aaaahuia / **MCMS CSRF.md** Secret

Last active 7 months ago

MCMS CSRF

MCMS CSRF.md

Product official website:

https://ms.mingsoft.net/

Product download address:

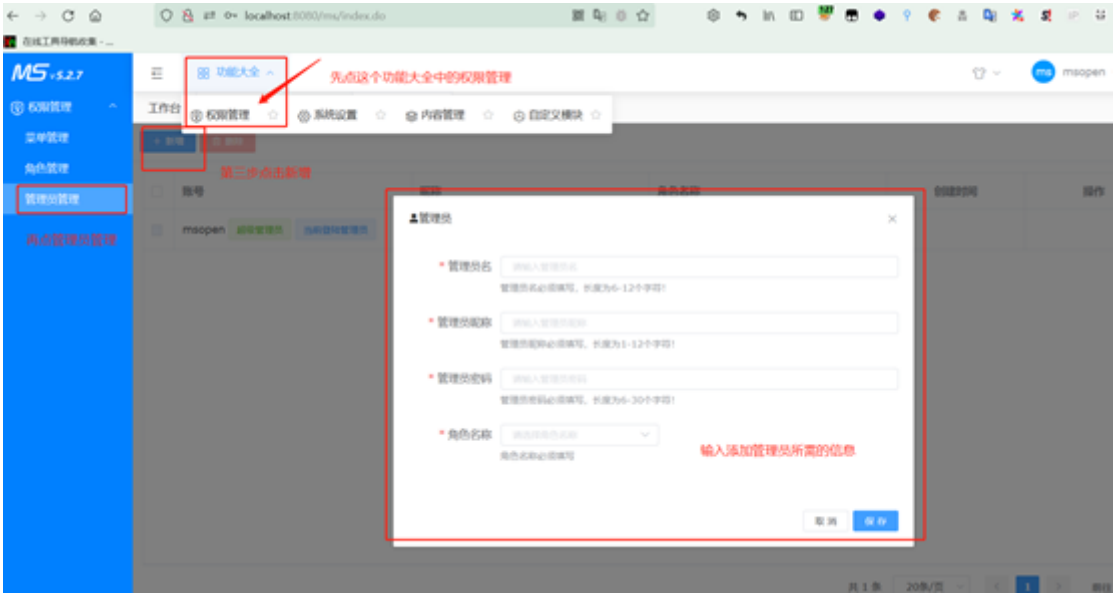
https://gitee.com/mingSoft/MCMS https://github.com/ming-soft/MCMS

Vulnerability Description:

There is a CSRF vulnerability in the background adding user of MCMs administrator. When adding a user without adding a token and verifying the reference, the attacker can phishing attack the administrator by constructing a special page. When the administrator accidentally accesses the special page constructed by the attacker, trigger the payload to secretly add the administrator user, and the attacker can obtain the privileges of the background administrator.

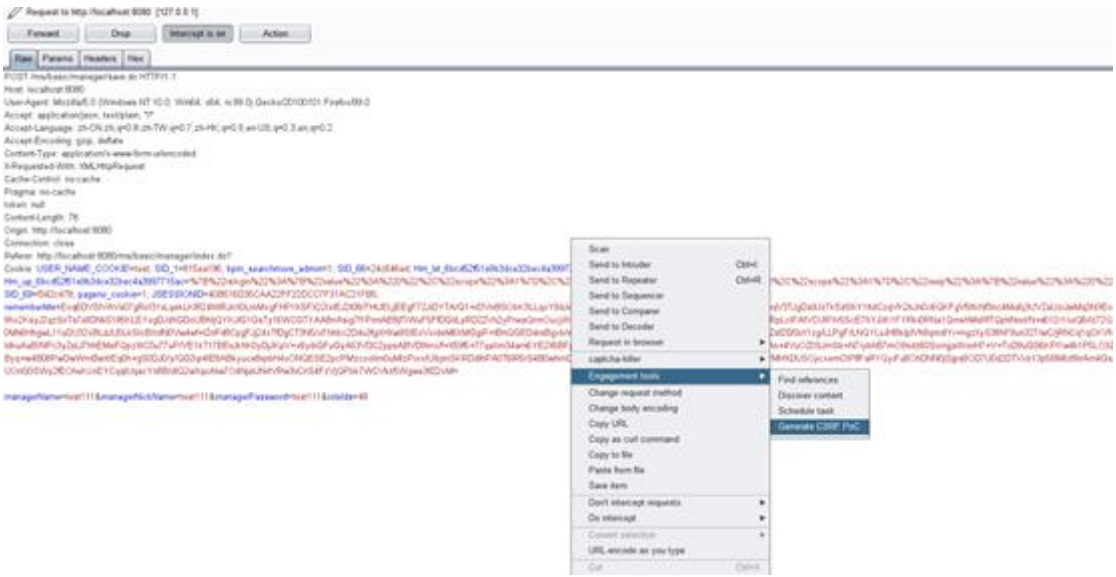
Vulnerability recurrence:

