

**TUGAS LAPORAN**  
**MANAJEMEN KEAMANAN INFORMASI**



**DIBUAT OLEH :**

**NAMA : AYUNI INDAH LESTARI**

**NIM : 09031181520003**

**KELAS : SIREG 6A**


**SISTEM INFORMASI**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS SRIWIJAYA**

**2018**

1. Target : [www.monitoring.telkomspeedy.com](http://www.monitoring.telkomspeedy.com)

- Langkah Pertama yaitu : Data Collection

#### Background

Site title	Home Monitoring	Date first seen	October 2010
Site rank		Primary language	English
Description	Not Present		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	0/10 		

#### Network

Site	<a href="http://monitoring.telkomspeedy.com">http://monitoring.telkomspeedy.com</a>	Netblock Owner	PT TELKOM INDONESIA
Domain	telkomspeedy.com	Nameserver	nspr1.telkom.net.id
IP address	180.250.242.58	DNS admin	hostmaster@telkom.net.id
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	onlinenic.com	Nameserver organisation	whois.pandi.or.id
Organisation	Divisi Multimedia, PT Telekomunikasi Indonesia, tbk, Menara Multimedia, Jl. Kebon Sirih No. 12, Jakarta Pusat, 10340, ID	Hosting company	PT Telekomunikasi Indonesia Tbk
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	 ID		

#### Hosting History

Netblock owner	IP address	OS	Web server	Last seen <a href="#">Refresh</a>
<a href="#">PT TELKOM INDONESIA Menara Multimedia Lt. 7 Jl. Kebonsirih No.12 JAKARTA</a>	180.250.242.58	Linux	Apache/2.2.22 Ubuntu	18-Aug-2014
<a href="#">PT TELKOM INDONESIA Menara Multimedia Lt. 7 Jl. Kebonsirih No.12 JAKARTA</a>	118.98.96.101	Linux	Apache/2.2.22 Ubuntu	27-Jul-2012

Pada gambar diatas, diketahui bahwa :

Netblock Owner : PT Telkom Indonesia Menara Multimedia Lt.7 Jl. Kebonsirih No.12

Jakarta

IP Address : 180.250.242.58

OS : Linux

Web Server : Apache versi 2.2.22 Ubuntu

Netblock Owner : PT Telkom Indonesia Menara Multimedia Lt.7 Jl. Kebonsirih No.12

Jakarta

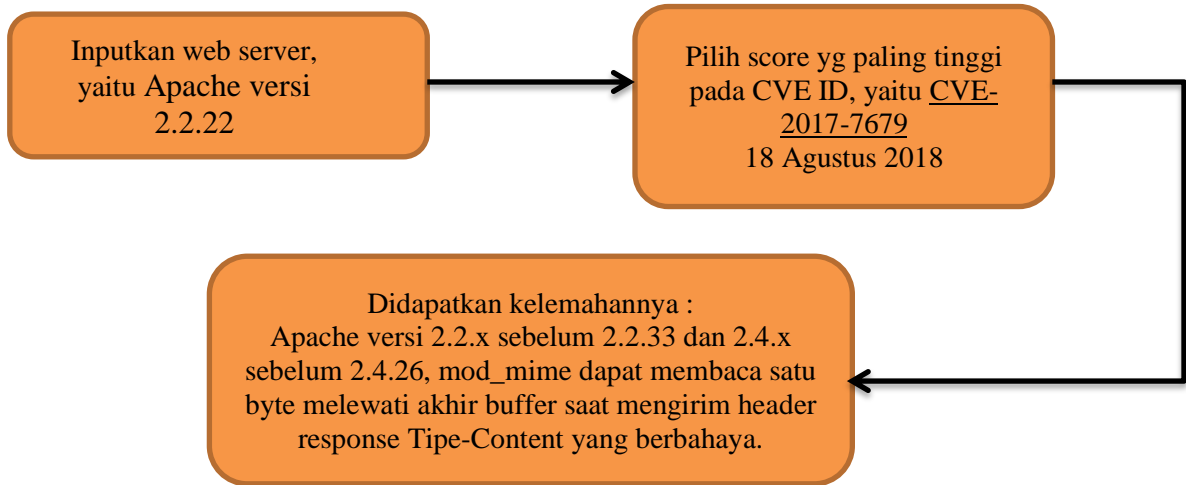
IP Address : 118.98.96.101

OS : Linux

Web Server : Apache versi 2.2.22 Ubuntu

- **Langkah Kedua yaitu : Vulnerabilities Web Server**

Cara untuk mengetahui kelemahan pada Web Server Apache versi 2.2.22 yaitu :




#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2017-7679</a>	<a href="#">119</a>		Overflow	2017-06-19	2018-01-18	7.5	None	Remote	Low	Not required	Partial	Partial	Partial

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod\_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.


