

Dirrectory Listing

I

BY
KVS SIVA KUMAR

USING PYTHON SCRIPTING



Directory Listing

Web application present the largest attack surface and so are the most common avenue for gaining access to the web server. When an overworked sysadmin or hapless web developer doesn't follow all security and installation procedures, It can be easy pickings for an attacker to gain access.

In a lot of cases there are configuration files, leftover development files, debugging scripts and other security breadcrumbs that can provide sensitive information or expose functionality that the software developer did not intend. The only way to discover this content is to use a brute-forcing tool to hunt down common filenames and directories.



III

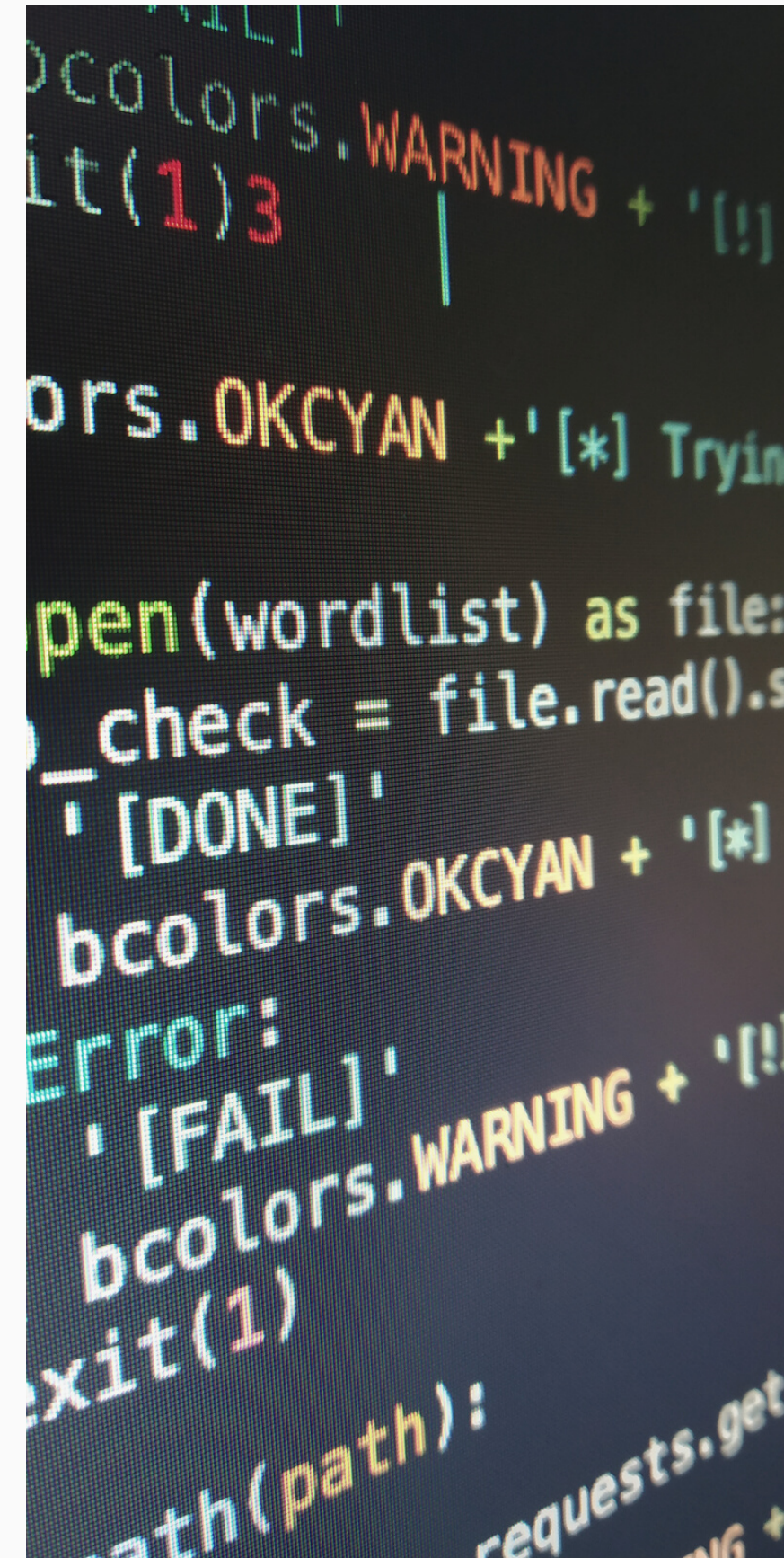
```
colors.WARNING + '[!]  
it(1)3  
  
ors.OKCYAN + '[*] Trying  
  
pen(wordlist) as file:  
_check = file.read().st  
'[DONE]'  
bcolors.OKCYAN + '[*]  
Error:  
'[FAIL]'  
bcolors.WARNING + '[!]  
exit(1)  
ath(path):  
requests.get
```

THE SCRIPT- PASTEBIN



What the script does?

- ✓ Checks the url is dead or not
- ✓ Checks if the wordlist is provided or not
- ✓ Bruteforces the URL with the path that was provided using wordlist
- ✓ If the path does not have the http code 500 then it prints the output



```
bcolors.WARNING + '[!]'
it(1)3

ors.OKCYAN + '[*] Trying
open(wordlist) as file:
_check = file.read().s
'[DONE]'
bcolors.OKCYAN + '[*]
Error:
'[FAIL]'
bcolors.WARNING + '[!]'
exit(1)
path(path):
requests.get
```



Working script: example

```
+ Ethical-Hacking git:(hackking) ✖ python script.py www.tesla.com payloads/SecLists/Fuzzing/fuzz-Bo0oM.txt
[*] Checking URL... [DONE]
[*] Trying The Wordlist... [DONE]
[*] Total Paths to Check: 4288

[*] Beginning Scan...

Printing The Directories Found:

[*] Full Path : www.tesla.com/!.gitignore (403)
[*] Full Path : www.tesla.com/!.htaccess (403)
[*] Full Path : www.tesla.com/!.htpasswd (403)
[*] Full Path : www.tesla.com/%20../ (403)
[*] Full Path : www.tesla.com/%2e%2e//google.com (403)
[*] Full Path : www.tesla.com/%2e%2e;/test (403)
[*] Full Path : www.tesla.com/%3f/ (403)
[*] Full Path : www.tesla.com/%C0%AE%C0%AE%C0%AF (403)
^C
[!] Error: User Interrupted Scan
```

URL

WordList

Results with url/path/

User interrupt

Any Questions?

THANK YOU

