**Un-validated Redirects & Forwards**

This occurs when a web application accepts untrusted user input that specifies a location to an external site, where the application utilises the provided location to redirect the browser to the location.

Instructions:

Create a new web application using xampp.

Create a few test html pages. (These will be used to perform valid redirects within the web application)

Create two php files redirect1.php and redirect2.php with the following code

redirect1.php

<!DOCTYPE html>

<html>

<body>

<?php

$goto = $\_GET["loc"];

echo "<script>location.href='$goto';</script>";

?>

</body>

</html>

redirect2.php

<!DOCTYPE html>

<html>

<body>

<?php

$goto = $\_GET["loc"];

$loc\_head = "Location: " . $goto;

header($loc\_head);

?>

</body>

</html>

How did you validate that the application is vulnerable to an un-validated redirect?

*In its current state, I can supply a url from outside the application which will cause the redirect to go to an external site. This could allow a malicious agent to supply a redirect to a victim to their own site.*

Fix the code to only allow the application to redirect to the test pages you created within the application.

What approach did you take?

*I created an array of allowed pages the application can navigate to with a function that checks if the value supplied is one of those pages. If no match is found, no redirect occurs.*

Demo your solution to your lecturer.