LAPORAN

TUGAS MANAJEMEN KEAMANAN INFORMASI

MENGANALISIS WEB NAKER.GO.ID DAN LUINO.CO.ID

OLEH :

RATIH FILARESY

09031281520099

SI Regular 6A

Dosen Pembimbing : Deris Stiawan, M.T., Ph.D.

SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

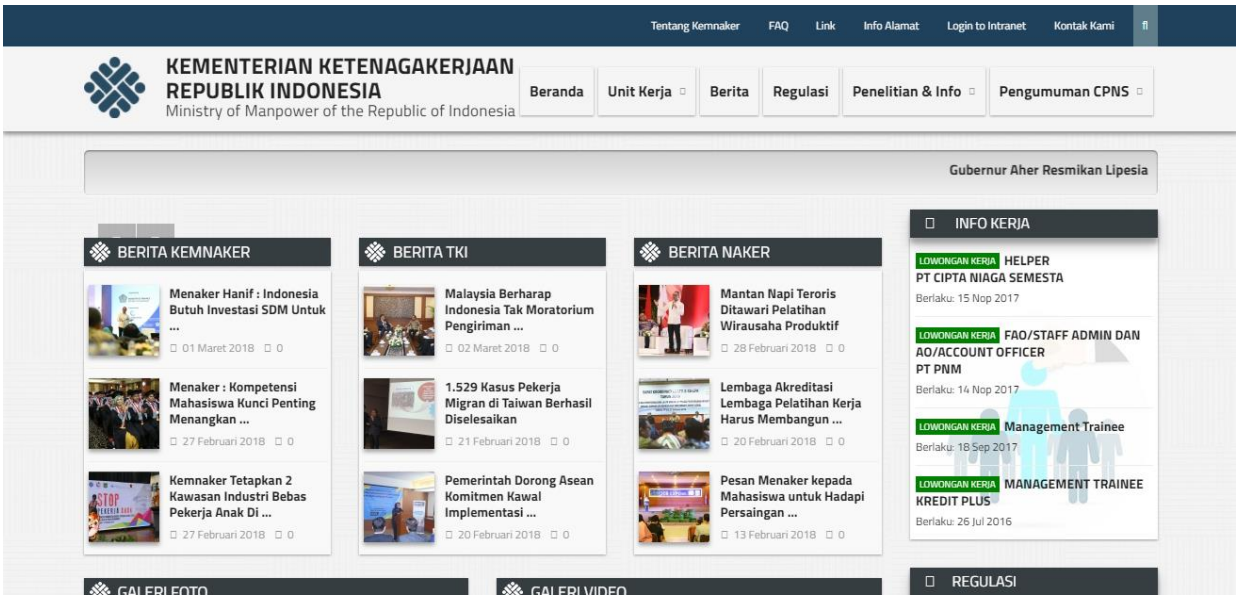
UNIVERSITAS SRIWIJAYA 2018

Melakukan scanning network dan scanning system dengan mengunkanan netcraft.com, dengan web target www.naker.go.id berikut adalah tabel tampilan dari scanning network dan scanning system :

WWW.NAKER.GO.ID

Domain	naker.go.id
IP address	103.87.196.1
Site title	Kementerian Ketenagakerjaan Republik Indonesia
Date first seen	July 2015
Netblock Owner	Kementerian Ketenagakerjaan RI
Nameserver	ns1.telkomhosting.com
DNS admin	hostmaster@telkom.net.id
Nameserver organisation	whois.onlinenic.com
Created On	07-Nov-2014 02:24:58 UTC
Last Updated On	23-Dec-2017 00:07:31 UTC
Expiration Date	07-Nov-2018 23:59:59 UTC
OS	Linux
Web server	Apache/2.4.12 Ubuntu
Client-Side	JavaScrpt
Character Encodeing	UTF8
HTTP Compression	Gzip Content Encoding

Web naker ini adalah web Kementrian Ketenagakerjaan Republik Indonesia yang manapilkan tentang berita Kemnaker, berita TKI, berita Naker, Info Kerja dan yang lainya yang berhubungan dengan ketenagakerjaan yang bisa dilihat seperti gambar dibawah ini.



Menganalisis menggunakan CVE untuk melihat kelemahan dari web server dan OS yang digunakan oleh naker.go.id , sebagai berikut :

- OS yang digunakan adalah Linux

Setelah dicari kelemahan pada linux di Common Vulnerabilities and Exposures, CVE menapilkan kekurangan kekurangan yang ada pada linux seperti gambar yang ditampilkan dibawah ini

