Penetration testing

1. Nmap

Iskorišten je nmap za skeniranje bek i front dela aplikacije. Upotrebljene su skripte za otkrivanje ranjivosti https://github.com/vulnersCom/nmap-vulners.

Komanda koja je korištena za bekend: nmap -sV --script vuln localhost -p 4430

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-19 00:08 Central Europe Daylight Time
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: www.sumatools.com

PORT     STATE SERVICE        VERSION
4430/tcp open  ssl/rsqlserver?
| fingerprint-strings:
|   GetRequest, 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: 0
|     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-Length: 0
|     Date: Sun, 18 Jun 2023 22:09:42 GMT
|     Connection: close
|   RPCCheck, RTSPRequest:
|     HTTP/1.1 400
|     Content-Type: text/html;charset=utf-8
|     Content-Language: en
|     Content-Length: 435
|     Date: Sun, 18 Jun 2023 22:09:42 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-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
```

Ranjivost koja je pronađena je mala dužina Diffie-Hellman grupe. Trenutna dužina je 1024 bita. Preporuka je da se poveća na 2048. Ova ranjivost nije alarmantna jer samo neki veoma moćni napadači poput vlade bi mogli ovo da iskorite.

Komanda koja je korištena za front: nmap -sV --script vuln localhost -p 4444

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-19 00:12 Central Europe Daylight Time
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: www.sumatools.com

PORT     STATE SERVICE  VERSION
4444/tcp open  ssl/http Node.js Express framework
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  BID:49303  CVE:CVE-2011-3192
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|    Disclosure date: 2011-08-19
|    References:
|      https://www.tenable.com/plugins/nessus/55976
|      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|      https://www.securityfocus.com/bid/49303
|_      https://seclists.org/fulldisclosure/2011/Aug/175
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

Jedina ranjivost koja je pronađena je otvorenost aplikacije na DoS napad što je i za očekivati.

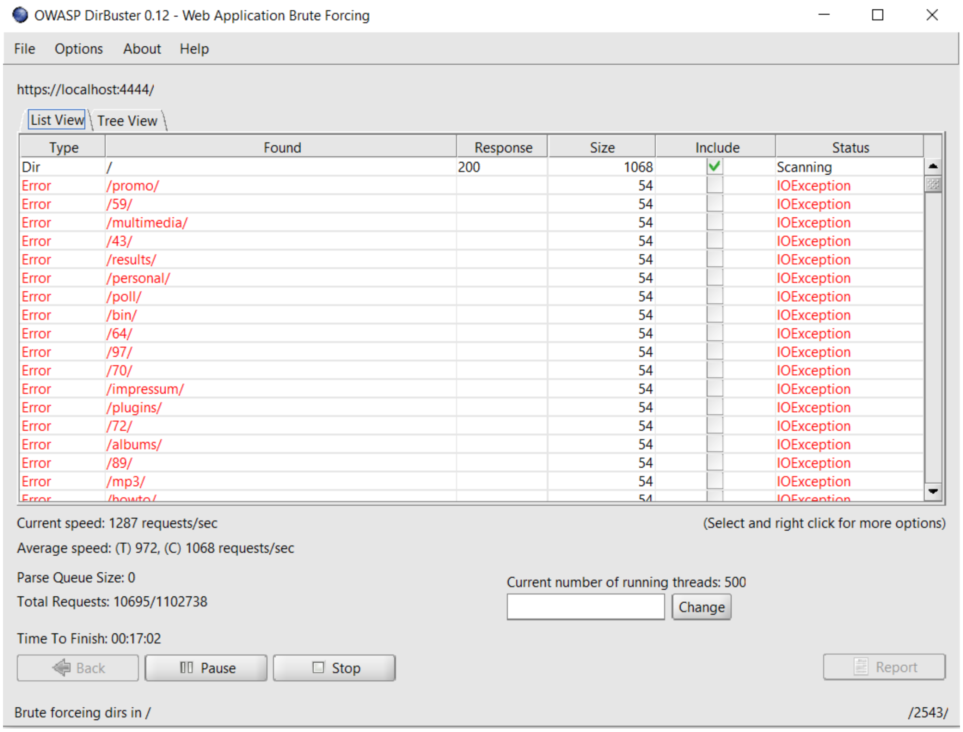
2. Nikto

Nikto je iskorišten samo za skeniranje beka I to komandom:
perl nikto.pl -h localhost -p 4430 -ssl -o reports/report.html

Njegov izveštaj je priložen ali nije uspeo da nađe nikakve ranjivosti (najverovatnije jer spring blokira skoro sve pozive na api I vraća 401 status kod).

3. DirBuster

DirBuster je iskorišten za formiranje stable direktorijuma na frontend delu aplikacije. Korištena je *directory-list-2.3-medium.txt* wordlista. Izveštaj generisan uz pomoć ovog alata je takođe priložen ali nije našao nikakave značajne fajlove osim *index.html*-a.



