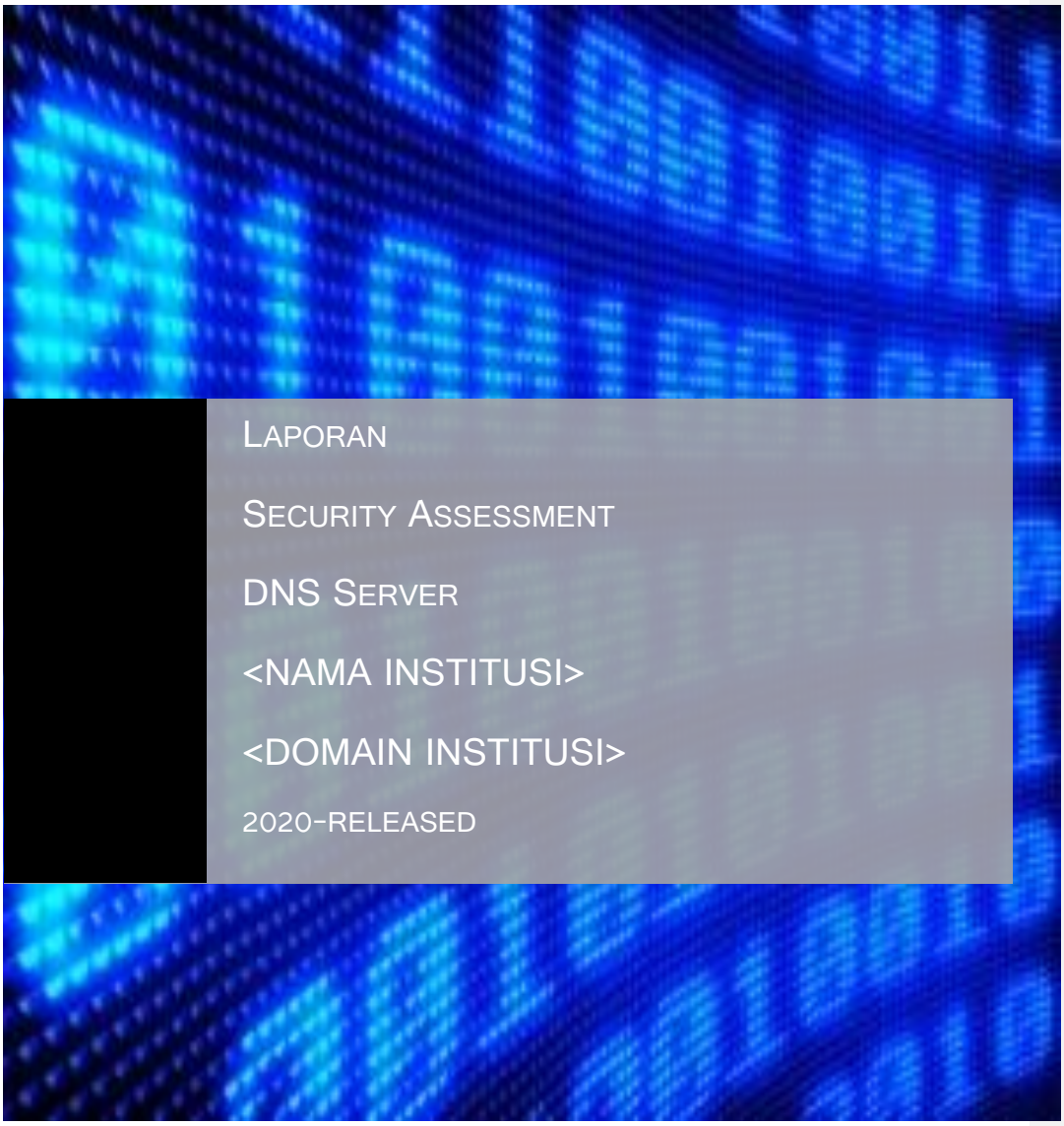


LAPORAN

SECURITY ASSESSMENT

DNS SERVER

<NAMA INSTITUSI>

<DOMAIN INSTITUSI>

2020-RELEASED

Oleh:

Tim CSIRT.ID

Keterangan Dokumen

Title	*Security Assessment DNS Server*
Version	*2020-RELEASED*
Author	*Tim Pondok Siber*
Auditor	*Ahmad Nazir Arrobi*
Reviewed By	*Ahmad Nazir Arrobi*
Approved By	
Document Classification	***Confidential/Sangat Rahasia***

