Příloha RD08 – Zajištění bezpečnostních testů

č. sml. Objednatele: ČÚZK-12466/2018 -24 č. sml. Zhotovitele: B181228

1 Úvod

Tento dokument stanovuje pravidla a postupy pro provádění bezpečnostních testů v prostředí Objednatele k zajištění bezpečnostního testování ISKN (dále též „bezpečnostní testování" nebo „bezpečnostní testy").

Interní testování Zhotovitele v oblasti bezpečnosti prováděné na technologické infrastruktuře Zhotovitele není obsahem tohoto dokumentu.

2 Členění zranitelností podle závažnosti

2.1 CRITICAL

Kritická, vyžaduje zpravidla okamžitý zásah nebo odstavení systému.

2.2 IMPORTANT

Důležitá, může být zdrojem budoucích potíží, je nezbytná náprava dle možností co nejdříve.

2.3 MEDIUM

Střední stupeň závažnosti, zvyšuje pravděpodobnost úspěšného útoku, zpravidla vyžaduje splnění určitých podmínek.

2.4 LOW

Nízký stupeň závažnosti, pouze mírně zvyšuje pravděpodobnost úspěšného útoku, vyžaduje splnění určitých podmínek.

2.5 INFORMATION

Informativní, nejedná se ve skutečnosti o zranitelnost, ale o informaci.

3 Pravidla a způsob provádění bezpečnostních testů

Bezpečnostní testování bude prováděno v testovacím prostředí Objednatele a v předem stanoveném a Objednatelem odsouhlaseném rozsahu.

Výjimky z rozsahu bezpečnostních testů jsou možné pouze po předchozím odsouhlasení Objednatele.

3.1 Kritéria pro stanovení rozsahu bezpečnostního testování

Bezpečnostní testování může být vyvoláno následujícími faktory:

3.1.1 Příprava dodávky ISKN

Zhotovitel při navrhování rozsahu bezpečnostního testu posuzuje:

- zda změna ISKN zasahuje přímo do bezpečnostních vlastností ISKN (změna je s přímým bezpečnostním dopadem, např. zavedení nové webové služby, změna autentizace nebo autorizace uživatele, změna technologie), nebo zda změna má nebo může mít nepřímý bezpečnostní dopad nebo zda může zasáhnout do bezpečnostních opatření ISKN (např. doplněný nebo změněný modul bez přímé vazby na bezpečnostní opatření),
- rozsah změn ISKN.

Závazný minimální rozsah bezpečnostních testů, v závislosti na charakteru změny vyjádřeném číslem verze dodávky ISKN, je uveden v tabulce „Tabulka 1 - rozsah bezpečnostních testů dle změn ISKN".

Změna ISKN označená jako	Jedná se o verzi změny (dodávky) označenou	Rozsah prováděných bezpečnostních testů Zhotovitelem
Velká	X.Y (např. 8.0, 8.1, ..)	Bude vždy provedena kompletní sada bezpečnostních testů dle bodu 4.1 tohoto dokumentu.
Malá	X.Y.Z (např. 8.0.1, 8.1.2, ...)	Bude provedena kompletní sada bezpečnostních testů dle bodu 4.1 pouze v případě, že bude implementována alespoň jedna změna ISKN s možným přímým nebo nepřímým bezpečnostním dopadem.
Patch/hotfix	X.Y.Z.xx (např. 8.0.1.03.CF4)*)	Zhotovitelem budou provedeny bezpečnostní testy vybraných a navržených testovacích scénářů pro příslušnou změnu s možným bezpečnostním dopadem, případně i další bezpečnostní testy navržené Objednatelem nad rámec návrhu Zhotovitele.

Tabulka 1 - rozsah bezpečnostních testů dle změn ISKN

*) stávající jmenná konvence

Bezpečnostní testy začleňuje Zhotovitel do harmonogramu dané dodávky ISKN (viz Příloha 15 ZD).

