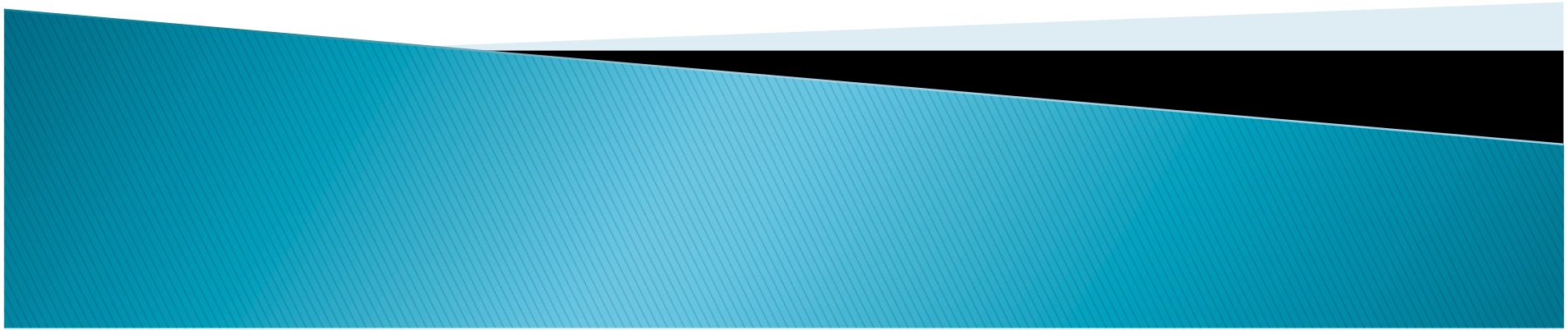
Fix Me Up:
Repairing Access-Control Bugs in Web Applications

