LAPORAN MANAJEMEN KEAMANAN INFORMASI

Oleh :

NELY YUPITA 09031281520093

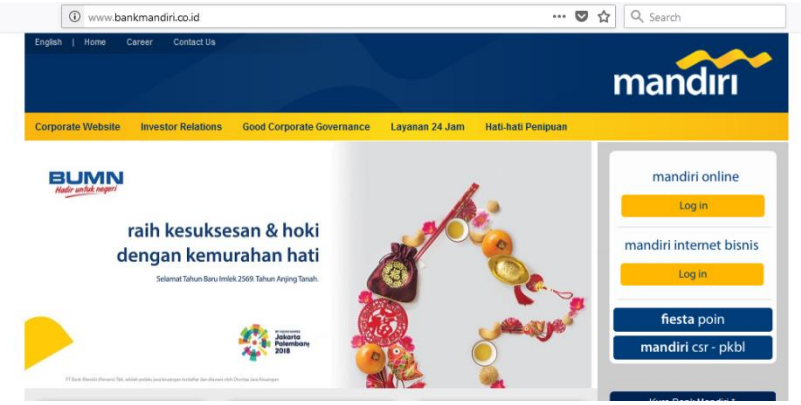
PROGRAM STUDI SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

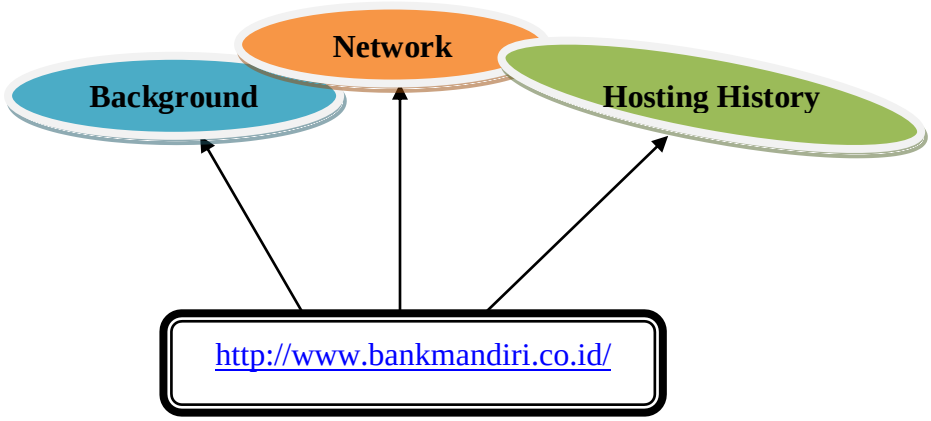
UNIVERSITAS SRIWIJAYA

TAHUN 2018

1. **Website Bank Mandiri (**http://www.bankmandiri.co.id/**)**



- **Tahap Pertama Data Analyst**



Keterangan :

Pada tahap pertama data analyst pada website bank mandiri terdapat 3 data yang yaitu Background, network, Hosting History.

Background

Site title	403 - Forbidden: Access is denied.	**Date first seen**	September 1999
Site rank	33289	**Primary language**	English
Description	*Not Present*		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

Gambar 1. Backgorund

Site tittle : 403-forbidden; access is denied
Site rank : 33289
Date first seen : september 1999
Primary language : english.

Network

Site	http://www.bankmandiri.co.id	**Netblock Owner**	PT TELKOM INDONESIA Menara Multimedia Lt.7 Jl. Kebon sirih No.12 JAKARTA
Domain	bankmandiri.co.id	**Nameserver**	ns1.bankmandiri.co.id
IP address	36.66.91.167	**DNS admin**	hostmaster@biz.net.id
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	pandi.or.id	**Nameserver organisation**	whois.pandi.or.id
Organisation	PT. Supra Primatama Nusantara, Mid Plaza II Lt.8, Jl. Jend. Sudirman Kav. 10 - 11, Jakarta, 10220, Indonesia	**Hosting company**	PT Telekomunikasi Indonesia Tbk
Top Level Domain	Indonesia (.co.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Gambar 2. Network

