ابزار نویسی

شرح ابزار

امکانات این بخش در ادامه بخش‌های تمرین عملی اول آورده شده است. در نتیجه در منوی اصلی گزینه‌ای تحت عنوان Find an open port’s service اضافه شده است:

```
-------------------- INFORMATION  SECURITY --------------------
SELECT AN OPTION:
     1) PING AND IP
     2) PING AND IP RANGE AND SHOW ACTIVE HOSTS
     3) SCAN OPEN PORTS OF AN ACTIVE HOST
     4) [NEW!] FIND AN OPEN PORT'S SERVICE
    -1) EXIT PROGRAM
```

با زدن گزینه ۴، تابع detect_port_services فراخوانی می‌شود:

```python
def detect_port_services(ip, range_start, range_end):
    port_services = {}
    port_detecting_progress = tqdm(range(range_start, range_end + 1))
    try:
        for port in port_detecting_progress:
            port_detecting_progress.set_description('checking port {}'.upper().format(port))

            setdefaulttimeout(2)
            s = socket(AF_INET, SOCK_STREAM)
            result = s.connect_ex((ip, port))

            # trying to get more information about port service
            try:
                message = b'WhoAreYou'
                s.send(message)
                banner = s.recv(100)
                s.close()
            except IOError:
                banner = b''

            if result == 0:
                service_name = getservbyport(port, 'tcp')
                port_services.update({port: (service_name, banner.replace(b'\r\n', b'').decode('utf-8'))})

            s.close()
        log_port_services(ip, range_start, range_end, port_services)

    except KeyboardInterrupt:
        print("\ncanceled...".upper())
    except gaierror:
        print("\nHostname Could Not Be Resolved".upper())
    return port_services
```

همانطور که میبینیم این تابع سرویس بازه‌ای از پورت‌های یک هاست فعال را به ما نشان می‌دهد. برای این که بتوان به اطلاعاتی در مورد سرویس پورت مورد نظر دست یافت، پیام WhoAreYou را به پورت هاست مورد نظر ارسال می‌کنیم و در صورت دریافت پیام، آن را به کاربر نمایش می‌دهیم. مقداری که این تابع بر می‌گرداند یک دیکشنری با کلیدِ شماره پورت و مقداری برابر با یک tuple با نام سرویس پورت و توضیحات آن سرویس می‌باشد. بعنوان مثال داریم:

```
{
    21: ('ftp', '220 daycent.com@Anzali FTP server (MikroTik 6.48.3) ready'),
    22: ('ssh', 'SSH-2.0-ROSSSH'),
    ...
}
```

همچنین در تابع log_port_services می‌توان داخل فایل result_port_services.txt نتایج تابع قبل را ثبت نمود.

```
def log_port_services(ip, range_start, range_end, port_services):
    try:
        with open("results/result_port_services.txt", "a") as file:
            file.write('@ {}'.upper().format(datetime.now()))
            file.write('\nhost {} open ports\' services from {} to {}:'.upper().format(ip, range_start, range_end
            [file.write('\n {}:\t{} {}'
                        .format(port,
                                port_services[port][0].upper(),
                                '' if not port_services[port][1] else '\n\t\t({})\n'
                                .format(port_services[port][1]))
                        ) for port in port_services.keys()]
            if not port_services.keys():
                file.write('\n× no open ports was founded!'.upper())
            file.write('\n----------------------------------------------------\n')
    except FileNotFoundError:
        print('PLEASE CREATE \"/results/result_detect_open_ports.txt\" AND TRY AGAIN.')
```

بعنوان مثال محتوای لاگ شده برای یکی از موارد به صورت زیر می‌باشد:

```
----------------------------------------------------
@ 2021-12-01 14:42:54.521259
HOST 89.43.3.170 OPEN PORTS' SERVICES FROM 1 TO 200:
 21:    FTP
        (220 daycent.com@Anzali FTP server (MikroTik 6.48.3) ready)

 22:    SSH
        (SSH-2.0-ROSSSH)

 23:    TELNET
 53:    DOMAIN
 80:    HTTP
----------------------------------------------------
```

نمونه خروجی

- خروجی برای هاست **89.43.3.170** از پورت‌های ۱ تا ۱۰۰۰

```
-------------------- INFORMATION  SECURITY --------------------
SELECT AN OPTION:
     1) PING AND IP
     2) PING AND IP RANGE AND SHOW ACTIVE HOSTS
     3) SCAN OPEN PORTS OF AN ACTIVE HOST
     4) [NEW!] FIND AN OPEN PORT'S SERVICE
    -1) EXIT PROGRAM
4
TARGET IP ADDRESS: 89.43.3.170
START OF RANGE   : 1
END  OF  RANGE   : 1000
CHECKING PORT 1000: 100%|██████████| 1000/1000 [00:29<00:00, 33.42it/s]

PORT SERVICES:
 21:    FTP
        (220 daycent.com@Anzali FTP server (MikroTik 6.48.3) ready)

 22:    SSH
        (SSH-2.0-ROSSSH)

 23:    TELNET
 53:    DOMAIN
 80:    HTTP
 443:   HTTPS
```

