Izveštaj penetracionog testiranja

Uvod

Na samom početku, u pripremnoj fazi testiranja, za analizu mreže, portova i servisa korišćen je alat *Namp*. Početna faza služi za prikupljanje što više informacija o potencijalnim metama. Nakon toga aplikacija je testirana upotrebom *Nikto* alata. *Nikto* obavlja skeniranje web servera i pronalazi preko 6700 potencijalno opasnih fajlova/programa, takođe proverava postojanje zastarelih verzija biblioteka i generalno problema vezanih za verzije biblioteka i zavisnosti. *Nikto* vrši i proveru konfiguracionih fajlova servera i omogućava brzo pronalaženje brojnih ranjivosti koje mogu postojati u sistemu. U nastavku su navedeni rezultati dobijeni upotrebom ova dva alata.

Nmap

- nmap -p 3000 -T4 -A -v localhost [frontend aplikacija]

```
PORT     STATE SERVICE  VERSION
3000/tcp open  ssl/http Node.js Express framework
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: C92B85A5B907C70211F4EC25E29A8C4A
|_http-title: Home Security System
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=adagrad interm/organizationName=FTN/stateOrProvinceName=SERBIA/countryName=RS
| Subject Alternative Name: DNS:localhost
| Issuer: commonName=ADAGRAD ROOT/organizationName=FTN/stateOrProvinceName=SERBIA/countryName=RS
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-06-22T10:32:11
| Not valid after:  2023-06-22T10:32:11
| MD5:   ff55 9fd0 dd33 e735 289f e02d cbec 7b9c
|_SHA-1: 3262 ef1d aa05 4285 00dd 2825 ebab c0e1 f5b0 f230
|_ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 1909
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
```

- nmap -p 8080 -T4 -A -v localhost [admin aplikacija]

```
PORT     STATE SERVICE       VERSION
8080/tcp open  ssl/http-proxy
| fingerprint-strings:
|   HTTPOptions:
|     HTTP/1.1 401
|     Vary: Origin
|     Vary: Access-Control-Request-Method
|     Vary: Access-Control-Request-Headers
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Cache-Control: no-cache, no-store, max-age=0, must-revalidate
|     Pragma: no-cache
|     Expires: 0
|     Strict-Transport-Security: max-age=31536000 ; includeSubDomains
|     X-Frame-Options: DENY
|     Content-Security-Policy: script-src 'self'
|     Content-Length: 0
|     Date: Wed, 29 Jun 2022 17:10:27 GMT
|     Connection: close
|   RPCCheck, RTSPRequest:
|     HTTP/1.1 400
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 435
|     Date: Wed, 29 Jun 2022 17:10:27 GMT
|     Connection: close
|     <!doctype html><html lang="en"><head><title>HTTP Status 400
|     Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-
size:12px;} a {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status 400
|_    Request</h1></body></html>
| http-auth:
| HTTP/1.1 401 \x0D
|_  Server returned status 401 but no WWW-Authenticate header.
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title.
| ssl-cert: Subject: commonName=ADAGRAD ROOT/organizationName=FTN/stateOrProvinceName=SERBIA/countryName=RS
| Issuer: commonName=ADAGRAD ROOT/organizationName=FTN/stateOrProvinceName=SERBIA/countryName=RS
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-04-09T12:57:52
| Not valid after:  2032-04-09T12:57:52
| MD5:   17c6 330e 7afe ca67 1fb0 114d 1fa7 2c71
|_SHA-1: 3eb0 c1f4 3c01 fba7 2ef0 b4f2 eba5 8e65 887c dbf3
|_ssl-date: TLS randomness does not represent time
```

- nmap -p 8081 -T4 -A -v localhost [myhouse aplikacija]

```
PORT     STATE SERVICE            VERSION
8081/tcp open  ssl/blackice-icecap?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 401
|     Content-Length: 0
|     Date: Wed, 29 Jun 2022 17:17:12 GMT
|     Connection: close
|   HTTPOptions:
|     HTTP/1.1 401
|     Vary: Origin
|     Vary: Access-Control-Request-Method
|     Vary: Access-Control-Request-Headers
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Cache-Control: no-cache, no-store, max-age=0, must-revalidate
|     Pragma: no-cache
|     Expires: 0
|     Strict-Transport-Security: max-age=31536000 ; includeSubDomains
|     X-Frame-Options: DENY
|     Content-Security-Policy: script-src 'self'
|     Content-Length: 0
|     Date: Wed, 29 Jun 2022 17:17:12 GMT
|     Connection: close
|   RPCCheck, RTSPRequest:
|     HTTP/1.1 400
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 435
|     Date: Wed, 29 Jun 2022 17:17:12 GMT
|     Connection: close
|     <!doctype html><html lang="en"><head><title>HTTP Status 400
|     Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-
size:12px;} a {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>HTTP Status 400
|_    Request</h1></body></html>
| ssl-cert: Subject: commonName=ADAGRAD ROOT/organizationName=FTN/stateOrProvinceName=SERBIA/countryName=RS
| Subject Alternative Name: DNS:localhost
| Issuer: commonName=ADAGRAD ROOT/organizationName=FTN/stateOrProvinceName=SERBIA/countryName=RS
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-06-22T10:29:03
| Not valid after:  2023-06-22T10:29:03
| MD5:   19e5 8dfe f5ec 1481 04da dc1e 8258 80b6
|_SHA-1: c34c 6b21 ef26 9453 6d84 e9f4 6707 101f 5bf8 a812
|_ssl-date: TLS randomness does not represent time
```

