Web Recon Tool

[1]Shubham Singh, [2]Neeraj Pahadiya, [3]Seema Jain
[1]Student, [2]Student, Department of Electronics and Communication Engineering, HMR Institute of Technology and Management, New Delhi
[3]Assistant Professor, Department of Electronics and Communication Engineering, HMR Institute of Technology and Management, New Delhi

***Abstract*— Our project aims at designing a Web Reconnaissance Tool that work on finding a web hidden directory from anywhere and all you need is an internet connection at your home. DIR is a Python-written method used to brute-force web directories and files that are secret. It can run on Windows, Linux, and macOS, and provides a simple but powerful interface for the command line. DIRis a professional command-line method for the brute force of web server folders and files. It has now become the Web content scanner. It provides users with the ability to explore complex web content as a feature-rich tool, with many wordlist vectors, high accuracy, impressive performance, advanced connection/request settings, modern brute-force techniques and nice results. It is a strong competitor in the directory scanner arena, with features such as multi-threading, proxy support, request latency, user agent randomization, and support for multiple extensions.**

***Index Terms:* Web Application, Web Server, Web Directory.**

1.INTRODUCTION

It is a simple command-line tool designed to brute force directories and files in websites. Which is a Python-based command-line website directory scanner designed to brute force site structure including directories and files. Dir is a professional command-line method for the brute force of web server folders and files. It has now become the Web content scanner. It provides users with the ability to explore complex web content as a feature-rich tool, with many wordlist vectors, high accuracy, impressive performance, advanced connection/ request settings, modern brute-force techniques and nice results. It is a strong competitor in the directory scanner arena, with features such as multi-threading, proxy support, request latency, user agent randomization, and support for multiple extensions.

Dir shines when it comes to recursive scanning. So for every directory it finds, it will go back through and crawl that directory for any additional directories. Recursive scanning, along with its speed and simple command-line usage, make DIR a powerful tool that every hacker and pen tester should know how to use. We can search for hidden and sensitive directories using DIR on our Kali Linux system. Dir is faster than infamous tool DIRB. In DIR we use Recursion, Threads, Prefixes/ Suffixes, Blacklist, Filters, Raw request, Wordlist formats, exclude extensions, Scan sub- directories, Proxies, Report saved auto in txt file. Considerations in choosing a web server include how well it works with the operating system and other servers; its ability to handle server-side programming; security characteristics; and the publishing, search engine and site-building tools that come with it. Web servers may also have different configurations and set default values. To create high performance, a web server, high throughput and low latency will help.

2. LITERATURE REVIEW

As per our analysis, there exist some tool based on web directory that can find hidden information in web application. Each tool has its unique features. Currently certain bug bounty hunter and penetration tester are officially registered and are working to provide better tool for bug hunter and pen testing.

Fuzzing is the process in which the detection of hidden files and directories is done. These interesting files and directories can contain some delicate data like SSH keys, username, passwords, etc. So, to delete these files and directories we use automated tools.

DIR is an automated tool developed in Python language which is the implantation of parent tool

DIR. This tool makes the task of fuzzing very easier and provides the list of interesting directories and files on the target server. We can also provide our custom wordlist which may contain more fuzzing words.

Each of these systems has their own unique features and comparison to one another lacks some advancement. Our designed system has application layer prototype. The application is able to synthesize the switch data with the help of stored database. The synthesized data are analyzed and father processing is carried out. In layman words,

Our tool provides features of finding web directory of any web application using a single command line Our project is different in a sense it has its own software level application to control the home appliances.

3. WORK DONE

A. Introduction

(i) Purpose: Accessible to Remote Areas

With the real – time conversation, we can use DIR tool from anywhere to find hidden directory of web application and this is also use by bug bounty and penetration tester to find out vulnerability in Web Server.

Provides Better Extension list

There is more 11000 directory list or web extensions that use in web application like

- .admin
- .ashx
- .asa
- .asp
- .bashrc

(ii) Scope:DIR is the only tool that work on web directory and web server in web application. Here, technological advancements come in handy for the bug bounty professional. Futuristic technologies like IoT and Cyber Security are ready to penetrate in the Cyber Security Sector. What's more in this mobile – dominated age, the hacker tries to hack any personal information of person by during Penetration Tester.As people tend to do their important activities through smartphones on the move, the mobile app development can facilitate them to fix by bug bounty hunter.

