Raccoon: Automated Verification of Guarded Race Conditions in Web Applications

Simon Koch
Institute for Application Security (TU Braunschweig)
Braunschweig, Germay
simon.koch@tu-braunschweig.de

Tim Sauer
Institute for Application Security (TU Braunschweig)
Braunschweig, Germay
tim.sauer@tu-braunschweig.de

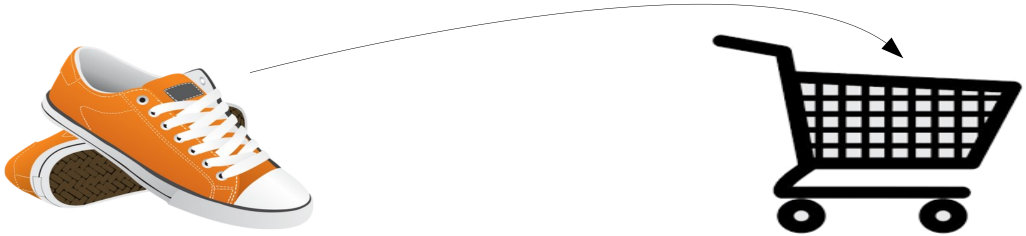
Martin Johns
Institute for Application Security (TU Braunschweig)
Braunschweig, Germay
m.johns@tu-braunschweig.de

Giancarlo Pellegrino
CISPA Helmholtz Center for Information Security
Saarbrücken, Germay
gpellegrino@cispa.saarland

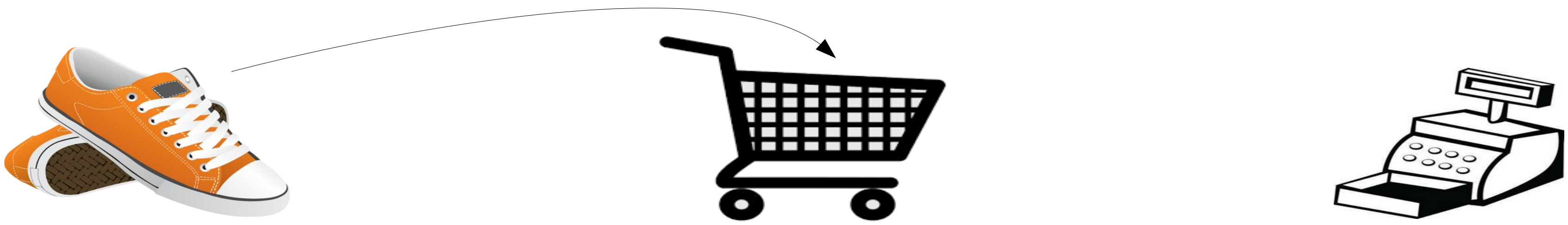
The Problem

The Problem

The Problem



The Problem

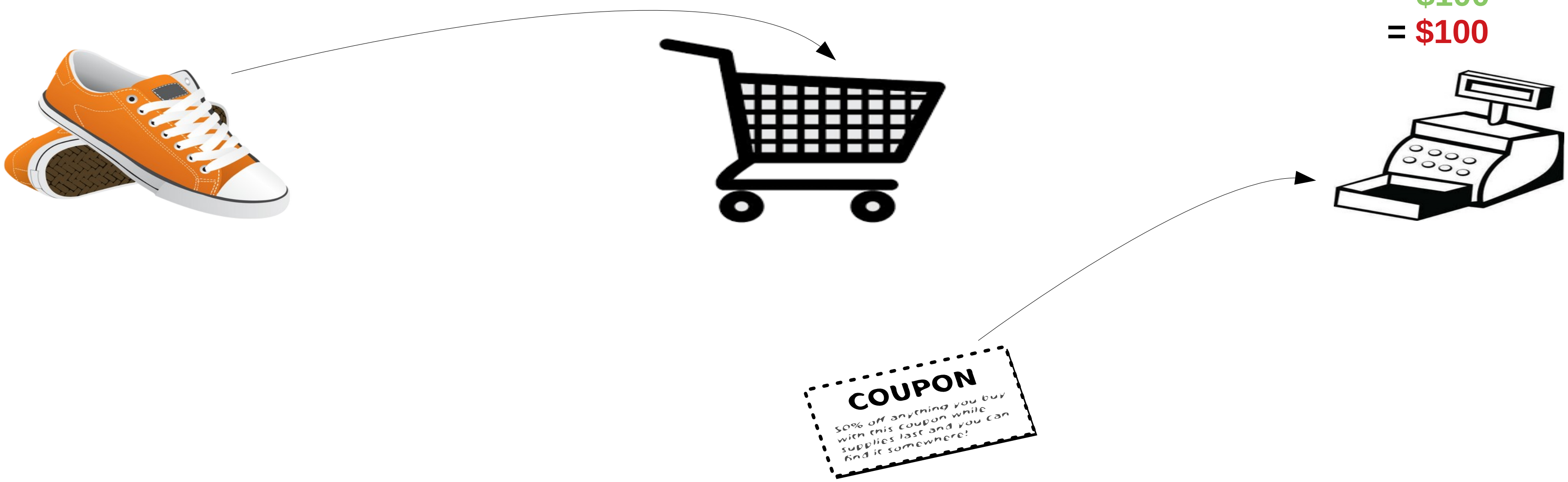


$200

The Problem

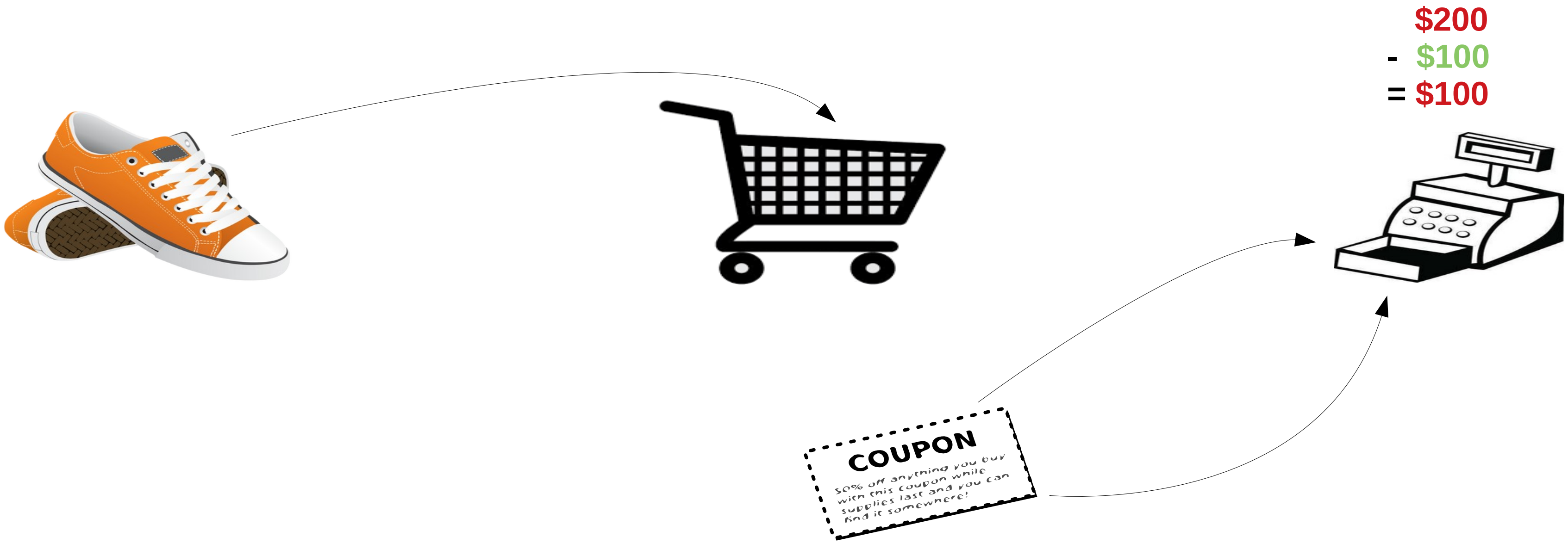
$200
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

