# Lab 13: HTML smuggling

# Table of Contents

	1
Goals	1
Requirements	1
Instructions	1

## Goals

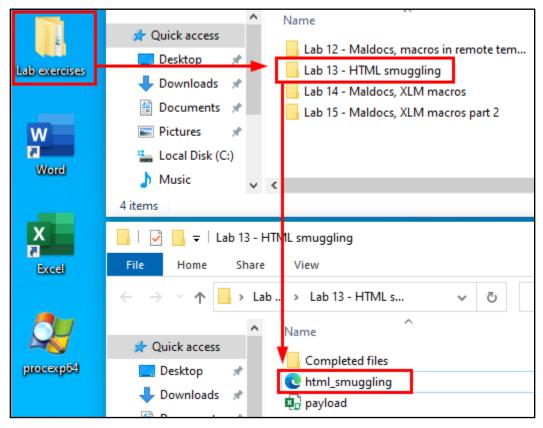
• Embed a payload file inside of an HTML document.

### Requirements

Windows 10 VM

### Instructions

1. In your Windows 10 VM, open the Lab 13 subfolder inside the Lab Exercises folder on your desktop. You should see the "html\_smuggling.html" file inside.



Location of "html\_smuggling.html"

2. Right click on "html\_smuggling.html", and in the menu that appears, click "Open with" and then "Choose another app".

Name		Date modified	Туре	Siz
Completed files		3/25/2021 3:38 PM	File folder	
C html_smuggling		0/00/0001 5.51 DM	Microsoft Edge H	
🖳 payload 🛛 😽	Open		Microsoft Excel M	
	Run as administrat	or		
6	Share with Skype			
	Scan with Microso	ft Defender		
E	Share Share			
2	Open with	>	<i>e</i> Internet Explorer	
	Give access to	>	💽 Microsoft Edge	
	Restore previous vo	ersions	Search the Micros	oft Store
	Send to	>	3 Choose another a	рр

Open with Another App

3. Click "More apps" near the bottom of the window that appears. Then find "Notepad" in the list and double-click on it.

r

[]	How do you want to open this file?				
How do you want to open this file?	Keep using this app				
Keep using this app	Microsoft Edge Do more online with the new browser from Microsoft.				
Microsoft Edge Do more online with the new browser from Microsoft.	Other options				
Other options	Internet Explorer				
Internet Explorer	Look for an app in the Microsoft Store				
Look for an app in the Microsoft Store	Notepad				
More apps $\downarrow$	Paint				
Always use this app to open html files	Windows Media Player				
Always use this app to open .html files	Always use this app to open .html files				
ОК	ОК				

Open with Notepad

-

4. In the Notepad window, find the line in the file that says "<< PASTE BASE64-ENCODED FILE HERE >>". Your Base64-encoded payload file will replace this line in the next steps.

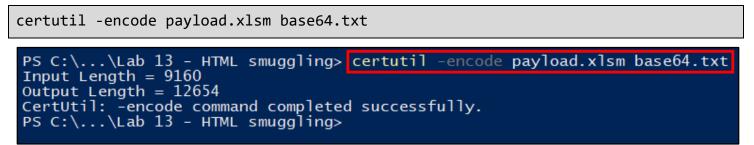
Line to be Replaced

5. To generate the Base64-encoded file, first open a PowerShell window by holding the Shift key on your keyboard and simultaneously right-clicking the white background of the "Lab 13 - HTML smuggling" folder. Then choose "Open PowerShell window here" from the menu.

📙   🛃 📑 🖬 🖛   Lab 13 -	HTML smuggling		
File Home Share	e View		
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\square$ > La	ab exercises > Lab 13 - HTML	smuggling > 🗸 친	, <u>,</u> , ,
🖈 Quick access	Name	^	
	Completed files	View	>
🔜 Desktop 📌	tml_smuggling	S <u>o</u> rt by	>
🕂 Downloads 🖈	🔊 payload	Grou <u>p</u> by	>
🔮 Documents 🛛 🖈		R <u>e</u> fresh	
📰 Pictures 🛛 🖈		Customize this <u>f</u> older	
🏪 Local Disk (C:)			
👌 Music		<u>P</u> aste	
🐺 Videos		Paste <u>s</u> hortcut	~ · · -
OneDrive	2	<u>U</u> ndo Delete Open Power <u>S</u> hell window here	Ctrl+Z
This PC		<u>G</u> ive access to	>
💣 Network		Ne <u>w</u>	>
		P <u>r</u> operties	
		}	
	<		

Open PowerShell Here

6. In the PowerShell window, run the command below to generate a Base64-encoded version of the "payload.xlsm" file.



Base64 Encode "payload.xlsm"