- خروجی برای هاست **89.43.3.85** از پورت‌های ۱ تا ۱۰۰۰

```
-------------------- INFORMATION  SECURITY --------------------
SELECT AN OPTION:
     1) PING AND IP
     2) PING AND IP RANGE AND SHOW ACTIVE HOSTS
     3) SCAN OPEN PORTS OF AN ACTIVE HOST
     4) [NEW!] FIND AN OPEN PORT'S SERVICE
    -1) EXIT PROGRAM
4
TARGET IP ADDRESS: 89.43.3.85
START OF RANGE   : 1
END  OF  RANGE   : 1000
CHECKING PORT 1000: 100%|██████████| 1000/1000 [00:53<00:00, 18.68it/s]

PORT SERVICES:
 22:    SSH
        (SSH-2.0-ROSSSH)

 53:    DOMAIN
 443:   HTTPS
```

- **خروجی برای هاست 89.43.3.69 از پورت‌های ۱ تا ۱۰۰۰**

```
-------------------- INFORMATION  SECURITY --------------------
SELECT AN OPTION:
     1) PING AND IP
     2) PING AND IP RANGE AND SHOW ACTIVE HOSTS
     3) SCAN OPEN PORTS OF AN ACTIVE HOST
     4) [NEW!] FIND AN OPEN PORT'S SERVICE
    -1) EXIT PROGRAM
4
TARGET IP ADDRESS: 89.43.3.69
START OF RANGE   : 1
END  OF  RANGE   : 1000
CHECKING PORT 1000: 100%|██████████| 1000/1000 [00:51<00:00, 19.26it/s]

PORT SERVICES:
 22:    SSH
        (SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u6)

 53:    DOMAIN
 80:    HTTP
        (<html><head><title>400 Bad Request</title></head><body bgcolor="white"><center><h1>400 Bad Req)

 122:   SMAKYNET
        (SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u6)

 443:   HTTPS
```

- **خروجی برای هاست 89.43.3.155 از پورت‌های ۱ تا ۱۰۰۰**

```
-------------------- INFORMATION  SECURITY --------------------
SELECT AN OPTION:
     1) PING AND IP
     2) PING AND IP RANGE AND SHOW ACTIVE HOSTS
     3) SCAN OPEN PORTS OF AN ACTIVE HOST
     4) [NEW!] FIND AN OPEN PORT'S SERVICE
    -1) EXIT PROGRAM
4
TARGET IP ADDRESS: 89.43.3.155
START OF RANGE   : 1
END  OF  RANGE   : 1000
CHECKING PORT 1000: 100%|██████████| 1000/1000 [00:33<00:00, 29.55it/s]

PORT SERVICES:
 53:    DOMAIN
 85:    MIT-ML-DEV
 443:   HTTPS
```

