Laboratory Exercise – Natas Level 0-6 (Exercise H1)

1. Overview

In this lab exercise, students will learn new skills by setting up the Sublime Text editor with Python and using it to test web applications. Using the Brigante (2020) environment, students will be presented with progressive challenges from the OverTheWire website (Natas) in which they will use previously learned skills to find the Capture the Flag (CTF) flags.

2. Resources required

This exercise requires the Brigante VM running in the Cyber Range.

3. Initial Setup

For this exercise, you will log in to your Cyber Range account, select the Brigante (2020) environment, click "start" to start your environment, and then "join" to get to your Linux desktop.

4. Tasks

Task 1: Setting up SublimeText

The first thing we need to do is download and install the GPG key (GNU PGP Key). This allows for a secure download from the creators of SublimeText. Then we will configure the repo for the version of SublimeText we are downloading. The final step is to update and install the application. This is a CentOS Linux distribution, so some of the commands will be slightly different.

- In a root terminal, type the following: yum install python python3-pip when prompt type y and press enter.
- In a root terminal, type the following: pip3 install requests-html and press enter.
- In a root terminal, type the following:
 rpm -v --import https://download.sublimetext.com/sublimehq-rpm-pub.gpg
 and press enter. The terminal will return to the prompt if completed correctly.
- Type the following: yum-config-manager --add-repo https://download.sublimetext.com/rpm/stable/x86 64/sublime-text.repo and press enter.
- Type the following: yum install sublime-text and press enter. When prompted type y and press enter.





 Package	Arch	Version	Reposito	ry Siz	e e
Installing: sublime-text	x86_64	3211-1	sublime-1	text 13	M
Transaction Summa	ry				
Install 1 Package	e				
Total download si Installed size: 3 Is this ok [y/d/N Downloading packa sublime-text-3211 Running transacti Running transacti Transaction test Running transaction	ze: 13 M 3 M]: y ges: -1.x86_64.rpm on check on test succeeded on	×86 64	I	13 MB 00:00:00	
Verifying : su	blime-text-3211-1.; blime-text-3211-1.;	(86_64 (86_64		1/ 1/	1 '1
Installed: sublime-text.x8	6_64 0:3211-1				
Complete! [root@ip-10-1-49-:	229 student]#				
xNDA1MTQwLTI3MDAtNDQ4ZC1iN	/IDU0LTBhN2UzN2JjOWQ4NC85NzN	12NTNjNS02NzZmLTQ1ZDItYWR			
		23	:06 Cyber Range Stu		
	Terminal - root@ip-10-1-159-180:	/home/student	+ - • ×		
File Edit View Terminal T Installing: sublime-text	x86 64 4126-1	sublime-text	20 M		
Transaction Summary					
Install 1 Package					
Total download size: Installed size: 48 M Is this ok [y/d/N]: y Downloading packages: sublime-text-4126-1.x Running transaction c Running transaction t	20 M 86_64.rpm heck est eded	20	MB 00:00		
Running transaction Installing : sublim Verifying : sublim	e-text-4126-1.x86_64 e-text-4126-1.x86_64		1/1 1/1		
Installed: sublime-text.x86_64	0:4126-1				
Complete! [root@ip-10-1-159-180	student]#				

Here is after I installed everything.

Now we can click on the magnifying glass at the bottom of the screen on the desktop and search for **Sublime Text**. Right click on the application logo and click **Add to Bookmarks**. In addition, you can click and drag the application logo to the desktop to create a shortcut. Once you have your shortcuts setup, click the **Launch** button.





In Sublime Text, we need to set up a few things so that we can build and see our code. To do this, we will need to install the **Package Control** and **Buildview**.

• To install the Package Control, press ctrl+shift+p, and then in the search box, type Install Package Control.

package
Package Control: Upgrade Package
Package Control: Advanced Install Package
Package Control: Create Package File
Package Control: Install Local Dependency
Package Control: List Unmanaged Packages
View Package File
Preferences: Package Control Settings – Default
Preferences: Package Control Settings – User
Install Package Control
Preferences: Browse Package s
Package Control: Upgrade/Overwrite All Packages

• To install a package press ctrl+shift+p and click on **Package Control: Install Package**.



• In the package control search box, type buildview.

Now to build our code, we will have to set the build language.

- In the SublimeText editor, type: ##!/usr/bin/env python
- Click the **Tools** menu, select **Build System**, and then check the **Python** box.

oto	Tools	Project	Preferenc	ces	Help		
	Co	mmand Pa	lette		Shift+Ctrl+		
	Sni	ppets					
	B <u>u</u>	ild System	1) Automatic
	<u>B</u> u	ild			Ctrl+I) ActionScript
	Bu	ild With			Shift+Ctrl+I) Ant
PqW	Ca	ncel Build) C Single File
< 01	Bu	ild <u>R</u> esults			I) C++ Single File
5.0	🖌 Sav	ve <u>A</u> ll on B	Build) Cargo
= (ı	Re	cord <u>M</u> acro	þ		Ctrl+Alt+0) D
	Pla	yback Ma	cro	Shift	+Ctrl+Alt+() D dub
base	Sa	<u>v</u> e Macro) Erlang
	Ma	cros			I) Haskell
	De	veloper				· C) JavaC
) Lua
) Make
						☑	9 Python
) R
) Ruby
						\square) Rust
						\square) ShellScript
						\Box) Syntax Tests
							New Build System

4

DA1MTQwLTI3MDAtNDQ4ZC1iMDU0LTBhN2UzN2JjOW	Q4NC85NzM2NTNjNS02N	NzZmLTQ1ZDItYWR 📋	🖻 🖈 🗉 🏟
		23:12	Cyber Range Stud
##!/usr/bin/env python	- Sublime Text (UNRE	GISTERED)	+ _ = ×
He Ealt Selection Find View Goto loois	Project Preferences	нер	+ 🔻
1 ##!/usr/bin/env python			
Line 1, Column 23		Tab Size	: 4 Plain Text

Here is mine after the above steps.

