

SMLOUVA O DÍLO

uzavřená dle ustanovení § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník
(dále jen „občanský zákoník“)

I. SMLUVNÍ STRANY

Česká republika – Ministerstvo školství, mládeže a tělovýchovy

Se sídlem: Karmelitská 529/5, 118 12 Praha 1
Jednající: Mgr. Martin Fíla, ředitel odboru ICT
IČO: 00022985
Bankovní spojení:
Číslo účtu:
(dále jen „Objednatel“).

a

EG ADVISORS.CZ S.R.O.

Se sídlem: Vrázova 2243/7, 150 00 Praha 5
IČO: 27086232
DIČ: CZ27086232
Zapsána v: Obchodním rejstříku vedeném Městským soudem v Praze oddíl C, vložka 95212
Jednající:
Bankovní spojení:
(dále jen „Zhotovitel“)

uzavírají níže uvedeného dne, měsíce a roku na základě vzájemného konsenzu a na základě průzkumu trhu tuto Smlouvu o dílo (dále jen „Smlouva“).

II. ÚČEL SMLOUVY

Účelem této Smlouvy je ověření, zda jsou informační systémy Objednatele zabezpečeny v souladu s platnou legislativou, včetně určení jak vzniklé nálezy eliminovat či snížit.

III. PŘEDMĚT SMLOUVY

- 3.1 Předmětem plnění této Smlouvy je závazek Zhotovitele zajistit provedení externího penetračního testu, který bude zahrnovat zejména dokument-závěrečnou zprávu dle specifikace uvedené v příloze č. 1. a dle legislativních požadavků (zákon č. 181/2014 Sb.) v oblasti informační bezpečnosti dle specifikace uvedené v příloze č. 1, která tvoří nedílnou součást této Smlouvy (dále jen „dílo“).
- 3.2 Zhotovitel se touto Smlouvou zavazuje zpracovat dílo dle specifikace uvedené v příloze č. 1. pro objednatel a objednatel se touto Smlouvou zavazuje řádně a včas provedené dílo převzít a zaplatit cenu díla dle čl. IV. této Smlouvy.

IV. CENA ZA DÍLO

- 4.1 Cena za dílo je sjednána na 392.000,- Kč bez DPH (slovy: tři sta devadesát dva tisíc korun českých. Daň z přidané hodnoty ve výši 21 % činí 82.320,- Kč a celková cena včetně DPH činí 474.320,- Kč (slovy: čtyři sta sedmdesát čtyři tisíc tři sta dvacet korun českých). Sazba daně z přidané hodnoty je ve Smlouvě uvedena v zákonné výši ke dni podpisu Smlouvy. V případě změny sazby DPH v průběhu účinnosti Smlouvy bude cena adekvátně změněna.

- 4.2 Objednatel se zavazuje zaplatit Zhotoviteli dohodnutou cenu za dílo, a to po řádném předání a převzetí díla. O předání a převzetí díla bude smluvními stranami sepsán a podepsán předávací protokol dle čl. VII. této Smlouvy, bez něhož není Zhotovitel oprávněn vystavit fakturu.
- 4.3 Cena je konečná a zahrnuje veškeré náklady spojené s provedením díla, včetně nákladů, které Zhotovitel vynaložil za účelem plnění této Smlouvy. Objednatel neposkytuje zálohy.
- 4.4 Cena za dílo sjednaná v čl. IV. odst. 4.1 této Smlouvy bude uhrazena do 30ti dnů ode dne doručení faktury na adresu objednatele uvedenou v čl. I. této Smlouvy. Faktura musí obsahovat všechny náležitosti účetního dokladu dle § 11 zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a daňového dokladu dle příslušných ustanovení zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. V případě, že faktura nebude obsahovat odpovídající náležitosti, je objednatel oprávněn zaslat ji ve lhůtě splatnosti zpět Zhotoviteli k doplnění, aniž se tak dostane do prodlení se zaplacením. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněné či opravené faktury.
- 4.5 Platba bude uskutečněna bezhotovostním převodem z účtu objednatele na účet Zhotovitele uvedený v čl. I. této Smlouvy, a to v české měně. Za datum úhrady se považuje den odepsání příslušné částky z účtu objednatele.
- 4.6 Zhotovitel je dle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

