

# Laporan Manajemen Keamanan Informasi

Pada Website [alpha.kemenkeu.go.id](http://alpha.kemenkeu.go.id) dan [www.antarafoto.com](http://www.antarafoto.com)



Dibuat Oleh :

Nim : 09031181520019

Nama : Ridwan Ariana

Dosen Pengampuh mata kuliah :

Derris stiawan,MT,Phd

Jurusan Sistem Informasi

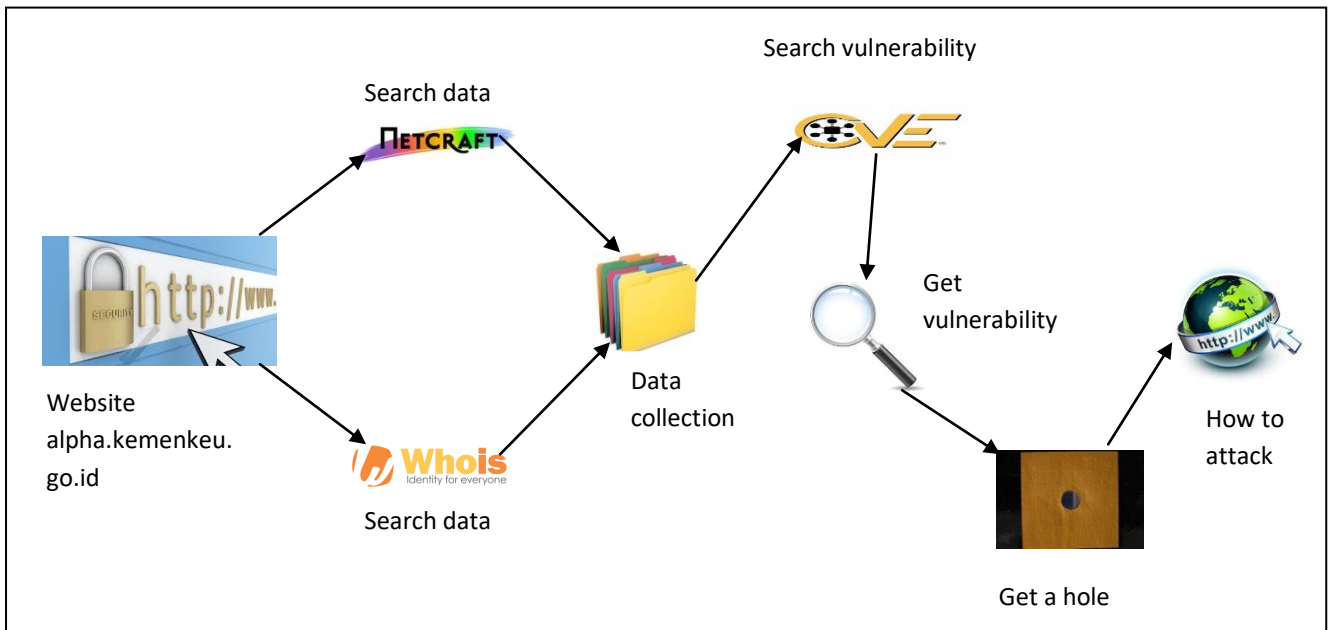
Fakultas Ilmu Komputer

Universitas Sriwijaya

2017-2018

## Analisa scanning target website : [alpha.kemenkeu.go.id](http://alpha.kemenkeu.go.id)

Pada bagian scanning website ini, website yang dipilih adalah website [alpha.kemenkeu.go.id](http://alpha.kemenkeu.go.id) . yang dimana website ini merupakan website kementerian keuangan negara yang berada di Jakarta . Berdasarkan hasil analisa scanning ini didapatkanlah alur perjalanan seperti berikut:



**Gambar alur scanning website**

Dari alur diatas akan dijelaskan pada tahapan dibawah ini :

### 1. Tahap data collection

Tahap ini merupakan tahap pengumpulan informasi yang bersangkutan dengan website seperti ip address, os yang dipakai, wb server yang digunakan, informasi domain, alamat, nomor telepon, dan sebagainya. Dalam laporan ini ,tahap data collecting menggunakan 2 website untuk mencari informasi website. Website tersebut adalah netcraft.com dan whois.com.