- On the Desktop, create a folder named **natas**.
- In Sublime Text, save your file as **natas0.py** in the natas folder you just created on the Desktop.
- Now we need to exit out of Sublime Text and open it back up.
- To get the split screen, press alt+shift+2.
- Press ctrl+b to build the output.

ND	A1MT	QwLTI3	MDAtNDQ4	ZC1iMI	OUOLTB	N2UzN	I2JjOWQ	4NC85Nz	M2NTNjNS02N	JzZmLTQ [*]	1ZDItYWR	t ¢	☆□	۲
										5	23:	14	Cyber Rang	ge Stude
					Build	outpu	ıt - Subl	ime Text	(UNREGISTER	RED)			• -	
	File	Edit	Selection	Find	View	Goto	Tools	Project	Preferences	Help				
	.			×	Build o	utput	×	+ 🔻	4 ►					+ 🔻
	1								1					
		Line 1,	Column 1								Tat	Size: 4	Plain Te	xt

Here is the end of my task 1.

Task 2: Python Programming Natas 0-1

The goal in the lesson is not to be an expert in Python. The idea is to learn how Python can be used to parse information from a website using simple scripts. Don't focus too much on being a perfect Python programmer. Rather focus on the patterns that you see when programming and parsing information.

• In a browser, navigate to <u>https://overthewire.org/wargames/natas/natas0.html</u>

To the left, you can see all the challenges. They are progressive and will get more difficult as we proceed.

- Copy and paste the link from the page into a new tab in the browser. <u>http://natas0.natas.labs.overthewire.org</u>
- Enter the username natas0 and the password natas0.

IATASO	
	You can find the password for the next level on this page.

• Right click on the page and click View Page Source.

The password can be shown in the page source as a comment. When testing a web application, it is always important to view the source. Sometimes you can find sensitive information that leads to a deeper understanding of the application or its owners.

To prevent error messages, we can create a new python2 build system inside of SublimeText.

- In SublimeText, click Tools -> Build System -> New Build System
- Copy and paste the following code:

```
{
    "cmd": ["python2", "-u", "$file"],
    "file_regex": "^[]*File \"(...*?)\", line ([0-9]*)",
    "selector": "source.python"
}
```


• Click File > Save As and name the file python2.sublime-build. Then click Save.

Here is mine after saving it.

• Click Tools -> Build System -> python2

to	Тоо	ls	Proje	ect	Pref	erenc	es	Help			
	(Con	nman	d Pa	lette		Ctr	l+Shift	+P		
		Snip	opets.								
		Buil	d Sys	tem					•	Automatic	
	F	Buil	d					Ctrl	+B	ActionScript	
	F	Buil	d Wit	.h			Ctrl	l+Shift	+B	🗌 Ant	
s.la	(Can	icel B	uild			C	trl+Bre	ak	🗌 C Single File	
late	F	Buil	d Res	ults					•	C++ Single File	
a c	S :	Sav	e All (on B	uild					Cargo	
(ie:	F	Rec	ord M	acro)		C	trl+Alt-	+Q	□ D	
	P	Play	yback	Ma	cro	Ctrl	+Alt	:+Shift-	+Q	🗌 D dub	
		Sav	e Ma	cro						🗌 Erlang	
(.*)		Mad	cros						•	🗌 Graphviz	
	1	Dev	elope	er					•	🗌 Haskell	
										🗌 JavaC	
										🗌 Lua	
										🗌 Make	
										Perl	
										Python	
										Python2	
										Python3	
										\frown	

• Exit out and restart SublimeText.

From this point on, be sure to pay close attention to the colors in the screenshots. A simple typo can lead to an error and the colors help pinpoint where the line error is. In Sublime Text editor, under the shebang (**#**!), add the following to the natas0.py file (see image below):

```
#!/usr/bin/env python
```

```
import requests
import re
url = 'http://natas0.natas.labs.overthewire.org/'
r = requests.get(url, auth = ('natas0', 'natas0'))
print r.text
```


• Save the code with CTRL+s (you will want to do this frequently).

Python Code Breakdown:

- **import requests** Imports the request module that allows http requests to be made.
- import re Imports the module "Regular expressions" allowing characters such as the backslash ('\') to be used without invoking their special meaning.
- r = requests.get(url, auth = ('natas0', 'natas0')) This sets the variable r to access the get request with authorization using the username and password that we set (username first, then password).
- **print r.text -** prints the results of the variable **r**. In this case, the get request with authorization.
- In the natas0.py tab, press CTRL+b to build the program and output it in a new tab.

