**Darba uzdevums**

Ieslodzījuma vietu pārvalde Eiropas reģionālā attīstības fonda darbības programmas "Izaugsme un nodarbinātība" 2.2.1. specifiskā atbalsta mērķa "Nodrošināt publisko datu atkalizmantošanas pieaugumu un efektīvu publiskās pārvaldes un privātā sektora mijiedarbību" 2.2.1.1. pasākuma "Centralizētu publiskās pārvaldes IKT platformu izveide, publiskās pārvaldes procesu optimizēšana un attīstība" ietvaros īsteno projektu Nr.2.2.1.1/17/I/012 “Ieslodzījuma vietu pārvaldes informācijas sistēmas pilnveidošana” (Projekts). Projekta ietvaros tiek izstrādāta jauna Ieslodzīto informācijas sistēma (IIS). Projektā nepieciešams veikt piegādātās IIS starpnodevuma drošības prasību testēšanu.

**Pasūtītājs**: Ieslodzījuma vietu pārvalde

**Priekšmets**: Jaunās Ieslodzīto informācijas sistēmas starpnodevuma (informācijas sistēma ar nepilnu funkcionalitāti) drošības testēšana

**EIS pozīcija:** CI110P.75.3 Pakalpojuma nosaukums: Sistēmas(u) drošības testēšanas pakalpojums.

1. Ieslodzīto informācijas sistēmas un to komponenšu (operētājsistēmas, datubāžu vadības sistēmas, serveru datu pārraides tīkls) drošības kontroļu novērtēšana:
	1. Informācijas sistēmu tehniskā drošības testēšana saskaņā ar OSSTMM v3.0 (*Open Source Security Testing Methodology Manual*) standartu, OWASP (*Open Web Application Security Project*) *Testing Guide* vadlīnijām, saskaņā ar minimālajām prasībām (skatīt Darba uzdevuma 1. pielikumu) un PTES (*Penetration Testing Execution Standard*) standartu;
	2. Sistēmu drošības konfigurācijas novērtējums;
2. Termiņš pirmreizējai testēšanai ir 15 (piecpadsmit) darbdienas. Testēšanas rezultātā iesniedzams testēšanas pārskats, kurā norādāms:
	1. Informācija par audita pieeju un metodiku;
	2. Informācija par audita tvērumu;
	3. Detalizēta informācija par atklātajām nepilnībām, riskiem vai neatbilstību likumdošanai vai labajai praksei, neatbilstībām tehniskajai specifikācijai, iespējamās sekas nepilnības nenovēršanas gadījumā un rekomendācijas nepilnības novēršanai.
	4. Aprakstot katru novērojumu jānorāda sekojošais:
		1. Nosaukums (kopsavilkums);
		2. Novērojums, kurā aprakstīts konstatējums par drošības risku vai neatbilstību;
		3. Iespējamās sekas, kas var iestāties ;
		4. Ietekmes novērtējums šādā skalā: kritiska, augsta, vidēja, zema, informatīva;
		5. Rekomendācija nepilnības novēršanai;
		6. Detalizēta tehniskā informācija (skripti, fotouzņēmumi u.c. pamatojošā informācija, kas ļauj pārliecināties par nepilnības esamību un ir nepieciešama tās novēršanai).
3. Ja drošības testēšanas rezultātā konstatētas kritiskas vai augstas nepilnības vai ievainojamības, jāveic atkārtots drošības novērtējums. Atkārtotais drošības novērtējums ietver visas programmatūras atkārotu testēšanu. Pēc atkārtotas testēšanas iesniedzams atkārtots testēšanas pārskats, atsevišķi izdalot novērstos trūkumus. Atkārtotas sistēmu drošības testēšanas jāveic pēc atklāto problēmu novēršanas saskaņā ar Pasūtītāja pieprasījumu.
4. Pakalpojumus, kas norādīti darba uzdevuma 1. un 3.punktā, Izpildītājs uzsāk ne vēlāk kā 5 (piecu) darbdienu laikā pēc Pasūtītāja rakstveida pieprasījuma saņemšanas.