Berikut adalah hasil dari data collecting menggunakan website tersebut:

## 1. Whois.com

kemenkeu.go.id

Updated 1 day ago 

```
Domain ID:PANDI-DO165709
Domain Name:KEMENKEU.GO.ID
Created On:17-Oct-2011 13:29:31 UTC
Last Updated On:23-Aug-2017 02:27:09 UTC
Expiration Date:25-Oct-2018 23:59:59 UTC
Status:ok
Registrant ID:cahyon-98451
Registrant Name:Cahyono Tri Birowo
Registrant Organization:Kementerian Keuangan Republik Indonesia
Registrant Street1:Lapangan Banteng Timur No 2-4
Registrant City:Jakarta
Registrant State/Province:DKI Jakarta
Registrant Postal Code:10710
Registrant Country:ID
Registrant Phone:+62.213441478
Registrant FAX:+62.213441478
Registrant Email:birowo@depkeu.go.id
```


Dan dengan menggunakan aplikasi zenmap didapatkanlah port yang aktif yaitu :

Discovered open port 443/tcp on 202.61.126.229

Discovered open port 80/tcp on 202.61.126.229

## 2. Netcraft.com

### Network

Site	<a href="http://alpha.kemenkeu.go.id">http://alpha.kemenkeu.go.id</a>	Netblock Owner	Pusat Sistem Informasi dan Teknologi Keuangan ( Pusintek )
Domain	<a href="http://kemenkeu.go.id">kemenkeu.go.id</a>	Nameserver	ns1.telkomhosting.com
IP address	202.61.126.229	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	kemenkeu.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
<a href="#">Pusat Sistem Informasi dan Teknologi Keuangan Pusintek Government / Direct member IDNIC Jakarta</a>	202.61.126.229	Linux	Microsoft-IIS/8.5	6-Mar-2018

## 2. tahap vulnerability

Pada tahap ini ,website yang telah di temukan data-data pentingnya seperti os,ip, web server,dan sebagainya.dengan data yang telah dikumpulkan di tahapdata

collecting, maka kita dapat mencari vulnerability/celah dari website tersebut. Hal ini dapat dilakukan karena website/sistem pasti terdapat celah dan tidak aman sepenuhnya. Dalam tahap ini, kita menggunakan suatu website bernama cvedetails.com. Website tersebut adalah . berikut adalah hasil pencarian celah/vulnerability pada website alpha.kemenkeu.go.id :

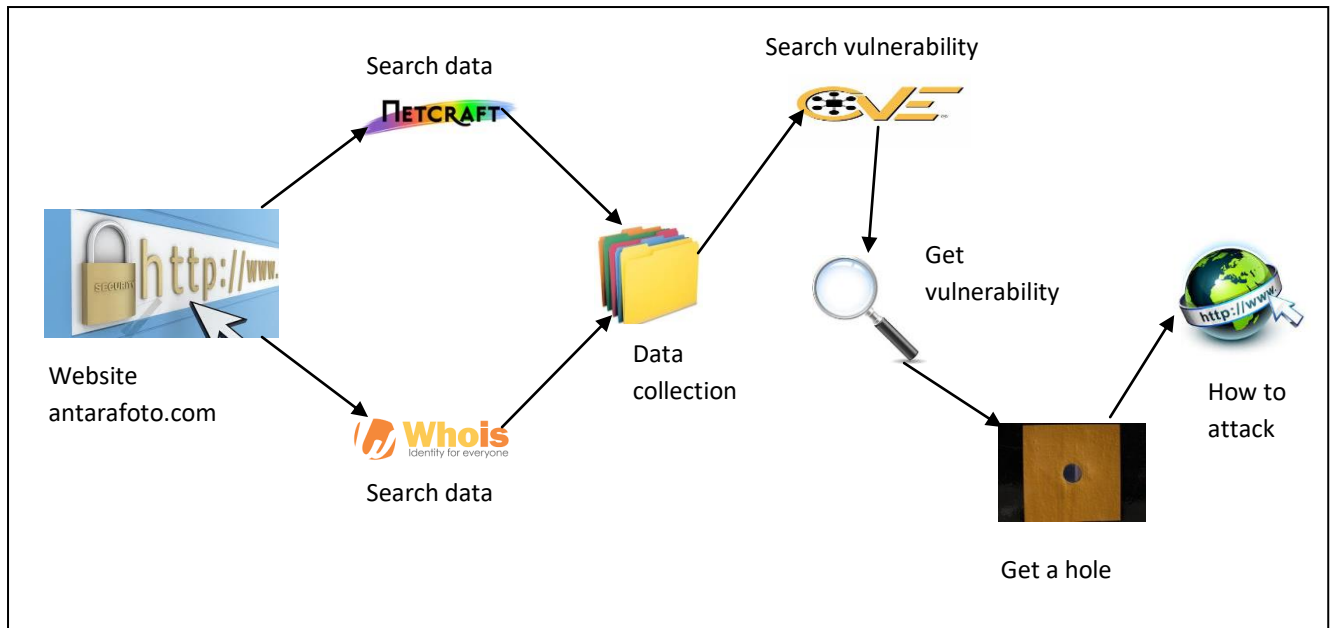
- CVSS Scores & Vulnerability Types	
CVSS Score	<b>5.1</b>
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	High (Specialized access conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Bypass a restriction or similar
CWE ID	<a href="#">254</a>

### Gambar vulnerable dari web server Microsoft-IIS/8.5

Setelah dicari celah berdasarkan web server dari website alpha.kemenkeu.go.id didapatkan suatu hasil dengan skor yang paling tinggi (seperti pada gambar). Yang dapat disimpulkan bahwa semakin besar skor dari website cvedetails terkait webserver tersebut, semakin besar celah yang dapat dimasuki/dibobol masuk secara paksa.

