International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET21837

Subdomain Takeover : A Challenge as Web App Vulnerability or Server-Side Vulnerability

Patel Vraj Vishnubhai, Dr. Priyanka Sharma
School of Information Technology, Artificial Intelligence, and Cyber Security, Rashtriya Raksha University, Gandhinagar, Gujarat, India

ABSTRACT

Article Info
Volume 8, Issue 3
Page Number: 58-64

Publication Issue :
May-June-2021

Article History
Accepted : 07 May 2021
Published: 12 May 2021

A subdomain is a domain that is a part of another domain. Subdomains are used to organize and navigate to various parts of your website. For example, your primary domain could be "xyz.com," while your blog could be on a subdomain at "blog.xyz.com." A subdomain takeover occurs when an attacker gains control over a subdomain of a target domain. Sub-domain takeover vulnerability occurs When a subdomain (subdomain.example.com) that refers to a service (eg GitHub, AWS / S3, ..) is deleted or deleted In this way, the attacker can create pages on the service in use and forward the pages to this subdomain.. If any person wants to take over, a subdomain then the person seeks to manually check one by one subdomain that takes too much time. Moreover, are there some tools available to check the subdomain takeover is possible or not? However, these tools take input as a text file, which has a particular subdomain. This means finding a subdomain with the other tools and then using one of these tools to identify subdomain takeover vulnerability. In my tools, we find the subdomain of a particular domain, then check the CNAME is available for a list of subdomains and if CNAME finds for a specific subdomain, then check the status code of the CNAME if it returns 404-status code. We might say that a particular subdomain is possible to takeover.

Keywords : Subdomain, Subdomain Takeover, Subdomain Takeover Tools, 404-Status Code

I. INTRODUCTION

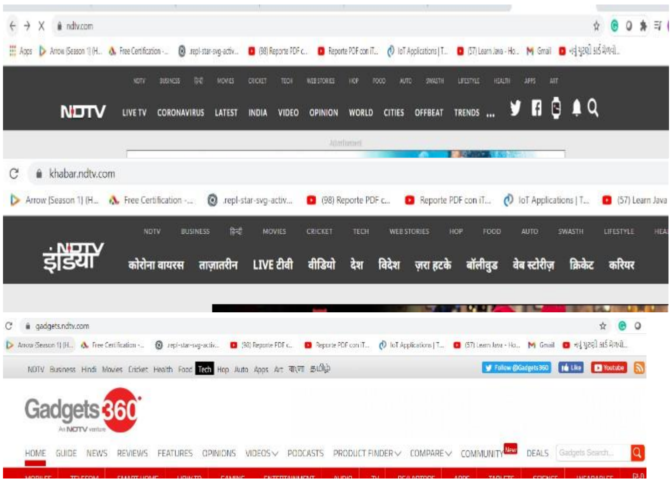
In this, there two crucial term
1. Subdomain
2. Takeover

SUBDOMAIN

A subdomain is a further part of your main domain. Subdomains are created to arrange and navigate to exclusive sections of your website.[7]For example, your

The primary domain could be "abc.com," while your blog could be on a subdomain at "blog.abc.com." This means it is a subcategory of the field. The subdomain is generally logically separated your websites into sub-sections. This means any large website is handled complex but logically divides your website into subsection website handle easily.

Let's understand what a subdomain is with a real example.


ndtv.com
NDTV
LIVE TV CORONAVIRUS LATEST INDIA VIDEO OPINION WORLD CITIES OFFBEAT TRENDS
khabar.ndtv.com
NDTV इंडिया
कोरोना वायरस ताज़ातरीन LIVE टीवी वीडियो देश विदेश ज़रा हटके बॉलीवुड वेब स्टोरीज़ क्रिकेट करियर
gadgets.ndtv.com
Gadgets 360
HOME GUIDE NEWS REVIEWS FEATURES OPINIONS VIDEOS PODCASTS PRODUCT FINDER COMPARE COMMUNITY DEALS

[1]

Here, ndtv.com is the Domain that consists of two parts TLD (highest level Domain), which is the .com and Second Level Domain (SLD) parts as ndtv, the name where you purchased it the domain registrar

The subdomain contains the middle name before the SLD. For example, if the ndtv blog is hosted at https://blog.ndtv.com, then that blog is the subdomain.[4]

TAKEOVER

The takeover means all processes are under control. That means, Gain access to any system/subdomain.