5.  Izpildītājs atbild par zaudējumiem, kuri Pasūtītājam radušies, ja Pasūtītāja informācijas sistēmas dati kļuvuši nesankcionēti pieejami, tikuši mainīti vai dzēsti (veiktas nesankcionētas darbības ar Pasūtītāja informācijas sistēmu), izņemot gadījumus, ja:

5.1. Izpildītājs informējis Pasūtītāju par konstatēto ievainojamību, kura izmantota nesankcionētām darbībām ar Pasūtītāja informācijas sistēmu;

5.2. pret ievainojamību, kura izmantota nesankcionētām darbībām ar Pasūtītāja informācijas sistēmām, standarta programmatūras ražotājs izlaidis drošības labojumu, bet Pasūtītājs šādu labojumu nav uzstādījis;

5.3. pēc drošības testēšanas mainīti informācijas sistēmas drošības uzstādījumi;

5.4. pēc drošības testēšanas veiktas informācijas sistēmas tehnisko resursu vai tīkla konfigurācijas izmaiņas (ja nesankcionēta darbība realizēta, izmantojot tīkla konfigurācijas izmaiņas vai izmainītos tehniskos resursus);

5.5. nesankcionētas darbības ar Pasūtītāja informācijas sistēmu veiktas, izmantojot Pasūtītāja piešķirtas sistēmas lietotāja tiesības;

5.6. nesankcionētas darbības ar Pasūtītāja informācijas sistēmām veiktas, izmantojot tehnoloģiskos risinājumus, kuri Līguma izpildes laikā nebija zināmi.

