

Refactoring for Security

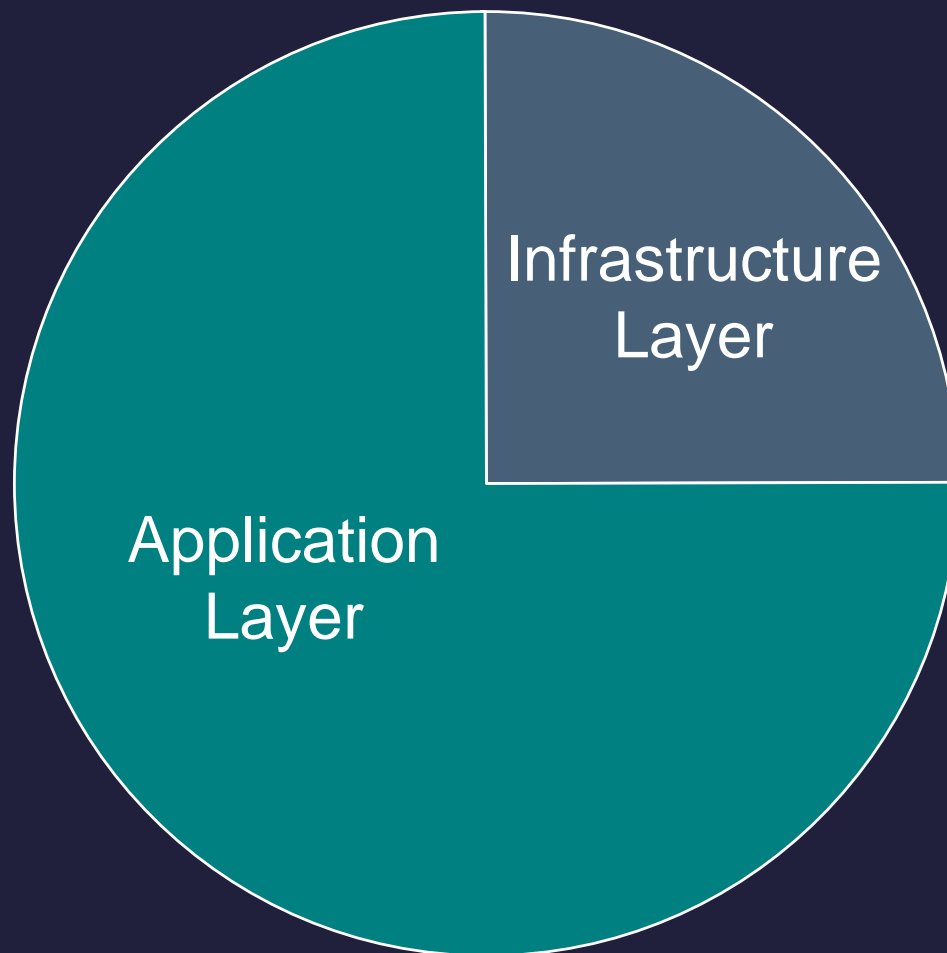
Toan Huynh

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.)

...

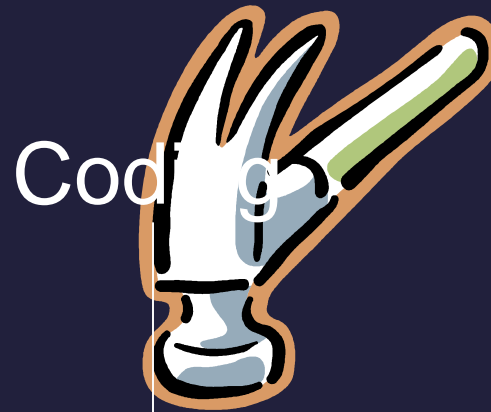
process input

...

The Problem (cont.)

