

# TUGAS KEAMANAN JARINGAN KOMPUTER



Oleh :

NAMA : KEFIN PRATAMA  
NIM : 09011181520020

FAKULTAS ILMU KOMPUTER  
JURUSAN SISTEM KOMPUTER  
UNIVERSITAS SRIWIJAYA  
2018

# WEB PEMERINTAH

Untuk web pemerintah saya menggunakan web <http://e-resources.pnri.go.id>

**Background**

Site title	Perpustakaan Nasional Republik Indonesia	Date first seen	September 2010
Site rank		Primary language	Indonesian
Description	Perpustakaan Nasional Republik Indonesia		
Keywords	Perpustakaan Nasional Republik Indonesia		
Netcraft Risk Rating [FAQ]	0/10		

**Network**

Site	<a href="http://e-resources.pnri.go.id">http://e-resources.pnri.go.id</a>	Netblock Owner	Perpustakaan Nasional RI
Domain	pnri.go.id	Nameserver	bima.pnri.go.id
IP address	103.28.21.51 (VirusTotal)	DNS admin	hostmaster@pnri.go.id
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	pnri.go.id
Top Level Domain	Indonesia (.go.id)	DNS Security Extensions	unknown
Hosting country	ID		

**Hosting History**

Netblock owner	IP address	OS	Web server	Last seen	Refresh
Perpustakaan Nasional RI Government / Direct Member IDNIC Jl. Salemba Raya No. 28A Jakarta Pusat, 10430	103.28.21.51	Linux	Apache/2.2.26 Unix PHP/5.5.6	1-Jun-2014	

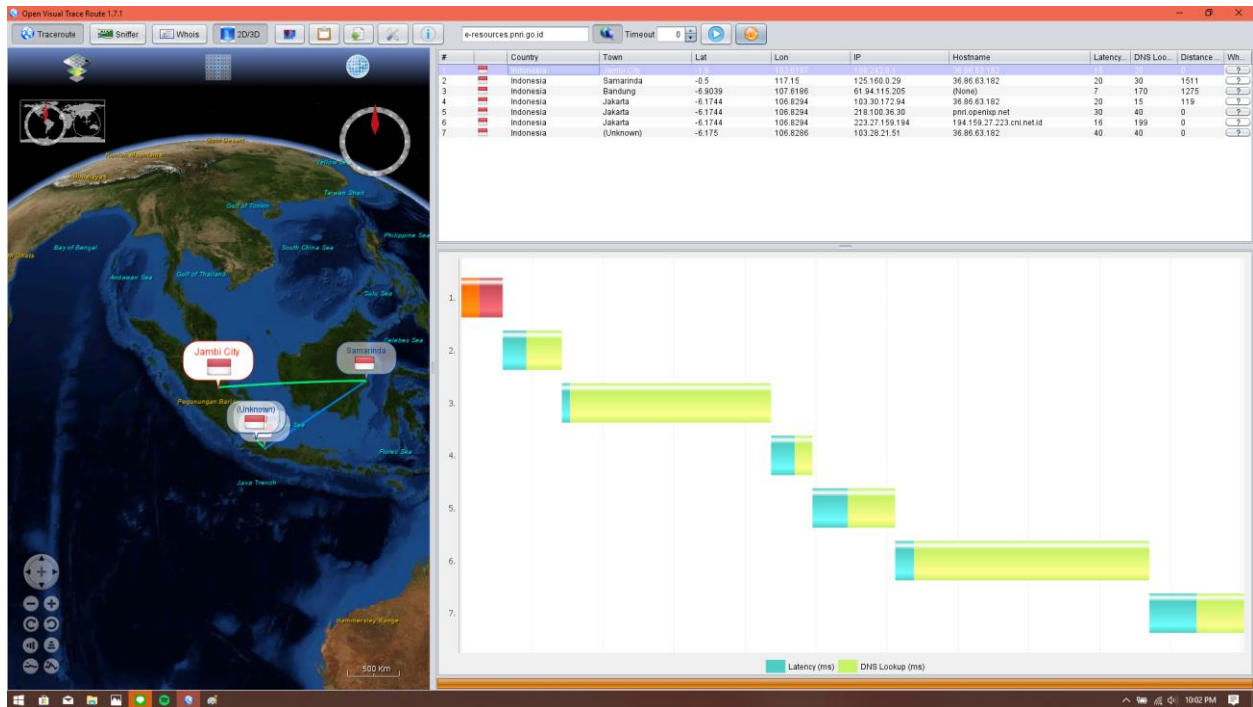
Pada gambar diatas berupa site report dr web pemerintah. Terdapat system operasi, domain, dll.

