International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Study of Directory Traversal Attack & Tools Used for Attack

Sanchi Sood[1], Mrs. N. Priya[2]

[1]MCA Computer Science Department,
[2]BE; M Tech; (PhD), Assistant Professor, School of Computer Science and IT,
[1,2]Jain Deemed-to-be University, Bengaluru, Karnataka, India

ABSTRACT

In a lot of cases, configuration files, leftover files, temporary files and many other of such types are left without any security due to many reasons like for fellow developer so that it can be easy access to him or you are still working on it or sometimes overwork so you don't remember or in hurry act sometime irresponsible but this can help attacker a lot to get information which can further lead to huge attacks.

An automated Dictionary Traversal tool can find those files easily & provide a great help to attacker. There are many tools of such kind like Dir Buster, Go Buster, DIRB etc. These tools are not only used for attack but also for pen-testing. Pen-tester could easily find these kinds of vulnerabilities with such tools & remove them to make the application secure.

Keywords: *Directory Traversal, Attack, Reconnaissance, Brute-force, Wordlist*

How to cite this paper: Sanchi Sood | Mrs. N. Priya "Study of Directory Traversal Attack & Tools Used for Attack" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.425-428, URL: www.ijtsrd.com/papers/ijtsrd37933.pdf

IJTSRD37933

INTRODUCTION

Directory Traversal Attack is done for information gathering or reconnaissance. It searches for unindexed resources with the help of a wordlist of most commonly used filenames. In simple terms, it basically gives access to restricted files & directories, so that attacker can get critical information & could lead to many other attacks. It's an easy to do attack as well as very easy to prevent. This attack is only possible if there is even a small kind of negligence in terms of security. There are many Automated Directory Traversal tools that do Brute-Force browsing with the intent of finding potential files & directories.

LITERATURE REVIEW

Security Misconfiguration is one out of top 10 OWASP vulnerabilities. Unpatched Flaws, Unused Pages, Unprotected Files & Directories are major causes of this vulnerability[1].Directory Traversal is one of the attacks that can happen because of Security Misconfigurations. In this attack, Attacker will scan web server using a wordlist of common filenames & extract information from hidden files & directories in the intent of finding some useful information. Wordlists should be maintained properly to do effective attack as wordlist have a major role. This basically works with the help of various HTTP status codes [2]. DirBuster& DIRB are top 2 tools that is used for such attack, as these two are really effective & have many features but has some flaws too like DIRB doesn't support multithreading & hence is slow and DirBuster supports only GUI operating System [3] (will be explained further in detail). In some case studies, this has been concluded that directory traversal attack could be dangerous and can provide important information to attackers, but It could be prevented easily as well [4].Most basic thing is to be giving unique name to files & not keeping the default names as then wordlist couldn't recognize them. It could be stopped by analysing multiple 404 error in logs or by enabling WAF.

DIRECTORY TRAVERSAL

Directory Traversal Attack is a type of Brute-force attack that can give potential access to restricted files and directories. This attack can also tell the attacker about directory structure of web application. Directory Traversal attack (Also known as Path Traversal) is in 12th rank of CWE (Common Weakness Enumeration) Top 25 Weakness. It is very important to make web application secure by giving protection to web content & giving controlled access.

Directory Traversal Attack is very easy to perform but the results could be harmful, in hacking Data means everything & if attacker get any important or privileged data, this simple attack could lead to many others. It can be easily prevented with some basic steps, but they must be followed properly without any mishandling.

WORKING METHODOLOGY

Working of directory traversal attack is quite simple. It basically works with wordlist; wordlist means the words which are most commonly used for critical or useful files and directories. Directory Traversal basically searches the web server for all the words defined in wordlist & revert with

HTTP Status codes which are basically responses of URL requests send by web server. A numeric code will be returned which will show whether the file is present or there could be chances URL defined is wrong like 404 defines Page not found, 200 defines successful etc. [5]

Here are the basic HTTP status codes used:
100: Continue – Which means request has been received & process is going on.

200: Successful – Which means Request is successful.

