Laporan Manajemen Keamanan Informasi

Pada Website ptba.co.id/kotaprabumulih.go.id

Dibuat Oleh :

Nim : 09031181520035

Nama : ORIEN PATRIANA

Jurusan Sistem Informasi

Fakultas Ilmu Komputer

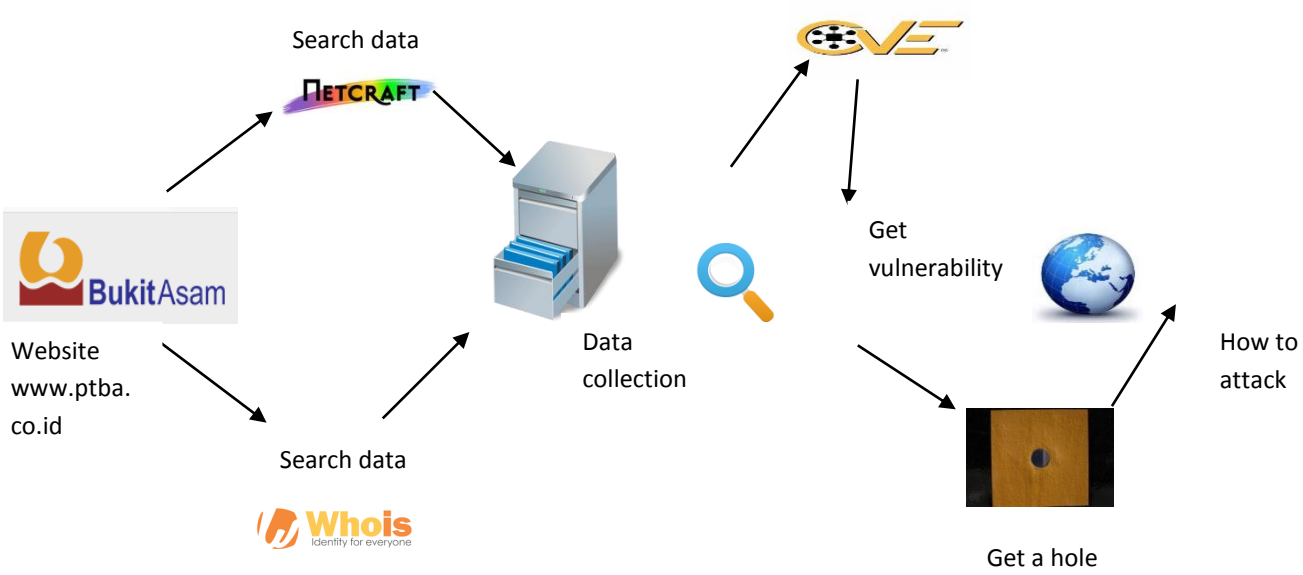
Universitas Sriwijaya

2017-2018

WWW.PTBA.CO.ID

Analisa scanning target website : www.ptba.co.id

Pada bagian scanning web, website yang dipilih adalah website www.ptba.co.id dimana website ini merupakan website pemerintahan yang berada di kota Prabumulih. Berdasarkan hasil analisa scanning didapatkanlah alur perjalanan seperti dibawah ini:



Gambar alur scanning website

Dari alur diatas dijelaskan bahwa pada tahapan berikut 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

ptba.co.id Updated 1 second ago

```
Domain ID:PANDI-DO151723
Domain Name:PTBA.CO.ID
Created On:04-Nov-2009 13:28:45 UTC
Last Updated On:11-Oct-2016 11:57:06 UTC
Expiration Date:05-Nov-2018 23:59:59 UTC
Status:ok
Registrant ID:08tlomb1
Registrant Name:Suharno
Registrant Organization:PT. Tambang Batubara Bukit Asam Tbk.
Registrant Street1:Menara Kadin Lt. 15
Registrant Street2:Jl. H.R. Rasuna Said Kav. 2-3
Registrant Street3:Kuningan
Registrant City:Jakarta Selatan
Registrant State/Province:DKI Jakarta
Registrant Postal Code:12950
Registrant Country:ID
Registrant Phone:+62.215254014
Registrant Email:tlombe@bukitasam.co.id
```