بررسی ابزارهای آماده

بررسی به کمک nmap و تایید صحت بخش ابزار نویسی

- خروجی برای هاست **89.43.3.170**

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-01 15:40 +0330
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:40
Completed NSE at 15:40, 0.00s elapsed
Initiating NSE at 15:40
Completed NSE at 15:40, 0.00s elapsed
Initiating NSE at 15:40
Completed NSE at 15:40, 0.00s elapsed
Initiating Ping Scan at 15:40
Scanning 89.43.3.170 [2 ports]
Completed Ping Scan at 15:40, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:40
Completed Parallel DNS resolution of 1 host. at 15:40, 0.00s elapsed
Initiating Connect Scan at 15:40
Scanning 170.mobinnet.net (89.43.3.170) [1000 ports]
Discovered open port 53/tcp on 89.43.3.170
Discovered open port 23/tcp on 89.43.3.170
Discovered open port 22/tcp on 89.43.3.170
Discovered open port 1723/tcp on 89.43.3.170
Discovered open port 21/tcp on 89.43.3.170
Discovered open port 443/tcp on 89.43.3.170
Discovered open port 80/tcp on 89.43.3.170
Discovered open port 8008/tcp on 89.43.3.170
Discovered open port 8010/tcp on 89.43.3.170
Discovered open port 2000/tcp on 89.43.3.170
Discovered open port 5060/tcp on 89.43.3.170
Completed Connect Scan at 15:40, 2.67s elapsed (1000 total ports)
Initiating Service scan at 15:40
Scanning 11 services on 170.mobinnet.net (89.43.3.170)
Service scan Timing: About 72.73% done; ETC: 15:43 (0:00:51 remaining)
Completed Service scan at 15:43, 160.44s elapsed (11 services on 1 host)
NSE: Script scanning 89.43.3.170.
Initiating NSE at 15:43
Completed NSE at 15:43, 40.34s elapsed
Initiating NSE at 15:43
Completed NSE at 15:43, 1.20s elapsed
Initiating NSE at 15:43
Completed NSE at 15:43, 0.00s elapsed
Nmap scan report for 170.mobinnet.net (89.43.3.170)
Host is up (0.024s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT     STATE    SERVICE     VERSION
21/tcp   open     ftp         MikroTik router ftpd 6.48.3
| ftp-syst:
|   SYST: UNIX MikroTik 6.48.3
22/tcp   open     ssh         MikroTik RouterOS sshd (protocol 2.0)
| ssh-hostkey:
|   1024 2f:56:7f:2c:ba:dc:1e:2a:2e:31:fb:96:4a:23:fd:ff (DSA)
|   2048 08:11:dc:a8:30:15:a1:0b:38:75:a6:23:60:77:57:33 (RSA)
23/tcp   open     tcpwrapped
53/tcp   open     domain?
80/tcp   open     http        MikroTik router config httpd
| http-title: RouterOS router configuration page
| http-robots.txt: 1 disallowed entry
|  /
| http-methods:
|   Supported Methods: GET HEAD
443/tcp  open     ssl/https?
1723/tcp open     pptp        MikroTik (Firmware: 1)
2000/tcp open     cisco-sccp?
5060/tcp open     tcpwrapped
8008/tcp open     http
| http-title: Did not follow redirect to https://170.mobinnet.net:8010/
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 302 Found
|     Location: https://:8010/nice%20ports%2C/Tri%6Eity.txt%2ebak
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|   GenericLines, HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 302 Found
```

همانگونه که در شکل بالا مشاهده می‌شود، سرویس‌های گفته شده با ابزار ما مطابقت دارد.

- **خروجی برای هاست 89.43.3.85**

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-01 15:45 +0330
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:45
Completed NSE at 15:45, 0.00s elapsed
Initiating NSE at 15:45
Completed NSE at 15:45, 0.00s elapsed
Initiating NSE at 15:45
Completed NSE at 15:45, 0.00s elapsed
Initiating Ping Scan at 15:45
Scanning 89.43.3.85 [2 ports]
Completed Ping Scan at 15:45, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:45
Completed Parallel DNS resolution of 1 host. at 15:45, 0.28s elapsed
Initiating Connect Scan at 15:45
Scanning 85.mobinnet.net (89.43.3.85) [1000 ports]
Discovered open port 443/tcp on 89.43.3.85
Discovered open port 53/tcp on 89.43.3.85
Discovered open port 22/tcp on 89.43.3.85
Discovered open port 5060/tcp on 89.43.3.85
Discovered open port 2000/tcp on 89.43.3.85
Discovered open port 8010/tcp on 89.43.3.85
Discovered open port 8008/tcp on 89.43.3.85
Completed Connect Scan at 15:45, 1.85s elapsed (1000 total ports)
Initiating Service scan at 15:45
Scanning 7 services on 85.mobinnet.net (89.43.3.85)
Service scan Timing: About 57.14% done; ETC: 15:49 (0:01:41 remaining)
Completed Service scan at 15:47, 160.30s elapsed (7 services on 1 host)
NSE: Script scanning 89.43.3.85.
Initiating NSE at 15:47
Completed NSE at 15:48, 40.57s elapsed
Initiating NSE at 15:48
Completed NSE at 15:48, 1.07s elapsed
Initiating NSE at 15:48
Completed NSE at 15:48, 0.00s elapsed
Nmap scan report for 85.mobinnet.net (89.43.3.85)
Host is up (0.049s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         MikroTik RouterOS sshd (protocol 2.0)
| ssh-hostkey:
|   1024 24:53:c5:a2:36:31:4f:d5:af:6e:07:e6:e6:65:a6:e7 (DSA)
|   2048 2c:8b:e9:7d:a4:6e:0e:37:5c:f9:b6:ea:0e:26:ee:87 (RSA)
53/tcp   open     domain?
443/tcp  open     tcpwrapped
2000/tcp open     cisco-sccp?
5060/tcp open     tcpwrapped
8008/tcp open     http
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 302 Found
|     Location: https://:8010/nice%20ports%2C/Tri%6Eity.txt%2ebak
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|   GenericLines, HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 302 Found
|     Location: https://:8010
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|   GetRequest:
|     HTTP/1.1 302 Found
|     Location: https://:8010/
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
| http-title: Did not follow redirect to https://85.mobinnet.net:8010/
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
8010/tcp open     ssl/xmpp?
```

