Hrvatska akademska i istraživačka mreža - CARNET

**Prilog 1. SPECIFIKACIJA PREDMETA NABAVE**

Nabava usluge provedbe sigurnosnih testiranja aplikativnih rješenja korištenih u okviru projekta e-Škole

Sadržaj

[1. UVOD 4](#_Toc61607612)

[1.1. Kontekst predmeta nabave 4](#_Toc61607613)

[1.2. Svrha predmeta nabave 5](#_Toc61607614)

[2. SPECIFIKACIJA USLUGE PROVEDBE SIGURNOSNIH TESTIRANJA APLIKATIVNIH RJEŠENJA KORIŠTENIH U OKVIRU PROJEKTA e-Škole 6](#_Toc61607615)

[2.1. Opis aplikativnih rješenja 7](#_Toc61607616)

[2.1.1. CARNET aero 7](#_Toc61607617)

[2.1.2. CARNET delta 7](#_Toc61607618)

[2.1.3. CARNET kapa 7](#_Toc61607619)

[2.1.4. CARNET mikro 7](#_Toc61607620)

[2.1.5. CARNET omega 8](#_Toc61607621)

[2.1.6. CARNET sigma 8](#_Toc61607622)

[2.1.7. CARNET fi 8](#_Toc61607623)

[2.1.8. Sustav za upravljanje API pozivima 9](#_Toc61607624)

[3. OPIS USLUGE 10](#_Toc61607625)

[3.1. Penetracijski test web aplikacije 10](#_Toc61607626)

[3.1.1. Opis aktivnosti 10](#_Toc61607627)

[3.1.2. Kompleksnost aplikacije 11](#_Toc61607628)

[3.1.3. Isporuke – Rezultati penetracijskog testa web aplikacije 11](#_Toc61607629)

[3.2. Penetracijski test web servisa 11](#_Toc61607630)

[3.2.1. Opis aktivnosti 11](#_Toc61607631)

[3.2.2. Kompleksnost web servisa 12](#_Toc61607632)

[3.2.3. Isporuke - Rezultati penetracijskog testiranja web servisa 12](#_Toc61607633)

[3.3. Penetracijski test mobilnih aplikacija 13](#_Toc61607634)

[3.3.1. Opis aktivnosti 13](#_Toc61607635)

[3.3.2. Kompleksnost aplikacije 14](#_Toc61607636)

[3.3.3. Isporuke – Rezultati penetracijskog testiranja mobilne aplikacije 14](#_Toc61607637)

[3.4. Penetracijski test *klijent – server* aplikacija 15](#_Toc61607638)

[3.4.1. Opis aktivnosti 15](#_Toc61607639)

[3.4.2. Kompleksnost aplikacije 15](#_Toc61607640)

[3.4.3. Isporuke – Rezultati penetracijskog testiranja *klijent – server* aplikacije 16](#_Toc61607641)

[3.5. Penetracijski test infrastrukturnog dijela informacijskog sustava izloženog internetu 16](#_Toc61607642)

[3.5.1. Opis aktivnosti 16](#_Toc61607643)

[3.5.2. Isporuke – Rezultati penetracijskog testa infrastrukturnog dijela informacijskog sustava izloženog internetu 17](#_Toc61607644)

[3.6. Testiranje performansi 18](#_Toc61607645)

[3.6.1. Opis aktivnosti 18](#_Toc61607646)

[3.6.2. Kompleksnost aplikacije 18](#_Toc61607647)

[3.6.3. Isporuke - Rezultati testiranja performansi 19](#_Toc61607648)

[3.7. Testiranje otpornosti sustava na DoS i DDoS napade 19](#_Toc61607649)

[3.7.1. Opis aktivnosti 19](#_Toc61607650)

[3.7.2. Kompleksnost aplikacije 20](#_Toc61607651)

[3.7.3. Isporuke – Rezultati testiranja otpornosti sustava na DoS i DDoS napade 20](#_Toc61607652)

[3.8. Savjetovanje 20](#_Toc61607653)

[3.9. Napomene 20](#_Toc61607654)

# UVOD

## 1.1. Kontekst predmeta nabave

Predmetni postupak javne nabave provodi se u sklopu programa „e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće“ (dalje u tekstu: Program e-Škole). Opći cilj Programa e-Škole je pridonijeti jačanju kapaciteta osnovnoškolskog i srednjoškolskog obrazovnog sustava s ciljem osposobljavanja učenika za tržište rada, daljnje školovanje i cjeloživotno učenje.

