

Prilog 2.

Tehnička specifikacija za nabavu usluge provedbe sigurnosnih testiranja aplikacija i usluga

# OPIS USLUGE

Kroz predmet nabave Naručitelj želi ojačati sigurnost svih aplikacija i sustava koje su u produkciji, koji će se ili razviti ili nadograđivati kroz projekte koje Naručitelj provodi, a s ciljem unaprjeđenja sigurnosti samih aplikacija, cjelokupnog ekosustava, sigurnosti podataka kojima ti sustavi raspolažu, ali i krajnjeg korisnika pojedinog sustava. Svrha sigurnosnih (penetracijskih) testiranja je ispitati i provjeriti mehanizme upravljanja podacima, kao i cjelokupnu softversku arhitekturu, ali i softverske pakete koji su dio cjelovitog rješenja u svrhu pronalaska ranjivosti koje je potrebno popraviti prije nego pojedina aplikacija ili sustav budu pušteni u produkcijsko okruženje. Svrha sigurnosne podrške za DNS infrastrukturu jest unaprjeđenje sigurnosti DNS infrastrukture.

# Penetracijski test web aplikacije

## Opis aktivnosti

Penetracijski test web aplikacije obuhvaća sljedeće aktivnosti:

1. Inicijalno prikupljanje informacija o ciljnoj web aplikaciji:

* analiza općenite strukture te pregled sadržaja ciljne web aplikacije
* identifikacija autentikacijskih mehanizama
* prikupljanje informacija o korištenim alatima i tehnologijama (programski jezik, aplikacijski poslužitelj, web poslužitelj, baza podataka i sl.)
* analiza ugrađenih sigurnosnih kontrola (web aplikacijski vatrozid, sigurnosni filteri i sl.)

1. Ručno i automatizirano ispitivanje sigurnosnih propusta specifičnih za web aplikacije koje minimalno uključuje:

* analiza *Cross Site Scripting/Cross Site Forgery* i drugih sličnih ranjivosti
* analiza *SQL/LDAP/Xpath/Command Injection* ranjivosti
* analiza *file upload* ranjivosti
* analiza *common/backup* file ranjivosti
* analiza *Null byte* ranjivosti
* analiza *HTTP response splitting* ranjivosti
* analiza *directory traversal* ranjivosti
* analiza *file inclusion* (*RFI/LFI*) ranjivosti
* analiza *command execution* ranjivosti
* provjera manipulacije korisničkog unosa
* analiza i testiranje kontrole prava pristupa pojedinog korisnika (testiranje mehanizma za autorizaciju)
* provođenje ispitivanja otpornosti zaporki kod servisa koji koriste autentikaciju zaporkom (*eng. brute-force*)
* nedostatci u implementaciji kriptografske zaštite
* nedostatci u zaštiti osjetljivih komunikacija
* provjera upravljanja sjednicama (*eng. session management, session hijacking*)
* identifikacija *information leakage/information disclosure* ranjivosti
* ranjivosti lanca isporuke web aplikacije
* provjera mehanizma rukovanja pogreškama (*eng. error handling*)
* ručno ispitivanje logičkih pogrešaka (ranjivosti nastale zbog pogrešaka u implementaciji poslovne logike aplikacije)
* analiza korištenih paketa i biblioteka u sklopu web aplikacije
  + U slučaju da se radi o web aplikaciji zasnovanoj na LLM-u (*Language Learning Model*), potrebno je web aplikaciju testirati i na sljedeće ranjivosti:
    - *Prompt injection*
    - Nesiguran prikaz izlaznih podatka (eng. *Insecure Output Handling*)
    - Trovanje podataka za treniranje modela (eng. *Training Data Poisonin*g)
    - Uskraćivanje usluge prema korištenom modelu (eng. *Model Denial of Service*)
    - Otkrivanje osjetljivih informacija (eng. *Sensitive Information Disclosure*)
    - Dizajn nesigurnog dodatka (eng. *Insecure Plugin Design*)
    - Davanje pretjeranih odgovora (eng. Excessive Agency)
    - Krađa modela (eng. *Model Teft*)

1. Ispitivanje radnog okruženja web aplikacije

* U slučaju da se radi o aplikaciji koja se poslužuje na virtualnoj mašini, potrebno je sigurnosno ispitati taj poslužitelj
* U slučaju da se radi o kontejneriziranoj aplikaciji, potrebno je sigurnosno ispitati kontejnersku sliku (eng. *container image*) te radno okruženje u kojem se takva aplikacija pokreće kako bi se utvrdilo da sigurnost ove aplikacije ne narušava neka druga aplikacija i vice versa

1. Izrada završnog izvještaja

* izrada dokumentacije s rezultatima testiranja

## Isporuke – Rezultati penetracijskog testa web aplikacije

Rezultat penetracijskog testa web aplikacije je dokumentacija koja se Naručitelju dostavlja u elektroničkom obliku.

