Keamanan Jaringan Komputer

Nama : M.Kadapi

Nim : 09011181520119

Dosen Pengampuh : Deris Setiawan.M.T,Phd

JURUSAN SISTEM KOMPUTER

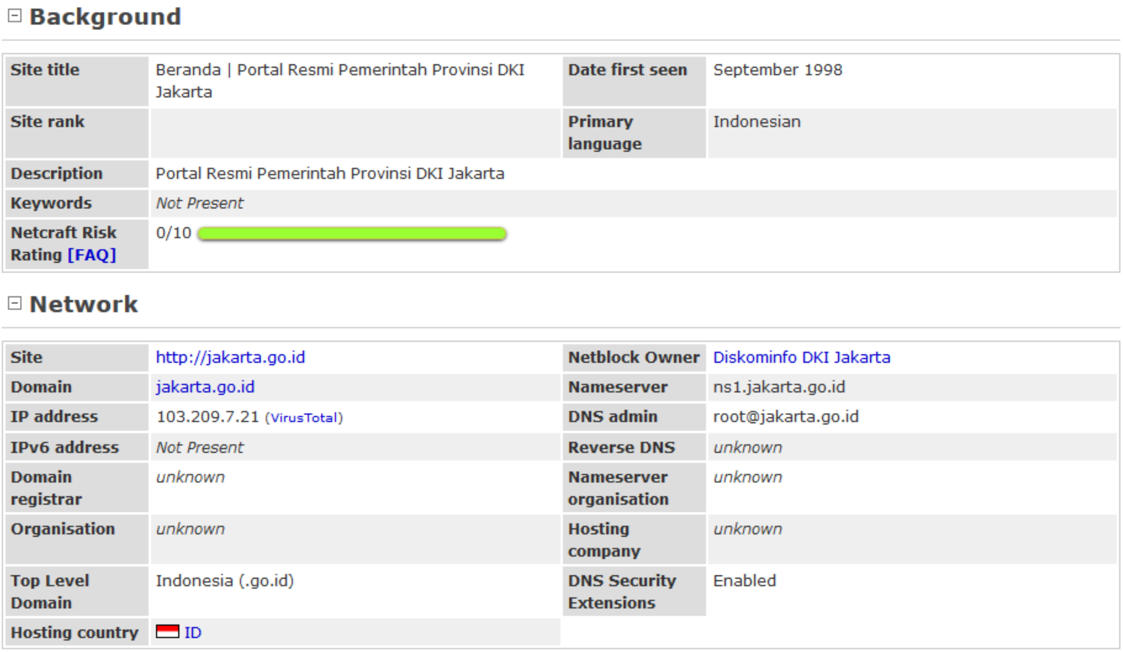
FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2019