Catatan Revisi

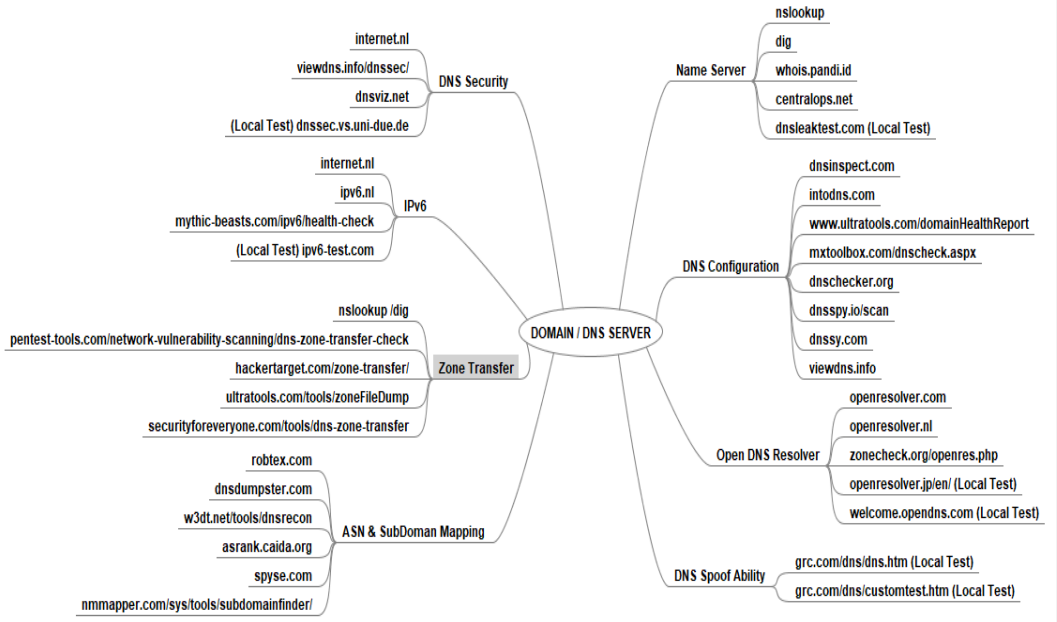
Version	***Date***	***Author***	***Description***

Daftar Isi

A. Executive Summary

Tim Indeks kerentanan Pondok Siber telah melakukan Penilaian terhadap konfigurasi dasar DNS Server pada domain prakerja.go.id sesuai dengan sesuai dengan standar Internet Engineering Task Force (IETF) RFC 1035 https://www.ietf.org/rfc/rfc1035.txt

Berikut adalah bagan proses pengujian DNS Server dengan menggunakan INDONESE Assessment Framework 2020-RELEASED



Hasil Penilaian		
No	**Kondisi eksisting Konfigurasi DNS Server**	**Hasil**
1	Name Server	✓
2	DNS Configuration	✗
3	DNS Security Test	✗
4	IPv6 Test	✓
5	Open DNS Resolver Test	✗
6	Zone Transfer DNS Server Test	✓
7	AS Number & Sub-Domain Mapping	✗
8	DNS Spoofability Test (Optional) – Tidak dilakukan pengujian	--

Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Bandung, 25 Desember 2021

Ahmad Nazir Arrobi
Team Member

B. Proses Audit Domain dan DNS Server

B.1. Name Server		
Tujuan : Untuk mengetahui informasi umum tentang Name Server pada domain prakerja.go.id , antara lain : • Tanggal dibuat, expire dan update domain terakhir, • Registrant Contact/Admin Contact/Technical Contact/Billing Contact, Registrar. • Name Server dan DNS Record • Grafik Route Domain		
Tools : http://centralops.net/ dan https://dnsdumpster.com/		
Hasil Penilaian dan Rekomendasi		
No	**Kondisi eksisting DNS dan Infrastruktur**	**Hasil**
1	Terdapat 2 atau lebih Name Server yang bersesuaian dengan domain dan atau Memiliki Backup Name Server pada network atau domain berbeda.	✓
	Rekomendasi :	
CVSS:3.0/		

Keterangan :

Commented [an1]:

✓ : Konfigurasi sudah bersesuaian dengan best practice

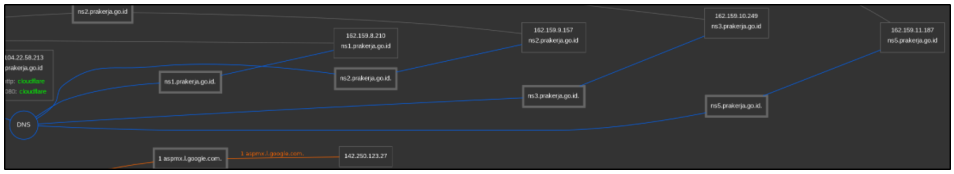
✗ : Terdapat ketidaksesuaian konfigurasi

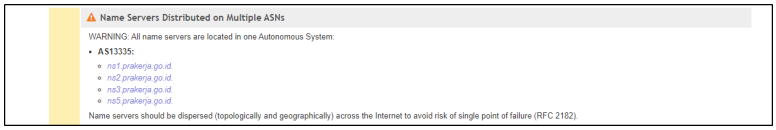
Proses Pengujian :

1. https://centralops.net

2. https://dnsdumpster.com

```
                                                    2232ADC8C2381A2895A5100E8020FABF
prakerja.go.id                          IN    NS    ns5.prakerja.go.id              86400s  (1.00:00:00)
prakerja.go.id                          IN    NS    ns1.prakerja.go.id              86400s  (1.00:00:00)
prakerja.go.id                          IN    NS    ns2.prakerja.go.id              86400s  (1.00:00:00)
prakerja.go.id                          IN    NS    ns3.prakerja.go.id              86400s  (1.00:00:00)
145.12.67.172.in-addr.arpa              IN    HINFO CPU: RFC8482                    3789s  (01:03:09)
                                                    OS:
```



B.2. DNS Configuration		
Tujuan : Untuk mengetahui dan menilai sejauh mana penerapan konfigurasi DNS Server dan implementasinya pada domain prakerja.go.id sesuai dengan standar Internet Engineering Task Force (IETF) RFC 1035 https://www.ietf.org/rfc/rfc1035.txt		
Tools : http://www.dnsinspect.com/		
Hasil Penilaian dan Rekomendasi		
No	**Konfigurasi yang tidak bersesuaian**	**Hasil**
1	Temuan 1 :  	✗
	Rekomendasi :Mengasosiasikan ke lebih dari satu ASN (Referensi: RFC 2182	
CVSS:3.0/		

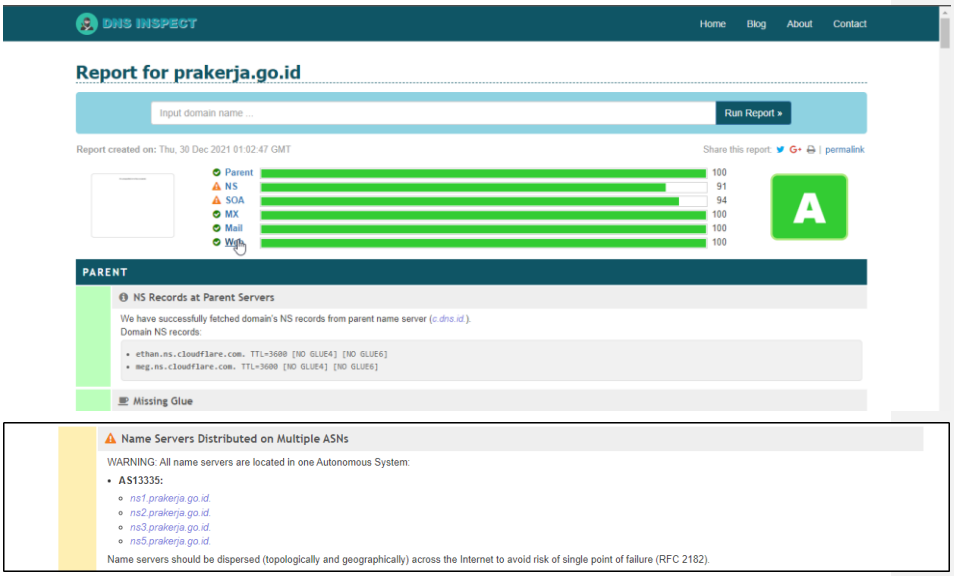
Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

