Smlouva o provedení externích penetračních testů

Č. j.	SÚJB/OI/15513/2016
Číslo smlouvy objednatele	16/05/0075
Číslo smlouvy zhotovitele	60212896-ICT0001

Smluvní strany

Objednatel	Česká republika – Státní úřad pro jadernou bezpečnost
Sídlo	Senovážné náměstí 9, 110 00 Praha 1
IČO	48136069
DIČ	není plátcem DPH
Zastoupený	Ing. Danou Drábovou, Ph.D., předsedkyní SÚJB
Bankovní spojení	ČNB Praha
Číslo účtu	3808881/0710

a

Zhotovitel	T-Mobile Czech Republic a.s. Zapsaný v obchodním rejstříku pod sp. zn. B 3787 vedenou Městským soudem v Praze
Sídlo	Tomíčkova 2144/1, Praha 4, PSČ 148 00
IČO	64949681
DIČ	CZ64949681
Zastoupený	Ing. Miroslavem Kláskem a Ing. Liborem Komárkem, na základě pověření (viz příloha č. 1 této smlouvy)
Bankovní spojení	
Číslo účtu	

I. Úvodní ustanovení

Smluvní strany uzavírají tuto smlouvu podle § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, na základě výsledku zadávacího řízení T004/16V/00022596 vyhlášeného na elektronickém tržišti TENDERMARKET jako veřejná zakázka malého rozsahu.

II. Předmět smlouvy

1. Zhotovitel se zavazuje, že na svůj náklad, na své nebezpečí, v souladu s touto smlouvou a ve sjednané době provede externí penetrační testy s cílem prověřit zabezpečení veřejné infrastruktury SÚJB dostupné z internetu (dále jen „dílo“) a objednatel se zavazuje řádně a včas provedené dílo převzít a zaplatit za něj cenu podle článku III. Podrobnosti k provedení testů jsou uvedeny v příloze č. 2,

III. Cena

1. Celková cena díla je 135.380,- Kč bez DPH (slovy stotřicetpěttisíctřistaosmdesát korun českých), cena s DPH je 163.809,80 Kč (slovy stošedesáttřitisícosmsetdevět korun českých osmdesát-haléřů).
2. Tato cena je nejvýše přípustná a nepřekročitelná a zahrnuje veškeré náklady zhotovitele spojené s řádným provedením díla.
3. Cena může být změněna při změně právních předpisů určujících sazby daně z přidané hodnoty, a to o stejnou výši, o jakou bude zvýšena nebo snížena sazba DPH. Na změnu

®certified; faflakovai; 29.8.2016
12:33:08; 1142390/280249

ceny se v takovém případě nebude uzavírat písemný dodatek a cena bude účtována podle právních předpisů platných v době uskutečnění zdanitelného plnění.

IV. Platební podmínky

1. Cena bude zaplacena na základě faktury vystavené zhotovitelem. Zhotovitel vystaví na základě předání Závěrečné zprávy vypracované ve struktuře podle přílohy č. 2 a Protokolu o předání a převzetí díla fakturu do 10 dnů od předání a převzetí díla.
2. Lhůta splatnosti faktury je 21 dnů ode dne dodání faktury objednateli.
3. Faktura musí obsahovat všechny náležitosti dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a číslo smlouvy objednatele.
4. Pokud faktura nebude obsahovat všechny smlouvou a zákonem stanovené náležitosti, je objednatel oprávněn ji do data splatnosti vrátit s tím, že zhotovitel je poté povinen vystavit novou fakturu s novou lhůtou splatnosti v délce 21 dnů. V takovém případě není objednatel v prodlení s úhradou.
5. Pokud objednatel uplatní nárok na odstranění vady díla ve lhůtě splatnosti faktury, není objednatel povinen až do odstranění vady díla uhradit cenu díla. Okamžikem odstranění vady díla začne běžet nová lhůta splatnosti faktury v délce 21 dnů.
6. Cena díla bude uhrazena bezhotovostně na účet zhotovitele a považuje se za uhrazenou okamžikem odepsání ceny díla z bankovního účtu objednatele.
7. Objednatel nebude poskytovat zhotoviteli jakékoliv zálohy na úhradu ceny díla nebo jeho části.