Site : http://www.bankmandiri.co.id
Domain : bankmandiri.co.id
Ip address : 36.66.91.167
Domain register : pandi.or.id
Organisation : PT. Supra Primatama NusantaraMid Plaza II Lt.8, Jl. Jend. Sudirman Kav. 10 - 11, Jakarta, 10220, Indonesia
Top level : domain Indonesia (.co.id)
Hosting country : ID
Netblock owner : PT Telkom Indonesia Menara Multimedia Lt.& Jl.Kebon sirih No.12 Jakarta
Nameserver : ns.1.bankmandiri.co.id
DNS admin : hostmaster@biz.net.id,nameserver
Nameserver organisation : whois.pandi.or.id
Hosting company : PT Telkomunikasi Indonesia Tbk.

Hosting History

Netblock owner	IP address	OS	Web server	Last seen (Refresh)
PT Excelcomindo Pratama Cellular, GPRS and Internet Service Provider	112.215.62.249	Windows Server 2008	Microsoft-IIS/7.5	23-Jul-2017
PT TELKOM INDONESIA Menara Multimedia Lt.7 Jl. Kebon sirih No.12 JAKARTA	36.66.91.167	Windows Server 2008	Microsoft-IIS/7.5	7-Jun-2017
Biznet ISP Internet Service Provider Jakarta, Indonesia	117.102.111.47	Windows Server 2008	Microsoft-IIS/7.5	9-May-2017
PT Excelcomindo Pratama Cellular, GPRS and Internet Service Provider	112.215.62.249	Windows Server 2008	Microsoft-IIS/7.5	23-Mar-2017
PT TELKOM INDONESIA Menara Multimedia Lt.7 Jl. Kebon sirih No.12 JAKARTA	36.66.91.167	Windows Server 2008	Microsoft-IIS/7.5	8-Mar-2017
Biznet ISP Internet Service Provider Jakarta, Indonesia	117.102.111.47	Windows Server 2008	Microsoft-IIS/7.5	7-Mar-2017
PT Excelcomindo Pratama Cellular, GPRS and Internet Service Provider	112.215.62.249	Windows Server 2008	Microsoft-IIS/7.5	3-Mar-2017
Biznet ISP Internet Service Provider Jakarta, Indonesia	117.102.111.47	Windows Server 2008	Microsoft-IIS/7.5	2-Mar-2017
PT TELKOM INDONESIA Menara Multimedia Lt.7 Jl. Kebon sirih No.12 JAKARTA	36.66.91.167	Windows Server 2008	Microsoft-IIS/7.5	20-Feb-2017
Biznet ISP Internet Service Provider Jakarta, Indonesia	117.102.111.47	Windows Server 2008	Microsoft-IIS/7.5	17-Feb-2017