(iii) Overview: This approach makes it simple for teachers and students to stay in touch when they leave a particular organization.

B Interface Requirement

GUI 1: Kali Linux Operating System.

GUI 2: Web Server and Directory.

C. Application

Dir is a professional command-line method for the brute force of web server folders and files. It has now become the Web content scanner. It provides users with the ability to explore complex web content as a feature-rich tool, with many wordlist vectors, high accuracy, impressive performance, advanced connection/request settings, modern brute-force techniques and nice results

D. System Testing

System testing is an important part of quality assurance since it is the final assessment of the analysis, design, and coding. Because it meets the overall testing aim, test case design focuses on a collection of approaches for creating tests. When a system is created, it is hoped that it will function correctly. The primary goal of testing an information system is to identify and repair mistakes. Both manual and digital operations should be included in the scope of system testing. The term "system testing" refers to a thorough examination of programmers, manual methods, computer operations, and controls.

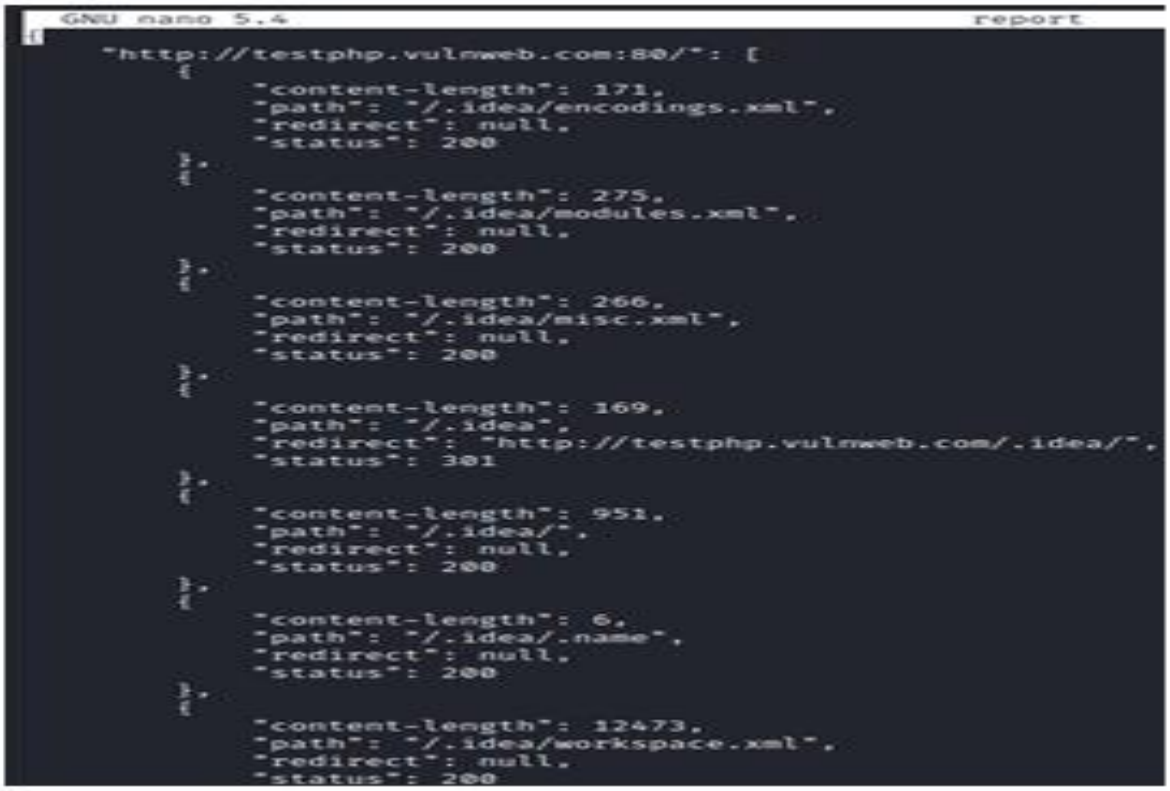
System testing is the process of determining whether or not the developed system meets the objectives and requirements. All testing must be carried out under the stated test circumstances.

Other technologies also implemented which is as follow:

1 Capture Hidden Directory of Web Application
2 Find possible sub-domain
3 Find all web extensions file in Web

Figure 1

In figure 1 we can see the kali Linux operating system that use in this project



In figure 2 we can see code for project

Figure 2

4. TOOLS

An advanced command-line tool designed to brute force directories and files in webservers, AKA web path scanner.

