IN5290 - Home exam 4 Web hacking 2 – Parameter tampering, Cross Site Scripting, Session hijacking – Home exam

Tanusan Rajmohan - tanusanr@ulrik.uio.no

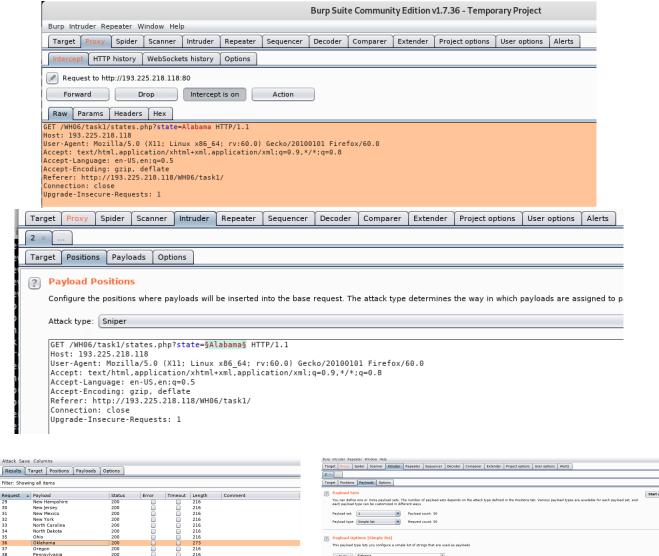


UNIVERSITETET I OSLO

Høsten 2018

Find the flag on the site http://193.225.218.118/WH06/task1 (parameter tampering)

The flag is UiOCTF{Where the Wind Comes Sweeping Down the Plain}. This flag was found by using burp suit. I first used the proxy part to intercept the site when I clicked on a link. Then I pressed forward, so it gave me the information when a link was clicked. Then I right-clicked and sent it to the intruder, where I pasted a file with all the states in the "payload" section. This lead to the state "Oklahoma" which stood apart from the rest and the 3 first states which was on the site. Then I changed the state parameter on the site to Oklahoma and found the flag. You can see the length was different like the 3 first sites in the images below.



ta	200 200			216 216						
	200			273			ad Options [Simple list]			
	200			215		This payload	yload type lets you configure a simple list of strings that are used as payloads.			
lia	200	<u> </u>		216		Paste	te Alabama A			
nd	200 200	<u> </u>		216 216		Load				
lina		_					Arkansas			
ta	200			216		Remove	Colorado			
	200 200			216 216		Clear	Connecticut			
	200			216			Belaware Florida			
	200			216			Georgia.			
	200			210		Add	Enter a new item			
						Add from Is	om list (Pro version only)			
ers Hex										
s.php?state=Oklahoma HTTP/1.1					Payload Processing					
.0 (X11; Linux x86 64; rv:60.0) Gecko/20100101 Firefox/60.0					You can define rules to perform various processing tasks on each payload before it is used.					
lication/vhtml+	x00_04; rv:00.	0/ GECK0/201	*/*:0=1	11610X/00.0						
lication/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 S.en;q=0.5					Add	d Enabled Rule				
, deflate						Edit				
25.218.118/WH06	/task1/									
						Remove	hve b			

Requ est Response Raw Params Hea st: 193. er-Agent

UiOCTF{Where the Wind Comes Sweeping Down the Plain}

193.225.218.118/WH06/task1/s ×

→ C ③ Not Secure | 193.225.218.118/WH06/task1/s

Redirect the following page to http://nrk.no (XSS) http://193.225.218.118/WH06/task2

This was done by testing a couple of scripting phrases, which lead to the command: $\langle IFRAMESRC = \#onmouseover =$ "document.location =' http://nrk.no'" >< /IFRAME >. The redirect was achieved by inserting this line in the postal code section of the site. After this was submitted, I just pressed submit again and it redirected me to the nrk.no webpage. See screenshots below (I also changed the input size just to se the whole line).

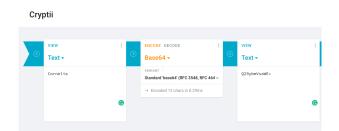
Mozilla Firefox	(←) → C ^a		
193.225.218.118/WH06/task × 🛠 Preferences × +	☆ Most Visited ⊕ Offensive Security ⊕ Kali Linux ⊕ Kali Docs ⊕ Kali Tools ⊕ Exploit-DB ▲ Aircrack-ng ⊕ Kali Fo Final step to be millioner: by a lottery ticket and wini		
(← → C û (193.225.218.118/WH06/task2/	That step to be minioner, by a locarly device and with		
A Most Visited D Offensive Security Kali Linux Kali Docs Kali Tools Exploit-D	First name:		
Fill in the form to be millioner after	Family		
rin in the form to be minioher after	name: Address:		
	City:		
Final step to be millioner: by a lottery ticket and win!			
	Postal code: /FRAME		
First name:	Comment:		
Family			
name: Address:	Submit		
Address:	😱 🖵 Inspector 🗈 Console 🗅 Debugger {} Style Editor @ Performance 🕩 Memory 🗦 Network 😝 Storage		
City:	□ Inspector □ Console □ Debugger {} Style Editor ④ Performance ● Memory ≥ Network ⑧ Storage + <t< th=""></t<>		
Postal code:) 		
	<pre>> > < <td>> < <td></td></td></pre>	> < <td></td>	
Comment:	<pre><td< th=""></td<></pre>		
Submit	<pre>v </pre>		
λοριερίους • Place • ■ Finder EM • 10:27,25 ■ # / •1 0 • Macella Finder. 0 0 0 0	Applications • Places • Friedox ESR • Los 37:26 III # / 4 • • • NRK.no - myheter, tvog zašo fra Norga og hele verden - Mozilla Firefox • • • • • • • • • • • • • • • • • • •		
(←) → C* @ (0 193.225.218.118/WH06/task2/index.ptp ···· ♡ ☆ IN □ ▲ Ξ Ø Most Veited © Offensive Security © Kali Linux © Kali Docs © Kaji Linux © Kali Docs © Kaji Korurs © Kali Training € Getting Started			
Fill in the form to be millioner after the course!	🕹 Most Visited 🔁 Offensive Security 🖶 Kall Linux 🖨 Kall Doss 🕀 Kall Tools 🕀 Exploit-DB 🔪 Aircrack-ng 🕲 Kall Forums 🕀 NetHunter 🖨 Kall Training 💊 Getting Started		
First name: Family name: Address:	NYHETSAKLDINGER DEderpart dode i smällylykke Zyde versionen Sijul utstyr for en halv million Syste service of basic locarcoma Syste service of basic locarcoma		
City:	V ATHELDIALEDIAUEK 221 FLYSTYRTI MERÄKER 2506 26.09 SKYTING PÅ BAR I CALFORNA 16.07		
	FREGATT KOLLIDERTE MED TANKSKIP		
Postal code:	SE NÅ		
Comment: Final step to be millioner: by a lottery ticket and win!	Se sendingen nå		
Pirst name:			
Pamly name:			
Address: City:			
Postal code:			
Convenant.			

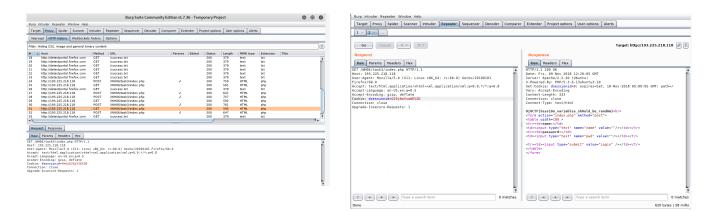
I also used these pages for look up and additional information: https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet http://www.asciitable.com/

Find the flag on the site http://193.225.218.118/WH06/task3 4 users are already logged in (they have valid sessions): Nora/flowers, Stine/Hedgedog, Veronica/Halifax, Kari/sunshine There's another logged in user: Cornelia

This task was done by Burp and a base64 converter. I first used Burp to monitor the proxy and find the sessionID which gave me the four IDs for the users that was mentioned. After thinking a bit and testing out, I found out that these IDs was made with a base64 converter. I also understood that the encoded versions was the names, so I encoded "Cornelia" and got the encoded value "Q29ybmVsaWE=" and the equal sign just means "%3D". So I used the repeater in Burp and pasted the sessionID for Cornelia and it gave me the flag: UiOCTF{Sess10n_var1ables_sh0uld_be_rand0m}

User	Session ID
Nora	Tm9yYQ%3D%3D
Stine	U3RpbmU%3D
Veronica	VmVyb25pY2E%3D
Kari	S2FyaQ%3D%3D
Cornelia	Tm9yYQ%3D%3D





I also had to change some of the settings in firefox so that Burp would intercept the traffic for the first task and the last task. See image below for which changes.

	Firefox about:pro		a			A				
st Visited 🔘 Offensive Secur	ity 🕲 Kali Linux 🕲	Kali Docs	🕲 Kali Tools	Exploit-DB	Nircrack-ng	Hali Forums	Netl	Hunter 🤅		
	Connection Settings									
🔆 General										
Q Search	Configure Proxy	Accessto	the Intern	et						
Privacy & Security	Auto-detect p	roxy setting	gs for this ne	t <u>w</u> ork						
Firefox Account	Use system pr	roxy setting	IS							
	<u>Manual proxy</u>	Manual proxy configuration								
	HTTP Pro <u>x</u> y	127.0.0.1					Port	8080		
	✓ Use this proxy server for all protocols									
	SS <u>L</u> Proxy	127.0.0.1					Port	8080		
		127.0.0.1					Port	8080		
	<u>F</u> TP Proxy	127.0.0.1								
	<u>F</u> TP Proxy SO <u>C</u> KS Host						Por <u>t</u>	8080		
	SO <u>C</u> KS Host	127.0.0.1	v4 💿 SO(CKS <u>v</u> 5			1 1	8080		
	SO <u>C</u> KS Host	127.0.0.1	v4 🖲 SOC	CKS <u>v</u> 5			1 1	8080		