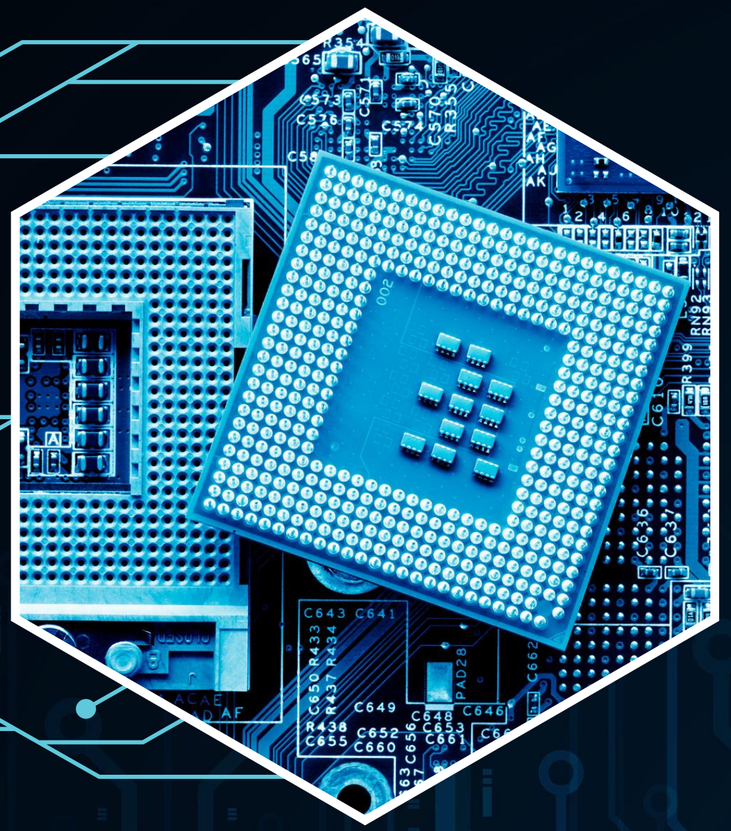
MSIB Batch7 GMUM



Kelompok 2

PENETRATION TESTING

Analisis Keamanan Sistem Website/Aplikasi Dinas Komunikasi Informatika Statistik dan Persandian Provinsi Sulawesi Selatan

Kelompok 2

Anggota Kelompok

Asyrof Hafizh Maulana

Bintang Safitri

Anissa Sahda Aulia

Devika Sari

Fitra Putra Aldi Wijaya

Pendahuluan

Keamanan siber menjadi hal yang krusial bagi lembaga pemerintah, termasuk Dinas Komunikasi, Informatika, Statistik, dan Persandian Provinsi Sulawesi Selatan, mengingat peran website dan aplikasi mereka dalam menyediakan informasi dan layanan publik. Ancaman seperti serangan cyber dan kebocoran data dapat merusak kepercayaan publik dan mengganggu layanan. Oleh karena itu, evaluasi keamanan rutin sangat penting untuk mendeteksi kerentanannya. Dokumen ini menyajikan hasil penetration testing yang dilakukan pada sistem digital dinas tersebut, dengan tujuan untuk memperbaiki kesiapan menghadapi tantangan keamanan siber dan menciptakan ekosistem digital yang lebih aman.

Kelompok 2

Tujuan Penetration Testing

1. **Untuk meningkatkan celah kemanann**
2. **mendeteksi potensi kerentanan keamanan yang ada dalam sistem**
3. **Membuat laporan lengkap terkait risiko, yang memberikan wawasan terperinci mengenai temuan**
4. **Meningkatkan pemahaman mengenai pentingnya keamanan informasi sebagai bagian integral dari pengelolaan digital pemerintahan yang lebih aman dan andal.**

Target website

bebastemuan.sulselprov.go.id

jdih.sulselprov.go.id

simrs.rsudsr.sulselprov.go.id

siapla.sulselprov.go.id

sipbm.sulselprov.go.id

inspektorat.sulselprov.go.id

rskddadi.sulselprov.go.id

bebastemuan.sulsel.prov.go.id

Situs web ini membahas digitalisasi aplikasi surat keterangan bebas temuan (SKBT). Situs web ini memberikan informasi tentang proses aplikasi, jumlah sertifikat yang dikeluarkan, dan informasi kontak. Ini adalah dokumen tentang digitalisasi aplikasi surat keterangan bebas temuan di Sulawesi Selatan.

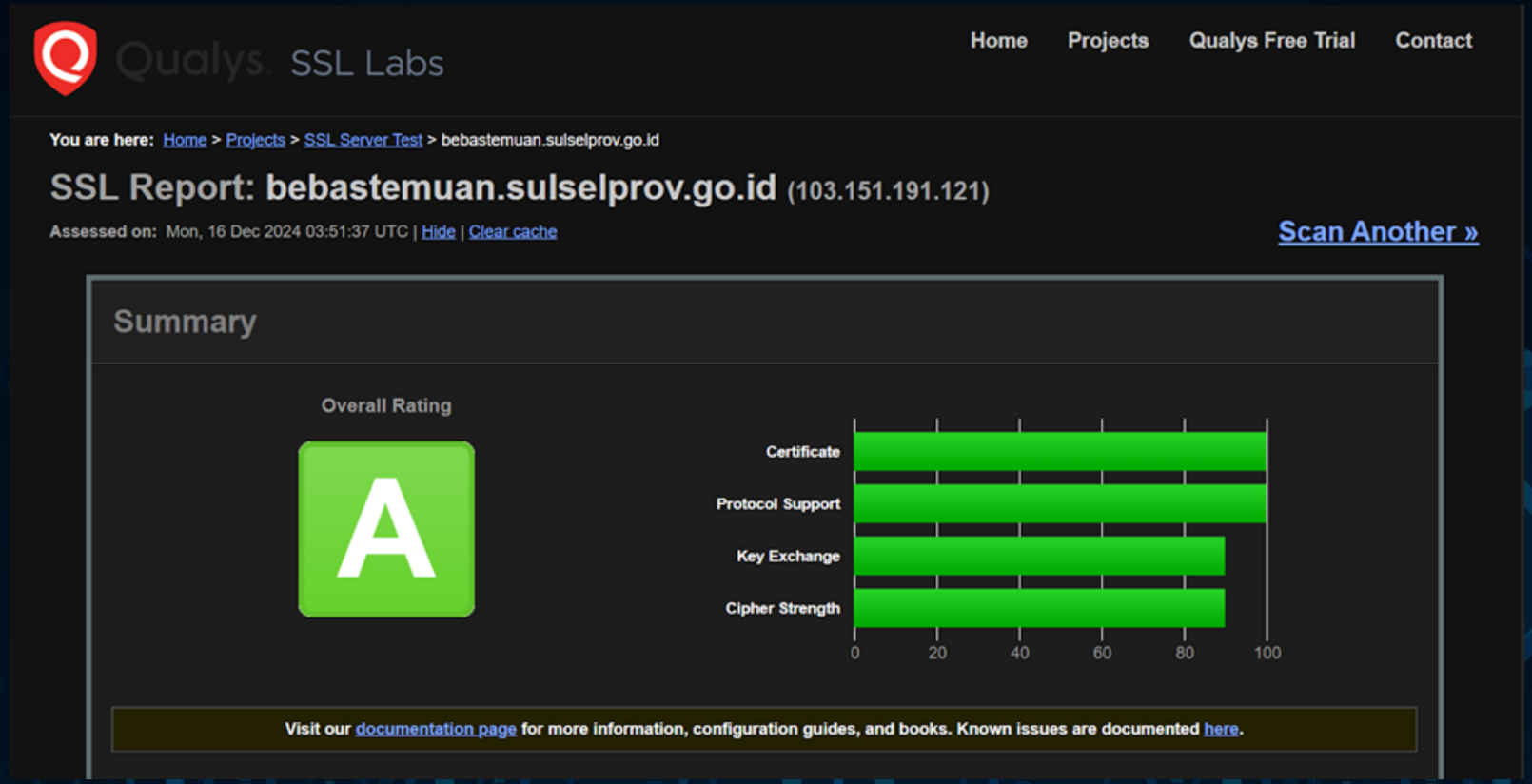
bebastemuan.sulsel.prov.go.id

website ini menggunakan software server sebagai berikut

Software / Version	Category
Animate.css	UI frameworks
cdnjs	CDN
Google Hosted Libraries	CDN
FancyBox	JavaScript libraries
Font Awesome	Font scripts
Bootstrap	UI frameworks
Google Font API	Font scripts
jQuery 3.5.1	JavaScript libraries
Laravel	Web frameworks
Nginx 1.18.0	Web servers, Reverse proxies
Open Graph	Miscellaneous
OWL Carousel	JavaScript libraries

bebastemuan.sulsel.prov.go.id

berikut SSL Report dari web ini



bebastemuan.sulsel.prov.go.id

Berikut hasil scan yang kami lakukan menggunakna tools Pentest Tools.

bebastemuan.sulsel.prov.go.id

Saran Perbaikan dari web ini

1. Implementasi Otentikasi Multi-Faktor (MFA):

MFA menambahkan keamanan tambahan dengan memerlukan lebih dari satu metode verifikasi identitas saat login. Hal ini mengurangi risiko akses tidak sah meskipun password pengguna telah diketahui oleh pihak lain.

2. Penggunaan HTTPS dengan Sertifikat SSL/TLS yang Valid:

Gunakan HTTPS untuk mengenkripsi komunikasi antara pengguna dan server agar data sensitif terlindungi selama transmisi. Ini mencegah serangan man-in-the-middle dan menjaga integritas data.