- **خروجی برای هاست 89.43.3.69**

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-01 15:53 +0330
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:53
Completed NSE at 15:53, 0.00s elapsed
Initiating NSE at 15:53
Completed NSE at 15:53, 0.00s elapsed
Initiating NSE at 15:53
Completed NSE at 15:53, 0.00s elapsed
Initiating Ping Scan at 15:53
Scanning 89.43.3.69 [2 ports]
Completed Ping Scan at 15:53, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:53
Completed Parallel DNS resolution of 1 host. at 15:53, 0.60s elapsed
Initiating Connect Scan at 15:53
Scanning 69.mobinnet.net (89.43.3.69) [1000 ports]
Discovered open port 443/tcp on 89.43.3.69
Discovered open port 53/tcp on 89.43.3.69
Discovered open port 22/tcp on 89.43.3.69
Discovered open port 1723/tcp on 89.43.3.69
Discovered open port 80/tcp on 89.43.3.69
Discovered open port 8080/tcp on 89.43.3.69
Discovered open port 5060/tcp on 89.43.3.69
Discovered open port 8010/tcp on 89.43.3.69
Discovered open port 7443/tcp on 89.43.3.69
Discovered open port 6666/tcp on 89.43.3.69
Discovered open port 1935/tcp on 89.43.3.69
Discovered open port 2000/tcp on 89.43.3.69
Discovered open port 8008/tcp on 89.43.3.69
Completed Connect Scan at 15:53, 3.02s elapsed (1000 total ports)
Initiating Service scan at 15:53
Scanning 13 services on 69.mobinnet.net (89.43.3.69)
Service scan Timing: About 61.54% done; ETC: 15:54 (0:00:32 remaining)
Service scan Timing: About 69.23% done; ETC: 15:56 (0:00:58 remaining)
Completed Service scan at 15:56, 157.54s elapsed (13 services on 1 host)
NSE: Script scanning 89.43.3.69.
Initiating NSE at 15:56
Completed NSE at 15:56, 41.06s elapsed
Initiating NSE at 15:56
Completed NSE at 15:56, 1.14s elapsed
Initiating NSE at 15:56
Completed NSE at 15:56, 0.00s elapsed
Nmap scan report for 69.mobinnet.net (89.43.3.69)
Host is up (0.063s latency).
Not shown: 984 closed tcp ports (conn-refused)
PORT     STATE    SERVICE    VERSION
22/tcp   open     ssh        OpenSSH 6.0p1 Debian 4+deb7u6 (protocol 2.0)
| ssh-hostkey:
|   1024 50:f2:b0:96:39:a5:ca:58:8c:fb:2b:bb:0a:d5:a5:ce (DSA)
|   2048 6b:06:64:be:4f:1e:f9:31:37:42:9c:f8:91:da:a5:37 (RSA)
|   256 a3:10:b6:7e:1c:c1:7b:33:11:24:90:33:c7:43:12:95 (ECDSA)
53/tcp   open     domain?
80/tcp   open     http       nginx
| http-methods:
|   Supported Methods: GET HEAD POST
| http-title: airVision: [NVR] - Software Portal
| http-favicon: Unknown favicon MD5: 0AEE66DCE5587FE6FAD5AE2826501ADD
443/tcp  open     tcpwrapped
1723/tcp open     pptp       MikroTik (Firmware: 1)
1935/tcp open     rtmp?
2000/tcp open     tcpwrapped
5060/tcp open     tcpwrapped
5900/tcp filtered vnc
6666/tcp open     irc?
| irc-info: Unable to open connection
7443/tcp open     ssl/http   Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
| ssl-date: 2021-12-01T12:26:45+00:00; 0s from scanner time.
| http-server-header: Apache-Coyote/1.1
| http-favicon: Unknown favicon MD5: 7CBC9499D4B44CE2E491893C886A4899
| ssl-cert: Subject: commonName=192.168.8.2/organizationName=ubnt.com/stateOrProvinceName=CA/countryName=US
| Issuer: commonName=192.168.8.2/organizationName=ubnt.com/stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2016-10-19T17:19:18
```

- **خروجی برای هاست 89.43.3.155**

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-01 16:03 +0330
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:03
Completed NSE at 16:03, 0.00s elapsed
Initiating NSE at 16:03
Completed NSE at 16:03, 0.00s elapsed
Initiating NSE at 16:03
Completed NSE at 16:03, 0.00s elapsed
Initiating Ping Scan at 16:03
Scanning 89.43.3.155 [2 ports]
Completed Ping Scan at 16:03, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:03
Completed Parallel DNS resolution of 1 host. at 16:03, 0.27s elapsed
Initiating Connect Scan at 16:03
Scanning 155.mobinnet.net (89.43.3.155) [1000 ports]
Discovered open port 53/tcp on 89.43.3.155
Discovered open port 443/tcp on 89.43.3.155
Increasing send delay for 89.43.3.155 from 0 to 5 due to 13 out of 32 dropped probes since last increase.
Increasing send delay for 89.43.3.155 from 5 to 10 due to 11 out of 15 dropped probes since last increase.
Discovered open port 2000/tcp on 89.43.3.155
Discovered open port 8010/tcp on 89.43.3.155
Discovered open port 5060/tcp on 89.43.3.155
Discovered open port 8008/tcp on 89.43.3.155
Discovered open port 85/tcp on 89.43.3.155
Completed Connect Scan at 16:04, 22.11s elapsed (1000 total ports)
Initiating Service scan at 16:04
Scanning 7 services on 155.mobinnet.net (89.43.3.155)
Service scan Timing: About 57.14% done; ETC: 16:07 (0:01:42 remaining)
Completed Service scan at 16:06, 160.29s elapsed (7 services on 1 host)
NSE: Script scanning 89.43.3.155.
Initiating NSE at 16:06
Completed NSE at 16:07, 40.49s elapsed
Initiating NSE at 16:07
Completed NSE at 16:07, 1.20s elapsed
Initiating NSE at 16:07
Completed NSE at 16:07, 0.00s elapsed
Nmap scan report for 155.mobinnet.net (89.43.3.155)
Host is up (0.022s latency).
Not shown: 992 closed tcp ports (conn-refused)
PORT     STATE    SERVICE     VERSION
53/tcp   open     domain?
85/tcp   open     http        MikroTik router config httpd
| http-title: RouterOS router configuration page
| http-robots.txt: 1 disallowed entry
|  /
| http-methods:
|   Supported Methods: GET HEAD
443/tcp  open     tcpwrapped
2000/tcp open     cisco-sccp?
5060/tcp open     tcpwrapped
8008/tcp open     http
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 302 Found
|     Location: https://:8010/nice%20ports%2C/Tri%6Eity.txt%2ebak
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|   GenericLines, HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 302 Found
|     Location: https://:8010
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Content-Security-Policy: frame-ancestors 'self'
|   GetRequest:
|     HTTP/1.1 302 Found
|     Location: https://:8010/
|     Connection: close
|     X-Frame-Options: SAMEORIGIN
|     X-XSS-Protection: 1; mode=block
```

بررسی SSL/TLS

از وبسایت https://www.ssllabs.com/ssltest برای این کار استفاده میکنیم:

Configuration

Protocols

TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Cipher Suites

# TLS 1.3 (suites in server-preferred order)	
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_128_CCM_8_SHA256 (0x1305) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_128_CCM_SHA256 (0x1304) ECDH x25519 (eq. 3072 bits RSA) FS	128
# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH secp256r1 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	128