A. Website Pemerintahan : http://jakarta.go.id

- **Detail Informasi**



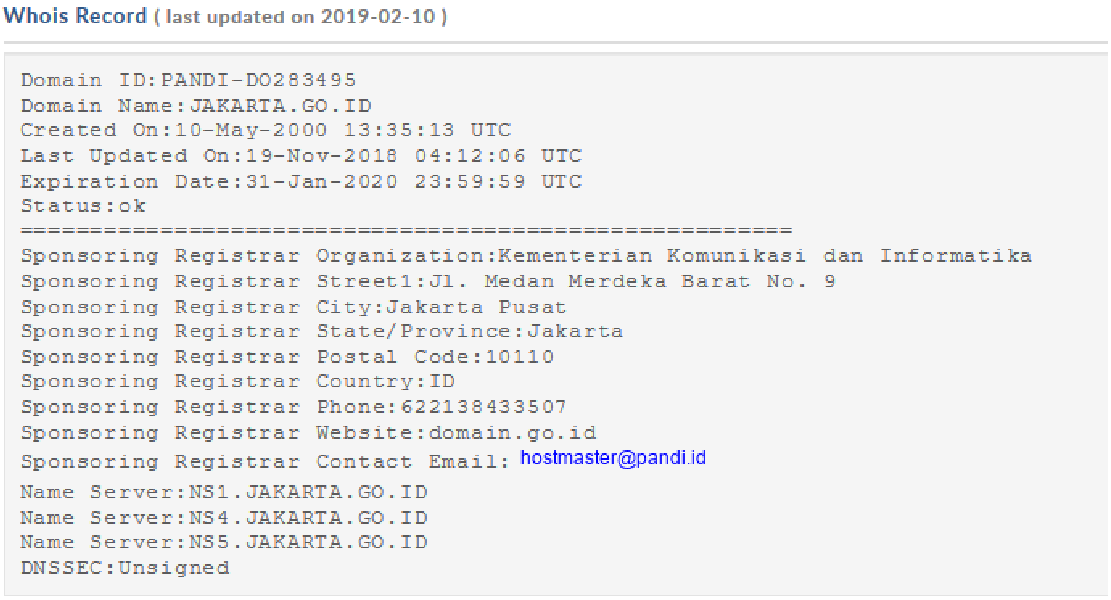
⊟ Background

Site title	Beranda | Portal Resmi Pemerintah Provinsi DKI Jakarta	**Date first seen**	September 1998
Site rank		**Primary language**	Indonesian
Description	Portal Resmi Pemerintah Provinsi DKI Jakarta		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

⊟ Network

Site	http://jakarta.go.id	**Netblock Owner**	Diskominfo DKI Jakarta
Domain	jakarta.go.id	**Nameserver**	ns1.jakarta.go.id
IP address	103.209.7.21 (VirusTotal)	**DNS admin**	root@jakarta.go.id
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	*unknown*
Top Level Domain	Indonesia (.go.id)	**DNS Security Extensions**	Enabled
Hosting country	ID		

- **Whois**



Whois Record (last updated on 2019-02-10)

```
Domain ID:PANDI-DO283495
Domain Name:JAKARTA.GO.ID
Created On:10-May-2000 13:35:13 UTC
Last Updated On:19-Nov-2018 04:12:06 UTC
Expiration Date:31-Jan-2020 23:59:59 UTC
Status:ok
=======================================================
Sponsoring Registrar Organization:Kementerian Komunikasi dan Informatika
Sponsoring Registrar Street1:Jl. Medan Merdeka Barat No. 9
Sponsoring Registrar City:Jakarta Pusat
Sponsoring Registrar State/Province:Jakarta
Sponsoring Registrar Postal Code:10110
Sponsoring Registrar Country:ID
Sponsoring Registrar Phone:622138433507
Sponsoring Registrar Website:domain.go.id
Sponsoring Registrar Contact Email: hostmaster@pandi.id
Name Server:NS1.JAKARTA.GO.ID
Name Server:NS4.JAKARTA.GO.ID
Name Server:NS5.JAKARTA.GO.ID
DNSSEC:Unsigned
```

- **CVE**

✓ CVE-2014-9342

Cross-site scripting (XSS) vulnerability in the tree view (pl_tree.php) feature in Application Security Manager (ASM) in F5 BIG-IP 11.3.0 allows remote attackers to inject arbitrary web script or HTML by accessing a crafted URL during automatic policy generation.

✓ CVE-2013-6024

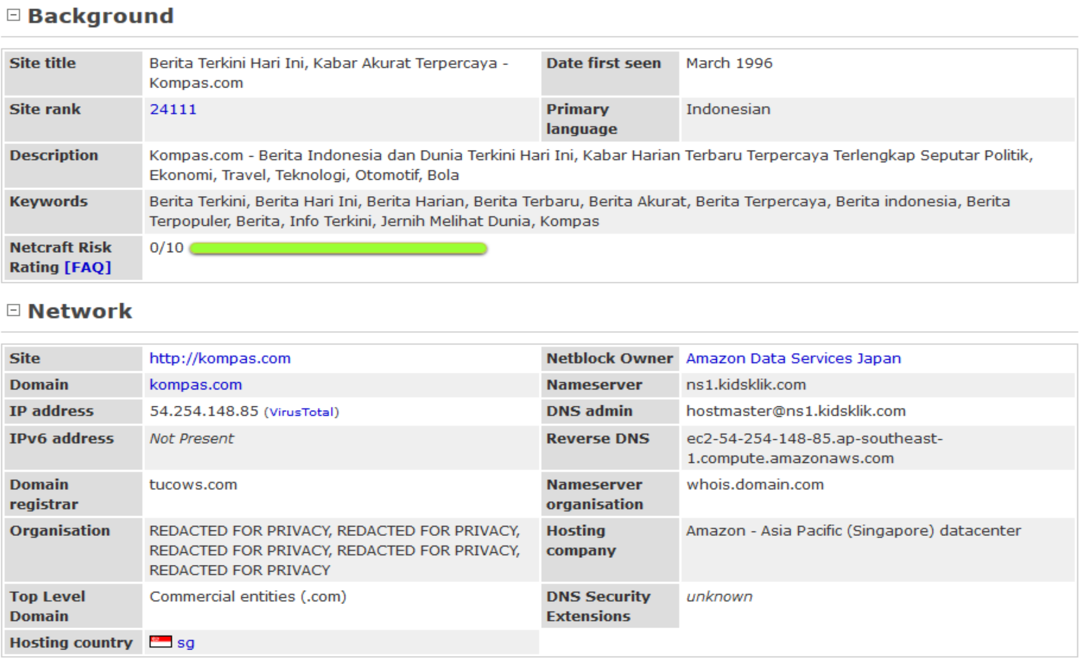
The Edge Client components in F5 BIG-IP APM 10.x through 10.2.4 and 11.x before 11.5.0, BIG-IP Edge Gateway 10.1.x and 10.2.x through 10.2.4 and 11.x before 11.5.0, and FirePass 6.0.0 through 6.1.0 and 7.0.0 allow attackers to obtain sensitive information from process memory via unspecified vectors.