## 2. Target : [www.sumbarprov.go.id](http://www.sumbarprov.go.id)

- Langkah Pertama yaitu : Data Collection

### Background

Site title	Not Present	Date first seen	June 2005
Site rank		Primary language	English
Description	Not Present		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	0/10 		

### Network

Site	<a href="http://sumbarprov.go.id">http://sumbarprov.go.id</a>	Netblock Owner	PT TELKOM INDONESIA Menara Multimedia Lt.7 Jl. Kebon sirih No.12 JAKARTA
Domain	<a href="http://sumbarprov.go.id">sumbarprov.go.id</a>	Nameserver	ns1.telkomhosting.com
IP address	36.67.167.34	DNS admin	hostmaster@telkom.net.id
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	unknown	Nameserver organisation	whois.onlinenic.com
Organisation	unknown	Hosting company	PT Telekomunikasi Indonesia Tbk
Top Level Domain	Indonesia (.go.id)	DNS Security Extensions	Enabled
Hosting country	 ID		

### Hosting History

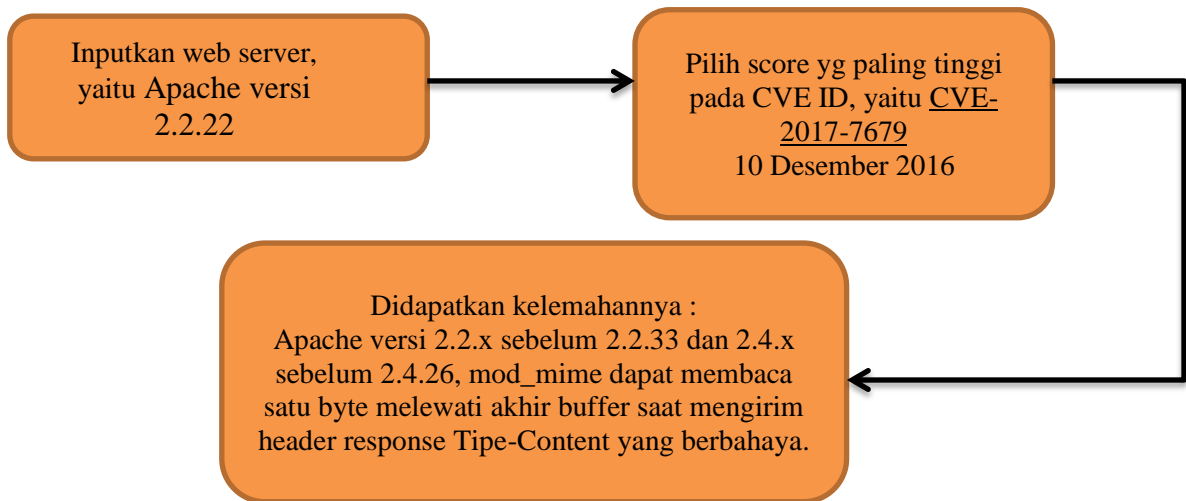
Netblock owner	IP address	OS	Web server	Last seen
PT TELKOM INDONESIA Menara Multimedia Lt.7 Jl. Kebon sirih No.12 JAKARTA	36.67.167.34	Linux	Apache	6-Mar-2018 <a href="#">Refresh</a>
KANTOR GUBERNUR SUMATERA BARAT	182.253.192.93	Linux	Apache/2.2.22 Ubuntu	10-Dec-2016
Hosting Services, Inc. 517 W 100 N STE 225 Providence UT US 84332	206.190.159.168	Linux	LiteSpeed	16-Jun-2015
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	203.130.196.151	Linux	Apache/2.2.3 Red Hat	3-Dec-2011
INDOSATM2 Dedicated Emerald Customer Jakarta	202.155.11.22	Windows 2000	Microsoft-IIS/5.0	18-Oct-2007

Pada gambar diatas, diketahui bahwa :

Netblock Owner	: Kantor Gubernur Sumatera Barat
IP Address	: 182.253.192.93
OS	: Linux
Web Server	: Apache versi 2.2.22 Ubuntu
Netblock Owner	: PT Telkom Divisi Multimedia
IP Address	: 203.130.196.151
OS	: Linux
Web Server	: Apache versi 2.2.3 RedHat
Netblock Owner	: Indosatm2 Dedicated Emerald Customer Jakarta
IP Address	: 202.155.11.22
OS	: Windows 2000
Web Server	: Microsoft-11S/5.0