If you takeover https://blog.ndtv.com then this URL(domain/subdomain) shows only the content you want to display on that URL (subdomain).

SUBDOMAIN TAKEOVER:

Subdomain Takeover is a type of vulnerability that occurs due to Misconfiguration in CNAME records.

Subdomain takeover may be a vulnerability class where a subdomain points to an external service that has been deleted. The external services are GitHub, Heroku, Gitlab, Tumblr, and so on. Let's assume we've got a subdomain sub.example.com that points to an external service such as GitHub if the GitHub page is removed by its owner and forgot delete the DNS entry that points to GitHub service. An attacker can take over the subdomain by adding a CNAME file containing the sub.example.com.[6]

Example:

Let us assume the domain is example.com and want to add some e-commerce for some shopping facility provide to example.com, Shopify provides some e-commerce facility. In the end, a configuration in Shopify service provides some addresses like xyz.shopify.com. Whenever anyone enters this URL, an e-commerce service is open, associated with example.com. However, the URL still shows at the end of shopify.com. No one or any brand wants to show shopify.com or something else in the URL.

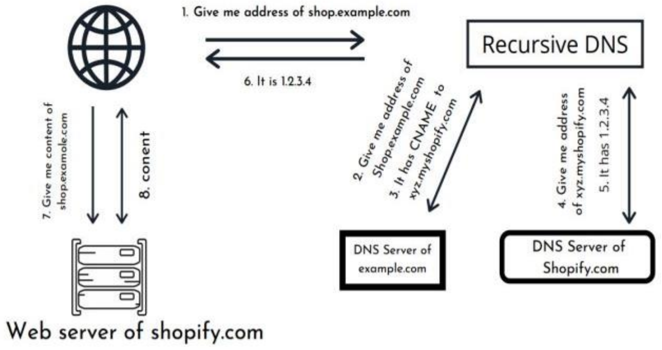
So in this scenario subdomain is generate in shop.example.com, and this particular subdomain is only associated with e-commerce. Moreover, we want to connect with shop.example.com and xyz.shopify.com, so we enter xyz.shopify.com in the canonical name of shop.example.com.

Shop.example.com ===========➔xyz.shopify.com

Subdomain Canonical Name

After some time, Shopify service is expired/not renewed in example.com. So xyz.shopify.com is for registration by anyone.

The below illustrates a web browser's behavior for the domain name, which has a picture CNAME record in place. CNAME records are handled by DNS (Domain namesystem). When a DNS resolver (recursive DNS) encounters a CNAME record while looking for a regularly requested resource (web sites), it will restart the query using the canonical name instead of the original name.


1. Give me address of shop.example.com
6. It is 1.2.3.4
Recursive DNS
2. Give me address of Shop.example.com
3. It has CNAME to xyz.myshopify.com
4. Give me address of xyz.myshopify.com
5. It has 1.2.3.4
7. Give me content of shop.examole.com
8. conent
DNS Server of example.com
DNS Server of Shopify.com
Web server of shopify.com

CNAME records mean canonical name records, is the type of record in DNS (Domain name system) that maps one domain to another.
CNAME records are handled by DNS (Domain name system). When a DNS resolver (recursive DNS) encounters a CNAME record while looking for a regularly requested resource (web sites), it will restart the query using the canonical name instead of the original name.[5] Above is shown in fig. recursive DNS looking for shop.example.com address. Still, it will find a CNAME record (xyz.myshopify.com) in shop.example.com. Then again, it will find a recursive DNS regenerate query with the CNAME. The canonical name that a CNAME record points to can be anywhere in the DNS, whether local or on a remote server in a different DNS zone.[5]

Since the CNAME name isn't deleted in example.com, So DNS zone registers xyz.shopify.com have complete controls over shop.example.com till the DNS name is present.

