
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/cors/alloworigin/dynamicAllowOrigin
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/urldom/location/hash/script.src.partial_domain
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/dom/toxicdom/external/sessionStorage/function/documentWrite
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/dom/toxicdom/document/cookie_set/documentWrite
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/address/location.hash/function
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/dom/toxicdom/localStorage/array
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/escape/serverside/encodeUrl/js_comment?q=a
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/reflected/escapedparameter/js_eventhandler_unquoted/UNQUOTED_ATTRIBUTE?q=a
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/escape/serverside/escapeHtml/attribute_unquoted?q=a
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/reflected/index.html
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/escape/serverside/encodeUrl/js_assignment?q=a
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/urldom/index.html

Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/angular/angular_post_message_parse/1.6.0
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/address/location/eval
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/reflected/filteredstrings/body/caseInsensitive/script?q=a
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/address/documentURI/documentwrite
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/urldom/location/search/button.formaction?//example.org
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/reflected/url/css_import?q=a
Method	GET
Parameter	X-Frame-Options
URL	https://public-firing-range.appspot.com/address/location.hash/rangeCreateContextualFragment
Method	GET
Parameter	X-Frame-Options
Instances	258
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
Source ID	3

Medium (Medium)	Secure Pages Include Mixed Content (Including Scripts)
Description	The page includes mixed content, that is content accessed via HTTP instead of HTTPS.
URL	https://public-firing-range.appspot.com/remoteinclude/parameter/script?q=http://g00gle.com/typosquatting_domain.js
Method	GET
Evidence	http://g00gle.com/typosquatting_domain.js
URL	https://public-firing-range.appspot.com/escape/serverside/escapeHtml/attribute_script?q=a
Method	GET
Evidence	http://irrelevant.google.com?a
URL	https://public-firing-range.appspot.com/remoteinclude/parameter/script?q=http://127.0.0.2/localhost_import.js
Method	GET
Evidence	http://127.0.0.2/localhost_import.js
URL	https://public-firing-range.appspot.com/mixedcontent/index.html
Method	GET
Evidence	http://public-firing-range.appspot.com/mixedcontent/script.js
URL	https://public-firing-range.appspot.com/reflected/parameter/attribute_script?q=a
Method	GET
Evidence	http://irrelevant.google.com/a
URL	https://public-firing-range.appspot.com/escape/serverside/encodeUrl/attribute_script?q=a
Method	GET
Evidence	http://irrelevant.google.com?a

URL	https://public-firing-range.appspot.com/remoteinclude/parameter/script?q=http://192.168.1.2/private_network_import.js
Method	GET
Evidence	http://192.168.1.2/private_network_import.js
Instances	7
Solution	A page that is available over SSL/TLS must be comprised completely of content which is transmitted over SSL/TLS. The page must not contain any content that is transmitted over unencrypted HTTP. This includes content from third party sites.
Other information	tag=script src=http://g00gle.com/typosquatting_domain.js

Reference	https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
CWE Id	311
WASC Id	4
Source ID	3

Medium (Medium)	**CSP Scanner: Wildcard Directive**
Description	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, script-src-elem, script-src-attr, style-src, style-src-elem, style-src-attr, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src, prefetch-src

URL	https://public-firing-range.appspot.com/invalidframingconfig/xfodenynoframeancestorsnone
Method	GET
Parameter	Content-Security-Policy
Evidence	frame-ancestors 'self'
URL	https://public-firing-range.appspot.com/invalidframingconfig/frameancestorsselfnoxfosameorigin
Method	GET
Parameter	Content-Security-Policy
Evidence	frame-ancestors 'self'
URL	https://public-firing-range.appspot.com/invalidframingconfig/xfoallowfromnocoverdomain
Method	GET
Parameter	Content-Security-Policy
Evidence	frame-ancestors https://google.com
URL	https://public-firing-range.appspot.com/invalidframingconfig/xfosameoriginnoframeancestorsself
Method	GET
Parameter	Content-Security-Policy
Evidence	frame-ancestors https://google.com
URL	https://public-firing-range.appspot.com/invalidframingconfig/frameancestorsnoxfoallowfrom
Method	GET
Parameter	Content-Security-Policy
Evidence	frame-ancestors https://example.com
URL	https://public-firing-range.appspot.com/invalidframingconfig/frameancestorsnonenoxfodeny
Method	GET
Parameter	Content-Security-Policy
Evidence	frame-ancestors 'none'
Instances	6
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://public-firing-range.appspot.com/mixedcontent/script.js
Method	GET
Parameter	X-Content-Type-Options
Instances	1
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://public-firing-range.appspot.com/escape/serverside/encodeUrl/js_assignment?q=a
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/dom/toxicdom/external/sessionStorage/function/documentWrite
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/urldom/location/hash/window.open
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/escape/serverside/escapeHtml/attribute_unquoted?q=a
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/angular/angular_post_message_parse/1.6.0
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/reflected/filteredstrings/body/caseInsensitive/script?q=a
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/escape/serverside/encodeUrl/js_comment?q=a
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/reflected/escapedparameter/js_eventhandler_quoted/DOUBLE_QUOTED_ATTRIBUTE?q=a
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/escape/serverside/encodeUrl/tagname?q=a
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/reflected/parameter/attribute_singlequoted?q=a

Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/angular/angular_body/1.2.0?q=test
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/address/location.hash/rangeCreateContextualFragment
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/escape/js/escape?q=a
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/dom/toxicdom/window/name/innerHtml
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/escape/serverside/escapeHtml/js_quoted_string?q=a
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/address/location/assign
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/reflected/parameter/attribute_script?q=a
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/flashinjection/callbackIsEchoedBack?callback=func
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/reverseclickjacking/multipage/ParameterInQuery/OtherParameter/WithoutXFO/?q=%26callback%3Dfoo%23
Method	GET
Parameter	X-Content-Type-Options
URL	https://public-firing-range.appspot.com/dom/toxicdomscripts/localStorage/array/eval
Method	GET
Parameter	X-Content-Type-Options
Instances	290
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Other information	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.

Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	**Web Browser XSS Protection Not Enabled**
Description	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server

URL	https://public-firing-range.appspot.com/cors/index.html
Method	GET
Parameter	X-XSS-Protection
URL	https://public-firing-range.appspot.com/address/URL/documentwrite

Method	GET
Parameter	X-XSS-Protection
Evidence	X-XSS-Protection: 0
URL	https://public-firing-range.appspot.com/address/location.hash/onclickAddEventListener
Method	GET
Parameter	X-XSS-Protection
Evidence	X-XSS-Protection: 0
URL	https://public-firing-range.appspot.com/reflected/parameter/attribute_name?q=a
Method	GET
Parameter	X-XSS-Protection
Evidence	X-XSS-Protection: 0
URL	https://public-firing-range.appspot.com/invalidframingconfig
Method	GET
Parameter	X-XSS-Protection
URL	https://public-firing-range.appspot.com/urldom/location/hash/document.location
Method	GET
Parameter	X-XSS-Protection
Evidence	X-XSS-Protection: 0
URL	https://public-firing-range.appspot.com/dom/toxicdom
Method	GET
Parameter	X-XSS-Protection
URL	https://public-firing-range.appspot.com/reverseclickjacking/singlepage/ParameterInFragment/OtherParameter/
Method	GET
Parameter	X-XSS-Protection
Evidence	X-XSS-Protection: 0
URL	https://public-firing-range.appspot.com/dom/javascripturi.html
Method	GET
Parameter	X-XSS-Protection
URL	https://public-firing-range.appspot.com/dom/toxicdom/localStorage/array/eval
Method	GET
Parameter	X-XSS-Protection
Evidence	X-XSS-Protection: 0
URL	https://public-firing-range.appspot.com/dom/toxicdom/document/referrer/documentWrite
Method	GET
Parameter	X-XSS-Protection
Evidence	X-XSS-Protection: 0
URL	https://public-firing-range.appspot.com/escape/js
Method	GET
Parameter	X-XSS-Protection
URL	https://public-firing-range.appspot.com/redirect
Method	GET
Parameter	X-XSS-Protection
URL	https://public-firing-range.appspot.com/address/location.hash/assign
Method	GET
Parameter	X-XSS-Protection
Evidence	X-XSS-Protection: 0
URL	https://public-firing-range.appspot.com/invalidframingconfig/xfodenynoframeancestorsnone
Method	GET
Parameter	X-XSS-Protection
URL	https://public-firing-range.appspot.com/address/location.hash/innerHtml
Method	GET
Parameter	X-XSS-Protection