3. Penambahan Header HTTP Strict-Transport-Security (HSTS):

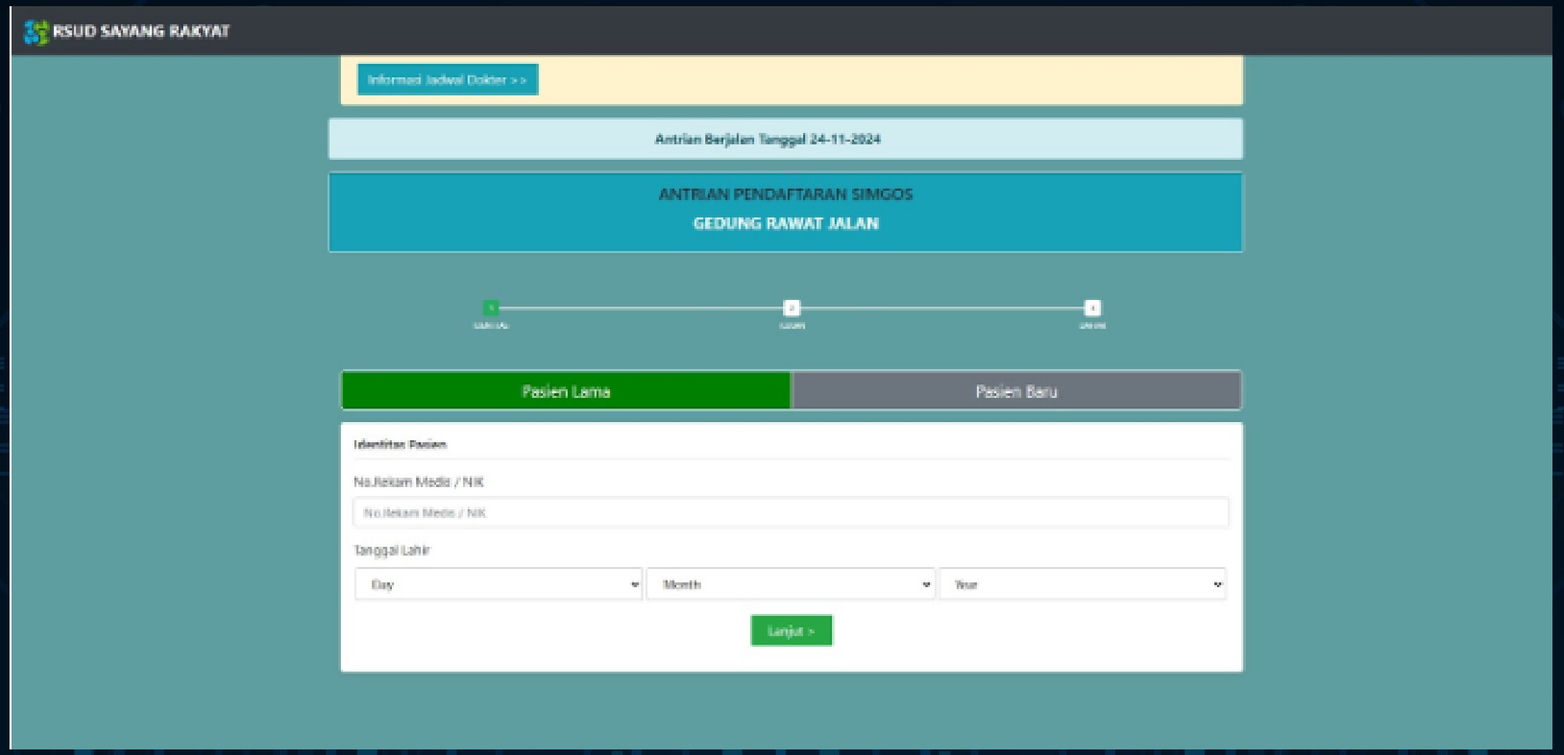
HSTS memaksa browser hanya menggunakan HTTPS, sehingga menghindari koneksi HTTP yang tidak aman. Konfigurasi ini meningkatkan keamanan dengan memastikan semua komunikasi tetap terenkripsi.

4. Pembatasan Upaya Login yang Gagal (Brute Force Protection):

Batasi jumlah percobaan login yang gagal dalam waktu tertentu untuk mencegah serangan brute force. Tambahkan mekanisme seperti CAPTCHA atau waktu tunggu setelah upaya gagal berturut-turut.

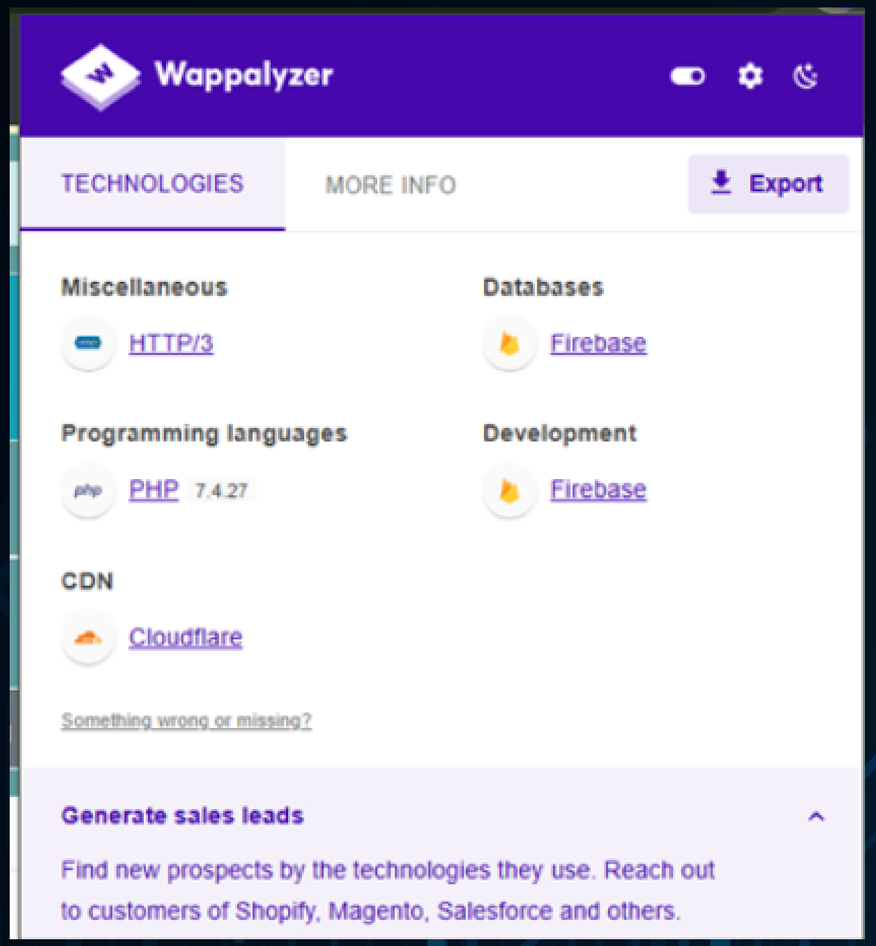
simrs.rsudsr.sulselprov.go.id

Website ini digunakan untuk mempermudah pendaftaran pasien di rumah sakit atau klinik secara online. Pasien dapat memilih untuk mendaftar sebagai pasien baru atau pasien lama, mengisi informasi yang dibutuhkan, dan mengecek status antrean mereka untuk mendapatkan layanan medis.



simrs.rsudsr.sulselprov.go.id

Website ini menggunakan teknologi sebagai berikut



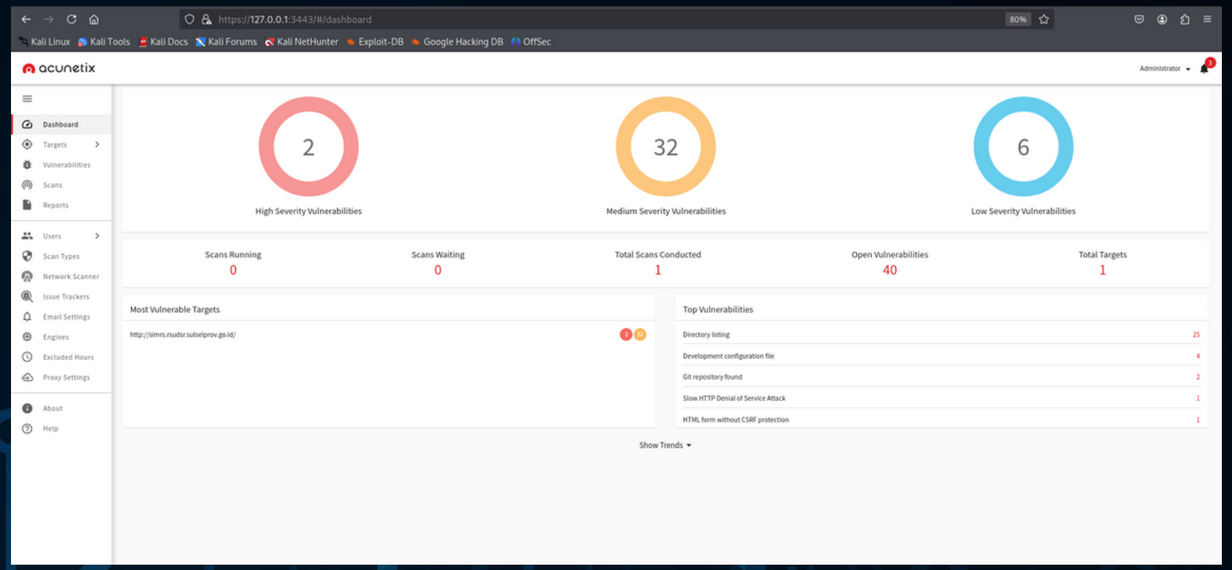
- **Website ini memanfaatkan PHP sebagai bahasa backend, Firebase untuk pengelolaan data (dan mungkin pengembangan aplikasi), dan Cloudflare sebagai CDN untuk performa dan keamanan.**

- **Teknologi ini menunjukkan bahwa website ini mengutamakan performa, modernitas (HTTP/3), dan pengelolaan data berbasis cloud.**

simrs.rsudsr.sulselprov.go.id

berikut hasil scan menggunakan Acunetix

Severity	Vulnerability	URL	Parameter	Status	Confidence %	Last Seen
	Git repository found	http://simrs.rsudsr.sulselprov.go.id/		Open	100	Dec 1, 2024, 10:32:26 PM
	Git repository found	http://simrs.rsudsr.sulselprov.go.id/apps/RegOnline/		Open	100	Dec 2, 2024, 12:17:13 AM
	Development configuration file	http://simrs.rsudsr.sulselprov.go.id/composer.lock		Open	95	Dec 1, 2024, 10:32:26 PM
	Development configuration file	http://simrs.rsudsr.sulselprov.go.id/vendor/twig/twig/composer.json		Open	95	Dec 1, 2024, 10:38:03 PM
	Development configuration file	http://simrs.rsudsr.sulselprov.go.id/vendor/twig/twig/.travis.yml		Open	95	Dec 1, 2024, 10:38:03 PM
	Development configuration file	http://simrs.rsudsr.sulselprov.go.id/report/composer.lock		Open	95	Dec 1, 2024, 10:59:36 PM
	Directory listing	http://simrs.rsudsr.sulselprov.go.id/vendor/		Open	100	Dec 1, 2024, 10:32:35 PM
	Directory listing	http://simrs.rsudsr.sulselprov.go.id/vendor/twig/		Open	100	Dec 1, 2024, 10:33:06 PM
	Directory listing	http://simrs.rsudsr.sulselprov.go.id/vendor/twig/twig/		Open	100	Dec 1, 2024, 10:33:06 PM
	Directory listing	http://simrs.rsudsr.sulselprov.go.id/vendor/twig/twig/test/		Open	100	Dec 1, 2024, 10:35:20 PM
	Directory listing	http://simrs.rsudsr.sulselprov.go.id/vendor/twig/twig/test/Twig/		Open	100	Dec 1, 2024, 10:38:03 PM
	Directory listing	http://simrs.rsudsr.sulselprov.go.id/vendor/twig/twig/test/Twig/Tests/		Open	100	Dec 1, 2024, 10:43:29 PM
	Directory listing	http://simrs.rsudsr.sulselprov.go.id/vendor/twig/twig/test/Twig/Tests/Loader/		Open	100	Dec 1, 2024, 10:43:35 PM
	Directory listing	http://simrs.rsudsr.sulselprov.go.id/vendor/twig/twig/test/Twig/Tests/Loader/Fixtures/		Open	100	Dec 1, 2024, 10:46:32 PM
	Directory listing	http://simrs.rsudsr.sulselprov.go.id/vendor/twig/twig/test/Twig/Tests/Loader/Fixtures/themes/		Open	100	Dec 1, 2024, 10:46:50 PM
	Directory listing	http://simrs.rsudsr.sulselprov.go.id/vendor/twig/twig/test/Twig/Tests/Loader/Fixtures/themes/theme1/		Open	100	Dec 1, 2024, 10:48:04 PM



simrs.rsudsr.sulselprov.go.id

High level :

