Compiled

```
└──# nmap -sCV -p3000,5000,7680 -A 10.10.11.26
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 07:05 PDT
Nmap scan report for 10.10.11.26
Host is up (0.29s latency).

PORT     STATE SERVICE    VERSION
3000/tcp open  ppp?
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Cache-Control: max-age=0, private, must-revalidate, no-transform
|     Content-Type: text/html; charset=utf-8
|     Set-Cookie: i_like_gitea=36d9d3b6ca2d437a; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=IEdbT9GPe_m1dHOyEmET_KDc1fY6MTcyMjc4MDMyMDE5MjAwMjIwMA;
Path=/; Max-Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Sun, 04 Aug 2024 14:05:20 GMT
|     <!DOCTYPE html>
|     <html lang="en-US" class="theme-arc-green">
|     <head>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <title>Git</title>
|     <link rel="manifest"
href="data:application/json;base64,eyJuYW1lIjoiR2l0Iiwic2hvcnRfbmFtZSI6IkdpdCIsInN0YXJ
0X3VybCI6Imh0dHA6Ly9naXR1YS5jb21waWx1ZC5odGI6MzAwMC8iLCJpY29ucyI6W3sic3JjIjoiaHR0cDovL
2dpdGVhLmNvbXBpbGVkLmh0YjozMDAwL2Fzc2V0cy9pbWcvbG9nby5wbmciLCJ0eXBlIjoiaW1hZ2UvcG5nIiw
ic216ZXMiOiI1MTJ4NTEyIn0seyJzcmMiOiJodHRwOi8vZ2l0ZWEuY29tcGlsZWQuaHRiOjMwMDA
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Allow: HEAD
|     Allow: HEAD
|     Allow: GET
|     Cache-Control: max-age=0, private, must-revalidate, no-transform
|     Set-Cookie: i_like_gitea=89db312b5bf60b1f; Path=/; HttpOnly; SameSite=Lax
```

```
|     Set-Cookie: _csrf=6ht4cJ6bnZbyC_AOtDG8HPhLRgE6MTcyMjc4MDMyNjcxMjQ5OTUwMA;
Path=/; Max-Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Sun, 04 Aug 2024 14:05:26 GMT
|_    Content-Length: 0
5000/tcp open  upnp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.3 Python/3.12.3
|     Date: Sun, 04 Aug 2024 14:05:20 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 5234
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="UTF-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>Compiled - Code Compiling Services</title>
|     <!-- Bootstrap CSS -->
|     <link rel="stylesheet"
href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css">
|     <!-- Custom CSS -->
|     <style>
|     your custom CSS here */
|     body {
|     font-family: 'Ubuntu Mono', monospace;
|     background-color: #272822;
|     color: #ddd;
|     .jumbotron {
|     background-color: #1e1e1e;
|     color: #fff;
|     padding: 100px 20px;
|     margin-bottom: 0;
|     .services {
|   RTSPRequest:
|     <!DOCTYPE HTML>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <title>Error response</title>
|     </head>
```

```
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 400</p>
|     <p>Message: Bad request version ('RTSP/1.0').</p>
|     <p>Error code explanation: 400 - Bad request syntax or unsupported method.</p>
|     </body>
|_    </html>
7680/tcp open  pando-pub?