Gambar 3. Hosting History

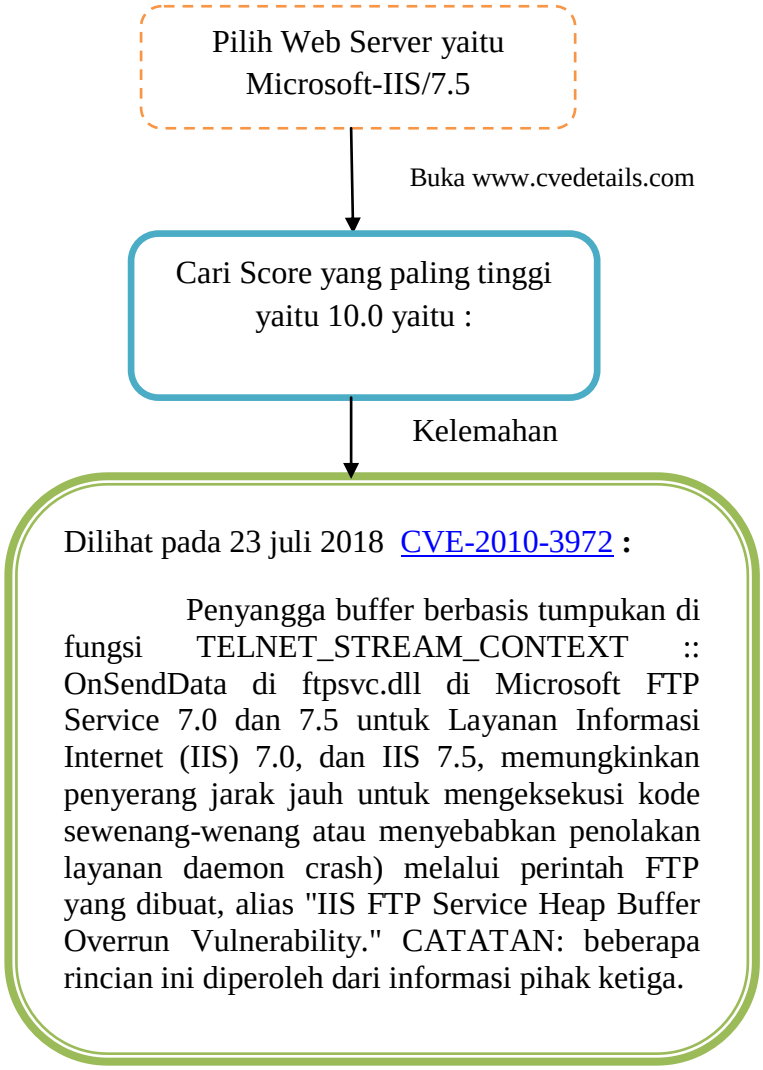
Pada Hosting History diatas kita akan melakukan pencarian vurnerabilities pada Web Server yang digunakan/dilihat sekarang pada 23 juli 2018 pada tahap kedua.

- **Tahap Kedua Vurnerabilities**

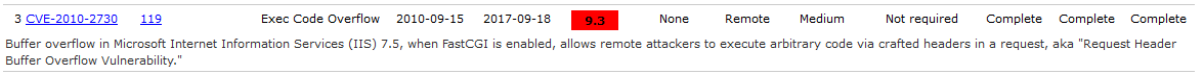
1. Vurnerabilities pada pada Score 6.8 pada www.cvedetails.com :

2	CVE-2010-3972	119	1	DoS Exec Code Overflow +Info	2010-12-23	2017-09-18	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

Heap-based buffer overflow in the TELNET_STREAM_CONTEXT::OnSendData function in ftpsvc.dll in Microsoft FTP Service 7.0 and 7.5 for Internet Information Services (IIS) 7.0, and IIS 7.5, allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted FTP command, aka "IIS FTP Service Heap Buffer Overrun Vulnerability." NOTE: some of these details are obtained from third party information.

