**Tim 20**

Marko Njegomir SW-38/2018

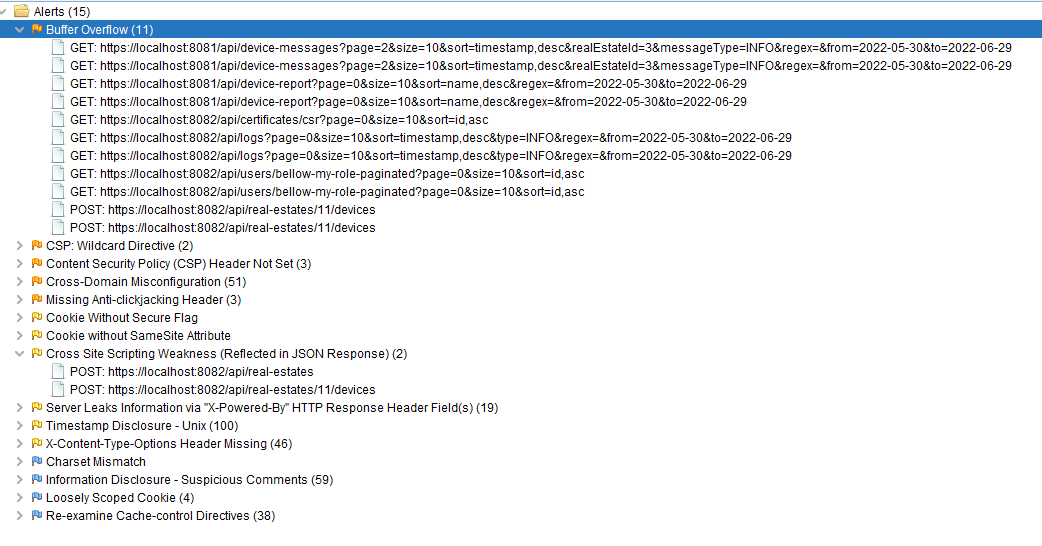
Dušan Erdeljan SW-43/2018

Dušan Brkić SW-42/2018

Penetraciono testiranje

# OWASP ZAP

OWASP ZAP smo koristili u Manual Explore modu, jer smo tako imali veću kontrolu nad testiranjem. Nakon autentifikacije korisnika, ručno smo prolazili kroz sve stranice i pristupali svim dostupnim linkovima, dok je isto vreme opcija Attack mode bila uključena kao i aktive scan opcija. Alat je tokom prolaska kroz stranice vršio penetracione testove.



*Ilustracija 1 Admin aplikacija i Smarth home aplikacija – Alerts za obe frontend I obe bekend aplikacije*

Cookie Without Secure Flag i Cookie without SameSite attribute probleme smo rešili tako što smo dodali ove flegove u cookie na bekendu.

Missing Anti-clickjacking Header je bio false positive pošto se X-Frame-Options: DENY polje nalazi u hederu što smo utvrdili pomoću Postman alata ručnim slanjem tog zahteva.

Cross-Domain Misconfiguration je takođe bio false positive pošto je Access-Control-Allow-Origin podešen u hederima svakog zahteva.

Missing Anti-clickjacking Header je takođe false positive zbog toga što je već postavljen X-Frame-Options: DENY u svim zahtevima.

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) je takođe false alarm, jer takvog polja u zaglavlju nema sa admin aplikacije.

Timestamp Disclosure – Unix su takođe false positive greške, pošto je alat neke brojeve u .js fajlovima tumačio kao datume.



*Ilustracija 2 "Timestamp Disclosure" - broj u linku u komentaru prepoznat pogrešno kao timestamp*

X-Content-Type-Options Header Missing su takođe false positive greške, zbog toga što se odnose samo na neke moziline tracking protection linkove koje je alat prikazao.

Information Disclosure - Suspicious Comments su takođe false positives zbog toga što se odnose na komentare u vendor kodu.

Loosely Scoped Cookie traži da se postavi specifičan path. Nama je su sve putanje na tom portu iz admin aplikacije i počinju sa /. Pošto je ovo samo informational alarm on se ne bi morao ni ispravljati. Mi smo ga ispravili dodavanjem path=/api polja u cookie.

Re-examine Cache-control Directives je takođe false positive jer svi zahtevi imaju postavljeno header polje Cache-Control: no-cache, no-store, max-age=0, must-revalidate.

Cross Site Scripting Weakness (Reflected in JSON Response) je ispravljen dodavanjem regex validacije na polje name u CreateRealEstateRequest i ConfigureDeviceRequest klasama.

Najozbiljniji problem čiji je Risk medium je bio Buffer Overflow. Uzrok ovih alarma bila su polja koja nisu imala ograničenja na dužinu, prvenstveno polja za datum i imena uređaja. Ovo je rešeno dodavanjem validacionih regeksa na bekendu, kao i dodavanjem novog Controller advice kontrolera, koji hvata određene greške nastale prilikom parsiranja datuma. Isto je urađeno i Admin i u Smart Home aplikaciji.

# Burp Suite PRO

Za potrebe automatskog testiranja smo takodje i koristili pro verziju Burp Suite alata. Pokrenuli smo alat sa unetim kredencijalima admina i izvrsili akciju celokupnog testiranja aplikacije, istestiravsi time admin i moja kuca aplikaciju. Na kraju rada alat je izgenerisao izvestaj, koji ce biti analiziran u daljnjem tekstu.

**1. TLS certificate**

Ovaj issue se prijavljuje jer alat ne moze da potvrdi da je sertifikat trusted. Ovaj problem se moze resiti tako sto se sertifikat doda u javin trusted keystore.

**2. Strict transport security not enforced**

Ukoliko nema ovog parametra, napadac je u mogucnosti da zaobidje SSL/TLS enkripciju i okrene nasu aplikaciju protiv njenih korisnika. Napadac moze da zameni https sa http na glavnoj stranici i browser u tom slucaju nece upozoriti korisnika na tako nesto. Da bi se resio ovaj issue kao parametar zaglavlja dodaje 'Strict-Transport-Security' i vrednost 'max-age=expireTime'.

**3. Cross-origin resource sharing**

Kao i prethodnom test suite-u, ovo smo istestirali rucno i uvideli da je parametar zaglavlja Access-Control-Allow-Origin odgovarajuce podešen u hederima svakog zahteva.

**4. Cross-domain Referer leakage**

Ovaj issue se javlja jer se zahteva resurs koji pripada razlicitom domenu. To je angularova biblioteka Material:

<link href="https://fonts.googleapis.com/css2?family=Roboto:wght@300;400;500&amp;display=swap" rel="stylesheet">

<link href="https://fonts.googleapis.com/icon?family=Material+Icons" rel="stylesheet">

**5. Frameable response (potential Clickjacking)**

Issue je isti kao i Missing Anti-clickjacking Header iz prethodnog test suite-a.

**6. Email addresses disclosed**

Issue se javlja jer postoji lazna hardkodovana imejl adresa u kodu klijentske aplikacije.

**7. Cacheable HTTPS response**

Issue je isti kao i Re-examine Cache-control Directives iz prethodnog test-suite-a.