V. Doba a místo plnění

1. Místem provádění díla je sídlo zhotovitele.
2. Zhotovitel se zavazuje započít s prováděním díla dnem podpisu smlouvy a dílo dokončit včetně vypořádání připomínek do 35 dnů od podpisu smlouvy.

VI. Provádění díla

1. Zhotovitel se zavazuje provést dílo s potřebnou odbornou péčí a v obvyklé kvalitě.
2. Zhotovitel je povinen dbát pokynů objednatele a při provádění díla postupovat tak, aby na majetku objednatele nebo třetích osob nezpůsobil žádnou škodu.
3. Zhotovitel není oprávněn poskytnout jakékoliv informace o provádění díla, zejména o výsledcích penetračních testů třetí osobě.
4. Objednatel je povinen poskytnout zhotoviteli součinnost při provádění díla, a to v takovém rozsahu, aby zhotovitel nebyl v prodlení s plněním podle této smlouvy.
5. Pro provedení díla bude vytvořen projektový tým, ve kterém budou zastoupeni i zástupci objednatele. Za každou stranu bude určen odpovědný pracovník. Ze strany objednatele bude odpovědný pracovník vybaven pravomocí sjednávat dílčí pracovní termíny, případně operativní změny v harmonogramu prací. Dále bude mít pravomoc podepsat Protokol o předání a převzetí díla v zastoupení objednatele.
6. Projektový tým povede Vedoucí projektu za zhotovitele. Způsob komunikace projektového týmu a další detaily řízení projektu upřesní Projektový tým na začátku provádění díla.
7. V případech, kdy bude nutno pro zpracování některých výstupů využít interních kapacit objednatele, bude tak postupováno po dohodě s objednatelem.
8. Zhotovitel nesmí k provedení díla využít třetí osoby.

®certified; faflakovai; 29.8.2016
12:33:08; 1142390/280249

9. Smluvní strany se zavazují, že s informacemi, které jim budou poskytnuty nebo které získají v souvislosti s plněním podle této smlouvy, budou nakládat způsobem odpovídajícím požadavkům právních předpisů, poskytnou jim řádnou ochranu, neposkytnou je třetí osobě a řádně tyto informace během plnění smlouvy zabezpečí před přístupem nepovolaných osob a zneužitím.
10. Objednatel je oprávněn si kdykoli vyžádat informace o stavu díla v průběhu provádění díla. Zhotovitel musí tyto informace poskytnout objednateli ve lhůtě 3 dnů.
11. Dílo bude předáno objednateli ve formě Závěrečné zprávy v českém jazyce dodané osobně jedenkrát digitálně, ve formátu Microsoft Word (DOC, DOCX), na nezavirovaném CD/DVD, a dvakrát analogově, v tištěné podobě.
12. Zhotovitel se zavazuje před dodáním díla v elektronické formě k provedení ochranných opatření proti zavirování. V případě zjištění zavirování díla zhotovitel neprodleně dodá dílo v nezavirované podobě.

VII. Předání a převzetí díla

1. Místem předání a převzetí díla je sídlo objednatele.
2. Smluvní strany se dohodly na ukončení penetračních testů a předání návrhu Závěrečné zprávy včetně prezentace výsledků v sídle zadavatele do 21 dnů od podpisu smlouvy.
3. Objednatel po předání návrhu Závěrečné zprávy do 7 dní uplatní připomínky a zjištěné vady formou zápisu o připomínkách a vadách (dále jen „zápis“) a zhotovitel do 7 dní od předání zápisu vypořádá připomínky, opraví vady díla a předá Závěrečnou zprávu.
4. Dílo bude předáno a převzato předáním Závěrečné zprávy a podpisem Protokolu o předání a převzetí díla odpovědnými pracovníky obou smluvních stran podle článku VI bodu 5, jejichž přehled je uveden v příloze č. 3, v sídle objednatele. Protokol o předání a převzetí díla bude vyhotoven ve dvou stejnopisech.
5. Dílo nesmí v okamžiku předání obsahovat vady.
6. Objednatel není povinen převzít dílo, které má vady. Nepřevezme-li objednatel dílo z tohoto důvodu, není v prodlení. Vady musí být objednatelem specifikovány v zápisu podepsaném odpovědnými pracovníky obou stran a tyto vady je zhotovitel povinen odstranit do 7 dnů. Po uplynutí lhůty k odstranění vad postupují smluvní strany podle odstavce 4.

