Algernon

Nmap

TCPポートスキャン.

```
$ ports=$(nmap -p- --min-rate=1000 -T4 192.168.140.65 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)

$ nmap -p$ports -sV -A 192.168.140.65
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 21:35 JST
Nmap scan report for 192.168.140.65
Host is up (0.24s latency).

PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst: 
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows
| http-methods: 
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
9998/tcp  open  http          Microsoft IIS httpd 10.0
|_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: Sun, 01 May 2022 12:36:19 GMT\x0D
| Connection: close\x0D
| Content-Length: 326\x0D
| \x0D
| <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">\x0D
| <HTML><HEAD><TITLE>Bad Request</TITLE>\x0D
| <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>\x0D
| <BODY><h2>Bad Request - Invalid Verb</h2>\x0D
| <hr><p>HTTP Error 400. The request verb is invalid.</p>\x0D
|_</BODY></HTML>\x0D
| http-title: Site doesn't have a title (text/html; charset=utf-8).
|_Requested resource was /interface/root
17001/tcp open  remoting      MS .NET Remoting services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode: 
|   3.1.1: 
|_    Message signing enabled but not required
```

```
| smb2-time:
|   date: 2022-05-01T12:36:23
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.34 seconds
```

UDPポートスキャン．

```
$ sudo nmap -Pn -sU --min-rate=10000 192.168.140.65
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-01 21:36 JST
Nmap scan report for 192.168.140.65
Host is up.
All 1000 scanned ports on 192.168.140.65 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds
```