Status codes are very much useful in web browsing. HTTP response status codes indicate whether a specific HTTP request has been completed. Responses are grouped into five classes: [2]

1. Informational responses (100–199)
2. Successful responses (200–299)
3. Redirects (300–399)
4. Client errors (400–499)
5. Server errors (500–599)[2]

Specially In subdomain takeover, status code-404 is very useful if any hacker or person finds the 404 error page(status code), which means that URL(subdomain) might lead to a takeover.

Status code 404 means the requested page by bowser is not found in the webserver. This error occurs when website content has been removed or moved to another URL. If 404 shows by a particular subdomain, it might be possible to specify that the subdomain is a takeover.

OBJECTIVE

The goal of the this project(tools) to provide almost all of the information about the subdomain and cheking which subdomain is possible to takeover or not ? In this tool find the subdomain of a particular domain then check the CNAME is available for a list of subdomain and if CNAME finds for particular subdomain then check the status code of the CNAME if it returns 404-status code then we might say that particular subdomain is possible to takeover.

II. PROBLEM OF STATEMENT

There are some tools available on the Internet/GitHub, which provide services like to check subdomain takeover vulnerability is possible or not? However, most of the tools get the input as a subdomain list as a text file and then find which subdomain might be possible to subdomain takeover vulnerability.

That means if anyone wants to find subdomain takeover vulnerability of a particular domain, find the subdomain of that domain with the other tools and save that subdomain and give as input to one of these tools to find out which subdomain might have subdomain takeover vulnerability. With this project, we provide list of subdomain takeover by just entering domain at the one place, means user don’t need to go many other tools to find the subdomain takeover vulnerability.moreover provide more information about the possible list of takeover subdomain.

III. RELATED WORKS

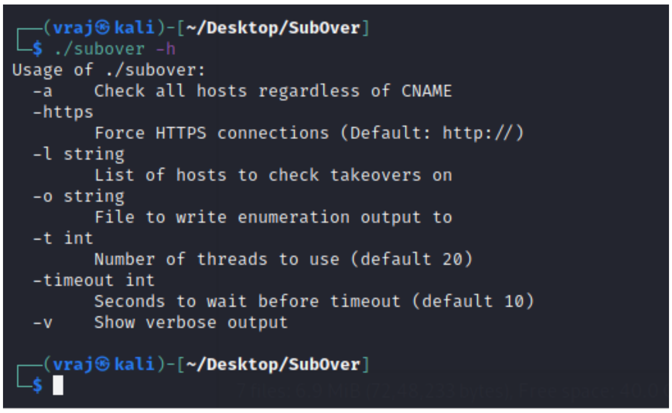
DNS is a crucial part of web services and internet service. The name server is responsible for the excellent work and security of their domain names. However, due to some security issues or DNS records misconfiguration, it might lead to a subdomain takeover. In the subdomain takeover, the first crucial step is to find out the subdomain of that domain. Subdomain find is a vital part of VAPT and ethical hacking of any domain. More domain means more information, more possibility of vulnerability, and increased attack vector of that domain. The subdomain is logically connected to that domain, and provides some types of service of that particular subdomain. A server issues a status code in response to a client request to the server for detailed data. In particular, the 404 status code means the server does not find the file or page that the browser is requesting to the server. Suppose any subdomain is generated a 404 error that means the particular that subdomain is possible to takeover.

IV. EXISTING SYSTEM (TOOLS)

There is a different tool available, which can provide the find subdomain, such as SubOver, SubRecon, 404_digger, Subdomain-takeover, and many more.