VIII. Vady díla

1. Zhotovitel se zavazuje provést dílo bez vad.
2. Práva z vadného plnění má objednatel v rozsahu stanoveném příslušnými ustanoveními občanského zákoníku, není-li ve smlouvě stanoveno jinak.
3. Má-li být vada díla odstraněna, je zhotovitel povinen ji odstranit bezplatně bez zbytečného odkladu, nejpozději do 7 dnů od oznámení vady objednatelem.

IX. Sankční ustanovení

1. Zhotovitel, který bude v prodlení s plněním podle smlouvy, zaplatí objednateli smluvní pokutu ve výši 0,05 % z ceny díla za každý den prodlení. Zhotovitel, který nedodrží ustanovení článku VI bodu 3, zaplatí objednateli smluvní pokutu ve výši 150 000,- Kč Smluvní pokuta je splatná do 21 dnů od data, kdy byla zhotoviteli doručena písemná výzva k jejímu zaplacení.

®certified; faflakovai; 29.8.2016
12:33:08; 1142390/280249

2. Objednatel, který bude v prodlení s úhradou faktury, je povinen zaplatit zhotoviteli úrok z prodlení ve výši 0,05 % z nezaplacené částky faktury za každý den prodlení. Úrok z prodlení je splatný do 21 dnů od data, kdy byla objednateli doručena písemná výzva k jeho zaplacení.
3. Zaplacením smluvní pokuty není dotčeno právo na náhradu škody vzniklé z porušení povinnosti, ke které se smluvní pokuta vztahuje.
4. Objednatel je oprávněn odstoupit od smlouvy v případě prodlení zhotovitele, které přesáhne 30 dnů.
5. Zhotovitel je oprávněn odstoupit od smlouvy v případě prodlení objednatele se zaplacením ceny díla, které přesáhne 30 dnů.
6. Odstoupení od smlouvy musí mít písemnou formu.

X. Vlastnické právo a práva autorská

1. Okamžikem předání a převzetí díla nabývá objednatel vlastnické právo k dílu a všem dílčím výstupům vzniklým při provádění díla a přechází nebezpečí škody na díle.
2. Zhotovitel se zavazuje, že neposkytne dílo ani jeho části třetí osobě bez písemného souhlasu objednatele.
3. Zhotovitel se zavazuje při provádění díla neporušit práva třetích osob, která těmto osobám mohou plynout z práv k duševnímu vlastnictví, zejména z autorských práv a práv průmyslového vlastnictví. Zhotovitel se zavazuje objednateli uhradit veškeré náklady, výdaje a majetkovou i nemajetkovou újmu, které objednateli vzniknou v důsledku uplatnění práv třetích osob vůči objednateli v souvislosti s porušením povinnosti zhotovitele podle předchozí věty.

XI. Závěrečná ustanovení

Zhotovitel není oprávněn dílo ani dílčí výstupy vzniklé při provádění díla poskytnout třetím osobám.

1. Tuto smlouvu je možné měnit pouze po dohodě smluvních stran, a to formou písemného číslovaného dodatku.
2. Tato smlouva je vyhotovena ve čtyřech stejnopisech. Každá ze smluvních stran obdrží dva stejnopisy.
3. Objednatel se zavazuje zveřejnit tuto smlouvu podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).
4. Smluvní strany souhlasí se zveřejněním celého obsahu smlouvy prostřednictvím registru smluv.