Program e-Škole se provodi kroz sljedeće projekte:

* Pilot projekt „e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot -projekt)" koji se provodio u razdoblju od 1. ožujka 2015. godine do 31. kolovoza 2018. godine u koji je bila uključena 151 škola diljem Hrvatske,
* Druga faza Programa e-Škole koja se provodi od 1. rujna 2018. godine u planiranom trajanju do kraja 2022. godine., a u koju su uključene sve škole u Hrvatskoj financirane iz državnog proračuna

Nositelj projekata je Hrvatska akademska i istraživačka mreža – CARNET (dalje u tekstu: Naručitelj ili CARNET). Projekti se financiraju sredstvima iz Europskog fonda za regionalni razvoj (dalje u tekstu: EFRR) u sklopu Operativnog programa ''Konkurentnost i kohezija'' 2014. - 2020. (OPKK) i iz Europskog socijalnog fonda (dalje u tekstu: ESF) u sklopu Operativnog programa ''Učinkoviti ljudski potencijali'' 2014. – 2020. (dalje u tekstu: OPULJP) te je iz tog razloga svaki projekt podijeljen na Projekt A (sufinanciran sredstvima EFRR-a) i Projekt B (sufinanciran sredstvima ESF-a).

Predmetni postupak javne nabave provodi se u sklopu druge faze Programa e-Škole. Ugovor o dodjeli bespovratnih sredstava za drugu fazu provedbe projekta sklopljen je 28. kolovoza 2020. godine, a njegovo predviđeno trajanje je do 31. prosinca 2022. godine. Predviđena vrijednost velikog projekta je oko 177.500.000,00 eura.

E-Škole su digitalno zrele škole, spojene brzom internet vezom, visoko opremljene adekvatnom IKT opremom, te visokom razinom automatizacije poslovnih i edukacijskih procesa. Zaposlenici u takvim školama su digitalno kompetentni, a učenici se potiču i uče da sami postanu digitalno kompetentni. Zaposlenici i učenici svakodnevno koriste IKT opremu u svrhu obrazovanja, uključujući, ali ne i ograničavajući se, na korištenje edukacijskih aplikacija i digitalnih obrazovnih sadržaja, osiguravajući na taj način da današnji učenici postanu konkurentni na tržištu rada sutrašnjice.

Nastavno na navedeno, u digitalno zrelim školama adekvatna uporaba informacijske i komunikacijske tehnologije (dalje u tekstu: IKT) doprinosi sljedećim važnim aspektima: učinkovitom i transparentnom upravljanju školom, razvoju digitalno kompetentnih nastavnika spremnijih za primjenu inovacija u vlastitim pedagoškim praksama i razvoju digitalno kompetentnih učenika spremnijih za nastavak školovanja i konkurentnijima na tržištu rada (indirektni cilj).

## 1.2. Svrha predmeta nabave

U svrhu unaprjeđenja obrazovnih procesa u školama i podizanja digitalne zrelosti škola, u okviru projekta razvijaju se nove i unaprjeđuju postojeće e-usluge. Prema sigurnosnoj politici CARNET-a svi programski sustavi nastali u CARNET-u ili proizvedeni za CARNET moraju biti izrađeni prema principima sigurnog programiranja, i takvi da je sigurnost ugrađena u njih od samog dizajna sustava. Prije stavljanja programskog sustava u produkciju potrebno je provesti sigurnosno testiranje s ciljem pronalaska sigurnosnih propusta, a programski sustav se ne smije staviti u produkciju ako nisu ispravljani prethodno pronađeni sigurnosni propusti.

Svrha nabave je odabrati Ponuditelja koji će za vrijeme trajanja projekta provoditi sigurnosna testiranja aplikativnih rješenja razvijenih i korištenih u sklopu projekta e-Škole, a s ciljem osiguravanja visoke razine sigurnosti svih dionika e-Škole projekta te očuvanjem povjerljivosti, cjelovitosti i raspoloživosti podataka koje se nalaze u spomenutim aplikativnim rješenjima.