☐	🐞	Git repository found	http://simrs.rsudsr.sulselprov.go.id/	Open	100	Dec 1, 2024, 10:32:26 PM

Direktori metadata Git (.git) ditemukan di folder ini. Penyerang dapat mengekstrak informasi sensitif dengan meminta direktori metadata tersembunyi yang dibuat oleh alat kontrol versi Git. Direktori metadata digunakan untuk tujuan pengembangan guna melacak perubahan pengembangan pada sekumpulan kode sumber sebelum dikomit kembali ke repositori pusat (dan sebaliknya). Ketika kode digulirkan ke server langsung dari repositori, kode tersebut seharusnya dilakukan sebagai ekspor, bukan sebagai copy pekerjaan lokal, dan oleh karena itu timbul masalah.

Vulnerability Description ▲

Git metadata directory (.git) was found in this folder. An attacker can extract sensitive information by requesting the hidden metadata directory that version control tool Git creates. The metadata directories are used for development purposes to keep track of development changes to a set of source code before it is committed back to a central repository (and vice-versa). When code is rolled to a live server from a repository, it is supposed to be done as an export rather than as a local working copy, and hence this problem.

The vulnerability affects **http://simrs.rsudsr.sulselprov.go.id/**

Discovered by **Git repository found**

File ini mungkin berisi informasi penting yang bisa digunakan oleh penyerang untuk melakukan serangan yang lebih berbahaya.

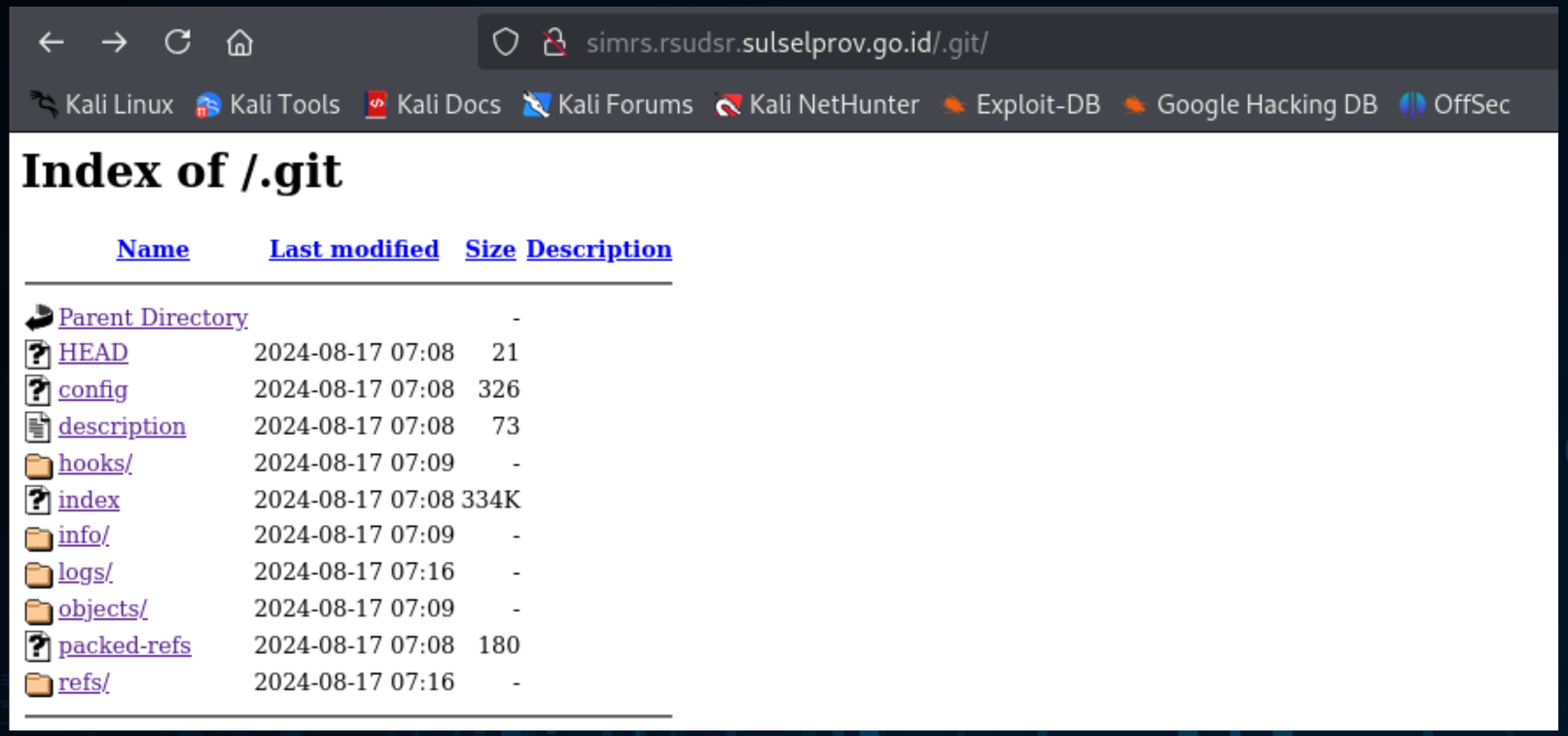
The impact of this vulnerability ▲

These files may expose sensitive information that may help an malicious user to prepare more advanced attacks.

simrs.rsudsr.sulselprov.go.id

POC

Direktori .git dapat diakses :



http://simrs.rsudsr.sulselprov.go.id/.git/

simrs.rsudsr.sulselprov.go.id

POC

Mengunduh metadata :

wget -r -np -nH --cut-dirs=3 -R "index.html*" http://simrs.rsudsr.sulselprov.go.id/.git/

```
┌──(asyrof㉿asyrof)-[~]
└─$ cd Downloads

┌──(asyrof㉿asyrof)-[~/Downloads]
└─$ wget -r -np -nH --cut-dirs=3 -R "index.html*" http://simrs.rsudsr.sulselprov.go.id/.git/
--2024-12-16 23:43:34--  http://simrs.rsudsr.sulselprov.go.id/.git/
Resolving simrs.rsudsr.sulselprov.go.id (simrs.rsudsr.sulselprov.go.id)... 172.67.203.188, 104.21.37.42, 2606:4700:3031::6815:252a, ...
Connecting to simrs.rsudsr.sulselprov.go.id (simrs.rsudsr.sulselprov.go.id)|172.67.203.188|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.tmp'

index.html.tmp                                          [ <=>                                                                   ]   2.70K  --.-KB/s    in 0s

2024-12-16 23:43:34 (68.4 MB/s) - 'index.html.tmp' saved [2769]

Loading robots.txt; please ignore errors.
--2024-12-16 23:43:34--  http://simrs.rsudsr.sulselprov.go.id/robots.txt
Reusing existing connection to simrs.rsudsr.sulselprov.go.id:80.
HTTP request sent, awaiting response... 404 Not Found
2024-12-16 23:43:35 ERROR 404: Not Found.

Removing index.html.tmp since it should be rejected.

--2024-12-16 23:43:35--  http://simrs.rsudsr.sulselprov.go.id/.git/?C=N;O=D
Reusing existing connection to simrs.rsudsr.sulselprov.go.id:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html?C=N;O=D.tmp'

index.html?C=N;O=D.tmp                                  [ <=>                                                                   ]   2.70K  --.-KB/s    in 0.005s

2024-12-16 23:43:35 (596 KB/s) - 'index.html?C=N;O=D.tmp' saved [2769]

Removing index.html?C=N;O=D.tmp since it should be rejected.

--2024-12-16 23:43:35--  http://simrs.rsudsr.sulselprov.go.id/.git/?C=M;O=A
Reusing existing connection to simrs.rsudsr.sulselprov.go.id:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html?C=M;O=A.tmp'

index.html?C=M;O=A.tmp                                  [ <=>                                                                   ]   2.70K  --.-KB/s    in 0.02s

2024-12-16 23:43:35 (147 KB/s) - 'index.html?C=M;O=A.tmp' saved [2769]

Removing index.html?C=M;O=A.tmp since it should be rejected.

--2024-12-16 23:43:35--  http://simrs.rsudsr.sulselprov.go.id/.git/?C=S;O=A
Reusing existing connection to simrs.rsudsr.sulselprov.go.id:80.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
```