7. If you look in the Lab 13 folder, you should now see the file "base64.txt" listed there. Double-click on the Base64.txt file to open it in Notepad. Then select and copy all of the text in the file.

base	64 - Notepad			🧾 Ь	ase64	- Notepad		
File Edi	t Format View Hel	р		File	Edit	Format View	Help	
	Undo	Ctrl+Z		gEI)	$\mathcal{T}$	Undo	Ctrl+Z	JGNsfM
UEs[ bCCi	Cut	Ctrl+X	-14A 14A	LEd/ sg11		Cut	Ctrl+X	-/X/uxF pg/aPs
AAA/	Сору	Ctrl+C	144	qcB∖	<u>г</u>	Сору	Ctrl+C	90X1oU
AAA/	Paste	Ctrl+V	444	Ai04	1	Paste	Ctrl+V	АВМААА
AAA/ AAA/	Delete	Del	14A 14A	ZW50 AAA/		Delete	Del	CAAAAC 5wECLQ
	Search with Bing	Ctrl+E	444	CQA4		Search with Bing	Ctrl+E	129ya2
AAA/	Find	Ctrl+F	444	AAAł		Find	Ctrl+F	AAAAAA
	Find Next	F3	14A 14A	b29r AAA/		Find Next	F3	4AAhAL L3NoZW
	Find Previous	Shift+F3	144	ACE4		Find Previous	Shift+F3	
AAA/	Replace	Ctrl+H	144	aGVI		Replace	Ctrl+H	AMEXEL
Rfd]	Go To	Ctrl+G	1/	AAA/ AABS		Go To	Ctrl+G	oWxQSw
WqOl idE/	Select All	Ctrl+A	-Coz 18D			Select All	Ctrl+A	-∍Gwvc3 ∆AAAAA
/d45	Time/Date	F5	Ju4	Lnht		Time/Date	F5	oQEAAJ
JigJxYyH+MZNssFazT5dWCZcW9HzIpILgyW AABkbZNQcm9Wcy9hcHAueG1sUEsFBgAA							адаакаа	
r8+pyP	]r2If5nX0B0xXU1/	Jz10tX10q	AdGJ		-END	) CERTIFICAT	E	

Copy All Contents in Base64.txt

8. Now replace the "<< PASTE BASE64-ENCODED FILE HERE >>" line in the "html\_smuggling.html" with the Base64encoded data that you just copied.

**NOTE:** Normally you would want to remove the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines from the Base64 output, as well as removing all the line breaks. However, to keep this exercise user-friendly, the

"html\_smuggling.html" template file has been modified to account for the difference. Just be aware of this difference when dealing with other tools that accept Base64 data on your own in the real world.

```
html_smuggling - Notepad
File Edit Format View Help
}
/* certutil -encode "MALICIOUS FILE.docx" base64.txt */
var file = hereDoc(function() {/*!
<< PASTE BASE64-ENCODED FILE HERE
                                                  Undo
*/});
                                                  Cut
/* Handle output encoded with certut
                                                  Copy
file = file.replace('----END CERTIF
file = file.replace('----BEGIN CERT
                                                  Paste
file = file.replace('\r','');
file = file.replace('\n','');
file = file.replace('\t','');
                                                  Delete
                                                  Select All
```