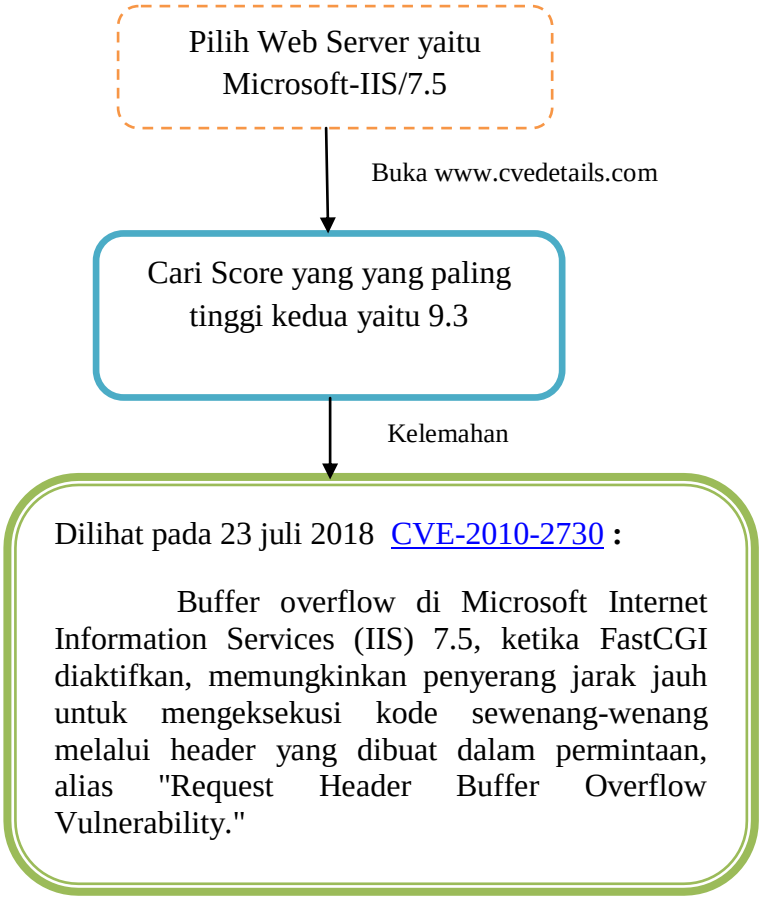


2. Vurnerabilities pada pada Score 9.3 pada www.cvedetails.com :

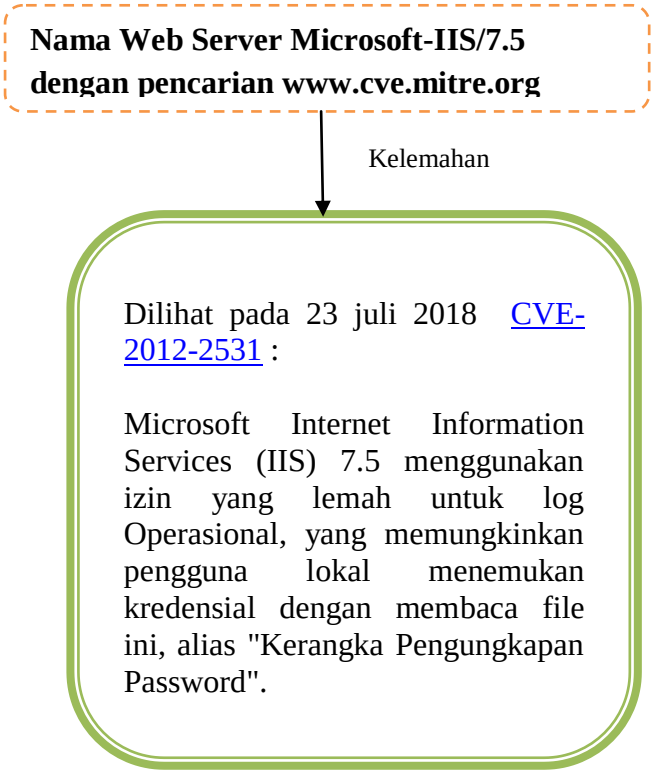


3	CVE-2010-2730	119	Exec Code Overflow	2010-09-15	2017-09-18	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

Buffer overflow in Microsoft Internet Information Services (IIS) 7.5, when FastCGI is enabled, allows remote attackers to execute arbitrary code via crafted headers in a request, aka "Request Header Buffer Overflow Vulnerability."

