

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

11 Februari 2018

Oleh zetc0de

## Laporan Bug Bounty Cyber Army Indonesia | 2

Deskripsi	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.
URL / Aplikasi	https://trust.netpurifier.id:8010/dblist.php
Dampak	Hacker dapat mencuri cookie user lain jika user mengeksekusi payload berbahaya
Langkah-langkah	1. Attacker membuat script XSS, https://pastebin.com/raw/qaRqTxvm  2. Lalu mengirimkan ke victim  3. Victim mengeksekusi payload  4. Victim ketriger
Bukti Temuan	FILTER DB01  Custom Database  Database - Running  Main Outrasse  Discuss 0 bytes Upload By Timestamp  Backup Database  Discuss 0 bytes Upload By Timestamp  Discuss 0 by
Remediasi / Rekomendasi	Filter Input
Referensi	https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)