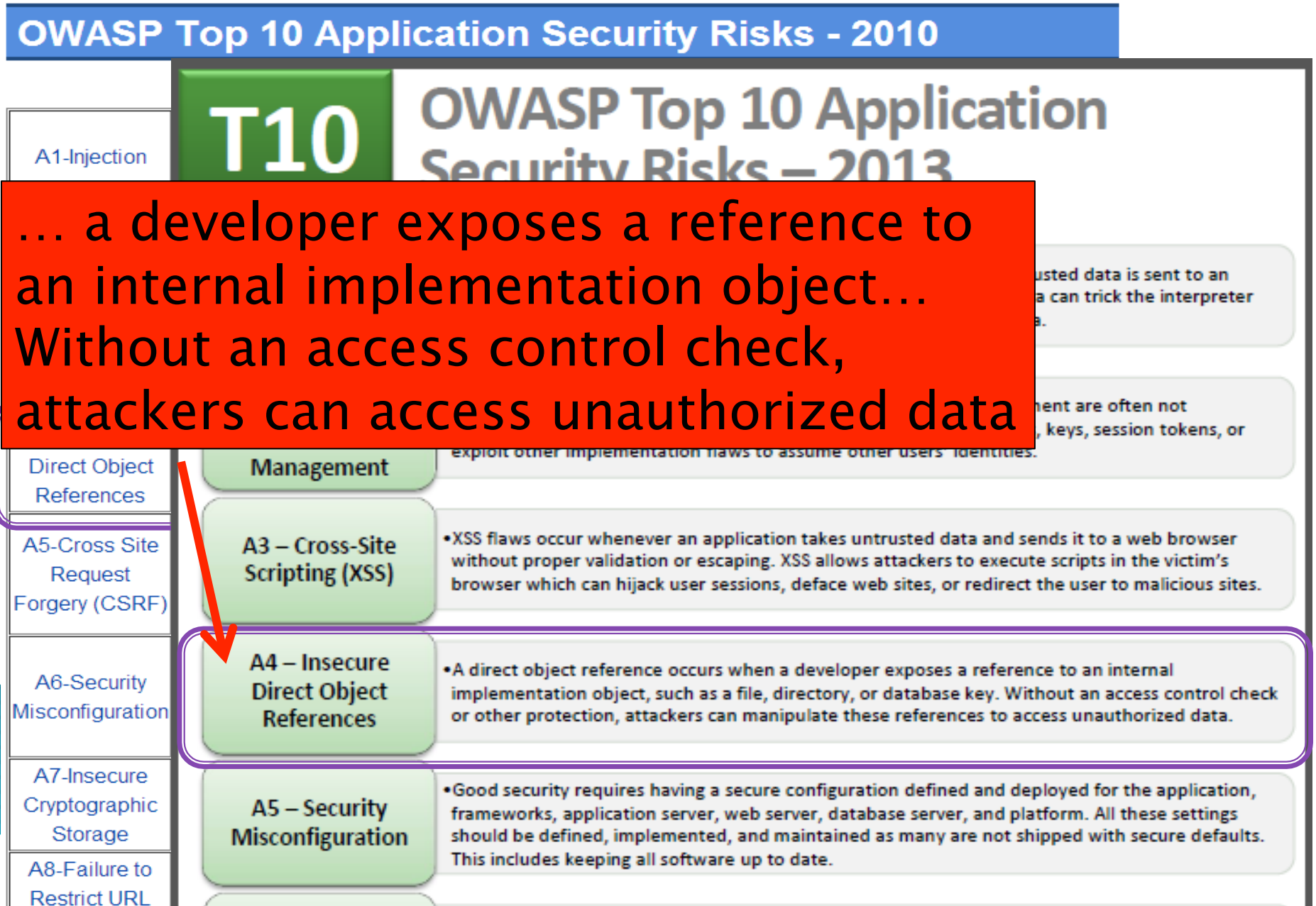
Sooel Son

Kathryn S. McKinley Vitaly Shmatikov

UT Austin and Microsoft Research



Access-control bugs