Pokud není v období 12 měsíců plánována / dodána dodávka ISKN typu X.Y, začlení Zhotovitel provedení kompletní sady bezpečnostních testů dle bodu 4.1 do vhodné dodávky ISKN typu X.Y.Z tak, aby odstup od minulého provedení kompletní sady bezpečnostních testů dle bodu 4.1 nebyl větší než 12 měsíců, případně lze po dohodě s Objednatelem provést na v té době vhodném testovacím prostředí Objednatele kompletní sadu bezpečnostních testů dle bodu 4.1 bez vazby na konkrétní dodávku ISKN.

3.1.2 Zjištění výskytu relevantní zranitelnosti v průběhu kybernetického bezpečnostního incidentu

V takovém případě je bezpečnostní testování prováděno v rozsahu nezbytném pro ověření, zda kybernetický bezpečnostní incident nebyl způsoben zranitelností.

Provedení bezpečnostní testů navrhuje Zhotovitel na základě zjištěných informací; součástí návrhu je i vhodné začlenění do harmonogramů aktuálních/plánovaných dodávek ISKN.

3.1.3 Informace zjištěné při činnostech prováděných Manažerem nebo Architektem kybernetické bezpečnosti VIS nebo Specialistou kybernetické bezpečnosti

Zdrojem těchto informací může být například sledování informačního servisu NÚKIB nebo security bulletinů (viz Příloha RD06); v takovém případě je bezpečnostní testování prováděno, pokud obsahuje komponentu, která může být na zranitelnost náchylná; účelem tohoto bezpečnostního testu je zjištění, zda ISKN danou zranitelnost obsahuje.

Provedení bezpečnostní testů navrhuje Zhotovitel na základě zjištěných informací; součástí návrhu je i vhodné začlenění do harmonogramů aktuálních/plánovaných dodávek ISKN.

3.2 Pravidelné bezpečnostní testy na produkčním prostředí

Zhotovitel provádí na produkčním prostředí Objednatele pravidelně minimálně 1 x za 12 měsíců sadu základních bezpečnostních testů v rozsahu bodu 4.1.

3.3 Pravidla provádění bezpečnostních testů

Bezpečnostní testy musí být opakovatelné a musí být prováděny neinvazivním způsobem.

Pro účely bezpečnostního testování na prostředí Objednatele poskytne Objednatel Zhotoviteli:

- testovací účet s přístupem do testovacího nebo produkčního prostředí Objednatele, v němž bude probíhat bezpečnostní testování,
- přístup k ISKN s právy běžného externího uživatele (případně více uživatelů, podle jejich rolí),
- vzdálený přístup do interní sítě Objednatele nebo fyzický přístup na pracoviště Objednatele, pokud to bude pro bezpečností testování potřebné,
- možnost připojení koncového zařízení Zhotovitele (testovacího notebooku nebo serveru) do testovacího prostředí Objednatele.

Zhotovitel je při provádění bezpečnostních testů povinen:

- bezpečnostní testy provádět dle schváleného PBT,
- neověřovat prakticky zjištěnou zranitelnost vůči útoku „Denial of Services" (DoS),
- neprovádět nevratné zásahy do systému (v případě úspěšného průniku),
- nepoužívat techniky „sociálního inženýrství" (telefonáty nebo maily pod předstíranou identitou, apod.),
- v případě zjištění závažné skutečnosti v průběhu testování (odstavení některé služby) okamžitě informovat Objednatele.

Bezpečnostní testování provádí Zhotovitel dle jím zpracovaných testovacích scénářů.

3.4 Způsob provádění bezpečnostních testů

Před zahájením bezpečnostního testování Zhotovitel vyhotoví a předá Objednateli dokument „Plán bezpečnostního testování ISKN pro dodávku X" (PBT), který bude minimálně obsahovat:

- na základě kritérií dle bodu 3.1.1 seznam změn ISKN včetně uvedení, jak danou změnu vyhodnotil, tj. zda tato změna má/může mít nebo nemá bezpečnostní dopad,
- na základě bodu 0 popis kybernetického incidentu, který může indikovat zranitelnost,
- na základě bodu 3.1.3 popis možné zranitelnosti a odkaz na zdroj,
- navržený rozsah bezpečnostních testů, který bude proveden,
- harmonogram termínů provádění bezpečnostních testů.

PBT podléhá schválení ředitele odboru informatiky ČÚZK.