Evidence	X-XSS-Protection: 0
URL	https://public-firing-range.appspot.com/remoteinclude/parameter/script?q=http://g00gle.com/typosquatting_domain.js
Method	GET
Parameter	X-XSS-Protection
Evidence	X-XSS-Protection: 0
URL	https://public-firing-range.appspot.com/dom/toxicdom/external/sessionStorage/function/innerHtml
Method	GET
Parameter	X-XSS-Protection
Evidence	X-XSS-Protection: 0
URL	https://public-firing-range.appspot.com/escape/serverside/encodeUrl/js_slashquoted_string?q=a
Method	GET
Parameter	X-XSS-Protection
Evidence	X-XSS-Protection: 0
URL	https://public-firing-range.appspot.com/reflected/parameter/body/400?q=a
Method	GET
Parameter	X-XSS-Protection
Evidence	X-XSS-Protection: 0
Instances	323
Solution	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
Other information	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
Reference	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://www.veracode.com/blog/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3

Low (Medium)	**Incomplete or No Cache-control and Pragma HTTP Header Set**
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://public-firing-range.appspot.com/flashinjection/callbackParameterDoesNothing?callback=func
Method	GET
Parameter	Cache-Control
URL	https://public-firing-range.appspot.com
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/urldom/index.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/flashinjection/callbackIsEchoedBack?callback=func
Method	GET
Parameter	Cache-Control
URL	https://public-firing-range.appspot.com/mixedcontent/index.html

Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/remoteinclude/script_hash.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/remoteinclude/object_hash.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/dom/index.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/dom/javascripturi.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/redirect/index.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/reflected/index.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/address/index.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/tags/index.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/cors/index.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/vulnerablelibraries/index.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/flashinjection/index.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/angular/index.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/escape/index.html

Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
URL	https://public-firing-range.appspot.com/remoteinclude/index.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=600
Instances	26
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
Source ID	3

Low (Medium)	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.

URL	https://public-firing-range.appspot.com/angular/angular_body_alt_symbols_raw/1.6.0?q=test
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/angularjs/1.6.0/angular.js
Evidence	<script src="//ajax.googleapis.com/ajax/libs/angularjs/1.6.0/angular.js"></script>
URL	https://public-firing-range.appspot.com/angular/angular_form_parse/1.6.0
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/angularjs/1.6.0/angular.js
Evidence	<script src="//ajax.googleapis.com/ajax/libs/angularjs/1.6.0/angular.js"></script>
URL	https://public-firing-range.appspot.com/remoteinclude/parameter/script?q=http://g00gle.com/typosquatting_domain.js
Method	GET
Parameter	http://g00gle.com/typosquatting_domain.js
Evidence	<script src="http://g00gle.com/typosquatting_domain.js"></script>
URL	https://public-firing-range.appspot.com/remoteinclude/parameter/script?q=http://192.168.1.2/private_network_import.js
Method	GET
Parameter	http://192.168.1.2/private_network_import.js
Evidence	<script src="http://192.168.1.2/private_network_import.js"></script>
URL	https://public-firing-range.appspot.com/escape/serverside/encodeUrl/attribute_script?q=a
Method	GET
Parameter	http://irrelevant.google.com?a
Evidence	<script src="http://irrelevant.google.com?a"/>
URL	https://public-firing-range.appspot.com/vulnerablelibraries/jquery.html
Method	GET
Parameter	https://code.jquery.com/jquery-1.8.1.js
Evidence	<script src="https://code.jquery.com/jquery-1.8.1.js"></script>
URL	https://public-firing-range.appspot.com/angular/angular_body_raw_escaped/1.4.0?q=test
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/angularjs/1.4.0/angular.js
Evidence	<script src="//ajax.googleapis.com/ajax/libs/angularjs/1.4.0/angular.js"></script>
URL	https://public-firing-range.appspot.com/escape/serverside/escapeHtml/attribute_script?q=a
Method	GET
Parameter	http://irrelevant.google.com?a
Evidence	<script src="http://irrelevant.google.com?a"/>