V. DOBA A MÍSTO PLNĚNÍ

- 5.1 Zhotovitel se zavazuje provést dílo ve lhůtě do 10ti dnů od účinnosti této Smlouvy. Zjistí-li Zhotovitel během provádění díla, že není schopen z jakýchkoli důvodů dílo provést, neprodleně oznámí tuto skutečnost objednateli, který může přiměřeně prodloužit dobu plnění, a to zejména, je-li zpoždění s prováděním díla vyvoláno objektivními důvody, na jejichž vznik neměl Zhotovitel žádný vliv, nebo jejich vznik nemohl ovlivnit. Ostatní činnosti podle přílohy č. 1 související s dílem bude Zhotovitel provádět průběžně a v přiměřené lhůtě podle požadavků objednatele do 10 dnů od předání podkladů.
- 5.2 Zhotovitel provede dílo v místě určeném dle přílohy č. 1., přičemž kroky směřující k provedení díla je oprávněn činit dle svého uvážení a odbornosti i jinde s tím, že takový postup nebude mít vliv na kvalitu provedení díla.

VI. PRÁVA A POVINNOSTI SMLUVNÍCH STRAN

- 6.1 Zhotovitel je povinen provádět dílo s potřebnou péčí, odborně, v souladu s právními předpisy, které se k danému předmětu plnění vztahují a podle požadavků uvedených v příloze č. 1. této Smlouvy a v termínu uvedeném v čl. V, resp. tak, aby bylo dosaženo cíle a účelu plnění.
- 6.2 Zhotovitel je povinen chránit a prosazovat práva a oprávněné zájmy Objednatele a řídit se jeho pokyny. Zjistí-li Zhotovitel, že pokyny Objednatele jsou nevhodné či neúčelné nebo v rozporu se zákonem a jinými právními předpisy, je povinen Objednatele na tuto skutečnost upozornit. Bude-li Objednatel přes toto upozornění na splnění svých pokynů trvat, má Zhotovitel právo požádat o písemné potvrzení pokynu nebo přerušit provádění díla za předpokladu, že pokyny jsou v rozporu se Smlouvou, nebo platnými právními předpisy. Zhotovitel se zavazuje oznámit Objednateli všechny okolnosti, které zjistil při plnění předmětu Smlouvy, které mohou mít vliv na změnu pokynů Objednatele.
- 6.3 Zhotovitel dává Objednateli souhlas s využíváním údajů o dílu a poskytování informací o dílu třetím osobám v rozsahu nezbytném pro účely administrace, a pro účely informovanosti a publicity specifikovanými v příslušných právních předpisech, především v zákoně č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů a v Nařízení Komise (ES) č. 1828/2006 ze dne 8. prosince 2006, kterým se stanoví prováděcí pravidla k nařízení Rady (ES) č. 1083/2006 o Evropském fondu pro regionální rozvoj.
- 6.4 Zhotovitel je povinen dodržet požadovanou certifikaci ISMS specialista dle metodiky norem ČSN EN 27001-2.
- 6.5 Zhotovitel je povinen Objednatele na jeho žádost informovat o průběhu plnění Smlouvy.
- 6.6 Zhotovitel je povinen neprodleně Objednateli písemně oznámit překážky, které mu brání v plnění a výkonu dalších činností souvisejících s plněním předmětu Smlouvy.

- 6.7 Zhotovitel se zavazuje k uchování účetních záznamů a dalších relevantních podkladů souvisejících s poskytnutím služeb dle platných právních předpisů.
- 6.8 Objednatel se zavazuje poskytnout Zhotoviteli veškerou nezbytnou součinnost k tomu, aby dílo mohlo být provedeno řádně a včas podle této Smlouvy.
- 6.9 Objednatel je povinen řádně a včas zaplatit za dodané plnění ze strany Zhotovitele.

