



REPUBLIKA SLOVENIJA  
MINISTRSTVO ZA DIGITALNO PREOBRAZBO

Številka:  
Datum:

---

## **Navodilo projektnim vodjem za varnostna preverjanja - Zahteve**

## KAZALO:

1 UVOD .....	3
2 PROCES .....	3
2.1 STATIČNI VARNOSTNI PREGLED IZVORNE KODE .....	3
2.2 VARNOSTNI PREGLED APLIKACIJ .....	3
3 PREDPOGOJI ZA IZVEDBO .....	4
3.1 STATIČNI VARNOSTNI PREGLED IZVORNE KODE .....	4
3.2 VARNOSTNI PREGLED APLIKACIJ .....	4
4 OSNOVNI PODATKI O PROJEKTU .....	5
5 PRILOGE .....	8
5.1 ODDAJANJE ZAHTEVKA ZA ROČNO VARNOSTNO PREVERJANJE IZVORNE KODE ( VARNOSTNO PREVERJANJE KODE- SOC S1) .....	8
5.2 ODDAJANJE ZAHTEVKA ZA VARNOSTNI PREGLED APLIKACIJ (VARNOSTNO PREVERJANJE APLIKACIJ–SOC S2) .....	9
6 SPREMEMBA PROCESA IZVAJANJA PREGLEDOV .....	10

## KAZALO TABEL:

Tabela 1: Osnovni podatki o projektu .....	5
Tabela 2: Osnovne zahteve za statično varnostno preverjanje izvirne kode .....	7
Tabela 3: Osnovne zahteve za varnostni pregled aplikacije .....	8

## 1 UVOD

Vsebina dokumenta je opis zahtev, ki so potrebne za izvedbo nalog, ki jih v okviru MDP izvaja SOC:

- statični varnostni pregled izvirne kode (izvaja skupina SOC S1),
- varnostni pregled aplikacij (izvaja skupina SOC S2).

Dokument je namenjen projektnim vodjem, skrbnikom aplikacij, upravljavcem procesa namestitve aplikacij in razvijalcem, ki razvijajo aplikativne informacijske rešitve za gostovanje na Državnem računalniškem oblaku (DRO).

## 2 PROCES

### 2.1 Statični varnostni pregled izvirne kode

Statični varnostni pregled izvirne kode se izvaja v okviru MDP delovnega procesa »Gostovanje informacijskih rešitev na infrastrukturi DRO«. Aktivnosti procesa potekajo preko dogovorjene objave izvirne in binarne kode v repozitoriju za upravljanje izvirne kode.

Statični varnostni pregled izvirne kode, poteka v dveh korakih:

1. **Samodejno varnostno preverjanje izvirne kode** z orodjem za statično varnostno analizo (**SAST analiza**), se izvede ob odložitvi nove verzije programske kode v repozitorij za upravljanje izvirne kode. SAST analizo proži izvajalec z ustrezno definicijo meta atributov projekta. Ob koncu SAST analize izvajalec prejme SAST poročilo v PDF in Excel obliki, ki se posreduje v repozitorij za upravljanje izvirne kode in v samodejno kreiran Redmine zahtevek. Izvajalec poročilo pregleda ter odpravi ranljivosti za rezultate, za katere meni, da so upravičeni in ponovno odloži novo verzijo programske kode v repozitorij za upravljanje izvirne kode. Programsko kodo lahko odloži večkrat in vsakič bo prejel novo SAST poročilo. Ko izvajalec oceni, da poročilo vsebuje le neupravičeno zaznane ranljivosti in je programska koda primerna za ročno varnostno preverjanje programske kode, odda zahtevek za ročni pregled izvirne kode, kot je opisano v elektronskem sporočilu, ki ga prejme ob končani SAST analizi, v zahtevek posreduje obrazložitve za preostale ranljivosti.
2. **Ročno varnostno preverjanje izvirne kode**, izvede varnostni inženir na osnovi poročila SAST analize. Varnostni inženir pregleda preostale zaznane ranljivosti na osnovi argumentov izvajalca. Varnostni inženir vsak rezultat posebej oceni ter ga označi za neupravičenega (false positive) oz. ga označi kot upravičenega ter z obrazložitvijo zavrne argumentacijo izvajalca. Vse obrazložitve ter oceno o primernosti aplikacije za nadaljnje postopke, poda varnostni inženir v poročilu »Poročilo varnostnega pregleda izvirne kode z oceno«. Po uspešni odpravi varnostnih pomanjkljivosti se pregledana verzija aplikacije posreduje v naslednjo fazo procesa objave in namestitve.

