

Refactoring for Security

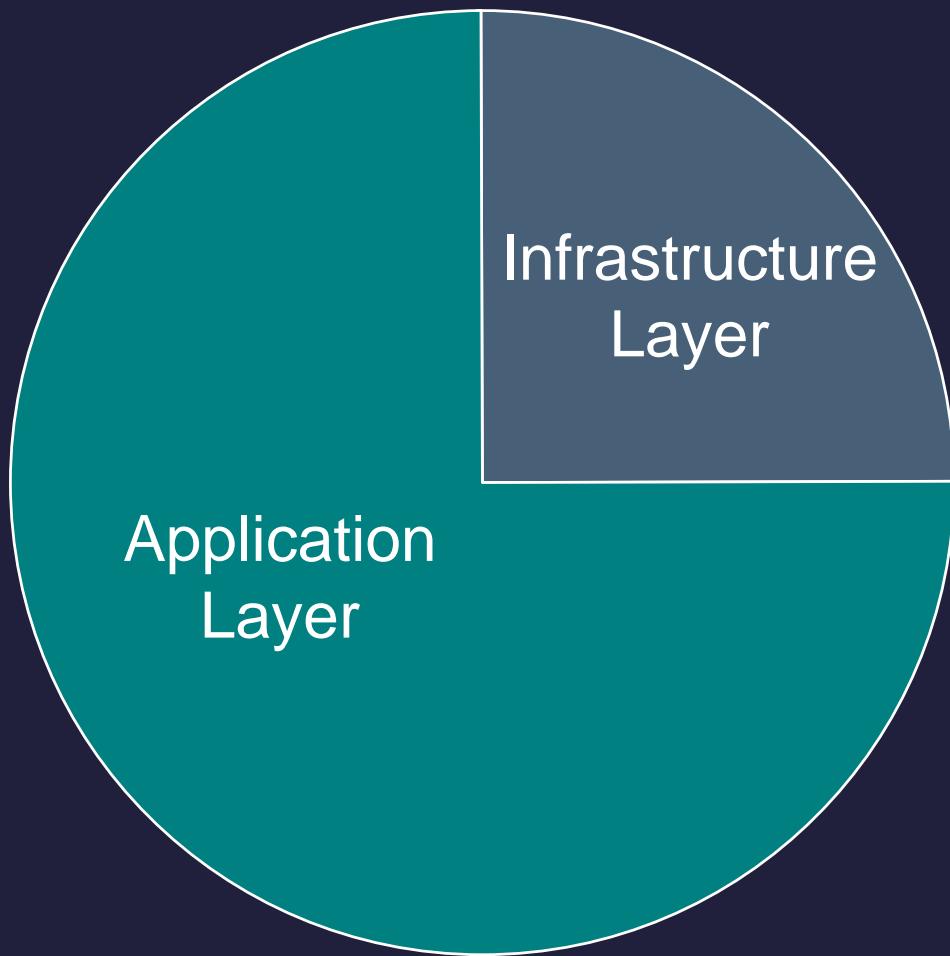
Toan Huynh

Department of Electrical and Computer Engineering

University of Alberta

huynh@ece.ualberta.ca

Cyberattacks on Web-based Systems



The Problem

...

```
if (input contains valid chars) then  
    process input  
end if
```

...

The Problem (cont.)

...

process input

...

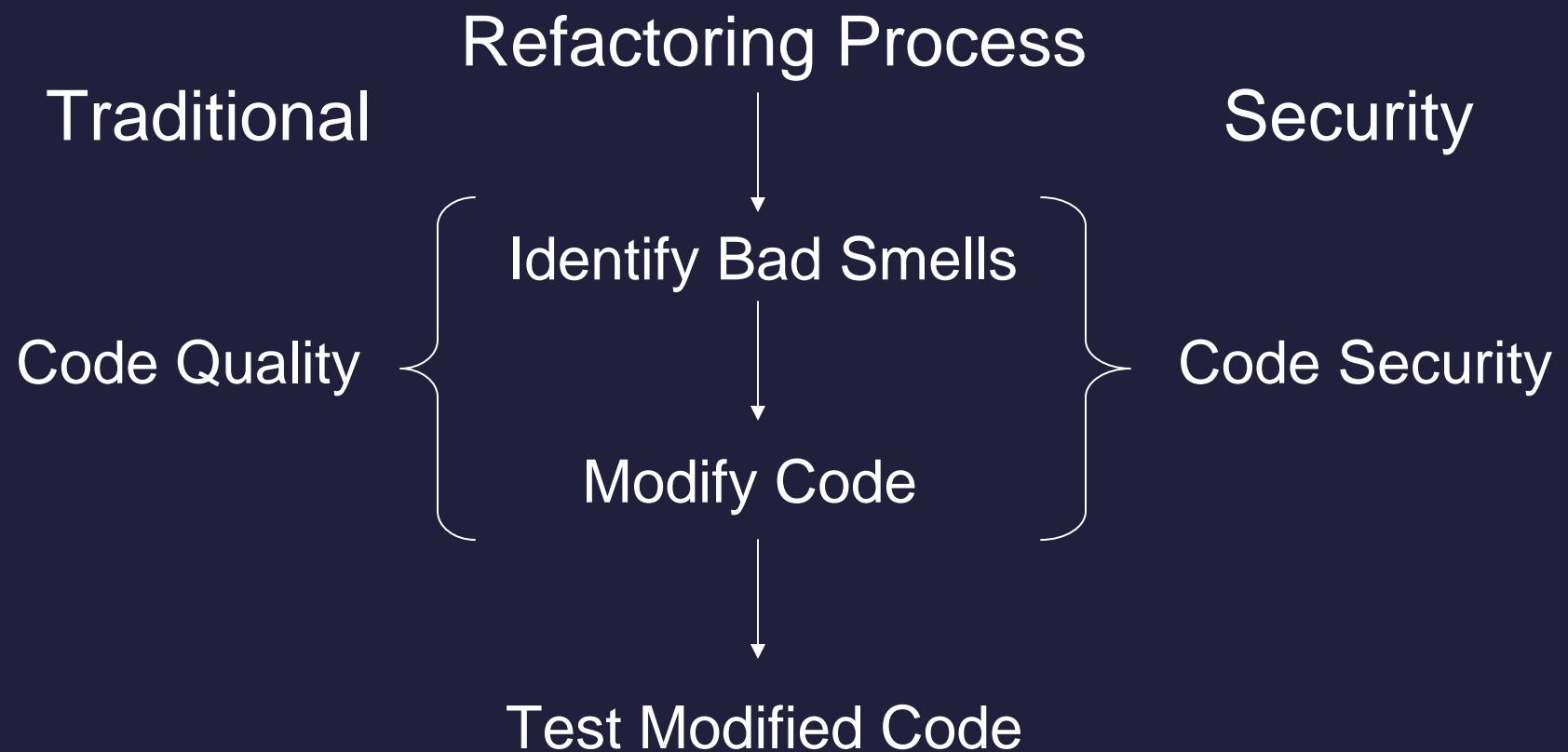
The Problem (cont.)