Na základě schváleného PBT provede Zhotovitel:

- v případě bodu 3.1.1 po úspěšném interním otestování v prostředí Zhotovitele bezpečnostní testování v testovacím prostředí Objednatele s instalovanou změnou ISKN , při zjištění kritické nebo důležité zranitelnosti (viz body 2.1 a 2.2) Zhotovitel v případě zranitelnosti, která vznikla v důsledku plnění Zhotovitele, zajistí odstranění příčiny/chyby způsobující tuto zranitelnost a provede opakované bezpečnostní testování se zaměřením na ověření odstranění zranitelnosti; o všech těchto skutečnostech bez prodlení informuje Objednatele,
- v případě bodů 0 a 3.1.3 v testovacím prostředí Objednatele testování s verzí ISKN shodnou jako na produkčním prostředí, při nižší závažnosti lze bezpečnostní test provést v rámci testování aktuálně připravované dodávky ISKN; bezpečnostní test lze po odsouhlasení Objednatele provést v produkčním prostředí,

- v případě bodu 3.2 v produkčním prostředí Objednatele bezpečnostní testování s aktuální verzí ISKN.

Po ukončení bezpečnostního testování předkládá Zhotovitel nejpozději do 5 pracovních dnů od ukončení bezpečnostních testů Objednateli dokument o provedení a dosažených výsledků bezpečnostních testů s názvem „Zpráva o výsledcích bezpečnostních testů ISKN dodávky X" (ZVBT), který musí obsahovat minimálně:

- přesnou identifikaci PBT, na jehož základě bylo testování prováděno,
- datum a čas provedení bezpečnostních testů,
- na jakém prostředí bylo testováno,
- ID testovacího scénáře,
- jméno testera, který bezpečnostní testování prováděl,
- manažerský souhrn s důležitými závěry bez technických detailů,
- technickou zprávu shrnující zjištění s technickými detaily,
- seznam zjištění; je-li součástí zprávy report generovaný nějakým nástrojem, je nutné specifikovat název a verzi nástroje, případně verzi pluginů; zjištění musí být v celé zprávě jednotně klasifikována podle bodu 2, přestože jsou použity různé nástroje, které mohou mít vlastní klasifikace,
- sumarizaci zjištěných zranitelností včetně návrhů opatření na jejich odstranění; pro kritické a důležité zranitelnosti, které byly nalezeny při bezpečnostním testu dle bodu 3.1.1 a které vznikly v důsledku plnění Zhotovitele i s uvedením způsobu, jak byly Zhotovitelem vyřešeny.

V případě, že ZVBT obsahuje zjištěné zranitelnosti, Zhotovitel zajistí svolání schůzky Zhotovitele a Objednatele, kde Zhotovitel prezentuje svá zjištění a blíže informuje o návrhu/návrzích řešení. Na schůzce Objednatel rozhodne o způsobu odstranění zranitelností nebo jejich eliminaci a o dalším postupu. Toto Zhotovitel zaznamená do zápisu ze schůzky, který podepisuje zástupce Zhotovitele a Objednatele.

Neodstranění kritických a důležitých zranitelností nalezených při postupu dle bodu 3.1.1 a nezopakování ověření odstranění těchto zranitelností s vyhovujícím výsledkem může být důvodem k odkladu instalace příslušné dodávky ISKN do produkčního prostředí. Pokud zjištěná zranitelnost nevznikla v důsledku plnění Zhotovitele, pak se odklad instalace nepovažuje za prodlevu v plnění na straně Zhotovitele.

3.5 Ochrana dat v průběhu testování

Zhotovitel se v průběhu realizace bezpečnostních testů řídí standardními pravidly pro zajištění důvěrnosti používaných informací, zejména pak:

- tam, kde je to možné, používá anonymizované informace,
- v případech, kdy použití anonymizovaných informací není možné (např. v rámci testování v produkčním prostředí), je povinen zajistit opatření, která znemožní jejich nekontrolovaný únik.

4 Bezpečnostní testy

V rámci bezpečnostních testů jsou testovány části ISKN, k nimž přistupují uživatelé nebo systémy, jak interní z vnitřní sítě resortu, tak externí, kteří mají přístup zajištěn pomocí dálkového přístupu z vnější sítě.