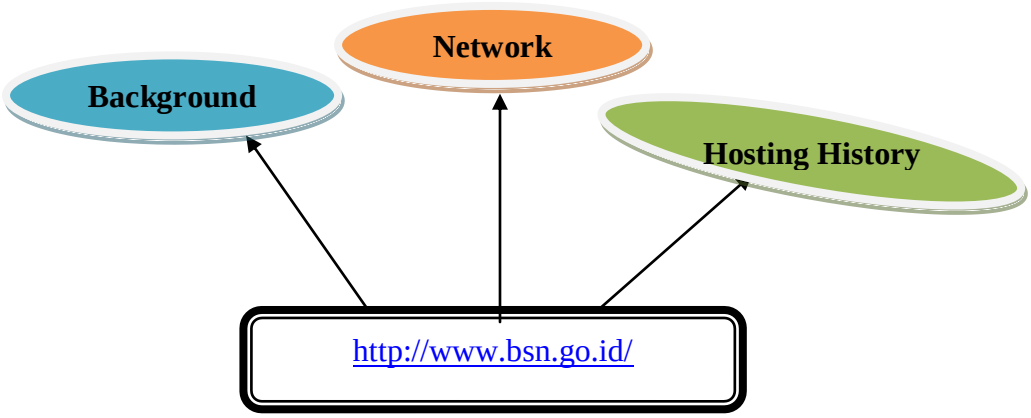


3. **Berikut hasil Securiy Vulnerabilities pada Microsoft-IIS/7.5 pada www.cve.mitre.org :**



2. **Website Badan Standarisai** (www.bsn.go.id)

- **Tahap Pertama Data Analyst**



Background

Site title	Home - BSN - Badan Standardisasi Nasional - National Standardization Agency of Indonesia - Setting the Standard in Indonesia ISO SNI WTO	**Date first seen**	September 1998
Site rank		**Primary language**	Indonesian
Description	Badan Standardisasi Nasional (BSN) mengambil alih fungsi dari Dewan Standardisasi Nasional (DSN). Kegiatan standardisasi dan penilaian kesesuaian di berbagai instansi merupakan simpul-simpul potensi nasional yang perlu dikoordinasikan dan disinkronisasikan dalam satu Sistem Standardisasi Nasional (SSN). Pengaturan standardisasi secara nasional ini diperlukan dalam rangka peningkatan keberterimaan produk nasional, dorongan produktivitans dan daya guna produksi serta menjamin mutu produk dan/atau jasa, sehingga dapat meningkatkan daya saing produk dan/atau jasa dipasar global.		
Keywords	Badan Standardisasi Nasional , National Standardization Agency of Indonesia, Standard, ISO, SNI, WTO, KAN, norm, accreditation, RSNI, Rancangan Standar Nasional Indonesia, SNI Award, Award, Laboratorium, Sertifikasi, MASTAN, download, koleksi, Perpustakaan, Library, Notifikasi		
Netcraft Risk Rating [FAQ]	0/10		

Gambar 1. Backgorund

Site tittle **:** Home-BSN-Badan standarisasi Nasional-National Standardization Agency of Indonesia-Setting the Standard in Indonesia ISO SNI WTO

Description **:** Badan Standardisasi Nasional (BSN) mengambil alih fungsi dari Dewan Standardisasi Nasional (DSN). Kegiatan standardisasi dan penilaian kesesuaian di berbagai instansi merupakan simpul-simpul potensi nasional yang perlu dikoordinasikan dan disinkronisasikan dalam satu Sistem Standardisasi Nasional (SSN). Pengaturan standardisasi

secara nasional ini diperlukan dalam rangka peningkatan keberterimaan produk nasional, dorongan produktivitans dan daya guna produksi serta menjamin mutu produk dan/atau jasa, sehingga dapat meningkatkan daya saing produk dan/atau jasa dipasar global.

Keywords **:** Badan Standardisasi Nasional , National Standardization Agency of Indonesia, Standard, ISO, SNI, WTO, KAN, norm, accreditation, RSNI, Rancangan Standar Nasional Indonesia, SNI Award, Award, Laboratorium, Sertifikasi, MASTAN, download, koleksi, Perpustakaan, Library, Notifikasi

Date first seen **:** September 1998

Primary languange **:** Indonesia

Network

Site	http://www.bsn.go.id	**Netblock Owner**	BADAN STANDARDISASI NASIONAL
Domain	bsn.go.id	**Nameserver**	bsn.go.id
IP address	123.231.232.228	**DNS admin**	admin@bsn.go.id
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	PT. Aplikanusa Lintasarta
Top Level Domain	Indonesia (.go.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Gambar 2. Network