Recursion brute-force is brute the scanning progress with CTRL+C, from here, you can save the progress, skip the current target, or skip the current sub – directory.

We can use our web content scanner on a specific targeted URL with the help of [-u] parameter. To get appropriate results we need to make sure that it is an authenticated URL follow this command to get the desired results.

We can save our output which we get from the attack in different-different formats to learn further from them. This parameter helps us to get through those details of these formats. Let's explore them one by one.

Save output in Simple format

We can save our result in the simple format with the help of [–simple-report] parameter. Through this feature, we can better analyse the results which we got from this attack. Follow this command to proceed further.

/dir.py -u http://testphp.vulnweb.com/ --simple-report=report

Quite Mode

Quite mode is used in a more hush-hush manner to run dir. If you're the type of person who doesn't want a huge banner telling everybody what you're doing on your system, you'll like this choice. Basically, this allows for a cleaner screen as it executes the commands you send it, without the funny cow showing up on top.

Just use this [-q] parameter with this command to see the results

./dir.py -u http://testphp.vulnweb.com/ -q

Normal scan vs Recursive scan

The method of scanning everything in a folder, including subfolders, is known to all of us. We compare a normal scan against a recursive scan in this section.

Firstly, we only use the [-u] parameter in the normal scan to get through victim URLs. In order to begin this scan, follow this instruction.

/dir.py -u http://testphp.vulnweb.com

5. CONCLUSION

When a security analyst performing website penetration testing the initial step should be finding hidden directories of a vulnerable website. These hidden web directories are essential because they can give useful information i.e., potential attack vectors that would not be visible on the public facing website.

One of the ways to achieve this is by attempting brute-forcing site structure that includes directories and files in websites and for that, you have to choose a powerful tool. Although there are many tools available used to perform site brute-forcing include but these have their own limitation such as only offers GUI interface that is not feasible all the time and does not include multithreading feature, among penetration testers for website brute-forcing is DIR.

As more persons are cared for security of information. This will help address many of the issues that currently most of companies suffered due to vulnerability in their websites and improve both web application security and person personal information.

6. ACKNOWLEDGEMENT

This study is a part of security research related to modern web recon tool in various fields, I am also thankful to my respected guide Prof. Mrs. Seema Jain without whom I ever think to complete my seminar and we would like to thank all who helped us a lot in completing our project work. Hopefully, it will help in making the cordiality process fair in the upcoming future.

REFERENCES

[1] D.T.Pham and M.S.Aksoy, "RULES: A Simple Rule Extraction System," Expert Systems with Applications, vol. 8, no.1, pp.59-65,1995.

[2] H.Mathkour,"RULES3-EXT: Improvements of RULES3 Induction Algorithm," Mathematical and Computational Applications, vol. 15, no.3, pp.318-324,2010.

[3] System Analysis and Designing by Eliasmawed.

[4] Software Engineering by RogerSPressman, McGrawHill

[5] G.Iannaccone, C.Chuah, R.Mortier, S.Bhatta-charyyaandC.Diot."AnalysisofLinkFailuresinlargeIPBackbone", Proceedings of second

ACMSigcomm Internet Measurement Workshop (IMW), SanFranciscoUSA,November2002

[6] K.Papagiannaki and C.Diot. “Analyzing Link Utilization at small Time scales”, SprintATLTechnicalReportTR03-ATL-010900, January2003

[7] Justis,R.T and Kreigsmann, B.(1979). The Feasibility Study as a tool for venture analysis. Business Journal of small Business management 17(1)35-42

[8] E. Tovar and O. Soto, "The Use of Competences Assessment to Predict the Performance of First Year Students," IEEE Frontiersin Education Conference pp.F3J-1, 2010.

[9] U.Dayal,“Query Processing in Multidatabase Systems,”W.Kim, D.S. Reiner, and D.S. Batory, eds., Query Processing in DatabaseSystems, pp.81–108, Springer-Verlag, 1985.

[10] L.G.DeMichiel, “Resolving Database operation in compatibility An Approach to Performing Relational Operations Over Mismatched Domains,” IEEE Trans. Knowledge and Data Eng.,vol. 1,no.4,pp.485-493,Dec.1989.