Isporučena dokumentacija treba sadržavati „Izvještaj o provedenom ispitivanju sigurnosti“ sa sljedećim informacijama:

* sažetak o provedenom ispitivanju za rukovoditelje
* opseg i metodologija ispitivanja
* sažeti pregled otkrivenih ranjivosti s pripadajućom klasifikacijom
* općenite informacije o ispitanom informacijskom sustavu
* opis svih identificiranih ranjivosti prema razini sigurnosnog rizika
* tehničke preporuke za uklanjanje identificiranih propusta
* ukupna ocjena sigurnosti ispitanog dijela informacijskog sustava

U slučaju da Naručitelj zatraži, Naručitelju će zajedno s izvještajima biti kao rezultat provedenog penetracijskog testa dostavljeni sljedeći zapisi:

* log zapisi o svim provedenim aktivnostima i pokušajima napada,
* tragovi mrežnog prometa koji upućuju na provođenje pojedinih aktivnosti,
* video zapisi s demonstracijom iskorištavanja svih ranjivosti koje omogućuju preuzimanje kontrole nad ciljnim sustavom.

# Penetracijski test web servisa

## Opis aktivnosti

Penetracijski test web servisa obuhvaća sljedeće aktivnosti:

1. Inicijalno prikupljanje informacija o ciljnom web servisu

* identifikacija i analiza dostupnih sučelja web servisa
* identifikacija autentikacijskih mehanizama
* analiza poruka koje se razmjenjuju putem web servisa
* analiza tehnologija i protokola korištenih za implementaciju web servisa
* analiza ugrađenih sigurnosnih kontrola (web aplikacijski vatrozid, sigurnosni filteri i sl.)

1. Ručno i automatizirano ispitivanje sigurnosnih propusta specifičnih za web aplikacije koje minimalno uključuju:

* testing WSDL sučelja
* strukturno XMLS testiranje (*eng. XML Structural Testing*)
* testiranje XML sadržaja (*eng. XML Content-level Testing*)
* testiranje HTTP GET parametara/REST testiranje (*eng. HTTP GET parameters/REST Testing*)
* manipulacija SOAP prilozima (*eng. SOAP attachment*)
* testiranje napada ponavljanjem sadržaja (*eng. Replay Testing*)
* analiza i testiranje kontrole prava pristupa web servisu (testiranje mehanizma za autorizaciju)
* testiranje drugih *endpoint*-a koje web servis može imati implementirano
  + U slučaju da se radi o web servisu zasnovanom na LLM-u (*Language Learning Model*), potrebno je web aplikaciju testirati i na sljedeće ranjivosti:
    - *Prompt injection*
    - Nesiguran prikaz izlaznih podatka (eng. *Insecure Output Handling*)
    - Trovanje podataka za treniranje modela (eng. *Training Data Poisonin*g)
    - Uskraćivanje usluge prema korištenom modelu (eng. *Model Denial of Service*)
    - Otkrivanje osjetljivih informacija (eng. *Sensitive Information Disclosure*)
    - Dizajn nesigurnog dodatka (eng. *Insecure Plugin Design*)
    - Davanje pretjeranih odgovora (eng. Excessive Agency)
    - Krađa modela (eng. *Model Teft*)

1. Ispitivanje radnog okruženja web servisa

* U slučaju da se radi o servisu koji se poslužuje na virtualnoj mašini, potrebno je sigurnosno ispitati taj poslužitelj
* U slučaju da se radi o kontejneriziranoj aplikaciji, potrebno je sigurnosno ispitati kontejnersku sliku (eng. *container image*) te radno okruženje u kojemu se takav servis pokreće kako bi se utvrdilo da sigurnost ovog servisa ne narušava neka druga aplikacija i vice versa

1. Izrada završnog izvještaja

* izrada dokumentacije s rezultatima testiranja

## Isporuke - Rezultati penetracijskog testiranja web servisa

Rezultat penetracijskog testa web servisa je dokumentacija koja se Naručitelju dostavlja u elektroničkom i papirnatom obliku.

