

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, h4 {color:white;background-color:#525076;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height:1px;background-color:#525076;border:none;}</style></head><body><h1>HTTP Status 400
|_     Request</h1></body></html>
|_   http-auth:
|_     HTTP/1.1 401 \x00
|_     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: 1765 330a 7afe c407 1f00 1140 1fa7 1c71
|_   SHA-1: 3e00 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, h4 {color:white;background-color:#525076;} h1 {font-size:12px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height:1px;background-color:#525076;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: 1865 8dfe f5ec 1481 06a4 c41e 8258 80b6
|_   |_   _SHA-1: c34c 6021 ef26 9453 6d84 e9f4 6707 181f 5bfb a612
|_   |_   _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-307: 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]`

```

+ Nikto v2.1.6
+-----+
+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    8081
+-----+
+ SSL Info:      Subject: /C=RS/ST=SERBIA/L=NS/O=FTN/OU=UNS/CN=ADAGRAD ROOT
+                  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 19:23:25 (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 dings)
+ 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.
+ OSVDB-27071: /phpimageview.php?pic=javascript:alert(8754): PHP Image View 1.0 is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Si
+ e Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Script
+ ing (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-4015: /jigsaw/: Jigsaw server may be installed. Versions lower than 2.2.1 are vulnerable to Cross Site Scripting (XSS) in the error page.
+ OSVDB-2754: /guestbook/?number=5&lng=%3Cscript%3Ealert(document.domain);%3C/script%3E: MPM Guestbook 1.2 and previous are vulnreable to XSS attacks.
+ Uncommon header 'content-disposition' found, with contents: inline;filename=f.txt
+ 7854 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:      2022-06-29 19:32:03 (GMT2) (519 seconds)
+-----+
+ 1 host(s) tested

```

Otkrivene potencijalne ranjivosti otklonjene su konfiguracijom HTTPS-a, 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...