## Analisa scanning target website : [antarafoto.com](http://antarafoto.com)

Pada bagian scanning website ini, website yang dipilih adalah website [antarafoto.com](http://antarafoto.com) . yang dimana website ini merupakan website berita foto tentang seputaran kejadian yang ada di Indonesia seperti foto berita festival danau sunter yang lagi hits akhir-akhir ini. Berdasarkan hasil analisa scanning ini didapatkanlah alur perjalanan seperti berikut :



**Gambar alur scanning website**

Dari alur diatas akan dijelaskan pada tahapan dibawah ini :

### 2. Tahap data collection

Tahap ini merupakan tahap pengumpulan informasi yang bersangkutan dengan website seperti ip address, os yang dipakai, wb server yang digunakan, informasi domain, alamat, nomor telepon, dan sebagainya. Dalam laporan ini ,tahap data collecting menggunakan 2 website untuk mencari informasi website. Website tersebut adalah netcraft.com dan whois.com.

Berikut adalah hasil dari data collecting menggunakan website tersebut:

### 3. Whois.com

**antarafoto.com** Updated 1 second ago

DOMAIN INFORMATION	
Domain:	antarafoto.com
Registrar:	OnlineNIC, Inc.
Registration Date:	2006-12-19
Expiration Date:	2019-12-19
Updated Date:	2016-10-25
Status:	clientTransferProhibited
Name Servers:	ns1.antara.net.id ns2.antara.net.id

REGISTRANT CONTACT	
Name:	Syofiar
Organization:	Biro Foto LKBN ANTARA
Street:	Jl. Antara No.59 Pasar Baru
City:	Jakarta Pusat
State:	DKI Jakarta
Postal Code:	10710
Country:	ID
Phone:	+62.2134833607
Fax:	+62.2134833607
Email:	noc@antara.net.id

Dan dengan menggunakan aplikasi zenmap didapatkanlah port yang aktif yaitu :

Discovered open port 993/tcp on 183.182.92.132

Discovered open port 995/tcp on 183.182.92.132


Discovered open port 443/tcp on 183.182.92.132

Discovered open port 80/tcp on 183.182.92.132

Discovered open port 465/tcp on 183.182.92.132

#### 4. Netcraft.com

##### ☐ Network

Site	<a href="http://antarafoto.com">http://antarafoto.com</a>	Netblock Owner	LKBN ANTARA
Domain	<a href="http://antarafoto.com">antarafoto.com</a>	Nameserver	ns1.antara.net.id
IP address	183.182.92.132	DNS admin	root@antarafoto.com
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	unknown
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="#">LKBN ANTARA Corporate / Direct member IDNIC Jl. Medan Merdeka Selatan No. 17 Wisma Antara Lt.19-20 Jakarta, 10110</a>	183.182.92.132	Linux	Apache/2.2.15 CentOS	6-Mar-2018
<a href="#">LKBN ANTARA Corporate / Direct member IDNIC Jl. Medan Merdeka Selatan No. 17 Wisma Antara Lt.19-20 Jakarta, 10110</a>	183.182.92.132	Linux	Apache/2.0.52 Red Hat	3-Mar-2011

#### 2. tahap vulnerability

Pada tahap ini ,website yang telah di temukan data-data pentingnya seperti os,ip, web server,dan sebagainya.dengan data yang telah dikumpulkan di tahapdata collecting,maka kita dapat mencari vulnerability/celah dari website tersebut. Hal ini dapat dilakukan karena website/sistem pasti terdapat celah dan tidak aman sepenuhnya. Dalam tahap ini,kita menggunakan suatu website bernama cvedetails.com. Website tersebut adalah . berikut adalah hasil pencarian celah/vulnerability pada website antarafoto.com:

#### – CVSS Scores & Vulnerability Types

CVSS Score	<b>7.8</b>
Confidentiality Impact	<b>None</b> (There is no impact to the confidentiality of the system.)
Integrity Impact	<b>None</b> (There is no impact to the integrity of the system)
Availability Impact	<b>Complete</b> (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	<b>Low</b> (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. )
Authentication	<b>Not required</b> (Authentication is not required to exploit the vulnerability.)
Gained Access	<b>None</b>
Vulnerability Type(s)	Denial Of Service
CWE ID	<a href="#">399</a>

#### **Gambar vulnerable dari web server Apache/2.2.15 CentOS**

Setelah dicari celah berdasarkan web server dari website antarafoto.com didapatkan suatu hasil dengan skor yang paling tinggi(seperti pada gambar). Yang dapat disimpulkan bahwa semakin besar skor dari website cvedetails terkait webserver tersebut, semakin besar celah yang dapat dimasuki/dibobol masuk secara paksa.