2 services unrecognized despite returning data. If you know the service/version,
please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-
service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port3000-TCP:V=7.94SVN%I=7%D=8/4%Time=66AF8AA0%P=aarch64-unknown-linux-
SF:gnu%r(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Ty
SF:pe:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\
SF:x20Bad\x20Request")%r(GetRequest,3000,"HTTP/1\.0\x20200\x20OK\r\nCache-
SF:Control:\x20max-age=0,\x20private,\x20must-revalidate,\x20no-transform\
SF:r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nSet-Cookie:\x20i_lik
SF:e_gitea=36d9d3b6ca2d437a;\x20Path=/;\x20HttpOnly;\x20SameSite=Lax\r\nSe
SF:t-Cookie:\x20_csrf=IEdbT9GPe_m1dHOyEmET_KDc1fY6MTcyMjc4MDMyMDE5MjAwMjIw
SF:MA;\x20Path=/;\x20Max-Age=86400;\x20HttpOnly;\x20SameSite=Lax\r\nX-Fram
SF:e-Options:\x20SAMEORIGIN\r\nDate:\x20Sun,\x2004\x20Aug\x202024\x2014:05
SF::20\x20GMT\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en-US\"\x20class=
SF:\"theme-arc-green\">\n<head>\n\t<meta\x20name=\"viewport\"\x20content=\
SF:"width=device-width,\x20initial-scale=1\">\n\t<title>Git</title>\n\t<li
SF:nk\x20rel=\"manifest\"\x20href=\"data:application/json;base64,eyJuYW1lI
SF:joiR2l0Iiwic2hvcnRfbmFtZSI6IkdpdCIsInN0YXJ0X3VybCI6Imh0dHA6Ly9naXR1YS5j
SF:b21waWxlZC5odGI6MzAwMC8iLCJpY29ucyI6W3sic3JjIjoiaHR0cDovL2dpdGVhLmNvbXB
