Zabezpečení proti SQL injection

ESO9 intranet a.s.
U Mlýna 2305/22, 141 Praha 4 – Záběhlice
tel.: +420 585 203 370-2
e-mail: info@eso9.cz
www.eso9.cz

Zpracoval:	Tomáš Urych
Dne:	19.9.2012
Revize:	Urych Tomáš
Dne:	8.10.2012

Obsah

1. Zabezpečení odkazů v aplikacích ESO9

1.1 Zneužití parametrů na odkazu

Vzhledem k charakteru aplikací postavených na technologii ESO9 je každá z činností takové aplikace definována jednoznačným odkazem (hyperlinkem). Odkaz přitom může obsahovat celou řadu parametrů, které definují vlastnosti nebo chování cílového formuláře nebo sestavy. Pokud je uživatel přihlášen v aplikaci (tj. je ověřen), má možnost explicitním zápisem odkazu do adresního řádku internetového prohlížeče spustit potenciálně nežádoucí nebo nebezpečnou akci nebo se dostat k datům, k nimž nemá běžným způsobem práce v ESO9 přístup.

Řešením tohoto problému je zabezpečení odkazů v aplikacích ESO9.

1.2 Zabezpečení odkazů

Všechny odkazy v aplikacích ESO9 jsou konstruovány následovně:

`http://server/aplikace/esoform.asp?PARAMETR=hodnota&PARAMETR2=hodnota2&...`
Je-li použito nastavení zabezpečení odkazů, je veškerý text za klíčovým slovem esoform.asp zašifrovaný. Odkaz z předchozího příkladu tedy bude vypadat následovně:

`http://server/aplikace/esoform.asp?3GAfPlIEn4YwFYh5g78plCwEd5I8/DNEUnVv9I44ncQw@`
Potenciální útočník tak nemá jak zapsat do adresního řádku prohlížeče explicitní odkaz do aplikace ESO9.
V zašifrovaném tvaru jsou předávány všechny odkazy v rámci celé aplikace a jejich zašifrování kontroluje aplikační server. Pokud přijde na aplikační server odkaz v otevřeném textu, je uživateli nahlášena chyba a příslušný odkaz se spolu s uživatelem, který jej spustil, zapíše do logovací databáze.

Zašifrované odkazy obsahují časovou značku, která omezuje jejich platnost na dobu timeout na uživatelské sezení (ve Správci ESO9 parametr *„Uzavřít neaktivní spojení“*).

1.3 Nastavení zabezpečení odkazů

Šifrování lze nastavit na úrovni aplikace ESO9 v programu Správce ESO9 volbou *„Zabezpečení odkazů“*. Ve výchozím nastavení je zabezpečení vypnuté. Pro účely např. implementace je vhodné založit nad ostrou aplikací, v níž se odkazy šifrují, aplikaci virtuální, v níž se šifrovat nebudou a která bude přístupná pouze správcům systému.

1.4 Co podléhá šifrování

Jak již bylo řečeno výše, je-li nastaveno zabezpečení odkazů na aplikaci ESO9, šifrují se všechny typy odkazů, které si mezi sebou předávají všechny tři vrstvy technologie ESO9, konkrétně:

- statické odkazy ve formulářích na další formuláře nebo sestavy (s vazbou i bez vazby)
- odkazy na číselníky
- akce v browse dostupné z kontextového menu
- odkazy na spuštění GS
- odkazy na nápovědu a vzájemné odkazy v rámci nápovědy
- odkazy do aplikací ESO9 ve stránkách volaných parametrem *TPage* (tj. odkazy ve statických stránkách ESO9 bez forem/bez dat)
- odkazy pro práci s dokumentovou databází (uložení souboru do DB a jeho stažení na klienta)
- odkazy z klienta pro akce volané s parametrem *RepeatForQuery*
- odkaz na vyhledávání fulltextem
- odkazy v Silverlight sestavách *"strom činností"* a *"vyhodnocení událostí"*
- odkazy v dočasných serverových sestavách (*TempPrint*) – při načítání uložených sestav se kontroluje čas jejich posledního generování, pokud je sestava starší, než timeout na uživatelské sezení, sestava se

vygeneruje znovu
- odkazy v navigaci

1.5 Kde se šifrování provádí

Vzhledem k počtu vrstev technologie ESO9 je třeba zpřístupnit šifrování na všech třech vrstvách, kde dochází ke generování odkazů zpět do aplikace. Na straně aplikačního serveru a klienta provádí šifrování automaticky obě tyto komponenty, na straně aplikační databáze je k tomuto účelu k dispozici assembly (DLL knihovna). Assembly není standardní součástí verzového skriptu, do zákaznické databáze ji lze nahrát na základě požadavku zákazníka.

1.6 Co k zabezpečení odkazů potřebuji

Možnost zabezpečení odkazů je v technologii ESO9 a v aplikacích ESO9Start od v4.5 doplněk č.1 ze září 2012.

1.6.1 Šifrování odkazů v MS SQL Serveru

Jak již bylo řečeno v kapitole 1.5, provádí se šifrování odkazů na všech třech vrstvách technologie ESO9; na databázové vrstvě je šifrování realizování DLL knihovnou (assembly). Tato knihovna není standardní součástí verzového databázového skriptu, na vyžádání si ji lze nechat zaslat ze společnosti ESO9 intranet.