Isporučena dokumentacija treba sadržavati „Izvještaj o provedenom ispitivanju sigurnosti“ sa sljedećim informacijama:

* sažetak o provedenom ispitivanju za rukovoditelje,
* opseg i metodologija ispitivanja,
* sažeti pregled otkrivenih ranjivosti s pripadajućom klasifikacijom,
* općenite informacije o ispitanom informacijskom sustavu,
* opis svih identificiranih ranjivosti prema razini sigurnosnog rizika,
* tehničke preporuke za uklanjanje identificiranih propusta,
* ukupna ocjena sigurnosti ispitanog dijela informacijskog sustava.

U slučaju da Naručitelj zatraži, Naručitelju će zajedno s izvještajima kao rezultat provedenog penetracijskog testa biti dostavljeni slijedeći zapisi:

* log zapisi o svim provedenim aktivnostima i pokušajima napada,
* tragovi mrežnog prometa koji upućuju na provođenje pojedinih aktivnosti,
* video zapisi s demonstracijom iskorištavanja svih ranjivosti koje omogućuju preuzimanje kontrole nad ciljnim sustavom.

# Penetracijski test mobilnih aplikacija

## Opis aktivnosti

Penetracijski test mobilnih aplikacija obuhvaća sljedeće aktivnosti:

1. Inicijalno prikupljanje informacija o ciljnoj mobilnoj aplikaciji

* analiza općenite strukture te pregled sadržaja ciljne mobilne aplikacije
* identifikacija autentikacijskih mehanizama
* prikupljanje informacija o korištenim alatima i tehnologijama (programski jezik, aplikacijski poslužitelj, web poslužitelj, klijentska aplikacija i sl.)
* analiza ugrađenih sigurnosnih kontrola

1. Ručno i automatizirano ispitivanje sigurnosnih propusta specifičnih za mobilne aplikacije koje minimalno uključuje:

* analiza Cross Site Scripting/Cross Site Forgeryi drugih sličnih ranjivosti,
* analiza *SQL/LDAP/Xpath/Command Injection* ranjivosti,
* analiza *file upload* ranjivosti,
* analiza *common/backup file* ranjivosti,
* analiza *Null byte* ranjivosti,
* analiza *HTTP response splitting* ranjivosti,
* analiza *directory traversal* ranjivosti,
* analiza *file inclusion* (RFI/LFI) ranjivosti,
* analiza *command execution* ranjivosti,
* provjera manipulacije korisničkog unosa (eng. *URL manipulation*),
* provođenje ispitivanja otpornosti zaporki kod servisa koji koriste autentikaciju zaporkom (eng*. brute-force*),
* nedostatci u implementaciji kriptografske zaštite,
* nedostatci u zaštiti osjetljivih komunikacija,
* analiza i testiranje kontrole prava pristupa pojedinog korisnika (testiranje mehanizma za autorizaciju)
* provjera upravljanja sjednicama (eng. *session management*, *session hijacking*),
* identifikacija *information leakage*/*information disclosure* ranjivosti,
* provjera mehanizma rukovanja pogreškama (eng. *error handling*),
* ručno ispitivanje logičkih pogrešaka (ranjivosti nastale zbog pogrešaka u implementaciji poslovne logike aplikacije).
  + U slučaju da se radi o mobilnoj aplikaciji zasnovanoj na LLM-u (*Language Learning Model*), potrebno je web aplikaciju testirati i na sljedeće ranjivosti:
    - *Prompt injection*
    - Nesiguran prikaz izlaznih podatka (eng. *Insecure Output Handling*)
    - Trovanje podataka za treniranje modela (eng. *Training Data Poisonin*g)
    - Uskraćivanje usluge prema korištenom modelu (eng. *Model Denial of Service*)
    - Otkrivanje osjetljivih informacija (eng. *Sensitive Information Disclosure*)
    - Dizajn nesigurnog dodatka (eng. *Insecure Plugin Design*)
    - Davanje pretjeranih odgovora (eng. Excessive Agency)
    - Krađa modela (eng. *Model Teft*)

1. Ispitivanje sigurnosti mobilne aplikacije:

* testiranje funkcionalnosti aplikacije i mrežne komunikacije,
* testiranje sigurnosti podataka u pohrani,
* reverzni inženjering (*eng. reverse engineering*) aplikacije,
* identifikacija i verifikacija ranjivosti.

1. Izrada završnog izvještaja

* Izrada dokumentacije s rezultatima testiranja

## Isporuke – Rezultati penetracijskog testiranja mobilne aplikacije

Rezultat penetracijskog testa mobilne aplikacije je dokumentacija koja se Naručitelju dostavlja u elektroničkom i papirnatom obliku.