Access-control bugs (2)

(From WhiteHat Website Security Report 2012)

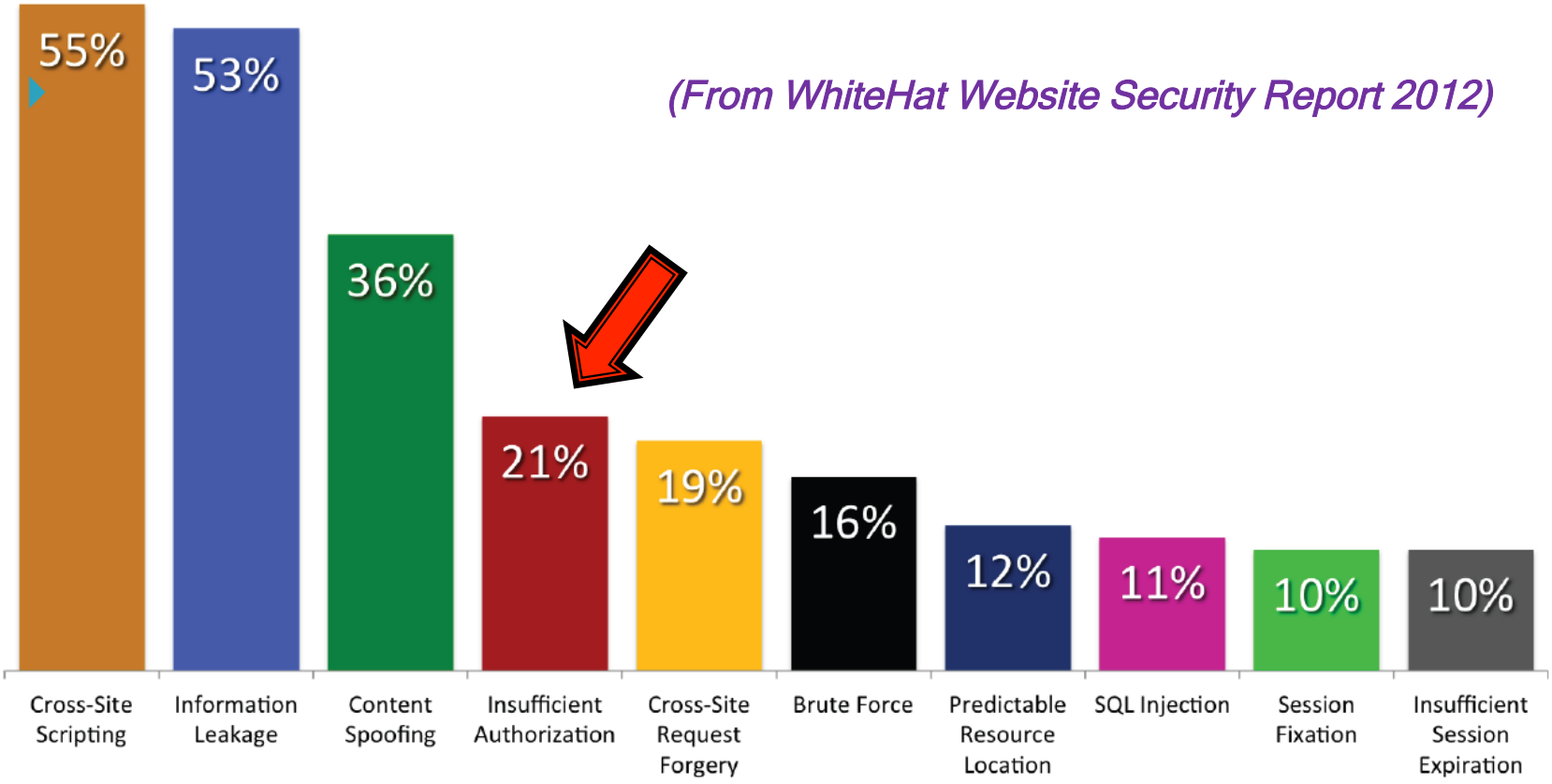


Figure 3. Top Ten Vulnerability Classes (2011)