1. SPECIFIKACIJA USLUGE PROVEDBE SIGURNOSNIH TESTIRANJA APLIKATIVNIH RJEŠENJA KORIŠTENIH U OKVIRU PROJEKTA e-Škole

Predmet ove nabave je vanjska usluga provođenja sigurnosnih testiranja aplikativnih rješenja razvijenih i korištenih u okviru projekta e-Škole, izrada pripadajućih izvještaja te savjetodavne usluge u području računalne sigurnosti i sigurnosnih testiranja.

Planirano trajanje ugovora je od potpisa ugovora do završetka provedbe projekta, odnosno 31. prosinca 2022. godine.

Za provedbu ovog ugovora Naručitelj će tražiti angažman stručnjaka za koje je poželjno da posjeduju neki od certifikata prema tablici u Prilogu 3 – Tehnički stručnjaci.

U sklopu ove nabave obuhvaćeno je osam aplikativnih rješenja prikazanih u Tablici. Za svako aplikativno rješenje proveden je postupak određivanja kompleksnosti prema opisu iz Poglavlja 3 ovog dokumenta. S obzirom da su pojedina aplikativna rješenja u fazi odabira Izvođača ili u ranoj fazi razvoja ili nadogradnje kompleksnost je određena sukladno setu podataka koji su trenutno dostupni te se stvarno stanje u konačnici može razlikovati. Određena aplikativna rješenja sastoje se od više zasebnih komponenti međusobno povezanih u cjelinu. Dodatno treba napomenuti da se tehnologije razlikuju od aplikacije do aplikacije budući da razvoj rade različiti Izvođači.

|  |  |  |  |
| --- | --- | --- | --- |
| R.br. | Naziv | Vrsta | Kompleksnost |
| 1. | CARNET aero | Web aplikacija + web servis + mobilna aplikacija\* | 3 |
| 2. | CARNET delta | Web aplikacija + web servis | 3 |
| 3. | CARNET kapa | Web aplikacija + web servis | 3 |
| 4. | CARNET mikro | Web aplikacija + web servis | 3 |
| 5. | CARNET omega | Web aplikacija + web servis | 3 |
| 6. | CARNET sigma | Web aplikacija + web servis | 3 |
| 7. | CARNET fi[[1]](#footnote-2) | N/A | N/A |
| 8. | Sustav za upravljanje API pozivima[[2]](#footnote-3) | N/A | N/A |

Priložena tablica služi da se stekne što bolji uvid u opseg poslova koje će odabrani Ponuditelj biti dužan izvršiti u prethodno definiranom trajanju ugovora. Pojedina aplikativna rješenja će biti puštana u produkciju u fazama, po završetku većeg seta funkcionalnosti, zbog toga će određena aplikativna rješenja biti potrebno testirati u nekoliko iteracija. Zbog toga postoji mogućnost da će takvo parcijalno testiranje aplikativnog rješenja imati manju kompleksnost od trenutne procjene kompletnog aplikativnog rješenja. Također se nakon svake odrađene iteracije očekuje provjera ispravljenih sigurnosnih propusta nakon što vlasnik aplikativnog rješenja primjeni ispravke pronađenih sigurnosnih propusta.

## Opis aplikativnih rješenja

### CARNET aero

Cloud i web aplikacije sa osnovnim funkcionalnostima za prihvat i prikaz podataka sa senzora temperature, vlage i CO2 i nabavka dva kompleta za praćenje kvalitete zraka od kojih svaki uključuje centralnu jedinicu i senzor za praćenje temperature, vlage i CO2

### CARNET delta

Aplikacija za analitiku učenja. Namijenjena je učenicima osnovnih i srednjih škola, njihovim roditeljima, školskim djelatnicima – učiteljima, nastavnicima, razrednicima, ravnateljima i stručnim službama u školama (psiholozima, pedagozima, stručnjacima edukacijsko-rehabilitacijskog profila i drugima).

Aplikacija nudi napredni pregled analitičkih podataka koji se prikupljaju kroz postojeće sustave, najvećim dijelom iz e-Dnevnika, ali i drugih sustava.

### CARNET kapa

Sustav za upravljanje GDPR relevantnim zahtjevima ispitanika, privolama i podacima kako pojedinaca i ustanova u primarnom i sekundarnom segmentu obrazovnog sustavu RH tako i visokoškolskih ustanova iz akademske zajednice, korištenjem modernih, automatiziranih i efikasnih koncepata.

