GRANTOVÁ AGENTURA ČESKÉ REPUBLIKY

SMLOUVA O DÍLO

Česká republika – Grantová agentura České republiky
se sídlem: Evropská 2589/33b, Praha 6, 160 00
zastoupená: doc. RNDr. Petrem Baldrianem, Ph.D., předsedou
IČO: 485 49 037
(dále jen **"objednatel"**)

a

Trusted Netwok Solutions a.s.
se sídlem: Žižkova 600, Bílovice nad Svitavou 664 01
zastoupená: Mgr Romanem Pavlíkem, členem představenstva
IČO: 26239701
DIČ: CZ26239701
Zapsána v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl B, vložka 3536
bank. spojení: [redacted] a.s
(dále jen **„zhotovitel")**

uzavírají tuto smlouvu o dílo (dále jen „**smlouva**") na základě výběrového řízení na veřejnou zakázku malého rozsahu s názvem **„Penetrační test IS GRIS"** (dále jen „veřejná zakázka"), která je vedena na elektronickém tržišti Tenderarena pod ID VZ0131962. Smluvní strany, vědomy si svých závazků v této smlouvě obsažených a s úmyslem být touto smlouvou vázány, dohodly se v souladu s ustanovením § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**") na následujícím znění smlouvy:

I. Předmět smlouvy

1. Zhotovitel se zavazuje provést na svůj náklad a nebezpečí pro objednatele dílo spočívající v provedení penetračních testů aplikací kritických pro chod objednatele a především testu aplikace GRIS, a to tak jak je blíže specifikováno v příloze č. 1 této smlouvy (dále jen „dílo").
2. Objednatel se touto smlouvou zavazuje, že řádně provedené a dokončené dílo převezme a zaplatí zhotoviteli cenu díla dle článku II. této smlouvy.

II. Cena za provedení díla

1. Cena za dílo činí 325000 Kč bez DPH (393250 Kč s DPH).
2. Smluvní strany se dohodly, že veškeré daňové doklady a podklady týkající se splatnosti a fakturace budou zasílány výlučně v elektronické podobě na e-mailovou adresu objednatele podatelna@gacr.cz, nedojde-li ke změně této adresy způsobem, který je touto smlouvou předvídán.

III. Místo, kvalita a doba provedení díla

1. Místem odevzdání díla je sídlo objednatele uvedené v záhlaví této smlouvy. Zhotovitel je povinen dílo předat kontaktní osobě objednatele po předchozí domluvě s kontaktní osobou objednatele, v pracovních dnech v době od 9:00 do 15:00, nedohodne-li se zhotovitel s kontaktní osobou objednatele jinak, například v elektronické podobě. Řádně provedené a dokončené dílo, kontaktní osoba objednatele, písemně potvrdí zhotoviteli.
2. Zhotovitel je povinen řádně provést dílo a dokončené dílo předat objednateli do 30. 6. 2022, přičemž přesný termín uskutečnění předmětu plnění bude upřesněn na základě dohody s kontaktní osobu objednatele.
3. Zhotovitel se zavazuje opatřit vše, co je zapotřebí k provedení díla podle této smlouvy.
4. Zhotovitel na sebe přebírá nebezpečí změny okolností podle § 1765 odst. 2 občanského zákoníku.
5. Zhotovitel poskytuje tímto objednateli záruku za jakost díla dodaného zhotovitelem objednateli v délce 24 měsíců od provedení a předání díla.
6. Kontaktní osobou objednatele je: [redacted], [redacted]@gacr.cz, +420 [redacted].
7. Kontaktní osobou zhotovitele je: [redacted], [redacted]@tns.cz, +420 [redacted].

IV. Povinnosti Smluvních stran

1. Zhotovitel je povinen:
   a) při provádění díla Služeb postupovat s náležitou odbornou péčí dle této smlouvy, právních předpisů a technických norem;
   b) zajistit ochranu od objednatele převzatých podkladových materiálů a k jejich ochraně zavázat také veškeré své zaměstnance či spolupracovníky, kteří s těmito materiály přijdou či by mohli přijít do styku. Zhotovitel se zejména zavazuje neposkytovat podkladové materiály objednatele ani výstupy plnění nikomu, s výhradou případů poskytnutí předchozího písemného souhlasu objednatele;
   c) umožnit objednateli průběžnou kontrolu kvality díla dle potřeb objednatele;
   d) bez zbytečného odkladu, nejpozději však do 5 pracovních dnů, písemně upozornit objednatele na nutnost poskytnutí součinnosti objednatele, případně objednatele stejným způsobem vyzvat k poskytnutí chybějících podkladových materiálů;
   e) zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví při provádění díla dle této smlouvy či v souvislosti s nimi. Tato povinnost zhotovitele trvá i po ukončení této smlouvy.