The first time you do this, you may have to click and drag the tab to the other side of the split screen to get the results in the screenshot below.

As you can see, the request is now in the build output tab and the next password for natas1 is there.

DgtYWY5NDljNmUxNzFhLzAxN	DA1MTQwLTI3MDAtNDQ4	ZC1iMDU0LTBhN2UzN2J	jOWQ4NC85NzM2NTNjNS0	2NzZmLTQ1ZDItYWR 📋	e 🖈 🗆 🍪
				23:24	Cyber Range Stud
File Edit Selection Find	Build View Goto Tools F	output - Sublime Text Project Preferences	(UNREGISTERED) Help		+ ×
<► natas0.py	× + • •	Build output	×		+ 🔻
<pre>1 #!/usr/bin/env p; 2 import requests 3 import re 4 5 6 url = 'http://na 7 8 r = requests.get 9 10 print r.text 11</pre>	rthon tas0.natas.la (url, auth =	<pre>1 <html> 2 <head> 3 - This stuf 4 <link 11="" 5="" 7="" 9="" <link="" <sbody="" <script="" guery-ui.gss"="" http:="" n="" rel="sty //query-ui.css 6 <link rel=" src="http://n 10 <scriptsvc" sty=""/> 12 <hl>atas0</hl> 13 <div 15="" 17="" <="" conte="" div="" id="conte 14 You can find t 15 16 <lThe passwo>div id="> 18 10 10 10 11 11 11 12 <hl>atas0</hl> 13 <div 14="" 15="" 16="" <lthe="" can="" conte="" find="" id="conte 14 You can find t 15 16 <lThe passwo>div
 10 </body> 10 </body> 11
 11
 12 <hl>atas0</hl> 13 <div id=" passwo="" t="" you="">div 17 10 </div></div></head></html></pre>	<pre>f in the header has no lesheet" type="text/cs atas.labs.overthewire: lesheet" href="http:// /> ttp://natas.labs.overt s> ttp://natas.labs.overt s> tp://n</pre>	thing to do with the 's" org/css/level.css"> matas.labs.overthewir natas.labs.overthewir newire.org/js/ ewire.org/js/ ewire.org/js/ org/js/wechall.js">"natas0", "pass": "n: ext level on this page REhslq8KtcA2uocGHPfM2	Level> e.org/css e.org/css cript> atas0" VzeFK6
Line 16, Column 68				Tab Siz	e: 4 Plain Text

Here is my Task 2 completed.

Task 3: Python Programming Natas 1-2

The next challenge is a bit easier since all we really need to do is change a few parameters to our code.

- In the natas0.py tab, change the url to <u>http://natas1.natas.labs.overthewire.org/</u>
- In the **r** variable, change the username 'natas0' to 'natas1'
- In the **r** variable, change the password 'natas0' to the password discovered in the previous task.
- Using the CTRL+SHIFT+S, save the file as natas1-2.py to the natas folder on your Desktop.
- In the natas1-2.py tab, press CTRL+b to build the program. See the images below.

Here you can see the password after building it out for natas2.

It appears there is a pattern of "<! --the password for natas# is passwordhere -->". Because of this, we can make a few adjustments to the Python code so we don't have to keep looking through the entire html output. Instead, we can use re.findall to search through the html page for this pattern.

- In the natas1-2.py tab, delete print r.text and in its place add print re.findal1('<!-The password for natas2 is (.*) -->', content) [0] (REMINDER: Don't forget to
 save the file every time you make a change.)
- Add the line content = r.text after the r = requests.get... as shown in the screenshot below
- In the natas1-2.py tab, press CTRL+b to build the program.

12

1 2 1ge/#/client/NGY0MTZhYTgttMjYxMy00MDhjUWE4ZDgttWWSNDJJNmUxHzFhL2AvND	Build output ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi [Finished in 0.4s] DAIMTQWLTI3MDAMDQ4ZCIMDU0UTBHN2U2h22jOWQ4NC85N2M2NTNjN502NzZmLTQ1ZDHYWR.	0 e * 0 🔅
~/Desktop/natas/natas	23:3	2 🔒 Cyber Range Stu
-/Desktop/na File Edit Selection Find View Goto Tools Project Preferences	itas/natas1-2.py - Sublime Text (UNREGISTERED) Help	+ . E ×
<pre> heat-Japy * import requests import requests import requests import requests import requests r = requests.get(url, auth = ('natas1', 'g309cREhslqBKtc g content = r.text lo print re.findall('<1The password for natas2 is (.*) r </pre>	EAZuucGHPfMZVzeFK6:))	
Line 10, Column 73	Tab	Size: 4 Python

Here is my password for natas2.

• To complete this task on the site, you simply use the username and password from natas1 at http://natas1.natas.labs.overthewire.org then right click outside of the container to view the source.

You can find rightclicking	You can find the password for the next level on this page, but rightclicking has been blocked!						
	right clicking has been blocked!						
	ОК						

13

Here is after logging into natas1 with my found password.