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

2-Step Solution



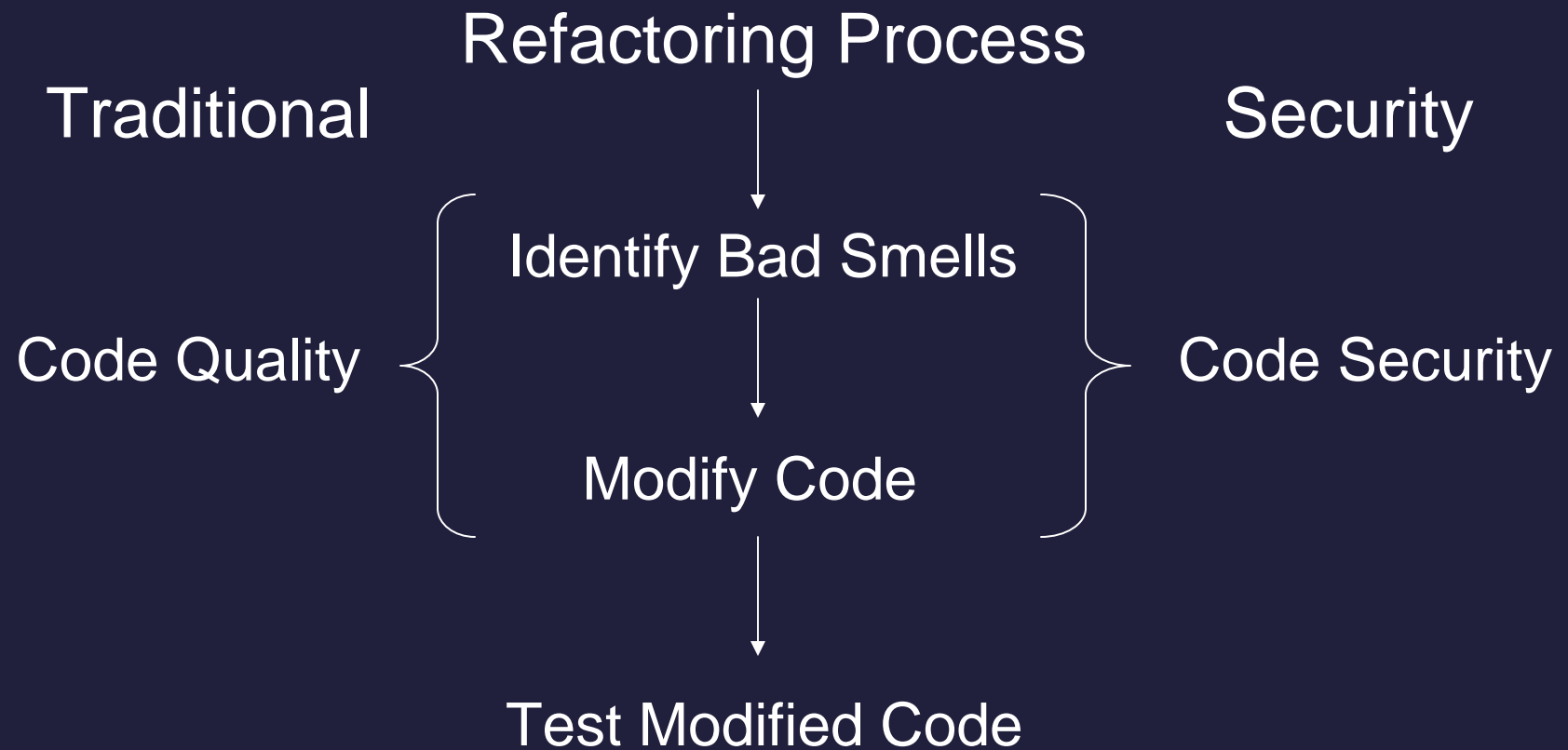
Coding

Programming



Refactor for Security

Refactoring: Traditional vs Security



Example : Cross-site Vulnerability

∴ Fragapalooza

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

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.)

∴ FragapaloozaJuly 15, 2004
2:48 am by **enck**

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): XSS Test #1

Text (Max 250): `<script>alert('XSS Vulnerability Detected')</script>`

Your name (Max 15): Anonym

Your Email (Max 100):

Post

Example (cont.)

∴ FragapaloozaJuly 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. 😊

XSS Test #1May 01, 2005
10:25 pm

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

from Anonym

Example (cont.)

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. 😊

[JavaScript Application]



test

OK

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

, 2005
:25 pm

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