2. Objednatel je povinen:
   a) předat zhotoviteli vyžádané podkladové materiály, nezbytné k řádnému splnění povinností zhotovitele dle této smlouvy;
   b) poskytnout zhotoviteli nezbytnou součinnost k provedení díla dle této smlouvy, zejména zajistit zhotoviteli spolupráci s příslušnými zaměstnanci objednatele;
   c) umožnit po předchozí dohodě zhotoviteli v případě potřeby přístup do svých objektů za účelem realizace předmětu plnění dle této smlouvy.

3. Smluvní strany jsou povinny:
   a) při plnění této smlouvy úzce spolupracovat, zejména si poskytovat úplné, pravdivé a včasné informace potřebné k řádnému plnění svých povinností, přičemž v případě změny podstatných okolností, které mají nebo mohou mít vliv na plnění smlouvy, jsou smluvní strany povinny o

takové změně informovat druhou smluvní stranu bezodkladně, nejpozději však do 3 pracovních dnů po zjištění takové změny;

b) plnit řádně a včas své povinnosti tak, aby nedocházelo k prodlení s jejich plněním. Pokud se některá ze smluvních stran dostane do prodlení s plněním svých povinností, je povinna písemně oznámit bez zbytečného odkladu druhé smluvní straně důvod prodlení a předpokládaný termín a způsob jeho odstranění.

V. Sankce

1. V případě porušení povinnosti zhotovitele dle čl. IV odst. 1 písm. a) až d) této smlouvy, se zhotovitel zavazuje objednateli zaplatit smluvní pokuty ve výši 10 000 Kč za každé jednotlivé porušení, a to i opakovaně.

2. V případě porušení povinnosti mlčenlivosti a ochrany osobních údajů objednatele specifikovaných v čl. VI této smlouvy se zhotovitel zavazuje objednateli zaplatit smluvní pokutu ve výši 100 000 Kč za každé jednotlivé porušení, a to i opakovaně.

3. V případě prodlení objednatele se zaplacením dohodnuté ceny za poskytnutí řádně provedeného díla dle smlouvy je zhotovitel oprávněn požadovat po objednateli zaplacení úroku z prodlení ve výši 0,1 % (slovy: jedna desetina procenta) z dlužné částky za každý i započatý den prodlení.

4. V případě prodlení zhotovitele s provedením díla dle této smlouvy se zhotovitel zavazuje objednateli zaplatit úrok z prodlení ve výši 0,1 % (slovy: jedna desetina procenta) z celkové ceny díla, uvedené v čl. II této smlouvy, a to za každý i započatý den prodlení.

5. Vznikem povinnosti platit smluvní pokutu, ani jejím skutečným zaplacením nezaniká povinnost smluvních stran splnit povinnost, jejíž plnění bylo zajištěno smluvní pokutou.

6. Smluvní sankce dle tohoto článku jsou splatné do 15 dnů ode dne doručení výzvy k jejich úhradě povinné straně.

7. Zaplacením smluvní pokuty a úroku z prodlení není dotčen nárok smluvních stran na náhradu škody nebo odškodnění v plném rozsahu ani povinnost zhotovitele řádně poskytnout plnění.

8. Žádná ze smluvních stran není povinna zaplatit smluvní pokutu či náhradu škody, pokud prokáže, že porušení povinností bylo způsobeno okolnostmi dle § 2913 odst. 2 občanského zákoníku.

Článek VI.
Ochrana důvěrných informací a zpracování osobních údajů

1. Smluvní strany se dohodly, že veškeré informace, které se zhotovitel dozvěděl v rámci uzavírání a plnění této smlouvy, tvořící její obsah, a informace, které zhotoviteli Objednatel sdělí nebo jinak vyplynou z plnění smlouvy, musí být zhotovitelem dle vůle objednatele utajeny (dále jen „***důvěrné informace***"). Zhotovitel nesmí důvěrné informace objednatele použít pro jiné účely než pro poskytnutí plnění dle této smlouvy, nesmí je zveřejnit ani poskytnout jiné osobě. Uvedené ustanovení se nevztahuje na obsah smlouvy, jejích příloh a případných dodatků.