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-5703	787		DoS	2018-01-16	2018-02-15	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.14.11 allows attackers to cause a denial of service (slab out-of-bounds write) or possibly have unspecified other impact via vectors involving TLS.														
2	CVE-2017-18017	416		DoS Mem. Corr.	2018-01-03	2018-01-17	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The tcpmss_mangle_packet function in net/netfilter/xt_TCPMSS.c in the Linux kernel before 4.11, and 4.9.x before 4.9.36, allows remote attackers to cause a denial of service (use-after-free and memory corruption) or possibly have unspecified other impact by leveraging the presence of xt_TCPMSS in an iptables action.														
3	CVE-2017-15126	416			2018-01-14	2018-02-06	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
A use-after-free flaw was found in fs/userfaultfd.c in the Linux kernel before 4.13.6. The issue is related to the handling of fork failure when dealing with event messages. Failure to fork correctly can lead to a situation where a fork event will be removed from an already freed list of events with userfaultfd_ctx_put().														
4	CVE-2017-13715	20		DoS Exec Code	2017-08-28	2017-09-08	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The __skb_flow_dissect function in net/core/flow_dissector.c in the Linux kernel before 4.3 does not ensure that n_proto, ip_proto, and thoff are initialized, which allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a single crafted MPLS packet.														
5	CVE-2017-12762	119		Overflow	2017-08-09	2017-08-25	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
In /drivers/isdn/i4l/isdn_net.c: A user-controlled buffer is copied into a local buffer of constant size using strcpy without a length check which can cause a buffer overflow. This affects the Linux kernel 4.9-stable tree, 4.12-stable tree, 3.18-stable tree, and 4.4-stable tree.														
6	CVE-2017-11176	416		DoS	2017-07-11	2018-01-26	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact.														
7	CVE-2017-8890	415		DoS	2017-05-10	2018-01-04	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call.														
8	CVE-2017-7895	189			2017-04-28	2018-01-04	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The NFSv2 and NFSv3 server implementations in the Linux kernel through 4.10.13 lack certain checks for the end of a buffer, which allows remote attackers to trigger pointer-arithmetic errors or possibly have unspecified other impact via crafted requests, related to fs/nfsd/nfs3xdr.c and fs/nfsd/nfsxdr.c.														

- Web server yang digunakan yaitu Apache/2.4.12 Ubuntu

  Kelemahan pada webserver yang digunakan yaitu seperti gambar yang dibawah ini

Name	Description
CVE-2017-8386	git-shell in git before 2.4.12, 2.5.x before 2.5.6, 2.6.x before 2.6.7, 2.7.x before 2.7.5, 2.8.x before 2.8.5, 2.9.x before 2.9.4, 2.10.x before 2.10.3, 2.11.x before 2.11.2, and 2.12.x before 2.12.3 might allow remote authenticated users to gain privileges via a repository name that starts with a - (dash) character.
CVE-2015-0228	The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

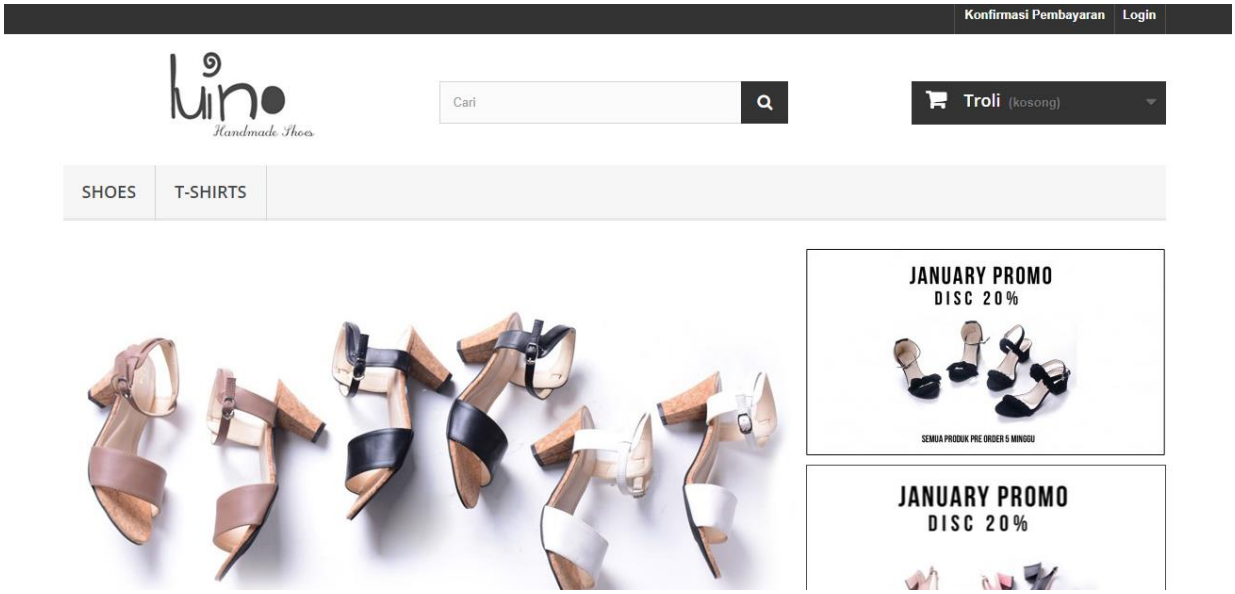
Pada target web yang kedua, saya juga melakukan scanning network dan scanning system dengan mengunkanan netcraft.com, dengan web target www.luino.co.id berikut adalah tabel tampilan dari scanning network dan scanning system :