1. **http://dnsinspect.com**


DNS INSPECT
Home
Blog
About
Contact
Report for prakerja.go.id
Input domain name ...
Run Report »
Report created on: Thu, 30 Dec 2021 01:02:47 GMT
Share this report: permalink
Parent 100
NS 91
SOA 94
MX 100
Mail 100
Web 100
A
PARENT
NS Records at Parent Servers
We have successfully fetched domain's NS records from parent name server (c.dns.id.).
Domain NS records:
ethan.ns.cloudflare.com. TTL=3600 [NO GLUE4] [NO GLUE6]
meg.ns.cloudflare.com. TTL=3600 [NO GLUE4] [NO GLUE6]
Missing Glue
Name Servers Distributed on Multiple ASNs
WARNING: All name servers are located in one Autonomous System:
AS13335:
ns1.prakerja.go.id.
ns2.prakerja.go.id.
ns3.prakerja.go.id.
ns5.prakerja.go.id.
Name servers should be dispersed (topologically and geographically) across the Internet to avoid risk of single point of failure (RFC 2182).

B.3. DNS Security Test		
Tujuan : Untuk mengetahui apakah DNS Server yang digunakan sudah menerapkan DNS Security.		
Tools : https://internet.nl,		
Hasil Penilaian dan Rekomendasi		
No	**Konfigurasi yang tidak bersesuaian**	**Hasil**
1	**DNSSEC signed**	✗
2	**DNSSEC validity**	✗
Rekomendasi : Memberikan DNSSEC signed dan validity		
CVSS:3.0/		

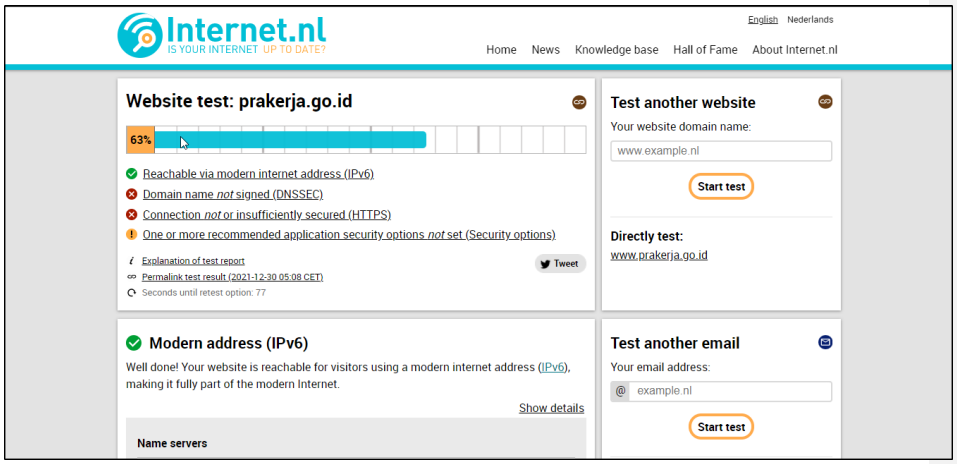
Keterangan :

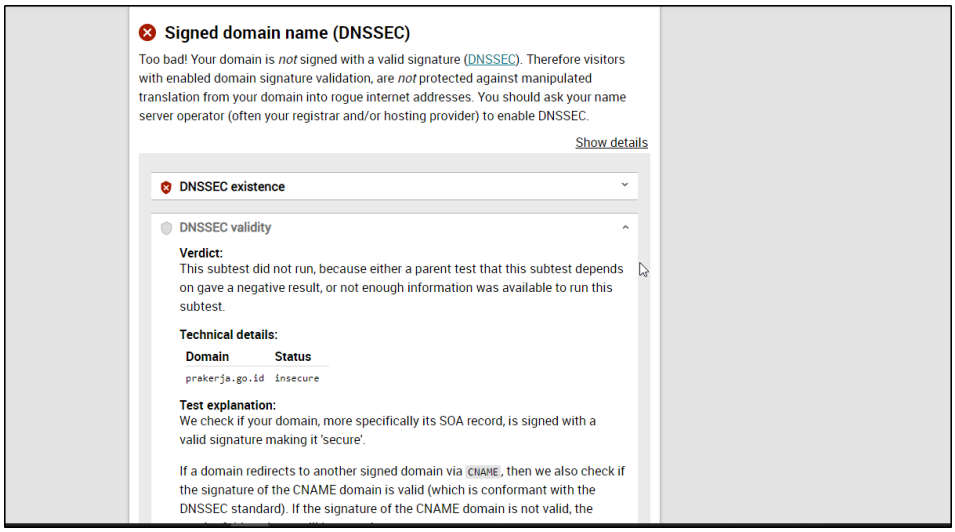
✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

