

Web Security and the OWASP Top 10: The Big Picture Security Misconfiguration

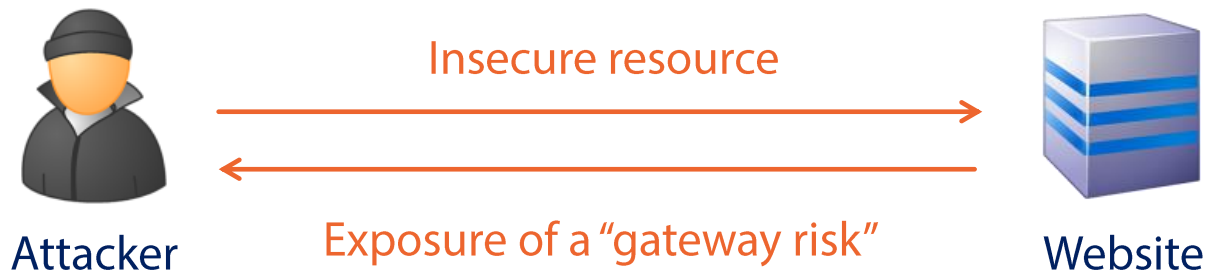
Troy Hunt
troyhunt.com
@troyhunt



pluralsight 
hardcore developer training

Security Misconfiguration Overview

Attack Vectors	Security Weaknesses		Technical Impacts
Exploitability Easy	Prevalence Common	Detectability Easy	Impact Moderate



Understanding Security Misconfiguration

- Is any of your software out of date? This includes the OS, Web/App Server, DBMS, applications, and all code libraries
- Are any unnecessary features enabled or installed (e.g. ports, services, pages, accounts, privileges)?
- Are default accounts and their passwords still enabled and unchanged?
- Does your error handling reveal stack traces or other overly informative error messages to users?
- Are the security settings in your development frameworks and libraries not set to secure values?

Common Defences Against Security Misconfiguration

**Always
harden the
install**

- Turn off features that aren't needed
- Apply the "principle of least privilege"



**Tune the app
security config**

- Ensure it's production-ready
- Defaults are often not right

**Ensure
packages are
up to date**

- Be conscious of 3rd party tool risks
- Have a strategy to monitor and update

Security Misconfiguration in the Wild – ELMAH

[Web](#) [Images](#) [Videos](#) [Shopping](#) [News](#) [More ▾](#) [Search tools](#)

About 225,000 results (0.08 seconds)

[Error log for /LM/W3SVC/2/ROOT on WIN-9UF06OH03DG \(Page #1\)](#)
[www.botas.cz/elmah.axd ▾](#)
Host, Code, Type, Error, User, Date, Time. WIN-9UF06OH03DG, 404, Http, The controller for path '/picture/aktuality/CGD4sm.jpg' could not be found. Details...

[Error log for /LM/W3SVC/9/ROOT on EVOLET \(Page #4\) - Evolet.biz](#)
[evolet.biz/elmah.axd?page=4&size=15 ▾](#)
Error Log for ROOT on EVOLET. RSS Feed · RSS Digest · Download Log · Help · About. Errors 46 to 60 of total 2,542 (page 4 of 170). Start with 10, 15, 20, 25, ...

[Error log for /LM/W3SVC/45673/ROOT on NT11 \(Page #1\) - RREM](#)
[rrem.dk/Elmah.axd ▾](#)
Host, Code, Type, Error, User, Date, Time. NT11, 404, Http, Error with ID '27ee5702-f4dc-433f-9401-25b86b9fec4' not found. Details... 26-01-2014, 09:54.

[Error log for /LM/W3SVC/9/ROOT on VMSHELDON \(Page #31\)](#)
[www.foxdevs.net/elmah.axd?page=31&size=30 ▾](#)
Host, Code, Type, Error, User, Date, Time. VMSHELDON, 404, Http, The controller for path '/robots.txt' was not found or does not implement IController. Details...