Penetration testing izvještaj – Tim 9

SEP 2023

Tim

- Miloš Popović, R2-31/2022
- Veljko Tošić, R2-4/2022
- Ivan Mršulja, R2-30/2022
- Marko Bjelica, R2-10/2022

Korišćeni alati

Za realizaciju dodatnog zadatka (*penetration testing*) odlučili smo se na korišćenje 2 alata:

1. *Nmap*
2. *Nikto*

Kao bonus, „konsultovali“ smo i *Github Dependabot*-a kako bi dobili obavještenja o eventualnim ranjivostima u zavisnostima koje naš projekat koristi.

Nmap

Prilikom svakog *penetration testing*-a prvo je potrebno izvršiti skeniranje mreže, u cilju detekcije svih dostupnih servisa, sakupljanja informacija o njima i planiranju sledećeg koraka. *Payment Service Provider*(PSP u nastavku) servis je pokrenut lokalno, sa svim svojim neophodnim zavisnostima i pokrenuto je skeniranje lokalne mreže.

```
ivanmrsulja@pop-os:~$ sudo nmap -PA -PU -O -sV -sS 127.0.0.1/32
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-22 12:16 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00013s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE     VERSION
631/tcp  open  ipp         CUPS 2.4
5432/tcp open  postgresql  PostgreSQL DB 9.6.0 or later
8089/tcp open  ssl/unknown
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

Prvo je bitno napomenuti da je opsjeg skeniranih adresa smanjen na samo jednu kako ne bi gubili vrijeme na filtriranje gomile ispisa koji ne znači ništa, u praksi bi se pokrenulo na nekom realnijem opsjegu npr. 127.0.0.0/24.

Iz ispisa alata, možemo primijetiti dobro poznate servise kao što su *PostgreSQL* baza i *IPP*, kao i neki nepoznati *SSL* servis. Naravno, u pitanju je *backend* naše aplikacije, ali kako je sertifikat ručno generisan, alat ne može sa sigurnošću znati o kome se radi. Takođe, možemo vidjeti i to, da se alat pokušao obratiti i ka dva nepoznata servisa na mreži za koje je izgenerisao sledeće *fingerprint*-e.