Environment construction reference: https://gitee.com/mingSoft/MCMS The description document in the document can be used After the environment is set up, access the background. The local access background address is: http://localhost:8080/ms/login.do Use the default account password: msopen / msopen After logging in, find the place to add administrator user as shown in the figure below:

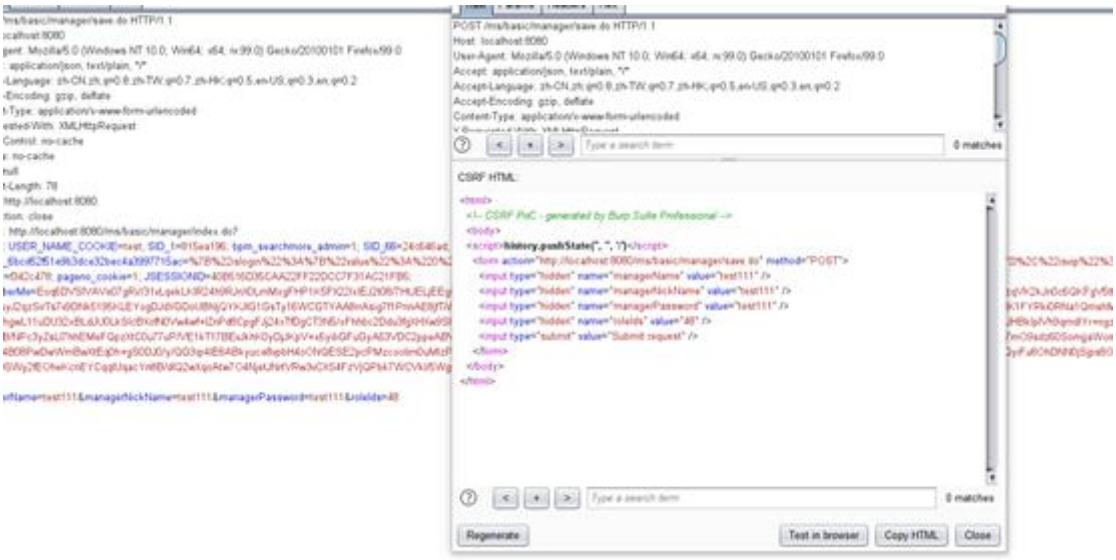


Add all the information needed to add the administrator, then click save and capture the package:

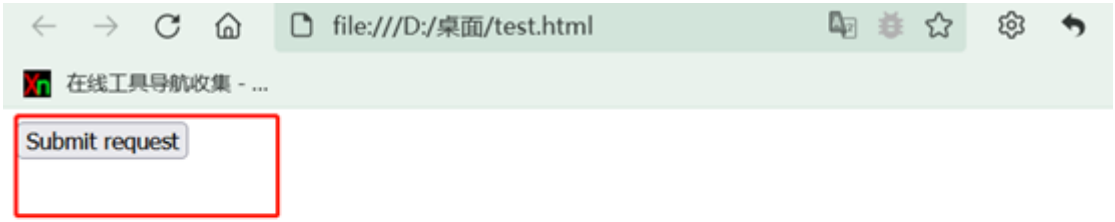
Use burp to generate the payload of CSRF, copy the HTML code and save it locally