300: Redirection – Which means some more action required to complete the request.

400: Client Error – Which means incorrect syntax or content.

Wordlist is the foundation of such kind of attack but if attacker put very common words in wordlist or words that are used earlier, or filenames are changed (that most usually happens) than it could result to nothing. So, wordlist should be managed properly to perform a successful attack.

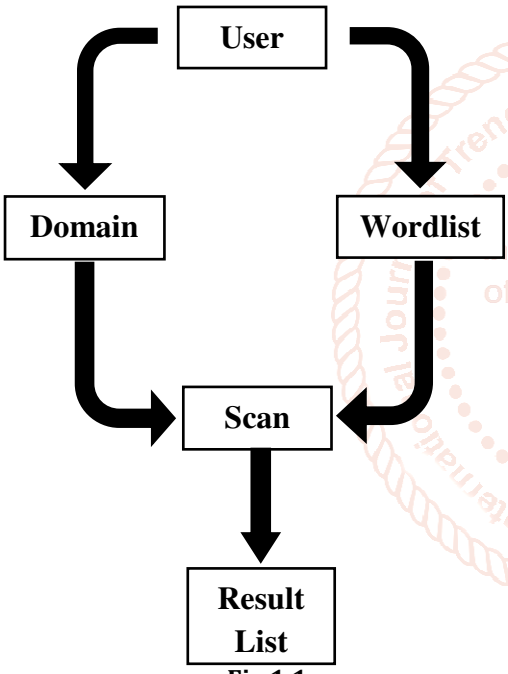

Fig 1.1

FLOWCHART

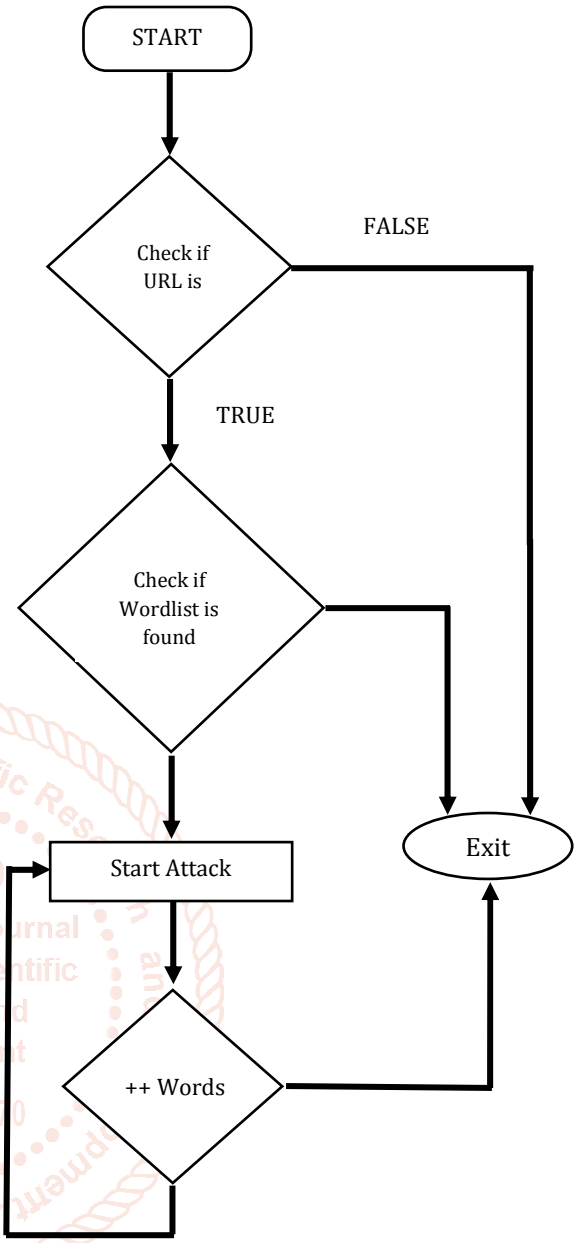

Fig 1.2

TOOLS

DIRBUSTER

DirBuster is a directory brute-forcer application developed by OWASP (Open Web Application Security Project). DirBuster is a Java application which offers GUI interface. It is used to find hidden files by brute-forcing files & directories with the intent of getting some valuable information that could help in attacks. Effectiveness of such tool could be determined by wordlist, more effective the wordlist, more effective will be the tool. DirBuster is most effective because it has a different approach for making the wordlist, it basically generates wordlists from scratch by crawling internet and using files & directory names that are used by developers. It comes up with 9 lists in total. There is also one option of Pure Brute Force which takes time but is more effective as compared to list based [6].