Postopek statičnega varnostnega pregleda izvirne kode se mora praviloma ponoviti, če je bila izvorna koda aplikacije v nadaljnjem procesu testiranja spremenjena.

### 2.2 Varnostni pregled aplikacij

V procesu varnostnega pregleda aplikacij se testiranje opravi na aplikaciji, ki je nameščena v testnem ali izjemoma produkcijskem okolju. Opravi se tako imenovani vdorni ali penetracijski test. Rezultat procesa je priprava poročila o najdenih pomanjkljivostih s priporočili, kako te pomanjkljivosti odpraviti.

Poročilo poleg osnovnih podatkov o testiranju, natančnega poteka izvajanja posamezne storitve (dokumentiran zapis zaznanih varnostnih pomanjkljivostih, opis scenarijev možnih

zlorab ...), ugotovitev, povezav na druge vire, vsebuje tudi priporočila in nasvete na podlagi dobrih praks, ki bodo naročniku v pomoč pri odpravi pomanjkljivosti.

V kolikor je potrebno, bo za namen čim boljšega razumevanja varnostnega pregleda aplikacije izvedena podrobna tehnična predstavitev rezultatov vdornega testiranja zainteresiranim ciljnim skupinam.

### 3 PREDPOGOJI ZA IZVEDBO

#### 3.1 Statični varnostni pregled izvirne kode

Za učinkovito in pravočasno izvedbo statičnega varnostnega pregleda izvirne kode mora razvijalec izpolniti predpogoje, ki so navedeni v Tabeli 2. Pravilna namestitve izvirne kode in pravilna konfiguracija manifest datoteke sta pogoj za avtomatski začetek izvedbe statične analize izvirne kode. Le ta se praviloma izvede v roku 24 ur po odložitvi kode na repozitorij za odlaganje izvirne kode. Ta čas pa se lahko podaljša v primeru, da je na repozitoriju odloženo večje število izvornih kod (iz več hkratnih projektov).

Navodila za oddajo zahtevka za ročno varnostno preverjanje izvirne kode (SOC1) se pošljejo kontaktnim osebam (navedenimi v manifest datoteki) po elektronski pošti skupaj z rezultati avtomatizirane analize izvirne kode.

#### 3.2 Varnostni pregled aplikacij

Zahteve za izpolnitev pogojev za pričetek aktivnosti varnostnega pregleda aplikacij se nahajajo v Tabeli 3.

**Za učinkovito in pravočasno izvedbo varnostnega pregleda aplikacije mora vodja projekta oddati zahtevek (SOC2). Navodila za oddajo zahtevka se nahajajo v poglavju 5 PRILOGE**

#### 5.1 Oddajanje zahtevka za ročno varnostno preverjanje izvirne kode ( varnostno preverjanje kode- SOC S1)

##### 5.1.2 Pogoji

Poročilo SAST analize vsebuje le neupravičeno zaznane ranljivosti.

##### 5.1.2 Oddajanje zahtevka v Redmine

Vsaka analiza izvirne kode **samodejno kreira zahtevek** na **sistemu Redmine** na spletnem naslovu <https://dro.sigov.si/redmine>. Zahtevku za verzijo programske opreme, ki je primerna za ročno varnostno preverjanje izvirne kode, je potrebno **spremeniti status** iz Statična analiza – Validacija v Pregled izv. kode – Naročen.

V Redmine zahtevku je potrebno dodati še komentarje za preostale varnostne ranljivosti iz SAST poročila. Komentarji se podajo v izvirno SAST poročilo v Excel obliki, v katero se doda kolona »Opomba izvajalca«, v katero se vnese opomba, zakaj gre za neupravičeno zaznano ranljivost.

**Zahtevkov, ki niso v statusu »Pregled izv. kode – Naročen« skupina SOC S1 ne vidi.**

##### 5.1.3 Rezultat

Rezultate statičnega varnostnega pregleda izvirne kode **skupina SOC S1** priloži k zahtevku v **sistemu Redmine v obliki PDF in Word (.docx, v kolikor je to potrebno), datoteke.**

V datoteki je navedeno:

- primernost aplikacije (neprimerna / pogojno primerna / primerna)

- opis ugotovljenih pomanjkljivosti (v primeru, da je primernost aplikacije neprimerna ali pogojno primerna).

