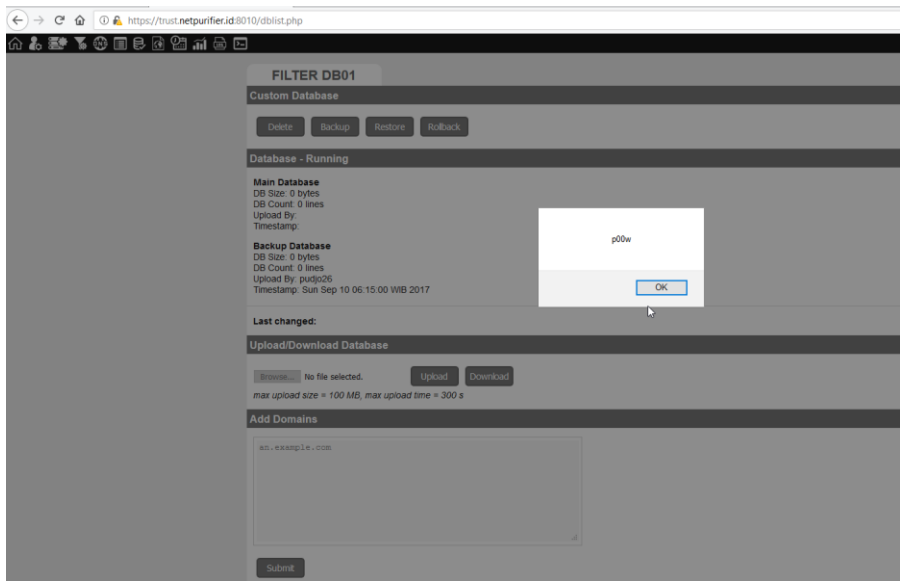




## **XSS 2 Via POST Request on <https://trust.netpurifier.id>**

**11 Februari 2018**

**Oleh zetc0de**

<b>Deskripsi</b>	Kami mendapatkan form input search pada file dblist.php, lalu kami coba masukan simple payload xss pada parameter caridb, kami coba eksekusi dan payload tereksekusi.
<b>URL / Aplikasi</b>	<a href="https://trust.netpurifier.id:8010/dblist.php">https://trust.netpurifier.id:8010/dblist.php</a>
<b>Dampak</b>	Hacker dapat mencuri cookie user lain jika user mengeksekusi payload berbahaya
<b>Langkah-langkah</b>	<ol style="list-style-type: none"> <li>1. Attacker membuat script XSS, <a href="https://pastebin.com/raw/qaRqTxvm">https://pastebin.com/raw/qaRqTxvm</a></li> <li>2. Lalu mengirimkan ke victim</li> <li>3. Victim mengeksekusi payload</li> <li>4. Victim ketriger</li> </ol>
<b>Bukti Temuan</b>	
<b>Remediasi / Rekomendasi</b>	Filter Input
<b>Referensi</b>	<a href="https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)">https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)</a>