BÁO CÁO

Dò quét thông tin lỗ hổng bảo mật hệ thông

THEO HỒ SƠ

HỒ SƠ: muc tieu 2

I Thông tin về dò quét

1.1 Thông tin tiến trình dò quét

1.1.1 Lần quét 1

_id	Name	Target	Date_Create	Date_Stop	Module	Status
6159d7c9c188719222e2b9cf	test_running	192.168.8.106	03/10/2021T12:18:17	03/10/2021T12:38:04	DirSearch, WebAppDetect, Nuclei, Wappalyzer, Nmap	StatusSuccess

1.2 Thông tin đối tượng dò quét

1.2.1 IP

TT	IN_IP
1	192.168.8.106

1.2.2 DOMAIN

TT	IN_DOMAIN
1	test.khoa.doamina

1.2.3 DESCRIBE

TT	IN_DESCRIBE
1	day la muc tieu 2

1.2.4 NAME

TT	IN_NAME
1	muc tieu 2

1.2.5 AUTHEN

TT	IN_AUTHEN
1	**username** **password** admin

II Thu thập, dò quét thông tin

2.1 SERVICES

TT	name	product	version	port	protocol
1	http	Apache httpd	2.4.10	8080.0	tcp
2	http	Joomla	3.4.3	8080.0	tcp

2.2 PORTS

TT	RECON_PORTS
1	8080.0

2.3 OS

TT	RECON_OS
1	linux
2	windows
3	embedded

2.4 WEBAPP

TT	RECON_WEBAPP
1	http://192.168.8.106:8080

2.5 CVE

2.6 VULN

TT	name	host	matched	ip	results
1	robots.txt file	http://192.168.8.106:8080	http://192.168.8.106:8080/robots.txt	192.168.8.106	[]
2	Clickjacking (Missing XFO header)	http://192.168.8.106:8080	http://192.168.8.106:8080	192.168.8.106	[]
3	Clickjacking (Missing XFO header)	http://192.168.8.106:8080/	http://192.168.8.106:8080/	192.168.8.106	[]
4	Joomla htaccess file disclosure	http://192.168.8.106:8080	http://192.168.8.106:8080/htaccess.txt	192.168.8.106	[]
5	Joomla Panel	http://192.168.8.106:8080/	http://192.168.8.106:8080/administrator/	192.168.8.106	[]
6	CSP Not Enforced	http://192.168.8.106:8080/	http://192.168.8.106:8080/	192.168.8.106	[]
7	X-Content-Type-Options unidentified	http://192.168.8.106:8080/	http://192.168.8.106:8080/	192.168.8.106	[]
8	Strict Transport Security Not Enforced	http://192.168.8.106:8080/	http://192.168.8.106:8080/	192.168.8.106	[]
9	CSP Not Enforced	http://192.168.8.106:8080	http://192.168.8.106:8080	192.168.8.106	[]
10	X-Content-Type-Options unidentified	http://192.168.8.106:8080	http://192.168.8.106:8080	192.168.8.106	[]
11	Strict Transport Security Not Enforced	http://192.168.8.106:8080	http://192.168.8.106:8080	192.168.8.106	[]
12	Joomla manifest file disclosure	http://192.168.8.106:8080/	http://192.168.8.106:8080/administrator/manifests/files/joomla.xml	192.168.8.106	[]

2.7 CONFIG

2.8 TECHNOLOGY

TT	port	product	name	version
1	8080.0	http	Apache	2.4.10 (Debian) PHP/5.6.12
2	8080.0	http	Joomla	
3	8080.0	http	php	
4	8080.0	http	apachegeneric	

2.9 DIR

TT	RECON_DIR
1	http://192.168.8.106:8080/language/
2	http://192.168.8.106:8080/libraries/

2.10 FILE

TT	RECON_FILE
1	http://192.168.8.106:8080/templates/
2	http://192.168.8.106:8080/templates/beez3/
3	http://192.168.8.106:8080/templates/index.html
4	http://192.168.8.106:8080/templates/protostar/
5	http://192.168.8.106:8080/templates/system/
6	http://192.168.8.106:8080/tmp/
7	http://192.168.8.106:8080/web.config.txt
8	http://192.168.8.106:8080/2/issue/createmeta

III Thông tin lỗ hổng bảo mật

IV Lịch sử khai thác lỗ hổng