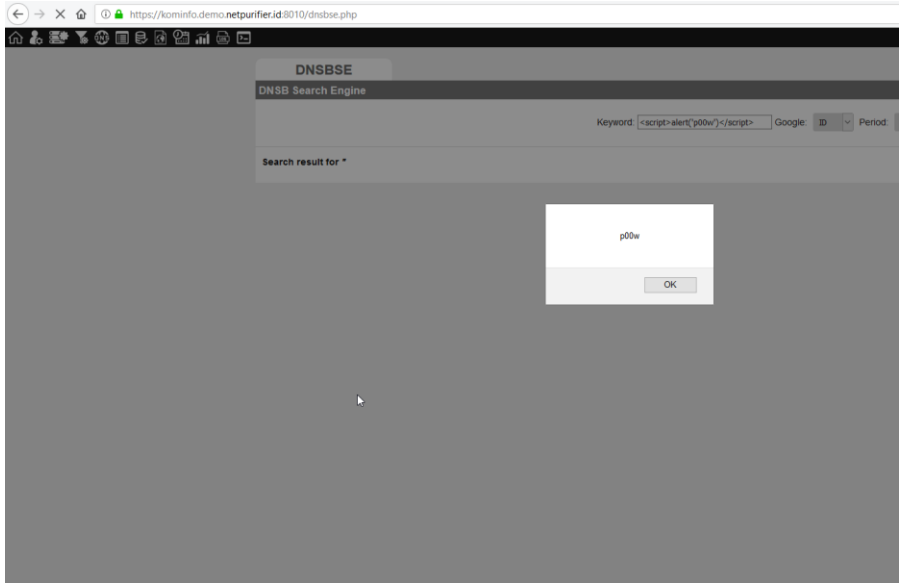




XSS 2 Via POST Request

11 Februari 2018

Oleh zetc0de

Deskripsi	Kami mendapatkan form input search pada parameter cari di file dnsbse.php , lalu kami coba masukan simple payload xss, kami coba eksekusi dan payload tereksekusi.
URL / Aplikasi	https://koinfo.demo.netpurifier.id:8010/dnsbse.php
Dampak	Hacker dapat mencuri cookie user lain jika user mengeksekusi payload berbahaya
Langkah-langkah	<ol style="list-style-type: none"> 1. Attacker membuat script XSS, https://pastebin.com/raw/541geyx5 2. Lalu mengirimkan ke victim 3. Victim mengeksekusi payload 4. Victim ketriger
Bukti Temuan	<p>https://drive.google.com/open?id=1FrkeRWRs5WnXkGT-Z9ylSiB5atc8pLv8</p> 
Remediasi / Rekomendasi	Filter Input
Referensi	https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