```
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5432-TCP:V=7.80%I=7%D=1/22%Time=63CD1B1B%P=x86_64-pc-linux-gnu%r(SM
SF:BProgNeg,8C,"E\0\0\0\x8bSFATAL\0VFATAL\0C0A000\0Munsupported\x20fronten
SF:d\x20protocol\x2065363\.19778:\x20server\x20supports\x203\.0\x20to\x203
SF:\.0\0Fpostmaster\.c\0L2132\0RProcessStartupPacket\0\0");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8089-TCP:V=7.80%T=SSL%I=7%D=1/22%Time=63CD1B2B%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,186,"HTTP/1\.1\x20401\x20\r\nVary:\x20Origin\r\nVary:\x2
SF:0Access-Control-Request-Method\r\nVary:\x20Access-Control-Request-Heade
SF:rs\r\nContent-Type:\x20application/json\r\nContent-Length:\x20175\r\nDa
SF:te:\x20Sun,\x2022\x20Jan\x202023\x2011:16:59\x20GMT\r\nConnection:\x20c
SF:lose\r\n\r\n{\"path\":\"/error\",\"message\":\"Full\x20authentication\x
SF:20is\x20required\x20to\x20access\x20this\x20resource\",\"timestamp\":\"
SF:2023-01-22T12:16:59\.721063\",\"statusCode\":401,\"statusReason\":\"Una
SF:uthorized\"}\r\n")%r(HTTPOptions,2A4,"HTTP/1\.1\x20401\x20\r\nVary:\x20
SF:Origin\r\nVary:\x20Access-Control-Request-Method\r\nVary:\x20Access-Con
SF:trol-Request-Headers\r\nX-Content-Type-Options:\x20nosniff\r\nX-XSS-Pro
SF:tection:\x201;\x20mode=block\r\nCache-Control:\x20no-cache,\x20no-store
SF:,\x20max-age=0,\x20must-revalidate\r\nPragma:\x20no-cache\r\nExpires:\x
SF:200\r\nStrict-Transport-Security:\x20max-age=31536000\x20;\x20includeSu
SF:bDomains\r\nX-Frame-Options:\x20DENY\r\nContent-Security-Policy:\x20scr
SF:ipt-src\x20'self'\r\nContent-Type:\x20application/json\r\nContent-Lengt
SF:h:\x20170\r\nDate:\x20Sun,\x2022\x20Jan\x202023\x2011:16:59\x20GMT\r\nC
SF:onnection:\x20close\r\n\r\n{\"path\":\"/\",\"message\":\"Full\x20authen
SF:tication\x20is\x20required\x20to\x20access\x20this\x20resource\",\"time
SF:stamp\":\"2023-01-22T12:16:59\.794141\",\"statusCode\":401,\"statusReas
SF:on\":\"Unauthorized\"}\r\n")%r(RTSPRequest,24E,"HTTP/1\.1\x20400\x20\r\
SF:nContent-Type:\x20text/html;charset=utf-8\r\nContent-Language:\x20en\r\
SF:nContent-Length:\x20435\r\nDate:\x20Sun,\x2022\x20Jan\x202023\x2011:16:
SF:59\x20GMT\r\nConnection:\x20close\r\n\r\n<!doctype\x20html><html\x20lan
SF:g=\"en\"><head><title>HTTP\x20Status\x20400\x20\xe2\x80\x93\x20Bad\x20R
SF:equest</title><style\x20type=\"text/css\">body\x20{font-family:Tahoma,A
SF:rial,sans-serif;}\x20h1,\x20h2,\x20h3,\x20b\x20{color:white;background-
SF:color:#525D76;}\x20h1\x20{font-size:22px;}\x20h2\x20{font-size:16px;}\x
SF:20h3\x20{font-size:14px;}\x20p\x20{font-size:12px;}\x20a\x20{color:blac
SF:k;}\x20\.line\x20{height:1px;background-color:#525D76;border:none;}</st
SF:yle></head><body><h1>HTTP\x20Status\x20400\x20\xe2\x80\x93\x20Bad\x20Re
SF:quest</h1></body></html>");
```

U pitanju su *frontend* i *backend* servis naše aplikacije, respektivno. Bitno je napomeuti da *TLS/SSL* nije bio podešen za *frontend* u trenutnku testiranja, međutim, to nije predstavljao problem kako bi se testiranje sprovelo uspješno. Vidimo da je alat pokušao otvoriti *TCP* konekciju sa *frontend* serverom, gdje je dobio *Method Not Supported* kao odgovor (očekivano), dok mu je *backend* server javio da je potrebno prvo odraditi potpunu autetifikaciju kako bi pristup resursima bio moguć (takođe očekivano).

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
```

Takođe, alat je pronašao i neke detalje vezane za *host* mašinu na kojoj su pokrenute instance ovih servisa, gdje vidimo da je riječ o *up-to-date* verziji *Linux*-a na lokalnoj mreži (*network distance* je 0).

Sa prikupljenim podacima možemo krenuti dalje u ispitivanje rajivosti samih servisa.