<html>

- chtml>
 chead>
 clink rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
 clink rel="stylesheet" href="http://natas.labs.overthewire.org/js/jouery-u.j.l.js">
 clink rel="stylesheet" href="http://natas.labs.overthewire.org/js/wechall.css" />
 cscript src="http://natas.labs.overthewire.org/js/wechall.js"</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</cscript</csc

- <div id="content">
 You can find the password for the next level on this page.
- <!--The password for natas1 is gtVrDuiDfck831PqWsLEZy5gyDz1clto --> </div>

- </body> </html>

e.virginiacyberrange.net/range/#/clie	nt/NGY0MTZhYTgtMjYxMy00MDhjL\	VE4ZDgtYWY5NDljNmUxNzFhLzAxN	DA1MTQwLTI3MDAtNDQ4ZC1iMDU	JOLTBhN2UzN2JjOWQ4NC85	NzM2NTNjN		ZmLTQ1	ZDItY
://natas1.natas.labs 🗾 ~/Deskt	cop/natas/natas						6	
6	http:	//natas1.natas.labs.overthewire.c	org/ - Mozilla Firefox				• •	• ×
M OverTheWire: Natas Leve 🗙	natas1.natas.labs.overthew 🛛 🗙	http://natas1.natas.labs.over ×	http://natas0.natas.labs.over 🗙	💩 New Tab	× +			
↔ → ♂ ŵ	(i) view-source:http://natas1.	natas.labs.overthewire.org/		⊚ ☆		111\ C	0 🔮	Ξ
<pre>chead- 3 <!-- This stuff in the head<br--><link rel="stylesheet" typ<br=""/><link her<br="" rel="stylesheet"/><link her<br="" rel="stylesheet"/><link her<br="" rel="stylesheet"/>chick rel="stylesheet" her cscript src="http://natas.] <script src="http://natas.]<br"><script src=http://natas.] <script src=http://natas.] <div do "contextmenu="javas" <div do "contextmenu="javas" </div do "contextmenu="javas" </di></th><td><pre>wder has nothing to do with the l pe="text/css" href="http://natas. ff="http://natas.labs.overthewire off="http://natas.labs.overthewire inf="http://natas.labs.overthewire info"-http://natas.labs.overthewire. labs.overthewire.org/js/wechall-c labs.overthewire.org/js/wechall-c { "level": "natasl", "pass": "gi ccript:alert('right clicking has for the put rightclicking has been blocked is h4ubbcXrWqsTo7GGnnUMLppXb0c</pre></td><td>evel> labs.overthewire.org/css/level.c .org/css/iquery-ui.css" /> .org/css/vechall.css" /> .g.l.js"></script> ata.js> ata.js>src="htt DScREhslqBMtCA2uocGHPfMZVzeFK6" been blocked!');return false;"> d! gfBZ7><td><u>ss</u>"> <u>p://natas.labs.overthewire.org/j</u> };</td><th>i<u>s/wechall.js</u>"≻</th><td></td><th></th><th></th><td></td></pre>	<u>ss</u> "> <u>p://natas.labs.overthewire.org/j</u> };	i <u>s/wechall.js</u> "≻						

I found it using the shortcut ctrl+u. Right clicking did not work for me.

Task 4: Python Programming Natas 2-3

Visit <u>http://natas2.natas.labs.overthewire.org/</u> for the next challenge and use the username natas2 and the password retrieved from the previous task.

- orrangounce - oronanis roomen - ornani - orrang record - ornanis - orang	ubbi encerna Eliteritaria incerna Eleadiana Eliteritaria en encer Eleadore en encer Eleadore
NATAS2	
	There is nothing on this page

• Right click on the page and view the source code

1 chtnl>
2 Sileau
3 This stuff in the header has nothing to do with the level
<pre>4 <link href="<u>http://natas.labs.overthewire.org/css/level.css</u>" rel="stylesheet" type="text/css"/></pre>
5 <link href="<u>http://natas.labs.overthewire.org/css/jquery-ui.css</u>" rel="stylesheet"/>
<pre>6 <link href="<u>http://natas.labs.overthewire.org/css/wechall.css</u>" rel="stylesheet"/></pre>
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="<u>http://natas.labs.overthewire.org/js/jquery-ui.js</u>"></script>
<pre>9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>>>>></pre>
<pre>10 <script>var wechallinfo = { "level": "natas2", "pass": "ZluruAthQk7Q2MqmDeTiUij2ZVWy2mBi" };</script></pre>
11 <body></body>
12 <h1>natas2</h1>
13 <div id="content"></div>
14 There is nothing on this page
15
16
17

It appears that nothing is there. Let's check this out in the Python code. First we need to make a few changes. Since the pattern is no longer there we need to take this out for now. We also need to add a new print function.

- Change all locations where you have natas1 to natas2.
- Delete the print re.findall('<!--The password for natas2 is (.*) -->', content) [0]
- Add **print content** to call the variable content.

• Save this file as natas2-3.py and then build the output.

Notice the img src location. It appears to be in a directory called **files**.

	4 ►	Build output ×
1	1	<html></html>
		<head></head>
		This stuff in the header has nothing to do with the level
		
		<pre><link href="http://natas.labs.overthewire.org/css/jquery-ui.css" rel="stylesheet"/></pre>
		<pre><link href="http://natas.labs.overthewire.org/css/wechall.css" rel="stylesheet"/></pre>
		<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
		<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
		<script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script> <script< th=""></script<>
		<pre>src="http://natas.labs.overthewire.org/js/wechall.js"></pre>
		<pre><script>var wechallinfo = { "level": "natas2", "pass": "ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi"</pre></th></tr><tr><th></th><th></th><th>};</script></pre>
		<body></body>
		<h1>natas2</h1>
		<div id="content"></div>
		There is nothing on this page
		
	19	[Finished in 0.3s]
- 1		

• Change the url in the natas2-3 tab to match the img src location by appending the url with /files/.

