LAPORAN

TUGAS MANAJEMEN KEAMANAN INFORMASI

OLEH :

MADRI (09031281520109)

SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

ANALISIS KEAMANAN WEBSITE

1. BUNGOKAB.GO.ID

a. Scanning

pada proses scanning di dapatkan informasi-informasi website bungokab.go.id sebagai berikut :

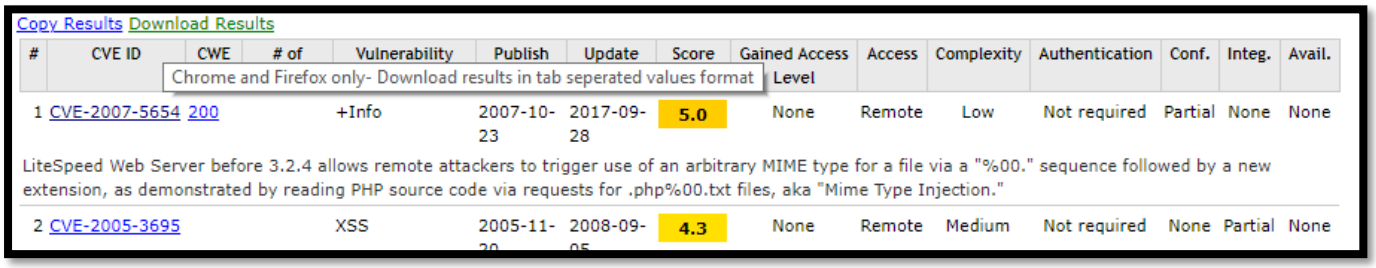
Site title	Pemerintah Kabupaten Bungo | bungokab.go.id	Server-Side	PHP Enabled
Date first seen	Februari 2007	Client-Side	JavaScript
Primary language	Indonesia	PHP Application	CodeIgniter Framework
Site	http://www.bungokab.go.id	Doctype	HTML5
Domain	bungokab.go.id	Os	Linux
IP address	45.64.98.18	Web server	LiteSpeed
Top Level Domain	Indonesia (.go.id)	Hosting country	ID
Netblock Owner	Argon Data Communication	Reverse DNS	server18id.galuhmedia.co.id
Nameserver	ns1.galuhweb.net	Nameserver organisation	whois.PublicDomainRegistry.com
DNS admin	root@server18id.galuhmedia.co.id	Last update	11 April 2017
Create on	17 November 2006	Expiration date	31 Januari 2019

Dan dengan menggunakan aplikasi zenmap didapatkanlah port yang yang terbuka pada website bungokab.go.id :

- Discovered open port 53/tcp on 45.64.98.18

b. Vurnerability

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 website cvedetails.com. Berikut adalah hasil pencarian celah/vulnerability pada website bungokab.go.id :



Copy Results Download Results

#	CVE ID	CWE	# of	Vulnerability	Publish	Update	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
				Chrome and Firefox only- Download results in tab seperated values format										
1	CVE-2007-5654	200		+Info	2007-10-23	2017-09-28	5.0	None	Remote	Low	Not required	Partial	None	None
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."														
2	CVE-2005-3695			XSS	2005-11-20	2008-09-05	4.3	None	Remote	Medium	Not required	None	Partial	None

Vurnerability Details : CVE-2007-5654

LiteSpeed Web Server sebelum 3.2.4 memungkinkan penyerang jarak jauh untuk memicu penggunaan jenis MIME yang sewenang-wenang untuk sebuah file melalui "% 00." urutan diikuti oleh ekstensi baru, seperti yang ditunjukkan dengan membaca kode sumber PHP melalui permintaan file .php% 00.txt, alias "Mime Type Injection".

CVSS Score & Vurnerability

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

2. Bhinneka.Com

a. Scanning

pada proses scanning di dapatkan informasi-informasi website bungokab.go.id sebagai berikut :

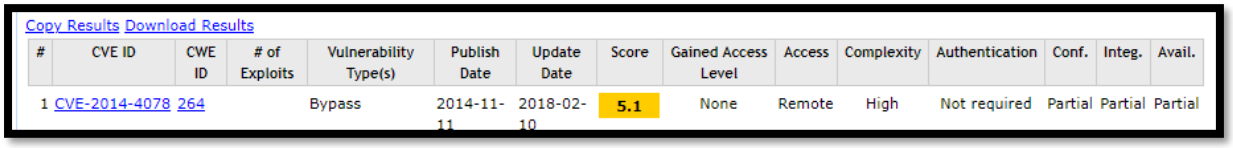
Site rank	584519	Network	Amazon Web Services - Route 53
Date first seen	September 1997	Nameserver	ns-1815.awsdns-34.co.uk
Primary language	English	DNS admin	awsdns-hostmaster@amazon.com
Site	http://bhinneka.com	Reverse DNS	ip49-178.cbn.net.id
Domain	bhinneka.com	Os	Windows Server 2012
IP address	202.158.49.178	Web server	Microsoft-IIS/8.5
Top Level Domain	Commercial entities (.com)	Hosting country	ID
Netblock Owner	Network Operations Center	Reverse DNS	server18id.galuhmedia.co.id
Nameserver	ns-1815.awsdns-34.co.uk	Nameserver organisation	whois.nic.uk
DNS admin	awsdns-hostmaster@amazon.com	Hosting company	CBN Internet
Reverse DNS	ip49-178.cbn.net.id	Registration Date	07 Agustus 1997
Update Date	03 Februari 2018	Expiration Date	06 Agustus 2027

Dan dengan menggunakan aplikasi zenmap didapatkanlah port yang yang terbuka pada website bhinneka.com :

- Discovered open port 443/tcp on 202.158.49.178
- Discovered open port 80/tcp on 202.158.49.178
- Discovered open port 53/tcp on 202.158.49.178

b. 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 bhinneka.com :



Copy Results Download Results

#	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-2014-4078	264		Bypass	2014-11-11	2018-02-10	5.1	None	Remote	High	Not required	Partial	Partial	Partial

Vurnerability Details : CVE-2014-4078

Fitur Keamanan IP di Microsoft Internet Information Services (IIS) 8.0 dan 8.5 tidak memproses dengan benar wildcard mengizinkan dan menolak aturan untuk domain dalam daftar "Alamat IP dan Pembatasan Domain", yang mempermudah penyerang jarak jauh untuk melewati aturan yang ditetapkan. via permintaan HTTP, alias "IIS Security Feature Bypass Vulnerability."

CVSS Score & Vurnerability

CVSS Score	5.1
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	264