Nikto

Za ispitivanje ranjivosti aplikacije korišćen je *Nikto* alat. Pokrenuto je skeniranje *frontend* dijela aplikacije s obzirom na to da je *backend*-u nemoguće pristupiti direktno zbog podešenog CORS-a.

```
ivanmrsulja@pop-os:~/Desktop/enterprise_system_simulaion/payment-service-provider-front$ nikto -h http://127.0.0.1:5173
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost
+ Target Port:        5173
+ Start Time:         2023-01-22 12:00:12 (GMT1)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'access-control-allow-origin' found, with contents: *
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /index.html, fields: 0xW/19b 0xmsYscvtJHoIQDBunkTBwqLm5Me8
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'content-security-policy' found, with contents: default-src 'none'
+ Uncommon header 'access-control-allow-methods' found, with contents: GET,HEAD,PUT,PATCH,POST,DELETE
+ 6544 items checked: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2023-01-22 12:00:20 (GMT1) (8 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Prije nego iskomentarišemo rezultate skeniranja, bitno je napomenuti da nam je *vite* server pukao prilikom testiranja gdje je sajt postao neupotrebljiv dok se nije odradio *refresh* stranice. Razlog za ovo je *debug* režim rada, koji je bacao grešku prilikom pokušaja pristupa putanji koja nije definisana u *vue router*-u. Malom ispravkom u *vite-config.js* fajlu da se koristi *build* režim rada, nestala je i greška te je testiranje nastavljeno. Nedostatak *X-Frame-Options header*-a nas je zbunio, s obzirom da je eksplicitno podešen na *backend*-u.

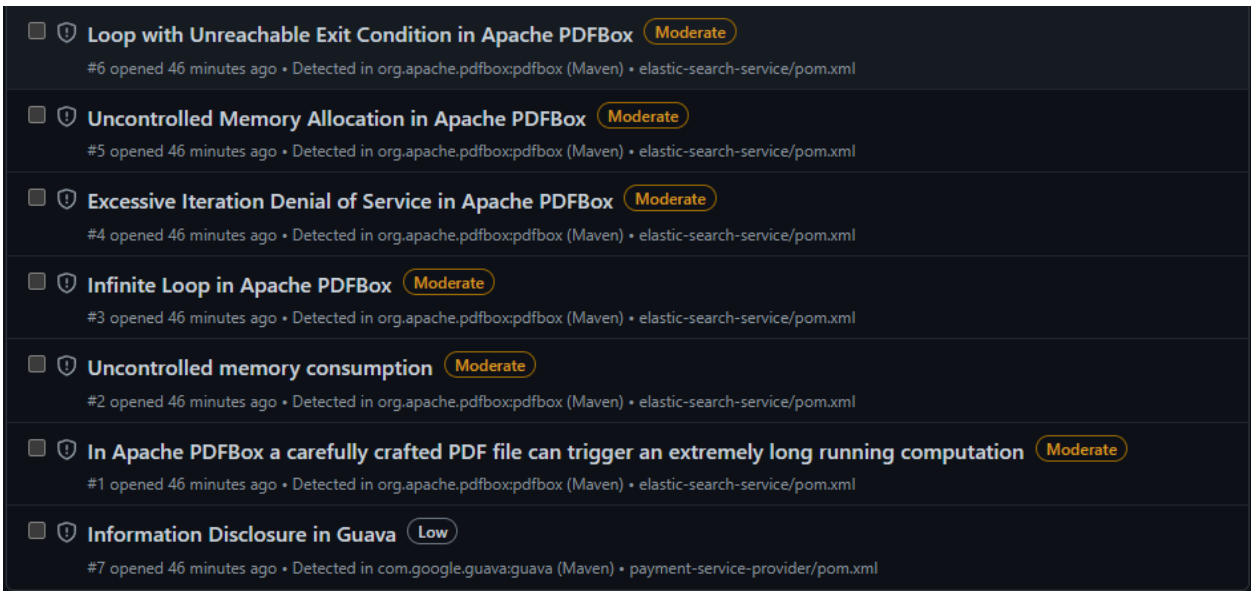
X-Content-Type-Options	ⓘ	nosniff
X-XSS-Protection	ⓘ	1; mode=block
Cache-Control	ⓘ	no-cache, no-store, max-age=0, must-revalidate
Pragma	ⓘ	no-cache
Expires	ⓘ	0
Strict-Transport-Security	ⓘ	max-age=31536000 ; includeSubDomains
X-Frame-Options	ⓘ	DENY