SF:pbGVkLmh0YjozMDAwL2Fzc2V0cy9pbWcvbG9nby5wbmciLCJ0eXBlIjoiaW1hZ2UvcG5nIi
SF:wic2l6ZXMiOiI1MTJ4NTEyIn0seyJzcmMiOiJodHRwOi8vZ2l0ZWEuY29tcGlsZWQuaHRiO
SF:jMwMDA")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:
SF:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20
SF:Bad\x20Request")%r(HTTPOptions,1A4,"HTTP/1\.0\x20405\x20Method\x20Not\x
SF:20Allowed\r\nAllow:\x20HEAD\r\nAllow:\x20HEAD\r\nAllow:\x20GET\r\nCache
SF:-Control:\x20max-age=0,\x20private,\x20must-revalidate,\x20no-transform
SF:\r\nSet-Cookie:\x20i_like_gitea=89db312b5bf60b1f;\x20Path=/;\x20HttpOnl
SF:y;\x20SameSite=Lax\r\nSet-Cookie:\x20_csrf=6ht4cJ6bnZbyC_AOtDG8HPhLRgE6
SF:MTcyMjc4MDMyNjcxMjQ5OTUwMA;\x20Path=/;\x20Max-Age=86400;\x20HttpOnly;\x
SF:20SameSite=Lax\r\nX-Frame-Options:\x20SAMEORIGIN\r\nDate:\x20Sun,\x2004
SF:\x20Aug\x202024\x2014:05:26\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(
SF:RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\
SF:x20Request");
```

```
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5000-TCP:V=7.94SVN%I=7%D=8/4%Time=66AF8AA0%P=aarch64-unknown-linux-
SF:gnu%r(GetRequest,1521,"HTTP/1\.1\x20200\x20OK\r\nServer:\x20Werkzeug/3\
SF:.0\.3\x20Python/3\.12\.3\r\nDate:\x20Sun,\x2004\x20Aug\x202024\x2014:05
SF::20\x20GMT\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-L
SF:ength:\x205234\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html
SF:\x20lang=\"en\">\n<head>\n\x20\x20\x20\x20<meta\x20charset=\"UTF-8\">\n
