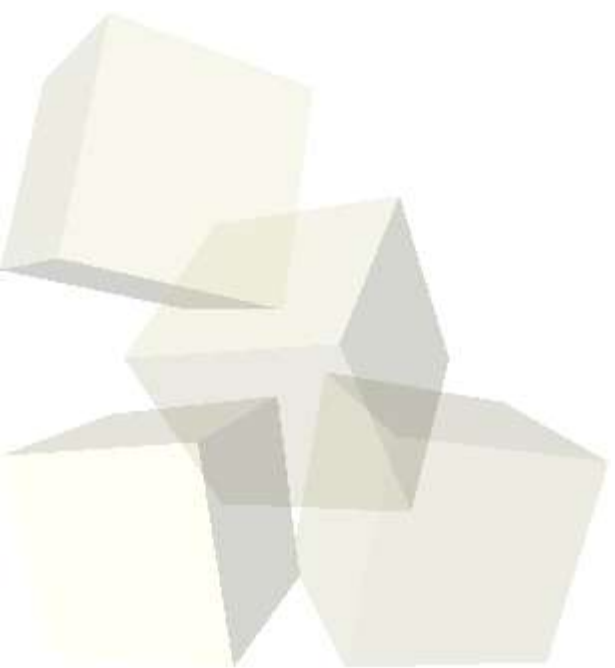




# **Modern ASP.NET Caveats**

**H D Moore**





- # Incompatible changes

- # Many sites stuck with 1.0

- # Migration creates security holes

- # Security improvements

- # Keys can be isolated by app

- # Remoting deserialization checks

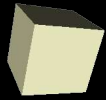




# Insecure Configuration

- # Configuration is #1 issue
- # Information disclosure
- # Crypto should be mandatory
- # Many large sites vulnerable
- # Most .NET resource sites leak
- # <http://research.microsoft.com>





- # Plain old bugs
- # Easy to force verbose errors
- # XSS validation too broken to use
- # Cookieless sessions being used
- # Sliding sessions can collide
- # Insecure docs still #1 complaint





## # DigitalOffense related resources

# <http://www.digitaloffense.net/confs/core02/slides/>

# <http://www.digitaloffense.net/dnascan.pl.gz>

# <http://builder.com.com/5100-6387-1044868.html>

# <http://www.microsoft.com/technet/security/bulletin/ms02-026.mspx>

## # Compatibility issues (1.0 to 1.1)

# <http://www.gotdotnet.com/team/changeinfo/default.aspx>

## # Contact information

# hdm [at] digitaloffense.net