Pielikums

pie darba uzdevuma

**Minimālās prasības drošības testa pārskatam,**

**veicot drošības auditu informācijas sistēmai**

| **ID** | **Tests** | **Iegūtie pierādījumi** | **Atstātais iespaids** | **Rekomen-dācijas** |
| --- | --- | --- | --- | --- |
| Informācijas ievākšana |
| OTG-INFO-001 | Veikt meklēšanas dziņos pieejamās informācijas izpēti un informācijas noplūdes meklēšanu |   |   |   |
| OTG-INFO-002 | *Web* servera identifikācija |   |   |   |
| OTG-INFO-003 | *Web* serveru metadatņu izpēte informācijas noplūdes meklēšanā |   |   |   |
| OTG-INFO-004 | Aplikāciju identifikācija uz *web* servera |   |   |   |
| OTG-INFO-005 | *Web* lapu komentāru un metadatu pārbaude meklējot informācijas noplūdi |   |   |   |
| OTG-INFO-006 | Identificēt aplikācijas piekļuves punktus |   |   |   |
| OTG-INFO-007 | Izveidot aplikācijas izpildes karti |   |   |   |
| OTG-INFO-008 | Identificēt aplikācijas izstrādē izmantoto *framework* |   |   |   |
| OTG-INFO-009 | Identificēt pašu *web* aplikāciju |   |   |   |
| OTG-INFO-010 | Izveidot aplikācijas arhitektūras karti |   |   |   |
| Konfigurācijas un piegādes vadības testi |
| OTG-CONFIG-001 | Pārbaudīt tīkla/infrastruktūras konfigurāciju |   |   |   |
| OTG-CONFIG-002 | Pārbaudīt aplikācijas platformas konfigurāciju |   |   |   |
| OTG-CONFIG-003 | Pārbaudīt datņu paplašinājumu apstrādi, meklējot sensitīvu informāciju |   |   |   |
| OTG-CONFIG-004 | Rezerves kopiju un datnes bez atsaucēm, meklējot sensitīvu informāciju |   |   |   |
| OTG-CONFIG-005 | Identificēt infrastruktūras un aplikācijas administratoru saskarnes |   |   |   |
| OTG-CONFIG-006 | Testēt HTTP metodes |   |   |   |
| OTG-CONFIG-007 | Testēt HTTP precīza transporta drošību |   |   |   |
| OTG-CONFIG-008 | Testēt RIA pār/domēnu politiku |   |   |   |
| Identitātes pārvaldības testi |
| OTG-IDENT-001 | Testēt lomu definīcijas |   |   |   |
| OTG-IDENT-002 | Testēt lietotāja reģistrācijas procesu |   |   |   |
| OTG-IDENT-003 | Testēt kontu izveides procesu |   |   |   |
| OTG-IDENT-004 | Testēt kontu identifikatora piešķiršanu un uzminamu lietotāju kontu kontroli |   |   |   |
| OTG-IDENT-005 | Pārbaudīt vai nav vāja vai neieviesta lietotājvārdu politika |   |   |   |
| OTG-IDENT-006 | Pārbaudīt piekļuves un Viesu/Testa kontus |   |   |   |
| OTG-IDENT-007 | Testēt kontu bloķēšanas/atbloķēšanas procesus |   |   |   |
| Autentifikācijas testēšana |
| OTG-AUTHN-001 | Testēt lietotāju datu pārraidi šifrētā kanālā |   |   |   |
| OTG-AUTHN-002 | Pārbaudīt noklusējuma lietotāju piekļuves informāciju |   |   |   |
| OTG-AUTHN-003 | Testēt vāju konta bloķēšanas mehānismu |   |   |   |
| OTG-AUTHN-004 | Pārbaudīt vai var apiet autentifikācijas shēmu |   |   |   |
| OTG-AUTHN-005 | Pārbaudīt paroles atcerēšanās funkcionalitāti |   |   |   |
| OTG-AUTHN-006 | Pārbaudīt pārlūkprogrammas kešatmiņas ievainojamības |   |   |   |
| OTG-AUTHN-007 | Pārbaudīt vājas paroles politiku |   |   |   |
| OTG-AUTHN-008 | Pārbaudīt vājas drošības jautājuma/atbildes izmantošanas iespēju |   |   |   |
| OTG-AUTHN-009 | Pārbaudīt vājas paroles nomaiņas vai atiestatīšanas funkcionalitāti |   |   |   |
| OTG-AUTHN-010 | Pārbaudīt vai nav iespējama vāja autentifikācija alternatīvā kanālā |   |   |   |
| Autorizācijas pārbaude |
| OTG-AUTHZ-001 | Pārbaudīt direktorijas pārskatīšanas/datņu iekļaušanas iespējas |   |   |   |
| OTG-AUTHZ-002 | Pārbaudīt autentifikācijas shēmas apiešanas iespējas |   |   |   |
| OTG-AUTHZ-003 | Pārbaudīt iespējas eskalēt privilēģijas |   |   |   |
| OTG-AUTHZ-004 | Pārbaudīt nedrošas tiešās atsauces uz objektiem |   |   |   |