**Search Results**

There are 5213 CVE entries that match your search.

Name	Description
<a href="#">CVE-2019-7675</a>	An issue was discovered on MOBOTIX S14 MX-V4.2.1.61 devices. The default management application is delivered over cleartext HTTP with Basic Authentication, as demonstrated by the /admin/index.html URI.
<a href="#">CVE-2019-7323</a>	GUP (generic update process) in LightySoft LogMX before 7.4.0 does not properly verify the authenticity of updates, which allows man-in-the-middle attackers to execute arbitrary code via a Trojan horse update. The update process relies on cleartext HTTP. The attacker could replace the LogMXUpdater.class file.
<a href="#">CVE-2019-6802</a>	CRLF Injection in pyppiserver 1.2.5 and below allows attackers to set arbitrary HTTP headers and possibly conduct XSS attacks via a %0d%0a in a URI.
<a href="#">CVE-2019-6500</a>	In Axdway File Transfer Direct 2.7.1, an unauthenticated Directory Traversal vulnerability can be exploited by issuing a specially crafted HTTP GET request with %2e instead of '.' characters, as demonstrated by an initial /#2ddocumentation/%2e%2e/ substring.
<a href="#">CVE-2019-6447</a>	The ES File Explorer File Manager application through 4.1.9.7.4 for Android allows remote attackers to read arbitrary files or execute applications via TCP port 59777 requests on the local Wi-Fi network. This TCP port remains open after the ES application has been launched once, and responds to unauthenticated application/json data over HTTP.
<a href="#">CVE-2019-6256</a>	A Denial of Service issue was discovered in the LIVES55 Streaming Media libraries as used in Live555 Media Server 0.93. It can cause an RTSPServer crash in handleHTTPCmd_TunnelingPOST, when RTSP-over-HTTP tunneling is supported, via x-sessioncookie HTTP headers in a GET request and a POST request within the same TCP session. This occurs because of a call to an incorrect virtual function pointer in the readSocket function in GroupsockHelper.cpp.
<a href="#">CVE-2019-5489</a>	The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of the mincore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.
<a href="#">CVE-2019-3822</a>	libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header ("lib/uaauth/ntlm.c:curl_auth_create_ntlm_type3_message()"), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large 'nt response' data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a 'large value' needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header.
<a href="#">CVE-2019-3581</a>	Improper input validation in the proxy component of McAfee Web Gateway 7.8.2.0 and later allows remote attackers to cause a denial of service via a crafted HTTP request parameter.
<a href="#">CVE-2019-3500</a>	aria2c in aria2 1.33.1, when --log is used, can store an HTTP Basic Authentication username and password in a file, which might allow local users to obtain sensitive information by reading this file.
<a href="#">CVE-2019-3462</a>	Incorrect sanitization of the 302 redirect field in HTTP transport method of apt versions 1.4.8 and earlier can lead to content injection by a MITM attacker, potentially leading to remote code execution on the target machine.
<a href="#">CVE-2019-2550</a>	Vulnerability in the Oracle FLEXCUBE Direct Banking component of Oracle Financial Services Applications (subcomponent: Logoff Page). The supported version that is affected is 12.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/L/I:L/A:N).
<a href="#">CVE-2019-2549</a>	Vulnerability in the Oracle FLEXCUBE Direct Banking component of Oracle Financial Services Applications (subcomponent: Logoff Page). The supported version that is affected is 12.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Direct Banking, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Direct Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/L/I:L/A:N).
<a href="#">CVE-2019-2546</a>	Vulnerability in the Oracle Applications Manager component of Oracle E-Business Suite (subcomponent: SQL Extensions). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).
<a href="#">CVE-2019-2538</a>	Vulnerability in the Oracle Managed File Transfer component of Oracle Fusion Middleware (subcomponent: MFT Runtime Server). Supported versions that are affected are 19.1.0.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Managed File Transfer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Managed File Transfer accessible data as well as unauthorized read access to a subset of Oracle Managed File Transfer accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).
<a href="#">CVE-2019-2519</a>	Vulnerability in the PeopleSoft Enterprise SCM eProcurement component of Oracle PeopleSoft Products (subcomponent: Manage Requisition Status). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM eProcurement. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise SCM eProcurement, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise SCM eProcurement accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM eProcurement accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/L/I:L/A:N).
<a href="#">CVE-2019-2512</a>	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). Supported versions that are affected are 8.4, 15.1, 15.2, 16.1, 16.2, 17.7, 17.12 and 18.8. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera P6 Enterprise Project Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in