2. Netcraft.com

Network

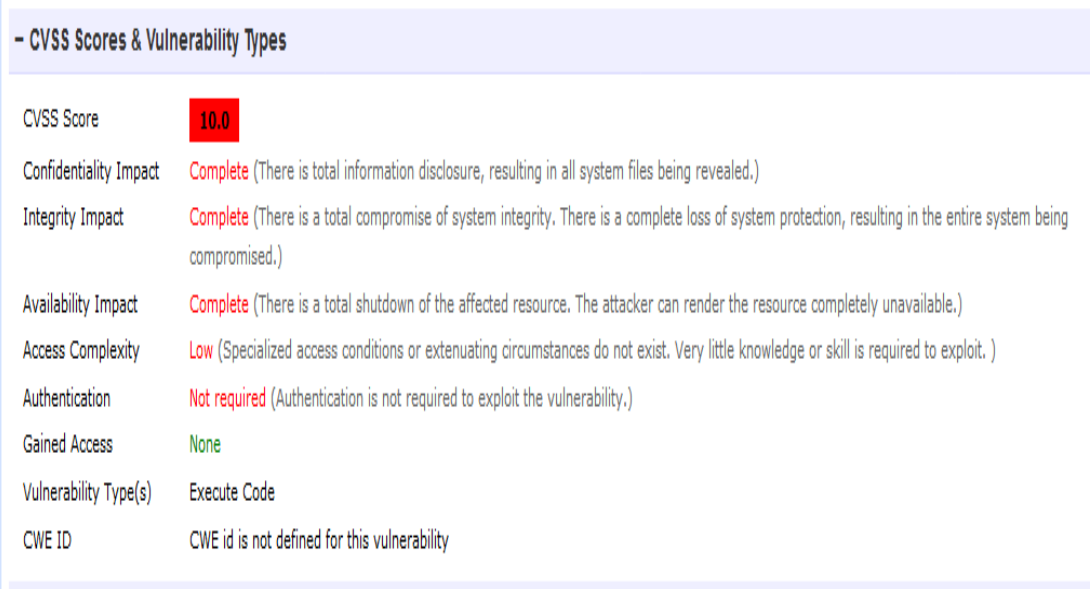
Site	http://ptba.co.id	**Netblock Owner**	Network Operations Center
Domain	ptba.co.id	**Nameserver**	ns1.cbn.net.id
IP address	*unknown*	**DNS admin**	hostmaster@cbn.net.id
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	pandi.or.id	**Nameserver organisation**	whois.pandi.or.id
Organisation	PT. Tambang Batubara Bukit Asam Tbk., Menara Kadin Lt. 15, Jl. H.R. Rasuna Said Kav. 2-3, Kuningan, Jakarta Selatan, 12950, Indonesia	**Hosting company**	*unknown*
Top Level Domain	Indonesia (.co.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Network Operations Center PT. Cyberindo Aditama Manggala Wanabakti IV, Suite 808A Jl. Gatot Subroto, Jakarta Jakarta 10270	202.158.49.50	Linux	Apache/2.2.14 Ubuntu	10-Jul-2015

3. Tahap vulnerability

   Pada tahap ini ,website yang telah di temukan data-data pentingnya. Dengan pengumpulan data pada tahap data collecting, maka kita dapat mencari vulnerability/celah dari website tersebut. Hal ini dapat dilakukan karena pasti pada website/sistem terdapat celah dan tidak aman sepenuhnya. Dalam tahap ini,kita menggunakan suatu website bernama cvedetails.com. berikut adalah hasil pencarian celah/vulnerability pada website www.ptba.co.id:



- CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	CWE id is not defined for this vulnerability