Site : http://www.bsn.go.id
Domain : bsdn.go.id
Ip address : 123.231.232.228
Top level domain : Indonesia (.co.id)
Hosting country : ID
Netblock owner : BADAN STANDARDISASI NASIONAL
Nameserver : bsn.go.id
DNS admin : admin@bsn.go.id
Hosting company : PT.Aplikanusa Lintasarta

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
BADAN STANDARDISASI NASIONAL Jakarta Raya	123.231.232.228	Linux	Apache/2.4.6 CentOS OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.6.31	6-Mar-2018
BADAN STANDARDISASI NASIONAL Jakarta	202.169.54.10	Linux	Apache/2.4.6 CentOS OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16	13-Sep-2016
BADAN STANDARDISASI NASIONAL Jakarta	202.169.54.3	Linux	Apache/2.2.15 CentOS	21-May-2015
Badan Standarisasi Nasional Manggala Wanabakti Jl. Gatot Subroto Jakarta	202.158.23.134	Linux	Apache/2.2.15 CentOS	23-Jan-2014
Badan Standarisasi Nasional Manggala Wanabakti Jl. Gatot Subroto Jakarta	202.158.23.131	Windows Server 2003	Apache/2.2.4 Win32 PHP/5.2.6	26-Sep-2011
Badan Standarisasi Nasional Manggala Wanabakti Jl. Gatot Subroto Jakarta	202.158.23.131	NT4/Windows 98	Microsoft-IIS/4.0	21-Jun-2006

Gambar 3. Hosting History

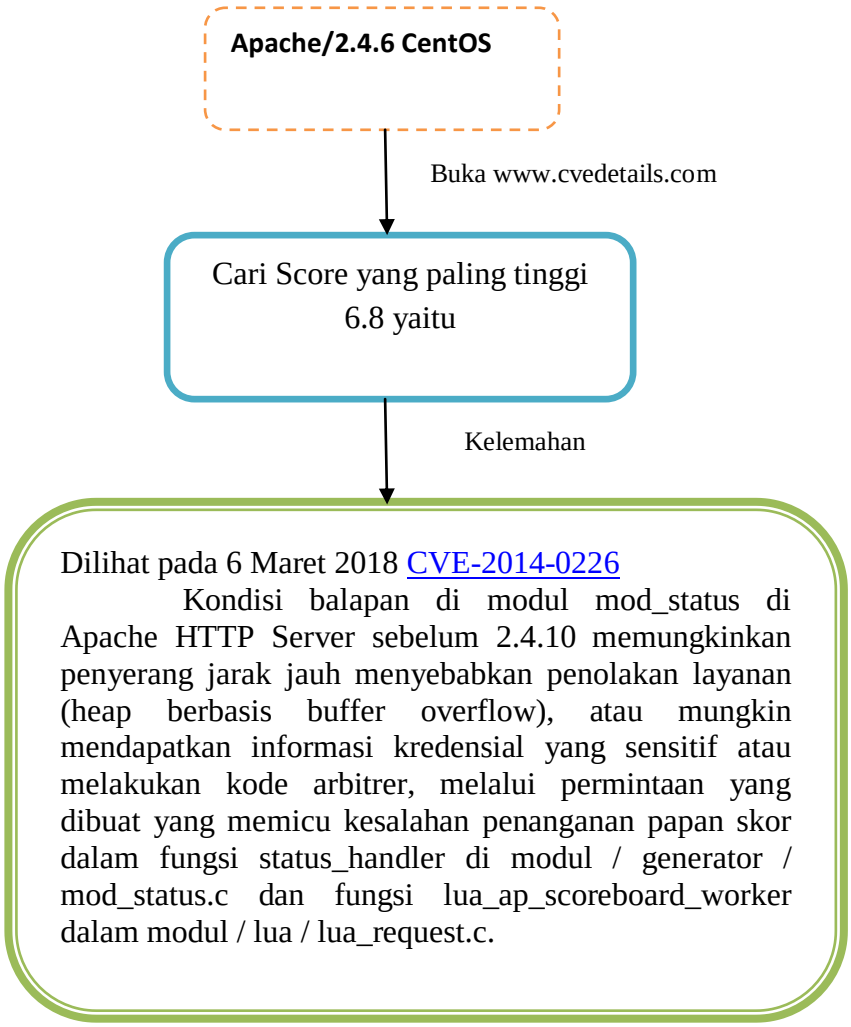
Pada Hosting History diatas kita akan melakukan mencari vurnerability pada Web Server yang digunakan sekarang pada 6 Maret 2018 pada tahap kedua.