FTP - 21TCP

anonymous ログインができる．

```
$ ftp 192.168.140.65 21
Connected to 192.168.140.65.
220 Microsoft FTP Service
Name (192.168.140.65:funa): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

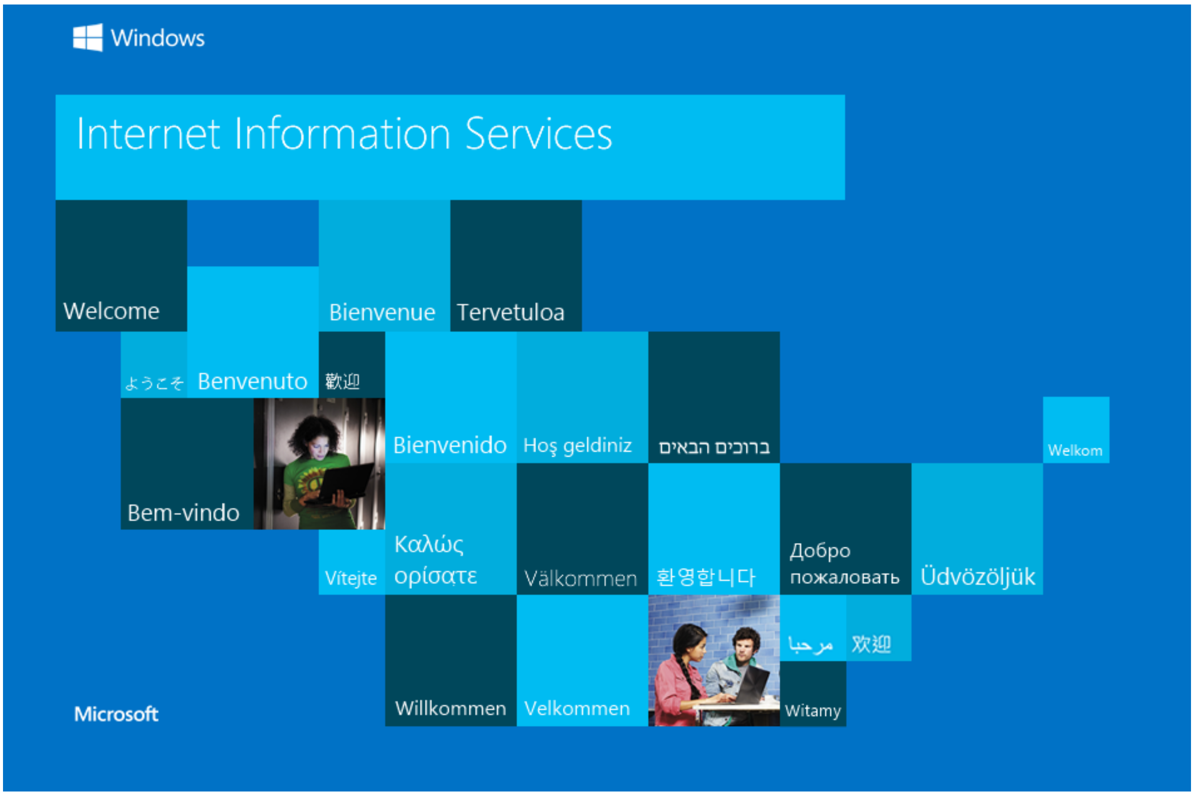
とくに情報は無かった．

HTTP - 80TCP

Internet Information Services (IIS) が表示される．

IIS というのは GUI で設定が可能な web サーバアプリケーション．

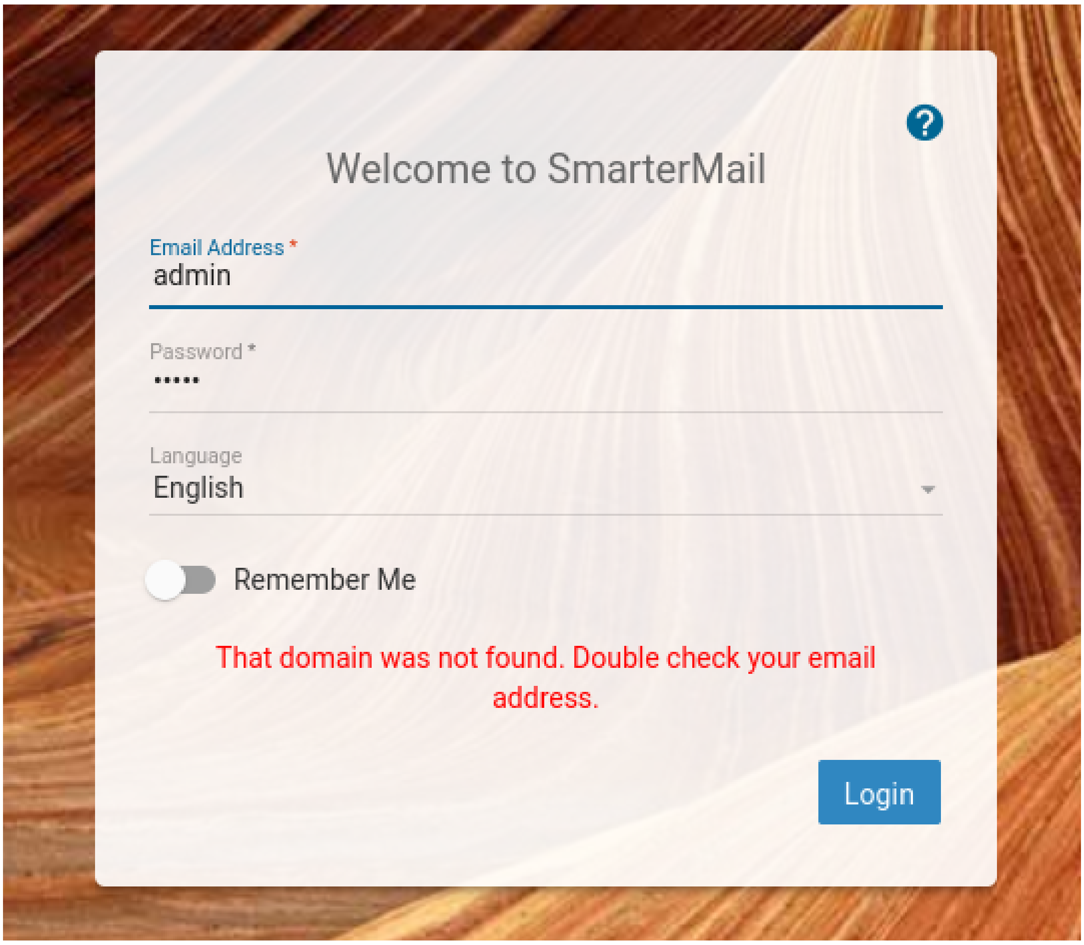
Apache, nginx のような機能が GUI で設定できると考えて良さそう．



HTTP - 9998TCP

SmarterMail のログインページが表示される．

デフォルトである `admin:admin` ではログインできなかった．



Email Address * admin

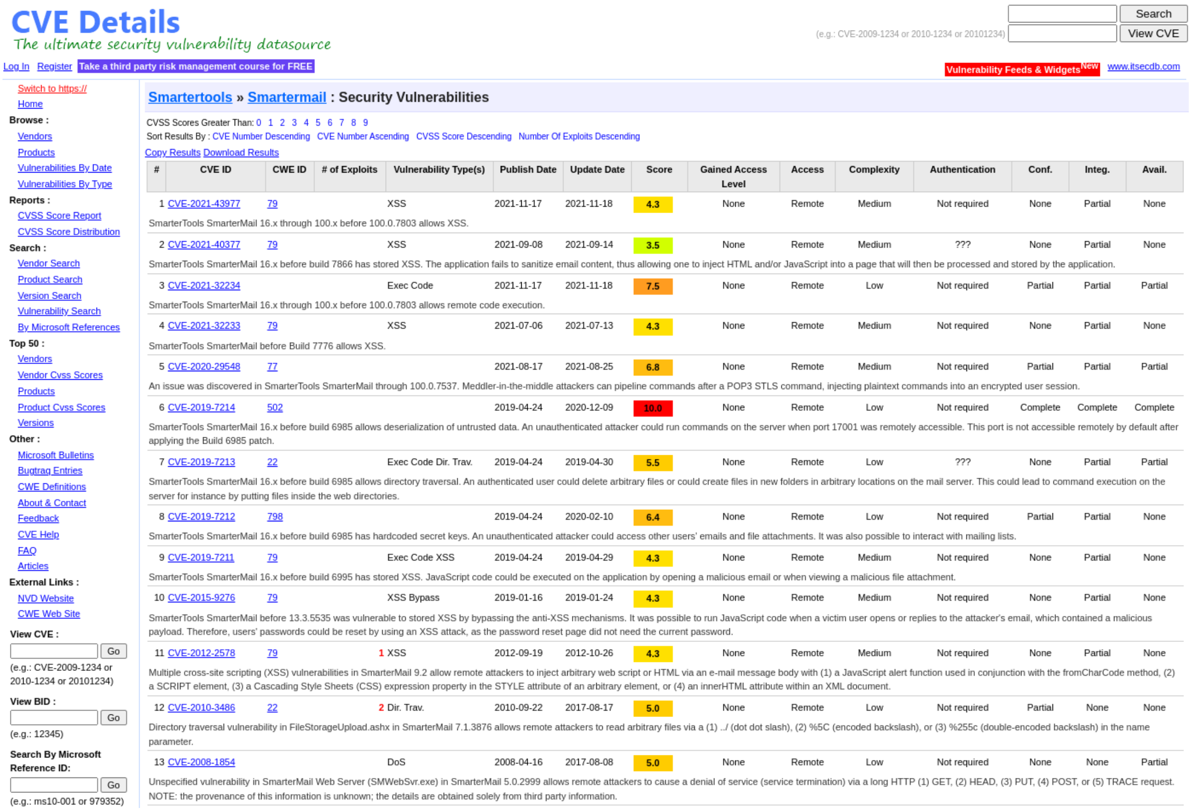
Password * •••••

Language English

Remember Me

That domain was not found. Double check your email address.

SmarterMail の CVE を検索すると，`CVE-2019-7214` という `Score` 10.0 の脆弱性が見つかる．



Smartertools » Smartermail : Security Vulnerabilities

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2021-43977	79		XSS	2021-11-17	2021-11-18	4.3	None	Remote	Medium	Not required	None	Partial	None
SmarterTools SmarterMail 16.x through 100.x before 100.0.7803 allows XSS.														
2	CVE-2021-40377	79		XSS	2021-09-08	2021-09-14	3.5	None	Remote	Medium	???	None	Partial	None
SmarterTools SmarterMail 16.x before build 7866 has stored XSS. The application fails to sanitize email content, thus allowing one to inject HTML and/or JavaScript into a page that will then be processed and stored by the application.														
3	CVE-2021-32234			Exec Code	2021-11-17	2021-11-18	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
SmarterTools SmarterMail 16.x through 100.x before 100.0.7803 allows remote code execution.														
4	CVE-2021-32233	79		XSS	2021-07-06	2021-07-13	4.3	None	Remote	Medium	Not required	None	Partial	None
SmarterTools SmarterMail before Build 7776 allows XSS.														
5	CVE-2020-29548	77			2021-08-17	2021-08-25	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
