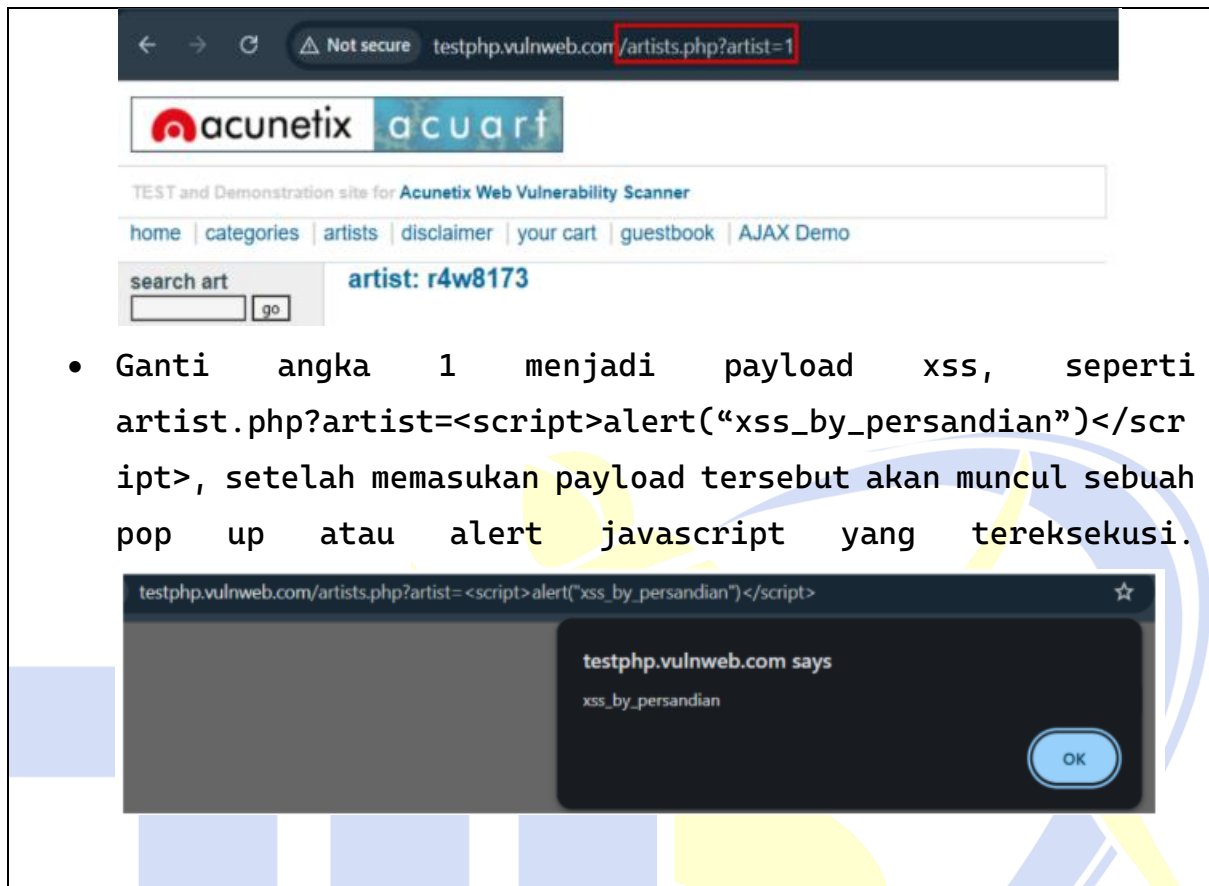


LAPORAN INSIDEN SIBER KUTAI KARTANEGARA

RINGKASAN TEMUAN CELAH KEAMANAN	
Vuln Type	Cross Site Scripting (XSS)
Severity/Score	High (5.3) CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
Endpoint Url	artists.php?artist=xss
Impact	1. Rusaknya tampilan website karena injeksi kode/script yang dimasukan oleh Attacker. 2. Bisa terjadi pencurian akun admin oleh Attacker. 3. Hilangnya integritas atau nama instansi yang terdampak.
Remediation	1. Melakukan validasi atau sanitasi pada form inputan. 2. Menerapkan htmlspecialchars atau htmlentities untuk melakukan validasi inputan. 3. Menerapkan Escape seperti validasi pada framework Laravel yang menggunakan ({{\$inputan}}).
Reference	1. https://www.first.org/cvss/calculator/3-1 2. https://owasp.org/wwwcommunity/attacks/xss
PROOF OF CONCEPT	
• Pergi pada website http://testphp.vulnweb.com, dan akses pada menu artists. Pada menu tersebut terdapat sebuah endpoint parameter artist=1.	



← → ↻ Not secure testphp.vulnweb.com/artists.php?artist=1

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go artist: r4w8173

- Ganti angka 1 menjadi payload xss, seperti `artist.php?artist=<script>alert("xss_by_persandian")</script>`, setelah memasukan payload tersebut akan muncul sebuah pop up atau alert javascript yang tereksekusi.

testphp.vulnweb.com/artists.php?artist=<script>alert("xss_by_persandian")</script>

testphp.vulnweb.com says
xss_by_persandian

OK