®certified; faflakovai; 29.8.2016
12:33:08; 1142390/280249

5. Nedílnou součástí této smlouvy jsou tyto přílohy:
Příloha č. 1 – Pověření Ing. Miroslava Kláska a Ing. Libora Komárka
Příloha č. 2 - Podrobnosti plnění díla
Příloha č. 3 – neveřejná - Odpovědní pracovníci

Za objednatele
V Praze dne ...

Za zhotovitele
V Praze dne

Ing. Dana Drábová, Ph.D.
předsedkyně

Ing. Miroslav Klásek
Senior manažer presalesu

Za zhotovitele
V Praze dne

Ing. Libor Komárek
Senior manažer prodeje státní správě

®certified; faflakovai; 29.8.2016
12:33:08; 1142390/280249

Příloha č. 1 – Pověření

POVĚŘENÍ

Společnost T-Mobile Czech Republic a.s., se sídlem v Praze 4, Tomíčkova 2144/1, PSČ 149 00, IČ 64949681, (dále jen „Společnost") jednající prostřednictvím představenstva Společnosti tímto **p o v ě ř u j e** níže uvedeného zaměstnance:

Ing. Libora KOMÁRKA
nar. 25. 08. 1967

aby za Společnost jednal a vykonával:

- veškeré úkony, které souvisí se smlouvami o poskytování služeb elektronických komunikací služeb a o prodeji komunikačního zařízení a jejich příslušenství firemním zákazníkům a se smlouvami o zprostředkování anebo spolupráci při uzavírání uvedených smluv; zejména se jedná o uzavírání, změny a ukončování takových smluv,
- veškeré úkony, které souvisí se smlouvami, které upravují komplexní řešení ProfiNet, prodej jakýchkoli nehlasových služeb a služeb s přidanou hodnotou; zejména se jedná o uzavírání, změny a ukončování takových smluv,
- veškeré úkony, které souvisí se smlouvami o poskytování ICT řešení, jež upravují podmínky pronájmu komunikačních zařízení a souvisejícího vybavení vč. požadované softwarové podpory; zejména se jedná o uzavírání, změny a ukončování takových smluv,
- veškeré úkony podle zákona o veřejných zakázkách, to znamená, aby podával nabídky a prováděl veškeré právní úkony ve veřejných zakázkách a výběrových řízeních, zejména svým čestným prohlášením prokazoval základní i další kvalifikační předpoklady pro plnění veřejné zakázky.

Zmocněnec není oprávněn zmocnit ani jinak pověřit jinou osobu, aby místo něho jednala za Společnost, s výjimkou oprávnění ke zmocnění zaměstnanců Společnosti, aby místo pověřeného zaměstnance zastupovali Společnost při otevírání obálek, prohlídce místa plnění, nebo při ústním vysvětlení nabídky v termínech stanovených zadavateli veřejných zakázek v jednotlivých výběrových řízeních. Pověřený zaměstnanec dále není oprávněn jakýkoli majetek Společnosti převádět či zatěžovat právy třetích osob.

Podepisování pověřeného zaměstnance se děje tak, že k napsané nebo vytištěné obchodní firmě společnosti či otisku razítka společnosti připojí pověřený zaměstnanec svůj podpis.

V Praze dne 17. března 2016

Mark Klein
předseda představenstva

Martin Schlieker
člen představenstva

Toto pověření přijímám:

Ing. Libor Komárek

T-Mobile Czech Republic a.s., Tomíčkova 2144/1, 148 00 Praha 4, Czech Republic, IČ: 64949681, DIČ: CZ64949681
Zapsaná do OR u Městského soudu v Praze, B.3787

®certified; faflakovai; 29.8.2016
12:33:08; 1142390/280249

POVĚŘENÍ

Společnost T-Mobile Czech Republic a.s., se sídlem v Praze 4, Tomíčkova 2144/1, PSČ 149 00, IČ 64949681, (dále jen „Společnost") jednající prostřednictvím představenstva Společnosti tímto **pověřuje** níže uvedeného zaměstnance:

Ing. Miroslava KLÁSKA
nar. 23. 6. 1975

aby za Společnost jednal a vykonával:

- veškeré úkony, které souvisí se smlouvami o poskytování služeb elektronických komunikací služeb a o prodeji komunikačního zařízení a jejich příslušenství firemním zákazníkům a se smlouvami o zprostředkování anebo spolupráci při uzavírání uvedených smluv; zejména se jedná o uzavírání, změny a ukončování takových smluv,
- veškeré úkony, které souvisí se smlouvami, které upravují komplexní řešení ProfiNet nebo Firemní řešení, prodej jakýchkoli nehlasových služeb a služeb s přidanou hodnotou; zejména se jedná o uzavírání, změny a ukončování takových smluv, popř. smlouvy budoucí,
- veškeré úkony, které souvisejí se smlouvami o bezpečnostním auditu, zachování důvěrnosti informací a prodeji a servisu hardware, zejména se jedná o uzavírání, změny a ukončování takových smluv.
- veškeré úkony, které souvisí se smlouvami o poskytování ICT řešení, jež upravují podmínky pronájmu komunikačních zařízení a souvisejícího vybavení vč. požadované softwarové podpory; zejména se jedná o uzavírání, změny a ukončování takových smluv,
- veškeré úkony podle zákona o veřejných zakázkách, to znamená, aby podával nabídky a prováděl veškeré právní úkony ve veřejných zakázkách a výběrových řízeních, zejména svým čestným prohlášením prokazoval základní i další kvalifikační předpoklady pro plnění veřejné zakázky.

Zmocněnec není oprávněn zmocnit ani jinak pověřit jinou osobu, aby místo něho jednala za Společnost, s výjimkou oprávnění ke zmocnění zaměstnanců Společnosti, aby místo pověřeného zaměstnance zastupovali Společnost při otevírání obálek, prohlídce místa plnění, nebo při ústním vysvětlení nabídky v termínech stanovených zadavateli veřejných zakázek v jednotlivých výběrových řízeních. Pověřený zaměstnanec dále není oprávněn jakýkoli majetek Společnosti převádět či zatěžovat právy třetích osob.

Podepisování pověřeného zaměstnance se děje tak, že k napsané nebo vytištěné obchodní firmě společnosti či otisku razítka společnosti připojí pověřený zaměstnanec svůj podpis.

V Praze dne 17. března 2016

Mark Klein
předseda představenstva

Martin Schlieker
člen představenstva

Toto pověření přijímám:

Ing. Miroslav Klásek

®certified; faflakovai; 29.8.2016
12:33:08; 1142390/280249

Příloha č. 2 – Podrobnosti plnění díla

Externí penetrační test:
Objednatel požaduje identifikaci všech otevřených portů a služeb, popis slabin pro všechny potenciálně zranitelné služby a návrh doporučení.
Objednatel požaduje manuální prověření nálezů tak, aby byly vyfiltrovány false-positive nálezy. Zranitelnosti mohou být prozkoumány až na úroveň identifikace konkrétních exploitů, nicméně jejich použití, které by mohlo narušit důvěrnost, integritu či dostupnost systémů musí být konzultováno s objednatelem.

Provedení „black-box test“.

IPv4 rozsah:

- **80.95.112.0/24**

IPv6 rozsah:

- **2a00:11b0:f100:400::242 hornet.erc-cr.cz**
- **2a00:11b0:f100:400::246 www.sujb.cz**
- **2a00:11b0:f100:400::247 ns.erc-cr.cz**

Test webových aplikací:
Provedení „black-box test“.