VII. PŘEDÁNÍ A PŘEVZETÍ DÍLA

- 7.1 Zhotovitel je povinen předat dílo objednateli včas, v požadované kvalitě dle přílohy č. 1 této Smlouvy a bez jakýchkoli faktických či právních vad. O přesném termínu a způsobu předání díla vyrozumí Zhotovitel objednatele minimálně tři dny předem, a to písemně nebo elektronicky.
- 7.2 O předání a převzetí díla bude smluvními stranami sepsán předávací protokol. Předávací protokol bude obsahovat zejména specifikaci předávaného díla, místo a datum jeho předání, jakož i výslovné prohlášení objednatele, zda dílo přebírá či nikoli a pokud ne, z jakých důvodů.
- 7.3 Objednatel je oprávněn odmítnout převzetí díla, bude-li se na něm či jeho části vyskytovat v okamžiku předání vada či více vad s výjimkou ojedinělých drobných vad, které je však Zhotovitel povinen odstranit neprodleně po převzetí díla. O odmítnutí převzetí díla bude rovněž sepsán protokol, v němž budou specifikovány vady díla, případně jiná porušení této Smlouvy.
- 7.4 Převzetím díla objednatel, přechází na objednatele veškerá vlastnická práva a autorská oprávnění a objednatel je dále oprávněn použít dílo k účelům, které budou v souladu s jeho potřebami, jakožto i k předání díla třetím stranám.

VIII. ZÁRUKA ZA JAKOST, PRÁVA Z VAD

- 8.1 Zhotovitel odpovídá za vady díla, pokud byly způsobeny porušením jeho povinností.
- 8.2 Objednatel je povinen zjištěné vady bezodkladně oznámit Zhotoviteli, a to písemně, telefonicky či elektronickou poštou nebo jiným prokazatelným způsobem. Uplatní-li objednatel právo z vadného plnění, potvrdí mu Zhotovitel v písemné formě, kdy objednatel právo uplatnil, jakož i datum provedení opravy, je-li možná nebo dohodnutá. Zhotovitel je povinen vady odstranit v dohodnuté lhůtě, nejpozději však do 10 dnů ode dne, kdy objednatel právo z vadného plnění uplatnil.

IX. ODPOVĚDNOST ZA ŠKODU

Pokud porušením povinností Zhotovitele vyplývajících z obecně závazných právních předpisů či z této Smlouvy vznikne objednateli škoda, a to i v důsledku užívání díla, odpovídá za ni Zhotovitel, a to bez ohledu na zavinění.

X. DŮVĚRNOST INFORMACÍ

- 10.1 Zhotovitel se zavazuje během plnění Smlouvy i po uplynutí doby, na kterou je tato Smlouva uzavřena, zachovávat mlčenlivost o všech skutečnostech, o kterých se při provádění díla dozví, a nakládat s nimi jako s důvěrnými (s výjimkou informací, které již byly veřejně publikované).
- 10.2 Zhotovitel se zavazuje, že pokud v souvislosti s realizací této Smlouvy při plnění svých povinností přijdou jeho pověřeni zaměstnanci do styku s osobními údaji ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, učiní veškerá opatření, aby nedošlo k neoprávněnému nebo nahodilému přístupu k těmto údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož aby i jinak neporušil tento zákon. Zhotovitel nese plnou odpovědnost za případné porušení zákona z jeho strany.
- 10.3 Zhotovitel není oprávněn jakkoliv využít informace, údaje a dokumentaci, která mu byla zpřístupněna v souvislosti s prováděním díla, ve prospěch svůj nebo ve prospěch třetí osoby. Zhotovitel je povinen dodržovat tyto povinnosti také po ukončení tohoto smluvního vztahu.
- 10.4 Zhotovitel je povinen učinit veškerá nezbytná opatření k ochraně informací a údajů zpřístupněných Objednatel.