Isporučena dokumentacija treba sadržavati „Izvještaj o provedenom ispitivanju sigurnosti“ sa sljedećim informacijama:

* sažetak o provedenom ispitivanju za rukovoditelje,
* opseg i metodologija ispitivanja,
* sažeti pregled otkrivenih ranjivosti s pripadajućom klasifikacijom,
* općenite informacije o ispitanom informacijskom sustavu,
* opis svih identificiranih ranjivosti prema razini sigurnosnog rizika,
* tehničke preporuke za uklanjanje identificiranih propusta,
* ukupna ocjena sigurnosti ispitanog dijela informacijskog sustava.

U slučaju da Naručitelj zatraži, Naručitelju će zajedno s izvještajima kao rezultat provedenog penetracijskog testa biti dostavljeni sljedeći zapisi:

* log zapisi o svim provedenim aktivnostima i pokušajima napada,
* tragovi mrežnog prometa koji upućuju na provođenje pojedinih aktivnosti,
* video zapisi s demonstracijom iskorištavanja svih ranjivosti koje omogućuju preuzimanje kontrole nad ciljnim sustavom.

# Penetracijski test infrastrukturnog dijela informacijskog sustava izloženog internetu

## Opis aktivnosti

Penetracijsko testiranje obuhvaća sljedeće aktivnosti:

1. Penetracijsko testiranje infrastrukturnog dijela informacijskog sustava (generičko)
2. Penetracijsko testiranje infrastrukturnog dijela informacijskog sustava po specifičnim scenarijima

Obuhvaćeno je testiranje:

* mrežno-komunikacijske opreme kroz koju je ostvarena veza na Internet
* vatrozidne zaštite i druge sigurnosne uređaje
* poslužitelja elektroničke pošte uključujući „web mail“ pristup
* javno dostupnih servisa
* aplikacijskih poslužitelja
* sustava za upravljanje kontejneriziranim aplikacijama (Docker, Podman, Kubernetes, OKD…)
* sustava za upravljanje virtualnim strojevima
* imeničkih direktorija (*Active Directory*, *LDAP*) te poslužitelja na kojima se nalaze
* testiranje sustava koji se koristi kao lanac isporuke aplikacija
* svih ostalih usluga i poslužitelja dostupnih s internet mreže

Penetracijsko testiranje provodi se korištenjem jedne od javno dostupnih metodologija penetracijskog testiranja što minimalno obuhvaća:

* prikupljanje informacija o sustavu
* mapiranje mreže
* penetracija informacijskog sustava
* dobivanje pristupa i povećanje ovlasti
* daljnje popisivanje objekata
* kompromitacija sustava
* održavanje pristupa i skrivanje tragova

1. Izrada završnog izvještaja

* izrada dokumentacije s rezultatima testiranja

## Isporuke – Rezultati penetracijskog testa infrastrukturnog dijela informacijskog sustava izloženog internetu

## Rezultat penetracijskog testiranja infrastrukturnog dijela sustava je dokumentacija koja se Naručitelju dostavlja u elektroničkom i papirnatom obliku.

Isporučena dokumentacija treba sadržavati „Izvještaj o provedenom ispitivanju sigurnosti“ sa sljedećim informacijama:

* sažetak o provedenom ispitivanju za rukovoditelje,
* opseg i metodologija ispitivanja,
* sažeti pregled otkrivenih ranjivosti s pripadajućom klasifikacijom,
* općenite informacije o ispitanom informacijskom sustavu,
* opis svih identificiranih ranjivosti prema razini sigurnosnog rizika,
* tehničke preporuke za uklanjanje identificiranih propusta,
* ukupna ocjena sigurnosti ispitanog dijela informacijskog sustava.

Naručitelju će zajedno s izvještajima kao rezultat provedenog penetracijskog testa biti dostavljeni sljedeći zapisi:

* log zapisi o svim provedenim aktivnostima i pokušajima napada,
* tragovi mrežnog prometa koji upućuju na provođenje pojedinih aktivnosti,
* video zapisi s demonstracijom iskorištavanja svih ranjivosti koje omogućuju preuzimanje kontrole nad ciljnim sustavom.

## Naručitelj se obvezuje Izvršitelju izvršiti plaćanje u roku od 30 (trideset) dana od zaprimanja računa koji je ispostavljen na temelju ovjerenog primopredajnog zapisnika i u skladu s pravilima financijskog poslovanja korisnika Državnog proračuna.

