Unvalidated Redirect/Forward Prevention

CYBER SECURITY &
PRIVACY FOUNDATION

- Input should be mapped to a set of fixed input values (numbers), rather than the actual URL.

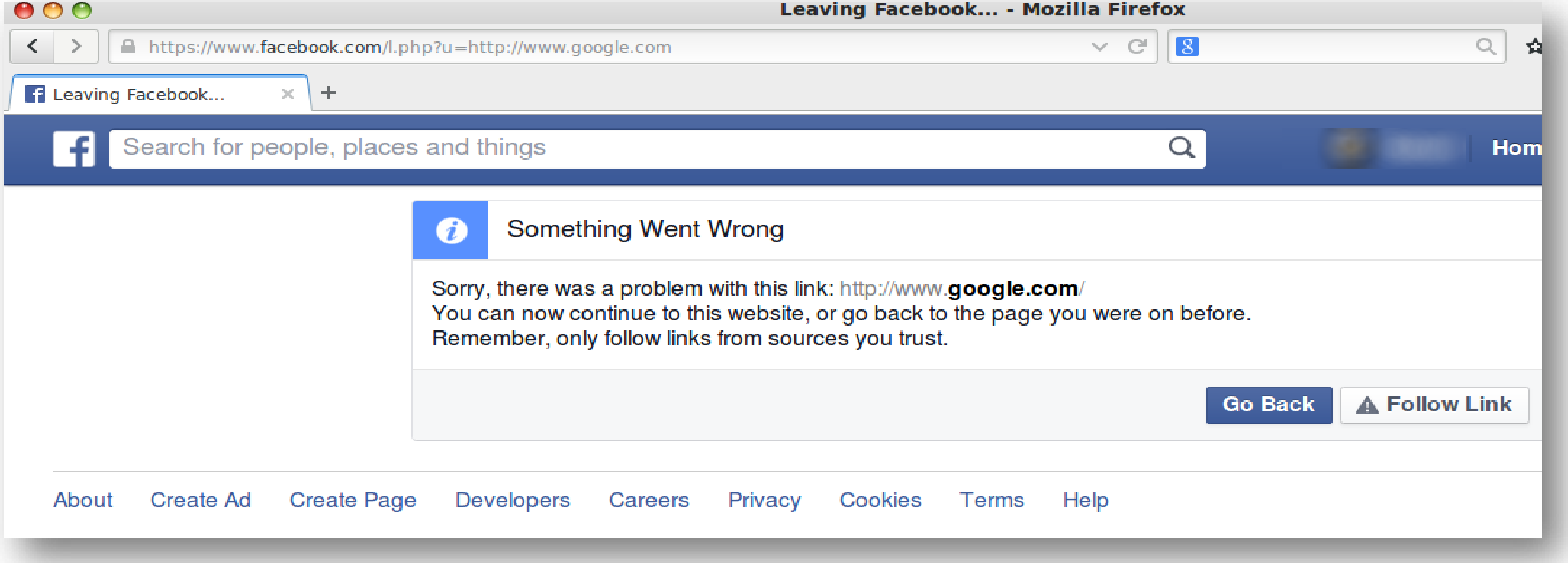
- The Web application then translate this value to the target URL.

- For example, value ‘1’ could map to “http://www.example.com” and “2” could map to “http://www.bing.com”

Example PHP Code

```
<?php
      $urls=array(1=>”http://www.example.com”, 2=>
“http://www.bing.com”,3=> “http://www.google.com”);
    $target_id=$_GET[‘id’];
    header(“location: “. $urls[$target_id]);
?>
```

Display a clear warning that they are leaving the current site, and have them click a link to confirm button.



Leaving Facebook... - Mozilla Firefox

https://www.facebook.com/l.php?u=http://www.google.com

Something Went Wrong

Sorry, there was a problem with this link: http://www.**google.com**/
You can now continue to this website, or go back to the page you were on before.
Remember, only follow links from sources you trust.

- Try to avoid using redirects and forwards.

- Ensure that the supplied value is valid, appropriate for the application, and is authorized for the user.