### CARNET mikro

Aplikacija za upravljanje i nadzor lokalnih mreža škola omogućit će stručnjaku tehničke podrške pojednostavljeni prikaz stanja lokalne mreže ustanove za koju je nadležan te olakšano upravljanje školskom lokalnom računalnom mrežom.

Aplikacija se sastoji od tri komponente: aplikacija za upravljanje i nadzor LAN-a škola, Captive Portal servis i sustav za aktivni monitoring LAN-a škola.

### CARNET omega

Sustav za dodjeljivanje infrastrukturnih resursa i upravljanje udomljavanjem CARNET-ovih usluga u sklopu koje se svim školama, njihovim zaposlenicima, nastavnicima i učenicima otvara besplatan elektronički identitet i e-mail adresa, a školama je omogućena i izrada web stranica. Cilj je uspostaviti hosting uslugu nove generacije na najnovijim tehnologijama, optimiziranom potrošnjom resursa, unaprijeđenom i unificiranom administracijom od strane korisnika i CARNET-a.

CARNET omega sustav se sastoji od više informacijskih podsustava koji zajedno čine integralnu cjelinu:

1. Središnja administratorska aplikacija za upravljanje CARNET omega podsustavima
* središnje mjesto preko kojeg administratori pristupaju svojim uslugama i upravljaju resursima i svim podsustavima CARNET omega za svoju domenu
1. Upravljani sustav elektroničke pošte korisnika
2. Sustav za upravljanje sadržajem mrežnih (*web*) stranica (*Content Management System* - CMS)
3. Sustav za upravljanje DNS zapisima
* za ustanove osnovnih i srednjih škola u Republici Hrvatskoj
1. Sustav za upravljanje alatima i uslugama u javnom oblaku za krajnje korisnike (kao npr. Microsoft 365 ili Google G Suite)
2. Upravljani sustav za dijeljenje dokumenata (*fileshare* sustav) i upravljanje dokumentima (DMS)
3. Sustav za upravljanje računalnom infrastrukturom dostupnom na zahtjev
* komponenta sustava koja korisnicima omogućuje samostalnu izradu i administraciju virtualnih poslužitelja

### CARNET sigma

Sustav za informatizaciju poslovanja ustanova (SIGMA) (ERP sustava izgrađenog u okviru pilot projekta) u svrhu informatizacije preostalih poslovnih procesa u školama (vezanih uz poslovanje škole kao pravnog subjekta).

### CARNET fi

Obuhvaća implementaciju autentikacijske metode prema FIDO2 specifikaciji dostupnoj na adresi https://fidoalliance.org/specifications/ (dalje u tekstu FIDO2 autentikacija) kao jedne od metoda koje se mogu koristiti u scenariju višestupanjske autentikacije u sustavu AAI@EduHr. Ta metoda autentikacije treba se moći koristiti i kao jedina metoda autentikacije (umjesto korisničke oznake i lozinke u scenariju jednostupanjske autentikacije).

Implementacija treba osigurati mogućnost korištenja vanjskih uređaja (FIDO sigurnosnih ključeva, mobilnih uređaja) za autentikaciju putem operativnih sustava i internet preglednika koji podržavaju FIDO2 putem USB, NFC i Bluetooth načina povezivanja.

Sustav treba omogućiti postavljanje i korištenje tog faktora kao jedinog (paswordless), kao drugi faktor ili kao jedan od više faktora u procesu autentikacije korisnika. Za uređaje koji podržavaju samo FIDO U2F očekuje se podrška u smislu mogućnosti postavljanja i korištenja tog faktora kao drugog faktora.

### Sustav za upravljanje API pozivima

Sustav za upravljanje API pozivima kojim se osigurava jednostavnije upravljanje API pozivima s jednog mjesta, jednostavnije upravljanje pravima pristupa nad pojedinim servisima, povećanje sigurnosti uvođenjem novog sloja među aplikacijama i mogućnost dizajniranja novih API poziva na samom sustavu uporabom postojećih pozadinskih sustava, razmjenom datoteka ili izvorom podataka iz relacijske baze podataka. Nadogradnjom sustava se implementirani sustav integrira s novim servisima i uslugama, kao i dograđuje s novim tehnološkim rješenjima.