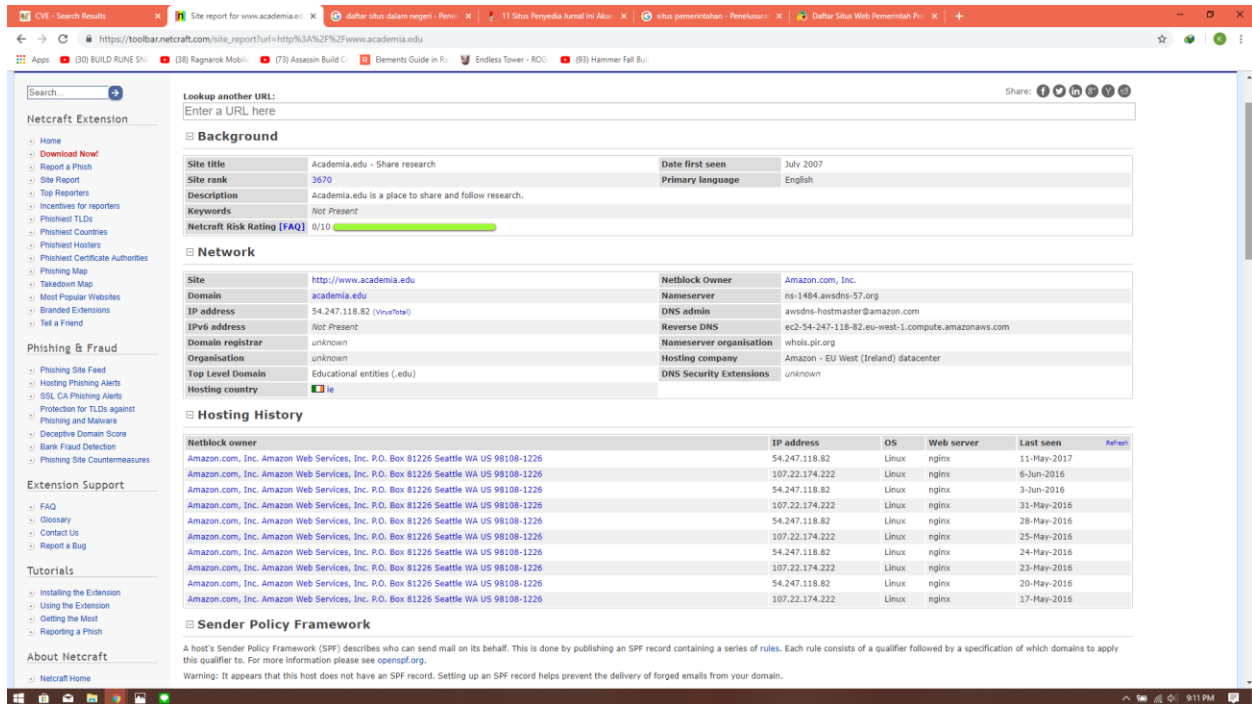
Pada gambar diatas terdapat CVE dari web pemerintah yang saya pilih untuk tugas kali ini.



Pada gambar diatas terdapat tracking dari web pemerintah yang saya pilih.