An issue was discovered in SmarterTools SmarterMail through 100.0.7537. Meddler-in-the-middle attackers can pipeline commands after a POP3 STLS command, injecting plaintext commands into an encrypted user session.														
6	CVE-2019-7214	502			2019-04-24	2020-12-09	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
SmarterTools SmarterMail 16.x before build 6985 allows deserialization of untrusted data. An unauthenticated attacker could run commands on the server when port 17001 was remotely accessible. This port is not accessible remotely by default after applying the Build 6985 patch.														
7	CVE-2019-7213	22		Exec Code Dir. Trav.	2019-04-24	2019-04-30	5.5	None	Remote	Low	???	None	Partial	Partial
SmarterTools SmarterMail 16.x before build 6985 allows directory traversal. An authenticated user could delete arbitrary files or could create files in new folders in arbitrary locations on the mail server. This could lead to command execution on the server for instance by putting files inside the web directories.														
8	CVE-2019-7212	798			2019-04-24	2020-02-10	6.4	None	Remote	Low	Not required	Partial	Partial	None
SmarterTools SmarterMail 16.x before build 6985 has hardcoded secret keys. An unauthenticated attacker could access other users' emails and file attachments. It was also possible to interact with mailing lists.														
9	CVE-2019-7211	79		Exec Code XSS	2019-04-24	2019-04-29	4.3	None	Remote	Medium	Not required	None	Partial	None
SmarterTools SmarterMail 16.x before build 6995 has stored XSS. JavaScript code could be executed on the application by opening a malicious email or when viewing a malicious file attachment.														
10	CVE-2015-9276	79		XSS Bypass	2019-01-16	2019-01-24	4.3	None	Remote	Medium	Not required	None	Partial	None
SmarterTools SmarterMail before 13.3.5535 was vulnerable to stored XSS by bypassing the anti-XSS mechanisms. It was possible to run JavaScript code when a victim user opens or replies to the attacker's email, which contained a malicious payload. Therefore, users' passwords could be reset by using an XSS attack, as the password reset page did not need the current password.														