در هنگام اولین اتصال به سرویس‌دهنده (وب سرور)، سرویس‌گیرنده (مرورگر کاربر) سعی می‌کند از طریق بالاترین نسخه‌ای که پشتیبانی می‌کند (مثلاً TLS ۱.۲) ارتباط را ایجاد کند. اگر وب سرور نیز قابلیت پشتیبانی از این نسخه را داشته باشد ارتباط برقرار می‌شود در غیر این صورت اگر مثلاً وب سرور از نسخه‌ی TLS ۱.۰ استفاده کند، مرورگر کاربر نیز به نسخه‌ی پایین‌تر یعنی TLS ۱.۰ سوییچ می‌کند. به این رویکرد downgrade گفته می‌شود می‌تواند توسط یک نفوذگر داخل شبکه‌ی کاربر نیز اتفاق بیافتد. که در اینجا نفوذگر مرورگر کاربر را وادار می‌کند تا از طریق SSLv۳ اتصال را برقرار نماید. در SSLv۳ برای رمزنگاری از روش‌های RC۴ و یا یک روش رمز بلوکی در حالت CBC استفاده می‌شود. در ساختار رمز بلوکی در حالت CBC این پروتکل مشکلی وجود دارد که باعث می‌شود نفوذگر بتواند با آزمون خطا، با تعداد درخواست های اندکی، قسمتی از درخواست رمز شده بین مرورگر و وب سرور را حدس بزند. این داده‌ی حدس زده شده می‌تواند کوکی کاربر باشد که نفوذگر با استفاده از آن می‌تواند وارد حساب کاربر بشود.اصل مبنای تئوری این آسیب پذیری توسط Serge Vaudenay در سال ۲۰۰۱ مطرح شده بود، اما او فکر می‌کرده است که امکان استفاده عملی از این آسیب پذیری وجود ندارد و نهایتا این آسیب‌پذیری توسط مهندسان گوگل اعلام شد و Poodle نام گرفت.

کاربران هر وب‌سایتی (سرویس دهنده) که از SSLv۳ پشتیبانی کند (در تنظیمات وب سرور غیر فعال نکرده باشد)، آسیب‌پذیر می‌باشند. در واقع حتی اگر وب سایت از نسخه‌های TLS استفاده کند به دلیل قابلیت downgrade (بازگشت به نسخه‌ی قبلی) آسیب‌پذیر می‌باشد زیرا نفوذگر داخل شبکه می‌تواند مرورگر کاربر را وادار کند تا از طریق SSLv۳ اتصال برقرار کند.

نفوذگر (داخل شبکه‌ی کاربر) با بهره‌برداری از این آسیب‌پذیری می‌تواند اطلاعات حساس کاربر مانند (کوکی که هویت کاربر است) را برباید و در نهایت وارد حساب کاربر شود.[۱]

مقایسه دو سایت sazkala.com و shahreketabonline.com

به کمک وب‌سایت گفته شده اطلاعات سایت های گفته شده را مورد بررسی قرار می‌دهیم.

برای sazkala داریم:

```
Domain Name: sazkala.com
Registry Domain ID: 1756049692_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.webnic.cc
Registrar URL: webnic.cc
Updated Date: 2018-09-25T22:02:22Z
Creation Date: 2012-10-31T02:20:57Z
Registrar Registration Expiration Date: 2023-10-31T10:20:57Z
Registrar: WEBCC
Registrar IANA ID: 460
Registrar Abuse Contact Email: compliance_abuse@webnic.cc
Registrar Abuse Contact Phone: +60.389966799
Domain Status: clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibite
Domain Status: clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: mahan yousefinezhadan
Registrant Organization: na
Registrant Street: Al Basatin St Al Basatin St
Registrant City: Sohar
Registrant State/Province: SR
Registrant Postal Code: 311
Registrant Country: OM
Registrant Phone: +968.22951108
Registrant Phone Ext:
Registrant Fax: +968.
Registrant Fax Ext:
Registrant Email: sepidmoj@yahoo.com
Registry Admin ID: Not Available From Registry
```

همچنین برای shahreketabonline نیز خواهیم داشت:

---

[۱] منبع: https://bayan.blog.ir/1393/07/23-1

```
Domain Name: SHAHREKETABONLINE.COM
Registry Domain ID: 1736117960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://tucowsdomains.com
Updated Date: 2020-09-14T11:20:45
Creation Date: 2012-07-28T08:11:25
Registrar Registration Expiration Date: 2023-07-28T08:11:25
Registrar: TUCOWS, INC.
Registrar IANA ID: 69
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Ontario
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: CA
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext:
Registrant Email: https://tieredaccess.com/contact/71f408f4-1a28-481f-8d98-d980f28a3f0d
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
```

همانگونه که میبینیم برای sazkala تقریبا اکثر اطلاعات ممکن برای افراد از طریق ابزاری مثل whois و یا سایر سایت‌ها با سرویس‌های مشابه امکان پذیر می‌باشد. از این اطلاعات می‌توان به مشخصات و راه‌های ارتباطی با registrant این دامنه اشاره نمود. اما در مقابل وبسایت shahreketabonline اکثر این موارد به جهت حفظ حریم خصوصی ویرایش شده اند.