SF:\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=device-wi
SF:dth,\x20initial-scale=1\.0\">\n\x20\x20\x20\x20<title>Compiled\x20-\x20
SF:Code\x20Compiling\x20Services</title>\n\x20\x20\x20\x20<!--\x20Bootstra
SF:p\x20CSS\x20-->\n\x20\x20\x20\x20<link\x20rel=\"stylesheet\"\x20href=\"
SF:https://stackpath\.bootstrapcdn\.com/bootstrap/4\.5\.2/css/bootstrap\.m
SF:in\.css\">\n\x20\x20\x20\x20<!--\x20Custom\x20CSS\x20-->\n\x20\x20\x20\
SF:x20<style>\n\x20\x20\x20\x20\x20\x20\x20\x20/\*\x20Add\x20your\x20custo
SF:m\x20CSS\x20here\x20\*/\n\x20\x20\x20\x20\x20\x20\x20\x20body\x20{\n\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-family:\x20'Ubuntu\x2
SF:0Mono',\x20monospace;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:background-color:\x20#272822;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20color:\x20#ddd;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\.jumbotron\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20background-color:\x20#1e1e1e;\n\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20color:\x20#fff;\n\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20padding:\x20100px\x2020px;\n\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20margin-bottom:\x200;\n\x20\x20\x20\x20\x20\x20\x
SF:20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20\.services\x20{\n\x20")%r(RTSP