2. Smluvní strany se dohodly, že zhotovitel nesdělí důvěrné informace třetí osobě a přijme taková opatření, která znemožní jejich přístupnost třetím osobám. Ustanovení předchozí věty se nevztahuje na případy, kdy:
    a) má zhotovitel opačnou povinnost stanovenou zákonem,
    b) se takové důvěrné informace stanou veřejně známými či dostupnými jinak než porušením povinností vyplývajících z tohoto článku, nebo
    c) objednatel dá k zpřístupnění konkrétní důvěrné informace písemný souhlas.

3. V souvislosti s plněním této smlouvy Smluvními stranami bude docházet i ke zpracování osobních údajů ve smyslu Nařízení Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „***Nařízení***“) a zákona č. 110/2019 Sb., o zpracování osobních údajů v platném znění (dále jen „***Zákon***“).

4. Objednatel jakožto správce osobních údajů (dále v tomto článku označen jen jako „***správce***“), tímto pověřuje ve smyslu článku 28 Nařízení zhotovitele jako zpracovatele osobních údajů (dále v tomto článku označena jen jako „***zpracovatel***“) zpracováním osobních údajů poskytnutých správcem a zaměstnanci nebo potenciálními zaměstnanci správce pro účel plnění povinností vyplývajících z této smlouvy.

5. Správce i zpracovatel postupují při své činnosti týkající se nakládání s osobními údaji ve smyslu Zákona a Nařízení. Zpracovatel zpracovává osobní údaje v rozsahu a v souladu s Nařízením a v rozsahu stanoveném touto smlouvou. Zpracovatel zpracovává osobní údaje pouze na základě doložených pokynů správce.

7. Další povinnosti zpracovatele jsou následující:
    a) Zpracovatel osobních údajů zpracovává osobní údaje v rozsahu nezbytném pro plnění účelu podle této smlouvy, a to pouze po nezbytně nutnou dobu;
    b) Zpracovatel nesmí s poskytnutými osobními údaji jakkoliv nakládat nad rámec účelu, za kterým mu byly poskytnuty, v rámci tohoto účelu pak zpracovatel musí s osobními údaji nakládat jen v rozsahu nezbytně nutném;
    c) Zpracovatel se zavazuje přijmout taková technická a organizační opatření k zabezpečení osobních údajů, aby nemohlo dojít k neoprávněnému, nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů;
    d) Zpracovatel zajistí informovanost a školení svých zaměstnanců pracujících s osobními údaji. Především zajistí, aby jeho zaměstnanci pracující s osobními údaji byli v souladu s platnými a účinnými právními předpisy vázáni povinností mlčenlivosti ve smyslu Nařízení a poučeni o možných následcích pro případ porušení této povinnosti;
    e) Zpracovatel není oprávněn zapojit do zpracování žádného dalšího zpracovatele bez předchozího písemného souhlasu správce;
    f) Zpracovatel poskytne správci nezbytnou spolupráci, součinnost a informace potřebné k vyřízení jakékoli stížnosti nebo žádosti subjektu údajů týkající se jejich osobních údajů nebo dozorového orgánu ochrany osobních údajů v souvislosti se zmírňováním a nápravou incidentů v oblasti zabezpečení osobních údajů a porušení zabezpečení údajů (jako např. ztráta, krádež, vymazání, zveřejnění nebo poškození osobních údajů, za účelem opravy,

změny, přenesení nebo vymazání osobních údajů nebo za účelem plnění jakýchkoliv jiných povinností správce podle Nařízení;

g) Zpracovatel ohlásí správci jakékoliv porušení zabezpečení osobních údajů neprodleně bez zbytečného odkladu poté, co porušení zjistí a ohlášení případně doplní o informace požadované správcem;

h) Zpracovatel v souladu s rozhodnutím správce všechny osobní údaje vrátí správci po ukončení zpracování, a vymaže existující kopie, pokud právní předpisy EU nebo České republiky nepožadují uložení daných osobních údajů;

i) Zpracovatel poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v článku 28 Nařízení, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje. Zpracovatel neprodleně informuje správce v případě, že podle jeho názoru určitý pokyn porušuje Zákon nebo Nařízení nebo jiné předpisy EU, České republiky nebo jiného členského státu EU týkající se ochrany osobních údajů.