11	CVE-2012-2578	79	1	XSS	2012-09-19	2012-10-26	4.3	None	Remote	Medium	Not required	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in SmarterMail 9.2 allow remote attackers to inject arbitrary web script or HTML via an e-mail message body with (1) a JavaScript alert function used in conjunction with the fromCharCode method, (2) a SCRIPT element, (3) a Cascading Style Sheets (CSS) expression property in the STYLE attribute of an arbitrary element, or (4) an innerHTML attribute within an XML document.														
12	CVE-2010-3486	22	2	Dir. Trav.	2010-09-22	2017-08-17	5.0	None	Remote	Low	Not required	Partial	None	None
Directory traversal vulnerability in FileStorageUpload.ashx in SmarterMail 7.1.3876 allows remote attackers to read arbitrary files via a (1) ../ (dot dot slash), (2) %5C (encoded backslash), or (3) %255c (double-encoded backslash) in the name parameter.														
13	CVE-2008-1854			DoS	2008-04-16	2017-08-08	5.0	None	Remote	Low	Not required	None	None	Partial
Unspecified vulnerability in SmarterMail Web Server (SMWebSvr.exe) in SmarterMail 5.0.2999 allows remote attackers to cause a denial of service (service termination) via a long HTTP (1) GET, (2) HEAD, (3) PUT, (4) POST, or (5) TRACE request. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.														

> CVE-2019-7214
>
> SmarterTools SmarterMail 16.x before build 6985 allows deserialization of untrusted data. An unauthenticated attacker could run commands on the server when port 17001 was remotely accessible. This port is not accessible remotely by default after applying the Build 6985 patch.

Nmap の結果を見ると，`17001` ポートが開いているため，バージョンが `16.x` かは確認できないが試してみる価値はありそう．

SmarterMail Build 6985 - RCE のエクスプロイトコードをコピーし，IP アドレスを自分の環境のものに書き換えて実行する．

```
$ python3 smartermail_deserialisation_attack.py
```

実行する際に `netcat` でリバースシェルを受け取る．

```
$ nc -lvp 6666
listening on [any] 6666 ...
```

シェルは返ってこなかった．