**Sérülékenységvizsgálati jegyzőkönyv**

{TÖRLENDŐ\_RÉSZ} **Sablon** {TÖRLENDŐ\_RÉSZ\_VÉGE}

**<Érintett alkalmazás neve (Rövidítése)>**

**<n.m> verzió**

Készült: <év>. <hónap>. <nap>.

**Készítette:**

# Dokumentum kontroll

## Dokumentum jellemzők

|  |  |
| --- | --- |
| Projekt hivatalos neve: | <Projekt hivatalos neve> |
| Projekt rövid neve | <projekt rövid neve> |
| Dokumentum címe: | <Projekt hivatalos neve> – <Alcím> – <Érintett alkalmazás neve (Rövidítése)> |
| Verziószám: | <n.m> |
| Állapot: |  |
| Kiadás kelte: | <0000>. <00. 00.> |
| Utolsó mentés kelte: | <0000>. <00. 00.> |
| Készítette: |  |
| Fájlnév: | <FileName> |

## Jóváhagyások

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Név | Szervezeti egység | Szervezet | Dátum | Aláírás |
| <XY> |  | <IdomSoft Zrt.> | <0000>. <00. 00.> |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Változtatások jegyzéke

|  |  |  |
| --- | --- | --- |
| Verzió | Dátum | Változtatás rövid leírása |
| <1.0> | <0000>. <00. 00.> | <Első verzió> |
|  |  |  |
|  |  |  |

## Kapcsolódó dokumentumok

|  |  |
| --- | --- |
| Dokumentum címe | Dokumentum helye /fájl neve |
|  |  |
|  |  |

Tartalomjegyzék

[1 Dokumentum kontroll 2](#_Toc185424141)

[1.1 Dokumentum jellemzők 2](#_Toc185424142)

[1.2 Jóváhagyások 2](#_Toc185424143)

[1.3 Változtatások jegyzéke 2](#_Toc185424144)

[1.4 Kapcsolódó dokumentumok 2](#_Toc185424145)

[2 Vezetői összefoglaló 7](#_Toc185424146)

[3 Cél és hatókör 7](#_Toc185424147)

[4 Felhasznált dokumentumok 7](#_Toc185424148)

[5 Tesztelés körülményei 7](#_Toc185424149)

[5.1 A tesztelésben közreműködő személyek 8](#_Toc185424150)

[5.2 A tesztelés időpontja 8](#_Toc185424151)

[5.3 Tesztelési módszerek és eszközök 8](#_Toc185424152)

[5.4 Teszteléshez használt jogosultságok 9](#_Toc185424153)

[6 A feltárt sérülékenységek 9](#_Toc185424154)

[6.1 Sérülékenység-<N> 9](#_Toc185424155)

[7 További tesztesetek 10](#_Toc185424156)

Ábrajegyzék

**Nincs ábrajegyzék-bejegyzés.**

{TÖRLENDŐ\_RÉSZ}

**Informatív leírás**

Ezen sablon annak érdekében került kiadásra, hogy segítséget nyújtson az egységes Sérülékenységvizsgálati jegyzőkönyv dokumentumok létrehozásában. Az Informatív leírás fejezet általános információkat fogalmaz meg, mely nem eleme a sablon alapján kialakításra kerülő Sérülékenységvizsgálati jegyzőkönyv dokumentumnak. Az elkészítés során törölni kell a fájlból minden további, a kitöltést segítő magyarázó résszel együtt.

**Dokumentum célja**

A dokumentumcélja**:**

* pontosan dokumentálja a vizsgálat hatókörét és körülményeit,
* megnevezze az elvégzett vizsgálatok során alkalmazott módszertanokat,
* mutassa be a feltárt sérülékenységeket szakértők számára reprodukálható módon,
* tegyen ajánlást a feltárt sérülékenységek kritikusság szerinti besorolására a kihasználhatóság nehézsége, és az ismert kockázati tényezők figyelembevételével,
* adjon javaslatot a feltárt sérülékenységek elhárítására vonatkozóan.