The Problem


COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

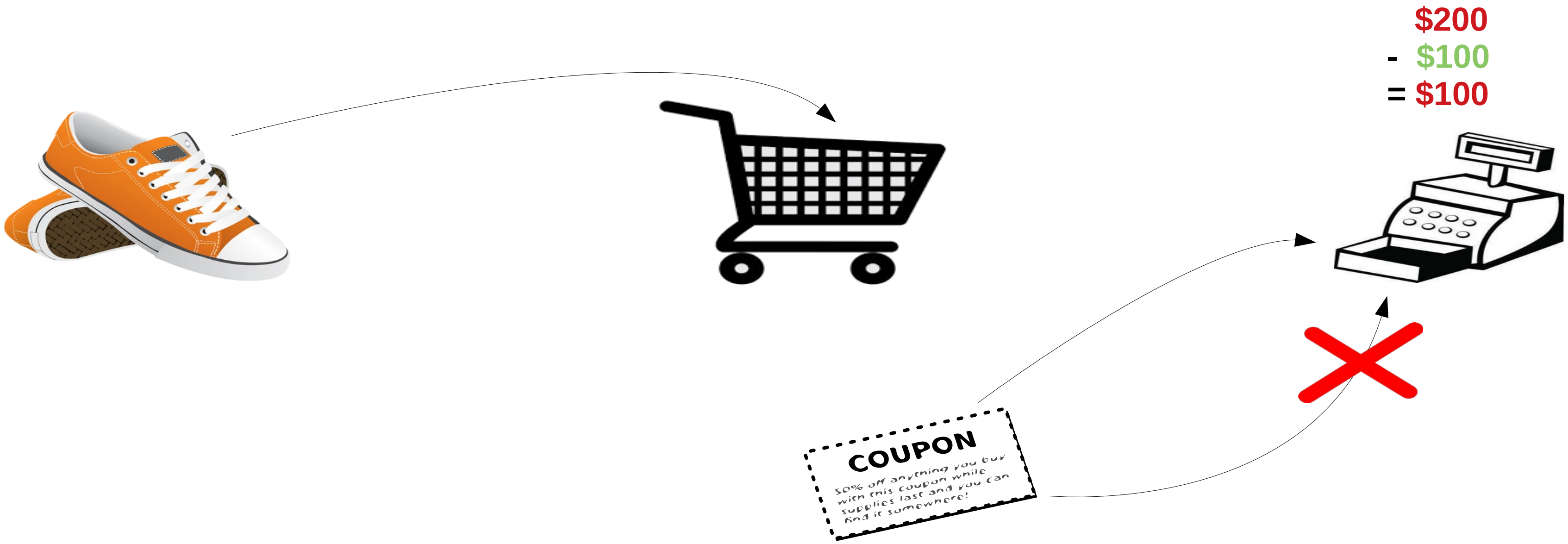
$200
- $100
= $100

The Problem


COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

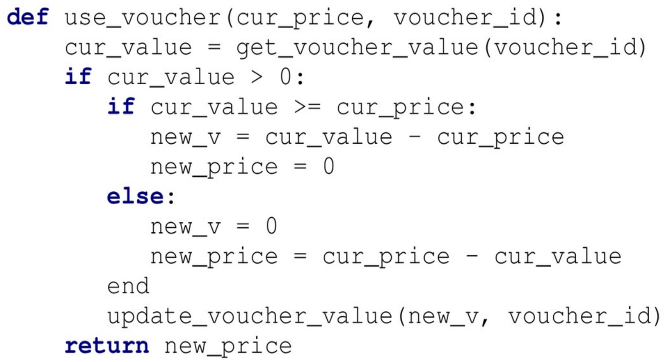
$200
- $100
= $100

The Problem



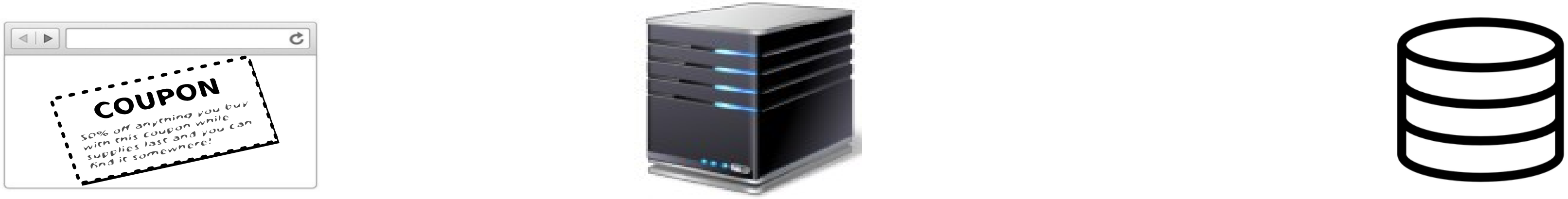
$200
- $100
= $100

COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

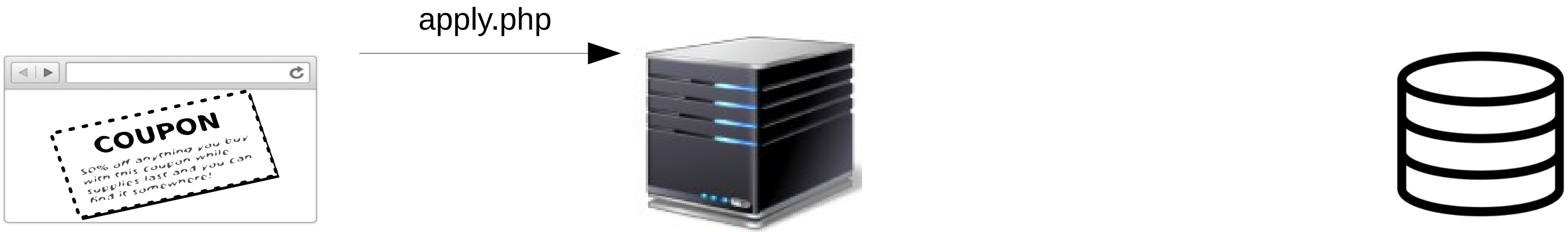


```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```

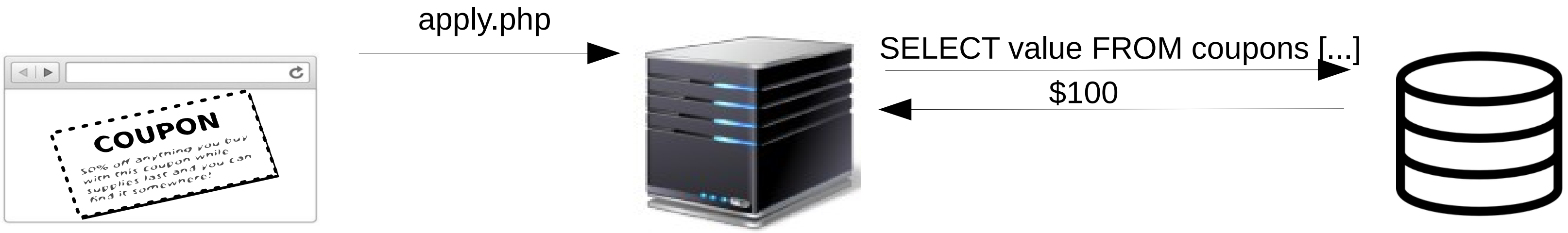
```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```


COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

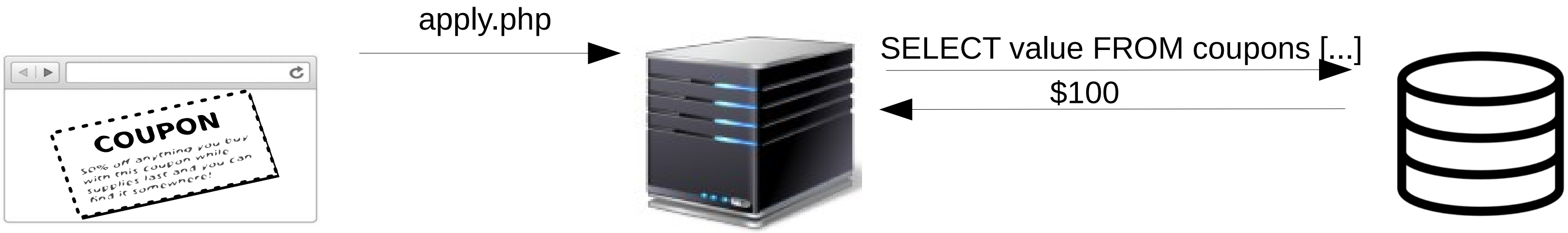
```
def use_voucher(cur_price, voucher_id):
  cur_value = get_voucher_value(voucher_id)
  if cur_value > 0:
    if cur_value >= cur_price:
      new_v = cur_value - cur_price
      new_price = 0
    else:
      new_v = 0
      new_price = cur_price - cur_value
    end
    update_voucher_value(new_v, voucher_id)
  return new_price
```


apply.php
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```


apply.php
SELECT value FROM coupons [...]
$100
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
        if cur_value >= cur_price:
            new_v = cur_value - cur_price
            new_price = 0
        else:
            new_v = 0
            new_price = cur_price - cur_value
        end
        update_voucher_value(new_v, voucher_id)
    return new_price
```

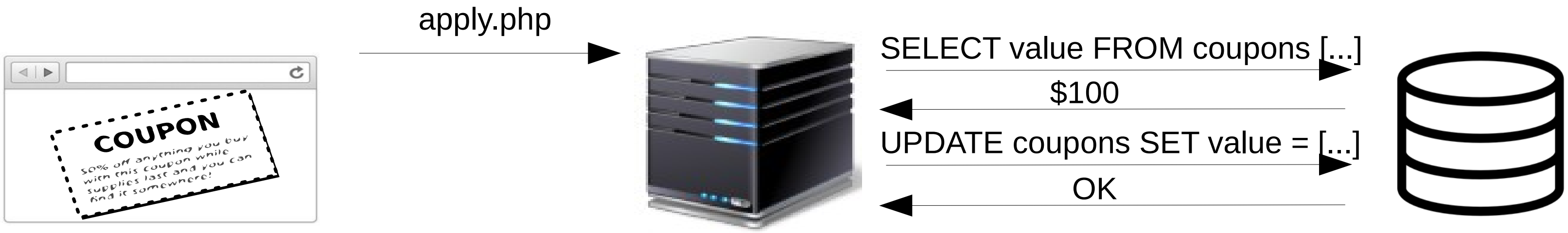

COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

apply.php

SELECT value FROM coupons [...]

$100

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```


COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

apply.php

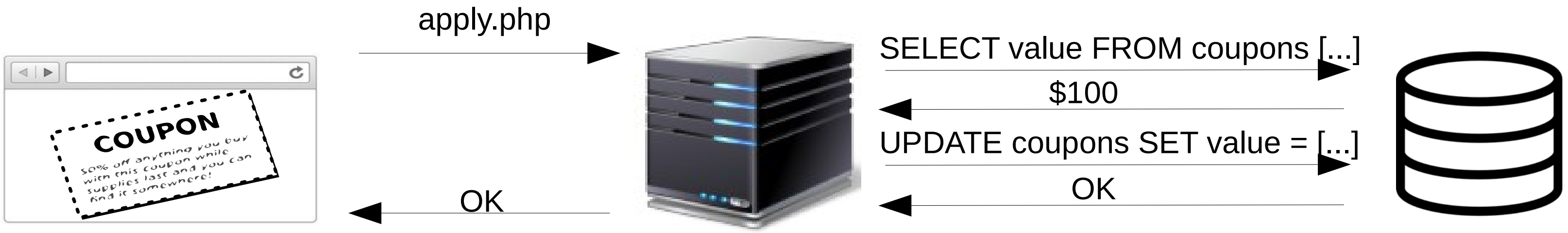
SELECT value FROM coupons [...]

$100

UPDATE coupons SET value = [...]

OK

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```


COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

apply.php

OK

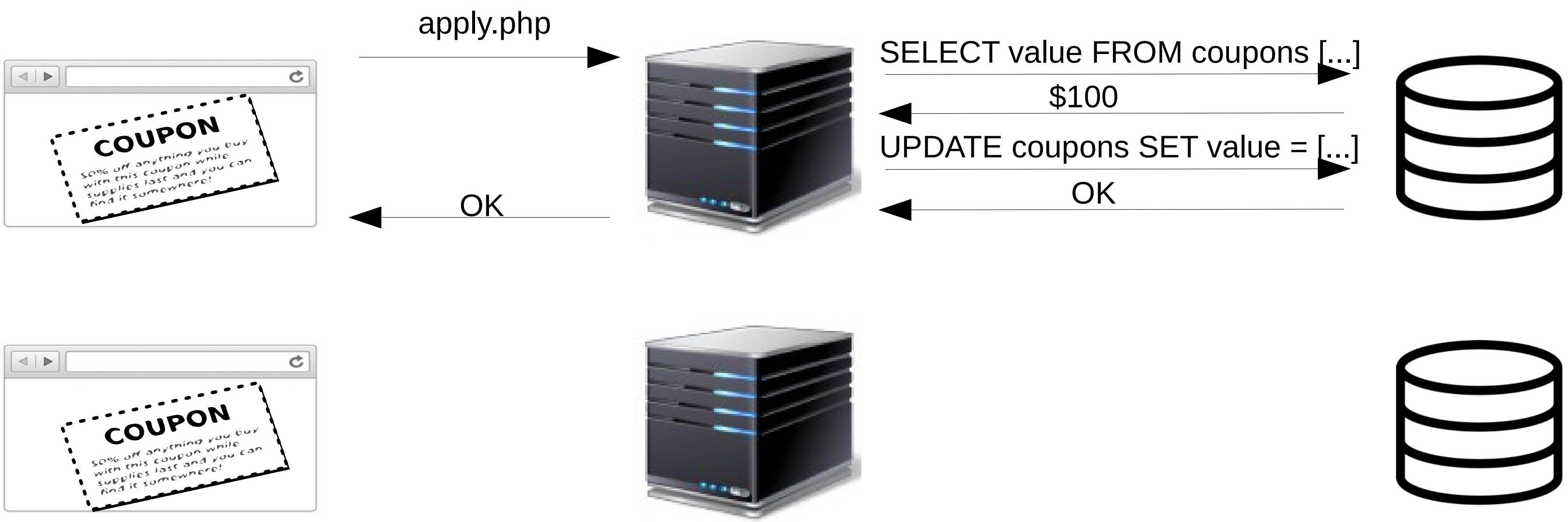
SELECT value FROM coupons [...]

$100

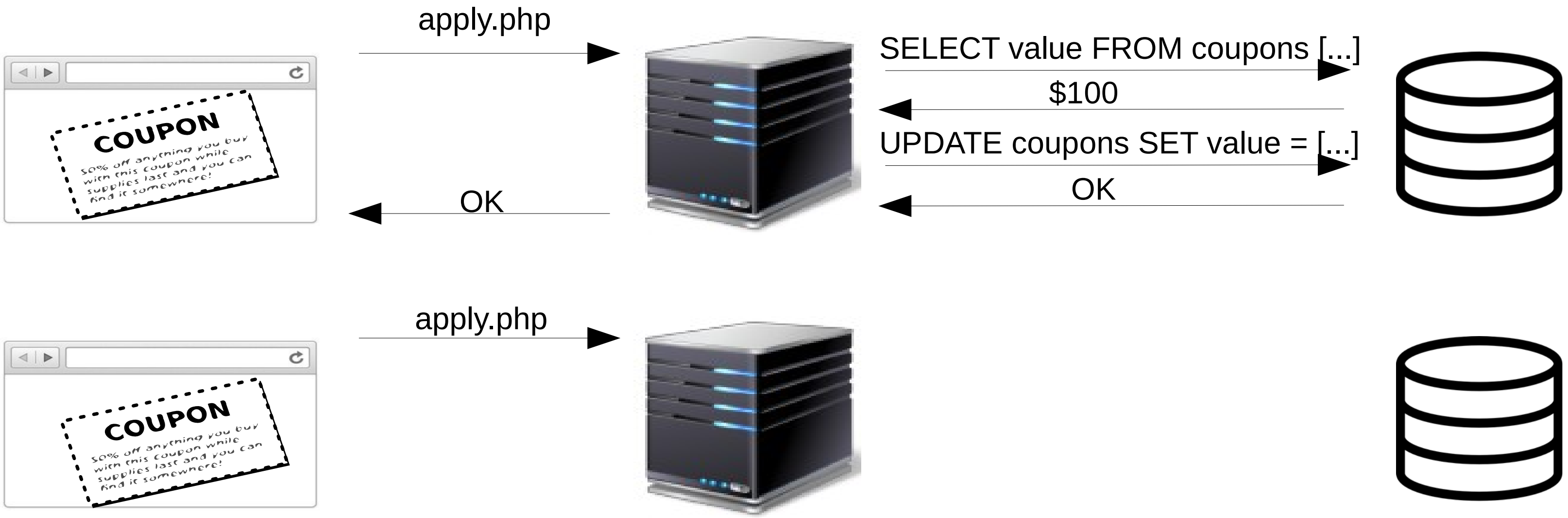
UPDATE coupons SET value = [...]

OK

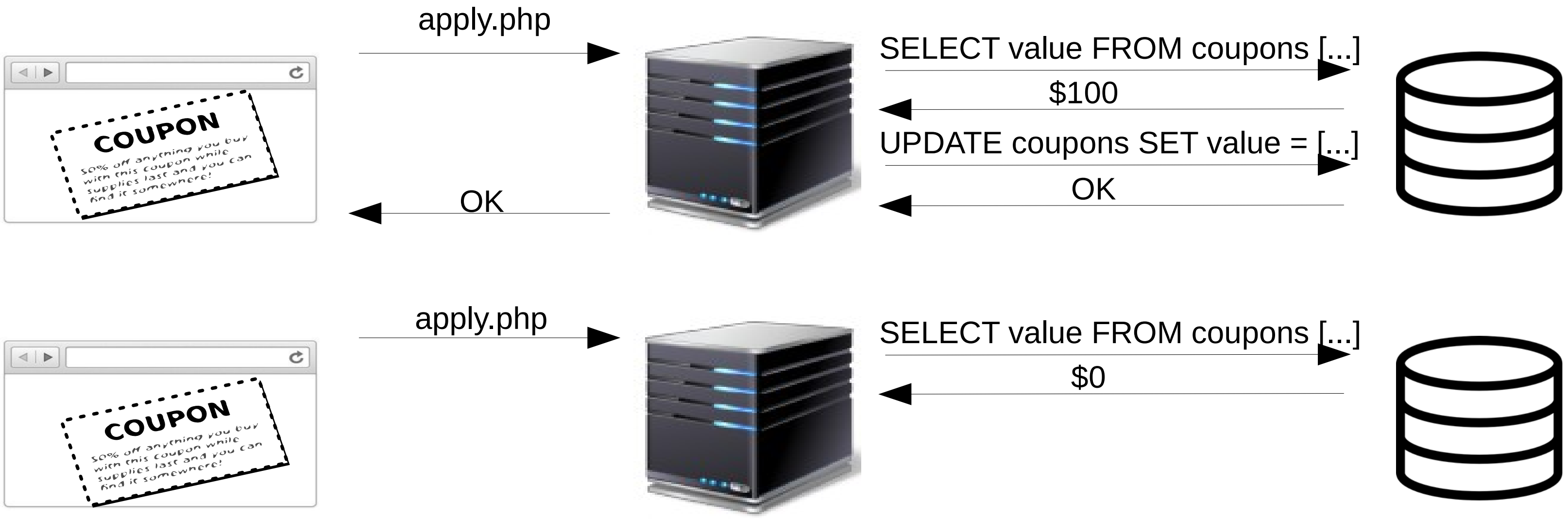
```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```