ADVANTAGES

1. GUI Interface: DirBuster provides GUI interface, which is obviously very easy to understand and use. DirBuster can be used by anyone without any hustle.
2. Effective Wordlist: DirBuster Wordlists are quite effective as it uses a different approach for making the wordlist, it basically generates wordlists from scratch by crawling internet and using files & directory names that are used by developers. It comes up with 9 lists in total.
3. Pure Brute Force: If user doesn't know any list or doesn't getting any list from wordlist-basedapproach, there is another option in DirBuster Pure Brute Force which is very effective & give results definitely.
4. Customize Thread-Count: DirBuster gives an option of customizing Thread Count, in that way user can increase Thread Count & get effective result but, in less time, or vice versa. It depends on user requirement.

DISADVANTAGES

1. Compatibility with CLI OS: DirBuster provides GUI interface which is an advantage as well as disadvantage, as it is easy to use but it is not compatible with CLI (Command Line Interface) Operating System.
2. Time Consuming: DirBuster supports Multi-Threading & user can actually specify the number of threads you want to use. But when I kept number of threads to 10, it was taking 52 days to give result which is not feasible.
3. Generate Errors: When user increases the number of threads for getting faster result, it actually stops after getting 20 consecutive errors.

DIRB

DIRB is a CLI (Command Line Interface) based Web Content Scanner. It is written in C language. DIRB works by launching a Dictionary based attack on a web server and as a result show hidden files & Directories. It comes with preinstalled files & directories but if user wants, he can add his own list for search. DIRB is mostly used in Web Application testing or Auditing. It can also be used as a CGI Scanner. It comes preinstalled in Kali; user just have to type dirb in prompt. Before performing any kind of attack, it is better to understand the structure or files or directories, so that attack could be more effective & DIRB is best suited tool for such task.

ADVANTAGES

1. CLI Interface: Command Line Interface gives quite flexibility of using the tool in both CLI as well as GUI Operating systems. For attacks or testing, most users prefer command line format.
2. Easy to Use: DIRB is very easy to use as it supports Command Line Interface, User just have to type dirb & then URL in the prompt & That's it. So, it is not complicated. There are some additional options as well which user can add in command line & take full advantage.
3. Usage: DIRB is most used tool as a Directory-forcing tool. It is mostly used in Web Application Testing or Auditing. If user is little knowledgeable, DIRB can also be used as a CGI Scanner.

DISADVANTAGES

1. Doesn't supports Multithreading: DIRB has one major disadvantage as Multithreading is quite helpful in directory brute-force tools but DIRB doesn't support what makes this tool really slow.
2. Slow in use: DIRB works really well if user is using small wordlist. But if wordlist is quite long, DIRB works very slow.

GOBUSTER

As we saw in previous two tools, they are mostly used but both have one common issue, Speed. GoBuster performs task very fast. GoBuster is a Command Line Interface based tool & has been developed in Go Language. It doesn't come preinstalled. GoBuster has 3 modes; First is DNS mode which is used to find subdomain of given domain, second is DIR mode which is used to find hidden files & directories, and Third is VHOST mode which is used to find virtual hosts of server; Virtual hosts means sometimes one server host many domains so GoBuster can find about them [7].

ADVANTAGES

1. Speed: As compared to other Directory Brute-forcing tools, GoBuster is very fast. GoBuster has been developed in Go language & This language is known for speed.
2. Concurrency: This tool supports multithreading & hence can concurrently scans with faster processing speed.
3. Multiple-Modes: GoBuster has 3 modes; DNS, DIR & VHOST. GoBuster can be used to find Subdomain as well as hidden files & Directories. It can also find virtual hosts of server.