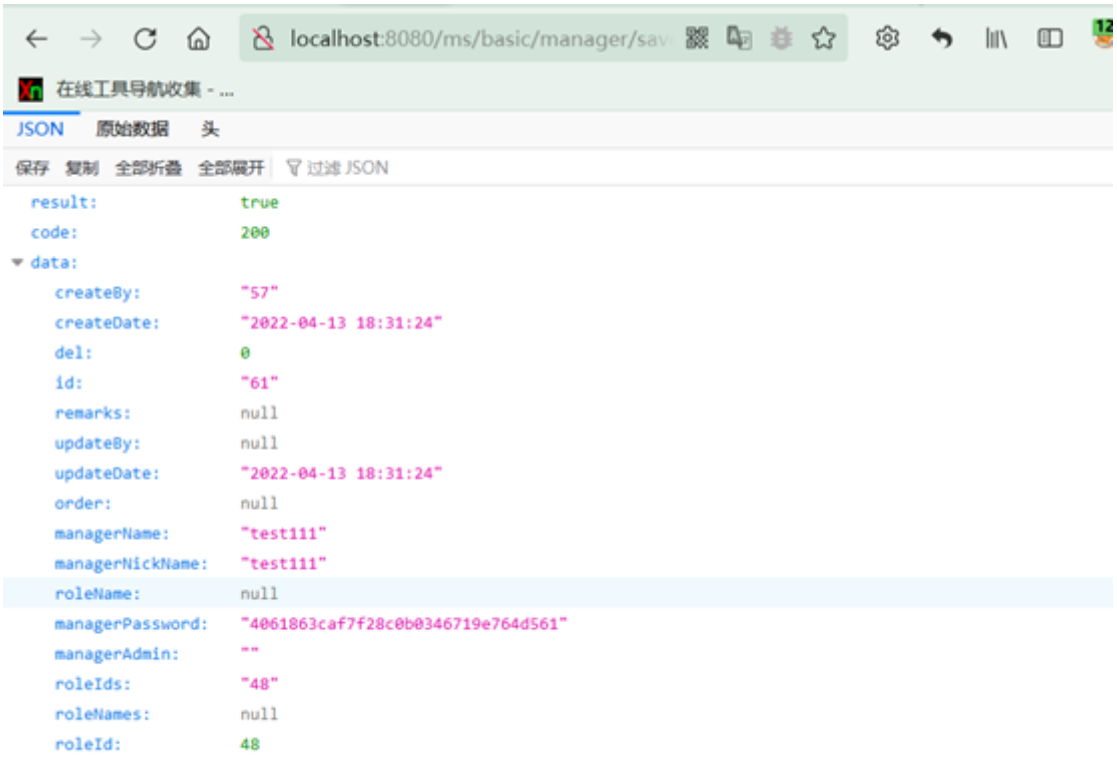
Save the following HTML code as test.html



Then use the same browser you just logged in to open the locally saved HTML page



Click submit request above to see the return value and successfully add the administrator.


localhost:8080/ms/basic/manager/sav
在线工具导航收集 - ...
JSON
原始数据
头
保存
复制
全部折叠
全部展开
过滤 JSON
result: true
code: 200
data:
createBy: "57"
createDate: "2022-04-13 18:31:24"
del: 0
id: "61"
remarks: null
updateBy: null
updateDate: "2022-04-13 18:31:24"
order: null
managerName: "test111"
managerNickName: "test111"
roleName: null
managerPassword: "4061863caf7f28c0b0346719e764d561"
managerAdmin: ""
roleIds: "48"
roleNames: null
roleId: 48

OK!