Zahtevku se glede na rezultat statičnega varnostnega pregleda izvirne kode določi status:

- o Pregled izvirne kode - Uspešen,
- o Pregled izvirne kode - Neuspešen,
- o Pregled izvirne kode - Pogojno uspešen.

V kolikor je aplikacija **pogojno primerna oz. primerna** za nadaljnje postopke, se **lahko namesti v testno okolje**.

V najkrajšem možnem času je potrebno odpraviti vse pomanjkljivosti in ustrezno poročati skupini SOC.

V primeru, da je aplikacija **neprimerna** za nadaljnje postopke, se **morajo vse problematične pomanjkljivosti odpraviti**, nova različica aplikacije pa mora **ponovno prestati SAST analizo in ročni pregled izvirne kode**.

5.2 Oddajanje zahtevka za varnostni pregled aplikacij (varnostno preverjanje aplikacij–SOC S2).

## 4 OSNOVNI PODATKI O PROJEKTU

Za vsak projekt mora vodja projekta zagotoviti osnovne podatke, ki so navedeni v

Tabela 1.

Naziv	Naziv projekta
Verzija	Verzija programske opreme
Opis	Kratek opis projekta
Naročnik	Kdo je naročnik projekta
Kontakt naročnika	Kontaktne podatki naročnika
Izvajalec	Razvijalec programske opreme
Kontakt izvajalca	Kontaktne podatki razvijalca
URL*	Spletni naslov
Tehnologija	Uporabljena tehnologija
Okolja	Okolja kjer je nameščena programska oprema
Virtualno okolje (DA/NE)	Ali je uporabljeno virtualno okolje?
Rok	Predviden rok izvedbe projekta
Namešča	Namestitveni inženir

\* če obstaja testna postavitve

Tabela 1: Osnovni podatki o projektu

Pred izvedbo varnostnega pregleda izvorne kode mora vodja projekta skupaj z razvijalcem izpolniti zahteve navedene v Tabeli 2.

Aktivnost ali zadeva	Opis
<b>Dokumentacija</b>	Za uspešno razumevanje delovanja aplikacije je potrebno zagotoviti dokumentacijo o sami aplikaciji, komponentah in povezavah z drugimi sistemi.
<b>Uporabljene tehnologije</b>	V sklopu dokumentacije morajo biti razvidne tudi naslednje vsebine: a) arhitekturna postavitev rešitve; b) uporabljene tehnologije; c) uporabljeni programski jeziki; č) implementirane varnostne kontrole (glej naslednjo zahtevo).
<b>Opis izvedenih varnostnih kontrol</b>	Opis implementiranih varnostnih kontrol: minimalno OWASP TOP 10 (XSS, SQLInjection zaščita, CSRF, Reflected XSS, Session Management ...). Seznam lastno razvitih knjižnic in metod, ki se uporabljajo za implementacijo posamezne varnostne kontrole.
<b>Objava izvorne kode v repozitorij za upravljanje izvorne kode</b>	Aplikacije se v MDP okolju nameščajo po dogovorjenem postopku razvoja in objave aplikacij. V okviru tega postopka je potrebno dokumentacijo, bazne objekte, aplikativne objekte in izvorno kodo objaviti v repozitorij za upravljanje izvorne kode. Navodila dostopa in drevesne strukture repozitorija vzdržuje MDP (Sektor za upravljanje s podatkovnimi zbirkami in inf.)
<b>Dostopne pravice</b>	SOC ekipi je potrebno zagotoviti dostop do dela repozitorija projekta, kjer se nahajajo poročila. (uporabniki so v AD grupi SOC)
<b>Objava nove verzije aplikacije in njene izvorne kode</b>	Novo verzijo izvorne kode (tudi začetno) se v repozitoriju za upravljanje izvorne kode objavi z novo oznako (tag), ki je dejansko kopija trenutne verzije (trunk) v trenutku označitve.
<b>Priprava/dopolnitev MANIFEST datoteke</b>	Proces, ki prek CI postopkov sproži pregled izvorne kode, potrebuje določene metapodatke projekta, ki jih prebere iz dogovorjene datoteke MANIFEST.MF: SoC/MANIFEST.MF. V datoteki je potrebno vpisati metapodatke: <b>SoC-ProjectName:</b> ImeProjekta (string) <b>SoC-ScanPresetID:</b> ID Nabora pravil po katerih se ravna pregled (int) <b>SoC-ZippedFile:</b> ImePaketa.zip <b>SoC-Tag:</b> ime_veje_ki_je_objavljena_za_pregled <b>SoC-PreScanEmailNotification:</b> a1@example.com, a2@example.com <b>SoC-PostScanEmailNotification:</b> <b>SoC-ScanFailureEmailNotification:</b>  Razvijalec mora obvezno vpisati atribut SoC-ProjectName, pri čemer SoC-ProjectName vrednost uskladi s SoC ekipo.  Obvezen je tudi vpis atributa SoC-Tag, katerega vrednost vsebuje oznako (tag) veje izvorne kode, ki jo razvijalec daje v pregled.
<b>Prevzem rezultatov</b>	Razvijalec prevzame rezultate pregleda preko prejete elektronske pošte, če je vpisal v atribut SoC-PostScanEmailNotification ustrezen elektronski naslov.  Rezultate CI postopek objavi tudi v repozitoriju za upravljanje izvorne kode <b>SoC/Reports/Cx-ProjectName-TagName-\$Date.pdf</b>
<b>Uskladitveni sestanek</b>	V primeru, da želi razvijalec za ugotovljene napake dodatno razlago, dogovori s SoC ekipo uskladitveni sestanek. Pred sestankom