**Dokumentumnak nem célja**

A dokumentumnak nem célja:

* az alkalmazott vizsgálati módszertanok mély szakmai bemutatása,
* a feltárt sérülékenységek szakirodalmi megnevezésén túl a sérülékenység lényegének részletes kifejtése, ha azok a szakértők előtt ismertnek tekinthetők,
* olyan megvizsgált teszteset leírása, amelynek végrehajtása nem tárt fel sérülékenységet — ha a tesztelő úgy ítéli meg, akkor ettől eltérhet.

**Felhasználói körök**

A dokumentum érzékeny tartalma miatt csak azok számára publikálható, akik számára ez a munkavégzéshez — elsősorban hibaelhárítás — szükséges. A dokumentumból kivonatot — pl. vezetői összefoglalót — kaphatnak egyes szereplők (monitoring).

| Felhasználói kör | Felhasználás módja |
| --- | --- |
| Architekt | A rá vonatkozó fejezetek, ha a feltárt sérülékenység elhárításához szükséges az ő bevonása. |
| Biztonsági felelős | A teljes dokumentum. |
| Fejlesztő | A rá vonatkozó fejezetek, ha a feltárt sérülékenység elhárításához szükséges az ő bevonása. |
| Integrátor | A rá vonatkozó fejezetek, ha a feltárt sérülékenység elhárításához szükséges az ő bevonása. |
| Minőségbiztosító | A vezetői összefoglaló tájékoztató, illetve monitoring céllal. |
| Projektvezető | A vezetői összefoglaló tájékoztató, illetve monitoring céllal. |
| Üzemeltető | A rá vonatkozó fejezetek, ha a feltárt sérülékenység elhárításához szükséges az ő bevonása. |
| Adminisztrátor | A rá vonatkozó fejezetek, ha a feltárt sérülékenység elhárításához szükséges az ő bevonása. |

**Felhasznált dokumentumok**

* A választott tesztelési módszertannak megfelelő mélységű rendszerdokumentáció
* Informatikai rendszerterv
* Rendszerbiztonsági terv
* Hálózati kapcsolatok terv
* Felsőszintű architektúra terv
* Logikai rendszerterv
* Fizikai rendszerterv
* Tartalmi elvárások

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Vezetői összefoglaló

{TÖRLENDŐ\_RÉSZ}

A fejezet célja: összefoglalja a sérülékenységvizsgálat eredményeit vezetői szintű személyek számára.

A fejezet tartalmi elvárásai:

* a vizsgálat hatásköre (scope),
* a vizsgálat időintervalluma,
* a feltárt sérülékenységek súlyosságuk szerint csoportosítva.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Cél és hatókör

{TÖRLENDŐ\_RÉSZ}

A fejezet célja: bemutatja a dokumentum célját és hatókörét.

A fejezet tartalmi elvárása: azonosítsa a vizsgálattal érintett rendszert, rendszer elemet és komponenst. Határozza meg a dokumentum célját, mely lehet:

* célorientált behatolási teszt (klasszikus penetration test),
* komponensek hardening-jének vizsgálata (tipikusan automatákkal történő vizsgálat),
* meghatározott célú audit (pl. code review),
* a lehető legtöbb sérülékenység feltárása automata és manuális eszközökkel.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Felhasznált dokumentumok

{TÖRLENDŐ\_RÉSZ}

A fejezet célja: a tesztelés tervezéséhez felhasznált dokumentumok megnevezése.

A fejezet tartalmi elvárása: megadja azon dokumentumokat, melyek olyan információkat tartalmaznak, amelyek a sérülékenységvizsgálat tervezésekor szerepet játszottak.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Tesztelés körülményei

{TÖRLENDŐ\_RÉSZ}

A fejezet célja: bemutatja a sérülékenységvizsgálat körülményeit.

A fejezet tartalmi elvárása: mutassa be a vizsgálat körülményeit az alábbi alfejezetekre bontva.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## A tesztelésben közreműködő személyek

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: azonosítja a sérülékenységvizsgálat résztvevőit.

Az alfejezet tartalmi elvárásai: azonosítsa a vizsgálatban résztvevő tesztelőket, illetve a munkájukat támogató szakértőket (név, feladatkör).

