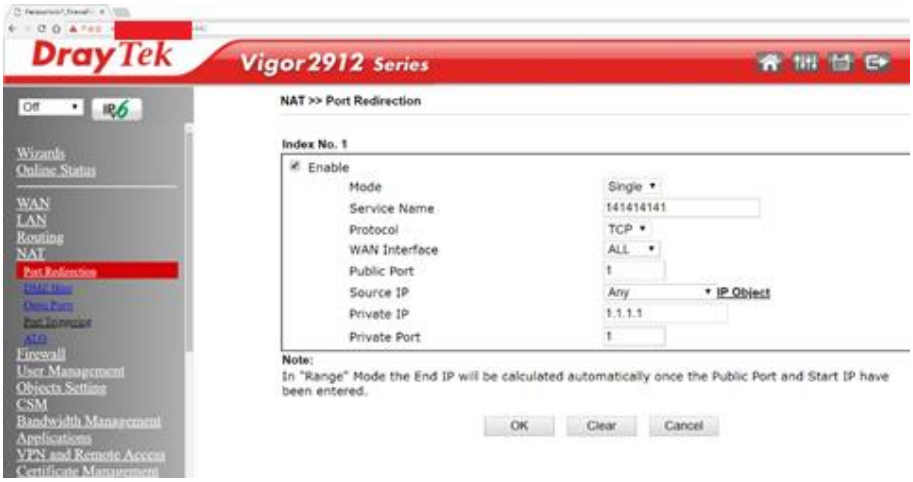
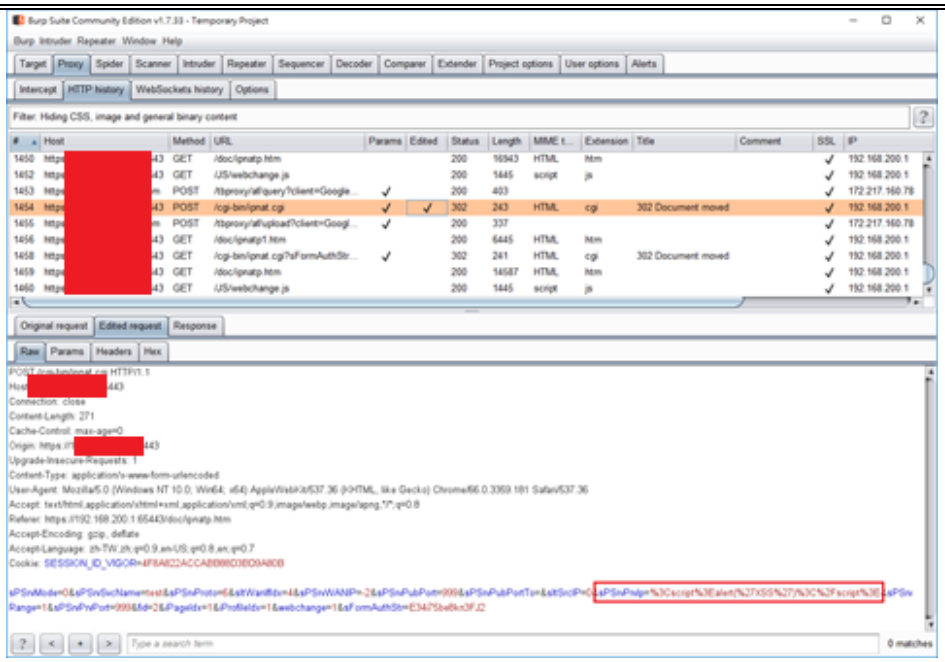
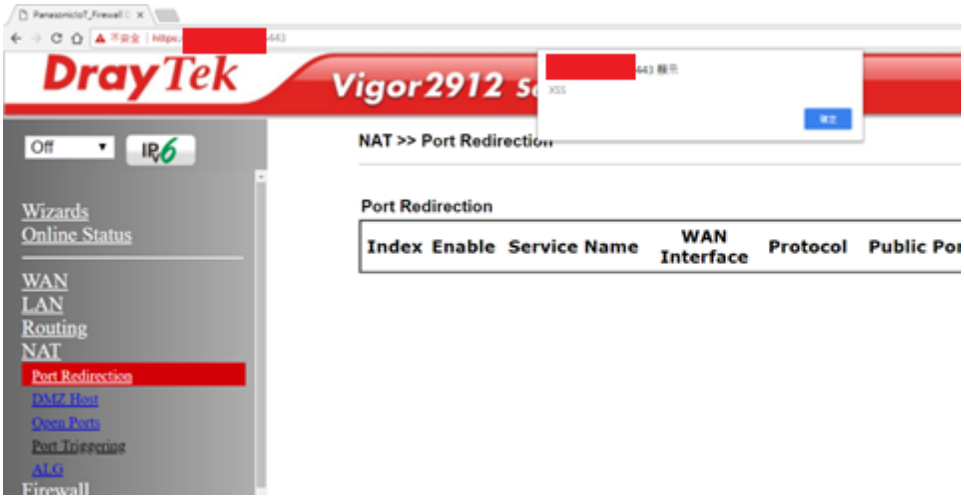
(5)Severity – High DrayTek Port Redirection Stored XSS

Subject	DrayTek Port Redirection 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 Redirection" page Attacker can inject malicious code in this page  Attacker can temper the parameter to malicious code		

<table>
<tr>
<td></td>
<td>


The malicious code will be run when user access this page


</td>
</tr>
<tr>
<td>Remedation</td>
<td>Escaping untrusted HTTP request data based on the context in the HTML output</td>
</tr>
</table>