8. Smluvní ujednání o zpracování osobních údajů ve smyslu tohoto článku se uzavírá na dobu trvání této smlouvy.

9. Další vzájemná práva a povinnosti smluvních stran, práva a povinnosti smluvních stran vůči třetím osobám a veřejným orgánům v souvislosti se zpracováním osobních údajů, vyplývajících ze Zákona nebo Nařízení, nejsou shora uvedeným dotčeny.

10. Z tohoto ujednání o zpracování osobních údajů neplynou pro smluvní strany žádné finanční závazky, odměna za zpracování osobních údajů je již zahrnuta v odměně zhotovitele stanovené dle čl. II této smlouvy.

VII. Závěrečná ustanovení

1. Tato smlouva obsahuje úplné ujednání o předmětu smlouvy a všech náležitostech, které smluvní strany měly a chtěly ve smlouvě ujednat, a které považují za důležité pro závaznost této smlouvy. Žádný projev stran při jednání o této smlouvě ani projev učiněný po uzavření této smlouvy nesmí být vykládán v rozporu s výslovnými ustanoveními této smlouvy a nezakládá žádný závazek žádné ze stran.
2. Smluvní strany si nepřejí, aby nad rámec výslovných ustanovení této smlouvy byla jakákoliv práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění této smlouvy.
3. Smluvní strany se dohodly, že část obsahu této smlouvy tvoří Všeobecné obchodní podmínky, které jsou k této smlouvě přiloženy. Odběratel prohlašuje, že se s obsahem Všeobecných obchodních podmínek náležitě seznámil a je jimi vázán. Tyto Všeobecné obchodní podmínky se uplatní výlučně před obchodními podmínkami zhotovitele. Tyto Všeobecné obchodní podmínky jsou rovněž dostupné na https://gacr.cz/uredni-deska/verejne-zakazky/.
4. Nedílnou součást této smlouvy tvoří její přílohy:
    a. Příloha č. 1 – Technická specifikace
    b. Všeobecné obchodní podmínky Grantové agentury České republiky

5. Obsah této smlouvy, jakož i jejích příloh, lze měnit nebo doplňovat pouze písemnou dohodou smluvních stran ve formě číslovaných dodatků této smlouvy, podepsaných oprávněnými zástupci obou smluvních stran.
6. Práva a povinnosti smluvních stran výslovně neupravených touto smlouvou se řídí občanským zákoníkem a ostatními příslušnými právními předpisy českého právního řádu.
7. Zhotovitel bere na vědomí, že objednatel je povinným subjektem dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a že objednatel je povinen poskytovat informace dle výše uvedeného zákona o svobodném přístupu k informacím.
8. Smluvní strany souhlasí se zveřejněním této smlouvy v úplném znění, stejně jako s uveřejněním úplného znění dodatků, kterými se tato smlouva doplňuje, mění, nahrazuje nebo ruší, a to zejména prostřednictvím Registru smluv (smlouvy.gov.cz) v souladu se zákonem č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů. Smluvní strany se dohodly, že uveřejnění této smlouvy zajistí objednatel nejpozději do 3 měsíců ode dne podpisu této smlouvy.
9. Pokud je tato smlouva uzavírána v písemné formě, je sepsána ve dvou vyhotoveních stejné právní síly, z nichž každá strana obdrží po jednom vyhotovení. Tato smlouva může být uzavřena i elektronickými prostředky v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.

Smluvní strany prohlašují, že si tuto smlouvu přečetly, že s jejím obsahem jakož i právními důsledky souhlasí a na důkaz toho k ní připojují svoje podpisy:

V Bílovicích nad Svitavou dne	V Praze dne
Za zhotovitele:	Za objednatele:
_____	_____
Mgr. Roman Pavlík	doc RNDr. Petr Baldrian, Ph.D.

Příloha č. 1 – Technická specifikace

Na základě zjištěné bezpečnostní události je potřebné provést black box penetrační testy na IS GRIS jakožto významného informačního systému dle ZKB a zároveň aplikace kritické pro chod GA ČR, a to jak z pohledu anonymního uživatele, tak po přihlášení uživatele (žadatele o grant) do IS GRIS.

IS GRIS a jeho komponenty jsou pro uživatele dostupné na doméně gris.cz / IP 195.113.149.199

Bezpečnostní test bude nedestruktivní a bude se soustředit výhradně na identifikaci zranitelností, ne na jejich zneužití.