Content-Security-Policy	ⓘ	script-src 'self'
Content-Type	ⓘ	application/json
Transfer-Encoding	ⓘ	chunked
Date	ⓘ	Sun, 22 Jan 2023 14:24:06 GMT
Keep-Alive	ⓘ	timeout=60
Connection	ⓘ	keep-alive

Onde gdje nije podešen, to je sam *vite* server, gdje nam realno nije ni potreban jer se dobavljaju samo *index.html* sa uglifikovanim i minifikovanim *.js bundle*-ovima, tako da je ovo okarakterisano kao *false positive*. Slična je i situacija sa *access-control-allow-origin*, koji iako je a *backend*-u strogo podešen da može primati zahtjeve samo od onih servisa od kojih mora, logično je da na frontendu bude "*" jer njemu treba da svi mogu da mu pristupe. Prijavljeni *server leak*-ovi preko *ETag*-ova su, srećom, takođe *false positive*, jer se *ETag*-ovi nalaze u pojedinim sličicama koje koristimo na *frotend*-u i ne sadrže nikakve osjetljive informacije. Posljednja 3 prijavljena *uncommon header*-a ne predstavljaju grešku već samo daju određene

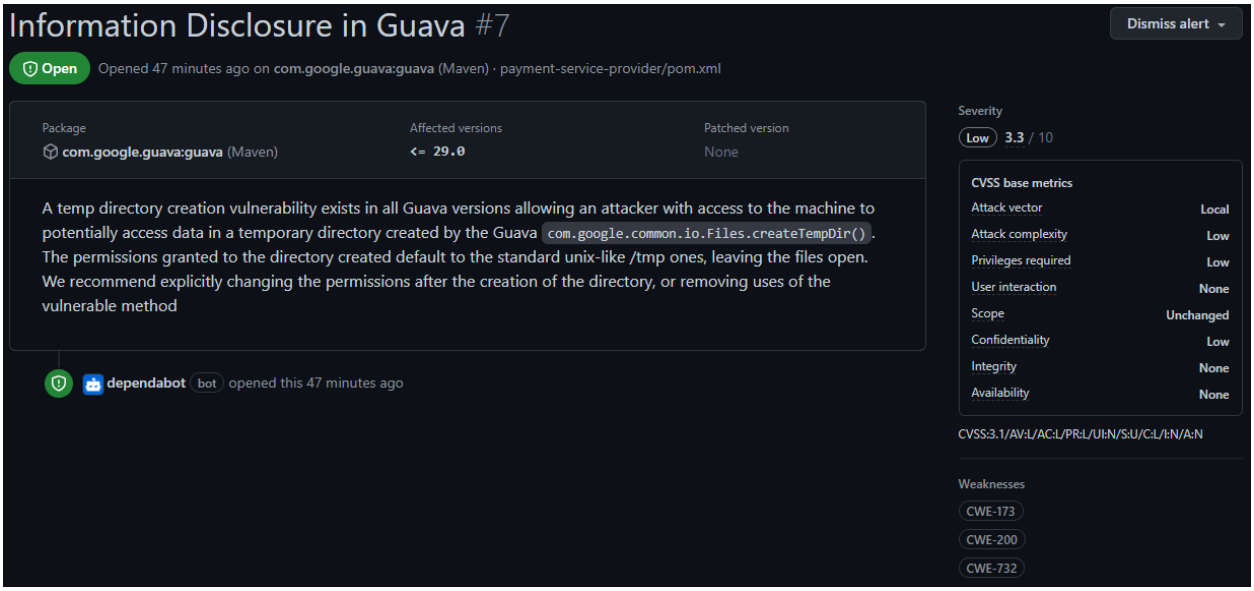
detalje implementacije. Štaviše, ovo je i potvrda da je konfiguracija na *backend*-u dobro odrađena s obzirom da su vrijedosti ovih *header*-a ručno postavljane u konfiguraciji *Spring Security*-a.

Github Dependabot

Github dependbot prijavio je puno ranjivosti:



Prvih 6 vezano je za *pdfbox* biblioteku i njenu lošu implementaciju, koja čak nije ni korišćena za realizaciju funkcionalosti *PSP* servisa, već *ES* servisa za potpuno drugi predmet. Sve u svemu, *update*-ovanjem verzije biblioteke, otklonjeno je i prvih 6 problema. Realan problem bio je *Information Disclosure* problem u *Guava* biblioteci u *PSP* servisu, pogotovo jer se ona koristi kao tranzitivna zavisnost u *bitcoinj* biblioteci.



Za izvršenje ovog nnapada potreban lokalni pristup serveru, te je jedini način zaštite manuelno postavljanje prava pristupa na kreirani *temp* fajl. Ništa kritično, ali zanimljivo da se navede.