# WEB LUAR NEGERI

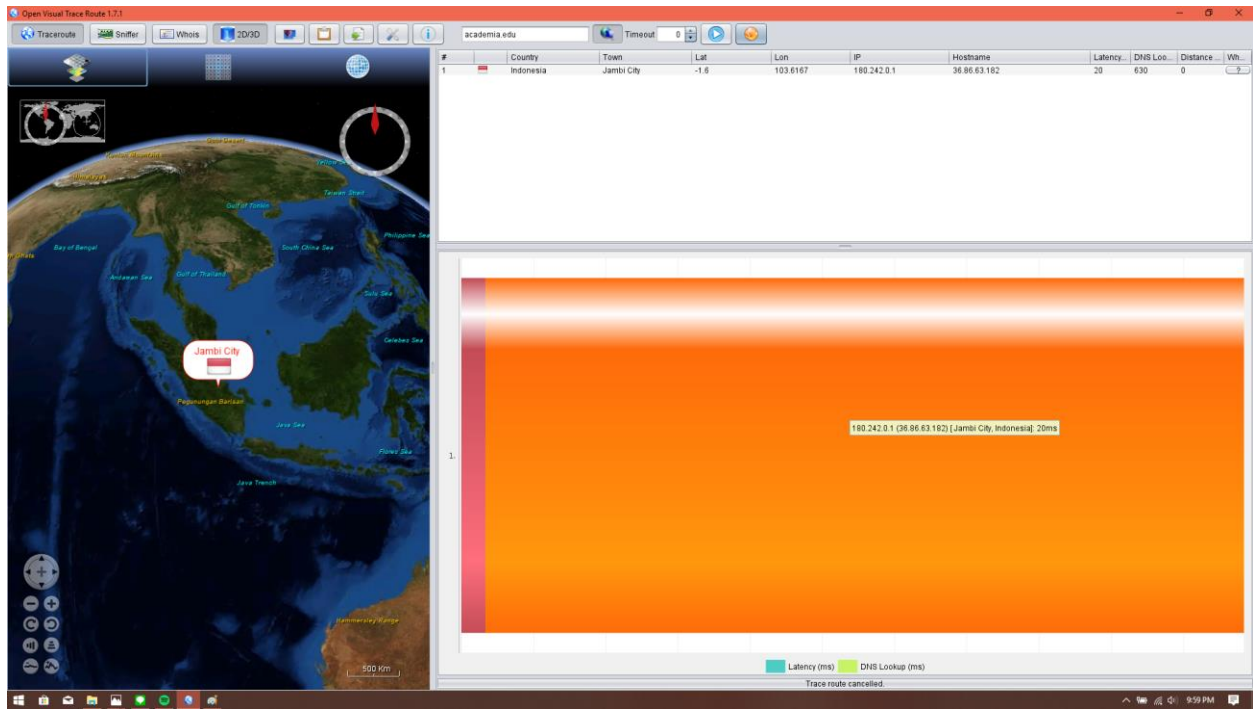
Untuk web luar negeri saya menggunakan <http://academia.edu>



Pada gambar diatas adalah berupa site report dr web luar negeri yang saya gunakan

Name	Description
CVE-2019-7675	An issue was discovered on MOBOTIX S14 MX-V4.2.1.61 devices. The default management application is delivered over cleartext HTTP with Basic Authentication, as demonstrated by the /admin/index.html URI.
CVE-2019-7323	GUIP (generic update process) in LogiSoft LogMX before 7.4.0 does not properly verify the authenticity of updates, which allows man-in-the-middle attackers to execute arbitrary code via a Trojan horse update. The update process relies on cleartext HTTP. The attacker could replace the LogMXUpdater.class file.
CVE-2019-6802	CRLF Injection in pypiserver 1.2.5 and below allows attackers to set arbitrary HTTP headers and possibly conduct XSS attacks via a %0d%0a in a URI.
CVE-2019-6500	In Asxay File Transfer Direct 2.7.1, an unauthenticated Directory Traversal vulnerability can be exploited by issuing a specially crafted HTTP GET request with %2e instead of '.' characters, as demonstrated by an initial /h2documentation/%2e%2e/ substring.
CVE-2019-6447	The ES File Explorer File Manager application through 4.1.9.7.4 for Android allows remote attackers to read arbitrary files or execute applications via TCP port 59777 requests on the local Wi-Fi network. This TCP port remains open after the ES application has been launched once, and responds to unauthenticated application/json data over HTTP.
CVE-2019-6256	A Denial of Service issue was discovered in the LIVES55 Streaming Media libraries as used in Live555 Media Server 0.93. It can cause an RTSPServer crash in handleHTTPCmd_TunnelingPOST, when RTSP-over-HTTP tunneling is supported, via x-sessioncookie HTTP headers in a GET request and a POST request within the same TCP session. This occurs because of a call to an incorrect virtual function pointer in the readSocket function in GroupsockHelper.cpp.
CVE-2019-5489	The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of the fincore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.
CVE-2019-3822	libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header ('lib/vauth/ntlm.c:curl_auth_create_ntlm_type3_message()'), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large 'nt response' data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a 'large value' needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header.
CVE-2019-3581	Improper input validation in the proxy component of McAfee Web Gateway 7.8.2.0 and later allows remote attackers to cause a denial of service via a crafted HTTP request parameter.
CVE-2019-3500	aria2c in aria2 1.33.1, when --log is used, can store an HTTP Basic Authentication username and password in a file, which might allow local users to obtain sensitive information by reading this file.
CVE-2019-3462	Incorrect sanitization of the 302 redirect field in HTTP transport method of apt versions 1.4.8 and earlier can lead to content injection by a MITM attacker, potentially leading to remote code execution on the target machine.
CVE-2019-2550	Vulnerability in the Oracle FLEXCUBE Direct Banking component of Oracle Financial Services Applications (subcomponent: Logoff Page). The supported version that is affected is 12.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/A:N).
CVE-2019-2549	Vulnerability in the Oracle FLEXCUBE Direct Banking component of Oracle Financial Services Applications (subcomponent: Logoff Page). The supported version that is affected is 12.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Direct Banking, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Direct Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/A:N).
CVE-2019-2546	Vulnerability in the Oracle Applications Manager component of Oracle E-Business Suite (subcomponent: SQL Extensions). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/A:N).
CVE-2019-2538	Vulnerability in the Oracle Managed File Transfer component of Oracle Fusion Middleware (subcomponent: MFT Runtime Server). Supported versions that are affected are 19.1.0.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Managed File Transfer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Managed File Transfer accessible data as well as unauthorized read access to a subset of Oracle Managed File Transfer accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/A:N).
CVE-2019-2519	Vulnerability in the PeopleSoft Enterprise SCM eProcurement component of Oracle PeopleSoft Products (subcomponent: Manage Requisition Status). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM eProcurement. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise SCM eProcurement, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise SCM eProcurement accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM eProcurement accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/A:N).