WWW. LUINO.CO.ID

Domain	Luino.co.id
IP address	103.247.9.25
Site title	Luino Store
Domain registrar	Pandi.or.id
Organisation	Luino, jl delta barat 12 blok c 141, bekasi 17148, indonesia
Netblock Owner	Rumahweb Indonesia
Nameserver	ns1.rumahweb.com
DNS admin	notroot@rumahweb.co.id
Reverse DNS	Brahma.satu.rumahweb.com
Nameserver organisation	whois.rumahweb.com
Hosting company	Rumahweb.com
OS	Linux
Web server	LiteSpeed
Client-Side	JavaScrpt
Character Encodeing	UTF8

HTTP Compression	Gzip Content Encoding
Privacy Management	P3P

Web luino adalah web yang menjual sepatu, tas, dan baju dengan brand dia sendiri. Tampilan web ini bisa dilihat seperti gambar dibawah ini.



Menganalisis menggunakan CVE untuk melihat kelemahan dari web server dan OS yang digunakan oleh luino.co.id , sebagai berikut :

- OS yang digunakan yaitu linux

  Bayak terdapat kelamahan linux saat dicari pada web cve details

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-5703	787		DoS	2018-01-16	2018-02-15	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.14.11 allows attackers to cause a denial of service (slab out-of-bounds write) or possibly have unspecified other impact via vectors involving TLS.														
2	CVE-2017-18017	416		DoS Mem. Corr.	2018-01-03	2018-01-17	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The tcpmss_mangle_packet function in net/netfilter/xt_TCPMSS.c in the Linux kernel before 4.11, and 4.9.x before 4.9.36, allows remote attackers to cause a denial of service (use-after-free and memory corruption) or possibly have unspecified other impact by leveraging the presence of xt_TCPMSS in an iptables action.														
3	CVE-2017-15126	416			2018-01-14	2018-02-06	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
A use-after-free flaw was found in fs/userfaultfd.c in the Linux kernel before 4.13.6. The issue is related to the handling of fork failure when dealing with event messages. Failure to fork correctly can lead to a situation where a fork event will be removed from an already freed list of events with userfaultfd_ctx_put().														
4	CVE-2017-13715	20		DoS Exec Code	2017-08-28	2017-09-08	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The __skb_flow_dissect function in net/core/flow_dissector.c in the Linux kernel before 4.3 does not ensure that n_proto, ip_proto, and thoff are initialized, which allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a single crafted MPLS packet.														
5	CVE-2017-12762	119		Overflow	2017-08-09	2017-08-25	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
In /drivers/isdn/i4l/isdn_net.c: A user-controlled buffer is copied into a local buffer of constant size using strcpy without a length check which can cause a buffer overflow. This affects the Linux kernel 4.9-stable tree, 4.12-stable tree, 3.18-stable tree, and 4.4-stable tree.														
6	CVE-2017-11176	416		DoS	2017-07-11	2018-01-26	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact.														
7	CVE-2017-8890	415		DoS	2017-05-10	2018-01-04	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call.														
8	CVE-2017-7895	189			2017-04-28	2018-01-04	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
The NFSv2 and NFSv3 server implementations in the Linux kernel through 4.10.13 lack certain checks for the end of a buffer, which allows remote attackers to trigger pointer-arithmetic errors or possibly have unspecified other impact via crafted requests, related to fs/nfsd/nfs3xdr.c and fs/nfsd/nfsxdr.c.														

- Web server yang digunakan yaitu LiteSpeed

  Kelemahan dari LiteSpeed

Name	Description
CVE-2015-3890	Use-after-free vulnerability in Open Litespeed before 1.3.10.
CVE-2012-4871	Cross-site scripting (XSS) vulnerability in service/graph_html.php in the administrator panel in LiteSpeed Web Server 4.1.11 allows remote attackers to inject arbitrary web script or HTML via the gtitle parameter.
CVE-2010-2333	LiteSpeed Technologies LiteSpeed Web Server 4.0.x before 4.0.15 allows remote attackers to read the source code of scripts via an HTTP request with a null byte followed by a .txt file extension.
CVE-2007-5654	LiteSpeed Web Server before 3.2.4 allows remote attackers to trigger use of an arbitrary MIME type for a file via a "%00." sequence followed by a new extension, as demonstrated by reading PHP source code via requests for .php%00.txt files, aka "Mime Type Injection."
CVE-2005-3695	Cross-site scripting (XSS) vulnerability in admin/config/confMgr.php in LiteSpeed Web Server 2.1.5 allows remote attackers to inject arbitrary web script or HTML via the m parameter.