1. **https://internet.nl/**


Internet.nl
IS YOUR INTERNET UP TO DATE?
English Nederlands
Home News Knowledge base Hall of Fame About Internet.nl
Website test: prakerja.go.id
63%
Reachable via modern internet address (IPv6)
Domain name not signed (DNSSEC)
Connection not or insufficiently secured (HTTPS)
One or more recommended application security options not set (Security options)
Explanation of test report
Permalink test result (2021-12-30 05:08 CET)
Seconds until retest option: 77
Tweet
Test another website
Your website domain name:
www.example.nl
Start test
Directly test:
www.prakerja.go.id
Modern address (IPv6)
Well done! Your website is reachable for visitors using a modern internet address (IPv6), making it fully part of the modern Internet.
Show details
Name servers
Test another email
Your email address:
@ example.nl
Start test


Signed domain name (DNSSEC)
Too bad! Your domain is not signed with a valid signature (DNSSEC). Therefore visitors with enabled domain signature validation, are not protected against manipulated translation from your domain into rogue internet addresses. You should ask your name server operator (often your registrar and/or hosting provider) to enable DNSSEC.
Show details
DNSSEC existence
DNSSEC validity
Verdict:
This subtest did not run, because either a parent test that this subtest depends on gave a negative result, or not enough information was available to run this subtest.
Technical details:
Domain Status
prakerja.go.id insecure
Test explanation:
We check if your domain, more specifically its SOA record, is signed with a valid signature making it 'secure'.
If a domain redirects to another signed domain via CNAME, then we also check if the signature of the CNAME domain is valid (which is conformant with the DNSSEC standard). If the signature of the CNAME domain is not valid, the

B.4. Ipv6 Test		
Tujuan : Untuk mengetahui apakah DNS Server yang digunakan pada domain prakerja.go.id sudah menerapkan Ipv6.		
Tools : https://internet.nl		
Hasil Penilaian dan Rekomendasi		
No	**Konfigurasi yang tidak bersesuaian**	**Hasil**
1	**IPv6 addresses for name servers**	✓
2	**IPv6 reachability of name servers**	✓
Rekomendasi :		
CVSS:3.0/		

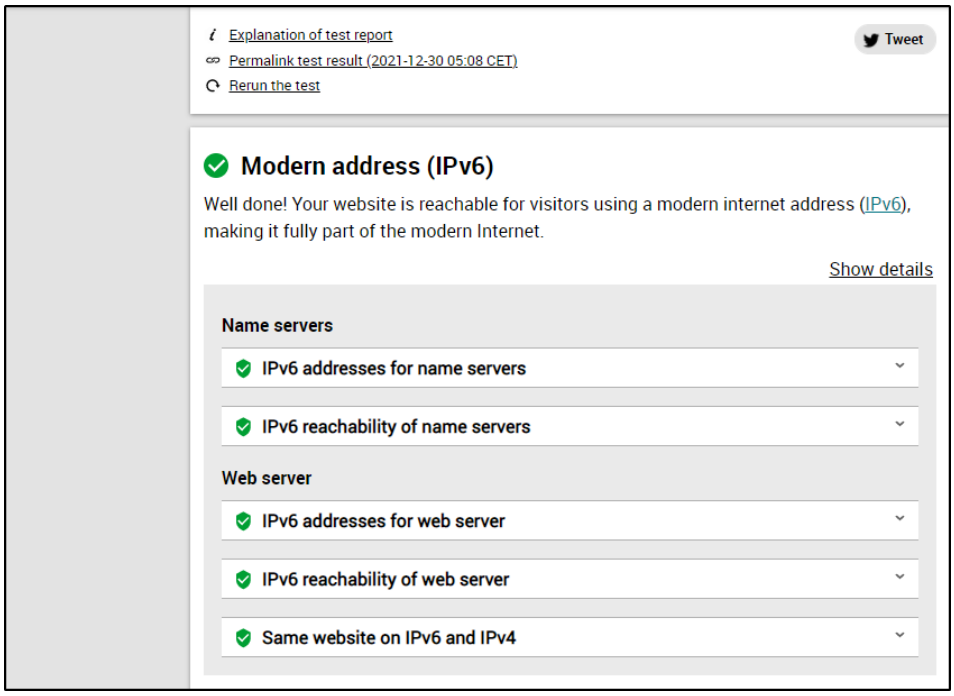
Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