Percentage likelihood that at least one serious* vulnerability will appear in a website

Forced-browsing attack

CVE-2004-2144,CVE-2004-2257,
CVE-2005-1688,CVE-2005-1697,
CVE-2005-1698,CVE-2005-1827,
CVE-2005-1654,CVE-2005-1668,
CVE-2005-1892,CVE-2009-2960,
CVE-2009-3168,CVE-2009-3597,
CVE-2011-0316,CVE-2012-3030,
CVE-2012-6451
.....

http://host/delete.php?id=victim_id

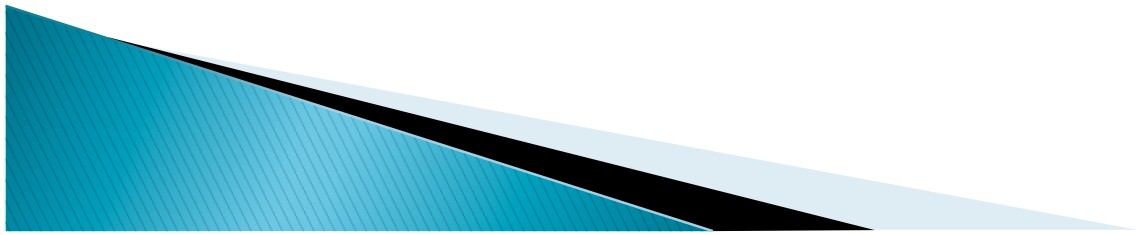

Make sure that every entry is locked with the proper access-control logic

About FixMeUp

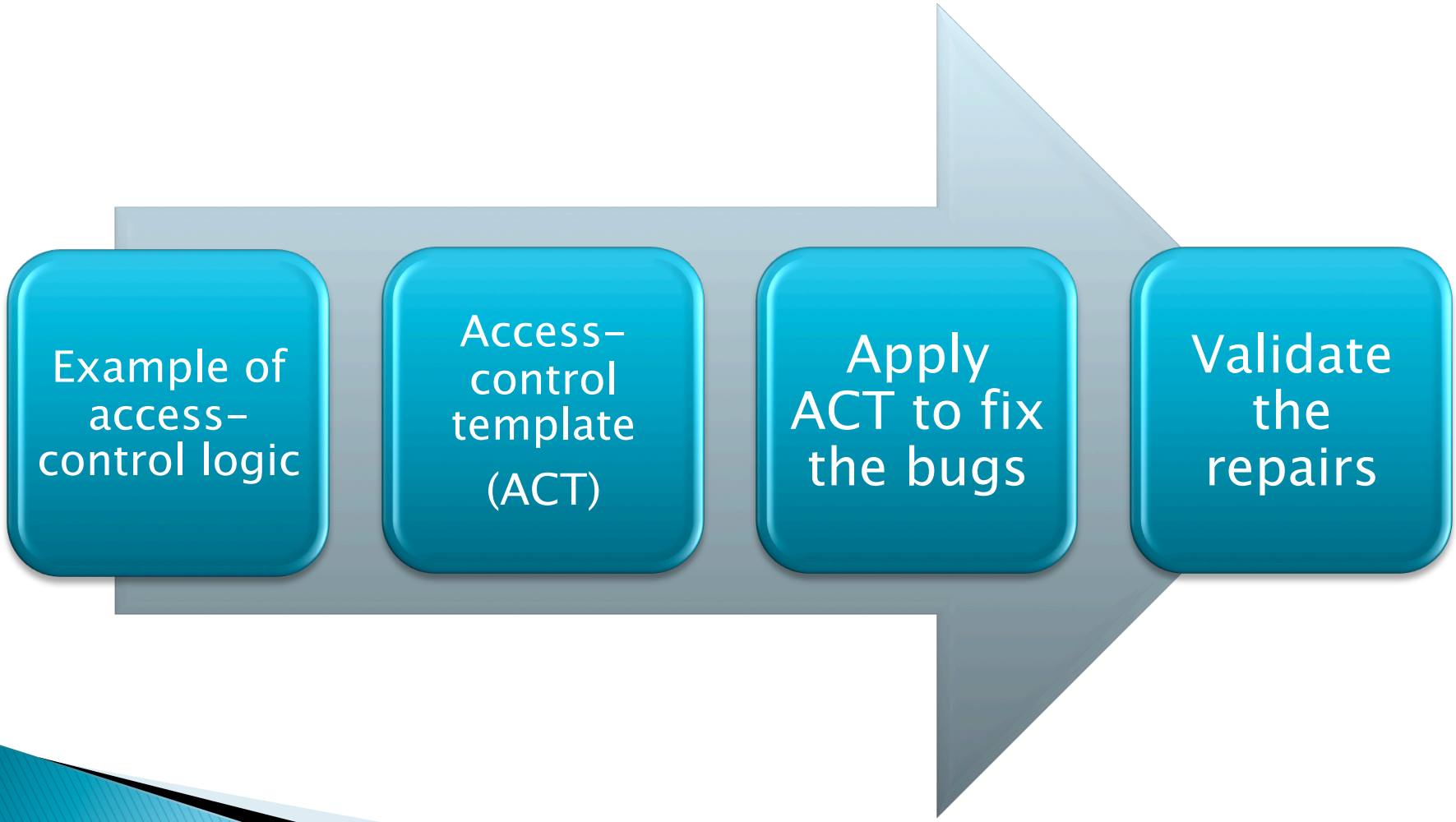
Static program transformation tool for finding and fixing access-control bugs in PHP applications