URL:

- **http://www.sujb.cz**
- **http:// www.sujb.cz/monras/aplikace/monras_cz.html**
- **https://www.sujb.cz/ireg/priv/irdpo/list_dp.jsp?**

Testování proběhne v souladu s metodikou OWASP Testing Guide

Externí penetrační testy
Metodika penetračních testů zhotovitele vychází ze standardu OSSTMM a metodologie OWASP. Metodika bude upravena po detailním seznámení s prostředím objednatele. Vhodnost metodiky bude ověřena v rámci první iterace penetračních testů. Metodika umožňuje provádět a zkoušet nové testy a reagovat tak na vývoj zranitelností HW a SW.
Realizace bude provedena dle testovacích plánů, které budou přesně specifikovat způsob, rozsah a metodu testování.
Seznam testů a jejich popis bude uveden v návrhu testů. Přesný postup ověření zranitelnosti ve specifickém prostředí bude popsán v Závěrečné zprávě, která bude výsledkem externích penetračních testů.

Fáze externího penetračního testu
• příprava testovacího plánu a schválení plánu,
• provedení penetračního testu dle plánu a jeho vyhodnocení.
1) Příprava testovacího plánu

®certified; faflakovai; 29.8.2016
12:33:08; 1142390/280249

Zhotovitel připraví a navrhne rozsah testu, jeho typ, naplánuje čas a datum provedení testu a určí cílové komponenty nebo systémy. V této fázi komunikuje Zástupce pro technická jednání zhotovitele s objednatelem, který poskytuje součinnost a informace nutné k provedení testovacího plánu.
Plánovaný penetrační test a jeho rozsah musí být schválen Zástupcem pro technická jednání objednatele. V rámci schválení penetračního testu se objednatel seznámí s rozsahem testu, cílovými systémy, které jsou předmětem testu a souvisejícími riziky. Objednatel může k posouzení žádosti vyžadovat další informace od zhotovitele apod. Objednatel může omezit rozsah testu, navrhnout a implementovat další opatření před provedením penetračního testu.

2) Provedení penetračního testu
V této fázi zhotovitel provede cílený penetrační test dle metodiky a schváleného testovacího plánu. V případě, že by zhotovitel nalezl zranitelnost, která nesnese odkladu a významně ohrožuje bezpečnost systému, oznámí tuto skutečnost objednateli.

Fáze provedení penetračního testu
1. **Příprava testovacích nástrojů** – aktualizace nástrojů nebo jejich bází dat.
2. **Sběr informací** – sběr informací a to pasivně dostupnými prostředky nebo aktivně síťovými skenery. Síťové skenery zahajují aktivitu na sítí a testují porty systémů, služby a jejich verze. V této fázi zhotovitel detekuje existující moduly a pluginy určité aplikace. Typickým nástrojem této kategorie je síťový skener Nmap, bezpečnostní skener Nessus a aplikační skener Nikto nebo veřejné služby Whois, DNS. Nástroje se liší podle typu cílového systému a služeb, které na něm běží.
3. **Analýza zranitelností systémů** - na základě informací o dostupných službách (otevřených portech) a jejich verzích zhotovitel vyhledá zdokumentované zranitelnosti.
4. **Exploitace zranitelností** - získání přístupu do systému použitím programu, který využívá zranitelnost aplikace s cílem spustit vlastní kód. Takovým programem (exploitem) může být jednoduchý skript v jazyce C, perlu nebo pythonu, který zranitelnost vyvolá a pošle do aplikace kód, který zpravidla vytvoří uživatele nebo spustí vzdálený shell na síťovém portu. Typickým příkladem pokročilejších nástrojů pro exploitaci je metasploit framework obsahující sadu otestovaných exploitů nebo Core Impact Pro. Existují i veřejně dostupné databáze exploitů, ale každý takový program je potřeba otestovat v laboratorních podmínkách, zda nenaruší intergitu systému a neobsahuje další nežádoucí instrukce. V případě webových aplikací jsou typickými nástroji BurpSuite – webová proxy s doplňujícími moduly pro manuální testování, sada vstupů (řetězců) pro testy zranitelností XSS, CSRF, nástroj SQLmap pro testy zranitelností typu SQL Injection a nástroje pro lámání hesel online nebo offline (THC Hydra, Medusa, Hashcat nebo John the Ripper).
5. **Postexploitace** - eskalace práv uživatele na administrátora systému a získání přístupu k dalším systémům. Součásti této fáze je i pochopení role systému, komunikace s ostatními systémy, obsah diskového prostoru, běžící procesy, existující skripty, výčet existujícího softwaru, uživatelské a aplikační účty, lámání jejich hesel, získání přístupu do databáze apod.