Pada gambar diatas adalah berupa CVE dari web luar negeri yang saya gunakan




Pada gambar diatas adalah berupa tracking dari web luar negeri yang saya pilih


# WEB DALAM NEGERI

Untuk web dalam negeri saya menggunakan <http://jurnal.lipi.go.id>

## Background

Site title	Jurnal Online	Date first seen	August 2004
Site rank		Primary language	English
Description	Sistem publikasi full-online untuk Jurnal Ilmiah dan komunitas ilmiah (Full-online publication system for scientific Journals).		
Keywords	portal, jurnal, online, publikasi, journal, publication, sains, ilmu, pengetahuan, science, scientific, community, Indonesia, global, free, gratis, cuma-cuma, fisika, physics, net, teori, terapan, organisasi, organization, profesi, profesional		
Netcraft Risk Rating [FAQ]	0/10 		

## Network

Site	<a href="http://www.jurnal.lipi.go.id">http://www.jurnal.lipi.go.id</a>	Netblock Owner	Lembaga Ilmu Pengetahuan Indonesia
Domain	lipi.go.id	Nameserver	dns1.lipi.go.id
IP address	203.160.128.143 (VirusTotal)	DNS admin	penjaga@lipi.go.id
IPv6 address	Not Present	Reverse DNS	fisikanet.lipi.go.id
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	lipi.go.id
Top Level Domain	Indonesia (.go.id)	DNS Security Extensions	unknown
Hosting country	 ID		