Předmětem plnění je poskytování služeb spočívající zejména v:

1. Provádění vnějších penetrační testů představujících simulaci napadení systémů útočníkem. Cílem testů je zjistit, jak snadno identifikovatelný cíl informační systémy zadavatele představují, jaké informace lze získat o zvenčí dostupných systémech, jak detekovat zranitelnosti, které mohou být zneužity k získání neautorizovaného přístupu k citlivým systémovým zdrojům, a navrhnout doporučení k jejich odstranění.
   Vnější penetrační testy budou provedeny ze sídla dodavatele vůči testovaným z vnějšku dostupným systémům bez ohledu na jejich místo provozu.
   Podrobný postup vnějších penetračních testů je uveden v článku „Postup testování".

2. Provedení automatizovaného vulnerability skenu externího síťového perimetru zadavatele (rozsah IP adres: 195.113.149.193 – 195.113.149.206).
3. Vypracování písemných zpráv o stavu technické bezpečnosti prověřovaných webových aplikací a IT infrastruktury zadavatele vypracované dodavatelem, které dodavatele zadavateli předá v dohodnutém elektronickém formátu. Požadavky na zpracování písemné zprávy jsou uvedeny v článku „Obsah a struktura zprávy z testů".

Postup testování

Testování se bude skládat z následujících fází. V případě potřeby budou dohodnuty individuální postupy testování v závislosti na typu webové aplikace, popřípadě IT infrastruktury.

- Identifikace cíle;
- Identifikace aktivních služeb;
- Identifikace zranitelností;
- Získání přístupu;
- Eskalace privilegií a ovládnutí cíle;
- Reakce na testy.

Penetračním testováním, které je předmětem plnění, není pouze provádění automatizovaných (vulnerability) skenů.
Pro testování budou využity především následující metodiky a doporučení týkající se bezpečnosti informačních systémů. Metodiky mohou být interně přizpůsobeny.

- Doporučení OWASP (Open Web Application Security Project), která se zaměřují na pomoc organizacím při identifikaci bezpečnostních hrozeb webových aplikací;
- Standard OSSTMM (Open Source Security Testing Methodology Manual) – metodologie pro testování bezpečnosti;
- Doporučení organizace IETF (Internet Engineering Task Force) – organizace vydávající RFCs tzv. standardy internetu;
- Doporučení organizace NIST (např. NIST SP 800-44 Guidlines on Securing Public Web Servers);
- Common Criteria (ISO/IEC 15408) – standard pro hodnocení úrovně bezpečnosti systémů;

- Materiály a doporučení ISACA (Information Systems Audit and Control Association) určené certifikovaným auditorům informačního systému (CISA);
- Normy pro řízení bezpečnosti IS/ICT, řízení kvality projektu a provádění auditů:
    - normy řady ISO/IEC 27000 pro oblast řízení bezpečnosti informačních systémů;
    - BS 7799-3 Směrnice pro řízení rizik souvisejících s informační bezpečností;
    - ČSN EN ISO 19011:2002 – Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu;
    - ČSN ISO 10006 – Management jakosti – Směrnice jakosti v managementu projektu.

Obsah a struktura písemné zprávy z testů

Výstupem každého testu je zpráva o stavu technické bezpečnosti prověřovaného systému a IT infrastruktury, která je rozdělena na část manažerského shrnutí a na detailní zprávu. Výstupy jsou standardně dodávány i na elektronickém médiu spolu s výstupy z použitých nástrojů a případnými doplňujícími informacemi k testům (např. screenshoty z průběhu testů).

1. Manažerské shrnutí

Pro účely managementu organizace je vypracována speciální hodnotící zpráva s cílem podchytit a stručně a srozumitelně popsat zjištěné výsledky testování a analýz.
Cílem manažerského shrnutí bude podat stručné informace o průběhu testu, ohodnotit bezpečnost webových aplikací a IT infrastruktury, tak i jednotlivých zkoumaných oblastí, a popsat nejdůležitější doporučovaná bezpečnostní opatření, která budou podrobně popsána v detailní zprávě.