simrs.rsudsr.sulselprov.go.id

POC

Melihat hasil unduhan metadata :

```
┌──(asyrof㉿asyrof)-[~/Downloads]
└─$ ls
'ACUNETIX LINUX'                                burpsuite_community_linux_v2024_10_2.sh   git_metadata_poc.py        openvas.pdf                                                                packed-refs               prepare-commit-msg.sample
'ACUNETIX LINUX-20241202T023508Z-001.zip'       commit-msg.sample                         heads                      origin                                                                     post-update.sample        remotes
 HEAD                                           config                                    index                     'owasp zap'                                                                 pre-applypatch.sample     tugas9
 Nessus-10.8.3-ubuntu1604_amd64.deb             description                              'index(1)'                 pack-1d408dcd0ebc0ac18dd6251ec9e7184b231dee3c(1)(1).idx'   pre-commit.sample         update.sample
 Sample-SQL-File-100rows.sql                    dmde-4-2-2-816-lin64-gui                 'index(2)'                 pack-1d408dcd0ebc0ac18dd6251ec9e7184b231dee3c(1).idx'      pre-merge-commit.sample  'web poc'
 applypatch-msg.sample                          dmde-4-2-2-816-lin64-gui.zip             'jawaban modul 4 no 3.txt'  pack-1d408dcd0ebc0ac18dd6251ec9e7184b231dee3c(1).pack'   pre-push.sample
 arachni-1.6.1.3-0.6.1.1                        exclude                                   main                       pack-1d408dcd0ebc0ac18dd6251ec9e7184b231dee3c.idx          pre-rebase.sample
 arachni-1.6.1.3-0.6.1.1-linux-x86_64.tar.gz    fsmonitor-watchman.sample                 nmap                       pack-1d408dcd0ebc0ac18dd6251ec9e7184b231dee3c.pack         pre-receive.sample

┌──(asyrof㉿asyrof)-[~/Downloads]
└─$ cat HEAD
0000000000000000000000000000000000000000 b784b1bbfe02a81ddbf84ba1c6bc6c5c468f28d6 alamsyah <alamsyah.amra@gmail.com> 1690448519 +0800    clone: from https://git.simpel.web.id/simpel-development/antrian-online-web.git

┌──(asyrof㉿asyrof)-[~/Downloads]
└─$ cat config
[core]
        repositoryformatversion = 0
        filemode = false
        bare = false
        logallrefupdates = true
        symlinks = false
        ignorecase = true
[remote "origin"]
        url = https://git.simpel.web.id/simpel-development/antrian-online-web.git
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
        remote = origin
        merge = refs/heads/main

┌──(asyrof㉿asyrof)-[~/Downloads]
└─$ cat  packed-refs
# pack-refs with: peeled fully-peeled sorted
b784b1bbfe02a81ddbf84ba1c6bc6c5c468f28d6 refs/remotes/origin/main
c86941dc714bec61067644330a1799fc39d5f30f refs/remotes/origin/master

┌──(asyrof㉿asyrof)-[~/Downloads]
└─$
```

simrs.rsudsr.sulselprov.go.id

POC

penjelasan :

.git/HEAD

Ini adalah informasi tentang commit pertama setelah repositori Git di-clone dari URL yang diberikan. Commit tersebut mencatat waktu dan identitas pengguna yang melakukan clone serta sumber repositori yang digunakan.

```
┌──(asyrof㉿asyrof)-[~/Downloads]
└─$ cat HEAD
0000000000000000000000000000000000000000 b784b1bbfe02a81ddbf84ba1c6bc6c5c468f28d6 alamsyah <alamsyah.amra@gmail.com> 1690448519 +0800    clone: from https://git.simpel.web.id/simpel-development/antrian-online-web.git
```

.git/config

File konfigurasi ini mengatur repositori Git untuk berinteraksi dengan remote bernama origin yang terhubung ke URL https://git.simpel.web.id/simpel-development/antrian-online-web.git. Cabang lokal main dikonfigurasi untuk melacak cabang main di remote dan melakukan penggabungan otomatis saat melakukan git pull. Pengaturan lainnya mencakup pengelolaan file dan referensi di repositori lokal.

```
┌──(asyrof㉿asyrof)-[~/Downloads]
└─$ cat config
[core]
        repositoryformatversion = 0
        filemode = false
        bare = false
        logallrefupdates = true
        symlinks = false
        ignorecase = true
[remote "origin"]
        url = https://git.simpel.web.id/simpel-development/antrian-online-web.git
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
        remote = origin
        merge = refs/heads/main
```

simrs.rsudsr.sulselprov.go.id

POC

penjelasan :

File packed-refs

File packed-refs ini mencatat referensi untuk cabang-cabang yang ada di repositori Git, seperti origin/main dan origin/master, beserta ID commit yang terkait. Referensi-referensi ini dipaketkan untuk efisiensi penyimpanan dan akses, serta diurutkan dan diproses dalam cara tertentu (peeled, fully-peeled).

```
┌──(asyrof㉿asyrof)-[~/Downloads]
└─$ cat  packed-refs
# pack-refs with: peeled fully-peeled sorted
b784b1bbfe02a81ddbf84ba1c6bc6c5c468f28d6 refs/remotes/origin/main
c86941dc714bec61067644330a1799fc39d5f30f refs/remotes/origin/master

┌──(asyrof㉿asyrof)-[~/Downloads]
└─$
```

simrs.rsudsr.sulselprov.go.id

Saran Perbaikan dari web ini

Blokir Akses ke Direktori .git

Atur server untuk menolak akses publik ke direktori .git dengan menambahkan aturan di file konfigurasi server:

- Apache :

```
<DirectoryMatch "^/.*/\.git/">
    Order deny,allow
    Deny from all
</DirectoryMatch>
```

- Nginx :

```
location ~ /\.git {
    deny all;
}
```

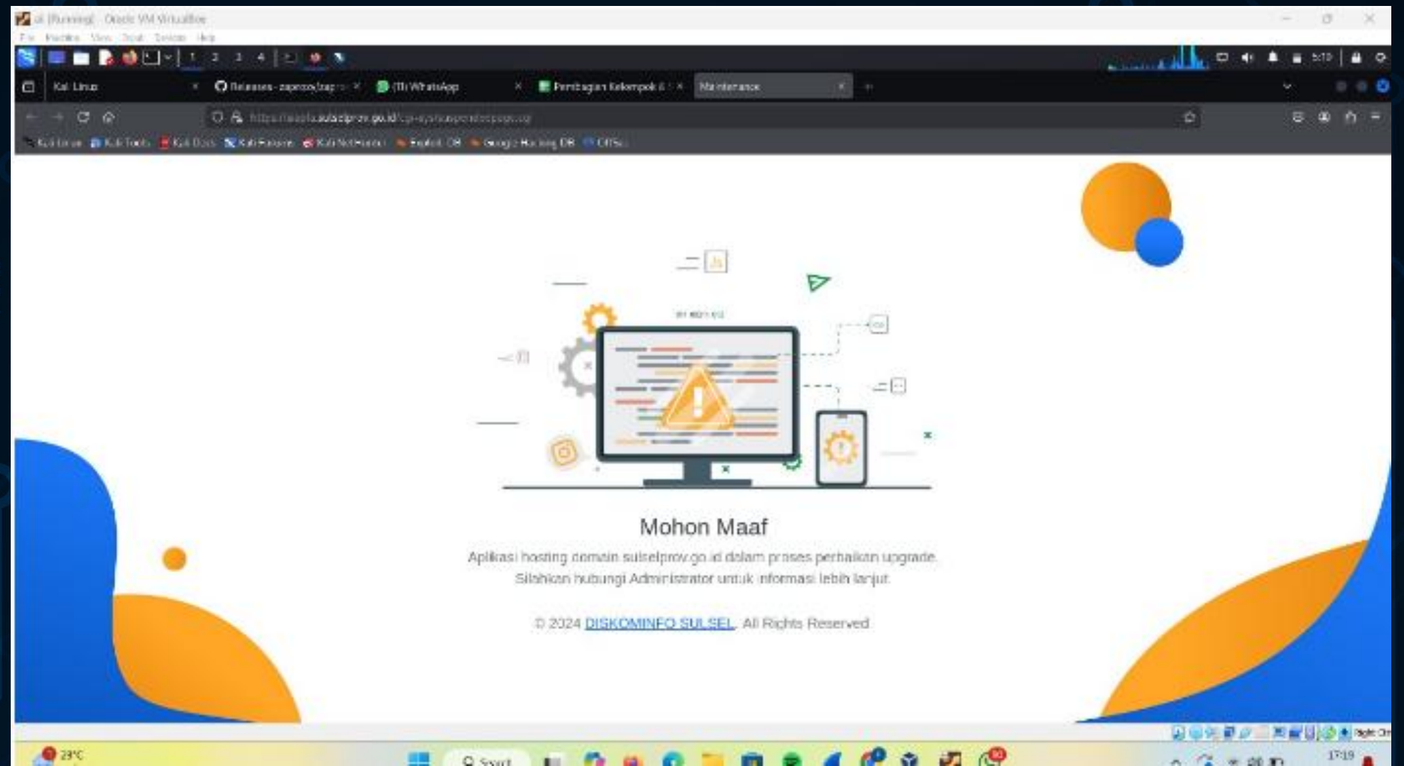
Program ini berfungsi untuk mencegah akses tidak sah ke folder .git di server web, sehingga kode sumber dan data sensitif tetap aman

- Tujuan: Aturan ini digunakan untuk mencegah publik mengakses direktori .git pada server Apache. Direktori .git adalah tempat penyimpanan riwayat perubahan kode dan file konfigurasi repositori Git yang dapat berisi informasi sensitif.

- Fungsi: Dengan aturan ini, Apache akan menolak akses ke direktori .git dari siapa saja yang mencoba mengaksesnya melalui web. Ini membantu menghindari potensi risiko keamanan, di mana penyerang bisa mengeksploitasi repositori Git yang terakses untuk mendapatkan informasi sensitif (misalnya, kredensial atau API keys).

siapla.sulselprov.go.id

Situs SIAPLA (Sistem Informasi Administrasi dan Pelaporan) Pemerintah Provinsi Sulawesi Selatan kemungkinan merupakan platform yang digunakan untuk mengelola administrasi pemerintahan, seperti pengelolaan anggaran, pelaporan kinerja, dan pemantauan proyek-proyek pemerintah. Sistem ini bertujuan untuk meningkatkan transparansi, akuntabilitas, dan efisiensi dalam pelaksanaan kegiatan pemerintahan di provinsi tersebut.



