Hello my name is Paul Ionescu and I lead the IBM Security Systems Ethical Hacking Team. Today I will cover number five on the OWASP Top 10 list: Security Misconfiguration.

Vulnerabilities in the Security Misconfiguration category allow attackers to take advantage of various server or application features intended for debugging or testing environments.

Such flaws include but are not limited to: Debugging enabled, Incorrect folder permissions, Using default credentials or Being able to access remotely setup or server management pages.

Here's our Altoro Mutual demo application, an extremely insecure banking site. Besides using a very old version of IIS it has directory listing enabled on the admin directory.

This allows an attacker to navigate without any problems and access the contents of this directory.

Incidentally the admin has left around an Excel document with a lot of juicy PII in it. We can find in here social services numbers, credit cards and home addresses!

You can prevent such issues by ensuring your servers are configured securely. The principle of least privilege should be observed in this case as well.
Many servers come with debugging and management features turned off by default nowadays. Be extra careful with turning such features back on. Disable default credentials and of course disable directory listing.

Besides using such countermeasures you can use a tool like AppScan Standard to test for common Security Misconfiguration issues. The Infrastructure category in AppScan will specifically look for common mistakes in server configuration.

Here's how we can use AppScan to detect the vulnerability that we demonstrated earlier on our Altoro Mutual web site.

In the interest of time we will only enable the Infrastructure tests in the test policy.

Now let's point AppScan at our misconfigured server and run a full scan.

A few minutes later the scan has, of course, identified the problematic directory and a few other directories as well.

Hope you have found this short video useful and best of luck developing secure applications.