# OPIS USLUGE

# 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 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
* 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)
1. Izrada završnog izvještaja
* izrada dokumentacije s rezultatima testiranja

## Kompleksnost aplikacije

|  |  |  |
| --- | --- | --- |
| **Kompleksnost 1**  | **Kompleksnost 2**  | **Kompleksnost 3**  |
| - do 10 interaktivnih web formi u aplikaciji- bez web servisa - 1 rola - vremenski rok za testiranje: **5 radnih dana**  | - od 10 do 30 interaktivnih web formi u aplikaciji - do 5 rola - vremenski rok za testiranje: **10 radnih dana**  | - više od 30 interaktivnih web formi u aplikaciji - više od 5 rola - vremenski rok za testiranje: **15 radnih dana** |

## Isporuke – Rezultati penetracijskog testa web aplikacije

Rezultat penetracijskog testa web 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

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(OWASP-WS-002)
* 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*)
1. Izrada završnog izvještaja
* izrada dokumentacije s rezultatima testiranja

## Kompleksnost web servisa

|  |  |  |
| --- | --- | --- |
| **Kompleksnost 1**  | **Kompleksnost 2**  | **Kompleksnost 3**  |
| - broj metoda: do 20 - autentikacija: korisničko ime/zaporka - enkripcija: osnovna (bez enkripcije/enkriptiran komunikacijski kanal) - vremenski rok za testiranje: **5 radnih dana** | - broj metoda: do 75 - autentikacija: certifikati, pametne kartice itd. - enkripcija: napredna (enkripcija podataka, digitalni potpisi itd.) - vremenski rok za testiranje: **10 radnih dana** | - broj metoda: više od 75 - autentikacija: certifikati, pametne kartice itd. - enkripcija: napredna (enkripcija podataka, digitalni potpisi itd.) - vremenski rok za testiranje: **15 radnih dana** |

## 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.

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 web aplikacije koje minimalno uključuje:
* analiza Cross Site Scripting/Cross Site Forgeryi drugih sličnih ranjivosti,
* analiza *SQL/LDAP/Xpath 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,
* 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),
1. Ispitivanje sigurnosti mobilne aplikacije koje minimalno uključuje:
* 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

## Kompleksnost aplikacije

|  |  |  |
| --- | --- | --- |
| **Kompleksnost 1**  | **Kompleksnost 2**  | **Kompleksnost 3**  |
| - Android ili Windows Phone aplikacija koja ne komunicira s poslužiteljem - Android ili Windows Phone aplikacija koja poziva do 10 metoda kroz nekriptirani kanal ili kroz kriptirani kanal bez certificate pinninga ,bez autentikacije ili korištenjem korisničkog imena i zaporke - vremenski rok za testiranje: **5 radnih dana** | - iPhone aplikacija - Aplikacija koja poziva do 30 metoda - Korištenje naprednih autentikacijskih mehanizama (OTP generator, klijentski certifikati, formalni proces „aktivacije“ aplikacije) - Digitalno potpisivanje ili korištenje challenge-response mehanizama za osjetljive upite - vremenski rok za testiranje: **12 radnih dana** | - Korištenje naprednih komunikacijskih tehnologija (npr. NFC) - Obfuscirana aplikacija - Korištenje anti-debug tehnika - Aplikacija koja poziva više od 35 metoda - Korištenje vlastitog kriptografskog protokola za komunikaciju s poslužiteljem (enkripcija prometa neovisna o SSL protokolu, cert pinning) - vremenski rok za testiranje: **16 radnih dana** |

## 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.

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 *klijent – server* aplikacija

## Opis aktivnosti

Penetracijski test *klijent – server* aplikacije obuhvaća sljedeće aktivnosti:

1. Inicijalno prikupljanje informacija o ciljnoj *klijent – server* aplikaciji
* analiza općenite strukture te pregled sadržaja ciljne *klijent – server* aplikacije
* identifikacija autentikacijskih mehanizama
* prikupljanje informacija o korištenim alatima i tehnologijama (programski jezik, aplikacijski pristupni sloj, baza podataka i sl.)
* analiza ugrađenih sigurnosnih kontrola (aplikacijski vatrozid, sigurnosni filteri i sl.)
1. Ručno i automatizirano ispitivanje sigurnosnih propusta specifičnih za *klijent – server* aplikacije koje minimalno uključuje:
* analiza *SQL/LDAP* ranjivosti
* analiza *file upload* ranjivosti
* analiza *common/backup* file ranjivosti
* analiza *Null byte* ranjivosti
* analiza *file inclusion (RFI/LFI)* ranjivosti
* analiza *command execution* ranjivosti
* analiza *reverse engineering* ranjivosti
* provjera manipulacije korisničkog unosa
* 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
* provjera mehanizma rukovanja pogreškama (*eng. error handling*)
* ručno ispitivanje logičkih pogrešaka (ranjivosti nastale zbog pogrešaka u implementaciji poslovne logike aplikacije)
1. Izrada završnog izvještaja
* Izrada dokumentacije s rezultatima testiranja

## Kompleksnost aplikacije

|  |  |
| --- | --- |
| **Kompleksnost 1**  | **Kompleksnost 2**  |
| - do 30 interaktivnih formi u aplikaciji - do 5 rola - vremenski rok za testiranje: **10 radnih dana**  | - više od 30 interaktivnih formi u aplikaciji - više od 5 rola- vremenski rok za testiranje: **15 radnih dana**  |

## Isporuke – Rezultati penetracijskog testiranja *klijent – server* aplikacije

Rezultat penetracijskog testa *klijent - server* 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.

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 infrastrukturnog dijela informacijskog sustava izloženog internetu

Napomena:

Naručiteljeva infrastruktura je zasnovana na OKD4 platformi (*eng. the community distribution of Red Hat OpenShift Kubernetes platform*).

## Opis aktivnosti

Penetracijsko testiranje obuhvaća sljedeće aktivnosti:

1. Penetracijsko testiranje infrastrukturnog dijela informacijskog sustava

Obuhvaćeno je testiranja minimalno:

* 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
* 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.

# Testiranje performansi

Napomena:

Naručiteljeva infrastruktura je zasnovana na OKD4 platformi (*eng. the community distribution of Red Hat OpenShift Kubernetes platform*).

## Opis aktivnosti

Ispitivanje performansi obuhvaća sljedeće aktivnosti:

1. Testiranje performansi minimalno uključuje:
* analiza arhitekture sustava
* definiranje testnih scenarija u dogovoru s Naručiteljem
* simulacija povećanog opterećenja, odnosno istovremenog pristupa većeg broja korisnika prema prethodno utvrđenim scenarijima
* analiza i praćenje ponašanja aplikacije pod povećanim opterećenjem
* analizu odziva web poslužitelja i ostalih komponenti sustava pri povećanim opterećenjem
* identifikaciju „uskih grla“ ciljnog sustava
* izradu završnog izvještaja s preporukama za unapređenje performansi sustava, što po potrebi uključuje preporuke za:
	+ unapređenje sklopovlja
	+ izmjene u postavkama pojedinih komponenti sustava
	+ izmjene ili nadogradnje na aplikativnoj razini
	+ optimizaciju ili povećanje propusnosti komunikacijskog kanala
1. Izrada završnog izvještaja
* izrada dokumentacije s rezultatima testiranja

## Kompleksnost aplikacije

|  |  |  |
| --- | --- | --- |
| **Kompleksnost 1**  | **Kompleksnost 2**  | **Kompleksnost 3**  |
| - autentikacija: ne koristi se - broj računala s kojih se provodi ispitivanje: 1 - broj fizičkih ili logičkih poslužitelja: do 2 - korištenje jednostavnih web formi bez međusobne ovisnosti između pojedinih koraka - prikupljanje performansnih metrika s poslužitelja u opsegu: odgovornost Naručitelja - vremenski rok za testiranje: **10 radnih dana** | - autentikacija: korisničko ime/zaporka, soft certifikati - broj računala s kojih se provodi ispitivanje: više od 1 - broj fizičkih ili logičkih poslužitelja: do 5 - korištenje jednostavnih web formi bez međusobne ovisnosti između pojedinih koraka - prikupljanje performansnih metrika s poslužitelja u opsegu: odgovornost Naručitelja - vremenski rok za testiranje: **15 radnih dana** | - autentikacija: dvofaktorka autentikacija (ključevi pohranjeni na vanjskom mediju: token, pametne kartica i sl.) - broj računala s kojih se provodi ispitivanje: više od 1 - korištenje složenih web formi s međusobnom ovisnosti između pojedinih koraka rada u aplikaciji - prikupljanje performansnih metrika s poslužitelja u opsegu: odgovornost Ponuditelja - vremenski rok za testiranje: **20 radnih dana** |

## Isporuke - Rezultati testiranja performansi

Rezultat testiranja performansi je dokumentacija koja se Naručitelju dostavlja u elektroničkom i papirnatom obliku.