	posreduje v elektronski obliki pojasnitev nestrinjanja z ugotovitvami oziroma razlago ustreznosti varnostne kontrole.
<b>Ponovitev pregleda</b>	Po odpravi pomanjkljivosti razvijalec ponovno objavi kodo v repozitoriju za upravljanje izvirne kode z novo oznako (TAG) verzije. V MANIFEST datoteki ustrezno izpolni atribut SoC-TAG, ki ima vrednost nove verzije=TAG-a.
<b>Primernost</b>	<b>Z znižanjem veljavnih varnostnih tveganj pod sprejemljivo mejo je produkt primeren za nadaljnje postopke – namestitev v testno okolje.</b>

Tabela 2: Osnovne zahteve za statično varnostno preverjanje izvirne kode

Pred izvedbo statičnega varnostnega pregleda aplikacije mora vodja projekta skupaj z razvijalcem izpolniti zahteve navedene v Tabeli 3.

Aktivnost ali zadeva	Opis
<b>Navodila za uporabo</b>	Za uspešno razumevanje delovanja aplikacije je potrebno zagotoviti dokumentacijo – uporabniška navodila, ki opisujejo namen in način uporabe aplikacije.
<b>Uporabniške vloge</b>	Pripravljeni morajo biti uporabniški računi za vsako različno vlogo/privilegije. V kolikor se uporablja varnostna shema, mora biti shema ustrezno pripravljena za uporabniške vloge. Skrbniki lahko preverijo delovanje s testnimi certifikati, ki se bodo uporabljali med samim testiranjem aplikacije. Podatke o certifikatih je mogoče dobiti s poizvedbo na soc.mdp@gov.si.
<b>Dostop do aplikacije</b>	Aplikacija mora biti dostopna iz SOC segmenta, namenjenega testiranju (10.5.240.*). URL naslovi, na katerih se nahaja aplikacija, morajo biti posredovani na soc.mdp@gov.si. Na testni sistem naj bo nameščena zadnja različica aplikacije, ki se med testiranjem ne sme spreminjati.
<b>Testno okolje</b>	Testno okolje naj bo čim boljša kopija produkcijskega okolja z vsemi komponentami, ki bodo nameščene tudi v produkciji. Okolje se med izvajanjem testiranja ne sme spreminjati, saj so lahko v nasprotnem primeru rezultati testiranja nezanesljivi.
<b>Testni podatki</b>	V podatkovni bazi morajo biti vneseni že nekateri podatki, ki prikazujejo delovanje same aplikacije (Podatki funkcionalnega testiranja). V kolikor so v njej podatki preneseni iz produkcijskih baz, ki vsebujejo tudi osebne podatke, naj bodo ti podatki ustrezno maskirani ali anonimizirani.
<b>Poročilo o uspešno izvedenem funkcionalnem testu</b>	Projektni vodja mora zgotoviti poročilo o uspešnem funkcionalnem testiranju, ki vsebuje primere, ki so bili testirani in jih je možno ponoviti v taki ali deloma spremenjeni obliki.
<b>Arhiviranje</b>	Pred samo izvedbo testiranja je priporočljivo, da se naredi kopija aplikacijskega okolja in podatkovne baze, v kolikor jo aplikacija ali sistem uporablja. Tako se bo lahko v primeru, da avtomatska orodja po nesreči pobrišejo vsebine, hitro in enostavno nazaj vzpostavilo delujoče okolje.
<b>Kick-off sestanek</b>	Za uspešno izvedbo pregleda se priporoča kick-off sestanek pred samo izvedbo testiranja. Na njem naj bodo skrbniki aplikacije, odgovorni za namestitev aplikacije na sisteme. Odgovorni za vsebinski del naj na kratko (30min) predstavijo delovanje aplikacije in njene posebnosti.
<b>Izvedba pregleda in priprava poročila</b>	Izvede se pregled aplikacije skladno z metodologijo in pripravi poročilo o rezultatih testiranja
<b>Predstavitev</b>	Po potrebi se lahko opravi predstavitev na sestanku.