apply.php
SELECT value FROM coupons [...]
$100
UPDATE coupons SET value = [...]
OK
OK
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```


apply.php
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!
SELECT value FROM coupons [...]
$100
UPDATE coupons SET value = [...]
OK
OK
apply.php
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```


COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

apply.php

SELECT value FROM coupons [...]

$100

UPDATE coupons SET value = [...]

OK

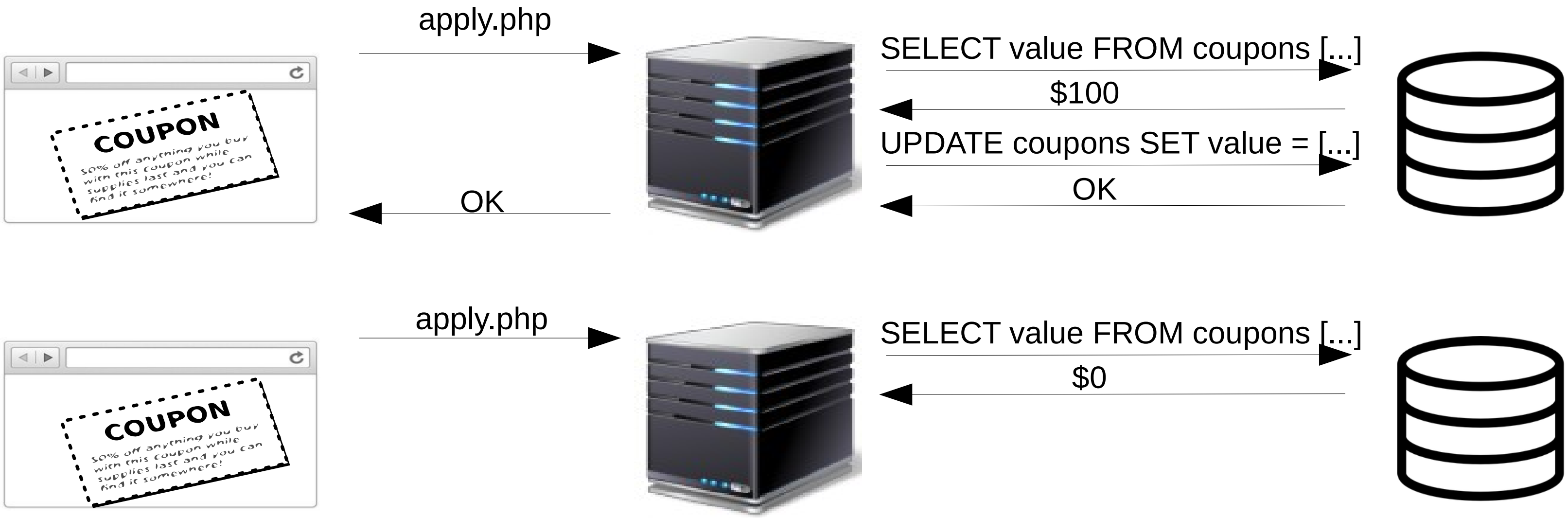
OK

apply.php

SELECT value FROM coupons [...]