It appears that we are able to navigate to the files folder. Note: if your build output loses its format coloring, use CTRL+SHIFT+P and search for **Set Syntax**: **HTML**. **IMPORTANT**: Be sure to complete this in the Build output tab.

16

KISES

This is hard to read. Let's install a package that will organize this code a little better.

- In the build output tab, press CTRL+SHIFT+P and type install package and click Package Control: Install Package then search for HTMLBeautify and click on it to install.
- In the build output tab, press CTRL+SHIFT+P and type HTMLBeautify and click on it

naco		
1	install	
Ine	Package Control: Install Package	
ιÞο	Package Control: Install Local Dependency	
.mn	Package Control: Advanced Install Package	
	Selection: Select All	Ctrl+A

htmlb

HTMLBeautify

A plugin for Sublime Text that formats (indents) HTML source code. It makes code easier for humans install v2018.03.01.21.41.57; github.com/rareyman/HTMLBeautify

[html	
HTML Beautify	Ctrl+Alt+Shift+F
HTML Prettify	Ctrl+Shift+H
HTML: Encode Special Characters	
HTMLPrettify: Set Keyboard Shortcuts	Ctrl+Alt+H, k
HTMLPrettify: Set Plugin Options	Ctrl+Alt+H, o

<pre></pre>				
<pre>clocrype HTML PUBLIC *-//W3C//DTD HTML 3.2 Final//EN'> clocrype HTML 3.</pre>	A >	Build output ×		
<pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre>	↓ <p< th=""><th>Build output x <!DOCTYPE HTML PUBLIC "-//W3C//DTD <html> <head> <title>Index of /files</title></head> <tobdy> <hl>Index of /files</hl> <1 href="?C=N;0=D">Nameth>Nameth><a <th="" href="2;0=N;0=Name</a
th>
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<th valign=" top"<th="" valign="</th><th>HTML 3.2 Final//EN"> <pre> ile> mg src="/icons/blank.gif" alt="[ICO]"> ile> /th><a>/th>>= /th>>= "?C=M;0=A">Last modified /th>> /th>> /th>> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> <th>< /</th></pre></tobdy></html></th></p<>	Build output x HTML PUBLIC "-//W3C//DTD<br <html> <head> <title>Index of /files</title></head> <tobdy> <hl>Index of /files</hl> <1 href="?C=N;0=D">Nameth>Nameth><a <th="" href="2;0=N;0=Name</a
th>
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<1
<th valign=" top"<th="" valign="</th><th>HTML 3.2 Final//EN"> <pre> ile> mg src="/icons/blank.gif" alt="[ICO]"> ile> /th><a>/th>>= /th>>= "?C=M;0=A">Last modified /th>> /th>> /th>> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> /th> <th>< /</th></pre></tobdy></html>	< /	
OverTheWite: Name File Edit Selection File File Edit Selection File File Edit Selection File Fi	13 14 15 16 17 18 giniacyberrange.net/range/#/client/NGYOMT2h/TigHM tas2.natas.labs 1 Build output - Sublime	<pre>>303</pre>	<pre></pre>	d 0
Overtmetwire. Nata • Control will ward and a start of the selection find View Goto Tools Project Preferences Help • Overtmetwire. Nata • Overtmetwire. Nata <td< th=""><th></th><th>Build output - Sublime Te:</th><th>ct (UNREGISTERED)</th><th></th></td<>		Build output - Sublime Te:	ct (UNREGISTERED)	
Control of the state of the	OverTheWire: Natas File Edit Selection Fir	nd View Goto Tools Project Preferences Help		
Tab Size: 4 HTML	 → C û I motsula py I d'//usr/Vin/env Import request Import request	<pre>python atas2.natas.labs.overthewire.org/files/' sturt, auth = ('natas2', 'h4ubbcXrWqsTo76GnnUME.pp) t</pre>	Outstand x cloctrye (FMR Public *-//WSC//OTD HTML 3.2 Final//EM*> cloctrye (FMR Public *-//WSC//OTD HTML 3.2 Final/PEM*> cloctrye (FMR Public *-//WSC//OTD HTML 3.2 Final/PEM*> cloctrye cloctrye <t< th=""><th></th></t<>	
	Line 7, Column 19		Tab Size: 4 HTML	

Here is after I used htmlbeautify.

This will have to do for now. Take notice of the **href="users.txt."** This looks interesting. Let's visit this location using our code.

- In the natas2-3.py tab, change the url to match http://natas2.natas.labs.overthewire.org/files/users.txt
- Save the file and then build the program.

There you have it, the next password for natas3.

Joshua Lane CYSE450 Section 23190 10/26/2022

Here is the password for natas3.

Task 5: Python Programming Natas 3-4

As completed in previous tasks, we want to change the Python code to match our new parameters.

• Take a look at the screenshot to check if you have all the parameters correct.