Paste the Base64 Data Here

<pre>mtml_smuggling-Notepad -</pre>	
<pre>return f.toString().     replace(/^[^\]+\/\*!?/, '').     replace(/^[^\]+\/\*!?/, '');     replace(/\*\/[^\]+\$/, ''); } /* certutil -encode "MALICIOUS FILE.docx" base64.txt */ var file = hereDoc(function() {/*!BEGIN CERTIFICATE UEsDBBQABgAIAAAIQAf7j+FbQEAAFkEAAATAAgCW0NvbnRlbnRfVHlwZXNdLnht bCCiBAIooAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>	$\times$
<pre>replace(/^[^\/]+\/\*!?/, ''). replace(/\*\/[^\/]+\$/, ''); } /* certutil -encode "MALICIOUS FILE.docx" base64.txt */ var file = hereDoc(function() {/*!BEGIN CERTIFICATE UEsDBBQABgAIAAAAIQAF7j+FbQEAAFkEAAATAAgCW0NvbnRlbnRfVHlwZXNdLnht bCCiBAIooAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>	
replace(//*//[^//]+\$/, ''); } /* certutil -encode "MALICIOUS FILE.docx" base64.txt */ var file = hereDoc(function() {/*! BEGIN CERTIFICATE UEsDBBQABgAIAAAAIQAF7j+FbQEAAFkEAAATAAgCW0NvbnRlbnRfVHlwZXNdLnht bCCiBAIooAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
<pre>} /* certutil -encode "MALICIOUS FILE.docx" base64.txt */ var file = hereDoc(function() {/*!BEGIN CERTIFICATE UEsDBBQABgAIAAAAIQAf7j+FbQEAAFkEAAATAAgCW0NvbnRlbnRfVHlwZXNdLnht bCCiBAIooAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>	
<pre>var file = hereDoc(function() {/*!BEGIN CERTIFICATE UEsDBBQABgAIAAAAIQAf7j+FbQEAAFkEAAATAAgCW0NvbnRlbnRfVHlwZXNdLnht bCCiBAIooAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>	
<pre>var file = hereDoc(function() {/*!BEGIN CERTIFICATE UEsDBBQABgAIAAAAIQAf7j+FbQEAAFkEAAATAAgCW0NvbnRlbnRfVHlwZXNdLnht bCCiBAIooAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>	
<pre>var file = hereDoc(function() {/*!BEGIN CERTIFICATE UEsDBBQABgAIAAAAIQAf7j+FbQEAAFkEAAATAAgCW0NvbnRlbnRfVHlwZXNdLnht bCCiBAIooAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA</pre>	
UEsDBBQABgAIAAAAIQAf7j+FbQEAAFkEAAATAAgCW0NvbnRlbnRfVHlwZXNdLnht bCCiBAIooAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
UEsDBBQABgAIAAAAIQAf7j+FbQEAAFkEAAATAAgCW0NvbnRlbnRfVHlwZXNdLnht bCCiBAIooAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
bCCiBAIooAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
bCCiBAIooAACAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
	>

"html\_smuggling.html" After Adding Base64-Encoded Data

9. After pasting in the Base64 data, scroll to the bottom of the "html\_smuggling.html" file, and find the line that says "/\* Change the downloaded filename below \*/". Then change the value of the "fileName" variable under this line to a filename with a ".xlsm" extension. (This is the filename that your payload file will be saved as when it is downloaded by the target, so it should have the same extension as the original payload file.) The filename I'm using for this example is "Invoice.xlsm".

Invoice.xlsm

\*html\_smuggling - Notepad
File Edit Format View Help
var data = base64ToArrayBuffer(file);
var blob = new Blob([data], {type: 'octet/stream'});
/\* Change the downloaded filename below \*/
var fileName = 'Invoice.xlsm';

Totally Legit-Looking Filename Goes Here

- 10. Save your changes to the "html\_smuggling.html" file when they are complete, and close the open Notepad windows.
- 11. Now double-click on the "html\_smuggling.html" file to open the file in a web browser and observe how the embedded payload is automatically downloaded when the HTML file is opened.

ß	html_smugg	gling.ht	tml × +			-		×
$\leftarrow$	$\rightarrow$	С	ြဲ File   C:/Users/VMuser/Desktop/Lab%20exerci ငို့	ŏ	ଽ∕≡	Ē		
		_						
<b>8</b> 6	Invoice.xlsr <u>Open file</u>	m				S	show all	$\times$

Invoice.xlsm Automatically Downloaded When "html\_smuggling.html" is Opened

12. Open the downloaded file to confirm that it was correctly decoded from the Base64 data you created and that it executes successfully.

Auto	Save 💽 Of	f) »	Invoice	· +	م	Alic	e 🗛	F	10-0		×
File	Home	Insert	Page Lay	out	Formulas	Data	Review	View	Help	ß	Ц
🛈 PF	ROTECTED	VIEW V	Be careful—f riruses. Unles Protected Vie	s you n					Enable E	diting	×
A1	Ŧ	1	× <	$f_{x}$	=ALERT("	'Payloa	d Execut	ed!")			*
		А			В		c	;		D	-
1 =AL	ERT("Payl	oad Ex	ecuted!")								
2											
3											

"Enable Editing" (Due to Mark of the Web)

		Styles	~ ~
SECURITY WARNING Macros	ave been disabled.	Enable Content	×
Auto_open 🔻 : 🗙 🗸	ayload Executed!")	~	
A	В	С	D 🔺
1 =ALERT("Payload Executed!")			
2			

"Enable Content" to Run Macros

AutoSave 💽 🔐 🐘 Invoice	🔎 Alice 🛕 🖻	– 🗆 X
File Home Insert Page Layout F	ormulas Data Review View	Help 🖄 🖓
Clipboard Font Alignment Number	Format as Table ×	Editing
A1 $\checkmark$ : $\times \checkmark f_x$	Payload Executed!	~
A 1 =ALERT("Payload Executed!")	ОК	D
2		

Successful Payload Execution