**Tim 20**

Marko Njegomir SW-38/2018

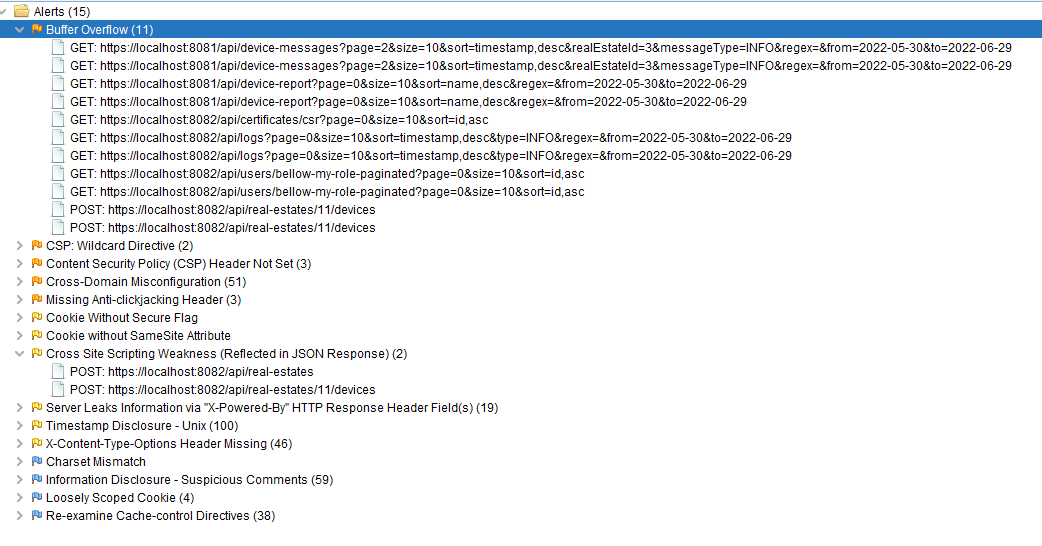
Dušan Erdeljan SW-43/2018

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*

**1. Cookie Without Secure Flag i Cookie without SameSite attribute**

Ove probleme smo rešili tako što smo dodali ove flegove u cookie na bekendu.

**2. Missing Anti-clickjacking Header**

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

**3. Cross-Domain Misconfiguration**

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

**4. Missing Anti-clickjacking Header**

U pitanju je još jedan false positive zbog toga što je već postavljen X-Frame-Options: DENY u svim zahtevima.

**5. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**

Ovaj alarm je takođe false alarm, jer takvog polja u zaglavlju nema sa admin aplikacije.

**6. Timestamp Disclosure – Unix**

Ovo 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*

**7. X-Content-Type-Options Header Missing**

Opet su u pitanju false positive greške, zbog toga što se odnose samo na neke moziline tracking protection linkove koje je alat prikazao.

**8. Information Disclosure - Suspicious Comments**

U pitanju su takođe false positives zbog toga što se odnose na komentare u vendor kodu.

**9. Loosely Scoped Cookie**

Ovaj alarm 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.

**10. Re-examine Cache-control Directives**

Još jedan false positive jer svi zahtevi imaju postavljeno header polje Cache-Control: no-cache, no-store, max-age=0, must-revalidate.

**11. Cross Site Scripting Weakness (Reflected in JSON Response)**

Nedostatak je ispravljen dodavanjem regex validacije na polje name u CreateRealEstateRequest i ConfigureDeviceRequest klasama.

**12. Buffer Overflow**

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 takođe i koristili pro verziju Burp Suite alata. Pokrenuli smo alat sa unetim kredencijalima admina i izvršili akciju celokupnog testiranja aplikacije, istestiravši time admin i moja kuca aplikaciju. Na kraju rada alat je izgenerisao izveštaj, koji će biti analiziran u daljnjem tekstu.

**1. TLS certificate**

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

**2. Strict transport security not enforced**

Ukoliko nema ovog parametra, napadač je u mogućnosti da zaobiđe SSL/TLS enkripciju i okrene našu aplikaciju protiv njenih korisnika. Napadač može da zameni https sa http na glavnoj stranici i browser u tom slučaju nece upozoriti korisnika na tako nešto. Ovaj issue smo rešili tako što smo kao parametar zaglavlja dodali 'Strict-Transport-Security' i vrednost 'max-age=expireTime'.

**3. Cross-origin resource sharing**

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

**4. Cross-domain Referer leakage**

Ovaj issue se javlja jer se zahteva resurs koji pripada različitom 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.