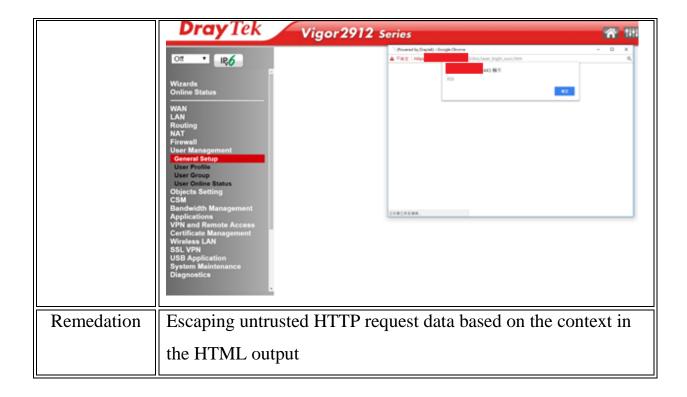
(6) Severity – High DrayTek General Setup Stored XSS

Subject	DrayTek General 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.		
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.		
Environment	Please follow the appendix		
Log Data	1.txt, 2.txt		
Test	The vulnerability occur on "User Management" → "General		
Procedures	Setup" page		
	Attacker can inject malicious code in this page		
	User Management >> General Setup Wizards Online Status WAN LAN Routing NAT Firewall User Profile User Profile User Group User Profile User Group User Online Status Objects Setting CSM Bandwiddt Management Applications VPN and Remode Access Certificate Management Wireless LAN SSL VPN USB Application The malicious code will be run when	rent IP address. method based on user profile rent user profiles. TPS	s. Administrator may set essful login. exiew: Set to Fectory Default ript>



1