

# Symbolic Execution for PHP Web Applications

Stefan Mühlbauer

Technische Universität Braunschweig, Germany

September 9, 2016

# PHP

---

- Script language, widely used for server-side web applications
- ranked 6th on TIOBE index (09/16)

# PHP

---

- Script language, widely used for server-side web applications
- ranked 6th on TIOBE index (09/16)
- Popular projects, such as *Wordpress*, *MediaWiki* or *vBulletin*



# Motivation

---

Tool support: Syntax highlighting  
for nested code (HTML, JavaScript)

# Motivation

---

Tool support: Syntax highlighting  
for nested code (HTML, JavaScript)

```
echo '<p>What a ' ;  
if (sunny) {  
    echo 'sunny day';  
} else {  
    echo 'rainy day</p>';  
}
```

# Motivation

---

Tool support: Syntax highlighting  
for nested code (HTML, JavaScript)

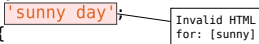
```
echo '<p>What a ' ;  
if (sunny) {  
    echo 'sunny day';  
} else {  
    echo 'rainy day</p>';  
}
```

# Motivation

---

Tool support: Syntax highlighting  
for nested code (HTML, JavaS-HTML validation of possible out-  
cript) put

```
echo '<p>What a ';  
if (sunny) {  
    echo 'sunny day';  
} else {  
    echo 'rainy day</p>';  
}
```



# Symbolic Execution

---

```
$x = input();  
$y = 2;  
$z = x + y;
```

```
if ($z > 0) {  
    $r = 'A';  
} else {  
    $r = 'B';  
}
```

```
print($r);
```



# Symbolic Execution

---

```
$x = input(); //  $x \leftarrow \alpha$   
$y = 2;  
$z = x + y;
```

```
if ($z > 0) {  
    $r = 'A';  
} else {  
    $r = 'B';  
}
```

```
print($r);
```

# Symbolic Execution

---

```
$x = input(); //  $x \leftarrow \alpha$   
$y = 2;      //  $y \leftarrow 2$   
$z = x + y;
```

```
if ($z > 0) {  
    $r = 'A';  
} else {  
    $r = 'B';  
}
```

```
print($r);
```

# Symbolic Execution

---

```
$x = input(); //  $x \leftarrow \alpha$   
$y = 2;      //  $y \leftarrow 2$   
$z = x + y;  //  $z \leftarrow \alpha + 2$ 
```

```
if ($z > 0) {  
    $r = 'A';  
} else {  
    $r = 'B';  
}
```

```
print($r);
```

# Symbolic Execution

---

```
$x = input(); //  $x \leftarrow \alpha$ 
$y = 2;       //  $y \leftarrow 2$ 
$z = x + y;    //  $z \leftarrow \alpha + 2$ 

if ($z > 0) { // if  $(\alpha + 2) > 0$ 
    $r = 'A';
} else {
    $r = 'B';
}

print($r);
```

# Symbolic Execution

---

```
$x = input(); //  $x \leftarrow \alpha$ 
$y = 2;      //  $y \leftarrow 2$ 
$z = x + y;  //  $z \leftarrow \alpha + 2$ 

if ($z > 0) { // if  $(\alpha + 2) > 0$ 
    $r = 'A'; //  $r \leftarrow 'A'$ 
} else {
    $r = 'B';
}

print($r);
```

# Symbolic Execution

---

```
$x = input(); //  $x \leftarrow \alpha$ 
$y = 2;       //  $y \leftarrow 2$ 
$z = x + y;   //  $z \leftarrow \alpha + 2$ 

if ($z > 0) { // if  $(\alpha + 2) > 0$ 
    $r = 'A'; //  $r \leftarrow 'A'$ 
} else {
    $r = 'B'; //  $r \leftarrow 'B'$ 
}

print($r);
```

# Symbolic Execution

---

```
$x = input(); //  $x \leftarrow \alpha$ 
$y = 2;       //  $y \leftarrow 2$ 
$z = x + y;   //  $z \leftarrow \alpha + 2$ 

if ($z > 0) { // if  $(\alpha + 2) > 0$ 
    $r = 'A'; //  $r \leftarrow 'A'$ 
} else {
    $r = 'B'; //  $r \leftarrow 'B'$ 
}

print($r);    // Choice( $\alpha + 2 > 0$ , 'A', 'B')
```