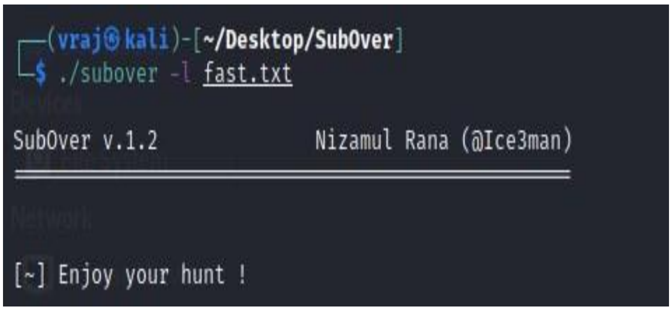
(1) SubOver

Sub over is a Hostile Subdomain Takeover tool to begin with written in python however rewritten from scratch in Golang. Since its a redesign, it's been geared toward pace and performance in mind.[3]



```
┌──(vraj㉿kali)-[~/Desktop/SubOver]
└─$ ./subover -h
Usage of ./subover:
  -a    Check all hosts regardless of CNAME
  -https
        Force HTTPS connections (Default: http://)
  -l string
        List of hosts to check takeovers on
  -o string
        File to write enumeration output to
  -t int
        Number of threads to use (default 20)
  -timeout int
        Seconds to wait before timeout (default 10)
  -v    Show verbose output

┌──(vraj㉿kali)-[~/Desktop/SubOver]
└─$ █
```

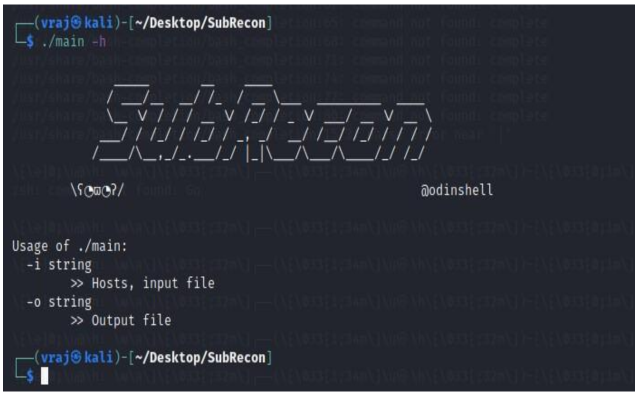
As seen in fig, this tool takes input as a text file, not the domain, that text file containing the subdomain list. That means we need to find a subdomain with the other tool.



```
┌──(vraj㉿kali)-[~/Desktop/SubOver]
└─$ ./subover -l fast.txt

SubOver v.1.2              Nizamul Rana (@Ice3man)
 ═══════════════════════════════════════════════


[~] Enjoy your hunt !
```

(2) SubRecon

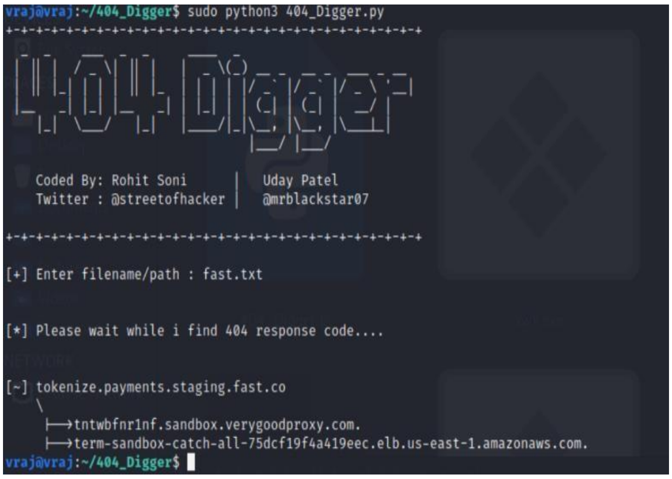
SubRecon Fast Subdomain Takeover Enumeration tools and this tool is written in Go. It makes use of Golang programming and for this reason is very fast..[3]



```
┌──(vraj㉿kali)-[~/Desktop/SubRecon]
└─$ ./main -h

       _____       __    ____
      / ___/__  __/ /_  / __ \___  _________  ____
      \__ \/ / / / __ \/ /_/ / _ \/ ___/ __ \/ __ \
     ___/ / /_/ / /_/ / _, _/  __/ /__/ /_/ / / / /
    /____/\__,_/_.___/_/ |_|\___/\___/\____/_/ /_/

   \ʕ◔ϖ◔ʔ/                                        @odinshell


Usage of ./main:
  -i string
        >> Hosts, input file
  -o string
        >> Output file

┌──(vraj㉿kali)-[~/Desktop/SubRecon]
└─$ █
```