1. https://internet.nl/


Explanation of test report
Permalink test result (2021-12-30 05:08 CET)
Rerun the test
Tweet
Modern address (IPv6)
Well done! Your website is reachable for visitors using a modern internet address (IPv6), making it fully part of the modern Internet.
Show details
Name servers
IPv6 addresses for name servers
IPv6 reachability of name servers
Web server
IPv6 addresses for web server
IPv6 reachability of web server
Same website on IPv6 and IPv4

B.5. Open DNS Resolver Test		
Tujuan : Untuk mengetahui apakah DNS Server yang digunakan pada domain prakerja.go.id memiliki konfigurasi “Open DNS” Referensi : https://www.us-cert.gov/ncas/alerts/TA13-088A		
Tools : http://openresolver.com/		
Hasil Penilaian dan Rekomendasi		
No	**Name Server Open DNS**	**Hasil**
1	162.159.8.210	✗
2	162.159.9.157	✗
3	162.159.10.249	✗
4	---.---.---.---	-
5	162.159.11.187	✗
Rekomendasi :		
CVSS:3.0/		

Keterangan :

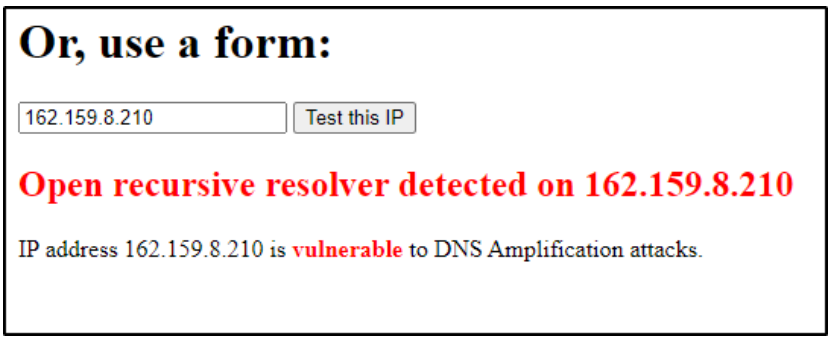
✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

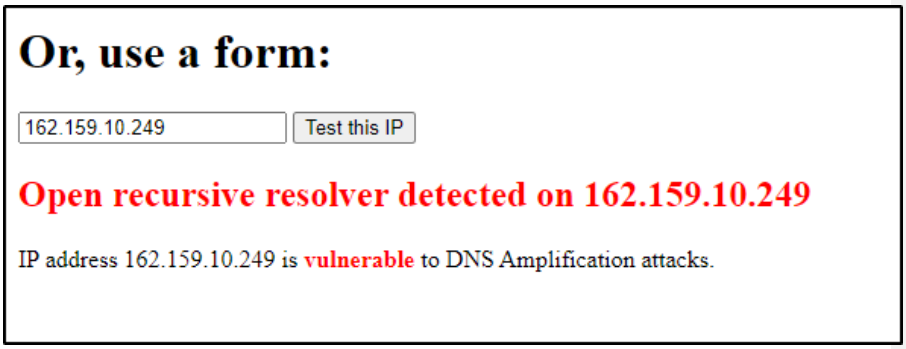
Proses Pengujian :