https://localhost:4444/

Type	Found	Response	Size	Include	Status
Dir	/	200	1068	☑	Scanning
Error	/promo/		54	□	IOException
Error	/59/		54	□	IOException
Error	/multimedia/		54	□	IOException
Error	/43/		54	□	IOException
Error	/results/		54	□	IOException
Error	/personal/		54	□	IOException
Error	/poll/		54	□	IOException
Error	/bin/		54	□	IOException
Error	/64/		54	□	IOException
Error	/97/		54	□	IOException
Error	/70/		54	□	IOException
Error	/impressum/		54	□	IOException
Error	/plugins/		54	□	IOException
Error	/72/		54	□	IOException
Error	/albums/		54	□	IOException
Error	/89/		54	□	IOException
Error	/mp3/		54	□	IOException
Error	/howto/		54	□	IOException

Current speed: 1287 requests/sec

(Select and right click for more options)

Average speed: (T) 972, (C) 1068 requests/sec

Parse Queue Size: 0

Total Requests: 10695/1102738

Current number of running threads: 500

Time To Finish: 00:17:02

Brute forceing dirs in /

/2543/

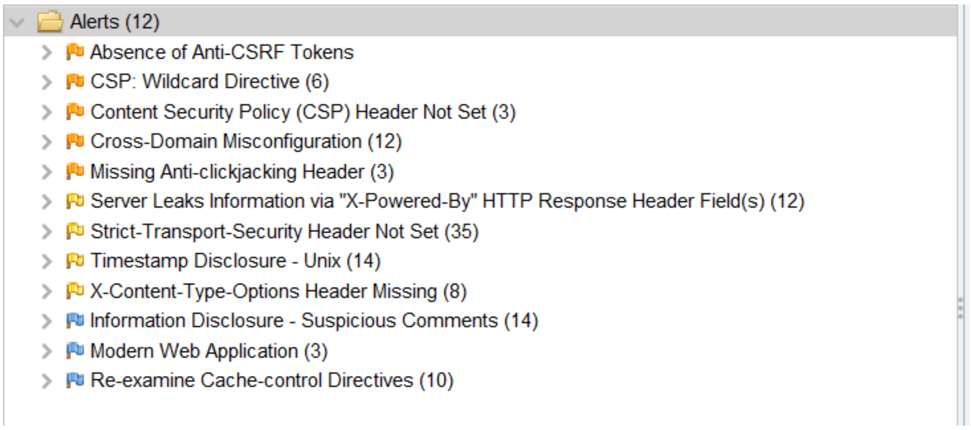
DirBuster u akciji (busting 😉)

4. OWASP ZAP

Automatsko skeniranje ovog alata nije bilo moguće iskoristiti na bekend delu aplikacije zbog spring security-a koji vraća 401 status kod. Zbog ovoga je korišten manual explore.

Na frontend delu je bilo moguće odraditi automatko skeniranje ranjivosti.

Ni na bekend ni na frontend delu nije pronađena nijedna ranjivost koja je ima *HIGH* rizik. Izveštaji za oba skeniranja su priložena.

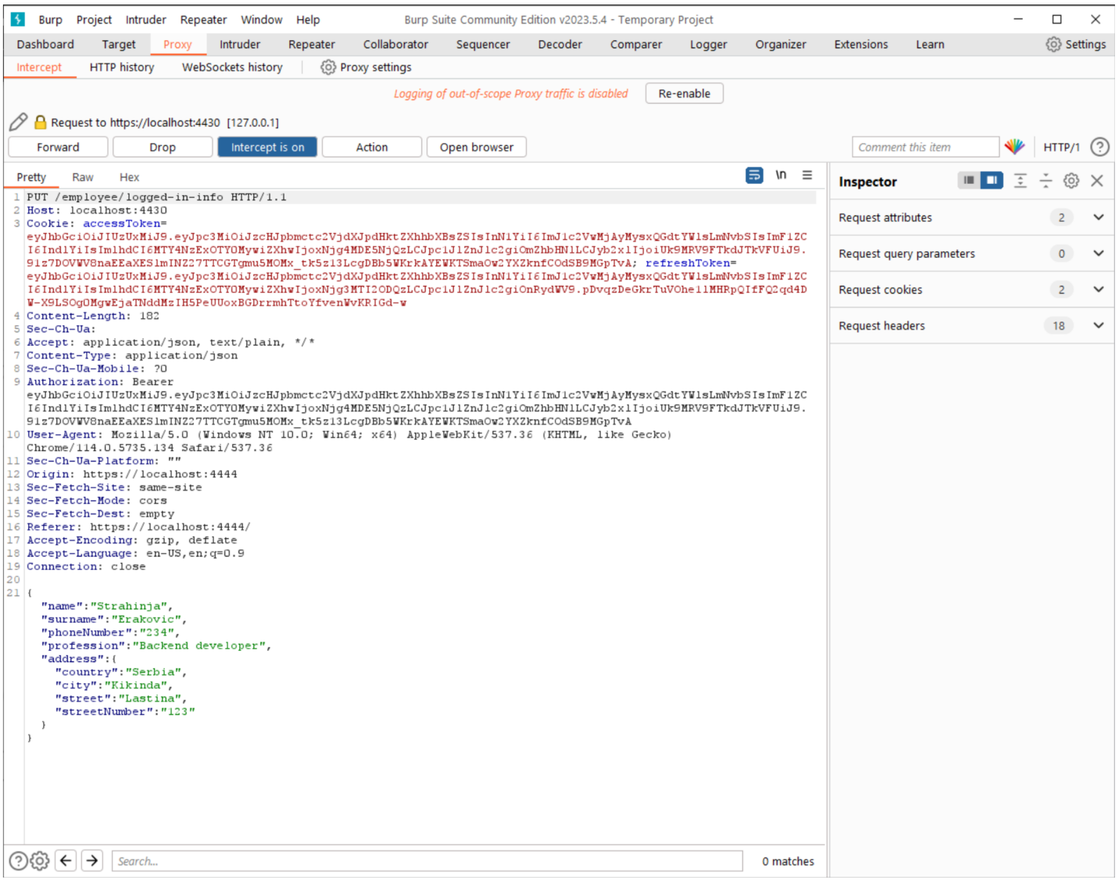


Alerts (12)
- Absence of Anti-CSRF Tokens
- CSP: Wildcard Directive (6)
- Content Security Policy (CSP) Header Not Set (3)
- Cross-Domain Misconfiguration (12)
- Missing Anti-clickjacking Header (3)
- Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (12)
- Strict-Transport-Security Header Not Set (35)
- Timestamp Disclosure - Unix (14)
- X-Content-Type-Options Header Missing (8)
- Information Disclosure - Suspicious Comments (14)
- Modern Web Application (3)
- Re-examine Cache-control Directives (10)

Ranjivosti pronađene na frontend delu

5. BURP SUITE

Ovaj alat se koriti za presretanje API poziva koje frontend vrši i moguća je izmena *payload*-a. Ovaj alat bi mogao da se iskoriti za *SQL injection* ali pošto je u projektu uvek korišten *HQL* ili *Nativ SQL* uz parametre sa *@Param* notacijom *SQLI* nije moguć.


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2023.5.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Request to https://localhost:4430 [127.0.0.1]
Forward
Drop
Intercept is on
Action
Open browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request cookies 2
Request headers 18
Search...
0 matches