4.1 Seznam bezpečnostních testů

Seznam základních bezpečnostních testů je uveden v tabulce „Tabulka 2 - seznam testů".

Předmět testu	Test interní části ISKN	Test externí části ISKN
syntaxe všech uživatelských vstupů	Ano	Ano
odolnosti proti známým typům útoků (XSS, CSRF, Session Steal, ClickJacking apod.)	Ano	Ano
zákazu používaní tzv. skrytých polí pro důvěrná (citlivá) data	Ano	Ano
zákazu používání přídavných identifikací uživatelských „session" a obdobných autentizačních prostředků zakomponovaných v URL	Ano	Ano
zákazu uvádění názvů souborů a adresářových cest v chybových hlášeních	Ne	Ano
možností uživatelova odhlášení	Ano	Ano
automatického odhlášení po definované době jeho nečinnosti	Ne	Ano
omezení pro používání Cookies na Cookies s časově omezenou platností, které jsou posílány zpět pouze stejnému serveru	Ano	Ano
použité komponenty musí být podepsány důvěryhodnou certifikační autoritou	Ano	Ano
komunikace aplikace s datovými zdroji v interní síti musí být autentizovaná	Ano	Ano
možnost napadení DoS útokem	Ne	Ano
další zranitelnosti definované tímto dokumentem (specifické zranitelnosti)	Ano	Ano
testy na zranitelnosti uvedených v tabulce „Tabulka 3 - seznam zranitelností podle OWASP Top 10 – 2017[1].	Ano	Ano

Tabulka 2 - seznam testů

4.2 Realizace bezpečnostních testů

Objednatel připouští realizaci bezpečnostních testů níže uvedenými způsoby, přičemž jejich použití k ověření oblastí testování uvedených v bodě 4.1 ponechává na Zhotoviteli.

4.2.1 Automatizované testy a automatizované testy s manuálním podílem

Pro automatizované testy a automatizované testy s manuálním podílem bude použit některý ze SW nástrojů. Druh aktuálně použitého SW nástroje uvede Zhotovitel v dokumentu PBT.

[1] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

4.2.2 Manuální testování

Manuální testování provede Zhotovitel v těch případech, kdy není možné využít automatizované testy nebo by použití automatizovaných testů nebylo dostatečně efektivní.

4.3 Specifické testy

Metodika OWASP obsahuje standardizované testy, tj. nezahrnuje všechny testovací scénáře zranitelností, které se mohou při vývoji informačního systému vyskytnout. Vzhledem k tomu budou dále pro zajištění bezpečného fungování ISKN prováděny též i další specifické testy.

Specifické testy budou vycházet a zohledňovat možná specifika kódu, zjištění ze sledování informačního servisu NÚKIB apod., zranitelnosti zjištěné při provozu ISKN, které se vyskytly jako bezpečnostní události nebo incidenty u nichž je nutné zajistit přijetí bezpečnostní opatření k zajištění jejich neopakovatelnosti nebo eliminaci a které vznikly v době před odpovídající aktualizací metodiky OWASP.

Seznam testovacích scénářů pro specifické testy je uveden v tabulce „Tabulka 4 - seznam specifických zranitelností" v Příloze 1 tohoto dokumentu.

5 Předmět bezpečnostních testů ISKN

Bezpečností testy se týkají následujících částí ISKN. Zhotovitel je vždy povinen zahrnout do testování další nové části / funkcionality ISKN a dle toho aktualizovat tento dokument.

5.1 Externí části ISKN

- Dálkový přístup do ISKN,
- Platební portál,
- Služba sledování změn (externí část),
- WSDP,
- WSENX,
- WSGP,
- WSSSZ,
- WSZR.

5.2 Interní části ISKN

- Služba sledování změn (interní část),
- rozhraní grafického mapového serveru GSWS,
- rozhraní pro Informační systémy EPVDS, DMS, ISÚI, ISZR,
- rozhraní Oracle Forms, Oracle Report a Jasper reports serverů.

U testů Forms a Reports serverů není účelem testu otestovat potencionální zranitelnost způsobenou výrobcem (pokud se testování neprovádí na základě bodů 0 nebo 3.1.3), ale implementaci / použití daného produktu Zhotovitelem (např. nevhodné předávání parametrů v URL apod.).