(3) 404_digger

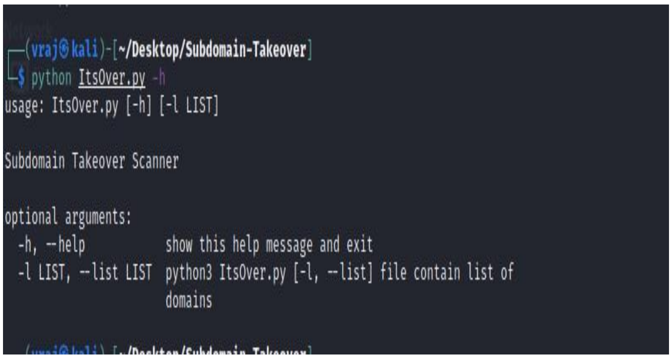
404_Digger is a tool used for finding subdomains with 404 Not Found status code and fetches CNAME, i.e., the canonical name of the subdomain.[3]



```
vraj@vraj:~/404_Digger$ sudo python3 404_Digger.py
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

    Coded By: Rohit Soni        |   Uday Patel
    Twitter : @streetofhacker   |   @mrblackstar07

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

[+] Enter filename/path : fast.txt


[*] Please wait while i find 404 response code....


[~] tokenize.payments.staging.fast.co
    \
     ├──>tntwbfnr1nf.sandbox.verygoodproxy.com.
     ├──>term-sandbox-catch-all-75dcf19f4a419eec.elb.us-east-1.amazonaws.com.
vraj@vraj:~/404_Digger$
```

(4) Subdomain-takeover

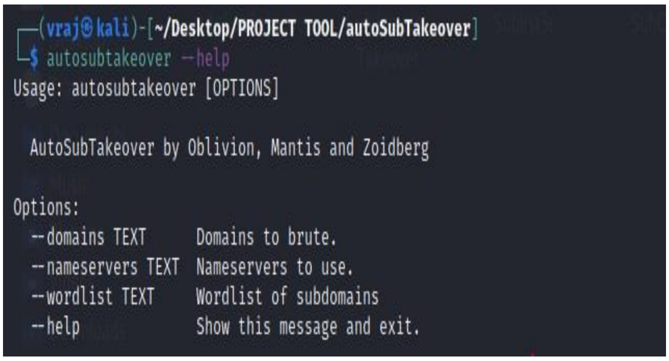
It is a simple program written on python3 .to check if the subdomain is vulnerable to takeover.[3]



```
┌──(vraj㉿kali)-[~/Desktop/Subdomain-Takeover]
└─$ python ItsOver.py -h
usage: ItsOver.py [-h] [-l LIST]

Subdomain Takeover Scanner

optional arguments:
  -h, --help            show this help message and exit
  -l LIST, --list LIST  python3 ItsOver.py [-l, --list] file contain list of
                        domains
```

