

BÁO CÁO

Dò quét thông tin lỗ hổng bảo mật hệ thống

THEO HỒ SƠ

HỒ SƠ: mục tiêu 1

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
614f19d3da27e888809a78e2	test_running	192.168.230.190	25/09/2021T08:45:07	25/09/2021T08:46:56	DirSearch, WebAppDetect, Nmap, PocCheck	StatusSuccess

1.2 Thông tin đối tượng dò quét

1.2.1 IP

TT	IN_IP
1	192.168.230.190

1.2.2 DOMAIN

TT	IN_DOMAIN
1	test.khoa.domain

1.2.3 DESCRIBE

TT	IN_DESCRIBE
1	đây là mục tiêu 1

1.2.4 NAME

TT	IN_NAME
1	mục tiêu 1

1.2.5 AUTHEN

TT	IN_AUTHEN	
1		
	username	admin
	password	admin

II Thu thập, dò quét thông tin

2.1 SERVICES

TT	name	product	version	port	protocol
1	http	Apache httpd	2.4.38	31337	tcp
2	http	Apache httpd	2.4.38	31338	tcp

2.2 PORTS

TT	RECON_PORTS
1	31337
2	31338

2.3 OS

TT	RECON_OS
1	linux

2.4 WEBAPP

TT	RECON_WEBAPP
1	http://192.168.230.190:31337
2	http://192.168.230.190:31338

2.5 DIR

TT	RECON_DIR
1	http://192.168.230.190:31337
2	http://192.168.230.190:31337/
3	http://192.168.230.190:31337/index.php/
4	http://192.168.230.190:31337/index.php/login/
5	http://192.168.230.190:31337/server-status/
6	http://192.168.230.190:31337/wp-admin/
7	http://192.168.230.190:31337/wp-admin/
8	http://192.168.230.190:31337/wp-content/
9	http://192.168.230.190:31337/wp-content/upgrade/
10	http://192.168.230.190:31337/wp-content/uploads/
11	http://192.168.230.190:31337/wp-includes/
12	http://192.168.230.190:31337/wp-signup.php/
13	http://192.168.230.190:31338
14	http://192.168.230.190:31338/
15	http://192.168.230.190:31338/js/
16	http://192.168.230.190:31338/doc/
17	http://192.168.230.190:31338/libraries/
18	http://192.168.230.190:31338/server-status/
19	http://192.168.230.190:31338/sql/
20	http://192.168.230.190:31338/templates/
21	http://192.168.230.190:31338/themes/
22	http://192.168.230.190:31338/tmp/
23	http://192.168.230.190:31338/vendor/

2.6 FILE

TT	RECON_FILE
1	http://192.168.230.190:31337/adminer.php
2	http://192.168.230.190:31337/dump.sql
3	http://192.168.230.190:31337/info.php
4	http://192.168.230.190:31337/license.txt
5	http://192.168.230.190:31337/php.ini
6	http://192.168.230.190:31337/readme.html
7	http://192.168.230.190:31337/wp-admin/setup-config.php
8	http://192.168.230.190:31337/wp-config.php
9	http://192.168.230.190:31337/wp-content/
10	http://192.168.230.190:31337/wp-admin/install.php

TT	RECON_FILE
11	http://192.168.230.190:31337/wp-cron.php
12	http://192.168.230.190:31337/wp-login.php
13	http://192.168.230.190:31338/CONTRIBUTING.md
14	http://192.168.230.190:31338/ChangeLog
15	http://192.168.230.190:31338/LICENSE
16	http://192.168.230.190:31338/README
17	http://192.168.230.190:31338/composer.lock
18	http://192.168.230.190:31338/favicon.ico
19	http://192.168.230.190:31338/index.php
20	http://192.168.230.190:31338/index.php/login/
21	http://192.168.230.190:31338/package.json
22	http://192.168.230.190:31338/robots.txt
23	http://192.168.230.190:31338/vendor/composer/autoload_real.php
24	http://192.168.230.190:31338/vendor/composer/ClassLoader.php
25	http://192.168.230.190:31338/vendor/composer/LICENSE
26	http://192.168.230.190:31338/vendor/autoload.php
27	http://192.168.230.190:31338/vendor/composer/autoload_namespaces.php
28	http://192.168.230.190:31338/vendor/composer/autoload_static.php
29	http://192.168.230.190:31338/vendor/composer/autoload_psr4.php
30	http://192.168.230.190:31338/vendor/composer/installed.json
31	http://192.168.230.190:31338/vendor/composer/autoload_files.php
32	http://192.168.230.190:31338/vendor/composer/autoload_classmap.php
33	http://192.168.230.190:31338/yarn.lock

III Thông tin lỗ hổng bảo mật

IV Lịch sử khai thác lỗ hổng