6 Testovací scénáře

Testovací scénáře musí zahrnovat následující údaje:

- název testovacího scénáře,

- ID testovacího scénáře,
- verze systému,
- počet provedení scénáře,
- účel testu – popis, co je testem ověřováno,
- výchozí stav systému a vstupní podmínky,
- kroky testu – popis testovacích kroků a dat používaných pro testování,
- očekávané výsledky – kritéria úspěšnosti testu přiřazené ke každému z testovacích kroků.

Testovací scénáře pro automatizované, resp. automatizované testy s manuálním podílem, jsou konfigurovány v rámci použitého SW nástroje. Základní schémata testovacích scénářů pro manuální testy jsou uvedena v Příloze č. 2.

7 Přechodná ustanovení

Zhotovitel se zavazuje v případě uvolnění nové verze OWASP tento dokument do měsíce od vydání nové verze OWASP aktualizovat v souladu s novou verzí a používat odpovídající postupy a druhy testů.

Příloha č. 1 - Seznamy testovaných zranitelností

Seznam zranitelností podle OWASP Top 10 - 2017.

Zranitelnost	Popis
A01: Injection	Zranitelnost typu injektáže (SQL, LDAP, XPath, NoSQL dotazů; příkazů operačního systému, XML parsování, SMTP hlaviček, programových argumentů, atd.) je velmi běžnou chybou webových aplikací, které nastává, pokud jsou přes neošetřený vstup uživatelem poskytnutá nedůvěryhodná data poslána do překladače jako část příkazu nebo dotazu. Např. u „SQL injection" jde o vykonání vlastního, pozměněného SQL dotazu za účelem neoprávněného přístupu k informacím, jejich změně nebo i ovládnutí daného zařízení. Zranitelnosti typu injektáže lze snadno zjistit při revizi kódu, ale těžší je zjišťovat jejich přítomnost pomocí testů vzhledem k velké variabilitě manipulace parametrů http dotazů.
A02: Broken Authentication	Vývojáři často vytváří autentizační mechanismy a řízení relací, ale jejich správné vytvoření není jednoduché. Jako výsledek těchto snah bývají často zranitelnosti v oblastech odhlášení, správy hesel, dlouhé časové limity pro relace, aktualizace účtů atd. Útočníci mohou kompromitovat hesla, klíče nebo autentizační identifikátory k předstírání jiných uživatelských identit. Nalezení těchto zranitelností může být občas těžké, protože každá takováto implementace bývá jedinečná.
A03: Sensitive Data Exposure	Nejběžnější chybou je nešifrování citlivých dat. Pokud se používá šifrování, jde o generování slabých klíčů, použití slabých šifrovacích algoritmů nebo slabé hashovací techniky pro hesla. Zranitelnosti v prohlížeči jsou velmi časté a snadno odhalitelné, ale těžko zneužitelné ve velkém měřítku.
A04: XML External Entities (XXE)	Ve výchozím nastavení mnoho starších procesorů XML umožňuje specifikaci externí entity, URI, která je dereferencována a vyhodnocena během zpracování XML. Nástroje SAST mohou tento problém zjistit kontrolou závislostí a konfigurace. Nástroje DAST vyžadují další ruční kroky k odhalení a zneužití tohoto problému. Jde o novou zranitelnost, zatím nebyla testována.
A05: Broken Access Control	Aplikace často používají skutečný název nebo klíč objektu při generování webových stránek. Aplikace ne vždy ověřuje, zda je uživatel oprávněn přistupovat k cílovému objektu. Útočník tak může neoprávněně manipulovat s těmito odkazy a přistupovat k jiným objektům (bez autorizace). Testeři můžou snadno manipulovat hodnoty parametrů k detekci takovýchto zranitelností. Analýza kódu rychle ukáže, zda povolení je řádně ověřeno.
A06: Security Misconfiguration	Bezpečnostně chybná konfigurace může nastat na jakékoliv úrovni infomačního systému ať už to je webový server, aplikační server, databáze, framework, atd. Vývojáři a systémoví administrátoři musí úzce spolupracovat, aby zajistili, že konfigurace všech částí infomačního systému je v pořádku. Automatizované scannery jsou vhodné pro detekci chybějících patchů, použití defaultních účtů, nepotřebných služeb, apod.
A07: Cross Site Scripting (XSS)	XSS je nejrozšířenější zranitelnost webových aplikací. XSS zranitelnost nastává, pokud aplikace zahrne uživatelem poskytnutá data do webové stránky a pošle ji do prohlížeče, aniž by tato data řádně validoval nebo byly escapovány. To umožní ve webovém prohlížeči oběti spustit útočníkův