## Hosting History

Netblock owner	IP address	OS	Web server	Last seen	Refresh
LIPi Jakarta Raya	183.91.69.147	Linux	Apache/2.2.16 Debian	14-Oct-2012	
Infrastructure Colocation and Broadband IM2	202.155.61.29	-	Apache/2.0.54 Debian GNU/Linux mod_python/3.1.3 Python/2.3.5 PHP/4.3.10-16 mod_ssl/2.0.54 OpenSSL/0.9.7e	1-Oct-2005	
Infrastructure Colocation and Broadband IM2	202.155.61.29	Linux	Apache/2.0.54 Debian GNU/Linux mod_python/3.1.3 Python/2.3.5 PHP/4.3.10-15 mod_ssl/2.0.54 OpenSSL/0.9.7e	30-Sep-2005	
Indosat Internet Service Provider	202.155.61.29	Linux	Apache/2.0.54 Debian GNU/Linux mod_python/3.1.3 Python/2.3.5 PHP/4.3.10-15 mod_ssl/2.0.54 OpenSSL/0.9.7e	28-Aug-2005	
Indosat Internet Service Provider	202.155.61.29	Linux	Apache/2.0.52 Debian GNU/Linux mod_python/3.1.3 Python/2.3.4 PHP/4.3.10-2 mod_ssl/2.0.52 OpenSSL/0.9.7e	26-Feb-2005	
Lembaga Ilmu Pengetahuan Indonesia Jakarta 12720	202.47.65.66	Windows 2000	-	14-Jun-2004	
Lembaga Ilmu Pengetahuan Indonesia Jakarta 12720	202.47.65.66	unknown	Apache/2.0.52 Debian GNU/Linux mod_python/3.1.3 Python/2.3.4 PHP/4.3.10-2 mod_ssl/2.0.52 OpenSSL/0.9.7e	12-Jun-2004	
Lembaga Ilmu Pengetahuan Indonesia Jakarta 12720	202.47.65.66	Windows 2000	Apache/2.0.52 Debian GNU/Linux mod_python/3.1.3 Python/2.3.4 PHP/4.3.10-2 mod_ssl/2.0.52 OpenSSL/0.9.7e	6-Jun-2004	
Lembaga Ilmu Pengetahuan Indonesia Jakarta 12720	202.47.65.66	unknown	Apache/1.3.19 Unix SuSE/Linux	5-Jun-2004	

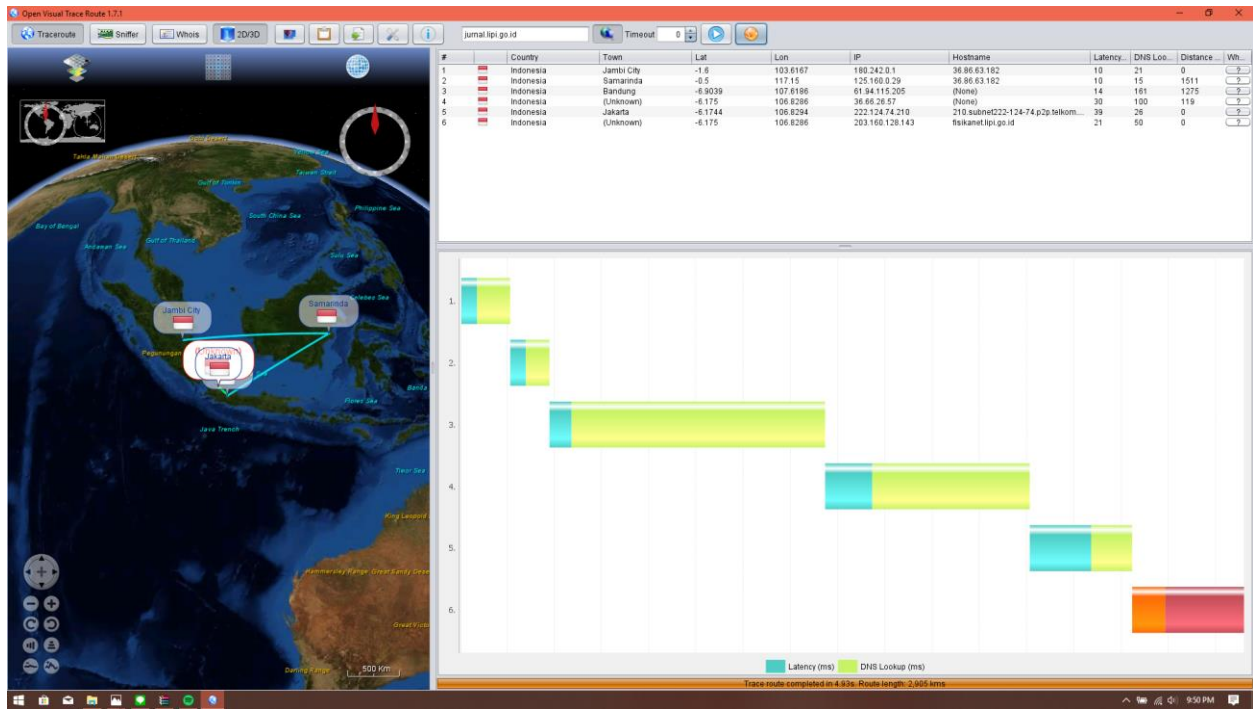
Pada gambar diatas berupa site report dari web dalam negeri yang saya gunakan.

## Search Results

There are 5213 CVE entries that match your search.