$0

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```



apply.php

SELECT value FROM coupons [...]

$100

UPDATE coupons SET value = [...]

OK

OK

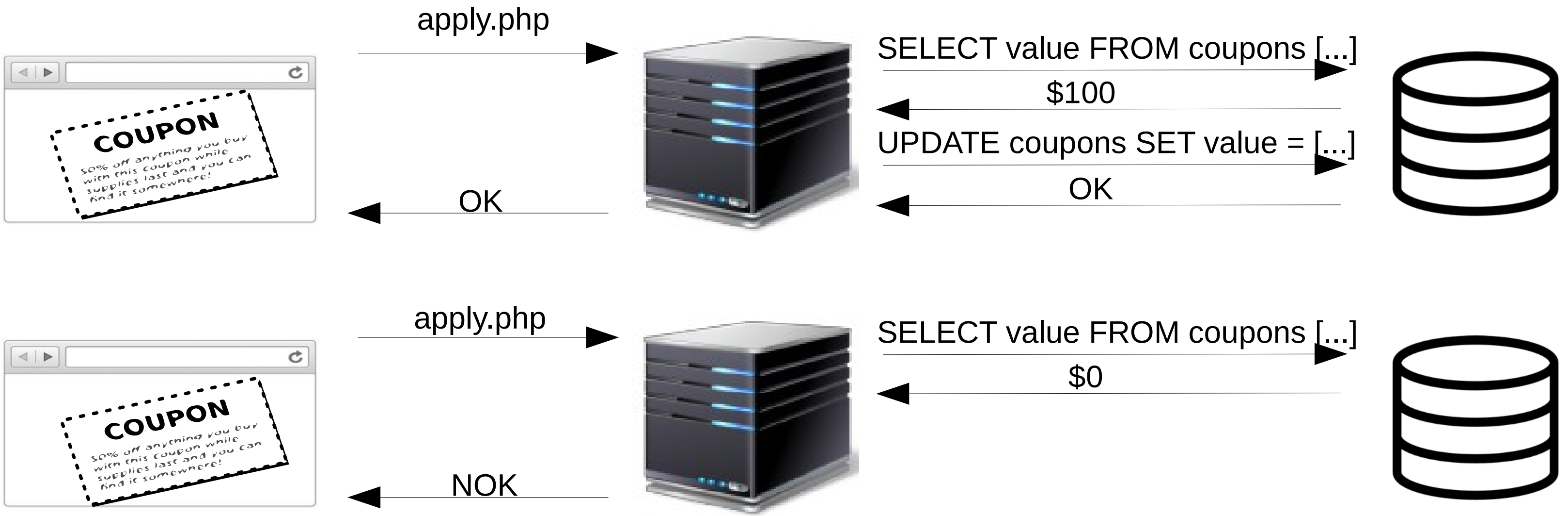
apply.php

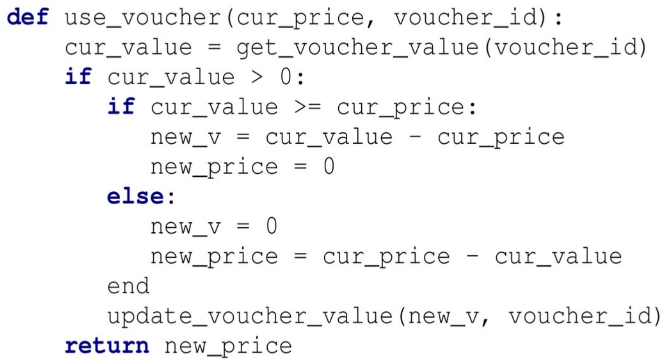
SELECT value FROM coupons [...]

$0

COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
        if cur_value >= cur_price:
            new_v = cur_value - cur_price
            new_price = 0
        else:
            new_v = 0
            new_price = cur_price - cur_value
        end
        update_voucher_value(new_v, voucher_id)
    return new_price
```


apply.php
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!
OK
SELECT value FROM coupons [...]
$100
UPDATE coupons SET value = [...]
OK
apply.php
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!
NOK
SELECT value FROM coupons [...]
$0

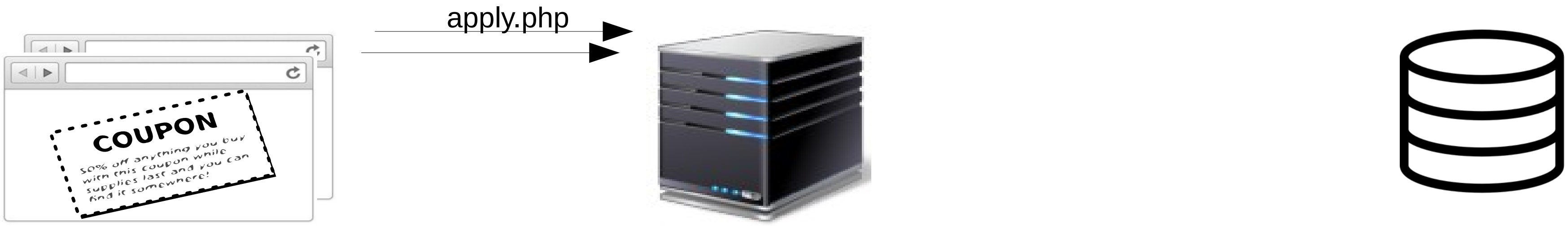


```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```

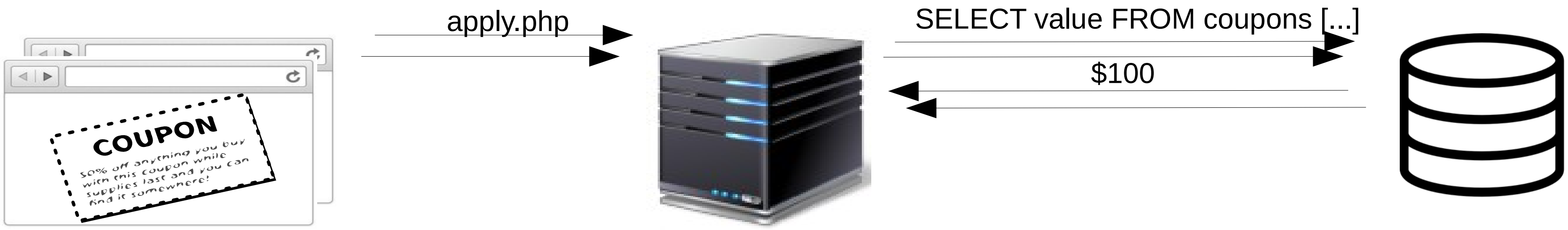
```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```

COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

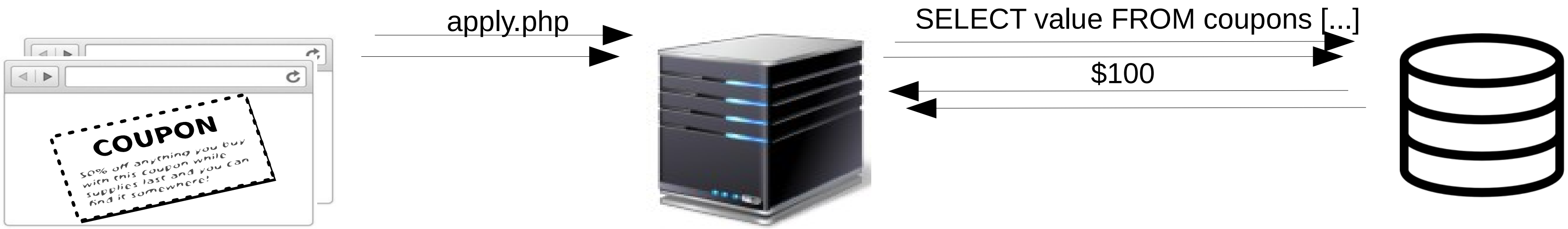
```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```