URL	https://public-firing-range.appspot.com/remoteinclude/parameter/script?q=https://google.com
Method	GET
Parameter	https://google.com
Evidence	<script src="https://google.com"></script>
URL	https://public-firing-range.appspot.com/angular/angular_body/1.2.24?q=test
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/angularjs/1.2.24/angular.js
Evidence	<script src="//ajax.googleapis.com/ajax/libs/angularjs/1.2.24/angular.js"></script>
URL	https://public-firing-range.appspot.com/angular/angular_body_raw_escaped_alt_symbols/1.4.0?q=test
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/angularjs/1.4.0/angular.js
Evidence	<script src="//ajax.googleapis.com/ajax/libs/angularjs/1.4.0/angular.js"></script>
URL	https://public-firing-range.appspot.com/angular/angular_body_raw_post/1.6.0
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/angularjs/1.6.0/angular.js
Evidence	<script src="//ajax.googleapis.com/ajax/libs/angularjs/1.6.0/angular.js"></script>
URL	https://public-firing-range.appspot.com/angular/angular_body_attribute_ng/1.4.0?q=test
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/angularjs/1.4.0/angular.js
Evidence	<script src="//ajax.googleapis.com/ajax/libs/angularjs/1.4.0/angular.js"></script>
URL	https://public-firing-range.appspot.com/angular/angular_body_alt_symbols/1.4.0?q=test
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/angularjs/1.4.0/angular.js
Evidence	<script src="//ajax.googleapis.com/ajax/libs/angularjs/1.4.0/angular.js"></script>
URL	https://public-firing-range.appspot.com/reflected/parameter/attribute_script?q=a
Method	GET
Parameter	http://irrelevant.google.com/a
Evidence	<script src="http://irrelevant.google.com/a"/>
URL	https://public-firing-range.appspot.com/angular/angular_post_message_parse/1.6.0
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/angularjs/1.6.0/angular.js
Evidence	<script src="//ajax.googleapis.com/ajax/libs/angularjs/1.6.0/angular.js"></script>
URL	https://public-firing-range.appspot.com/remoteinclude/parameter/script?q=http://127.0.0.2/localhost_import.js
Method	GET
Parameter	http://127.0.0.2/localhost_import.js
Evidence	<script src="http://127.0.0.2/localhost_import.js"></script>
URL	https://public-firing-range.appspot.com/angular/angular_body_raw/1.4.0?q=test
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/angularjs/1.4.0/angular.js
Evidence	<script src="//ajax.googleapis.com/ajax/libs/angularjs/1.4.0/angular.js"></script>
URL	https://public-firing-range.appspot.com/angular/angular_body/1.1.5?q=test
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/angularjs/1.1.5/angular.js
Evidence	<script src="//ajax.googleapis.com/ajax/libs/angularjs/1.1.5/angular.js"></script>
URL	https://public-firing-range.appspot.com/angular/angular_body/1.6.0?q=test
Method	GET
Parameter	//ajax.googleapis.com/ajax/libs/angularjs/1.6.0/angular.js
Evidence	<script src="//ajax.googleapis.com/ajax/libs/angularjs/1.6.0/angular.js"></script>
Instances	29
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	

CWE Id	829
WASC Id	15
Source ID	3

Low (Medium)	**Application Error Disclosure**
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

URL	https://public-firing-range.appspot.com/reverseclickjacking/singlepage/ParameterInFragment
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reverseclickjacking/multipage/ParameterInQuery/OtherParameter
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reflected/parameter
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reflected/url
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reflected/filteredstrings
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reflected/filteredcharsets
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reverseclickjacking/multipage/ParameterInQuery/InCallback
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/escape/serverside
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/dom/toxicdom/external/localStorage
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reflected/parameter/body/500?q=a
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reverseclickjacking/multipage
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/dom/toxicdom/external/sessionStorage
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/leakedcookie
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reflected/filteredcharsets/body
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reflected/url/a
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error

URL	https://public-firing-range.appspot.com/escape/js
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reverseclickjacking/multipage/ParameterInFragment/OtherParameter
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reverseclickjacking/singlepage
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reflected/filteredstrings/body
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	https://public-firing-range.appspot.com/reflected/escapedparameter
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
Instances	33
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	200
WASC Id	13
Source ID	3

Low (Medium)	**Cookie Without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