siapla.sulselprov.go.id

Berikut ini hasil Scanning Web

```
┌──(root㉿aldi)-[/home/aldiputra/rapidscan]
└─# nikto -h siapla.sulselprov.go.id -ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          103.151.191.12
+ Target Hostname:    siapla.sulselprov.go.id
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=siapla.sulselprov.go.id
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/ST=TX/L=Houston/O=cPanel, Inc./CN=cPanel, Inc. Certification Authority
+ Start Time:         2024-12-01 10:40:53 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache
+ /: Cookie ci_session created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerability. Previous versions contain other non-descript vulnerabilities.
+ /securecontrolpanel/: Web Server Control Panel.
+ /webmail/: Web based mail package installed.
+ : Server banner changed from 'Apache' to 'imunify360-webshield/1.21'.
+ /phpping/index.php?pingto=www.test.com%20|%20dir%20c:\\: Uncommon header 'cf-edge-cache' found, with contents: no-cache.
+ /cgi-bin/sbcgi/sitebuilder.cgi: SITEBUILDER v1.4 may allow retrieval of any file. With a valid username and password, request: /<CGIDIR>/sbcgi/sitebuilder.cgi?username=<user>&password=<password>&selectedpage=../../../../../../../../../../etc/passwd. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0756
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: Connect failed: ; Connection timed out at /var/lib/nikto/plugins/LW2.pm line 5254.
: Connection timed out
+ Scan terminated: 20 error(s) and 11 item(s) reported on remote host
+ End Time:           2024-12-01 10:53:57 (GMT-5) (784 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

siapla.sulselprov.go.id

lList Vulnerability

Rangkuman Kerentanan Utama:

1. Cookie ci_session tidak aman
2. Header HTTP keamanan tidak dikonfigurasi: X-Frame-Options, Strict-Transport-Security, dan X-Content-Type-Options.
3. Versi software rentan: Il0hamail 0.8.10 dan SITEBUILDER v1.4.

siapla.sulselprov.go.id

Berikut SSL Report dari web ini

siapla.sulselprov.go.id

Saran Perbaikan

Perbaikan:

- Tambahkan header HTTP keamanan:
  - Strict-Transport-Security
  - X-Frame-Options
  - X-Content-Type-Options
- Konfigurasi cookie dengan flag Secure.
- Perbarui software yang rentan (Webmail dan SITEBUILDER).
- Pantau log server untuk aktivitas mencurigakan.