apply.php
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

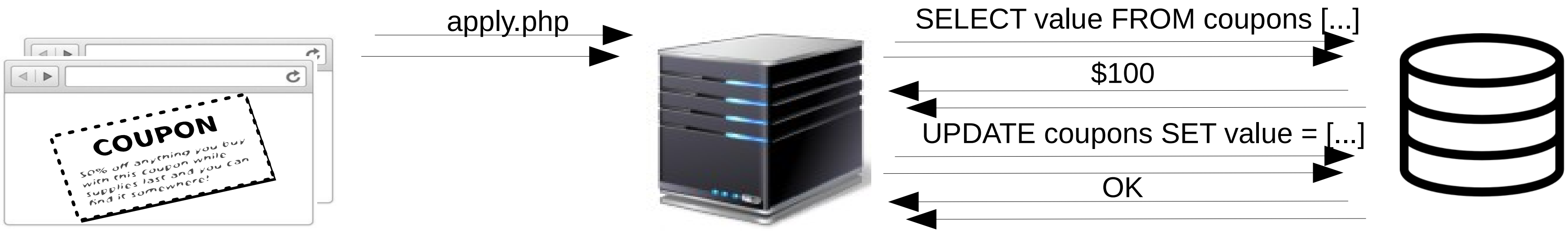
```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```


COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!
apply.php
SELECT value FROM coupons [...]
$100

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```


apply.php
SELECT value FROM coupons [...]
$100
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```



COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

apply.php

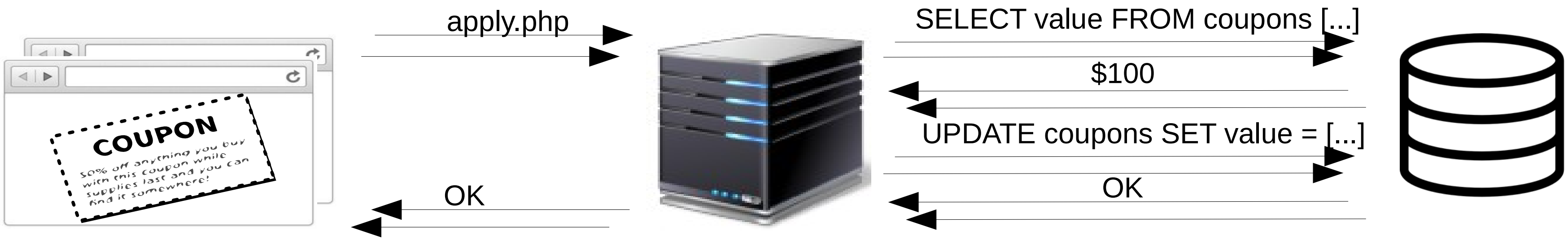
SELECT value FROM coupons [...]

$100

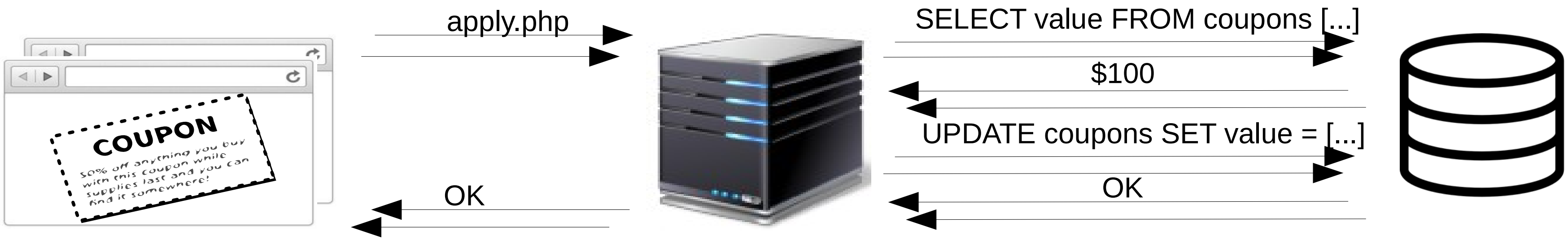
UPDATE coupons SET value = [...]

OK

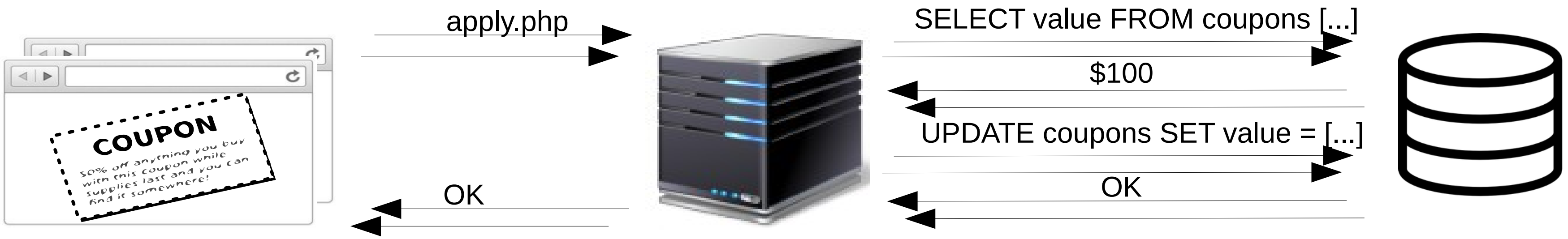
```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```


COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!
apply.php
OK
SELECT value FROM coupons [...]
$100
UPDATE coupons SET value = [...]
OK

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```


COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!
apply.php
OK
SELECT value FROM coupons [...]
$100
UPDATE coupons SET value = [...]
OK

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
       if cur_value >= cur_price:
          new_v = cur_value - cur_price
          new_price = 0
       else:
          new_v = 0
          new_price = cur_price - cur_value
       end
       update_voucher_value(new_v, voucher_id)
    return new_price
```


COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

apply.php

OK

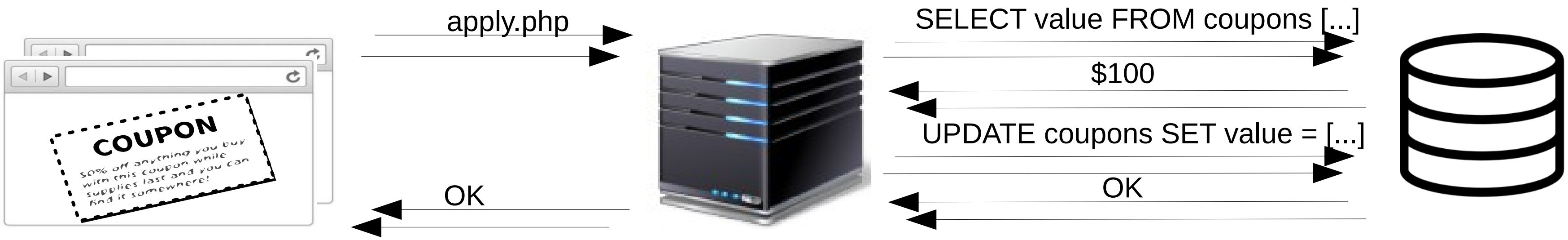
SELECT value FROM coupons [...]

$100

UPDATE coupons SET value = [...]

OK

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
        if cur_value >= cur_price:
            new_v = cur_value - cur_price
            new_price = 0
        else:
            new_v = 0
            new_price = cur_price - cur_value
        end
        update_voucher_value(new_v, voucher_id)
    return new_price
```


COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

apply.php

OK

SELECT value FROM coupons [...]