| Sesijas pārvaldības testi |
| OTG-SESS-001 | Sesiju pārvaldības apiešanas pārbaude |   |   |   |
| OTG-SESS-002 | *Cookies* parametru testēšana |   |   |   |
| OTG-SESS-003 | Sesiju fiksācijas pārbaude |   |   |   |
| OTG-SESS-004 | Sesiju mainīgo neaizsargātības pārbaude |   |   |   |
| OTG-SESS-005 | *CSRF* testi (starpvietņu pieprasījumu viltošana) |   |   |   |
| OTG-SESS-006 | Autorizācijas pabeigšanas pieprasījumi |   |   |   |
| OTG-SESS-007 | Sesijas izbeigšanās pārbaude |   |   |   |
| OTG-SESS-008 | Sesijas samaisīšanas/randomizācijas pārbaude |   |   |   |
| Ievades mainīgo pārbaudes |
| OTG-INPVAL-001 | Spoguļotas starpvietņu skriptēšanas pārbaude |   |   |   |
| OTG-INPVAL-002 | Saglabātas starpsaitņu skriptēšanas pārbaude |   |   |   |
| OTG-INPVAL-003 | *HTTP* darbību manipulācijas |   |   |   |
| OTG-INPVAL-004 | *HTTP* parametru piepildīšanas pārbaude |   |   |   |
| OTG-INPVAL-005 | *SQL* injekciju pārbaude |   |   |   |
| OTG-INPVAL-006 | *LDAP* injekciju pārbaude |   |   |   |
| OTG-INPVAL-007 | *ORM* injekciju pārbaude |   |   |   |
| OTG-INPVAL-008 | *XML* injekciju pārbaude |   |   |   |
| OTG-INPVAL-009 | *SSI* injekciju pārbaude |   |   |   |
| OTG-INPVAL-010 | *Xpath* injekciju pārbaude |   |   |   |
| OTG-INPVAL-011 | *IMAP/SMTP* injekciju pārbaude |   |   |   |
| OTG-INPVAL-012 | Koda injekcijas / Lokālās un attālinātās datnes injekcijas |   |   |   |
| OTG-INPVAL-013 | Komandu injekciju pārbaude |   |   |   |
| OTG-INPVAL-014 | Bufera pārpilde |   |   |   |
| OTG-INPVAL-015 | Ietvertu ievainojamību pārbaude |   |   |   |
| OTG-INPVAL-016 | *HTTP* sadalīšanas / pārcelšanas ievainojamības |   |   |   |
| Kļūdu apstrāde |
| OTG-ERR-001 | Kļūdu kodu analīze |   |   |   |
| OTG-ERR-002 | *Stack Traces* analīze |   |   |   |
| Kriptogrāfija |
| OTG-CRYPST-001 | Vāju SSL/TSL šifru meklēšana, nepietiekama transporta līmeņa aizsardzība |   |   |   |
| OTG-CRYPST-002 | *Oracle padding* testēšana |   |   |   |
| OTG-CRYPST-003 | Sensitīvas informācijas pārsūtīšana caur nešifrētiem kanāliem |   |   |   |
| Biznesa loģikas testēšana |
| OTG-BUSLOGIC-001 | Biznesa loģikas datu validācijas pārbaude |   |   |   |
| OTG-BUSLOGIC-002 | Pieprasījumu viltošanas pārbaude |   |   |   |
| OTG-BUSLOGIC-003 | Integritātes pārbaužu pārbaude |   |   |   |
| OTG-BUSLOGIC-004 | Procesu laika pārbaude |   |   |   |
| OTG-BUSLOGIC-005 | Funkciju lietojamības skaita ierobežojuma pārbaude |   |   |   |
| OTG-BUSLOGIC-006 | Darba plūsmas neievērošanas pārbaude |   |   |   |
| OTG-BUSLOGIC-007 | Aizsardzības pret nekorektu aplikācijas lietošanu pārbaude |   |   |   |
| OTG-BUSLOGIC-008 | Negaidītu datņu tipu pārbaude |   |   |   |
| OTG-BUSLOGIC-009 | Ļaunprātīgu datņu augšupielādes pārbaude |   |   |   |
| Klienta puses testēšana |
| OTG-CLIENT-001 | *DOM* balstīta starpvietņu skriptu pārbaude |   |   |   |
| OTG-CLIENT-002 | *JavaScript* izpildes pārbaude |   |   |   |
| OTG-CLIENT-003 | *HTML* injekciju pārbaude |   |   |   |
| OTG-CLIENT-004 | Klientu puses *URL* pārvirzīšanas pārbaude |   |   |   |
| OTG-CLIENT-005 | *CSS* injekciju pārbaude |   |   |   |
| OTG-CLIENT-006 | Klienta puses resursu manipulācijas pārbaude |   |   |   |
| OTG-CLIENT-007 | Starp izcelsmes resursu koplietošanas pārbaude |   |   |   |
| OTG-CLIENT-008 | *CSF* (*Cross Site Flashing*) pārbaude |   |   |   |
| OTG-CLIENT-009 | Klikšķu nozagšanas pārbaude |   |   |   |
| OTG-CLIENT-010 | *WebSockets* pārbaude |   |   |   |
| OTG-CLIENT-011 | *Web* ziņojumu pārbaude |   |   |   |
| OTG-CLIENT-012 | Lokālās glabāšanas pārbaude |   |   |   |