• Save the file as natas3-4.py and then build the program to look at the response.

I am not liking this color scheme as it is hard on the eyes. Let's use the package controller to install a better color scheme.

- Press CTRL+SHIFT+P and type Package Control: Install Package
- Click Package Control: Install Package
- Type Dark Neon Color Scheme and click the scheme.

tput	A V Build Output
	dark
ilS el	Darkula Color Scheme
ss	IntelliJ Darkula Sublime Text / TextMate Color Scheme
el	install v2019.09.20.07.17.25; packagecontrol.io/packages/Darkula%20Color%20Scheme
S	Dark Fusion Color Scheme
. s : s	Port of Atom's Dark Fusion Syntax
'na >v	install v1.5.0; github.com/willsoto/dark-fusion-syntax
JN	Dark Knight Color Scheme
	😍 An elegant dark color scheme for Sublime Text 🗲 .
as ="	install v0.1.4; packagecontrol.io/packages/Dark%20Knight%20Color%20Scheme
.s . m	Dark Neon Color Scheme
	Dark Neon theme for Sublime Text, Mou, & Others
· </th <th>install v2016.02.11.19.59.23; github.com/RainyDayMedia/DarkNeon</th>	install v2016.02.11.19.59.23; github.com/RainyDayMedia/DarkNeon
ed	Dark Pastel Color Scheme
	Dark pastel-colored Sublime Text / TextMate Color Scheme

- Press CTRL+SHIFT+P and type UI: Select Color Scheme and click the result.
- Click on Dark Neon (or the color scheme that you prefer).

Now let's look at the Build output.

►	Build output × Build output ×
	<html> <head></head></html>
	This stuff in the header has nothing to do with the level
	<pre><link href="http://natas.labs.overthewire.org/css/
level.css" rel="stylesheet" type="text/css"/></pre>
	<pre><link href="http://natas.labs.overthewire.org/css/jquery-ui.css" rel="stylesheet"/></pre>
	<link href="http://natas.labs.overthewire.org/css/wechall.css" rel="stylesheet"/>
	<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
	<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
	<pre><script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script src</pre></th></tr><tr><th></th><th>http://natas.labs.overthewire.org/js/wechall.js"></script></pre>
10	<script>var wechallinfo = { "level": "natas3", "pass": "</th></tr><tr><th></th><th>sJIJNW6ucpu6HPZIZAchaDtwd7oGrD14" };</script>
11	 body>
12	<hl>natas3</hl>
13	<pre><div_id="content"></div_id="content"></pre>
14	There is nothing on this page
15	No more information leaks!! Not even Google will find it this time
16	
17	
18	
19	_[Finished in 1.4s]

I am not a fan of the inefficiencies of moving to the browser to complete the challenges. I will show some screenshots, but will not be walking through the browser method; however, at this point, you should be able to test these on your own if you are interested. Here is what it looks like on the webpage.

1 <html>
2 <head>
3 </-- Nis stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jeuery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jeuery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jeuery-ui.css" />
7 <script src="http://natas.labs.overthewire.org/js/jeuery-ui.js"></script src="http://natas.labs.overthewire.org/css/jeuery-ui.css" />
8 <script src="http://natas.labs.overthewire.org/js/jeuery-ui.js"></script src="http://natas.labs.overthewire.org/js/jeuery-ui.js"</script>
8 <script src="http://natas.labs.overthewire.org/js/jeuery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/jeuery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/jeuery-ui.js"</script>
9 <script src="http://natas.labs.overthewire.org/js/jeuery-ui.js"</script>
10 <script src=http://natas.labs.overthewire.org/js/wechall.js"</script>2/script>
10 <script src=http://natas.labs.overthewire.org/js/wechall.js"</script>
11 <script src=http://natas.labs.overthewire.org/js/wechall.js"</script>
12 <script src=http://natas.labs.overthewire.org/js/wechall.js"</script>
12 <script src=http://natas.labs.overthewire.org/js/wechall.js"</pre>
12 <script src=http://natas.labs.overthewire.org/js/wechall.js"</pre>
12 <script src=http://natas.labs.overthewire.org/js/wechall.js"</pre>
13 <script src=http://natas.labs.overthewire.org/js/wechall.script</pre>
13 <</pre>
14
14
14
15
15
15
15
15
16 <</pre>
16
17
17
17
17
17
17
17
17
17
18
18
19
19
19
19
19
19
19
19
19
19
19
19
19
19
19
19
19
19
19
19 </

This hint should be easy to understand. If Google is not allowed to spider an application, this is defined in the robots.txt file. We covered this in earlier lessons. So, we should check to see if the page has a robot.txt file. From this point forward, **build the output** will mean you need to **press CTRL+B**.

• In the natas3-4.py file, append the url with /robots.txt, save the file, and then build the output.

There seems to be a file that is not allowed to be crawled. Let's navigate to the location in our Python script.

• Change the url to http://natas3.natas.labs.overthewire.org/s3cr3t, save the file, and then build the output.

There appears to be another users.txt file. Let's navigate to this location in our Python script.

Here is mine showing the new users.txt file.

• Change the url to http://natas3.natas.labs.overthewire.org/s3cr3t/users.txt, save the file, and then build the output.