- Lakukan audit keamanan berkala dengan tools seperti Nikto, OpenVAS, atau Nessus.

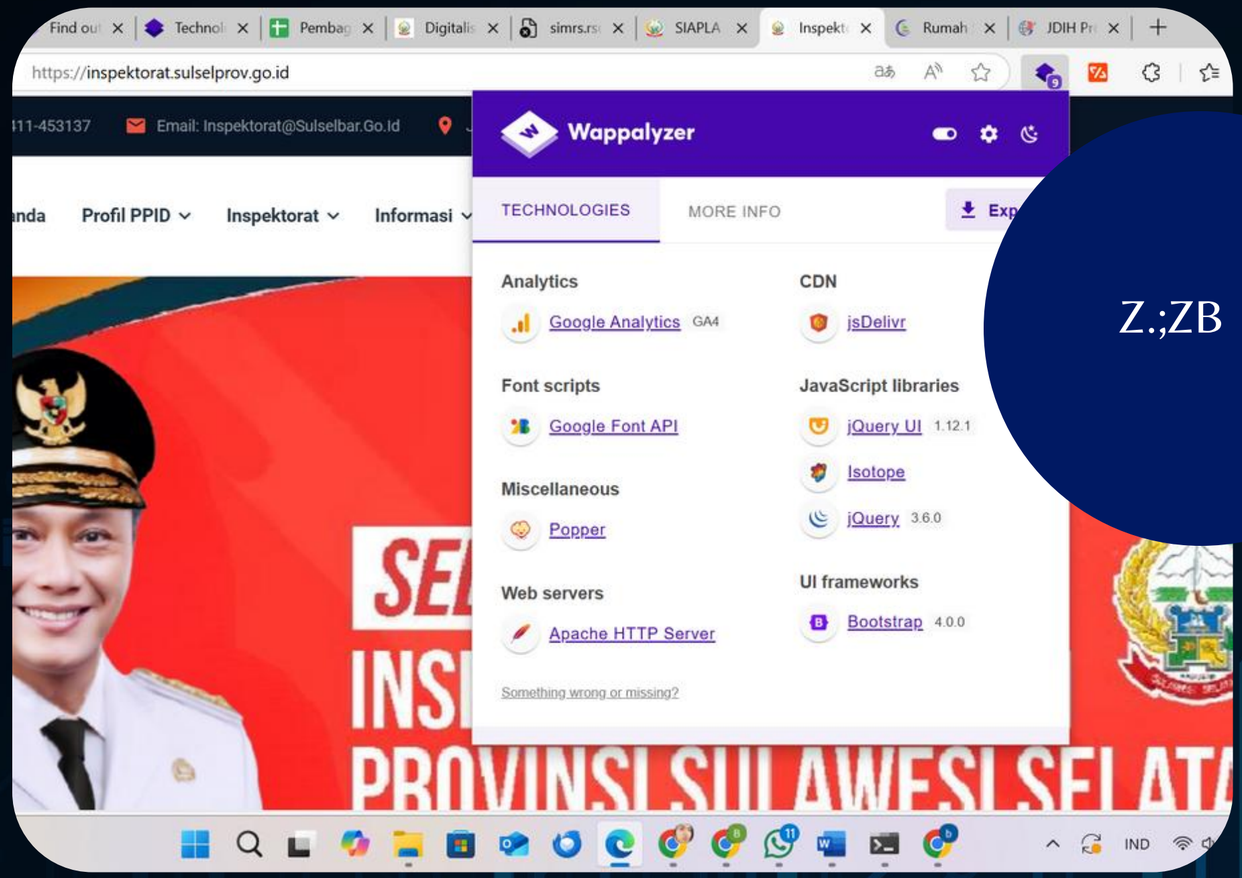
kelompok 2

Inspektorat.sulselprov.go.id

Website Inspektorat Daerah Provinsi Sulawesi Selatan berfungsi sebagai sarana utama untuk mewujudkan transparansi, komunikasi, dan pengawasan di lingkup pemerintahan daerah. Dengan fitur-fitur seperti informasi publik, layanan pengaduan, dan dokumentasi, website ini membantu masyarakat memahami serta berpartisipasi dalam pengawasan penyelenggaraan pemerintahan.

kelompok 2

Inspektorat.sulselprov.go.id



Z.;ZB L

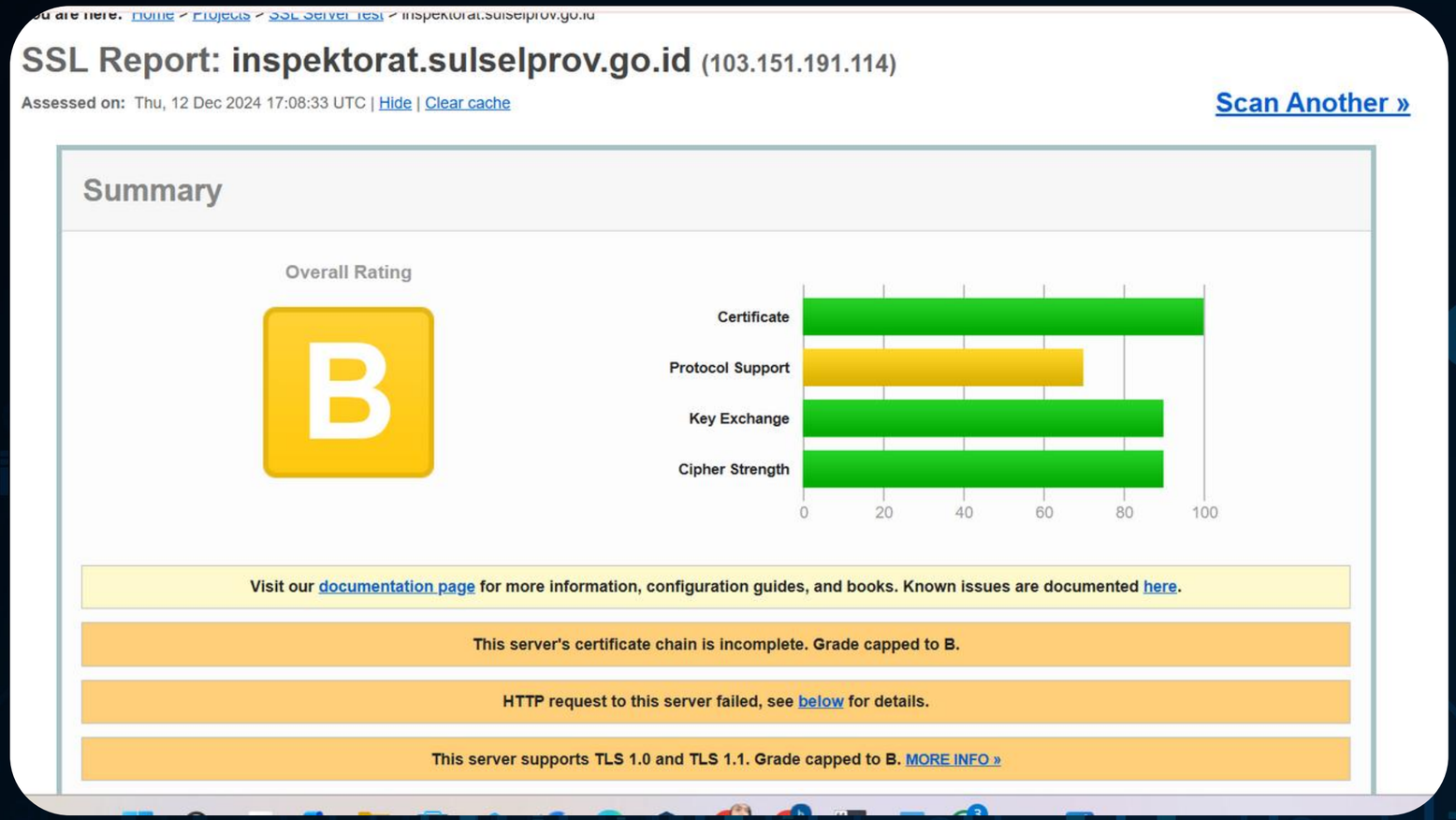
Teknologi yang digunakan dan diperoleh melalui tools Wappalyzer.

1. **Analytics : Google Analytics (GA4)**
2. **Font Scripts : Google Font API**
3. **Miscellaneous : Popper**
4. **Web Servers : Apache HTTP Server**
5. **CDN (Content Delivery Network) : jsDelivr**
6. **JavaScript Libraries : jQuery UI (v1.12.1), Isotope, jQuery (3.6.0)**
7. **UI Frameworks : Bootstrap (v4.0.0)**

kelompok 2

Inspektorat.sulselprov.go.id

Hasil Report SSL

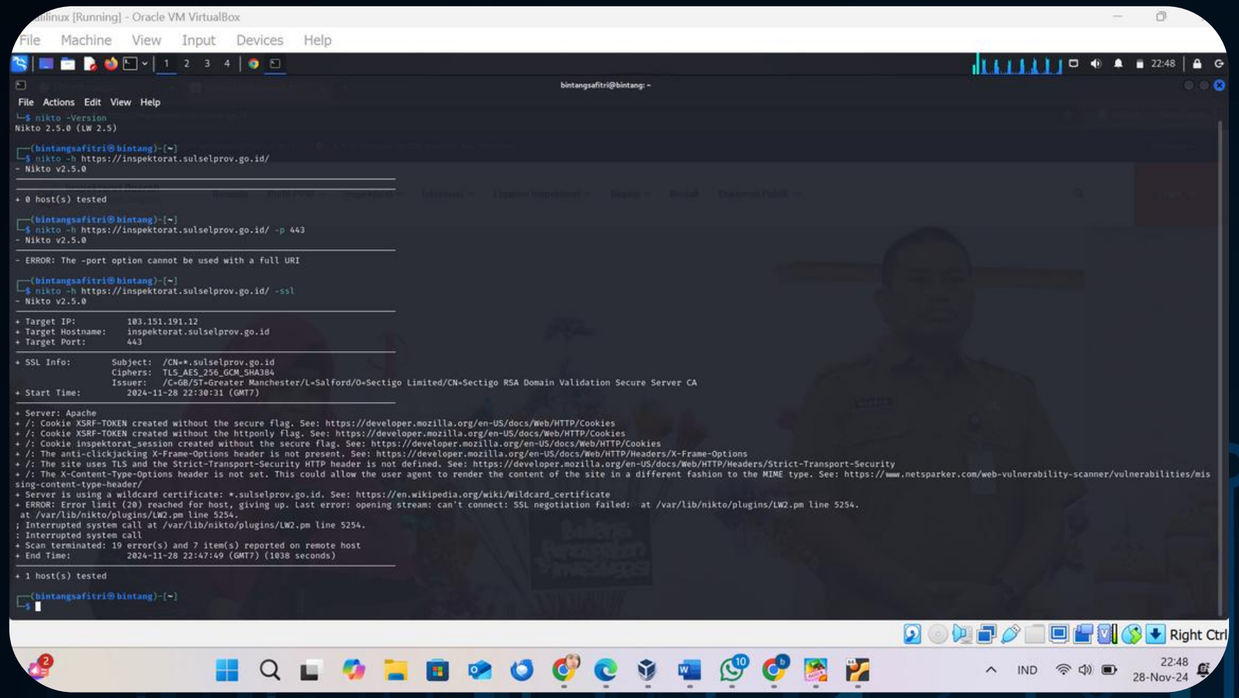


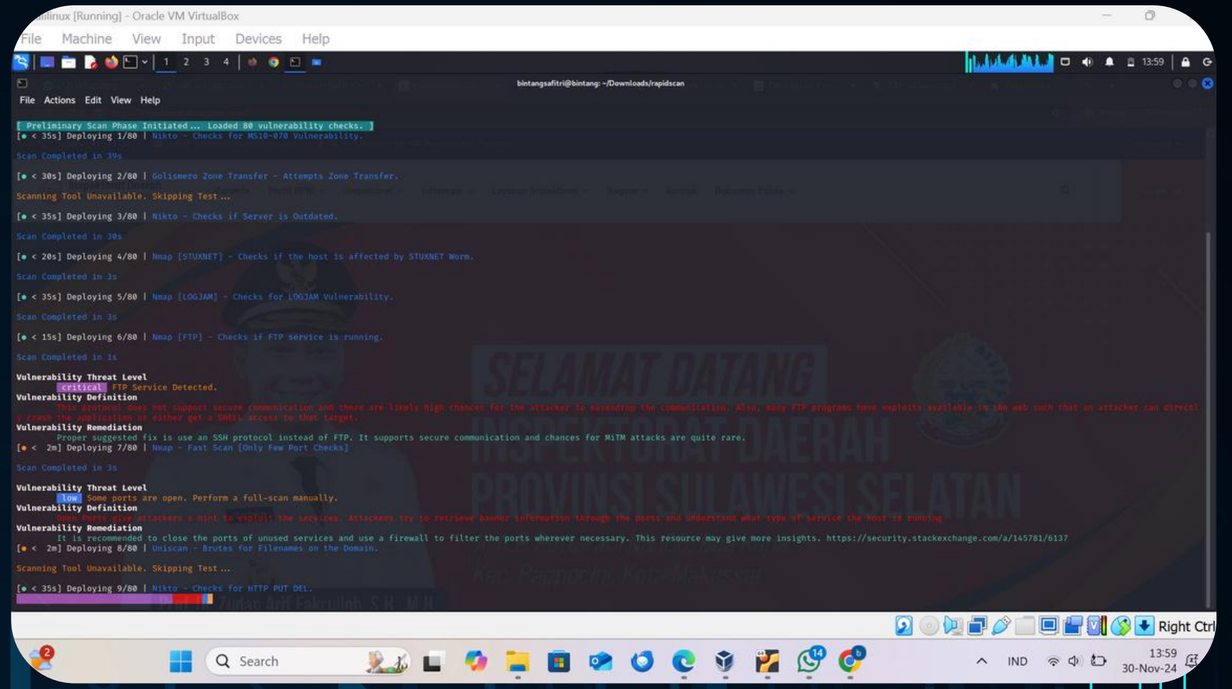
Rating keseluruhan adalah B, yang berarti situs ini memiliki tingkat keamanan yang cukup baik, tetapi masih ada beberapa masalah konfigurasi yang perlu diperbaiki.

kelompok 2

Inspektorat.sulselprov.go.id

Hasil Vulnerability Scanners





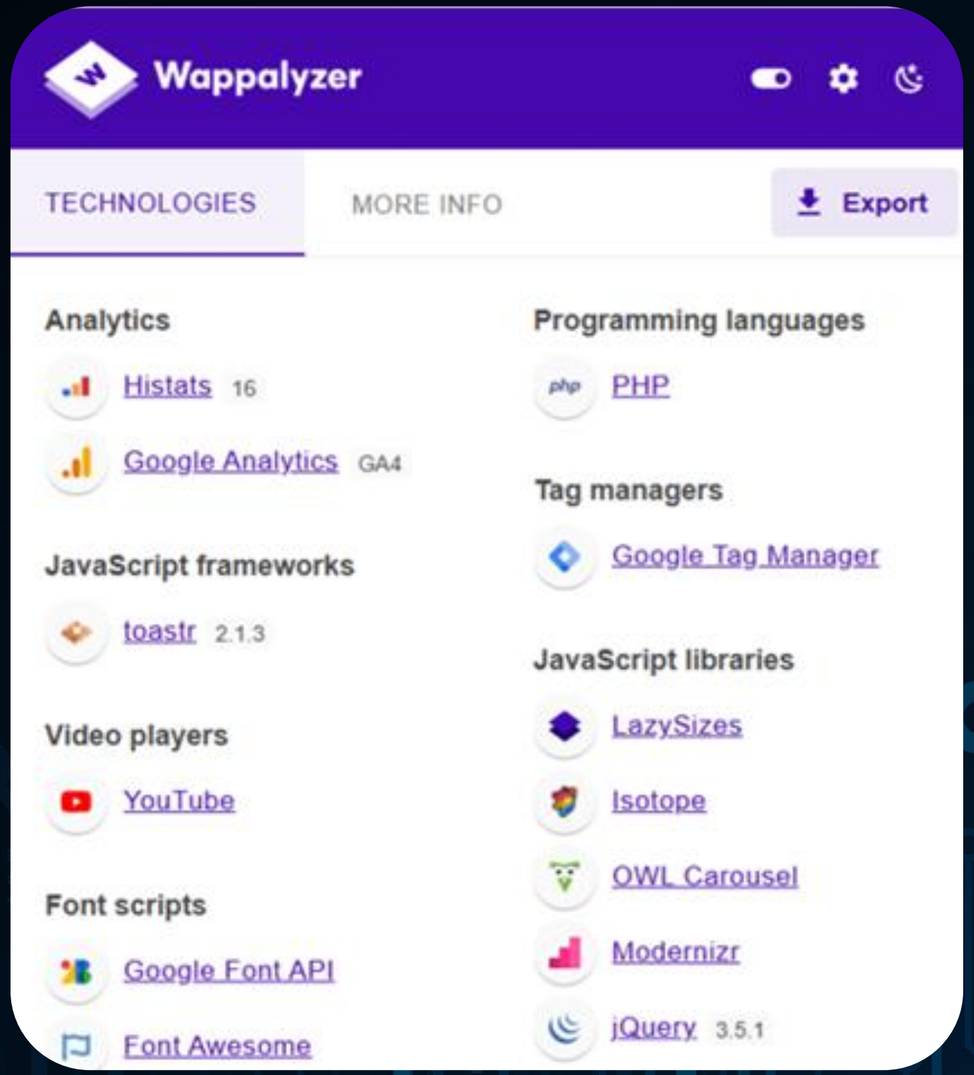
kelompok 2

rskddadi.sulselprov.go.id

Rumah sakit khusus di Provinsi Sulawesi Selatan adalah fasilitas pelayanan kesehatan yang dirancang untuk memberikan perawatan medis kepada pasien dengan kondisi atau penyakit tertentu, baik itu penyakit kronis, gangguan mental, rehabilitasi, atau perawatan yang membutuhkan keahlian medis spesifik. Rumah sakit ini biasanya dilengkapi dengan peralatan medis canggih dan tenaga medis yang terlatih di bidangnya, seperti spesialis, dokter, perawat, dan profesional kesehatan lainnya.

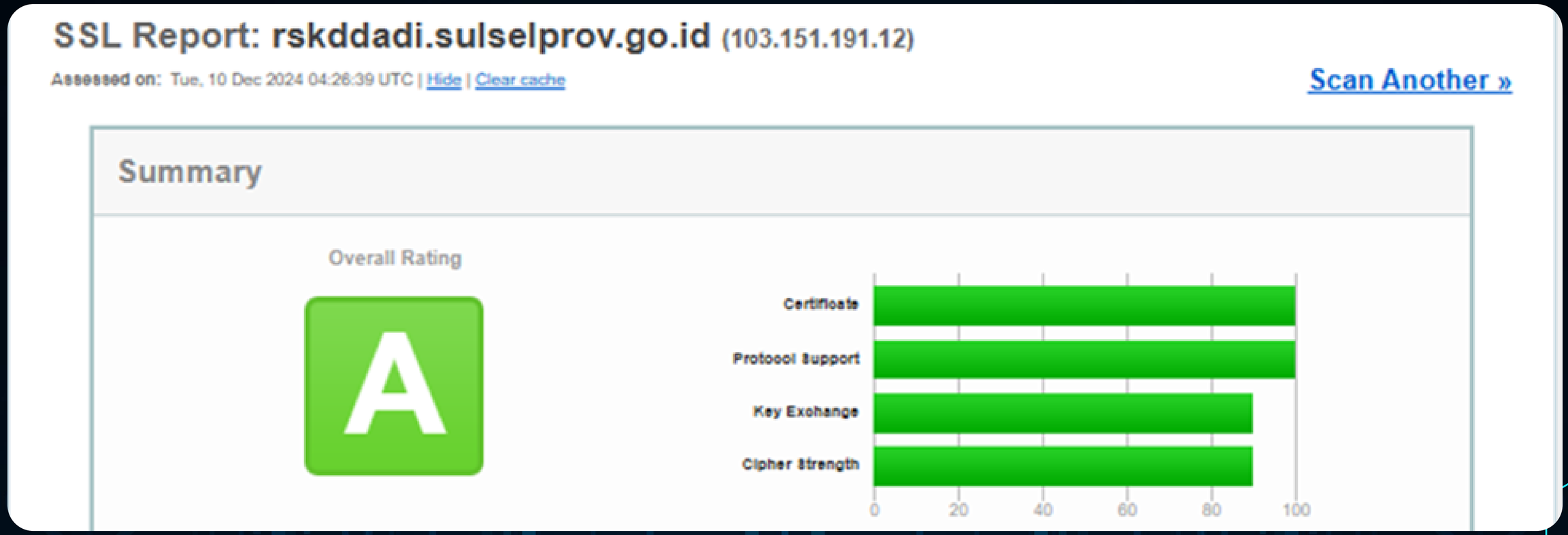
kelompok 2

Teknologi Yang Digunakan



kelompok 2

Hasil Report SSL

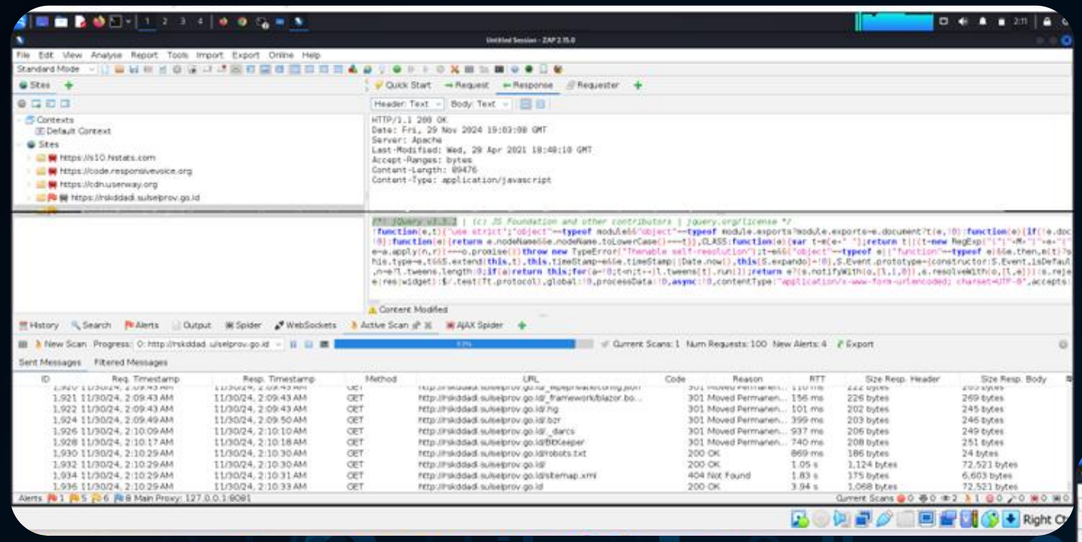


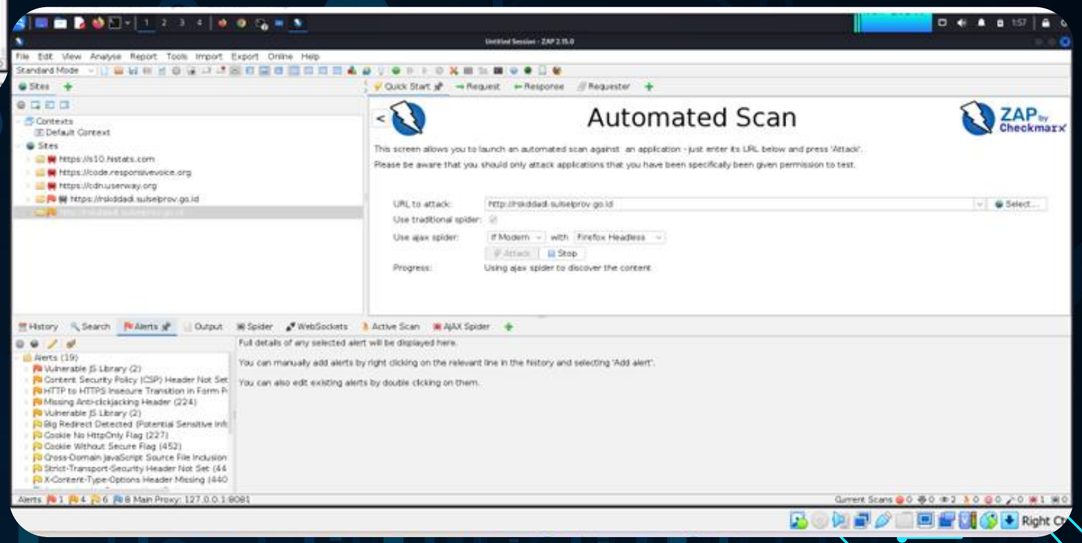
- **Overall Rating : A (ditampilkan dalam kotak hijau besar).**

Ini berarti konfigurasi SSL/TLS pada server dianggap aman dan memenuhi standar keamanan yang baik.