```
PUT /employee/logged-in-info HTTP/1.1
Host: localhost:4430
Cookie: accessToken=
eyJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJzcHJpbmctc2VjdXJpdHktZXhhbXBsZSIsInN1YiI6ImJlc2VwMjAyMysxQGdtYWlsLmNvbSIsImF1ZC
I6IndlYiIsImlhdCI6MTY4NzExOTYOMywiZXhwIjoxNjg4MDE5NjQzLCJpc1J1ZnJlc2giOmZhbHN1LCJyb2xlIjoiUk9MRV9FTkdJTkVFUiJ9.
91z7DOVWV8naEEaXES1mINZ27TTCGTgmu5MOMx_tk5z13LcgDBb5WKrkAYEWKTSmaOw2YXZknfCOdSB9MGpTvA; refreshToken=
eyJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJzcHJpbmctc2VjdXJpdHktZXhhbXBsZSIsInN1YiI6ImJlc2VwMjAyMysxQGdtYWlsLmNvbSIsImF1ZC
I6IndlYiIsImlhdCI6MTY4NzExOTYOMywiZXhwIjoxNjg3MTI2ODQzLCJpc1J1ZnJlc2giOnRydWV9.pDvqzDeGkrTuVOhe11MHRpQIfFQ2qd4D
W-X9LSOgOMgwEjaTNddMzIH5PeUUoxBGDrrmhTtoYfvenWvKRIGd-w
Content-Length: 182
Sec-Ch-Ua:
Accept: application/json, text/plain, */*
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJzcHJpbmctc2VjdXJpdHktZXhhbXBsZSIsInN1YiI6ImJlc2VwMjAyMysxQGdtYWlsLmNvbSIsImF1ZC
I6IndlYiIsImlhdCI6MTY4NzExOTYOMywiZXhwIjoxNjg4MDE5NjQzLCJpc1J1ZnJlc2giOmZhbHN1LCJyb2xlIjoiUk9MRV9FTkdJTkVFUiJ9.
91z7DOVWV8naEEaXES1mINZ27TTCGTgmu5MOMx_tk5z13LcgDBb5WKrkAYEWKTSmaOw2YXZknfCOdSB9MGpTvA
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.5735.134 Safari/537.36
Sec-Ch-Ua-Platform: ""
Origin: https://localhost:4444
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://localhost:4444/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "name":"Strahinja",
  "surname":"Erakovic",
  "phoneNumber":"234",
  "profession":"Backend developer",
  "address":{
    "country":"Serbia",
    "city":"Kikinda",
    "street":"Lastina",
    "streetNumber":"123"
  }
}
```

Presretanje zahteva uz pomoć *burp suit*-a