Postup registrace šifrovací knihovny do databáze SQL serveru:

- Povolit CLR integration (použití CLR knihoven):

```
EXEC dbo.sp_configure 'clr enabled',1
RECONFIGURE;
GO
```

- Povolit tvorbu nezabezpečených assembly:

```
ALTER DATABASE database_name set trustworthy on
GO
```

- Nahrát knihovnu ze souboru na disku:

```
CREATE ASSEMBLY HashURL AUTHORIZATION dbo from 'c:\HashURL.dll' WITH PERMISSION_SET = UNSAFE
GO
```

- Vytvořit nad assembly databázovou funkci, která bude dále využívána v aplikacích ESO9:

```
CREATE FUNCTION dbo.HashURL (@text [nvarchar](4000), @UserName [nvarchar](255), @AppName
[nvarchar](255))
RETURNS [nvarchar](4000) WITH EXECUTE AS CALLER
AS
EXTERNAL NAME HashURL.CHashURL.EncryptStr
GO
```

1.7 Zabezpečení externích odkazů

Jak již bylo řečeno v kapitole 1.2, neakceptuje aplikace ESO9 s nastaveným zabezpečením odkazů žádné odkazy v otevřeném formátu, tj. do aplikace ESO9 nelze vstoupit statickým odkazem např. na vybraný formulář nebo sestavu. Vzhledem k tomu, že se právě tento způsob vstupu do aplikace často využívá v zákaznických Profi řešeních, existuje i pro externí odkazy řešení založené na tabulce EXTERNIURL. V ESO9Start takové řešení nikde použité není, v případě požadavku zákazníka je tedy třeba jej implementovat vždy jako Profi úpravu.
V ESO9Start však existuje pro externí odkazy následující podpora.

1.7.1 Tabulka EXTERNIURL

Libovolné externí odkazy na stránky nebo sestavy v ESO9, které mají být v zabezpečené aplikaci povoleny, musí být předem zapsány v tabulce *EXTERNIURL*. Kromě URL vlastního obsahu zde lze ještě specifikovat způsob zabezpečení každého odkazu položkou *VLZPUSOBZABEZPECENI*:

- Hodnota 1 znamená, že odkaz má časově omezenou platnost (v intervalu *DTPLATNOSTOD – DTPLATNOSTDO*).
- Hodnota 2 znamená, že odkaz má platnost omezenu počtem spuštění (vlastní počet je uložen v položce *POCETSPUSTENI*). Při každém spuštění odkazu je počet spuštění snížen o jeden.
- Hodnota 3 je kombinací obou předchozích podmínek.

Každý odkaz může být povolen buď:

- všem uživatelům (položky *IDUZIVATEL* a *IDSKUPUZIV* prázdné)
- nebo pouze zadanému uživateli (vyplněna pouze položka *IDUZIVATEL*)
- nebo pouze zadané skupině uživatelů (vyplněna pouze položka *IDSKUPUZIV*, je-li vyplněna zároveň položka *IDUZIVATEL*, má vybraný uživatel přednost).

Vlastní odkaz (*URL*) musí začínat klíčovým slovem *ESOForm.asp* (tj. spuštění je povoleno ze všech aplikačních serverů, na nichž je daná aplikace nakonfigurovaná).

1.7.2 Zakládání externích odkazů

Externí odkazy se do tabulky *EXTERNIURL* zapisují procedurou `spZadejExterniURL`:

```
ALTER  PROCEDURE dbo.spZadejExterniURL
       @URL                 VARCHAR(4000),
       @VLZPUSOBZABEZPECENI SMALLINT,
       @DTPLATNOSTOD        DATETIME = NULL,
       @DTPLATNOSTDO        DATETIME = NULL,
       @POCETSPUSTENI       INT = NULL,
       @IDSKUPUZIV          INT = NULL,
       @IDUZIVATEL          INT = NULL
```

Pro daného uživatele, skupinu uživatelů a platnost je zapsané URL unikátní.

1.7.3 Použití externích odkazů

Po vložení externího odkazu do tabulky povolených odkazů je samozřejmě třeba jej před použitím ještě zašifrovat. K tomu slouží funkce `HashURLExternal`:

```
CREATE FUNCTION dbo. HashURLExternal (
                           @text [nvarchar](4000),
                           @UserName [nvarchar](255),
                           @AppName [nvarchar](255))
RETURNS [nvarchar](4000)
```

Výstupem uvedené funkce je zašifrovaný odkaz, který může být použit externě.

1.7.4 Kontrola externích odkazů

Každý externí odkaz je na vstupu aplikačního serveru ověřen proti tabulce *EXTERNIURL*. Kontrola se provádí procedurou `spOverExterniURL`:

```
ALTER  PROCEDURE dbo.spOverExterniURL
       @URL        VARCHAR(4000),
       @IDUZIVATEL INT
```

Pokud je v tabulce externích odkazů nalezen alespoň jeden s platným pověřením (tj. datem platnosti nebo počtem použití), bude proveden, jinak bude zakázán a informace o něm se zapíše do logovací databáze.