Given an example of correct access control …

- 1. Finds calling contexts that do not implement the correct access-control logic
- 2. Produces candidate repaired code that prevents forced-browsing attacks



FixMeUp workflow

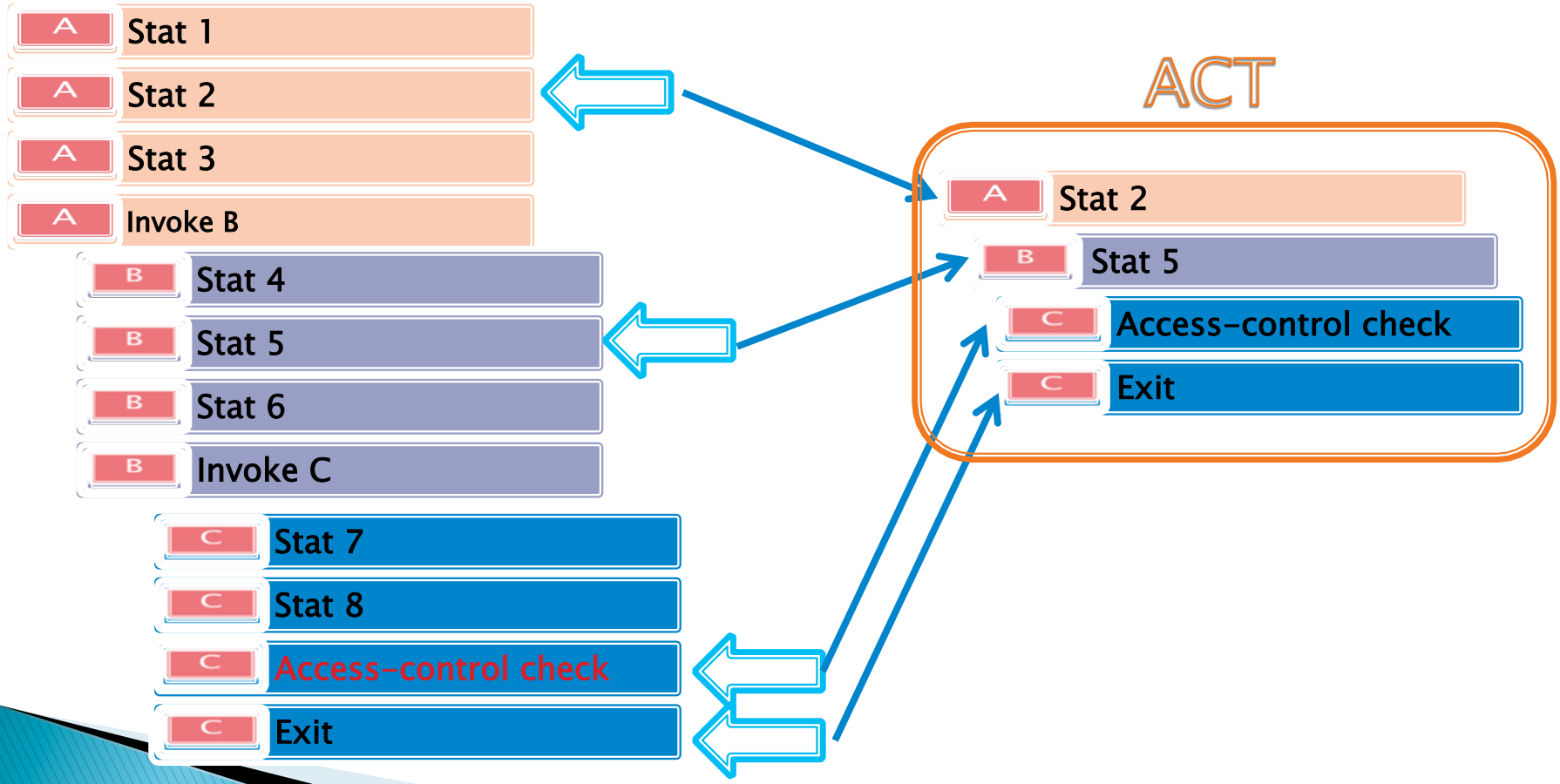


1.Example of access-control logic

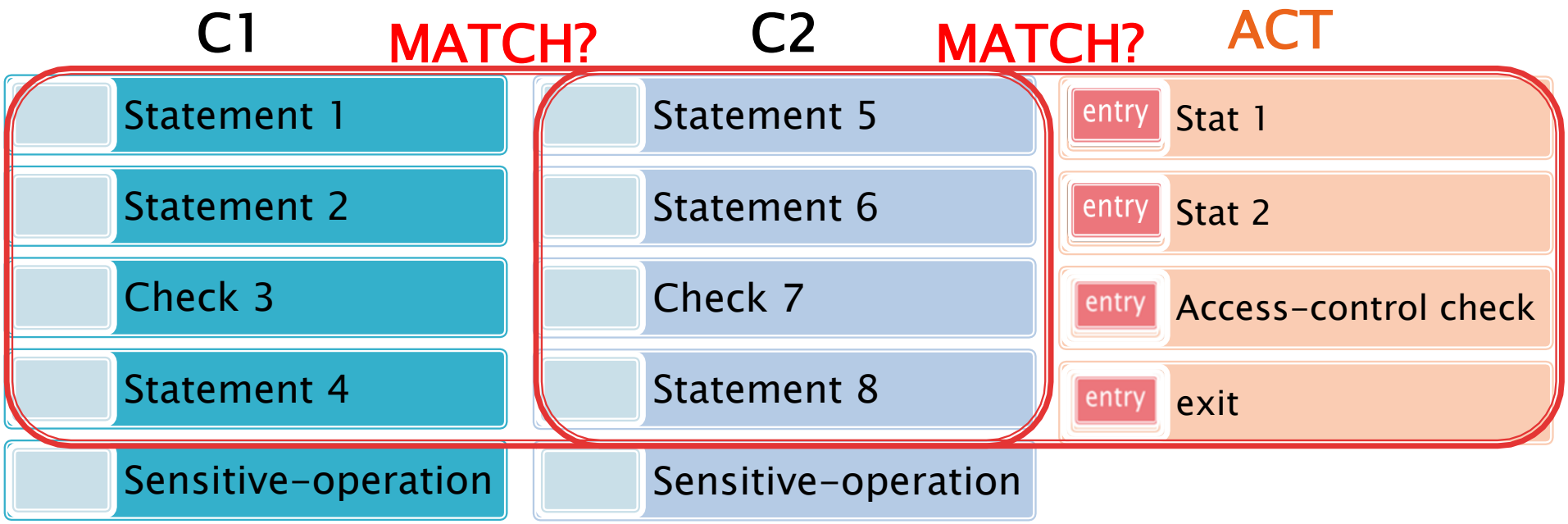
```
lockSession();
if(!empty($_SESSION['name']) && !empty($_SESSION['pass'])) {
  ……
 $logined = @mysql_affected_rows();
}
if($logined !== 1 && !empty($_COOKIE[COOKIE_USER]) && !empty
($_COOKIE[COOKIE_PASS])) {
  ……
 $logined = @mysql_affected_rows();
}
if($logined !== 1) {
  unlockSessionAndDestroyAllCokies();
  sleep(5);
  header('Location: '.QUERY_STRING_BLANK.'login');
  die();
}
```

