Robert Haken [MVP ASP.NET/IIS, MCT]
software architect, HAVIT, s.r.o.
haken@havit.cz, @RobertHaken, http://knowledge-base.havit.cz

[ASP].NET Worst Practices

Security Log

Results | Messages

	SecurityLogId	Date	Username	WasSuccessful	IpAddress	BadPassword
1	368276	2015-01-01 23:15:17.123	novak	1	195.47.29.10	NULL
2	368277	2015-01-02 13:10:01.020	novák	0	86.127.14.53	maruska
3	368278	2015-01-02 13:11:13.120	novak	1	86.127.14.53	NULL
4	368279	2015-01-03 16:30:34.280	admin	0	127.0.0.1	KrWsaD87,k23
5	368280	2015-01-03 16:31:09.833	admin	1	127.0.0.1	NULL
6	368281	2015-01-03 18:30:23.420	admin	0	127.0.0.1	KrEsaD87.k23

Kategorie

Performance killers

Finalizers vs. Garbage Collection

DEMO

```
private readonly Localization[] items;
public string GetLocalization(string key, CultureInfo culture)
{
    return items.
        Where(x => x.Equals(new Localization(key, culture))).
        Select(x => x.Text).
        FirstOrDefault();
}
public bool Equals(Localization other)
{
    if (object.ReferenceEquals(other, null)) return false;
    return (Key.Equals(other.Key) && LCID.Equals(other.LCID));
}
```

...kterak potěšit GarbageCollector

stovky řetězců per Page

tisíce Localizations v items

>200 000 volání constructoru per Page

<compilation debug="true" />

Optimize code = false

batchCompilation = false

no request timeout

vypínání cachování WebResources.axd, ScriptResource.axd, ...

aktivuje debugging-friendly specifika

- unminified verze JScriptů, CSS, ...
- #if DEBUG kód
- větší spotřeba paměti

<deployment retail="true|false"/>

machine.config/configuration/system.web

machine-wide

málo známé, málo používané , málo dokumentované

nastavuje debug="false"

vypíná výstup do trace

vypíná podrobné chyby pro remote clienty (customErrors)

```
private readonly Dictionary<string, string> localizedUrls;
private string GetUrl(string lang)
{
    if (localizedUrls.ContainsKey(lang))
        return localizedUrls[lang];
    return "/";
}
```

```
private string GetUrl(string lang)
{
    if (localizedUrls.TryGetValue(lang, out string url))
    {
        return url;
    }
    return "/";
}
```

Proč hledat dvakrát?

Sessions

DEMO

Kategorie

Vulnerabilities

ASP.NET Overposting / Mass Assignment

DEMO

Foreign Code Execution (Upload)

DEMO

Kategorie

Code Smell

Bug-only výjimky nezachytávejte

```
try
{
    DoSomething();
}
catch (NotImplementedException)
{
    // should not happen very often
}
```

NullReferenceException

InvalidOperationException

ArgumentException

ArgumentNullException

...

Re-inventing wheel

```
public static Exception SendAlert(string subject, string body)
{
    Exception exceptionOut = null;
    try
    {
        MailMessage message = new MailMessage();
        // ...
    }
    catch (Exception exception)
    {
        exceptionOut = exception;
    }
     return exceptionOut;
}

var ex = SendAlert(subject, body);
if (ex != null) // ?? catch (ex)
{
    Log(ex);
}
```

Kategorie

WTF?!

```
lock(new object())
{
    // thread-safe
}
```

...vygůglil jsem, že stačí lock na new object

```
private object myLock = new object();


lock(myLock)
{
    ...
}
```

```
[Flags]
public enum TreeNodeType
{
    Normal,
    Linked,
    Locked
}

if (t.HasFlag(TreeNodeType.Normal))
{
    // WTF? always true!
}
```

[Flags] vždy s hodnotami, jinak je

Normal = 0, Linked = 1, Locked = 2, ...

```
[Flags]
public enum TreeNodeType
{
    Normal = 1,
    Linked = 2,
    Locked = 4  // 8, 16, ...
}
```

Task: Importuj jen druhy 2, 4 a 5

```
int[] nenacitaneDruhy = new int[]
    { 1, 3, 6, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 19, 50, 51, 52, 53, 54 };

if (!nenacitaneDruhy.Contains(druhZakazky))
{
    // importuj
}
```

Pozitivní přístup!

```
DataSet dsResult = new DataSet();
SqlDataAdapter myDataAdapter = new SqlDataAdapter(
    "SELECT COUNT(*) FROM Uzivatel", "**ConnString**");
myDataAdapter.Fill(dsResult);
string count = dsResult.Tables[0].Rows[0][0].ToString();
dsResult = null;
```

Umím DataSety, tak je používám

```
int count2 = (int)cmd.ExecuteScalar();
```

```
query.DateTo = DateTime.Today.Date;
```

...pro jistotu.

```
// DateTime class
public static DateTime Today
{
    get
    {
        return Now.Date;
    }
}
```

Process Crash

DEMO

Code-review Req: "Stream vrácený metodou GetMemoryStream není disposován"

Oprava: ...doplněn `using`

```
public static MemoryStream GetMemoryStream(Stream stream)
{
    using (MemoryStream memoryStream = new MemoryStream())
    {
        byte[] readBuffer = new byte[4096];
        int bytesRead;

        while ((bytesRead = stream.Read(readBuffer, 0, readBuffer.Length)) > 0)
        {
            memoryStream.Write(readBuffer, 0, bytesRead);
        }

        return memoryStream;
    }
}
#endregion
```

Kategorie

Coding culture

```
// Kontrola vyplnění RČ a IČ dle právní formy
if (akce.DotacePrijemcePravniFormaTyp == 1)
    chybaAkce = "Pro typ '1' musí být zadáno RČ a nesmí být vyplněno IČ!";
if (akce.DotacePrijemcePravniFormaTyp == 2)
    chybaAkce = "Pro typ '2' musí být alespoň jedna z položek RČ a IČ vyplněna!";
if (akce.DotacePrijemcePravniFormaTyp == 3)
    chybaAkce = "Pro typ '3' musí být zadáno IČ a nesmí být vyplněno RČ!";
```

Magic Numbers NEEE!

```
public enum PravniForma
{
    Nepodnikatel = 1,
    Zivnostnik = 2,
    PravnickaOsoba = 3
}

switch (akce.DotacePrijemcePravniFormaTyp)
{
    case PravniForma.Soukromnik:
        chybaAkce = "...";
        break;
    case PravniForma.Zivnostnik:
        chybaAkce = "...";
        break;
    case PravniForma.PravnickaOsoba:
        chybaAkce = "...";
        break;
}
```

```
private void GetListForMonth(SqlConnection sqlConnection,
                             int month, int year, Dictionary<string, bool> list)
{
    list.Clear();
    // ...
    while (sqlDataReader.Read())
    {
        list.Add(sqlDataReader[0].ToString(), true);
    }
    // ...
}
```

```
var list = GetListForMonth(conn, 10, 2014,
```

```
var list = new List<string>();
GetListForMonth(conn, 10, 2014, list);
```

http://knowledge-base.havit.cz

Q & A