1. **http://openresolver.com/**

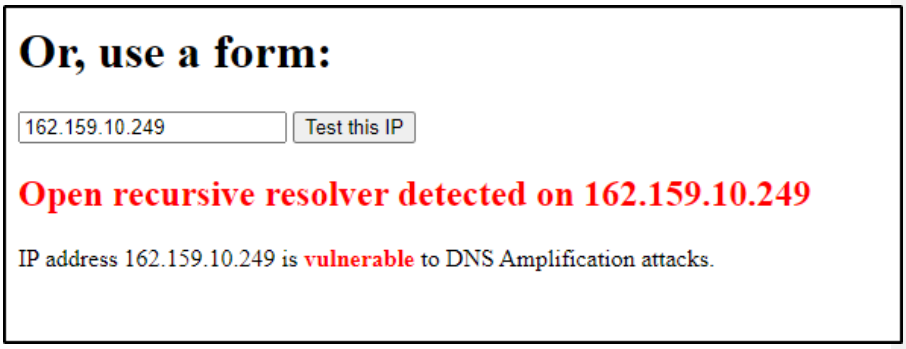
A.ns1prakerja.go.id



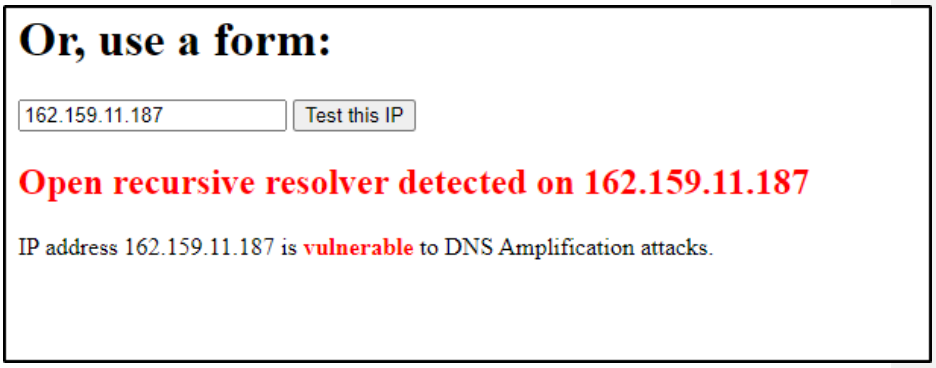
B.ns2prakerja.go.id



C.ns3prakerja.go.id



D.ns5prakerja.go.id


Or, use a form:
162.159.11.187
Test this IP
Open recursive resolver detected on 162.159.11.187
IP address 162.159.11.187 is vulnerable to DNS Amplification attacks.

B.6. Zone Transfer DNS Server (Domain Enumeration) Test		
Tujuan : Untuk mengetahui apakah zone transfer atau zone data atau zone file pada Authoritative DNS Server domain prakerja.go.id dapat ditampilkan. Referensi : https://en.wikipedia.org/wiki/DNS_zone_transfer http://www.exploit-db.com/download_pdf/13687/		
Tools : https://hackertarget.com/zone-transfer/		
Hasil Penilaian dan Rekomendasi		
No	**Name Server yang rentan**	**Hasil**
1.	162.159.8.210	✓
2.	162.159.9.157	✓
3.	162.159.10.249	✓
4.	---.---.---.---	-
5.	162.159.11.187	✓
Rekomendasi :		
CVSS:3.0/		

Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :

1. https://hackertarget.com/zone-transfer/

```
; <<>> DiG 9.10.3-P4-Debian <<>> axfr @ns1.prakerja.go.id prakerja.go.id
; (1 server found)
;; global options: +cmd
; Transfer failed.


; <<>> DiG 9.10.3-P4-Debian <<>> axfr @ns2.prakerja.go.id prakerja.go.id
; (1 server found)
;; global options: +cmd
; Transfer failed.


; <<>> DiG 9.10.3-P4-Debian <<>> axfr @ns3.prakerja.go.id prakerja.go.id
; (1 server found)
;; global options: +cmd
; Transfer failed.


; <<>> DiG 9.10.3-P4-Debian <<>> axfr @ns5.prakerja.go.id prakerja.go.id
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

B.7. AS Number & Sub-Domain Mapping
Tujuan : Untuk mengetahui informasi AS Number dan penggunaan Backup Network pada domain.
Tools : dnsinspect.com

Hasil Penilaian dan Rekomendasi		
No	**Kondisi eksisting DNS dan Infrastruktur**	**Hasil**
1	Terdapat 2 atau lebih ASN dan Name Server berada pada subnet (ASNs) yang berbeda.	✗
	Temuan 1 :	
	Rekomendasi : mengalokasikan lebih dari satu ASN (Referensi: RFC 2182)	
2	Terdapat informasi host atau sub-domain dengan IP Private	✗
	Temuan 1 :	
	Rekomendasi :	
CVSS:3.0/		

Keterangan :

✓ : Konfigurasi sudah bersesuaian dengan best practice

✗ : Terdapat ketidaksesuaian konfigurasi

Proses Pengujian :