✓ CVE-2012-3000

Multiple SQL injection vulnerabilities in sam/admin/reports/php/saveSettings.php in the (1) APM WebGUI in F5 BIG-IP LTM, GTM, ASM, Link Controller, PSM, APM, Edge Gateway, and Analytics and (2) AVR WebGUI in WebAccelerator and WOM 11.2.x before 11.2.0-HF3 and 11.2.x before 11.2.1-HF3 allow remote authenticated users to execute arbitrary SQL commands via the defaultQuery parameter.

B. WEBSITE DALAM NEGRI : *http://kompas.com*

- ### Detail Informasi



⊟ **Background**

Site title	Berita Terkini Hari Ini, Kabar Akurat Terpercaya - Kompas.com	**Date first seen**	March 1996
Site rank	24111	**Primary language**	Indonesian
Description	Kompas.com - Berita Indonesia dan Dunia Terkini Hari Ini, Kabar Harian Terbaru Terpercaya Terlengkap Seputar Politik, Ekonomi, Travel, Teknologi, Otomotif, Bola		
Keywords	Berita Terkini, Berita Hari Ini, Berita Harian, Berita Terbaru, Berita Akurat, Berita Terpercaya, Berita indonesia, Berita Terpopuler, Berita, Info Terkini, Jernih Melihat Dunia, Kompas		
Netcraft Risk Rating [FAQ]	0/10		

⊟ **Network**

Site	http://kompas.com	**Netblock Owner**	Amazon Data Services Japan
Domain	kompas.com	**Nameserver**	ns1.kidsklik.com
IP address	54.254.148.85 (VirusTotal)	**DNS admin**	hostmaster@ns1.kidsklik.com
IPv6 address	*Not Present*	**Reverse DNS**	ec2-54-254-148-85.ap-southeast-1.compute.amazonaws.com
Domain registrar	tucows.com	**Nameserver organisation**	whois.domain.com
Organisation	REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY	**Hosting company**	Amazon - Asia Pacific (Singapore) datacenter
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	sg		

- ### Whois

Domain Name: KOMPAS.COM

Registry Domain ID: 25458_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.tucows.com

Registrar URL: http://tucowsdomains.com

Updated Date: 2018-10-23T14:36:55

Creation Date: 1995-12-18T05:00:00

Registrar Registration Expiration Date: 2019-12-17T05:00:00

Registrar: TUCOWS, INC.