DISADVANTAGES

1. Recursive Search: GoBuster doesn't support searching directories recursively that means directories which are deep like more than a level needs scanning again.

DISCUSSION ABOUT TOOLS

We discussed here some most used tools; each have its own advantages as well as disadvantages. Every tool is good if you take benefits of its pros. It depends on you for what purpose you want to use & on that basis can decide easily. If you want to get result fast, GoBuster is surely the best choice, if you want scanning in detail, Dirb could do that job really well but if wordlist is quite long, DirBuster could do the job well in less time. Each tool has some extra features also & those should be utilized properly if you want good reconnaissance results. But you don't need tool always, you can also append the URL, if you know about the domain then work of tool could be done easily & quickly by yourself, without any tool[8].

USAGE

A. Reconnaissance: Before any attack, Information Gathering is a must. So, Directory Traversal tools are mostly used to find details about files & directories in a server.
B. Testing: Directory Traversal tools are used to know if there is any vulnerability in web application that can leak some important information.
C. Hacking Challenges: There are many online hacking challenges platform like HTB (Hack the Box), TryHackMe etc. where such tools are mostly used to solve their challenges.

PREVENTION

As I have mentioned before, Directory Traversal attack can cause harm only if some important or critical information got leaked, but as easy it is to perform, Prevention is easier to do & could be done with basic Security measures.

ACL & ROOT DIRECTORY

We can secure the web server with the help of ACL (Access Control List) & Root Directory. Access Control list can basically tell about the access rights in web server that which user or group is allowed to access, modify or execute which files on the server. It's a great way of Authorization that can secure the content of web server. Next way is Root directory which is the top-most directory & access of users is confined to it which means users can't access anything outside root directory.

LOG MANAGEMENT

This attack can be easily detected through logs because of its noise. Obviously, it's not possible that attacker will know exactly the pages, so most of the time, page name attacker enter will not even exist so 404(Page not found) error will be found in logs, & through those logs we can easily found out about the attack.

WAF

WAF or Web Application Firewall will block the particular IP Address from where too many 404 (Page not found) are generated, because that can only be generated if someone is trying any attack & hence server can be saved.

INPUT VALIDATION

Validating user input is one way to prevent Directory Traversal Attack, as through SQL injection commands user can get access out of root directory or manipulate other access privileges.

SOFTWARE PATCHING

Regularly patching software is obviously one of the ways in every kind of attack. Many times, web developer or sysadmin due to overwork or in hurry leave many security procedures, so little carefulness or regular review could help preventing this attack.

CONCLUSION

Reconnaissance is always first step in any attack. Directory Traversal or Directory Brute-Forcing is a great method of Reconnaissance & a successful information gathering could lead to some major attacks. We have studied some mostly used tools but actually this can be done without tool also, by just appending the URL, it could lead to your result quite easily & quickly but it could take more time sometimes if attacker has no knowledge about that domain. If user is using the tool, He/she should give utmost importance to wordlist as it plays major role. We discussed many preventions techniques & by now, it's quite clear how easy is this attack to perform & how easily it could be prevented also. We just have to take care of some minor details.

REFERENCES

[1] "OWASP Top 10 Vulnerabilities": https://owasp.org/www-project-top-ten/

[2] "5waysdirectory brute forcing webserver": https://www.hackingarticles.in/5-ways-directory-bruteforcing-web-server/

[3] "DirBuster and DIRB":https://tools.kali.org/ web-applications/

[4] "Directory Brute Force Attacks": https://docs. sucuri.net/attacks/brute-force/

[5] "Find directories using dirbuster": https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-directories-websites-using-dirbuster-0157593/

[6] "DirBuster":https://tools.kali.org/webapplications/dirbuster/

[7] "GoBuster":https://medium.com/bugbountywriteup/discovering-the-hidden-web-638a947361ad

[8] "Comparison between tools": https://sevenlayers.com/index.php/186-pentesting-101-web-fuzzing