# Sigurnosna podrška za DNS infrastrukturu

Sigurnosna podrška za DNS infrastrukturu se sastoji od sljedećih aktivnosti:

5.1 Detekcija zloupotrebe .hr domena

5.2 Red teaming

5.3 Modeliranje prijetnji

## Detekcija zloupotrebe .hr domena

Ponuditelj u svrhu detekcije zloupotrebe .hr domena pruža Naručitelju sljedeće usluge:

* nadogradnja trenutnih alata za detekciju zloupotrebe .hr domene
* razvoj novih alata za automatiziranu detekciju zloupotrebe .hr domene koji obuhvaćaju slučajeve kompromitacije koji nisu obuhvaćeni već postojećim alatima
* implementacija novo razvijenih alata u postojeću aplikaciju Naručitelja

## Red teaming

Ponuditelj će u tijeku trajanja ugovora izvršiti jednu red teaming vježbu za DNS infrastrukturu. Prije provođenja vježbe, Ponuditelj će u Naručiteljem dogovoriti metode koje će biti dopuštene tijekom provođenja vježbe. Navedeno će se odnositi na pokušaj kompromitacije dogovorenih dijelova DNS infrastrukture internom ili vanjskom red team vježbom.

## Modeliranje prijetnji

Ponuditelj će na osnovu postojeće dokumentacije i informacija o DNS infrastrukturi, njenom održavanju i načinu na koji su dodijeljeni pristupi određenim segmentima odraditi analizu rizika njenih komponenti. Kao isporučevinu navedene aktivnosti će izraditi izvješće s popisom mogućih prijetnji, procijenjenoj vjerojatnosti i preporukama za mitigaciju istih.

## Isporuke – Rezultati aktivnosti sigurnosne podrške za DNS infrastrukturu

Isporučena dokumentacija treba sadržavati izvještaje o provedenim aktivnostima od 5.1. do 5.3. sa sljedećim informacijama:

* sažetak o provedenom ispitivanju za rukovoditelje,
* opseg i metodologija detekcije zloupotrebe/red team vježbe/modeliranja prijetnji,
* sažeti pregled provedenih aktivnosti,
* općenite informacije o aktivnostima,
* opis svih identificiranih ranjivosti prema razini sigurnosnog rizika,
* tehničke preporuke za uklanjanje identificiranih propusta,
* ukupna ocjena sigurnosti DNS infrastrukture koja je bila predmet provedenih aktivnosti.

## Naručitelj se obvezuje Izvršitelju izvršiti plaćanje u roku od 30 (trideset) dana od zaprimanja računa koji je ispostavljen na temelju ovjerenog primopredajnog zapisnika i u skladu s pravilima financijskog poslovanja korisnika Državnog proračuna.

# Napomene

Ponuditelj i Naručitelj će preko osoba ovlaštenih za izvršenje Ugovora dogovarati datum početka i završetka pojedinih testiranja ovisno o kompleksnosti aplikacije. Ponuditelj je dužan osigurati resurse koji će omogućiti istovremeno provođenje tri testiranja te početak testiranja najkasnije 7 dana od potpisa pojedinačnog Ugovora.

Konkretne rokove završetka pojedinog testiranja utvrdit će Naručitelj u Pozivu na dostavu ponuda za sklapanje pojedinačnog ugovora na temelju Okvirnog sporazuma, a navedeni rok završetka će biti primjeren i ovisit će o tipu testiranja, složenosti, veličini i kompleksnosti aplikacije.

Naručitelj ima pravo, ako testiranje nije započelo, promijeniti specifikaciju pojedinog testiranja (primjerice aplikaciju koja će se testirati), u okviru ugovorenog troškovnika.

Ako Naručitelj, zbog specifičnih okolnosti, odustane od pojedinog termina testiranja prije početka testiranja, ovlaštene osobe Naručitelja i Ponuditelja potpisat će o tome Zapisnik.

Ako Naručitelj planira implementirati neke mehanizme zaštite (primjerice *Web application firewall*), testiranje će se uobičajeno provoditi na način da se prvo testira aplikacija bez uključene zaštite (*Web application firewall),* a nakon toga ponovit će se testiranje pronađenih ranjivosti s uključenom zaštitom. Sva isporučena dokumentacija mora sadržavati opis pronađenih ranjivosti sa i bez uključenih dodatnih mehanizama zaštite (*Web Application Firewall*). Ponuditelj se obvezuje navedeni način testiranja uključiti u jedinične cijene stavki Troškovnika od 1.1. do 4.2.

Isporučena dokumentacija definirana u točkama 1.2, 2.2, 3.2, 4.2 i 5.4. mora sadržavati potpise stručnjaka koji su sudjelovali u pojedinom testiranju.

Svi izvještaji koji su predmet ugovora o javnoj nabavi trebaju biti potpisani fizičkim ili digitalnim potpisom od strane stručnjaka koji su na njemu radili.