Registrar IANA ID: 69

Reseller: Virtual Interactive Center

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Registry Registrant ID:

Registrant Name: REDACTED FOR PRIVACY

Registrant Organization: REDACTED FOR PRIVACY

Registrant Street: REDACTED FOR PRIVACY

Registrant City: REDACTED FOR PRIVACY

Registrant State/Province: REDACTED FOR PRIVACY

Registrant Postal Code: REDACTED FOR PRIVACY

Registrant Country: REDACTED FOR PRIVACY

Registrant Phone: REDACTED FOR PRIVACY

Registrant Phone Ext:

Registrant Fax: REDACTED FOR PRIVACY

Registrant Fax Ext:

Registrant Email: REDACTED FOR PRIVACY

Registry Admin ID:

Admin Name: REDACTED FOR PRIVACY

Admin Organization: REDACTED FOR PRIVACY

Admin Street: REDACTED FOR PRIVACY

Admin City: REDACTED FOR PRIVACY

Admin State/Province: REDACTED FOR PRIVACY

Admin Postal Code: REDACTED FOR PRIVACY

Admin Country: REDACTED FOR PRIVACY

Admin Phone: REDACTED FOR PRIVACY

Admin Phone Ext:

Admin Fax: REDACTED FOR PRIVACY

Admin Fax Ext:

Admin Email: REDACTED FOR PRIVACY

Registry Tech ID:

Tech Name: REDACTED FOR PRIVACY

Tech Organization: REDACTED FOR PRIVACY

Tech Street: REDACTED FOR PRIVACY

Tech City: REDACTED FOR PRIVACY

Tech State/Province: REDACTED FOR PRIVACY

Tech Postal Code: REDACTED FOR PRIVACY

Tech Country: REDACTED FOR PRIVACY

Tech Phone: REDACTED FOR PRIVACY

Tech Phone Ext:

Tech Fax: REDACTED FOR PRIVACY

Tech Fax Ext:

Tech Email: REDACTED FOR PRIVACY

Name Server: ns1.kidsklik.com

Name Server: ns2.kidsklik.com

Registrar Abuse Contact Email: domainabuse@tucows.com

Registrar Abuse Contact Phone: +1.4165350123

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

"For more information on Whois status codes, please visit https://icann.org/epp"

Registration Service Provider:

Virtual Interactive Center, admin@vic.com

865 524 8888

865 524 0740 (fax)

Please contact us for domain login/passwords, DNS/Nameserver changes,

and general domain support questions.

- **CVE**

  ✓ CVE-2019-7401

NGINX Unit before 1.7.1 might allow an attacker to cause a heap-based buffer overflow in the router process with a specially crafted request. This may result in a denial of service (router process crash) or possibly have unspecified other impact.

- ✓ CVE-2018-8059

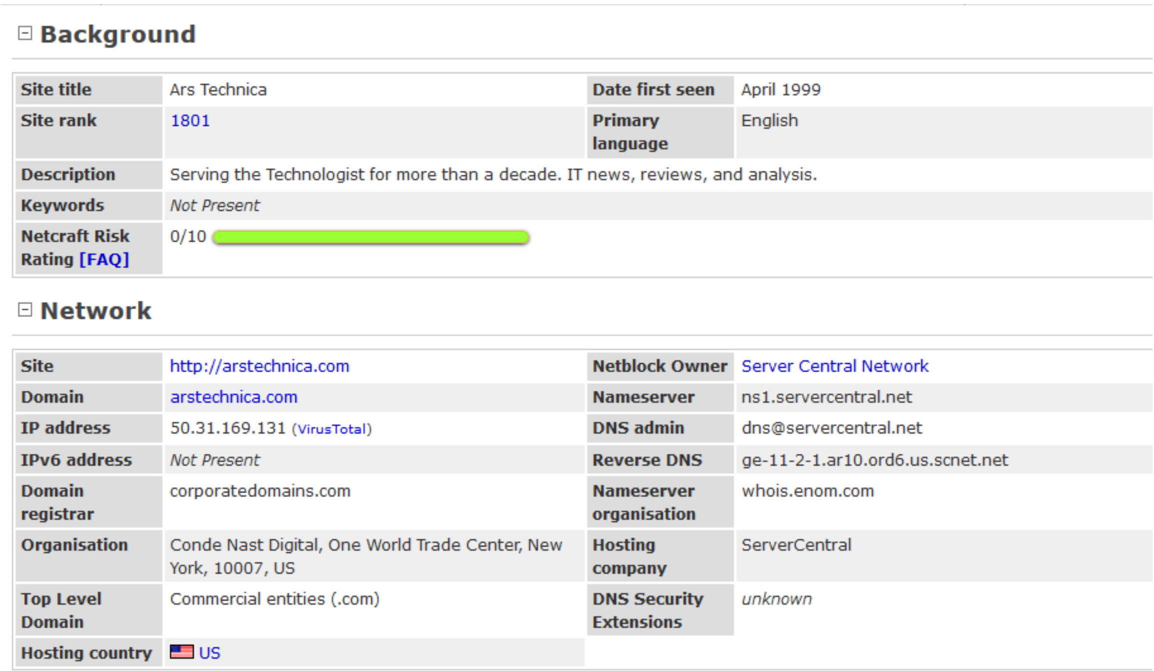
The Djelibeybi configuration examples for use of NGINX in SUSE Portus 2.3, when applied to certain configurations involving Docker Compose, have a Missing SSL Certificate Validation issue because no proxy_ssl_* directives are used.

