(8) Severity – High DrayTek(CSM-WEB Content) stored XSS

| Subject	DrayTek(CSM-WEB 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-WEB 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	[Step 1] Build a keyword content on "Object Setting"→"Keyword Object" page select No 1. [Step 2] Type some keyword in Profile Index and press OK. (We will use the website of uukt in this case)		
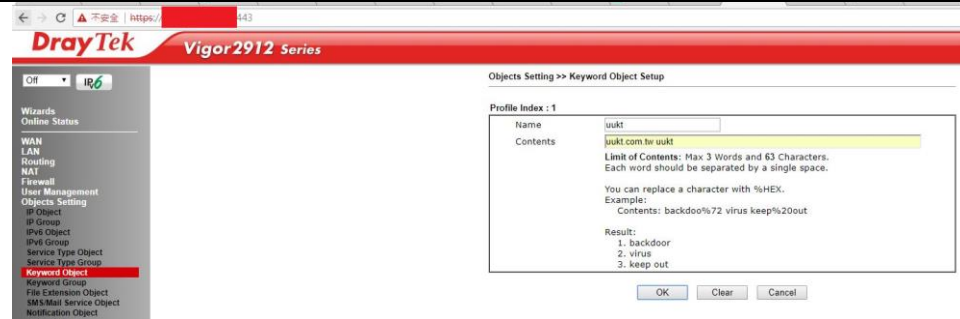
[Step 3]

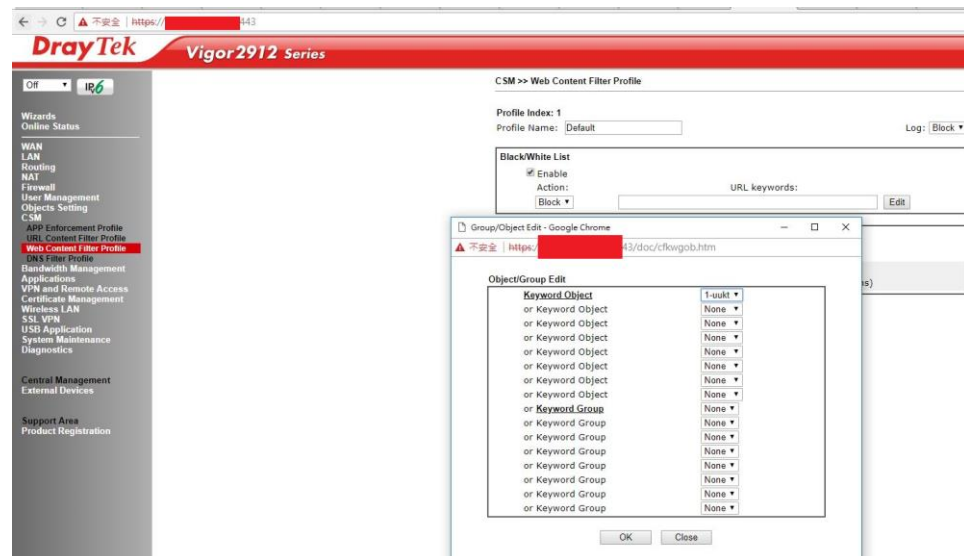It will add a new profiles in Kerword Object page after we press OK in Profile Index page.
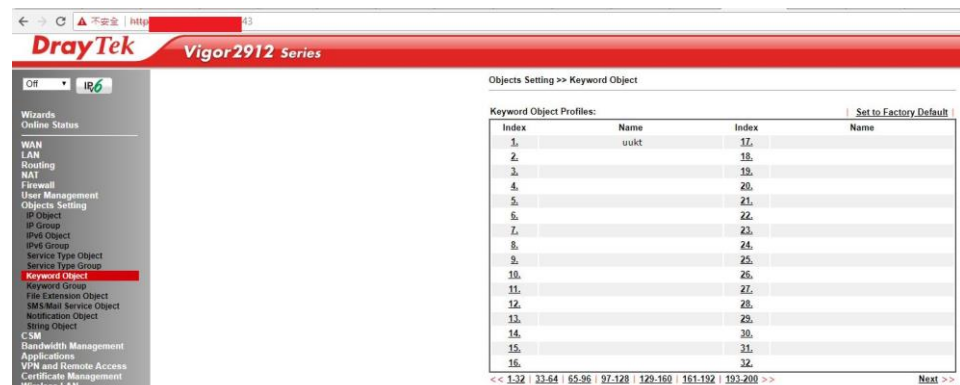
[Step 4]