<b>poročila</b>	
<b>Verifikacijski pregled</b>	Po odpravljenih pomanjkljivostih se opravi verifikacijski pregled. Za uspešno izvedbo je potrebno poskrbeti za okolje kot v primeru izvedbe testiranja.
<b>Primernost</b>	<b>Primernost za produkcijo</b>

Tabela 3: Osnovne zahteve za varnostni pregled aplikacije

## 5 PRILOGE

### 5.1 Oddajanje zahtevka za ročno varnostno preverjanje izvirne kode (varnostno preverjanje kode- SOC S1)

#### 5.1.2 Pogoji

Poročilo SAST analize vsebuje le neupravičeno zaznane ranljivosti.

#### 5.1.2 Oddajanje zahtevka v Redmine

Vsaka analiza izvirne kode **samodejno kreira zahtevek** na **sistemu Redmine** na spletnem naslovu <https://dro.sigov.si/redmine>. Zahtevku za verzijo programske opreme, ki je primerna za ročno varnostno preverjanje izvirne kode, je potrebno **spremeniti status** iz Statična analiza – Validacija v Pregled izv. kode – Naročen.

V Redmine zahtevek je potrebno dodati še komentarje za preostale varnostne ranljivosti iz SAST poročila. Komentarji se podajo v izvirno SAST poročilo v Excel obliki, v katero se doda kolona »Opomba izvajalca«, v katero se vnese opomba, zakaj gre za neupravičeno zaznano ranljivost.

**Zahtevkov, ki niso v statusu »Pregled izv. kode – Naročen« skupina SOC S1 ne vidi.**

#### 5.1.3 Rezultat

Rezultate statičnega varnostnega pregleda izvirne kode **skupina SOC S1** priloži k zahtevku v **sistemu Redmine v obliki PDF in Word (.docx, v kolikor je to potrebno), datoteke.**

V datoteki je navedeno:

- primernost aplikacije (neprimerna / pogojno primerna / primerna)
- opis ugotovljenih pomanjkljivosti (v primeru, da je primernost aplikacije neprimerna ali pogojno primerna).

Zahtevku se glede na rezultat statičnega varnostnega pregleda izvirne kode določi status:

- o Pregled izvirne kode - Uspešen,
- o Pregled izvirne kode - Neuspešen,
- o Pregled izvirne kode - Pogojno uspešen.

V kolikor je aplikacija **pogojno primerna oz. primerna** za nadaljnje postopke, se **lahko namesti v testno okolje.**

V najkrajšem možnem času je potrebno odpraviti vse pomanjkljivosti in ustrezno poročati skupini SOC.