Zranitelnost	Popis
	skript, který může např. neoprávněně převzít uživatelskou relaci, změnit obsah stránek, instalovat škodlivé programy apod. Detekce většiny XSS zranitelností je poměrně snadná jak testováním, tak i revizí kódu nebo konfigurací webového serveru.
A08: Insecure Deserialization	Tato zranitelnost je zahrnuta do Top 10 na základě průzkumu v oboru, nikoli na kvantifikovatelných údajích o výskytu. Některé nástroje mohou objevit chyby v deserializaci, ale pro potvrzení problému je často potřeba pomoc člověka. Očekává se, že údaje o prevalenci v případě nedostatků způsobených deserializací se zvýší, protože nástroj je stále vyvíjen, aby pomohl identifikovat a řešit problém. Dopad deserializačních zranitelností nemůže být podceňován. Tyto zranitelnosti mohou vést k útokům typu vzdálené spuštění kódu, což je jeden z nejzávažnějších možných útoků.
A09: Using Components with Known Vulnerabilities	Prakticky každá aplikace má problémy s použitím komponent (knihovny, frameworky a další softwarové moduly) obsahujících známé zranitelnosti, protože většina vývojářů se nesoustředí na zajištění aktualizací komponenty/knihoven. V mnoha případech vývojáři ani neznají, jaké všechny komponenty se používají, natož jejich verze. Závislosti komponent situaci ještě zhoršují. Detekce se provádí zpravidla lokálně v rámci zdrojového kódu, ale částečně ji lze provést i pomocí penetračního testu.
A10: Insufficient Logging & Monitoring	Tato zranitelnost je zahrnuta do Top 10 na základě průzkumu v oboru, nikoli na kvantifikovatelných údajích o výskytu. Jedna z možných strategií pro zjištění, zda je správně nastaven monitoring a logování, je prověřit protokoly po penetračním testování. Činnosti testerů by měly být dostatečně zaznamenány, aby bylo možné zjistit, jaké škody by mohly být způsobeny. Nejúspěšnější útoky začínají zkoumáním zranitelnosti. Povolení pokračování takových zkoumání může zvýšit pravděpodobnost úspěšného útoku téměř na 100%.

Tabulka 3 - seznam zranitelností podle OWASP Top 10 – 2017

Testovací scénáře OWASP TESTING GUIDE, dle nichž bude Zhotovitel provádět penetrační bezpečnostní testy, jsou uvedeny na adrese https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf. V případě vydání nové verze OWASP TESTING GUIDE provede Zhotovitel aktualizaci odkazu a testování bude probíhat pomocí této nové verze.

Seznam specifických zranitelností

Testovány budou specifické zranitelnosti uvedené v Tabulka 4 - seznam specifických zranitelností

Zranitelnost	Popis	Způsob testování
S01: Převzetí identity	Zneužití oprávněným uživatelem DP ISKN cizího oprávnění využitím chybného způsobu zpracování příkazu přesměrování. Po přihlášení se použije přesměrovací http příkaz s pozměněným parametrem PAR_LoginUsername, aplikace změní následně stávající účet na nový, zadaný v parametru PAR_LoginUsername; útočník tak získá oprávnění libovolného uživatele bez toho, že by musel znát jeho heslo.	Ruční test, který ověří, zda změna reaguje správně (musí vrátit HTTP chybu a přístup nepovolit).