2. Access-control template

- Compute an ACT

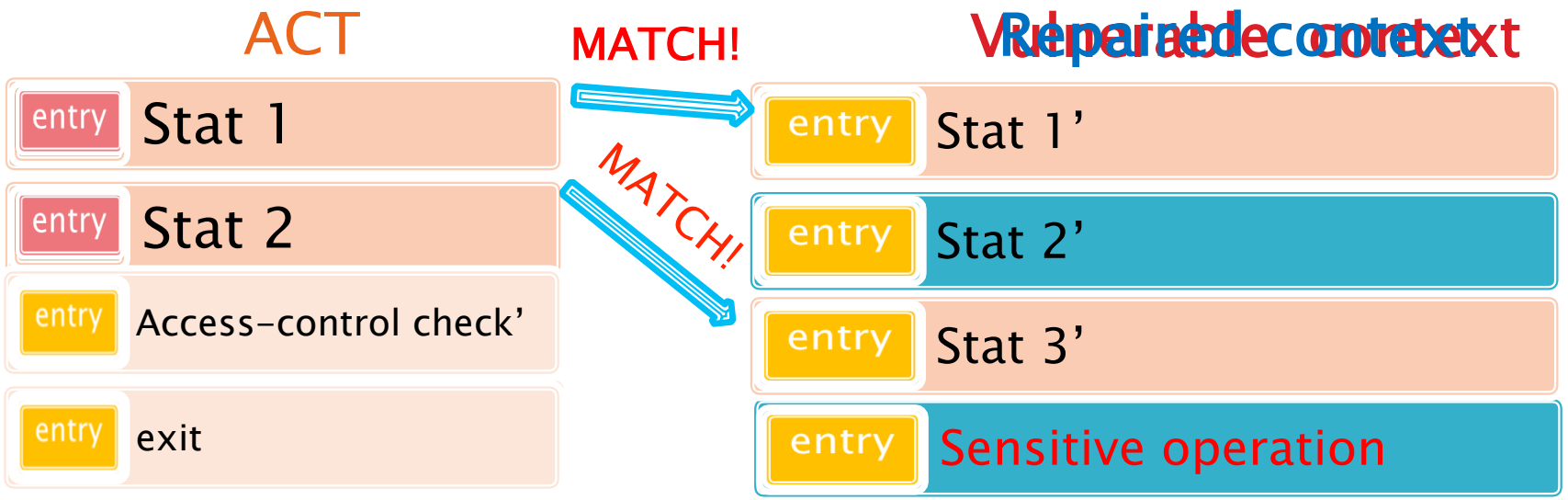


3. Apply ACT to fix the bugs



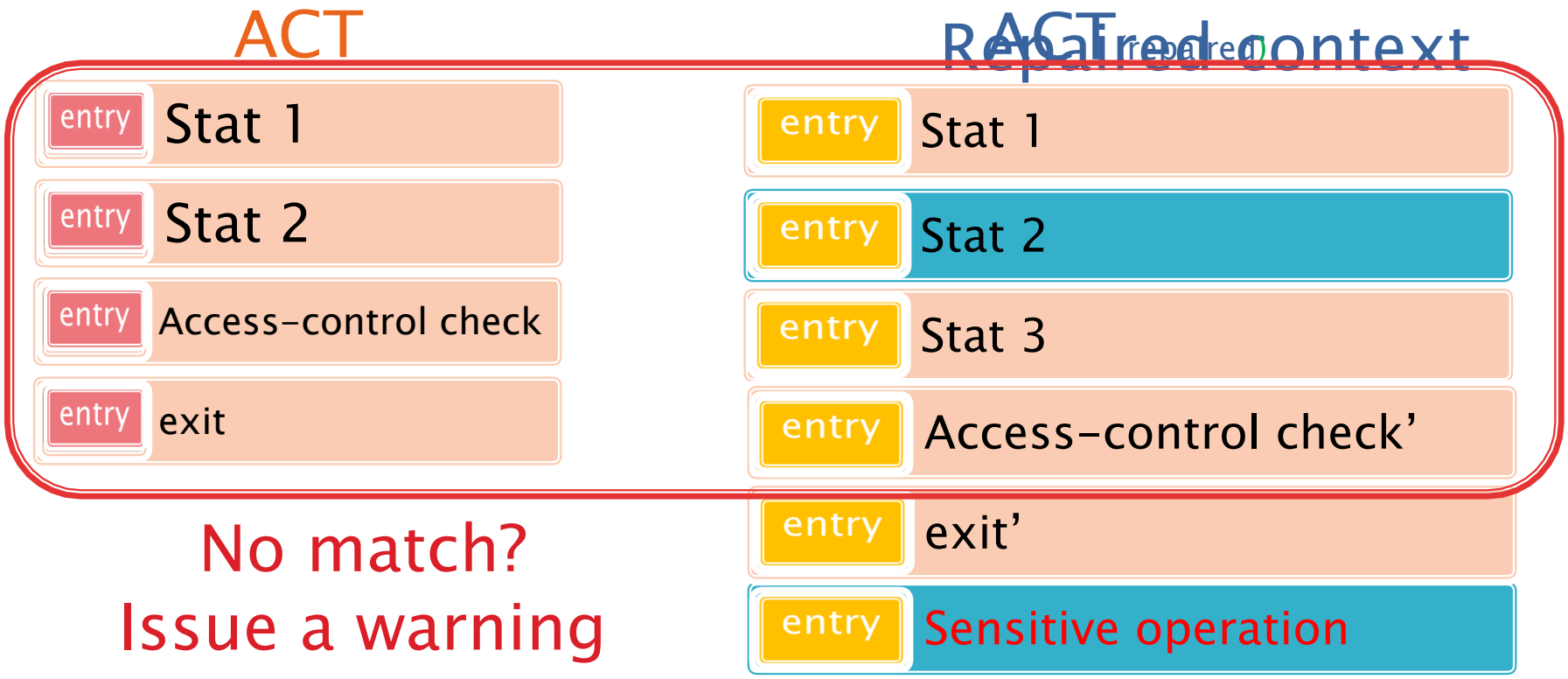
- Finds vulnerable contexts that do not implement the same logic as the ACT

3. Apply ACT to fix the bugs (2)



- Replicates ACT into the vulnerable context while reusing already existing statements

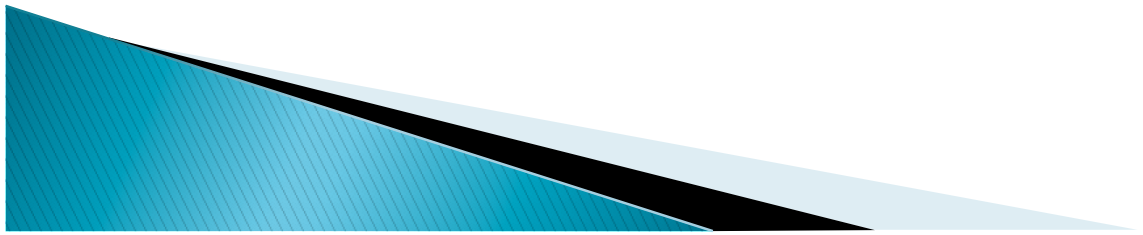
4. Validate repairs



- Recompute ACT – should be the same as before!