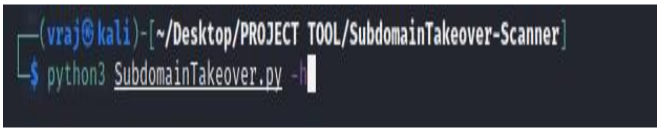
(5) Autosubtakeover

This tool builds in python language and takes a list of input such as single domain and list of domains and many. Again, this is not used to find subdomain of particular domain takes input only particular single that not find subdomain of the input domain.[3]



```
┌──(vraj㉿kali)-[~/Desktop/PROJECT TOOL/autoSubTakeover]
└─$ autosubtakeover --help
Usage: autosubtakeover [OPTIONS]

  AutoSubTakeover by Oblivion, Mantis and Zoidberg

Options:
  --domains TEXT      Domains to brute.
  --nameservers TEXT  Nameservers to use.
  --wordlist TEXT     Wordlist of subdomains
  --help              Show this message and exit.
```

(6) SubdomainTakeover-Scanner



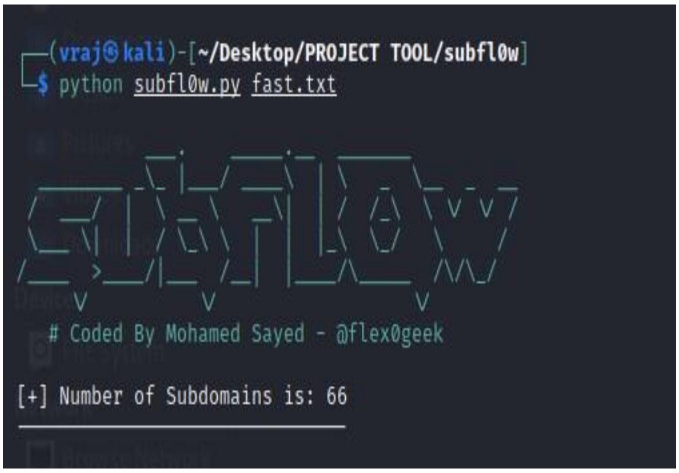
```
┌──(vraj㉿kali)-[~/Desktop/PROJECT TOOL/SubdomainTakeover-Scanner]
└─$ python3 SubdomainTakeover.py -h
```

```
> [?] Enter File Containing Subdomains: fast.txt
> [?] Enter Amount of Threads: 400
```

These tools are written in python language. This tool takes a text file, not a domain, and again this tool does not find the domain's subdomain.[3]

(7) Subflow

These tools are written in python language. This tool takes a text file, not a domain, and again this tool does not find the domain's subdomain.[3]



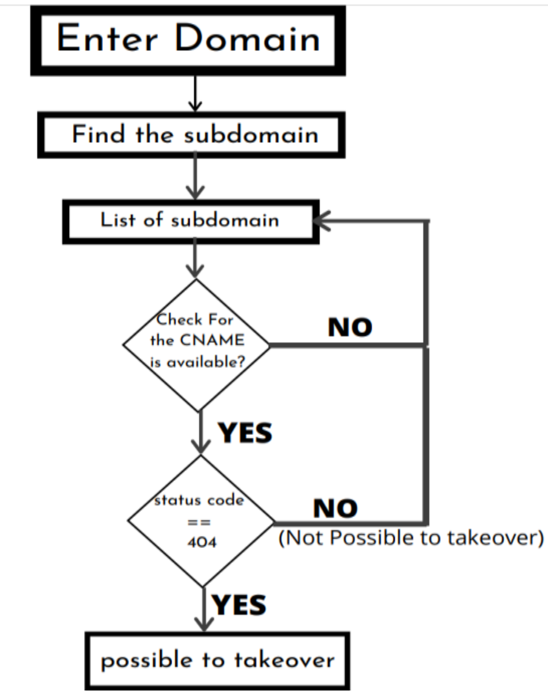
```
┌──(vraj㉿kali)-[~/Desktop/PROJECT TOOL/subfl0w]
└─$ python subfl0w.py fast.txt

  # Coded By Mohamed Sayed - @flex0geek

[+] Number of Subdomains is: 66
```

As above all of the tool is used for subdomain takeover. But all of this tool and available tool in GitHub/internet almost all of the device take input as a list of the subdomain text file. It is not generated by a particular that tool. This means the subdomain is found with a different tool, and the subdomain takeover is with the separate device/tools. In my system (proposed system), find the subdomain and determine and check the subdomain has CNAME. If any subdomain provides CNAME, we check the status code of that CNAME if it returns a 404 error (status code). We can say that a particular subdomain might have a subdomain takeover vulnerability. Also, provide more information about that subdomain that might have subdomain takeover vulnerability.