2. Detailní zpráva

Obsahem detailní zprávy jsou konkrétní zjištění související s jednotlivými zkoumanými oblastmi.
Detailní zpráva obsahuje následující informace:

- cíl a rozsah testu;
- popis předmětu testu;
- stanovení stupnice a metodiky hodnocení – kategorizace zjištěných zranitelností a jejich přehledné značení v rámci dokumentu;
- postup provedeného testu včetně nástrojů a technik použitých v jednotlivých fázích;
- popis zjištění z jednotlivých fází testu;
- popis nalezených zranitelnosti, každá v členění uvedeném níže;
- doporučení pro odstranění identifikovaných slabin a zranitelných míst;
- závěrečné zhodnocení provedeného testu a hodnocení aktuálně dosažené úrovně bezpečnosti testovaných aplikací.

Všechny identifikované zranitelnosti jsou popsány v následující struktuře:

a) Hodnocení/kategorizace zranitelnosti – veškeré nalezené problémy a zranitelnosti jsou rozděleny do pěti kategorií podle závažnosti:


kriticky závažná chyba (KRITICKÁ) – CRITICAL

Jako kritické chyby jsou označeny nedostatky, které byly při testech zneužity a vedly (mohou vést) k přímé kompromitaci testovaného systému.


závažné chyby (VYSOKÁ) – HIGH

Jako závažné klasifikujeme chyby, které bezprostředně umožňují kompromitaci systému, či jeho nedostupnost. U těchto chyb existuje velmi vysoká pravděpodobnost zneužití. Jejich okamžitá náprava je nutná.

 středně závažné chyby (STŘEDNÍ) – MEDIUM

Do této kategorie spadají chyby, jejichž využití k potenciálnímu útoku na informační systém je technologicky náročnější na realizaci, nebo které umožňují průnik do systému pouze v případě splnění několika určitých navzájem souvisejících podmínek. Jejich závažnost nelze podceňovat s ohledem na potenciálně hrozící zneužití.

 méně závažné chyby (NÍZKÁ) – LOW

Tato kategorie zahrnuje méně závažné chyby, které napomáhají napadení systému. Např. poskytují potenciálnímu útočníkovi informace, jež lze uplatnit v rámci útoku na informační systém – organizace o svém informačním systému prozrazuje více, než je nezbytně nutné. Ve většině případů se jedná pouze o konfigurační opomenutí apod.

 (INFORMATIVNÍ) – INFO

Informativní kategorie označuje vše, co lze zjistit o systémech a sítích, aniž by bylo možné jakýmkoliv způsobem zabránit úniku těchto informací. Tyto údaje nejsou většinou příliš důležité pro vedení vlastního útoku, ale mnohdy mohou napomoci útočníkovi při dokreslení či doplnění celkového obrazu o cíli potenciálního napadení.

b) Klasifikace dle schopnosti útočníka – skill, neboli schopnosti útočníka, je klasifikace, která popisuje nároky kladené na schopnosti a znalosti útočníka pro realizaci daného útoku:

 Pro identifikaci a případné zneužití zranitelnosti postačují základní znalosti a schopnosti uživatele – útočníka. Ke zneužití může dojít také neúmyslnou chybou nebo náhodným jednáním.

 Středně obtížná náročnost s využitím automatizovaných nástrojů. Technicky zdatní útočníci, kteří s větší mírou využívají manuální metody útoku, případně převzaté skripty.

 Velmi znalí a zkušení útočníci, kteří k útokům používají úzce specializované a sofistikované nástroje. Jedná se o přesně cílené útoky.

c) Zjištění – popis zranitelného místa/nálezu včetně popisu kde a jakým způsobem byla zranitelnost identifikována.

d) Riziko – popis rizik plynoucích z možného zneužití zranitelného místa včetně možných scénářů zneužití (kdo a za jakých podmínek může zranitelnost zneužít a jaké jsou možné dopady tohoto zneužití), posouzení dopadu rizika na produkční prostředí.

e) Doporučení – doporučení vedoucí k odstranění nalezených nedostatků, případně návrhy na zvýšení bezpečnosti stávajících bezpečnostních mechanismů a opatření. Tato doporučení se mohou týkat procesních změn, konfigurace zařízení (hardening systémů), návrhu nových bezpečnostních mechanismů pro zvýšení stávající úrovně bezpečnosti, doporučení pro uživatelská PC pro zvýšení bezpečnosti atd.

f) Přílohy (výstupy z použitých nástrojů, printscreeny, důkazy apod.).

Test proběhne v době mimo hlavní zátěž serveru tedy v brzkých ranních nebo pozdních večerních hodinách, dobu určí zadavatel.