- ✓ CVE-2018-16845

nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.

C. **WEBSITE LUAR NEGRI : *http://arstechnica.com***

- **Detail Informasi**



⊟ Background

Site title	Ars Technica	**Date first seen**	April 1999
Site rank	1801	**Primary language**	English
Description	Serving the Technologist for more than a decade. IT news, reviews, and analysis.		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10 🟩		

⊟ Network

Site	http://arstechnica.com	**Netblock Owner**	Server Central Network
Domain	arstechnica.com	**Nameserver**	ns1.servercentral.net
IP address	50.31.169.131 (VirusTotal)	**DNS admin**	dns@servercentral.net
IPv6 address	*Not Present*	**Reverse DNS**	ge-11-2-1.ar10.ord6.us.scnet.net
Domain registrar	corporatedomains.com	**Nameserver organisation**	whois.enom.com
Organisation	Conde Nast Digital, One World Trade Center, New York, 10007, US	**Hosting company**	ServerCentral
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	🇺🇸 US		

- **Whois**

Domain Name: arstechnica.com

Registry Domain ID: 3408778_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.corporatedomains.com

Registrar URL: www.cscprotectsbrands.com

Updated Date: 2017-12-26T06:19:03Z

Creation Date: 1998-12-30T05:00:00Z

Registrar Registration Expiration Date: 2019-12-30T05:00:00Z

Registrar: CSC CORPORATE DOMAINS, INC.

Registrar IANA ID: 299

Registrar Abuse Contact Email: domainabuse@cscglobal.com

Registrar Abuse Contact Phone: +1.8887802723

Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited

Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited

Domain Status: serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited

Registry Registrant ID:

Registrant Name: Domain Administrator

Registrant Organization: Conde Nast Digital

Registrant Street: One World Trade Center

Registrant City: New York

Registrant State/Province: NY

Registrant Postal Code: 10007

Registrant Country: US

Registrant Phone: +1.2122862860

Registrant Phone Ext:

Registrant Fax: +1.2122862860

Registrant Fax Ext:

Registrant Email: domain_admin@advancemags.com

Registry Admin ID:

Admin Name: Domain Administrator

Admin Organization: Advance Magazine Group

Admin Street: One World Trade Center

Admin City: New York

Admin State/Province: NY

Admin Postal Code: 10007

Admin Country: US

Admin Phone: +1.2122862860

Admin Phone Ext:

Admin Fax: +1.2122862860

Admin Fax Ext:

Admin Email: domain_admin@advancemags.com

Registry Tech ID:

Tech Name: Domain Administrator

Tech Organization: Advance Magazine Group Technical Services

Tech Street: 801 Pencader Dr

Tech City: Newark

Tech State/Province: DE

Tech Postal Code: 19702

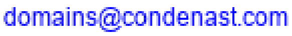
Tech Country: US

Tech Phone: +1.3028304630

Tech Phone Ext:

Tech Fax: +1.3028304630

Tech Fax Ext:

Tech Email: 

domains@condenast.com

Name Server: ns2.servercentral.net

Name Server: ns1.servercentral.net

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/.

- **CVE**

✓ CVE-2019-7401

NGINX Unit before 1.7.1 might allow an attacker to cause a heap-based buffer overflow in the router process with a specially crafted request. This may result in a denial of service (router process crash) or possibly have unspecified other impact.

✓ CVE-2018-8059

The Djelibeybi configuration examples for use of NGINX in SUSE Portus 2.3, when applied to certain configurations involving Docker Compose, have a

Missing SSL Certificate Validation issue because no proxy_ssl_* directives are used.

- ✓ CVE-2018-16845

  nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.