Evaluation

- 10 open-source interactive PHP server apps
- Generated 38 repairs
  - 31 correct
  - 7 in addition to already existing access-control logic
- 28 partial repairs
  - Reusing existing statements is important!
- 1 warning
- 1 unwanted side effect



Evaluation (2)

```
include('class/common.php') ; // [FixMeUp repair]
$GR_newone = new COMMON( ) ; / / [FixMeUp repair]
if (( $ SESSION [ ' no ' ] != 1)) { / / [FixMeUp repair]
 $GR_newone ->error( ' Require admin priviledge' , 1 , 'CLOSE' ) ; / /
[FixMeUp repair]
}
```

```
include('class/common.php') ; // existing statement
$GR = new COMMON( ) ; // existing statement
if (( $ SESSION [ ' no ' ] )) { / / [FixMeUp repair]
 $GR->error( ' Require login procedure' ) ; / / [FixMeUp repair]
}
.....
//@SSO( 'member')
@fwrite($tmpfs, $saveResult);
```

Evaluation (3)

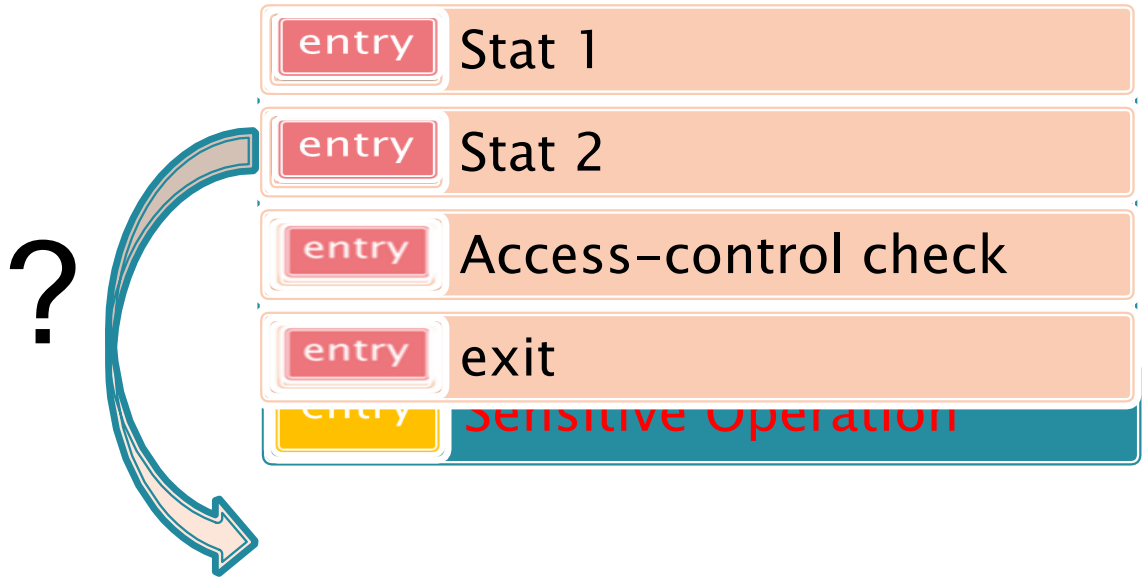
- Warning: after applying the ACT, repaired code does not implement the same logic as the ACT

```
Program Entry
 |- include ‘conf.php’ ;
session_start(); //existing statement
 . . .
if ($confirm==” ” ) {

}else if( $confirm== ”yes” ) {
  dbConnect () ; // existing statement
  if ( !verifyuser ( ) ) // [FixMeUp repair]
  {
     header('Location: ./login.php');//[FixMeUp repair]
     exit; // [FixMeUp repair]
  }
  $sql = ”DELETE FROM blogdata WHERE postid = $postid”;
  $query = mysql_query( $sql ) or die( "Cannot query the database .<br>” .
mysql_error() );
 .....
}
```