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## A tesztelés időpontja

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: leírja a vizsgálat időpontját.

Az alfejezet tartalmi elvárása: írja le a vizsgálat idejét.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Tesztelési módszerek és eszközök

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: a sérülékenységvizsgálat módszertanának és eszközeinek bemutatása.

Az alfejezet tartalmi elvárásai:

* mutassa be az alkalmazott tesztelési módszert — pl. black-box, grey-box, white-box,
* ismertesse a tesztelés fázisait, pl.:
  + információgyűjtés,
  + automata eszközök alkalmazása,
  + hamis pozitívok (false positives) kiszűrése,
  + intuitív elemzés,
  + visszafejtés (reverse engineering),
  + kiaknázás (exploit-álás),
* mutassa be az alkalmazott eszközöket és a vizsgálatokhoz használt segédprogramokat,
* mutassa be az alkalmazott sérülékenység besorolási módszertant — vagy ha ismert módszertan alapján történik, akkor hivatkozza meg, pl. <https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology>.

A fejezetnek nem feladata a részletes szakmai tartalom leírása, de meg kell nevezze a szakmában ismert és a vizsgálatban ténylegesen alkalmazott eljárásokat, valamint alkalmazásuk célját.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Teszteléshez használt jogosultságok

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: ismerteti a sérülékenységvizsgálathoz kapott jogosultságokat.

Az alfejezet tartalmi elvárásai:

* definiálja a vizsgálati hatókör, cél, illetve módszertan függvényében a tesztelők különböző hozzáférési szinttel rendelkező felhasználói fiókokat,
* definiálja a rendszerben alkalmazott biztonsági eszközök — pl. WAF, IPS, tűzfal — kikapcsolásának vagy szabályzat (policy) módosításának igényét.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# A feltárt sérülékenységek

{TÖRLENDŐ\_RÉSZ}

A fejezet célja: részletesen bemutatja a vizsgálat során feltárt sérülékenységeket.

A fejezet tartalmi elvárása: részletesen mutassa be a feltárt sérülékenységeket típusa szerint alfejezetekre bontva, az alább kifejtett tartalommal.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Sérülékenység-<N>

{TÖRLENDŐ\_RÉSZ}

Az alfejezetek célja: bemutatják a vizsgálat során feltárt sérülékenységeket egy-egy alfejezetben leírva.

Az alfejezet tartalmi elvárásai:

* nevezze meg a sérülékenységet szakirodalmi nevén, ha van — pl. reflected XSS — és írja le a sérülékenység reprodukálását képernyőképekkel alátámasztva,
* külön csatolja és hivatkozza meg a sérülékenység reprodukálása közben keletkezett:
  + teszt eszköz kimeneteket,
  + naplófájlokat,
  + egyéb bizonyítékokat;
* sorolja be a feltárt sérülékenységet az alkalmazott módszertan szerint és írja le a besorolást meghatározó szempontokat,
* adjon megoldási javaslatot a feltárt sérülékenység megszüntetésére vagy a sérülékenység okozta biztonsági kockázatok csökkentésére (workaround).

A fejezetet meg kell ismételni azt összes sérülékenységre.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# További tesztesetek

{TÖRLENDŐ\_RÉSZ}

Ez a fejezet opcionális, mivel a vizsgálatok gyakran intuitív, szerteágazó, iteratív elemeket tartalmaznak, amelyek gyakran csak utólag dokumentálhatók. Ezt érdemes további teszteléssel helyettesíteni.

A fejezet célja: leírja a vizsgálat során végrehajtott, de sérülékenységet fel nem táró teszteseteket.

A fejezet tartalmi elvárása: bemutathat minden olyan tesztesetet, amelyről a tesztelő úgy gondolja, hogy a vizsgálat teljességének dokumentálása érdekében érdemes leírni. Ezt a fejezetet a tesztelés céljának és módszertanának megfelelő minőségű dokumentálása helyettesítheti.

{TÖRLENDŐ\_RÉSZ\_VÉGE}