- **Tahap Kedua Vurnerabilities Web Server**

1. **Vurnerabilities pada Score 6.8 yang tertinggi pada www.cvedetails.com :**

4	CVE-2014-0226	362	1 DoS Exec Code Overflow +Info	2014-07-20	2017-12-08	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial

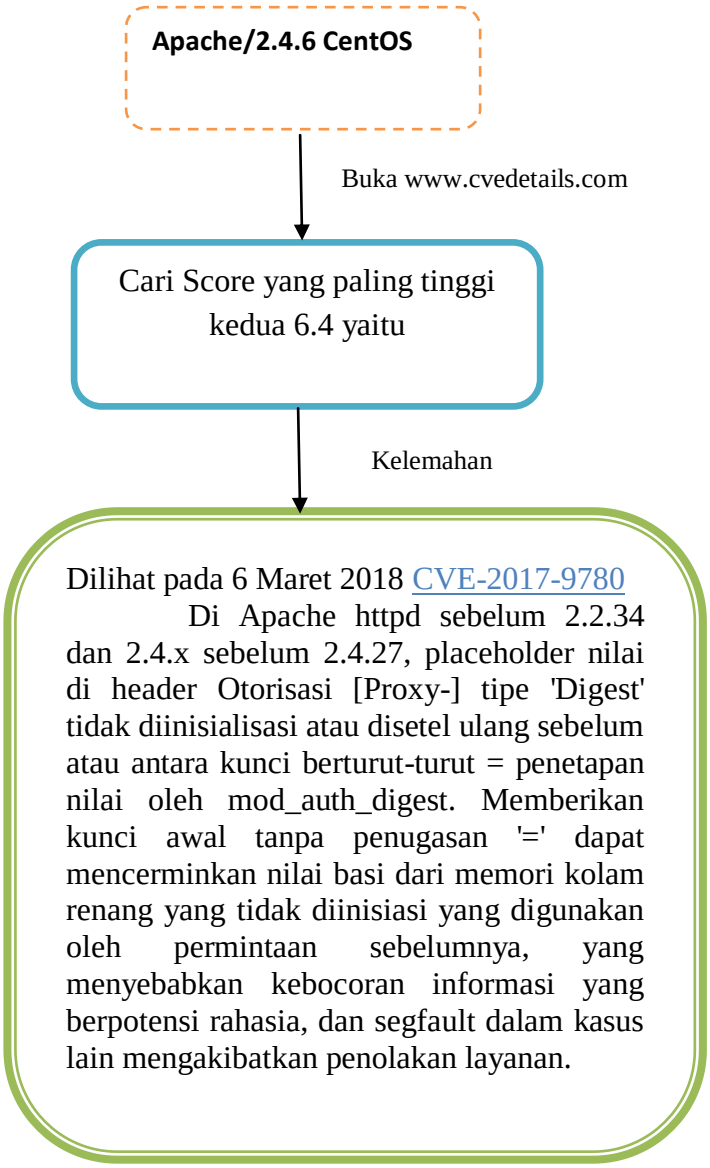
Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.



2. Vurnerabilities pada pada Score 6.4 yang tertinggi kedua pada www.cvedetails.com :

1	CVE-2017-9788	20	DoS +Info	2017-07-13	2018-01-04	6.4	None	Remote	Low	Not required	Partial	None	Partial

In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.



3. **Vurnerabilities pada pada Score 4.3 yang tertinggi ketiga pada www.cvedetails.com :**

9	CVE-2013-4352	DoS	2014-07-20	2014-08-04	4.3	None	Remote	Medium	Not required	None	None	Partial

The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing hostname value.