kelompok 2

Hasil ScanningVulnerability





List Vulnerability

a)**Vulnerability & Library**
b)**Cross-Domain JavaScript Source File Inclusion**
c)**X-Content-Type-Options Header Missing**

Saran Perbaikan

1. Vulnerable JavaScript Library
   1. Risiko: Pustaka JS yang rentan dapat dimanfaatkan untuk serangan.
   2. Solusi:

a) Perbarui pustaka JavaScript ke versi terbaru yang telah diperbaiki.

b) Gunakan tools seperti npm audit atau Snyk untuk memeriksa kerentanan.

c) Contoh perintah:

npm update <library-name>

npm audit fix

Saran Perbaikan

2. X-Content-Type-Options Header Missing

1. **Risiko: Browser dapat melakukan MIME-sniffing yang menyebabkan interpretasi file berbahaya.**
2. **Solusi:**

a) Tambahkan header X-Content-Type-Options dengan nilai nosniff untuk mencegah sniffing.

b) Contoh:

X-Content-Type-Options: nosniff

Saran Perbaikan

3. Cross-Domain JavaScript Source File Inclusion

1. **Risiko: Skrip dari domain eksternal dapat dimanipulasi, berpotensi menyebabkan Cross-Site Scripting (XSS).**
2. **Solusi:**

a) Batasi pemuatan skrip hanya dari sumber tepercaya menggunakan Content Security Policy (CSP).

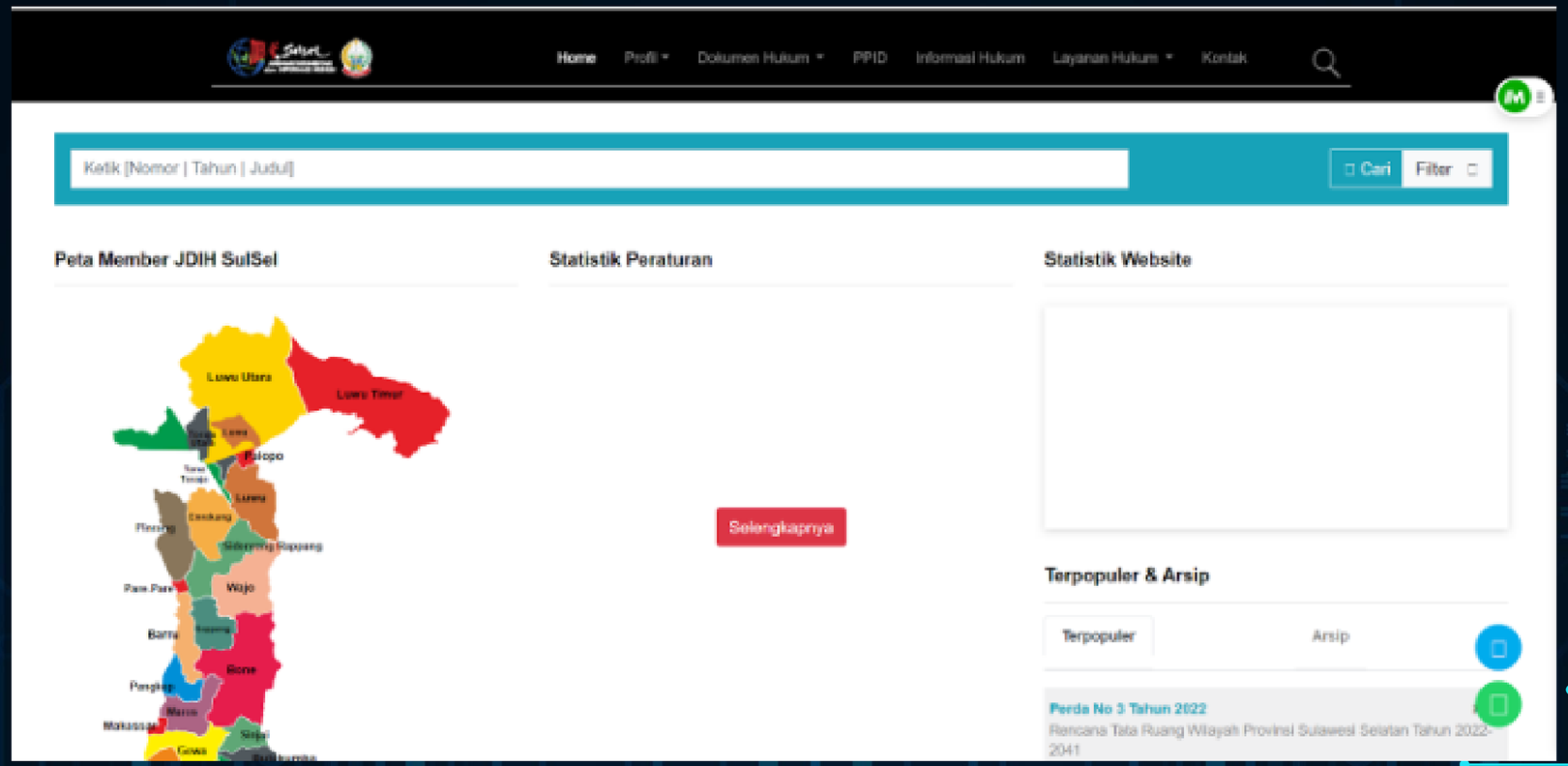
b) Contoh CSP:

Content-Security-Policy: script-src 'self' https://trusted-source.com

kelompok 2

jdih.sulselprov.go.id

Situs JDIH Sulawesi Selatan (http://jdih.sulselprov.go.id) adalah portal yang menyediakan akses terhadap dokumen hukum yang diterbitkan oleh pemerintah daerah, seperti peraturan daerah, keputusan gubernur, dan peraturan lainnya. Tujuannya adalah untuk mempermudah masyarakat dan pihak terkait dalam mengakses informasi hukum, meningkatkan transparansi, dan menyebarkan peraturan secara lebih efektif.



kelompok 2

jdih.sulselprov.go.id

Hasil Scan web menggunakan PentestTools

A. medium

1. Insecure Cookie Setting: Missing Secure Flag (tidak ada Secure flag)
2. Insecure Cookie Setting: Missing HttpOnly Flag (tidak ada HttpOnly flag)
3. Vulnerabilities in Server-Side Software

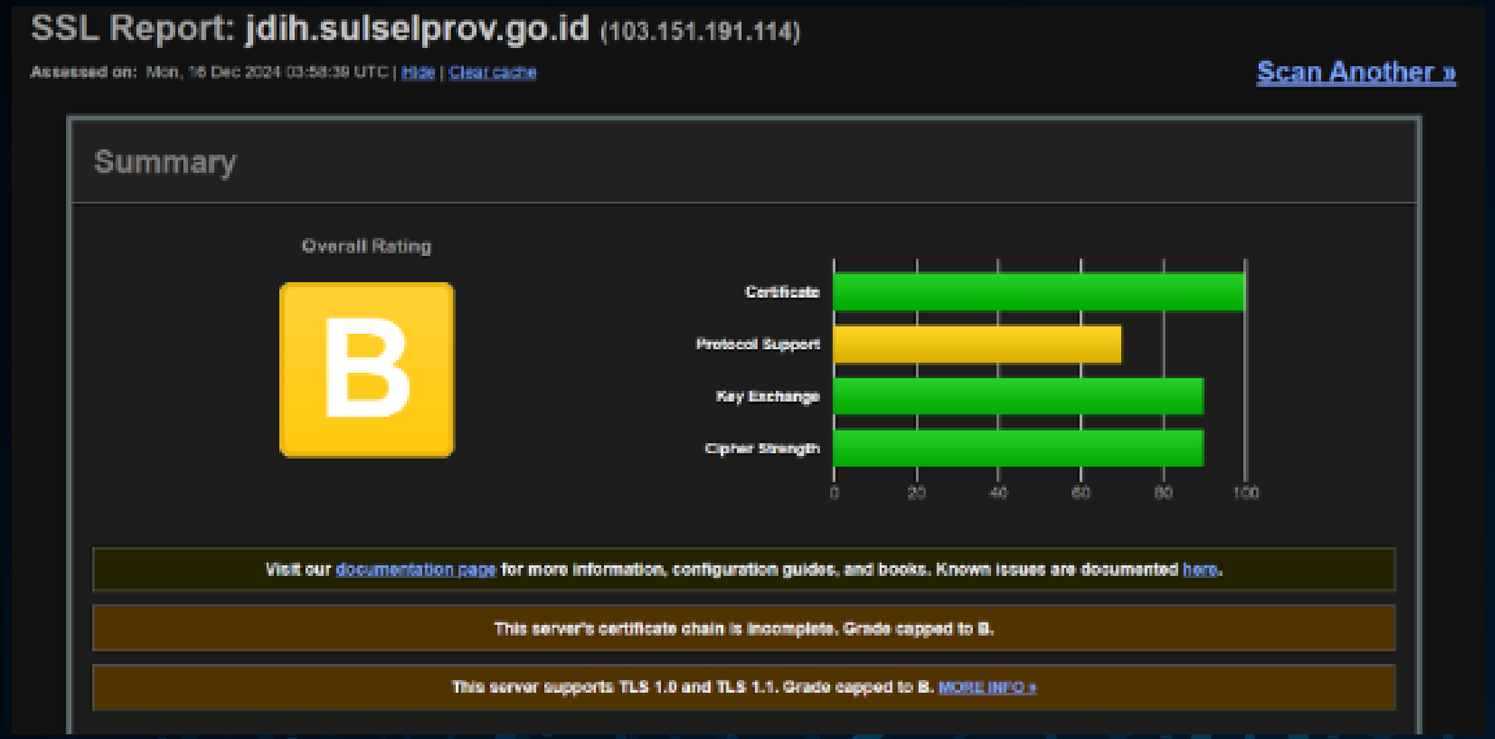
B. low

1. Missing security header: Strict-Transport-Security
2. Missing security header: Content-Security-Polic
3. Missing security header: Referrer-Policy
4. Missing security header: X-Content-Type-Options
5. Server software and technology found

kelompok 2