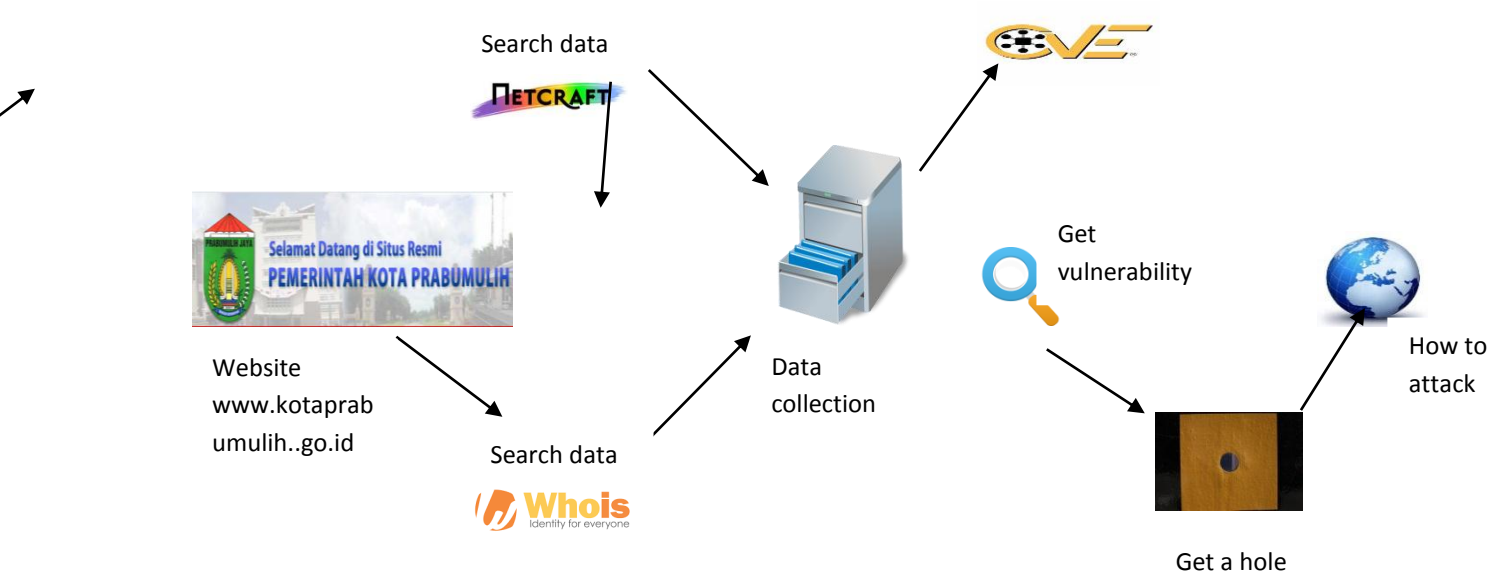
Gambar vulnerable dari web server Apache/2.2.14 Ubuntu

Setelah dicari celah berdasarkan web server dari website www.ptba.co.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

WWW.KOTAPRABUMULIH.GO.ID

Analisa scanning target website : www.kotaprabumulih.go.id

Pada bagian scanning web, website yang dipilih adalah website www.kotaprabumulih.go.id dimana website ini merupakan website pemerintahan yang berada di kota Prabumulih. Berdasarkan hasil analisa scanning didapatkanlah alur perjalanan seperti dibawah ini:



Gambar alur scanning website

Dari alur diatas dijelaskan bahwa pada tahapan berikut 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

kotaprabumulih.go.id

Updated 1 second ago

```
Domain ID:PANDI-DO53545
Domain Name:KOTAPRABUMULIH.GO.ID
Created On:10-May-2000 13:23:33 UTC
Last Updated On:21-Jan-2018 09:27:19 UTC
Expiration Date:31-Jan-2020 23:59:59 UTC
Status:ok
Registrant ID:kominf-7499
Registrant Name:Kominfo Prabumulih
Registrant Organization:Dinas Komunikasi dan Informatika Kota Prabumulih
Registrant Street1:Kantor Pemerintah Kota Prabumulih Lantai 2
Registrant Street2:Jalan Raya Prabumulih-Palembang Km.12  Desa Sindur
Registrant City:Prabumulih
Registrant State/Province:Sumatra Selatan
Registrant Postal Code:31142
Registrant Country:ID
Registrant Phone:+62.7133920052
Registrant FAX:+62.7133920052
Registrant Email:penkot@kotaprabumulih.go.id
```

