Hi my name is Jonathan and I'm a member of the IBM Security systems ethical hacking team.

Today, I'll be talking to you about unvalidated redirects and forwards. We'll discuss how to abuse them and how to protect yourself against them.

In some cases, your application may need to redirect to another location by sending a redirect header to the client in an HTTP response. This can sometimes be seen in applications that redirect after a successful authentication.

In some cases, the redirection will be in the login form or the URL. both of which can be tampered with by the user. Unvalidated redirects can also be seen in router type pages that redirect based on user supplied input.

Developers can prevent the weakness by validating user input and also verifying the URL in question is actually an approved target URL. You can use a map type method where URLs are mapped to names such as home page, product pages, or inventory page. This would prevent users from supplying an invalid URL.

In this example, we're going to send an email to somebody that redirects them to another location. In the email, I've made a hyperlink to Altoro's website which actually redirects you to another site which is clearly not Altoro Mutual.

To locate these types of vulnerabilities, you can use AppScan Standard. AppScan will supply demo.testfire.net as the parameter value and if the HTTP and if the HTTP response contains a redirect to that location, then AppScan will report this as a vulnerability.

We can easily locate the test used in this example by searching for 'phishing'.

Now that the scan has completed, we can see that the content parameter contains the demo.testfire.net URL which shows that this page is vulnerable.

Thank you very much for watching. This concludes our video on unvalidated redirects and forwards.