jdih.sulselprov.go.id

Hasil SSL Report



- Overall Rating: B
- Permasalahan:
- Sertifikat tidak lengkap (Certificate Chain Incomplete).
- Masih mendukung TLS 1.0 dan TLS 1.1.
- Rekomendasi:
- Lengkapi sertifikat.
- Nonaktifkan protokol lama, gunakan TLS 1.2/1.3.
- Tujuan: Meningkatkan keamanan dan peringkat ke A

kelompok 2

jdih.sulselprov.go.id

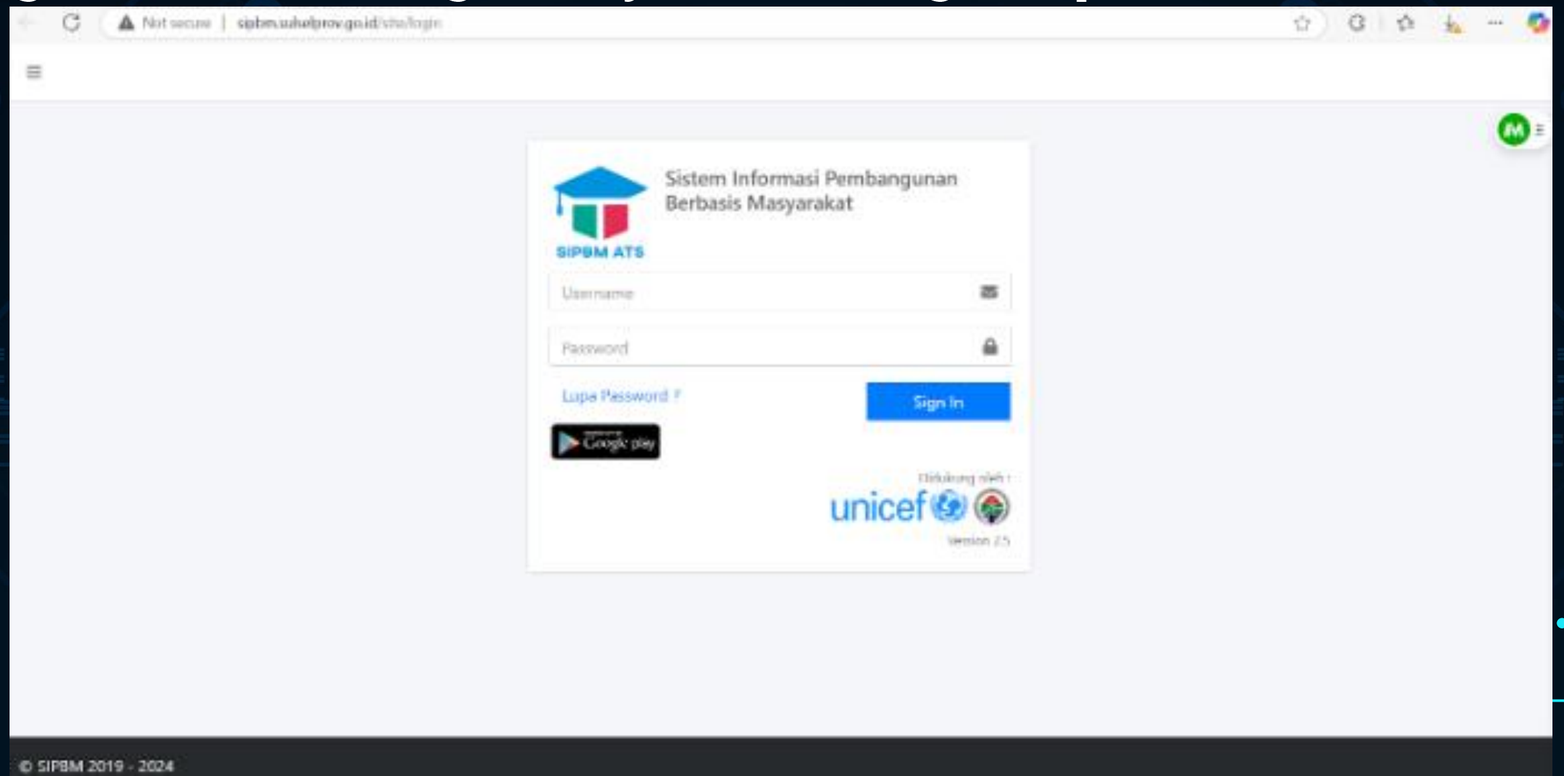
Saran Perbaikan dari web ini

- Pastikan cookie yang mengandung informasi sensitif selalu dikirim melalui saluran terenkripsi
- Tambahkan flag Secure pada cookie
- Tambahkan flag HttpOnly pada semua cookie untuk mencegah akses melalui skrip sisi klien
- Periksa versi perangkat lunak yang terpasang
- Perbarui ke versi terbaru
- Pertimbangkan penghapusan atau penggantian komponen yang sudah tidak didukung
- Tambahkan header HSTS
- Gunakan sintaks: Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]
- Nilai max-age disarankan di atas 7776000 detik
- Tambahkan header Referrer-Policy
- Pertimbangkan pengaturan no-referrer untuk mencegah pelacakan
- Tambahkan header X-Content-Type-Options: nosniff

kelompok 2

sipbm.sulselprov.go.id

SIPBM (Sistem Informasi Pengadaan Barang dan Jasa) Pemerintah Provinsi Sulawesi Selatan adalah platform yang digunakan untuk memfasilitasi proses pengadaan barang dan jasa secara elektronik. Tujuan adalah meningkatkan transparansi, efisiensi, dan akuntabilitas dalam pengadaan barang dan jasa di tingkat pemerintahan.



kelompok 2

sipbm.sulselprov.go.id

Hasil sacnning web menggunkan Pentest tools

High

1. Vulnerabilities found for server-side software

Medium

1. Insecure cookie setting: missing Secure flag
2. Communication is not secure

low

1. Missing security header: Referrer-Policy
2. Missing security header: Content-Security-Policy
3. Missing security header: X-Content-Type-Options
4. Missing security header: X-Content-Type-Options
5. Robots.txt file found

kelompok 2

sipbm.sulselprov.go.id

Saran Perbaikan dari web ini

1. Perbarui NGINX dan komponen lain ke versi terbaru.
2. Implementasikan SSL/TLS (HTTPS) untuk komunikasi aman.
3. Konfigurasi cookie dengan atribut Secure dan HttpOnly.
4. Perbarui Bootstrap ke versi terbaru untuk mencegah kerentanan XSS.
5. Lakukan audit rutin terhadap sistem untuk mendeteksi komponen usang atau rentan.

Kelompok 2

TERIMA KASIH