2. Netcraft.com

Network

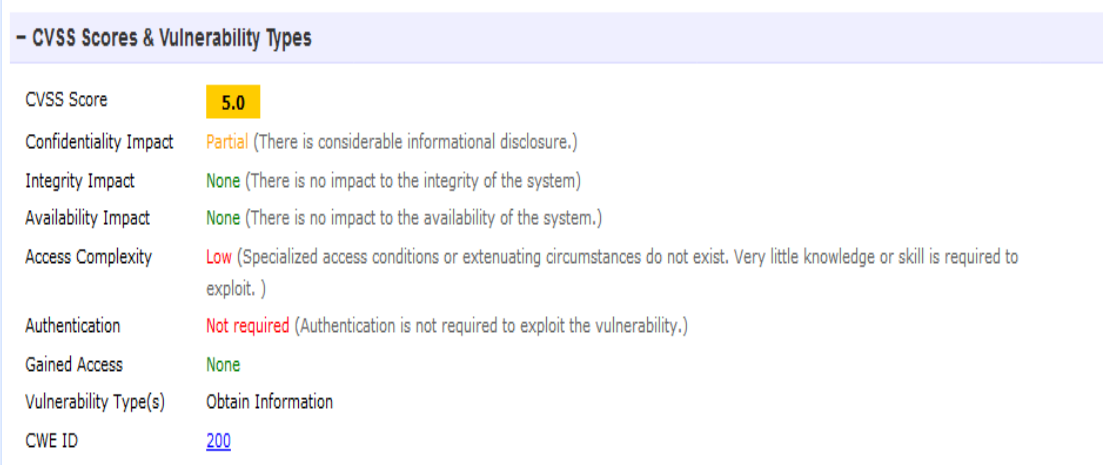
Site	http://www.kotaprabumulih.go.id	**Netblock Owner**	PT Cloud Hosting Indonesia
Domain	kotaprabumulih.go.id	**Nameserver**	ns01.cloudhost.id
IP address	103.15.226.60	**DNS admin**	admin@nightkidz.net
IPv6 address	*Not Present*	**Reverse DNS**	iix4.cloudhost.id
Domain registrar	*unknown*	**Nameserver organisation**	whois.pandi.or.id
Organisation	*unknown*	**Hosting company**	*unknown*
Top Level Domain	Indonesia (.go.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
PT Cloud Hosting Indonesia Corporate / Direct Member IDNIC Pinus Raya Reni Jaya AG-1 No.01 Pamulang Barat, Pamulang Tangerang Selatan, Banten	103.15.226.60	Linux	LiteSpeed	7-Mar-2018
Ronny Isdhianto Lebak Indah Jaya I No. 15 Surabaya OT ID 60134	67.228.98.196	Linux	LiteSpeed	29-Mar-2016
Internet Service Provider Jl. Jakarta No.5 Ulak Karang Padang Sumatra Barat 2513	119.2.71.99	Linux	Apache	27-Jun-2012
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	203.130.196.40	Windows Server 2003	Microsoft-IIS/6.0	28-Nov-2011
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	-	Microsoft-IIS/5.0	7-Apr-2005
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows Server 2003	unknown	5-Apr-2005
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows Server 2003	Microsoft-IIS/5.0	2-Apr-2005
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows Server 2003	unknown	1-Apr-2005
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows Server 2003	Microsoft-IIS/5.0	28-Mar-2005
PT TELEKOMUNIKASI INDONESIA Jln Japati No 1	203.130.196.20	Windows Server 2003	unknown	26-Mar-2005

3. Tahap vulnerability

   Pada tahap ini ,website yang telah di temukan data-data pentingnya. Dengan pengumpulan data pada tahap data collecting, maka kita dapat mencari vulnerability/celah dari website tersebut. Hal ini dapat dilakukan karena pasti pada website/sistem terdapat celah dan tidak aman sepenuhnya. Dalam tahap ini,kita menggunakan suatu website bernama cvedetails.com. berikut adalah hasil pencarian celah/vulnerability pada website www.kotaprabumulih.go.id:



– CVSS Scores & Vulnerability Types

CVSS Score	5.0
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Obtain Information
CWE ID	200

Gambar vulnerable dari web server Litespeed

Setelah dicari celah berdasarkan web server dari website www.kotaprabumulih.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.