- **Langkah Kedua yaitu : Vulnerabilities Web Server**

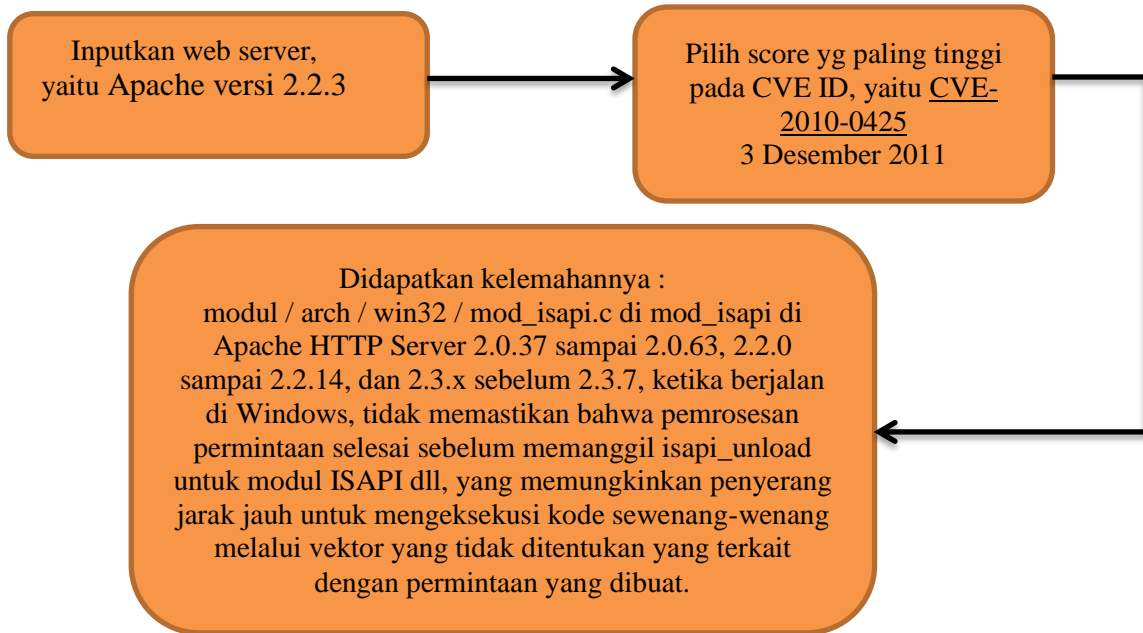
Cara untuk mendapatkan kelemahan pada Web Server Apache 2.2.22 yaitu :



#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2017-7679</a>	<a href="#">119</a>		Overflow	2017-06-19	2018-01-18	7.5	None	Remote	Low	Not required	Partial	Partial	Partial

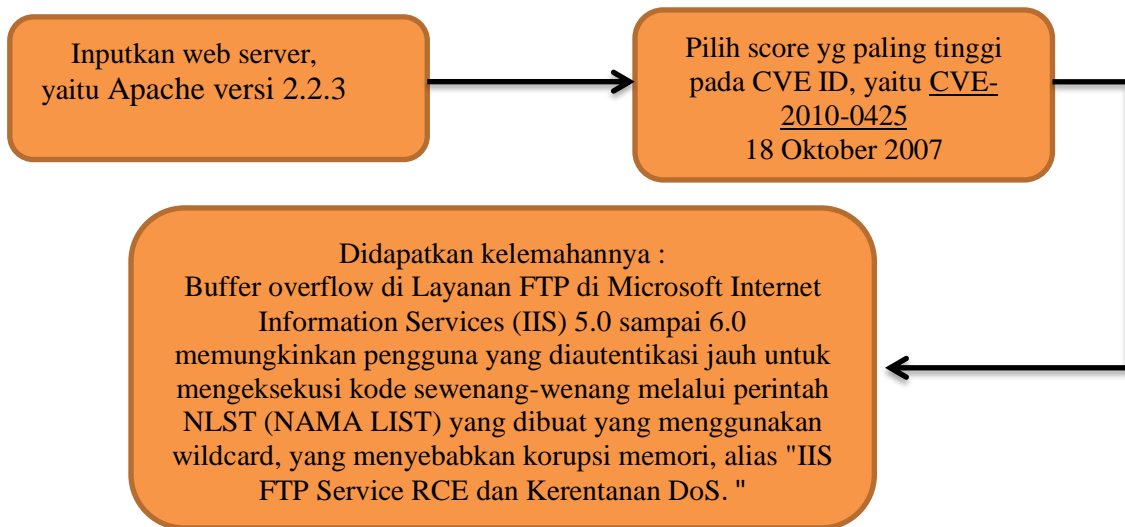
In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod\_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

Cara untuk mengetahui kelemahan pada Web Server Apache 2.2.3 yaitu :



27	<a href="#">CVE-2010-0425</a>	Exec Code	2010-03-05	2017-09-18	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."												

Cara untuk mengetahui kelemahan pada Web Server Apache 2.2.3 yaitu :



3	<a href="#">CVE-2009-3023</a>	119	2	Exec Code Overflow	Mem. Corr.	2009-08-31	2017-09-18	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
---	-------------------------------	-----	---	--------------------	------------	------------	------------	-----	------	--------	--------	--------------	----------	----------	----------

Buffer overflow in the FTP Service in Microsoft Internet Information Services (IIS) 5.0 through 6.0 allows remote authenticated users to execute arbitrary code via a crafted NLST (NAME LIST) command that uses wildcards, leading to memory corruption, aka "IIS FTP Service RCE and DoS Vulnerability."