Tabulka 4 - seznam specifických zranitelností

Příloha č. 2 - Základní schémata testovacích scénářů

TS 1. Testování možností uživatelova odhlášení a automatického odhlášení po definované době jeho nečinnosti

Testovací scénář pro testování možností uživatelova odhlášení a automatického odhlášení po definované době jeho nečinnosti zahrne následující informace:

Test č. 1

Účel testu: zjištění, zda uživatel má možnost v jakémkoliv místě aplikace (s výjimkou modálních – dialogových – oken) ukončit svou činnost prostřednictvím odhlášení.

Počet provedení jednotlivých kroků: dle potřeby a rozsahu aplikace.

Očekávané výsledky: úspěšné odhlášení ve zvolených místech aplikace.

Kroky testu:

- spuštění aplikace (zadání příslušné URL do prohlížeče),
- spuštění vybrané části aplikace,
- kontrola přítomnosti odhlašovacího aktivního prvku,
- prověření funkčnosti prvku pro odhlášení,
- prověření nemožnosti pokračování bez nezbytného nového přihlášení.

Test č. 2

Účel testu: zjištění, zda po uplynutí definované doby nečinnosti bude uživatel odhlášen.

Počet provedení jednotlivých kroků: 3 x na různých místech aplikace.

Očekávané výsledky: úspěšné odhlášení ve zvolených místech aplikace po uplynutí stanovené doby.

Kroky testu:

- spuštění aplikace (zadání příslušné URL do prohlížeče),
- spuštění vybrané části aplikace,
- zahájení nečinnosti,
- kontrola toho, zda po uplynulé definované době došlo k odhlášení,
- prověření nemožnosti pokračování bez nezbytného nového přihlášení.

TS 2. Ověření digitálních podpisů Java appletů a jiných komponent

Testovací scénář pro ověření digitálních podpisů Java appletů a jiných komponent zahrne následující informace:

Účel testu: zjištění, zda jsou používány pouze podepsané komponenty a zda jsou podepsané uznávanou certifikační autoritou.

Počet provedení jednotlivých kroků: jeden pro všechny komponenty.

Očekávané výsledky: identifikované certifikační autority, které vydaly certifikáty pro ověřování použitých komponent, budou na seznamu důvěryhodných certifikačních autorit.

Kroky testu:

- získání seznamu používaných komponent,
- získání certifikátů používaných pro ověření podpisu komponenty,

- zjištění, zda certifikační autority, které vydaly získaný certifikát, jsou uznávanými certifikačními autoritami

TS 3. Ověření použití autentizace pro komunikace aplikace s datovými zdroji v interní síti

Testovací scénář pro ověření použití autentizace pro komunikace aplikace s datovými zdroji v interní síti zahrne následující informace:

Účel testu: zjištění, zda komunikace aplikace s datovými zdroji v interní síti je autentizovaná.

Počet provedení jednotlivých kroků: dle potřeby a počtu zdrojů.

Očekávané výsledky: potvrzení přístupu pouze na základě řádné autentizace.

Kroky testu:

- získání seznamu používaných zdrojů v interní síti,
- ověření skutečnosti, zda jsou vydány přihlašovací údaje pro přístup aplikace k danému zdroji,
- ověření skutečnosti, zda není možný přístup k danému zdroji bez autentizace,
- pokud to možné je, ověří se, zda může i aplikace ISKN přistupovat bez řádné autentizace.

TS 4. Ověření nemožnosti převzetí identity pomocí parametru PAR_LoginUsername (zranitelnost S01)

Testovací scénář pro ověření nemožnosti převzetí identity pomocí parametru PAR_LoginUsername zahrne následující informace:

Účel testu: zjištění, zda není možné převzít cizí identitu způsobem, kdy se uživatel nejprve přihlásí pod vlastní identitou a následně odesláním http příkazu s parametrem PAR_LoginUsername s hodnotou rovnou cizímu uživatelskému jménu může získat přístup pod cizí identitou.

Počet provedení jednotlivých kroků: dle potřeby a počtu aplikací s přihlášením.

Očekávané výsledky: vrácené chybové hlášení.

Kroky testu:

- Přihlášení do aplikace pod identitou ID1,
- odeslání http příkazu s parametrem PAR_LoginUsername = ID2,
- ověření, zda aplikace vrátí chybové hlášení, nebo pokračuje dále.