SF:Request,16C,"<!DOCTYPE\x20HTML>\n<html\x20lang=\"en\">\n\x20\x20\x20\x2
SF:0<head>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20charset=\"utf-8\">\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20<title>Error\x20response</title>\n\x20\x
SF:20\x20\x20</head>\n\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20
SF:\x20<h1>Error\x20response</h1>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Erro
SF:r\x20code:\x20400</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Message:\x20B
SF:ad\x20request\x20version\x20\('RTSP/1\.0'\)\.</p>\n\x20\x20\x20\x20\x20
SF:\x20\x20\x20<p>Error\x20code\x20explanation:\x20400\x20-\x20Bad\x20requ
SF:est\x20syntax\x20or\x20unsupported\x20method\.</p>\n\x20\x20\x20\x20</b
SF:ody>\n</html>\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP (85%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

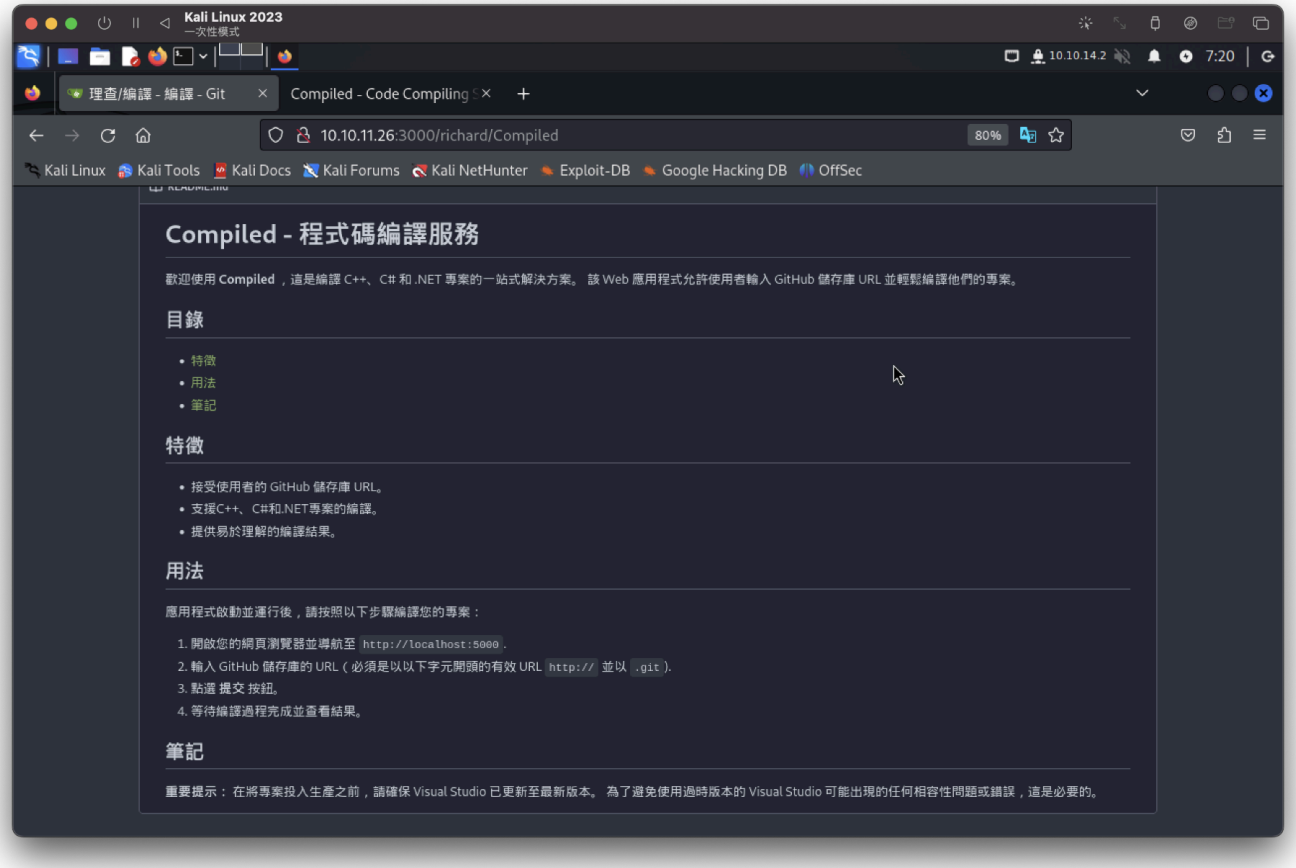
```
TRACEROUTE (using port 7680/tcp)
HOP RTT       ADDRESS
1   290.12 ms 10.10.14.1
2   290.41 ms 10.10.11.26

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 120.51 seconds
```

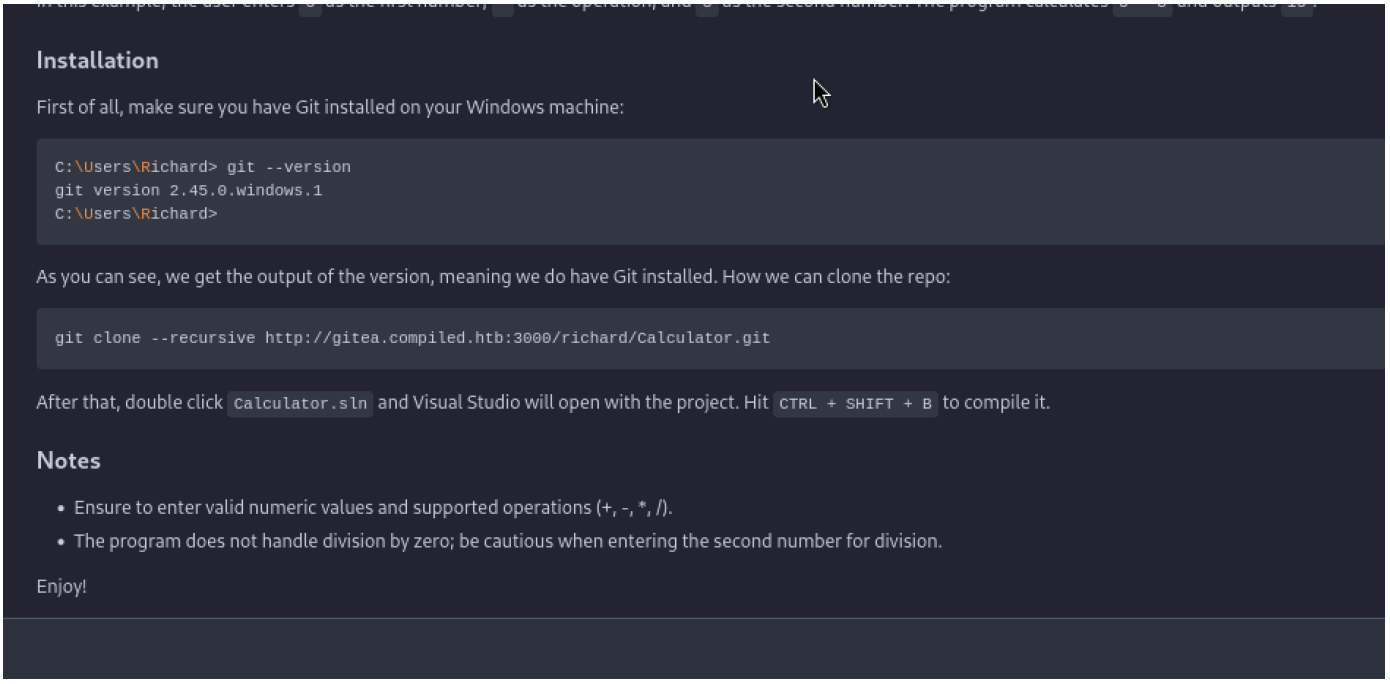
3000、5000port為WEB

3000port像是git。
有註冊使用者（已先註冊），
發現裡面有個用戶，有2項目錄

compiled資料夾



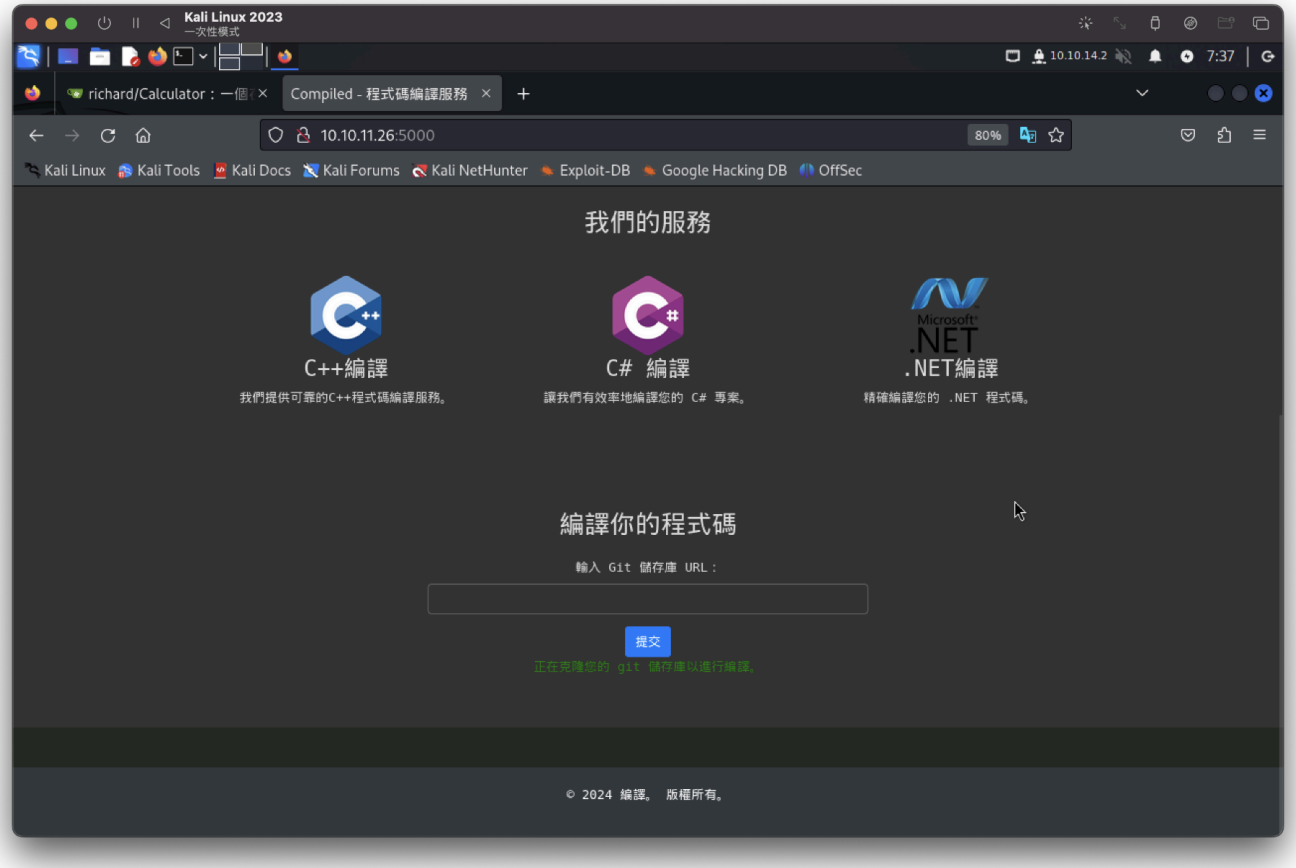
另一個資料夾



這就是一個編譯項目，而且下面有一個gitea.compiled.htb子域名

在所有目錄沒找到任何有關帳密文件

5000port，將兩個目錄的git連結放入後，出現



但不曉得跑去哪？

應該有關git clone漏洞，

找到文件：https://amalmurali.me/posts/git-rce/

我嘗試建立儲存庫（可上傳）