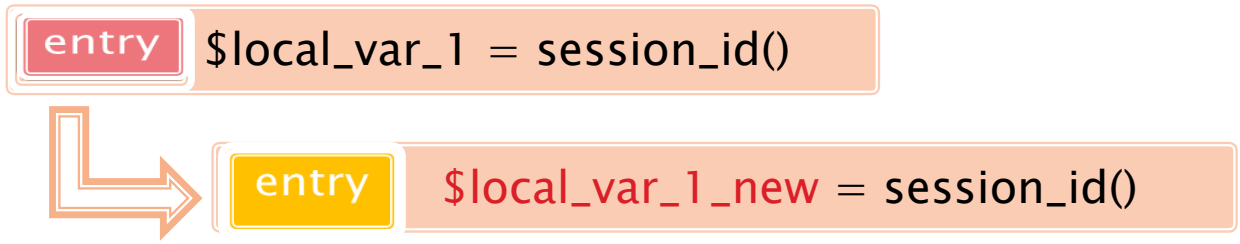
Limitations

- Environmental data dependencies, eval
- Unwanted side effects

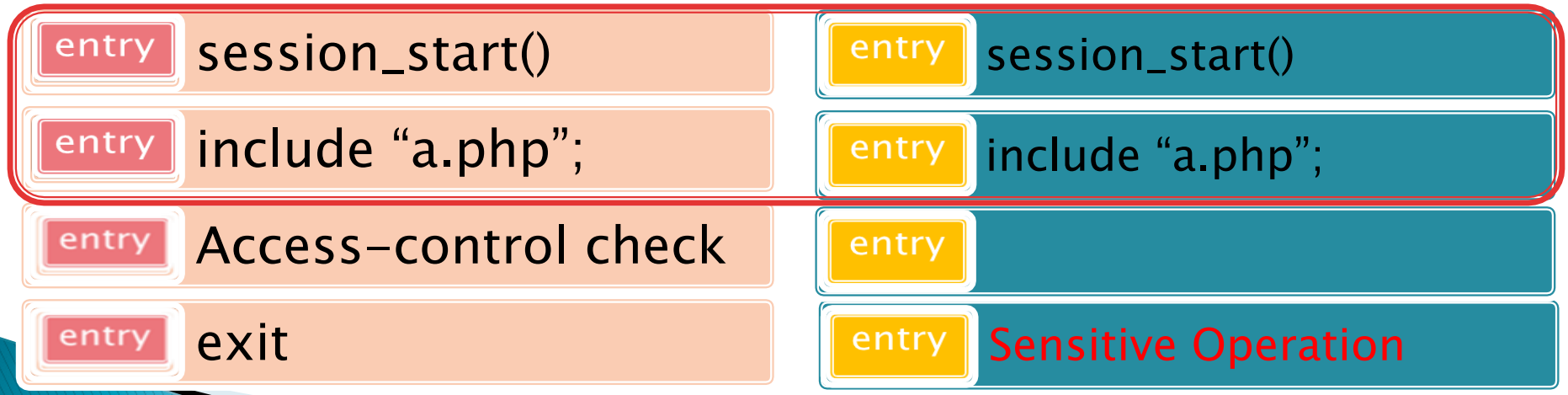


Avoiding unwanted side effects

- Use fresh variable names

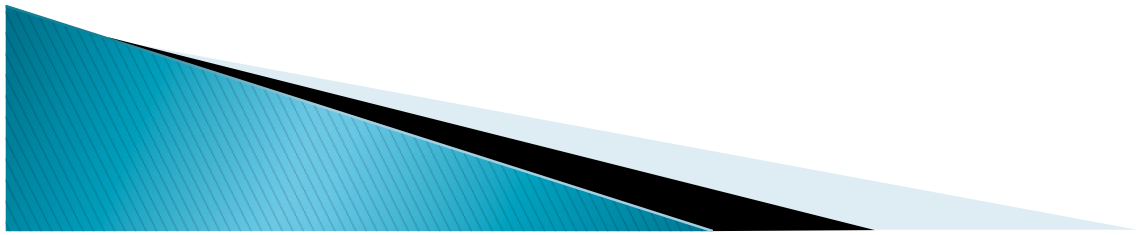


- Do not replicate already existing statements



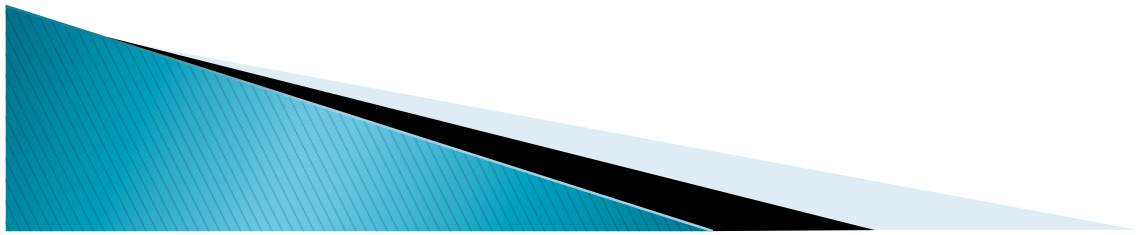
Related work

- Static detection of access-control bugs
- Dynamic detection of access-control bugs
- Dynamic repair of software bugs



Conclusion

- FixMeUp computes code templates for access-control logic from examples
- Finds and repairs access-control bugs in PHP applications
  - Reuses existing statements
  - Avoids introducing unwanted dependences
- Successfully repaired 30 access-control bugs in 10 real-world PHP applications



Q & A

Thank you