



(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 Procedures	<p>The vulnerability occur on "User Management" → "General Setup" page</p> <p>Attacker can inject malicious code in this page</p>  <p>The malicious code will be run when user access this page</p>		

	
Remediation	Escaping untrusted HTTP request data based on the context in the HTML output