اطلاعات قرار گرفته شده در این بخش مربوطه به کسی می‌باشد که در مورد این دامنه مسئولیت دارد و نه کسی که از آن استفاده می‌کند.[۲]

بررسی OWASP TOP 10[۳]

1. آسیب پذیری Broken Access Control

کنترل دسترسی سیاستی را اعمال می کند که کاربران نتوانند خارج از مجوزهای مورد نظر خود عمل کنند. خرابی‌ها معمولاً منجر به افشای اطلاعات غیرمجاز، اصلاح یا تخریب همه داده‌ها یا انجام یک کار تجاری خارج از محدودیت‌های کاربر می‌شوند. آسیب پذیری های رایج کنترل دسترسی عبارتند از:

- نقض اصل حداقل امتیاز یا رد کردن به طور پیش‌فرض، که در آن دسترسی فقط باید برای قابلیت‌ها، نقش‌ها یا کاربران خاص اعطا شود، اما برای همه در دسترس است.
- دور زدن بررسی‌های کنترل دسترسی با تغییر URL (دستکاری پارامتر یا مرور اجباری)، وضعیت برنامه داخلی، یا صفحه HTML، یا با استفاده از ابزار حمله برای اصلاح درخواست‌های API.

---

۲ https://lookup.icann.org/ و https://www.icann.org/resources/pages/faqs-84-2012-02-25-en#9

3 https://www.arvancloud.com/blog/%D8%A2%D8%B3%DB%8C%D8%A8-%D9%BE%D8%B0%DB%8C%D8%B1%DB%8C-%D8%A8%D8%B1%D9%86%D8%A7%D9%85%D9%87-%D8%AA%D8%AD%D8%AA-%D9%88%D8%A8-owasp/ و https://edu.thregence.ir/owasp-top-10/ و https://owasp.org/Top10 /

- اجازه مشاهده یا ویرایش حساب شخص دیگری با ارائه شناسه منحصر به فرد آن (اشاره های مستقیم ناامن شیء)
- دسترسی به API با کنترل‌های دسترسی از دست رفته برای POST، PUT و DELETE.
- بالا بردن امتیاز. به عنوان یک کاربر بدون وارد شدن به سیستم عمل کنید یا در هنگام ورود به عنوان کاربر به عنوان یک مدیر عمل کنید.
- دستکاری ابرداده، مانند بازپخش یا دستکاری رمز کنترل دسترسی JWT (JSON Web Token)، یا کوکی یا فیلد مخفی که برای افزایش امتیازات یا سوء استفاده از باطل کردن JWT دستکاری شده است.
- پیکربندی نادرست CORS اجازه دسترسی به API را از مبداهای غیرمجاز/غیر قابل اعتماد می دهد.
- مرور اجباری به صفحات تایید شده به عنوان کاربر احراز هویت نشده یا صفحات دارای امتیاز به عنوان یک کاربر استاندارد.

برای جلوگیری از آن می‌توان به صورت زیر عمل کرد:

- به جز برای منابع عمومی، به طور پیش فرض رد کنید.
- مکانیزم‌های کنترل دسترسی را یک‌بار پیاده‌سازی کنید و از آن‌ها در سراسر برنامه استفاده مجدد کنید، از جمله به حداقل رساندن استفاده از اشتراک‌گذاری منابع متقاطع (CORS).
- کنترل‌های دسترسی مدل باید مالکیت رکورد را اعمال کنند نه اینکه بپذیرند کاربر می‌تواند هر رکوردی را ایجاد، بخواند، به‌روزرسانی یا حذف کند.
- الزامات محدود تجاری برنامه منحصر به فرد باید توسط مدل های دامنه اعمال شود.
- فهرست دایرکتوری وب سرور را غیرفعال کنید و مطمئن شوید که فراداده فایل (به عنوان مثال git.) و فایل های پشتیبان در ریشه های وب وجود ندارد.
- خرابی‌های کنترل دسترسی را ثبت کنید، در صورت لزوم به مدیران هشدار دهید (مثلاً خرابی‌های مکرر).
- API و دسترسی کنترل‌کننده را محدود کنید تا آسیب‌های ناشی از ابزار حمله خودکار را به حداقل برسانید.
- پس از خروج از سیستم، شناسه های جلسه Stateful باید در سرور باطل شوند. توکن‌های JWT بدون وضعیت باید عمر کوتاهی داشته باشند تا فرصت برای مهاجم به حداقل برسد. برای JWT هایی که عمر طولانی تری دارند، بسیار توصیه می شود از استانداردهای OAuth برای لغو دسترسی پیروی کنند.

2. آسیب پذیری Cryptographic Failure

یک آسیب پذیری رایج است که وقتی اطلاعات حساس به صورت ایمن ذخیره نمی‌شود به وجود می آید.
اعتبار کاربری، اطلاعات نمایه، جزئیات سلامتی، اطلاعات کارت اعتباری و غیره تحت اطلاعات حساس در یک وب سایت قرار می‌گیرند.
این داده‌ها در پایگاه داده برنامه ذخیره می‌شوند. هنگامی که این داده‌ها با استفاده از رمزنگاری یا هش کردن نامناسب ذخیره می‌شوند، آسیب پذیر خواهد بود و به مهاجمان اجازه حمله خواهد داد.