V primeru, da je aplikacija **neprimerna** za nadaljnje postopke, se **morajo vse problematične pomanjkljivosti odpraviti**, nova različica aplikacije pa mora **ponovno prestati SAST analizo in ročni pregled izvirne kode.**



## 5.2 Oddajanje zahtevka za varnostni pregled aplikacij (varnostno preverjanje aplikacij–SOC S2)

### 5.2.1 Pogoji

Zahtevek za izvajanje varnostnega preverjanja (vdorni test) aplikacije je mogoče oddati le pod naslednjimi pogoji:

- aplikacija ima opravljen **ročni pregled izvirne kode**, ki ga izvaja **skupina SOC S1 z rezultatom primerno oz. pogojno primerno**,
- aplikacija je nameščena na testnem strežniku, in:
  - je enake različice, kot pri ročnem pregledu izvirne kode,
  - je funkcionalno pregledana in popolnoma delujoča,
  - je konfigurirana na način, ki najbolje predstavlja kasnejše produkcijsko okolje,
  - ima ustvarjen vsaj en testni uporabniški račun za vsako vlogo (npr. nizko privilegiran račun in administratorski račun s katerim lahko spreminjamo vloge drugega računa),
  - v aplikaciji so testni podatki, ki simulirajo delujočo aplikacijo v produkcijskem okolju.

Priporočamo, da se sistem pred varnostnim preverjanjem **arhivira** saj lahko med izvajanjem preverjanja pride do vnosa testnih vrednosti in motenj sistema.

### 5.2.2 Oddajanje zahtevka v Redmine

Vsi zahtevki za izvajanje varnostnega preverjanja se oddajo preko **sistema Redmine** na spletnem naslovu <https://dro.sigov.si/redmine> z naslednjimi podatki:

- vrsta zahtevka: **Varnostno preverjanje SOC S2**,
- dodeljen: **skupina SOC S2**,
- dodatni podatki v opisu zahtevka:
  - vrsta pregleda:
    - **penetracijski test** – aplikacija še nima opravljenega penetracijskega testa
    - **verifikacijski pregled** – na prejšnjem penetracijskem testu je bila aplikacija označena kot **neprimerna** ali **pogojno primerna** za nadaljnje postopke,
  - URL-naslov(e) do spletne aplikacije,
  - seznam uporabniških računov z različnimi vlogami,
    - uporabniška imena in gesla ali
    - certifikati (priporoča se uporaba obstoječih certifikatov npr. »Prošt«)
  - uporabniška navodila (če ta obstajajo),
  - različica aplikacije,
  - poročilo in priloge ročnega pregleda izvirne kode.

**Napačno oddanih zahtevkov skupina SOC S2 ne vidi.**

### 5.2.3 Rezultat

Rezultate varnostnega pregleda aplikacije **skupina SOC S2** priloži k oddanemu zahtevku v **sistemu Redmine v obliki Word (.docx) datoteke**.

V datoteki je navedeno:

- primernost aplikacije (neprimerna / pogojno primerna / primerna)
- opis ugotovljenih pomanjkljivosti (v primeru, da je primernost aplikacije neprimerna ali pogojno primerna).

V kolikor je aplikacija **pogojno primerna oz. primerna** za nadaljnje postopke, se **lahko namesti v produkcijsko okolje**.

V najkrajšem možnem času je potrebno odpraviti vse pomanjkljivosti in ustrezno poročati skupini SOC.

V primeru, da je aplikacija **neprimerna** za nadaljnje postopke, se **morajo vse visoko in srednje kritične pomanjkljivosti primerno odpraviti**, nova različica aplikacije pa mora **ponovno prestati ročni pregled izvirne kode in ponoven varnostni pregled aplikacije** (verifikacijski pregled).

## **6 SPREMEMBA PROCESA IZVAJANJA PREGLEDOV**

Skladno z dogovorom vodstva SOC, se pri obsežnejših in zahtevnejših sistemih , kadar je to smiselno zaradi obvladovanja rokov ali stroškov, lahko faze testiranj izvajajo vzporedno ali v drugačnem vrstnem redu. Predlog za spremembo procesa izvedbe je potrebno podrobno utemeljiti s strani vodje projekta. Vodstvo SOC se mora s spremembo strinjati.

Pogoji za namestitev v produkcijo pa ostajajo enaki: ustrezna potrditev varnostnega testa in ustrezna potrditev funkcionalnih zahtev.

Posebnosti in spremembe se za vsako spremembo posebej zavedejo, obrazložijo in potrdijo v sistemu Redmine.