- Secure coding practices are not being used which leads to
 - Buffer overflow exploits
 - SQL injection
 - Cross-site scripting
 - ...

2-Step Solution



Refactoring: Traditional vs Security



Example : Cross-site Vulnerability

.. Fragapalooza July 15, 2004
2:48 am by end

Welp it doesn't seem like that long ago we hosted our last Fragapalooza and here we are hosting another! **Fragapalooza 2004** is now underway. This whole weekend my life is devoted to making a bunch of gamers happy organizing the largest LAN party in Canada.

If you want to visit please feel free to bring lots of yummy food to eat. 😊

There are no comments yet!

Title (Max 50):

Text (Max 250):

Your name (Max 15):

Your Email (Max 100):

Example (cont.)

.. Fragapalooza July 15, 2004
2:48 am by **enek**

Welp it doesn't seem like that long ago we hosted our last Fragapalooza and here we are hosting another! **Fragapalooza 2004** is now underway. This whole weekend my life is devoted to making a bunch of gamers happy organizing the largest LAN party in Canada.

If you want to visit please feel free to bring lots of yummy food to eat. 😊

There are no comments yet!

Title (Max 50): <script>alert('XSS Vulnerability Detected')</script>

Text (Max 250):

Your name (Max 15):

Your Email (Max 100):

Example (cont.)



.. Fragapalooza

July 15, 2004
2:48 am by **enek**

Welp it doesn't seem like that long ago we hosted our last Fragapalooza and here we are hosting another! **Fragapalooza 2004** is now underway. This whole weekend my life is devoted to making a bunch of gamers happy organizing the largest LAN party in Canada.

If you want to visit please feel free to bring lots of yummy food to eat. 😊

XSS Test #1

May 01, 2005
10:25 pm

<script>alert('XSS Vulnerability Detected')</script>

from Anonym

Example (cont.)

Title (Max 50):

XSS Test #2

Text (Max 250):

Your name (Max 15):

Your Email (Max 100): '><script>alert('test')</script>"/>

Post

Example (cont.)

July 15, 2004
2:48 am by enek

Welp it doesn't seem like that long ago we hosted our last Fragapalooza and here we are hosting another! **Fragapalooza 2004** is now underway. This whole weekend my life is devoted to making a bunch of gamers happy organizing the largest LAN party in Canada.

If you want to visit please feel free to bring lots of yummy food to eat. ☺



The screenshot shows a JavaScript alert dialog box titled "[JavaScript Application]". Inside the dialog, there is a yellow warning icon with an exclamation mark and the word "test". At the bottom right of the dialog is an "OK" button. A red curved arrow points from the bottom of the slide towards the "test" text in the alert box. In the bottom right corner of the slide, there is a timestamp: "July 15, 2004 2:48 am by enek".

```
<script>alert('XSS Vulnerability Detected')</script>
```

Filter All Outputs

- All outputs should be validated before they are to be displayed.

Filter All Outputs (cont.)

```
<?php
...
$message = htmlspecialchars($row['message']);
print($message');
...
print($row['email']);
...
?>
```

Filter All Outputs (cont.)

```
<?php
...
$message = htmlspecialchars($row['message']);
print($message');
...
$email = htmlspecialchars($row['email']);
print($email);
...
?>
```

Summary

- Two step process will allow more secure applications to be developed
- More security refactors will be introduced
- A tool is under development