$\mathbf{H}_{\mathbf{U}}$ we have the passion of that $\mathbf{u}_{\mathbf{U}}$ as $\mathbf{H}_{\mathbf{U}}$ as $\mathbf{H}_{\mathbf{U}}$

	~/Des	ctop/natas/natas							23:56	Cyber Range Stud
atas I	File	Edit Selection	Find View Goto	~/Desktop/na Tools Project Preferences	tas/natas3-4.py - Sub Help	lime Te	ext (UNREGISTERED)			+ - = ×
	↓ 1 2 3 4 5 6 7 8 9 10	natas3-4.py env python ests ://natas3.nat s.get(url, au .text nt	× tas.labs.overthewin uth = ('natas3', '(re.org/s3cr3t/users.txt' 66ctbMJ5Nb4cbFwhpMPSvxGHhQ	+ v	4► 1 2 3	Build output × natas4:tKOcJIbzM4lTs8h [Finished in 368ms]	bCmzn5Zr4434fGZQm		+ •

Here is the end of task 5.

Here is after I logged into the natas4 webpage.

Task 6: Python Programming Natas 4-5

As completed in previous tasks we want to change the Python code to match our new parameters.

• Using the CTRL+SHIFT+S, save the file as natas4-5.py and then build the output.

This looks like a header issue. We know this because the site is referring to us visiting from "" which is null. This means we are missing a referrer in our header. We could fire up BurpSuite and capture the request and then change the header; however, this is not very efficient and we are already set up in

Python. According to <u>https://2.python-requests.org/en/master/user/quickstart/#custom-headers</u> we can just add a header request into our script.

source:https://2.python-requests.org/en/master/user/quickstart/#custom-headers

We need a referer header and it needs to come from the specified location.

- In the natas4-5.py file, add headers = { 'Referer' :
 'http://natas5.natas.labs.overthewire.org/'} as show in the screenshot below.
- Next, add , **headers** = **headers** inside the parentheses as show in the screenshot below, save the file, then build the output.

Here are my above steps completed with changing the code in the script and building it out to show the password for natas5.

Let's narrow this script down even more.

- In the natas4-5.py file, comment out print content by adding # before it. This means when we build the output, this command will be ignored.
- Add print re.findall('The password for natas5 is (.*)', content) [0] below this comment. See image below.
- Save the script as **natas5-6.py** and then build the output.

And there we have it! The password for natas5.

ZONsrtIkJoKALBCLi5eqFfcRN82Au2oD is the password.

Task 7: Python Programming Natas 5-6

As completed in previous tasks, we want to change the Python code to match our new parameters. We also want to comment out the line 16 the print re.findal1... and the headers on line 6. We then want to delete the # (comment) on the print content. We want to add a) # on line 10. There are a lot of changes in this script, so they are shown in the red boxes in the screenshot below. The # is called commenting out and can be used for quick changes in the code. Make sure you save the file after making all the edits.

Build the output.

∢ ►	Build output × Build output ×
1	<html></html>
	<head></head>
	This stuff in the header has nothing to do with the level
	<pre><link href="http://natas.labs.overthewire.org/css/</pre></th></tr><tr><th></th><th>level.css" rel="stylesheet" type="text/css"/></pre>
	<pre><link href="http://natas.labs.overthewire.org/css/jquery-ui.css" rel="stylesheet"/></pre>
	<pre><link href="http://natas.labs.overthewire.org/css/wechall.css" rel="stylesheet"/></pre>
	<pre><script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script></pre>
	<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
	<pre><script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="</pre></th></tr><tr><th></th><th>http://natas.labs.overthewire.org/js/wechall.js"></script></pre>
10	<script>var wechallinfo = { "level": "natas5", "pass": "</th></tr><tr><th></th><th>iX6I0fmpN7AY0QGPwtn3fXpbaJVJcHfq" };</script>
11	<body></body>
12	<hl>natas5</hl>
13	<pre><div id="content"></div></pre>
14	Access disallowed. You are not logged in
15	
16	
17	
18	[Finished in 0.4s]

