**Application Security Verification Standard: Report**

OWASP Standard za verifikaciju bezbednosti aplikacija (ASVS) je sveobuhvatan standard koji definiše osnovne zahteve za bezbednost veb aplikacija. Standard je podeljen na tri nivoa bezbednosti, svaki sa svojim ključnim zahtevima.

U narednom izveštaju, zahtevi će biti grupisani po nivoima, pa po kategorijama radi preglednosti. Kako se mnogi zahtevi odnose na slične stvari, oni će biti dalje grupisani radi konciznosti, a detaljniji opis i predlog rešenja će se nalaziti u adekvatnoj koloni.

Verzija praćenog standarda je 4.0.3

**Level 1:**

Ovo je nivo sigurnosti koji treba da zadovoljava svaka moderna aplikacija. Zahtevi u ovoj sekciji su relativno jednostavni, kako za razumevanje, tako i za implementaciju.

Stoga, ovaj nivo sigurnosti će biti najdetaljnije obrađen.

| Level 1 | | |
| --- | --- | --- |
| V2.1 sigurnost lozinke | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 2.1.1 - 2.1.4 | Jaka lozinka | Lozinke treba da sadrže od 12 do 64 karaktera (ali ne preko 128), uključeni svi Unicode karakteri, i ostali standardi vezani za lozinke. |
| 2.1.5 - 2.1.6 | Izmena lozinke | Implementirana izmena lozinke za koju je potrebna stara lozinka |
| 2.1.7 \* | Sigurne lozinke | Proveravati da li je lozinka na nekoj od listi čestih lozinki bilo interno ili uz pomoć API-a. |
| 2.1.8 - 2.1.12 | Unos lozinke | Korisnicima treba olakšati unošenje i izbor lozinke uz pomoć prikaza jačine lozinke, dozvole korišćenja password manager-a, privremenog prikaza lozinke itd. |
| V2.2 verifikacija (general authenticator security) | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 2.2.1 - 2.2.3 | Koristiti odgovarajuće mehanizme verifikacije | Koristiti CAPTCH-u. SMS/email koristiti isključivo kao sekundarnu verifikaciju, slati korisnicima obaveštenja vezana za promene lozinki i druge bitne informacije |
| V2.3 životni ciklus autentikatora | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 2.3.1 | Inicijalna lozinka | Sistemski generisana inicijalna lozinka koja je randomizovana i PRIVREMENA |
| V2.5 povratak kredencijala | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 2.5 | Generalno | Generalne konvencije vezane za povratak kredencijala, koristiti 2-factor autentikaciju, obaveštavati korisnika o dešavanjima vezanim za sigurnost (najčešće putem e-maila) |
| 2.5.2\* | Autentikacija bazirana na znanju ličnih informacija | Ne treba koristiti sigurnosna pitanja i druge vidove autentikacije bazirane na znanju ličnih informacija |
| V2.7 “out of bound” verifikacija | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 2.7.1 - 2.7.4 \* | Koristiti “out of bound” verifikaciju | Ovaj tip verifikacije se odnosi na uređaje ili aplikacije koje koriste siguran kanal komunikacije sa aplikacijom za verifikaciju. |
| V2.8 “one time” verifikacija | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 2.8.1 | “one time” verifikacija | Koristiti i ovaj vid verifikacije, najčešće kod poslat putem SMS-a ili e-maila koji ima vreme isteka |
| V3.1 osnovna sigurnost sesije | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 3.1.1 | Ne treba otkrivati session token | - |
| V3.2 sigurnost tokena | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 3.2.1 - 3.2.3 | Osnovna sigurnost tokena sesije | Token generisati prilikom autentikacije, generisati ga sigurnim algoritmom i čuvati na siguran način u pretraživaču. |
| V3.3 prekidanje važenja tokena | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 3.3.1 - 3.3.2\* | Token sesije ima adekvatno vreme važenja | Prekidati važenje tokena sesije prilikom napuštanja prozora ili nakon dugog vremena korišćenja/nekorišćenja. (30 dana) |