XI. SMLUVNÍ SANKCE

- 11.1 Pro případ nedodržení sjednané doby plnění ze strany Zhotovitele se Zhotovitel zavazuje zaplatit objednateli smluvní pokutu ve výši 0,1 % z ceny díla vč. DPH., a to za každý i započatý den prodlení. Smluvní pokuta ve stejné výši se sjednává i pro případ, že Zhotovitel neodstraní vadu ve lhůtě dle čl. VIII. této Smlouvy.
- 11.2 Zhotovitel se dále zavazuje uhradit Objednateli smluvní pokutu v případě porušení povinnosti mlčenlivosti specifikované v čl. X. této Smlouvy ve výši 100.000,- Kč, a to za každý jednotlivý případ porušení povinnosti.
- 11.3 V případě prodlení Objednatele s úhradou dle této Smlouvy je Zhotovitel oprávněn požadovat nejvýše zákonný úrok z prodlení, jiné sankce vůči Objednateli jsou nepřipustné.
- 11.4 Smluvní pokuty jsou splatné do 30 dnů po obdržení písemné výzvy oprávněné strany k jejímu zaplacení na adresu sídla povinné smluvní strany. Zaplacením smluvní pokuty není dotčeno právo na náhradu případně vzniklé škody.

XII. ODSTOUPENÍ OD SMLOUVY

- 12.1 Od této Smlouvy může kterákoli smluvní strana odstoupit, byla-li Smlouva porušena podstatným způsobem druhou smluvní stranou. Za podstatné porušení je ze strany Zhotovitele považováno více než 5 denní prodlení s předáním díla nebo opakované předání vadného díla nebo neodstranění vad ve lhůtě stanovené v čl. VIII. této Smlouvy. Za podstatné porušení Smlouvy ze strany objednatel se považuje více než 30denní prodlení s úhradou faktury oproti splatnosti sjednané v čl. IV. této Smlouvy. Účinky odstoupení od Smlouvy nastávají dnem, kdy je písemné odstoupení doručeno druhé smluvní straně.
- 12.2 Smluvní strany jsou povinny vypořádat vzájemné své závazky, zejména Zhotovitel vrátit objednateli veškeré obdržené platby a objednatel uhradit to, na co má Zhotovitel neprovedením díla rádně a včas, resp. provedením vadného díla podle zákona, a je-li to obvyklé, nárok. O vzájemném vypořádání svých závazků pořídí smluvní strany zápis.

XIII. KONTAKTNÍ OSOBY

- 13.1 Kontaktní osobou zodpovědnou za Objednatele ve všech záležitostech je:
- 13.2 Kontaktní osobou odpovědnou za Zhotovitele ve všech záležitostech je:
- 13.3 O případných změnách kontaktních osob musí být vždy písemně informována druhá smluvní strana.

XIV. ZÁVĚREČNÁ UJEDNÁNÍ

- 14.1 Tato Smlouva nabývá platnosti dnem jejího podpisu druhou ze smluvních stran. Účinnosti nabývá Smlouva dnem jejího zveřejnění v registru smluv dle zákona č. 340/2015 Sb., zákon o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv. Realizace plnění je tedy možná až od data účinnosti.
- 14.2 Tato Smlouva se uzavírá v písemné formě, veškeré její změny je možno učinit jen v písemné formě, a to vzestupně číslovanými dodatky podepsanými oběma smluvními stranami. Změny kontaktních osob nebo změny fakturačních údajů je možno provést pouze na základě písemného oznámení druhé smluvní straně.
- 14.3 Tato Smlouva byla vyhotovena ve třech stejnopisech, z nichž Objednatel obdrží dvě vyhotovení a Zhotovitel jedno vyhotovení.
- 14.4 Pokud se kterékoli ustanovení této Smlouvy stane nebo bude shledáno neplatným nebo nevymahatelným, nebude tím dotčena platnost a vymahatelnost ostatních ustanovení této Smlouvy. Smluvní strany se zavazují rádně jednat za účelem nahrazení neplatného či nevymahatelného ustanovení ustanovením platným a vymahatelným v souladu s účelem této Smlouvy.