®certified; faflakovai; 29.8.2016
12:33:08; 1142390/280249

3) Vyhodnocení penetračního testu
Zhotovitel vyhotoví Závěrečnou zprávu o nálezech zranitelností, která popisuje zjištění na základě provedeného penetračního testu. Zpráva u každé zranitelnosti klasifikuje její závažnost, místo výskytu, postup ověření zranitelnosti a jednoznačný odkaz testu v metodice, resp. ve standartu, který je součástí metodiky. Součástí zprávy je také doporučená strategie nápravy, tj. jak zranitelnosti odstranit a v jakém pořadí.

Metody a postupy pro testování webové části
Penetrační testy pro ověření webových částí se řídí metodikou OWASP, přesněji dokumentem OWASP Testing.
Penetrační test webové aplikace navazuje na metodiku v části – Fáze provedení penetračního testu (v bodech: sběr informací, analýza zranitelností a exploitace) a obecně probíhá v následujících fázích:
1. Sběr informací a identifikace počtu webových rozhraní a technologií.
2. Použití aplikace z hlediska uživatele, pochopení funkčnosti a použití aplikace v různých režimech (návštěvník, uživatel, případně administrátor, obnova a reset hesla).
3. Rozpoznání hranic webové aplikace a interakce s dalšími systémy.
4. Systematické mapování webových stránek, vstupních parametrů a polí přenášených http protokolem.
Pomocí nástroje webové proxy (BurpSuite) v manuálním režimu nebo v automatickém módu (Crawler) vytváří penetrační tester HTTP požadavky na jednotlivé stránky a mapuje chování a jednotlivé odpovědi, adresářovou strukturu a celkový model aplikace.
5. Testování webových stránek stránku po stránce a zkoušení různých kombinací vstupních parametrů. V případě podezření zranitelnosti tester dokumentuje pozorované chování a snaží se zranitelnost exploitovat.
Zhotovitel je v průběhu testování provázen dokumentem OWASP Testing Guide v.4 (od kapitoly 4 – Web Application Security), kde je definováno celkově 92 kontrol (rozuměj bezpečnostních testů) celkem v jedenácti kategoriích.

STRUKTURA ZÁVĚREČNÉ ZPRÁVY
Struktura zprávy:
1. Manažerský souhrn – stručný průřez průběhu testu společně s výsledky.
2. Popis testu – popis metodiky testů a přehled všech prováděných činností.
3. Zjištěné skutečnosti – detailní popis výsledku všech testů jednotlivých zařízení.
4. Shrnutí doporučení – přehled doporučení, kterými lze odstranit nedostatky nalezené v průběhu testu.
5. Závěr

Každý ve zprávě uvedený nález bude klasifikovaný dle závažnosti:
• INFO (informace),
• LOW (dopad nízkého stupně),
• MEDIUM (středně závažný nález),
• HIGH (závažný nález) a
• CRITICAL (kritický nález).

®certified; faflakovai; 29.8.2016
12:33:08; 1142390/280249

Zjištění kritického nálezu bude hlášeno zadavateli okamžitě po zjištění.
Každý nález bude mít uvedené doporučení, které by mělo slabinu a riziko z ní vyplývající eliminovat nebo aspoň snížit. Nálezy/doporučení musí být ve zvláštní kapitole uvedeny přehledně v tabulce.

Zpráva musí obsahovat stručný závěr vhodný pro prezentaci výsledků testů vedení SÚJB.

Prezentace výsledků
Součástí výstupů testu je prezentace výsledků v sídle zadavatele.

®certified; faflakovai; 29.8.2016
12:33:08; 1142390/280249