V. PROPOSED SYSTEM

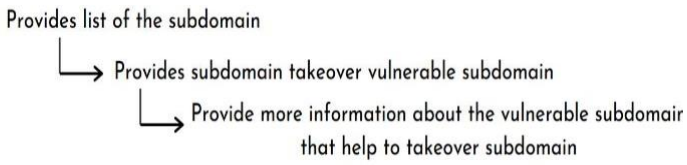
Therefore, in my tools (system), we find the subdomain of a particular domain then check the

CNAME is available for a list of subdomain and if CNAME finds for particular subdomain then check the status code of the CNAME if it returns 404-status code then we might say that particular subdomain is possible to takeover. In addition, provide more information about that subdomain which might have subdomain takeover vulnerability.



As shown in fig. user wants to find the subdomain of the particular domain just enter the domain and this tools find the subdomain of that domain after that just check CNAME of that list of the subdomain and then one by one check status code of that CNAME and if statuscode is equals to 404 then we can say that particular subdomain is might be takeover otherwise not takeover that subdomain. After that provide some more information about provide possible to takeover subdomain.

VI. EXPECTED OUTCOMES


Provides list of the subdomain
Provides subdomain takeover vulnerable subdomain
Provide more information about the vulnerable subdomair that help to takeover subdomain

IN the proposed system, we get input domains that users want to check that subdomain takeover. We get input and find that subdomain and save the subdomain file with the particular domain name; LIKE input domain is https://www.fast.co, then the file name is fast.txt. Then after the tool, find the CNAME of the subdomain file. Because the subdomain takeover occurs when misconfiguration happens in CNAME records, the 404 status code is also essential in the subdomain takeover. The 404 status code means the server does not find the browser's file page is requesting the server. Suppose any subdomain is generated a 404 error that means the particular that subdomain is possible to takeover. So after finding the CNAME of the subdomain, we can check the status code of the CNAME. If any CNAME of Subdomain generates a 404 status code, then we can say that subdomain is possible to takeover. After that, these tools provide more information on that subdomain, which is likely to take over. Like IP address and much more information.

VII. CONCLUSION

There are some tools available on Internet/GitHub, but some more improvement needs to be particular. Like if the subdomain finds with the other tools, we can then use them after getting one of the tools. This proposed system provides a subdomain and checks which subdomain is possible to takeover. These tools also provide more information on that subdomain, which might help to takeover that subdomain.

VIII. REFERENCES

[1]. https://www.ndtv.com
[2]. https://developer.mozilla.org/enUS/docs/Web/HTTP/Status
[3]. https://github.com/search?q=subdomain+takeover
[4]. https://themeisle.com/blog/what-are-subdomains

[5]. https://en.wikipedia.org/wiki/CNAME_record

[6]. https://github.com/EdOverflow/can-i-take-over-xyz

[7]. https://www.wpbeginner.com/glossary/subdomain

Cite this article as :

Patel Vraj Vishnubhai, Dr. Priyanka Sharma" Subdomain Takeover : A Challenge as Web App Vulnerability or Server-Side Vulnerability, International Journal of Scientific Research in Science, Engineering and Technology(IJSRSET), Print ISSN : 2395-1990, Online ISSN : 2394-4099, Volume 8, Issue 3, pp.58-64, May-June-2021. Available at doi : https://doi.org/10.32628/IJSRSET21837
Journal URL : https://ijsrset.com/IJSRSET21837