| V3.4 kontrola sesije uz pomoć “cookie”-a | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 3.4.1 - 3.4.5 | Sigurnost “cookie”-a | Većinom vezano za atribute koje poseduju |
| V3.7 odbrana od eksploatacije sesije | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 3.7.1 | Ponovna validacija | Pre izvršavanja osetljivih transakcija i davanja ličnih informacija tražiti ponovnu autentikaciju. |
| V4.1 generalna kontrola pristupa | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 4.1.1 - 4.15 | Generalna kontrola pristupa (privilegije) | Provera privilegija na sigurnom servisnom sloju aplikacije, zabrana pristupa sa korisničke aplikacije informacijama koje ne bi trebale biti dostupne. |
| V4.2 operativna kontrola pristupa | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 4.2.1 - 4.2.2 | Odbrana od IDOR i CSRF napada | Detaljnije obrađeno u prethodnim zadacima. |
| 4.2.3 - 4.2.4 | Zabrana pristupa fajl sistemu osim ako to nije eksplicitan zahtev | - |
| V5.1 validacija unosa | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 5.1.1 \* | Odbrana od HTTP parameter pollution napada | Korišćenje boljih i naprednijih frejmworka, poput Spring Boot-a |
| 5.1.2 - 5.1.8 | Generalna validacija unosa | Pozitivna validacija, odbrana od SSRF, CORS i drugih napada nevalidnih ili opasnih ulaza poput XML-ova. |
| V5.3 encoding izlaza i odbrana od “injection” napada | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 5.3.1 - 5.3.10 | Koristiti adekvatne enkodere | Enkoder treba da prati korisnički odabranu lokalizaciju |
| 5.3.1 - 5.3.10 | Odbrana od “injection” napada | Parametrizovani upiti, korišćenje adekvatnih enkodera za XML, js i druge tipove podataka. Odbrana od JSON, LDAP, OS command XML i drugih injection napada. |
| V5.5 prevencija deserijalizacije | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 5.5.1 | Provera integriteta serijalizovanih objekata ili potencijalna enkripcija istih | Radi odbrane od promene poslatih objekata. Potencijalnom server side validacijom ulaznih DTO-ova. |
| 5.5.2 - 5.5.4 | Ponovna odbrana od injection napada | Paziti na deserijalizaciju određenih tipova fajlova kako oni ne bi bili izvršeni |
| V6.2 algoritmi | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 6.2.1 | Osigurati error handling | Osigurane greške kriptografskih algoritama, i rukovanje greškama unutar koda. Odbrana od oracle padding napada |
| V7.1 logovanje | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 7.1.1 - 7.1.2 | Pazi šta se loguje | Osigurati da se ne loguju korisničke privatne informacije, šifre i ostali PII.  Takođe tokeni sesije se loguju isključivo hešovani. |
| V7.4 rukovanje greškama | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 7.4.1 | Generično rukovanje greškama | Koristiti opšte opise greški sa specifičnijim informacijama isključivo u formi ID-eva. |
| V8.2 čuvanje informacija na klijentskoj strani | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 8.2.1 - 8.2.3 | Brisanje bitnih klijentskih informacija | Brisanje informacija iz keša i memorije pretraživača, često putem zaglavlja http poziva, ali ponekad je potrebno brisati te stvari i ručno (u kodu) |
| V8.3 osetljive/privatne informacije | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 8.3.1 - 8.3.4\* | Generalno čuvanje privatnih informacija | Obaveštavanje korisnika o tome koje informacije se čuvaju. Davanje POTPUNE kontrole korisniku da obriše svoje privatne informacije iz sistema. Slanje osetljivih podataka u telu ili hederu upita (ne u samom upitu) |