Bulid a content filter pofile of web on "CSM"→"Web Content Filter Profile" page and selecet No 1 in "Web Content Filter Profile Table".
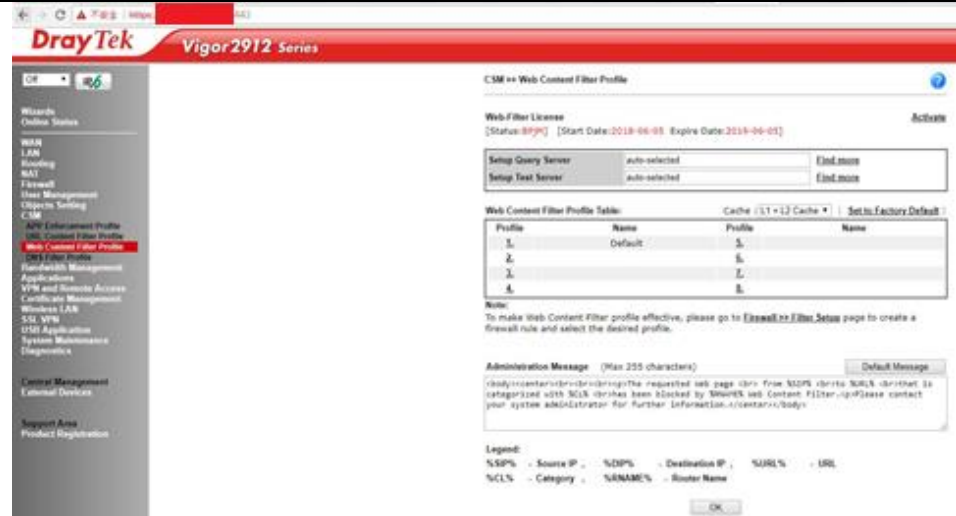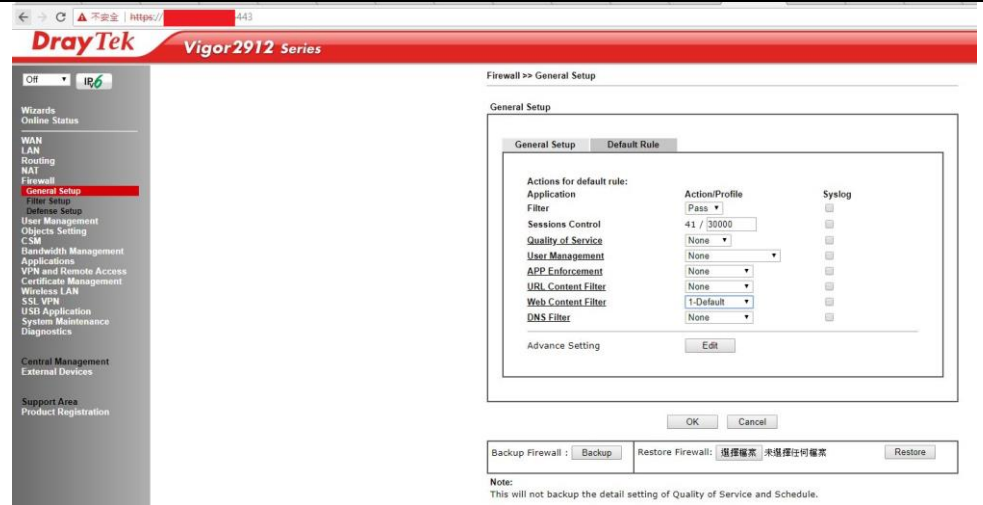
[Step 5]

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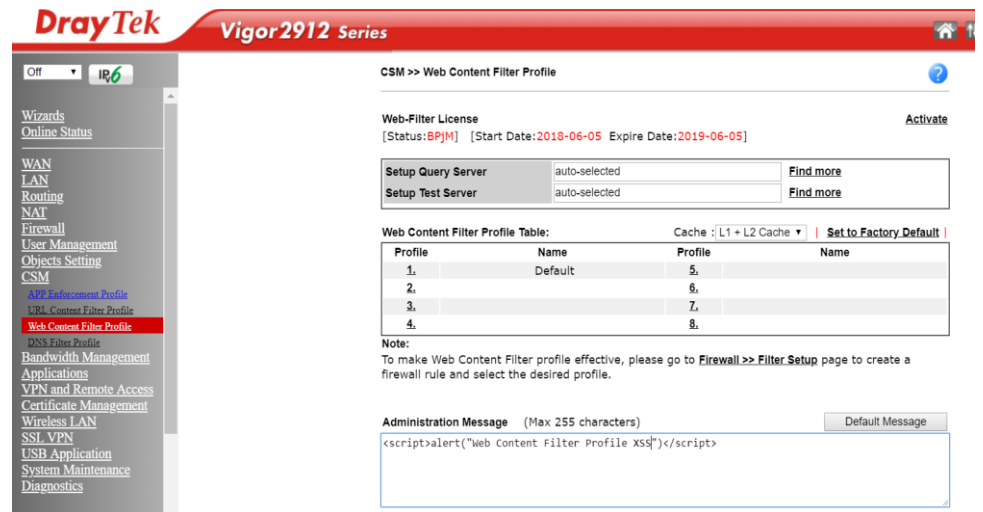

[Step 6]

Bulid a rule of firewall on "Firewall"→"General Setup"→"Default Rule" page and selecet Profile in "Web Content Filter Profile".
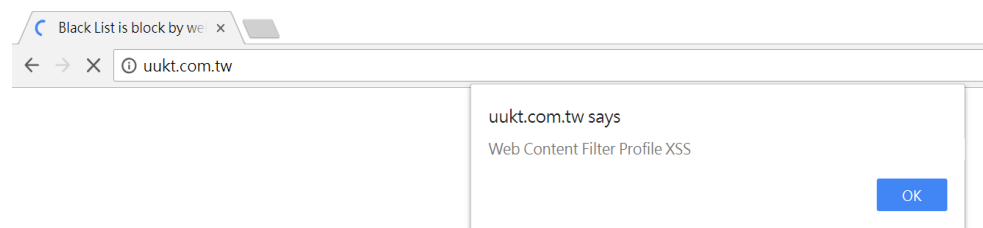
[Step 7]

Insert a XSS script "CSM"→"Web Content Filter Profile"→"Administration Message" field.

[Step 8]

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

Remedation	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.