Isporučena dokumentacija treba sadržavati „Izvještaj o provedenom testiranju performansi“ sa sljedećim informacijama:

* sažetak o provedenom ispitivanju za rukovoditelje
* opsegom i metodologijom ispitivanja
* rezultatima ispitivanja prema različitim scenarijima
* tehničkim preporukama za unaprjeđenje performansi sustava

# Testiranje otpornosti sustava na DoS i DDoS napade

## Opis aktivnosti

Ispitivanje otpornosti sustava obuhvaća sljedeće aktivnosti:

1. Testiranje performansi i otpornosti sustava na napade minimalno uključuje:
* analiza arhitekture sustava
* definiranje testnih scenarija u dogovoru s Naručiteljem
* test otpornosti sustava baziran na volumenu (*UDP flood, ICMP flood, spoofed-packet flood* i sl)
* test otpornosti sustava baziran na protokolu (*SYN flood, fragmented packet attack, Ping of Death, Smurf DDoS* i sl.)
* test otpornosti sustava na aplikacijskom sloju (*Slowloris, Zero-day DDoS, DDoS attack* prema Apache, Windows ili OpenBSD ranjivostima i sl.)
1. Izrada završnog izvještaja
* izrada dokumentacije s rezultatima testiranja što po potrebi uključuje preporuke za:
	+ unapređenje sklopovlja
	+ izmjene u postavkama pojedinih komponenti sustava
	+ izmjene ili nadogradnje na aplikativnoj razini
	+ optimizaciju ili povećanje propusnosti komunikacijskog kanala

## Kompleksnost aplikacije

|  |  |
| --- | --- |
| **Kompleksnost 1**  | **Kompleksnost 2**  |
| - broj tiera u arhitekturi: 1 ili 2 - broj fizičkih ili logičkih poslužitelja: do 4 - vremenski rok za testiranje: **5 radnih dana** | - broj tiera u arhitekturi: 3 ili više - broj fizičkih ili logičkih poslužitelja: 5 ili više - vremenski rok za testiranje: **10 radnih dana** |

## Isporuke – Rezultati testiranja otpornosti sustava na DoS i DDoS napade

Rezultat testiranja otpornosti sustava na DoS i DDoS napade je dokumentacija koja se Naručitelju dostavlja u elektroničkom i papirnatom obliku.

Isporučena dokumentacija treba sadržavati „Izvještaj o provedenom testiranju performansi“ sa sljedećim informacijama:

* sažetak o provedenom ispitivanju za rukovoditelje
* opsegom i metodologijom ispitivanja
* rezultatima ispitivanja prema različitim scenarijima
* tehničkim preporukama za unaprjeđenje performansi sustava

# Savjetovanje

Savjetovanje u području računalne sigurnosti i sigurnosnih testiranja, provođenje specifičnih sigurnosnih testiranja čija se kompleksnost ne može unaprijed definirati.

# 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 poslanog zahtijeva za pojedinačno testiranje.

Konkretne rokove završetka pojedinog testiranja utvrdit će Naručitelj, 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 7.2.

Isporučena dokumentacija definirana u točkama 3.1.3, 3.2.3, 3.3.3, 3.4.3, 3.5.2, 3.6.3 i 3.7.3 mora sadržavati potpise stručnjaka koji su sudjelovali u pojedinom testiranju.

1. Ne postoji specifikacija, razmatra se da spomenuto aplikativno rješenje bude integrirano kao modul za CARNET Omega [↑](#footnote-ref-2)
2. Ne postoji specifikacija, razmatra se da spomenuto aplikativno rješenje bude integrirano kao modul za CARNET Omega [↑](#footnote-ref-3)