$100

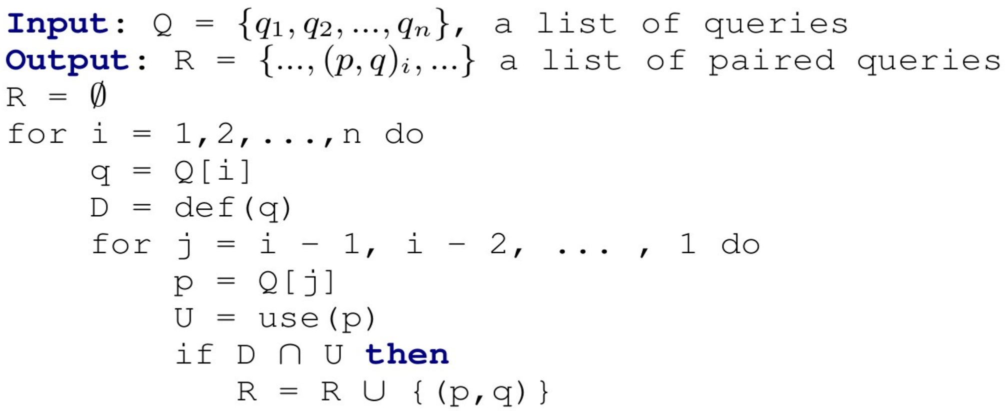
UPDATE coupons SET value = [...]

OK

(2008) Paleari et al.

R. Paleari, D. Marrone, D. Bruschi, and M. Monga, “On race vulnerabilities in web applications,” in Detection of Intrusions and Malware, and Vulnerability Assessment: 5th International Conference, DIMVA 2008, https://doi.org/10.1007/978-3-540-70542-0_7

(2008) Paleari et al.

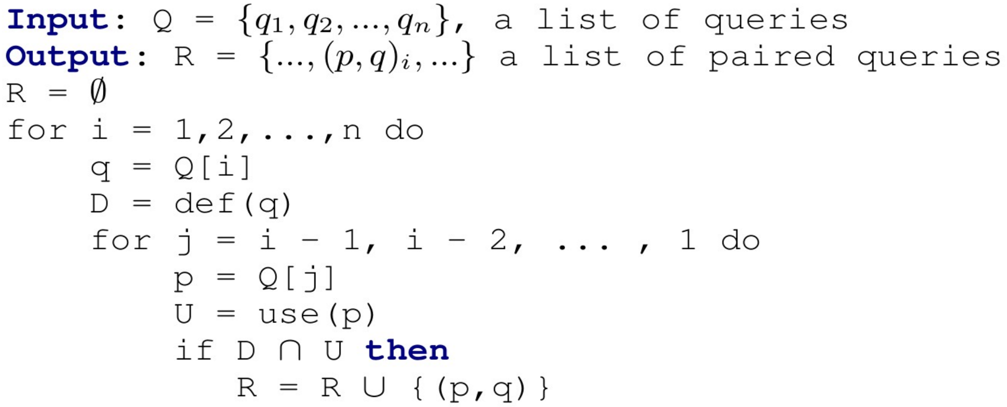


```
Input: Q = $\{q_1, q_2, ..., q_n\}$, a list of queries
Output: R = $\{..., (p, q)_i, ...\}$ a list of paired queries
R = $\emptyset$
for i = 1,2,...,n do
    q = Q[i]
    D = def(q)
    for j = i − 1, i − 2, ... , 1 do
        p = Q[j]
        U = use(p)
        if D ∩ U then
           R = R ∪ {(p,q)}
```

R. Paleari, D. Marrone, D. Bruschi, and M. Monga, “On race vulnerabilities in web applications,” in Detection of Intrusions and Malware, and Vulnerability Assessment: 5th International Conference, DIMVA 2008, https://doi.org/10.1007/978-3-540-70542-0_7

(2008) Paleari et al.

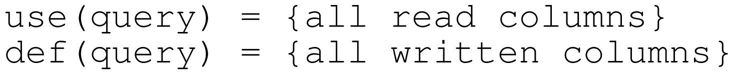
```
use(query) = {all read columns}
def(query) = {all written columns}
```



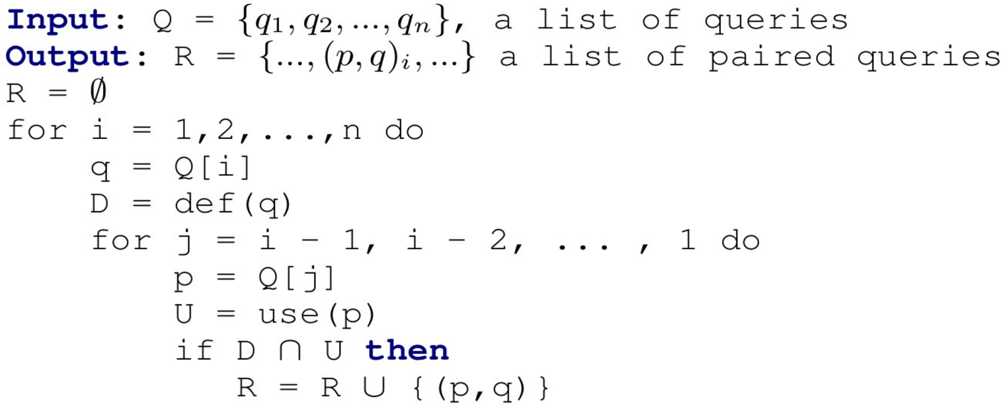
```
Input: Q = $\{q_1, q_2, ..., q_n\}$, a list of queries
Output: R = $\{..., (p, q)_i, ...\}$ a list of paired queries
R = $\emptyset$
for i = 1,2,...,n do
    q = Q[i]
    D = def(q)
    for j = i - 1, i - 2, ... , 1 do
        p = Q[j]
        U = use(p)
        if D ∩ U then
           R = R ∪ {(p,q)}
```

R. Paleari, D. Marrone, D. Bruschi, and M. Monga, “On race vulnerabilities in web applications,” in Detection of Intrusions and Malware, and Vulnerability Assessment: 5th International Conference, DIMVA 2008, https://doi.org/10.1007/978-3-540-70542-0_7

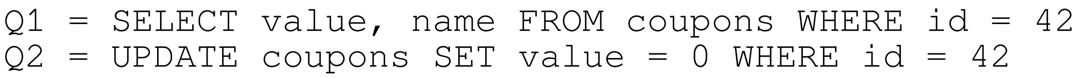
(2008) Paleari et al.



```
use(query) = {all read columns}
def(query) = {all written columns}
```



```
Input: Q = $\{q_1, q_2, ..., q_n\}$, a list of queries
Output: R = $\{..., (p,q)_i, ...\}$ a list of paired queries
R = $\emptyset$
for i = 1,2,...,n do
    q = Q[i]
    D = def(q)
    for j = i - 1, i - 2, ... , 1 do
        p = Q[j]
        U = use(p)
        if D ∩ U then
            R = R ∪ {(p,q)}
```