(Hashing تبدیل کاراکترهای رشته به رشته های با طول ثابت یا یک کلید است. برای رمزگشایی رشته، الگوریتم مورد استفاده برای فرم کلید باید در دسترس باشد.)
با استفاده از این آسیب پذیری، یک مهاجم می تواند، داده های ضعیف محافظت شده را برای سرقت هویت، تقلب کارت اعتباری و سایر جرایم تغییر دهد یا سرقت نماید.
برای راه حل می‌توان به موارد زیر اشاره کرد:

- اطمینان از الگوریتم های استاندارد مناسب قوی. الگوریتم رمزنگاری خود را ایجاد نکنید. فقط از الگوریتم های عمومی تایید شده مانند AES، رمزنگاری کلید عمومی RSA و SHA-۲۵۶ و غیره استفاده کنید.
- اطمینان از این که پشتیبان گیری خارج از رمزگذاری هستند، اما کلید ها به طور جداگانه مدیریت و پشتیبان گیری می شوند.

3. آسیب پذیری Injection

در این حالت مهاجم اطلاعات نامتعبر به سرور ارسال می‌کند. بعنوان مثلا SQL injection یکی از این نوع حملات می‌باشد.

مثلا تزریق SQL یا همان SQL Injection یکی از رایج ترین آسیب پذیری‌های مربوط به تزریق کد است که در برنامه های مختلف از جمله برنامه های تحت وب که با دیتابیس SQL کار می‌کنند، یافت می‌شود. اشکالات تزریق SQL می تواند ناشی از استفاده از داده های نامعتبر توسط یک برنامه هنگام ایجاد یک فراخوانی آسیب پذیر SQL باشد.

یکی از راه‌های جلوگیری از این حملات source code review می‌باشد. همچنین در CI/CD می‌توان از DAST و SAST نیز بهره برد.

4. آسیب پذیری Insecure Design

یک طراحی ایمن همچنان می‌تواند دارای نقص‌های پیاده‌سازی باشد که منجر به آسیب‌پذیری‌هایی می‌شود که ممکن است مورد سوء استفاده قرار گیرند. یک طراحی ناامن را نمی توان با یک پیاده سازی کامل برطرف کرد، زیرا طبق تعریف، کنترل های امنیتی مورد نیاز هرگز برای دفاع در برابر حملات خاص ایجاد نشده است. یکی از عواملی که به طراحی ناامن کمک می کند، فقدان نمایه ریسک تجاری ذاتی در نرم افزار یا سیستم در حال توسعه است و در نتیجه عدم تعیین سطح طراحی امنیتی مورد نیاز است.

برای جلوگیری از آن می‌توان موارد زیر را انجام داد.

- کتابخانه ای از الگوهای طراحی ایمن آماده برای استفاده ایجاد و استفاده کنید
- از مدل‌سازی تهدید برای احراز هویت حیاتی، کنترل دسترسی، منطق تجاری و جریان‌های کلیدی استفاده کنید
- زبان امنیتی و کنترل‌ها را در داستان‌های کاربر ادغام کنید
- بررسی‌های معقولیت را در هر لایه از برنامه خود ادغام کنید
- تست‌های واحد و ادغام را بنویسید تا تأیید کنید که تمام جریان‌های بحرانی در برابر مدل تهدید مقاوم هستند. موارد استفاده و موارد سوء استفاده را برای هر لایه از برنامه خود کامپایل کنید.
- جداسازی لایه‌های لایه در سیستم و لایه‌های شبکه بسته به نیازهای نوردهی و حفاظتی
- مصرف منابع توسط کاربر یا سرویس را محدود کنید

5. آسیب پذیری Security Misconfiguration

یکی از مسایل بسیار رایج در سامانه‌های آنلاین استفاده از تنظیمات ناامن و به‌ویژه تنظیمات پیش‌فرض است. در برخی موقعیت‌ها این تنظیمات بسیار خطرناک است و می‌توانند منجر به دسترسی مهاجم به سیستم شوند. تنظیمات ناامن محدود به بخش خاصی از سامانه نیست و می‌توانند در تمامی قسمت‌های برنامه رخ دهند. برای کشف این نوع آسیب‌پذیری‌ها می‌توان از اسکنرهای خودکار استفاده کرد. مدیر سامانه باید از نصب هرگونه سرویس زاید اجتناب و به‌طور مرتب سرویس‌های لازم را به‌روزرسانی کند، هم‌چنین با تنظیمات امنیتی آن‌ها آشنا باشد.

6. آسیب پذیری Vulnerable and Outdated Components

وقتی یک سرویس از مولفه‌های آسیب پذیر استفاده کند خود نیز آسیب پذیر خواهد بود. در نتیجه باید از مولفه‌هایی که در سیستم خود استفاده کرده ایم آگاه باشیم و در صورت لزوم آن‌ها را به روز رسانی نماییم. استفاده از اسکنرهای خودکار به‌روز شده نیز روش مناسبی برای کشف این آسیب‌پذیری به‌شمار می‌آید.

7. آسیب پذیری Identification and Authentication Failures

اگر قسمت‌هایی از برنامه که مسوولیت تصدیق اصالت و مدیریت نشست کاربران را به‌عهده دارند درست طراحی و پیاده‌سازی نشده باشد، این آسیب‌پذیری محتمل خواهد بود. این آسیب‌پذیری می‌تواند به حمله‌کننده اجازه‌ی دسترسی به گذرواژه، کلیدهای حساس، اطلاعات session و... را بدهد و در نتیجه‌ی آن مهاجم می‌تواند خود را به‌جای کاربر مجاز یا حتی مدیر سیستم معرفی کند. با استفاده از ابزارهای خودکار تست آسیب‌پذیری نیز به‌راحتی می‌توان از برخی اقسام این آسیب‌پذیری سواستفاده کرد. به‌دست آوردن یک جفت نام کاربری و گذرواژه‌ی صحیح با دسترسی پایین توسط مهاجم نیز می‌تواند بسیار خطرناک باشد. یکی از راه‌های جلوگیری از این آسیب‌پذیری، مراقبت از نام کاربری و عدم استفاده از گذرواژه‌ی ضعیف و پیش‌فرض، هم‌چنین پیاده‌سازی فرآیند captcha است. امن‌سازی فرآیند فراموشی رمز عبور، طراحی و پیاده‌سازی فرآیند تصدیق اصالت چند عامله، تغییرات دوره‌ای گذرواژه و محافظت از شماره‌ی نشست از دیگر راهکارهای جلوگیری از این آسیب‌پذیری هستند.

8. آسیب پذیری Software and Data integrity Failures

نقص نرم افزار و یکپارچگی داده‌ها مربوط به کد و زیرساختی است که در برابر نقض یکپارچگی محافظت نمی‌کند. یک نمونه از این موارد زمانی است که یک برنامه کاربردی به پلاگین‌ها، کتابخانه‌ها یا ماژول‌هایی از منابع نامعتبر، مخازن و شبکه‌های تحویل محتوا (CDN) متکی است. یک خط لوله CI/CD ناامن می‌تواند احتمال دسترسی غیرمجاز، کد مخرب یا به خطر افتادن سیستم را ایجاد کند. در نهایت، اکنون بسیاری از برنامه‌ها دارای قابلیت به‌روزرسانی خودکار هستند، که در آن به‌روزرسانی‌ها بدون تایید صحت کافی دانلود می‌شوند و روی برنامه مورد اعتماد قبلی اعمال می‌شوند. مهاجمان می‌توانند به‌طور بالقوه به‌روزرسانی‌های خود را برای توزیع و اجرا در همه نصب‌ها آپلود کنند. مثال دیگر جایی است که اشیا یا داده‌ها در ساختاری که مهاجم می‌تواند ببیند و تغییر دهد، کدگذاری یا سریال‌سازی می‌شوند، در برابر سریال‌زدایی ناامن آسیب‌پذیر است.

- از امضای دیجیتال یا مکانیسم‌های مشابه برای تأیید اینکه نرم‌افزار یا داده‌ها از منبع مورد انتظار هستند و تغییر نکرده‌اند، استفاده کنید.
- اطمینان حاصل کنید که کتابخانه ها و وابستگی ها، مانند npm یا Maven، مخازن قابل اعتماد را مصرف می کنند. اگر نمایه ریسک بالاتری دارید، میزبانی یک مخزن داخلی شناخته شده خوب را که بررسی شده است در نظر بگیرید.
- اطمینان حاصل کنید که یک ابزار امنیتی زنجیره تامین نرم‌افزار، مانند بررسی وابستگی OWASP یا OWASP CycloneDX، برای تأیید عدم وجود آسیب‌پذیری‌های شناخته شده در مؤلفه‌ها استفاده می‌شود.
- اطمینان حاصل کنید که یک فرآیند بررسی برای تغییرات کد و پیکربندی وجود دارد تا احتمال وارد شدن کد یا پیکربندی مخرب به خط لوله نرم افزار شما به حداقل برسد.
- اطمینان حاصل کنید که خط لوله CI/CD شما دارای تفکیک، پیکربندی و کنترل دسترسی مناسب است تا از یکپارچگی کد در فرآیندهای ساخت و استقرار اطمینان حاصل شود.

- اطمینان حاصل کنید که داده‌های سریالی بدون امضا یا رمزگذاری نشده به مشتریان غیرقابل اعتماد بدون بررسی یکپارچگی یا امضای دیجیتال برای تشخیص دستکاری یا پخش مجدد داده‌های سریالی ارسال نمی‌شوند.

9. آسیب پذیری Security Logging and Monitoring Failures

لاگینگ و مانیتورینگ فعالیت‌هایی هستند که باید به طور مکرر در وب سایت انجام شوند تا از امنیت آن اطمینان حاصل شود. عدم لاگینگ و نظارت کافی بر یک سایت (مانند ورود و خروج کاربران)، آن را در برابر فعالیت‌های خطرناک‌تر آسیب پذیر می‌کند.

10. آسیب پذیری Server-Side Request Forgery

نقص های SSRF زمانی رخ می دهد که یک برنامه وب در حال واکشی یک منبع راه دور بدون اعتبارسنجی URL ارائه شده توسط کاربر باشد. این اجازه می دهد تا مهاجم برنامه را وادار کند تا یک درخواست دستکاری شده را به مقصدی غیرمنتظره ارسال کند، حتی زمانی که توسط فایروال، VPN یا نوع دیگری از لیست کنترل دسترسی به شبکه (ACL) محافظت می شود. از آنجایی که برنامه های کاربردی وب مدرن ویژگی های مناسبی را در اختیار کاربران نهایی قرار می دهند، واکشی URL به یک سناریوی رایج تبدیل می شود. در نتیجه، بروز SSRF در حال افزایش است. همچنین، شدت SSRF به دلیل سرویس های ابری و پیچیدگی معماری ها بیشتر می شود.

- تمام داده های ورودی ارائه شده توسط مشتری را پاکسازی و اعتبارسنجی کنید
- طرح URL، پورت، و مقصد را با لیست مجاز مثبت اجرا کنید
- پاسخ های خام را برای مشتریان ارسال نکنید
- تغییر مسیرهای HTTP را غیرفعال کنید