Nikto

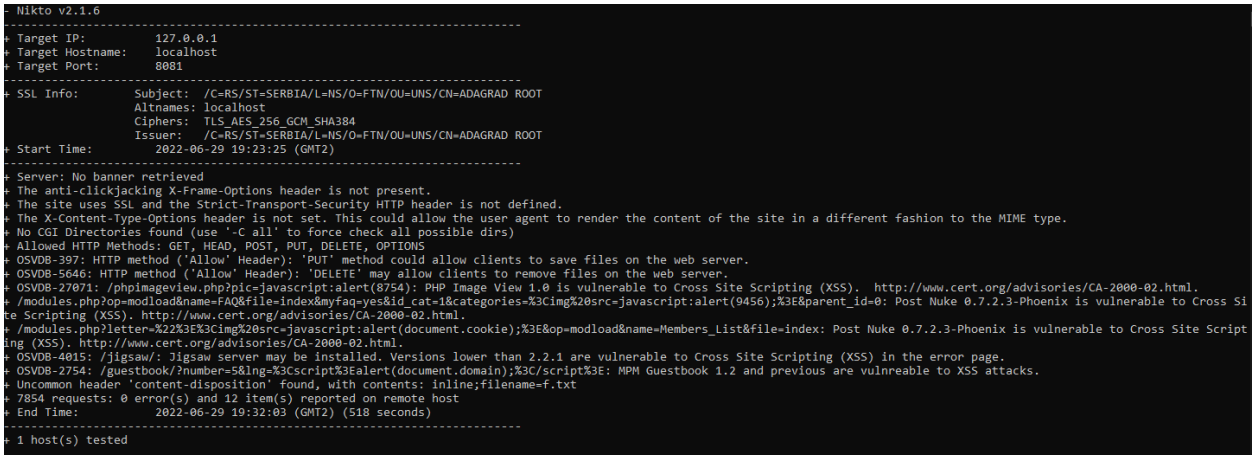
- perl nikto.pl -h localhost -p 3000 [frontend aplikacija]

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        3000
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=RS/ST=SERBIA/L=NS/O=FTN/OU=UNS/CN=adagrad interm
                   Altnames: localhost
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=RS/ST=SERBIA/L=NS/O=FTN/OU=UNS/CN=ADAGRAD ROOT
+ Start Time:         2022-06-29 18:44:13 (GMT2)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Retrieved x-powered-by header: Express
+ Retrieved access-control-allow-origin header: *
+ The anti-clickjacking X-Frame-Options header is not present.
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
+ 7857 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2022-06-29 18:47:12 (GMT2) (179 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- perl nikto.pl -h localhost -p 8080 [admin aplikacija]

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        8080
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=RS/ST=SERBIA/L=NS/O=FTN/OU=UNS/CN=ADAGRAD ROOT
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=RS/ST=SERBIA/L=NS/O=FTN/OU=UNS/CN=ADAGRAD ROOT
+ Start Time:         2022-06-29 18:51:46 (GMT2)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Hostname 'localhost' does not match certificate's names: ADAGRAD
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ Uncommon header 'content-disposition' found, with contents: inline;filename=f.txt
+ 7855 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2022-06-29 19:02:14 (GMT2) (628 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

- perl nikto.pl -h localhost -p 8081 [myhouse aplikacija]



Otkrivene potrencijalne ranjivosti otklonjene su konfiguracijom HTTP-s, striktnom validacijom svih mogućih ulaznih tačaka u sistem, upotrebom autentifikacije i autorizacije, RBAC-a sa permisijama, konfigurisanjem XSS filtera, upotrebom NoSQL baze za skladištenje podataka i kontrolisanog pristupa resursima u bazi, ažuriranjem problematičnih verzija biblioteka i zavisnosti, digitalnim potpisivanjem poruka koje aplikacije i uređaju razmenjuju…