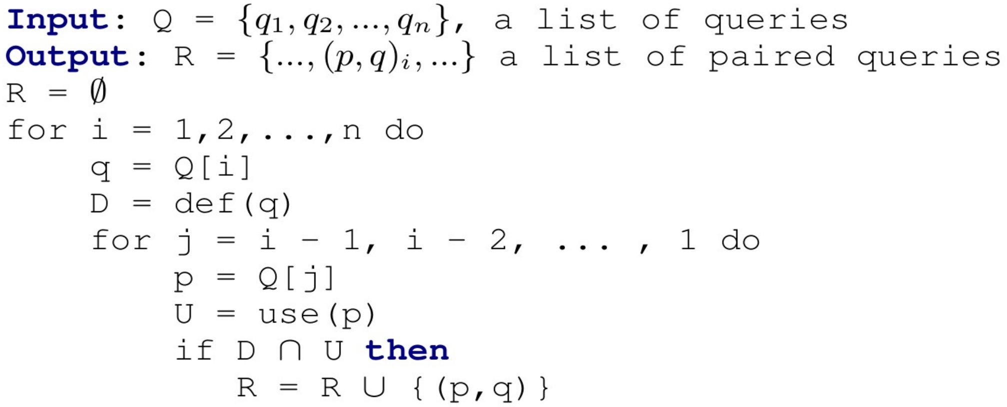


```
Q1 = SELECT value, name FROM coupons WHERE id = 42
Q2 = UPDATE coupons SET value = 0 WHERE id = 42
```

R. Paleari, D. Marrone, D. Bruschi, and M. Monga, “On race vulnerabilities in web applications,” in Detection of Intrusions and Malware, and Vulnerability Assessment: 5th International Conference, DIMVA 2008, https://doi.org/10.1007/978-3-540-70542-0_7

(2008) Paleari et al.

```
use(query) = {all read columns}
def(query) = {all written columns}
```



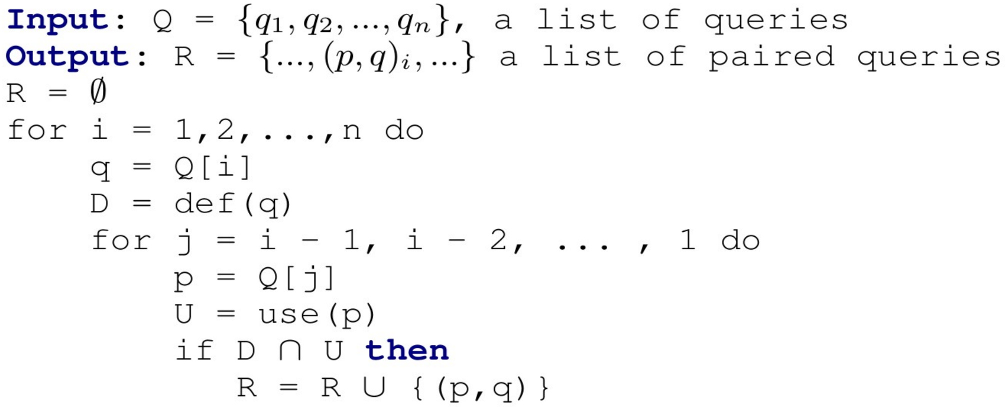
```
Input: Q = $\{q_1, q_2, ..., q_n\}$, a list of queries
Output: R = $\{..., (p, q)_i, ...\}$ a list of paired queries
R = $\emptyset$
for i = 1,2,...,n do
    q = Q[i]
    D = def(q)
    for j = i - 1, i - 2, ... , 1 do
        p = Q[j]
        U = use(p)
        if D ∩ U then
           R = R ∪ {(p,q)}
```

```
Q1 = SELECT value, name FROM coupons WHERE id = 42
Q2 = UPDATE coupons SET value = 0 WHERE id = 42

use(Q1) = {coupon.value, coupon.name}
def(Q2) = {coupon.value}
```

R. Paleari, D. Marrone, D. Bruschi, and M. Monga, “On race vulnerabilities in web applications,” in Detection of Intrusions and Malware, and Vulnerability Assessment: 5th International Conference, DIMVA 2008, https://doi.org/10.1007/978-3-540-70542-0_7

(2008) Paleari et al.

```
use(query) = {all read columns}
def(query) = {all written columns}
```



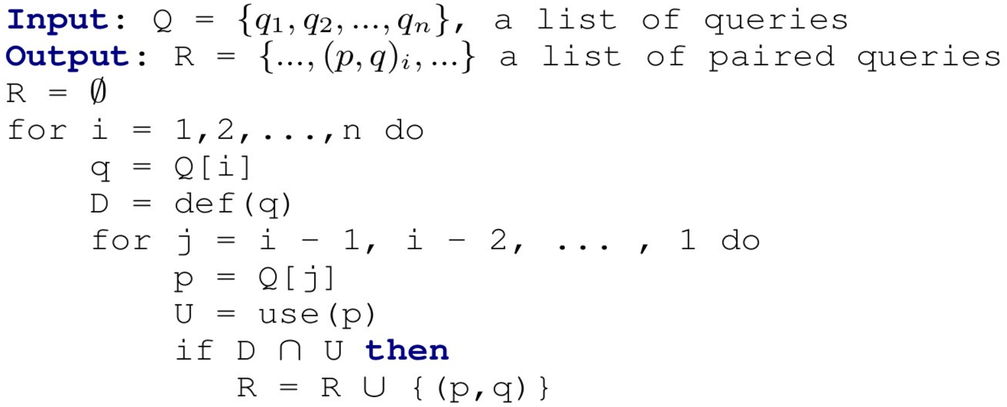
```
Input: Q = $\{q_1, q_2, ..., q_n\}$, a list of queries
Output: R = $\{..., (p, q)_i, ...\}$ a list of paired queries
R = $\emptyset$
for i = 1,2,...,n do
    q = Q[i]
    D = def(q)
    for j = i - 1, i - 2, ... , 1 do
        p = Q[j]
        U = use(p)
        if D ∩ U then
           R = R ∪ {(p,q)}
```

```
Q1 = SELECT value, name FROM coupons WHERE id = 42
Q2 = UPDATE coupons SET value = 0 WHERE id = 42

use(Q1) = {coupon.value, coupon.name}
def(Q2) = {coupon.value}

use(Q1) ∩ def(Q2) = {coupon.value}
```

R. Paleari, D. Marrone, D. Bruschi, and M. Monga, “On race vulnerabilities in web applications,” in Detection of Intrusions and Malware, and Vulnerability Assessment: 5th International Conference, DIMVA 2008, https://doi.org/10.1007/978-3-540-70542-0_7

(2008) Paleari et al.

```
use(query) = {all read columns}
def(query) = {all written columns}
```



```
Input: Q = $\{q_1, q_2, ..., q_n\}$, a list of queries
Output: R = $\{..., (p,q)_i, ...\}$ a list of paired queries
R = $\emptyset$
for i = 1,2,...,n do
    q = Q[i]
    D = def(q)
    for j = i - 1, i - 2, ... , 1 do
        p = Q[j]
        U = use(p)
        if D ∩ U then
            R = R ∪ {(p,q)}
```

```
Q1 = SELECT value, name FROM coupons WHERE id = 42
Q2 = UPDATE coupons SET value = 0 WHERE id = 42

use(Q1) = {coupon.value, coupon.name}
def(Q2) = {coupon.value}

use(Q1) ∩ def(Q2) = {coupon.value}
   (intersection → interdependence)
```

R. Paleari, D. Marrone, D. Bruschi, and M. Monga, “On race vulnerabilities in web applications,” in Detection of Intrusions and Malware, and Vulnerability Assessment: 5th International Conference, DIMVA 2008, https://doi.org/10.1007/978-3-540-70542-0_7

State of the Art

State of the Art

✓

State of the Art

✓

✓

State of the Art

- Automatic gathering data ