


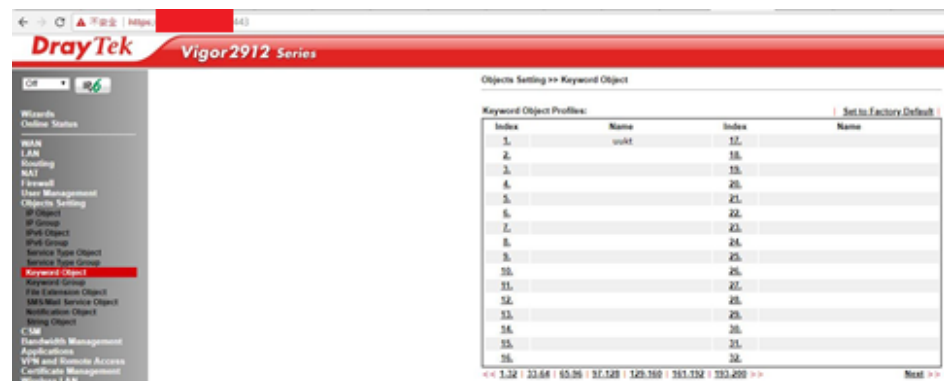
(10)Severity – High DrayTek(CSM-DNS Filter Profile Content) stored XSS

Subject	DrayTek(CSM-DNS Filter Profile Content) stored XSS	Severity	High
Category	Cross-Site Scripting (XSS)	Target	x.x.x.x
Position	http://x.x.x.x:443/		
Version	Firmware Version : 3.8.8.2		
Description	“CSM-DNS Filter Profile Content” enables attackers to inject client-side scripts into web pages viewed by other users.		
Threats	This vulnerability may cause Denial-of-Service (DoS) attack, deface, phishing and inject coin miner script.		
Test Procedures	<p>[Step 1]</p> <p>Build a keyword content on "Object Setting"→"Keyword Object" page select No 1.</p>  <p>[Step 2]</p> <p>Type some keyword in Profile Index and press OK. (We will use the website of uukt in this case)</p>		



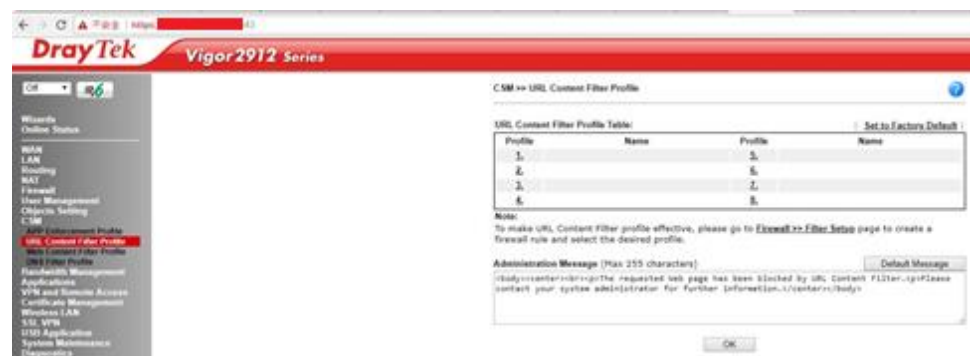
[Step 3]

It will add a new profiles in Kerword Object page after we press OK in Profile Index page.



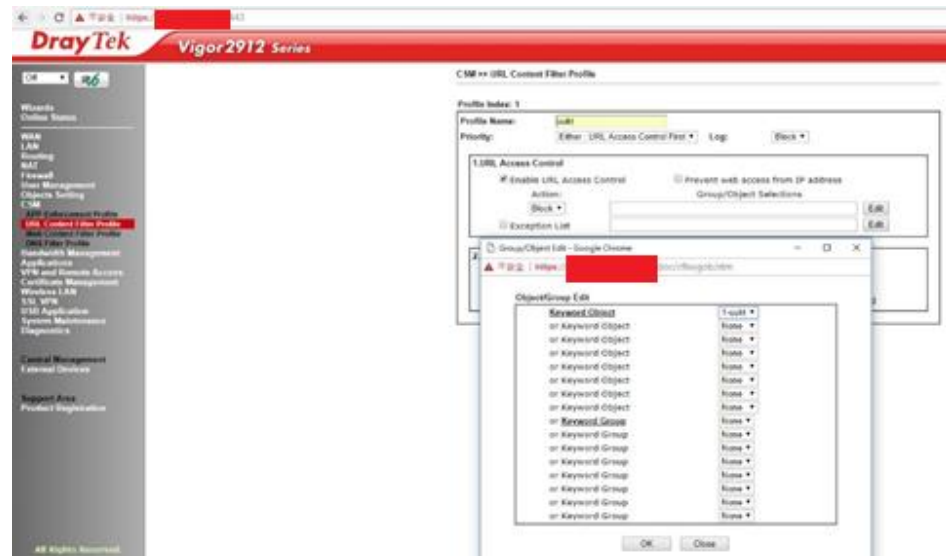
[Step 4]

Bulid a content filter pofile of web on "CSM"→"URL Content Filter Profile" page and selecet No 1 in "URL Content Filter Profile Table".



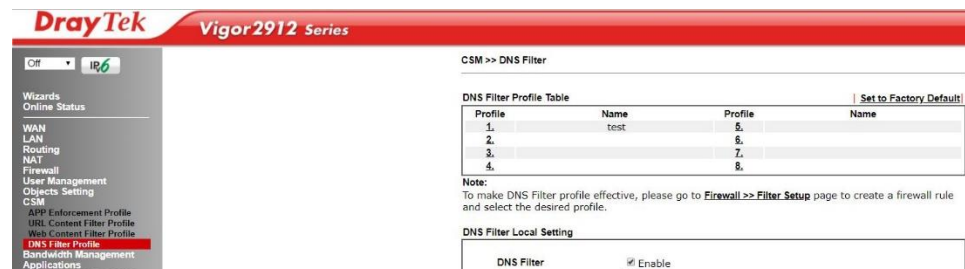
[Step 5]

Press “Edit” and choose the Keyword Object “uukt” that we set before and Action choose “Block”



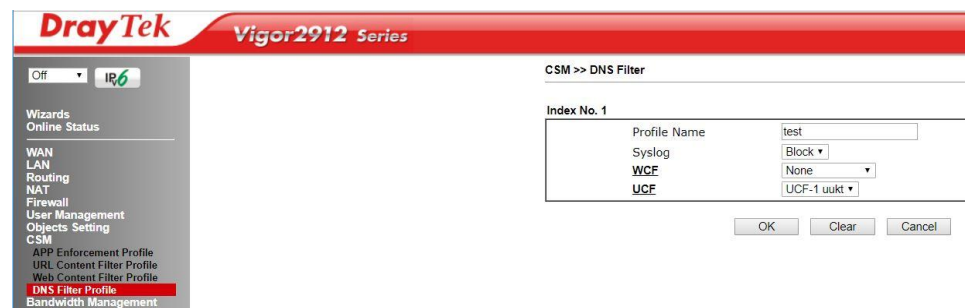
[Step 6]

Bulid a content filter pofile of web on "CSM"→"DNS Filter Profile" page and selecet No 1 in " DNS Filter Profile Table".



[Step 7]

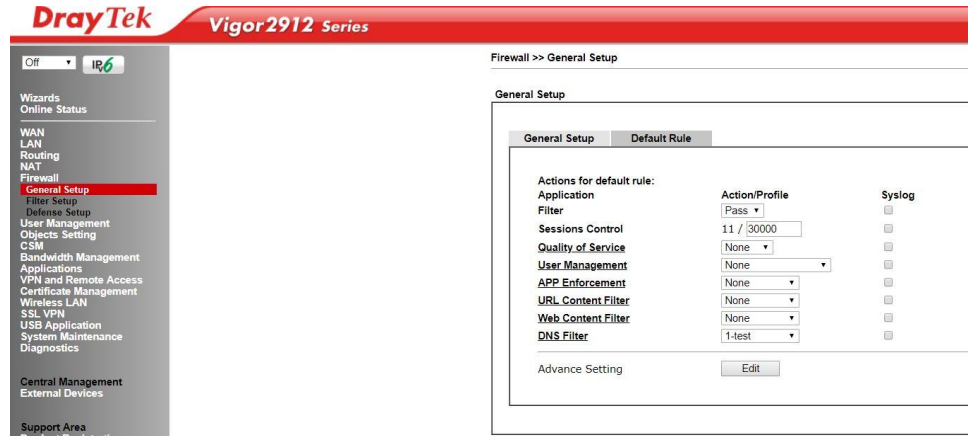
Set a Profile Name and choose the profile name that we set before.



[Step 8]

Build a rule of firewall on "Firewall"→"General Setup"→

"Default Rule" page and select Profile in "DNS Filter".



[Step 9]

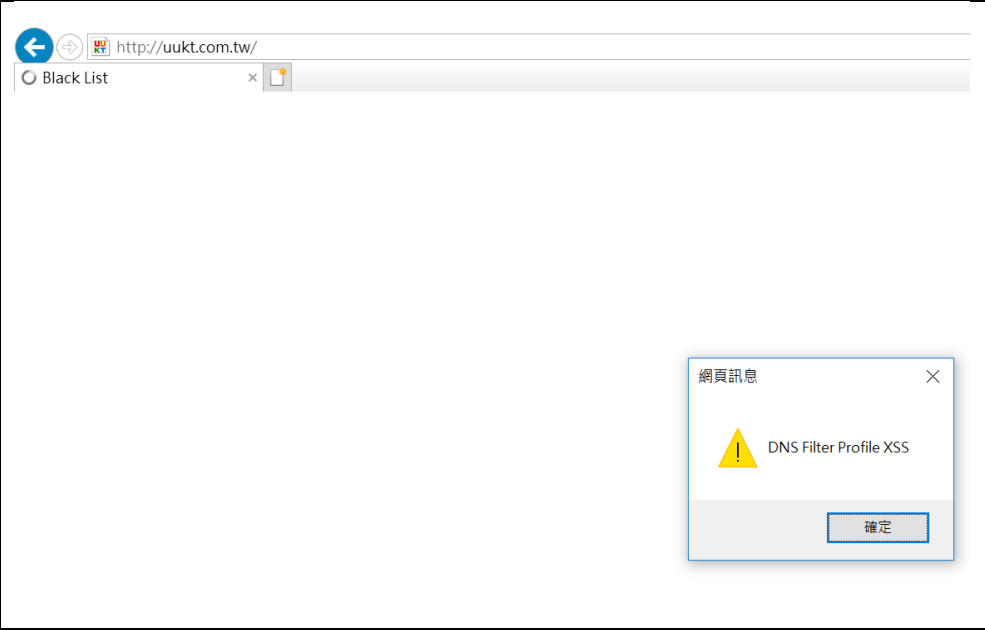
Insert a XSS script "CSM"→"DNS Filter Profile"→"

Administration Message" field.



[Step 10]

It will show a bounce window of XSS message when user visit the website of "uukt.com.tw".

	 A screenshot of a web browser window. The address bar shows 'http://uukt.com.tw/'. There is a tab titled 'Black List'. A warning dialog box is displayed in the bottom right corner with the title '網頁訊息' (Web Message), a yellow warning icon, and the text 'DNS Filter Profile XSS'. A '確定' (Confirm) button is at the bottom of the dialog.
Remediation	Escaping untrusted HTTP request data based on the context in the HTML output (body, attribute, JavaScript, CSS, or URL) will resolve Reflected and Stored XSS vulnerabilities.