URL	https://public-firing-range.appspot.com/leakedcookie/leakedcookie
Method	GET
Parameter	my_secret_cookie
Evidence	Set-Cookie: my_secret_cookie
URL	https://public-firing-range.appspot.com/leakedcookie/leakedinresource
Method	GET
Parameter	my_secret_cookie
Evidence	Set-Cookie: my_secret_cookie
Instances	2
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	16
WASC Id	13
Source ID	3

Low (Medium)	**Absence of Anti-CSRF Tokens**

Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

URL	https://public-firing-range.appspot.com/reflected/parameter/form
Method	GET
Evidence	<form method="POST">
URL	https://public-firing-range.appspot.com/angular/angular_body_raw_post/1.6.0
Method	POST
Evidence	<form action="" method="post">
URL	https://public-firing-range.appspot.com/reflected/parameter/form
Method	POST
Evidence	<form method="POST">
URL	https://public-firing-range.appspot.com/angular/angular_body_raw_post/1.6.0
Method	GET
Evidence	<form action="" method="post">
Instances	4
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Other information	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret] was found in the following HTML form: [Form 1: "q"].

Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9

Source ID	3

Low (Medium)	**Private IP Disclosure**
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	https://public-firing-range.appspot.com/remoteinclude/parameter/script?q=http://192.168.1.2/private_network_import.js
Method	GET
Evidence	192.168.1.2
URL	https://public-firing-range.appspot.com/badscriptimport/index.html
Method	GET
Evidence	192.168.1.2
Instances	2
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP/PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Other information	192.168.1.2
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	200
WASC Id	13
Source ID	3

Low (Medium)	**Cookie Without Secure Flag**
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://public-firing-range.appspot.com/leakedcookie/leakedcookie
Method	GET
Parameter	my_secret_cookie
Evidence	Set-Cookie: my_secret_cookie
URL	https://public-firing-range.appspot.com/leakedcookie/leakedinresource
Method	GET
Parameter	my_secret_cookie
Evidence	Set-Cookie: my_secret_cookie
Instances	2
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)
CWE Id	614
WASC Id	13
Source ID	3

Informational (Medium)	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://public-firing-range.appspot.com/reverseclickjacking/singlepage/ParameterInFragment/OtherParameter/
Method	GET
URL	https://public-firing-range.appspot.com/reverseclickjacking/multipage/ParameterInFragment/InCallback/WithXFO/
Method	GET
URL	https://public-firing-range.appspot.com/reverseclickjacking/multipage/ParameterInFragment/OtherParameter/WithoutXFO/
Method	GET
URL	https://public-firing-range.appspot.com/reverseclickjacking/multipage/ParameterInFragment/OtherParameter/WithXFO/
Method	GET
URL	https://public-firing-range.appspot.com/reverseclickjacking/singlepage/ParameterInFragment/InCallback/
Method	GET
URL	https://public-firing-range.appspot.com/reverseclickjacking/multipage/ParameterInFragment/InCallback/WithoutXFO/
Method	GET

Instances	6
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

Other information	<script>
	var resultDiv = document.getElementById('result');
	/**
	* Callback function that receives data from the JSONP callback and
	* prints a "stringified" representation of the response, just for
	* human debugging.
	*/
	function callbackFunc(data) {
	resultDiv.textContent = 'JSONP data received: ' + JSON.stringify(data);
	}
	try {
	// Retrieve the "q" parameter in the URL fragment
	var q = decodeURIComponent(new RegExp('[?&#]q=([^&]*)')
	.exec(location.hash)[1]);
	// Validate it (prevents trivial XSS)
	var allowedPattern = /^[a-zA-Z0-9\._&#=]+$/;
	if (allowedPattern.test(q)) {
	// The vulnerability arises because of this insecure concatenation
	var url = '/reverseclickjacking/jsonpendpoint?q=' + q
	+ '&callback=callbackFunc';
	/* Create the <script> tag that executes the JS code returned by
	* the JSONP endpoint. */
	var s = document.createElement('script');
	s.type = 'text/javascript';
	s.src = url;
	document.body.appendChild(s);
	}
	} catch(e) {
	resultDiv.textContent = 'Please specify a q parameter in the fragment.';
	}
	</script>

Reference	
CWE Id	200
WASC Id	13
Source ID	3