- 14.5 Smluvní strany se zavazují pokusit se vyřešit smírně jakýkoli spor mezi smluvními stranami, sporný nárok nebo spornou otázku vzniklou v souvislosti s touto Smlouvou (včetně otázek týkajících se její platnosti, účinnosti a výkladu). Nepovede-li tento postup k vyřešení sporu, bude spor předložen k rozhodnutí příslušnému soudu v České republice.
- 14.6 Práva a povinnosti smluvních stran výslovně v této Smlouvě neupravené se řídí příslušnými ustanoveními občanského zákoníku.
- 14.7 V souladu se zákonem o registru smluv zajistí Objednatel uveřejnění celého textu smlouvy, vyjma osobních údajů, a metadat smlouvy v registru smluv včetně případných oprav uveřejnění s tím, že nezajistí-li Objednatel uveřejnění smlouvy nebo metadat smlouvy v registru smluv do 30 dnů od uzavření smlouvy, pak je oprávněn zajistit jejich uveřejnění Zhotovitel ve lhůtě tří měsíců od uzavření smlouvy. Zhotovitel rovněž souhlasí s tím, že metadata vztahující se k této Smlouvě mohou být zveřejněna též na webových stránkách Objednatele.

Přílohy:

Příloha č. 1: Specifikace předmětu Smlouvy

V Praze dne 5.12.2017

v Praze dne 6.12.2017

Za Objednatele:


za Zhotovitele:

.....

.

.....

Mgr.
ředitel odboru ICT

 EG advisors s.r.o.
Vrázova 2243/7
150 00 Praha 5
IČ: 270 66 232

PŘÍLOHA Č. 1 SMLOUVY

Specifikace předmětu Smlouvy:

Požadujeme provedení externího penetračního testu v následujícím rozsahu:

- Identifikaci všech otevřených portů a služeb.
- Popis slabín pro všechny potenciálně zranitelné služby.
- Návrh doporučení.
- Manuální prověření nálezů s filtrací false-positive nálezů.
- Provedení „black-box test“.

IPv4 rozsah:

- 195.113.76.0/23

IPv6 rozsah:

- 2001:718:1e05::/48

Test webových aplikací:

Provedení „black-box test“.

URL:

- <http://www.msmt.cz>
- <http://www.op-vk.cz>
- <http://www.opvavpi.cz>
- <https://database.op-vk.cz>
- <https://admin.database.op-vk.cz>
- <https://www.akreditacnikomise.cz>
- <http://www.edu.cz/>
- <http://www.et2020.cz/>
- <http://www.generacey.cz/>
- <http://www.narodniporadenskeforum.cz>
- <https://www.nauvs.cz>
- <https://www.ruv.cz/app/>
- <http://www.skolinfo.cz/>
- <http://www.vzdelavani2020.cz/>
- <http://sberdat.uiv.cz>

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 zranitelnosti 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

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 našel zranitelnost, která nesnese odkladu a významně ohrožuje bezpečnost systému, oznámí tuto skutečnost objednateli.

Fáze provedení penetračního testu

1. Příprava testovacích nástrojů – aktualizace nástrojů nebo jejichází dat.

2. Sběr informací – sběr informací a to pasivně dostupnými prostředky nebo aktivně síťovými skenery. Síťové skenery zahajují aktivitu na síti 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, perl 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 integritu 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. Součástí 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.

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 exploítovat.

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.

Výstupem externího penetračního testu bude dokument – závěrečná zpráva.

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. Zjištění 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).

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.

Dokument bude zpracován a autorizován expertem s certifikací ISMS Specialista dle norem ISO 270001 a ISO 270002 a CISA nebo Lead Auditor ISO/IEC 27001:2013 nebo obdobná.

DOBĀ PLNĚNÍ

- doba zahájení prací: od nabytí účinnosti Smlouvy
- doba ukončení prací: 10 dnů ode dne předání podkladů ze strany objednatele

MÍSTO PLNĚNÍ

Místem plnění je sídlo objednatele, případně další místa specifikovaná Zhotovitelem. Sídlem zadavatele se rozumí Česká republika — Ministerstvo školství, mládeže a tělovýchovy, Karmelitská 529/5, Praha 1