| V9.1 bezbednost komunikacionih kanala | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 9.1.1 - 9.1.3\* | Korišćenje bezbednog i aktuelnog TLS-a | Obezbediti sigurnost na transportnom sloju za svu komunikaciju sa korisnikom, koristiti aktuelne alate za testiranje TLS-a i uključiti bezbednosne protokole u aplikaciju. |
| V10.3 integritet aplikacije \* | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 10.3.1 | Ažuriranje aplikacije | Obezbediti client ili server side automatsko ažuriranje softvera putem sigurnih kanala sa potpisima. |
| 10.3.2 | Potpisivanje koda | Radi provere validnosti |
| 10.3.3 | Odbrana od subdomain takeover napada | Provera isticanja DNS domena potencijalno i manuelno itd. |
| V11.1 sigurnost biznis logike | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 11.1.1 - 11.1.5 | Bezbednost toka i podataka unutar biznis logike | Koraci se moraju dešavati sekvencijalno u određenom poretku, podaci sa kojima se rukuje moraju biti u određenim granicama itd. |
| V12.1 uploadovanje fajlova | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 12.1.1 | Odbrana od velikih fajlova | Restrikcija veličine fajla kako ne bi došlo do DOS napada (tako lako) |
| Ostali \* | Ostali zahtevi ranije obrađeni pa se ne dupliraju | - |
| V12.3 pokretanje fajlova | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 12.3.1 -12.3.6 | Sigurno pokretanje/nepokretanje fajlova koje korisnici uploaduju | Većinom pređeno u poglavlju vezanom za injection napade. |
| V12.4 čuvanje fajlova | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 12.4.1 - 12.4.2 \* | Oprez od uploadovanih fajlova | Fajlove čiji izvor nije proveren treba skenirati i čuvati van root foldera |
| V12.5 preuzimanje fajlova | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 12.5.1 - 12.5.2 \* | Ograničavanje tipova fajlova koji mogu biti preuzeti | Ograničiti pristup fajlovima sa logovima, rezervnim podacima i podacima koji su zaštićeni. Null byte napad. |
| V12.6 SSRF zaštita | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 12.6.1 \* | Kreirati listu adresa odakle server sme da preuzima informacije | White listing over black listing |
| V13.1 uopštena web sigurnost | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 13.3.1 - 13.3.2 | Korišćenje istih parsera na svim komponentama | - |
| V13.2 RESTfull servisi | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 13.2.1 - 13.2.3 \* | Korišćenje rola | Sve uz pomoć “cookie”-a |
| V13.3 SOAP servisi | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 13.3.1 | Provera fajlova pre izvršavanja | - |
| V14.2 Dependency | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 14.2.1 - 14.2.3 | Korišćenje kompatibilnih biblioteki i brisanje nepotrebnih iz projekta | - |
| V14.3 slučajni sigurnosni propusti | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 14.3.2 - 14.3.3 | Slučajni propusti | U produkciji isključiti dev funkcionalnosti, iz hedera izbaciti osetljive informacije |
| V14.4 bezbednosni hederi | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 14.4.1 - 14.4.7 | U zahtevima treba da budu prisutni svi sigurnosni hederi | - |
| V14.5 validacija hedera | | |
| Zahtev | Opis zahteva | Predlog rešenja |
| 14.5.1 | Provera hedera na serveru | - |
| 14.5.2 \* | Ne koristiti Origin heder za autentikaciju | Origin heder se lako može promeniti od strane napadača |
| 14.5.3 | CORS White list | - |

**Level 2:**

Ovaj nivo sigurnosti po mojoj proceni nije u potpunosti potrebno implementirati za ovu aplikaciju. Ono što je izostavljeno iz prvog nivoa je izbor algoritama i implementacija/korišćenje proverenih podsistema koji izvršavaju određene funkcije na standardan i proveren način.

Takođe se oslanja i na manuelnu proveru istih, jer kako je i naglašeno u uputstvu, nije moguća provera celog sistema samo automatizovanim alatima.