Name	Description
<a href="#">CVE-2019-7675</a>	An issue was discovered on MOBOTIX S14 MX-V4.2.1.61 devices. The default management application is delivered over cleartext HTTP with Basic Authentication, as demonstrated by the /admin/index.html URL.
<a href="#">CVE-2019-7323</a>	GUP (generic update process) in LightySoft LogMX before 7.4.0 does not properly verify the authenticity of updates, which allows man-in-the-middle attackers to execute arbitrary code via a Trojan horse update. The update process relies on cleartext HTTP. The attacker could replace the LogMXUpdater.class file.
<a href="#">CVE-2019-6802</a>	CRLF Injection in pypiserver 1.2.5 and below allows attackers to set arbitrary HTTP headers and possibly conduct XSS attacks via a %0d%0a in a URI.
<a href="#">CVE-2019-6500</a>	In Axdway File Transfer Direct 2.7.1, an unauthenticated Directory Traversal vulnerability can be exploited by issuing a specially crafted HTTP GET request with %2e instead of '.' characters, as demonstrated by an initial /h2hdocumentation/%2e%2e/ substring.
<a href="#">CVE-2019-6447</a>	The ES File Explorer File Manager application through 4.1.9.7.4 for Android allows remote attackers to read arbitrary files or execute applications via TCP port 59777 requests on the local Wi-Fi network. This TCP port remains open after the ES application has been launched once, and responds to unauthenticated application/json data over HTTP.
<a href="#">CVE-2019-6256</a>	A Denial of Service issue was discovered in the LIVE555 Streaming Media libraries as used in Live555 Media Server 0.93. It can cause an RTSPServer crash in handleHTTPCmd_TunnelingPOST, when RTSP-over-HTTP tunneling is supported, via x-sessioncookie HTTP headers in a GET request and a POST request within the same TCP session. This occurs because of a call to an incorrect virtual function pointer in the readSocket function in GroupsockHelper.cpp.
<a href="#">CVE-2019-5489</a>	The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of the fncore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.
<a href="#">CVE-2019-3822</a>	libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header ("lib/vauth/ntlm.c:curl_auth_create_ntlm_type3_message()"), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large "nt response" data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a "large value" needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header.
<a href="#">CVE-2019-3581</a>	Improper input validation in the proxy component of McAfee Web Gateway 7.8.2.0 and later allows remote attackers to cause a denial of service via a crafted HTTP request parameter.
<a href="#">CVE-2019-3500</a>	aria2c in aria2 1.33.1, when --log is used, can store an HTTP Basic Authentication username and password in a file, which might allow local users to obtain sensitive information by reading this file.
<a href="#">CVE-2019-3462</a>	Incorrect sanitization of the 302 redirect field in HTTP transport method of apt versions 1.4.8 and earlier can lead to content injection by a MITM attacker, potentially leading to remote code execution on the target machine.
<a href="#">CVE-2019-2550</a>	Vulnerability in the Oracle FLEXCUBE Direct Banking component of Oracle Financial Services Applications (subcomponent: Logoff Page). The supported version that is affected is 12.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:A/N).
<a href="#">CVE-2019-2549</a>	Vulnerability in the Oracle FLEXCUBE Direct Banking component of Oracle Financial Services Applications (subcomponent: Logoff Page). The supported version that is affected is 12.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Direct Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Direct Banking, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Direct Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Direct Banking accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:A/N).
<a href="#">CVE-2019-2546</a>	Vulnerability in the Oracle Applications Manager component of Oracle E-Business Suite (subcomponent: SQL Extensions). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).
<a href="#">CVE-2019-2538</a>	Vulnerability in the Oracle Managed File Transfer component of Oracle Fusion Middleware (subcomponent: MFT Runtime Server). Supported versions that are affected are 19.1.0.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Managed File Transfer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Managed File Transfer accessible data as well as unauthorized read access to a subset of Oracle Managed File Transfer accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N).
<a href="#">CVE-2019-2519</a>	Vulnerability in the PeopleSoft Enterprise SCM eProcurement component of Oracle PeopleSoft Products (subcomponent: Manage Requisition Status). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM eProcurement. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise SCM eProcurement, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise SCM eProcurement accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM eProcurement accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:A/N).

Pada gambar diatas berupa CVE dari web dalam negeri yang saya gunakan



Pada gambar diatas berupa tracking dari web dalam negeri yang saya gunakan.