nge/#/client/N					🗆 🌍
				01:12 🔒 Cyber	Range Stu
File Edit	-/Desktop/natas/natas/6.py - Sublime Text : Selection Find View Goto Tools Project Preferences Help 255-6.py ×	(UNREGISTERE + ▼ ◀)	ED) ▶ Build output × Build	ld output ×	× + •
1 P 2 Im 3 Im 6 Ur 7 P 9 cc 10 pr 11 P 12 #5	<pre>instribution python port requests port requests port re enders = ('Referen' : 'http://natas5.natas.labs.overthewire.org') ' = 'http://natas5.natas.labs.overthewire.org' = requests.get(url, auth = ('natas5', 'ZONsrtikJoKALBCLiSeqFfcRN02Au200'))}; ntent = r.text int content arint re.findall('The password for natas5 is ('*)', content) [0]</pre>		<pre>1 defails 2 defails 3 class This stuff in the 1 with the level ->> 4 clink rel*stylesheet ' i/nata.labs.overthewire. 7 natas.labs.overthewire. 7 natas.labs.overthewire. 7 natas.labs.overthewire. 9 cscript scripts/relife 9 cscript scripts/neutrolife 9 cscripts/neutrolife 9 cscripts</pre>	<pre>weader has nothing to do type="text/css" href="http rere"http:// org/css/jayer/val.css" /> org/css/jayer/val.css" /> org/css/wethall.css" /> org/css/wethall.css" /> so.labs.overthewire.org/js/ bescript "css"http:// org/js/wethall.js">/>css ibab.overthewire.org/js/ bescript "css"http:// org/js/wethall.js">/>css ibab.overthewire.org/js/ bescript "css"http:// org/js/wethall.js">/>css ibab.overthewire.org/js/ bescript "css"http:// org/js/wethall.js">/>css ibab.overthewire.org/js/ bescript "css"http:// org/js/wethall.js">/>css ibab.overthewire.org/js/ bescript "css ibac.overthewire.org/js/ org/js/wethall.js">/>css ibab.overthewire.org/js/ org/js/wethall.js">/>css ibab.overthewire.org/js/ org/js/wethall.js">/>css ibab.overthewire.org/js/ org/js/wethall.js">/>css ibab.overthewire.org/js/ org/js/wethall.js">/>css ibab.overthewire.org/js/ org/js/wethall.js">/>css ibab.overthewire.org/js/ org/js/wethall.js">/>css ibab.overthewire.org/js/ org/js/wethall.js">/>css ibab.overthewire.org/js/ org/js/wethall.js">/>css ibab.overthewire.org/js/ org/js/wethall.js">/>css ibab.overthewire.org/js/ org/js/wethall.js">/>css ibab.overthewire.org/js/ org/js/wethall.js">/>css ibab.overthewire.org/js/ org/js/wethall.js">/>css ibab.overthewire.org/js/ org/js/wethall.js">/>s<!--/-->//overjs/ ibab.overthewire.org/js/ org/js/wethall.js">/>s<!--/-->//>s<!--/-->//>css</pre>	

Here is after I built the output and it said access disallowed.

According to the output, we do not have access to the page. This means that the page is using cookies. Again we could use Burp Suite to capture a request and look at the cookies; however, we can do a quick check with **r**.cookies. Take a look at this site for more details on writing Python code and cookies: https://2.python-requests.org/en/master/user/quickstart/#cookies

• In the natas5-6.py file, add print (r.cookies), save the file, and then build the output. See image below.

	http://natas.labs.overthewire.org/js/wechall.js">
10	<script>var wechallinfo = { "level": "natas5", "pass": "</td></tr><tr><td></td><td>iX6I0fmpN7AY00GPwtn3fXpbaJVJcHfq" };</script>
11	<body></body>
12	<h1>natas5</h1>
13	<div id="content"></div>
14	Access disallowed. You are not logged in
15	
16	
17	
18	<pre><<class 'requests.cookies.requestscookiejar'="">[<cookie fpr<="" loggedin="0" pre=""></cookie></class></pre>
	<pre>natas5.natas.labs.overthewire.org/>]></pre>
19	[Finished in 0.3s]

It appears that the cookie name is **loggedin** and it currently **=0**. It looks like all we need to do is add a cookie named **loggedin** and set the value to **1**. In the natas5-6.py file, do the following:

- Comment out **print (r.cookies)**.
- Add cookies = { 'loggedin' : '1' } under the url.
- Edit the **r** = **requests.get** function call by adding in **cookies**=**cookies** after url, and **exactly** as shown in the below image.
- Add **r**.cookies = ['loggedin'] under **r** = **requests.get**... line 13 in the image below.
- Comment out **print content**.
- Uncomment the print re.findall line and change natas5 to natas6.
- add </div> after the (/*) in the print function
- Save the file and then build the output.

There we have it, the level six password.

nge/#/clie	ent/NGY0MTZhYTgtMjYxMy00MDhjLWE4ZDgtYWY5NDljNmUxNzFhLzAxNDA1MTQwLTI3MDAtNDQ4	ZC1iMDU0LTBhN2U	JzN2JjC	WQ4NC85NzM2NTNjN	IS02NzZmLTQ1ZDItYV	VR 🛍	re 🖈 🗖 🍪
						01:16	Cyber Range Stu
	Build output - Sublime Text	(UNREGISTERED)					+ _ E X
File	Edit Selection Find View Goto Tools Project Preferences Help						
4 ►	natas5-6.py ×		4		× Build output	×	
1 2 3 4 5 6 7 8 9 10 11 12 13	<pre>#!/usr/bin/env python import requests import re #headers = {'Referer' : 'http://natas5.natas.labs.overthewire.org/' url = 'http://natas5.natas.labs.overthewire.org' cookies = {'loggedin' : '1'} r = requests.get(url, cookies=cookies, auth = ('natas5', 'Z9NsrtIkJoKALBCLI' r.cookies = ['loggedin'] content = r.text #print (r.cookies) print re.findalL('The password for natas6 is (.*)', content) [0]</pre>	SeqF	1 2	fOIvEOMDTPTgRhqm (Finished in 352	mvvAOt2EfXR6uOgR ms]		

Here it is built out to show the next password.

fOIvE0MDtPTgRhqmmvvAOt2EfXR6uQgR is the password I got for natas6.

In this lesson, we learned how to set up and use Sublime Text, and how to use Python to parse information from a web application. In the process, we gained access to a site by changing the referrer and we also discovered a cookie session name and modified the cookie to gain access.

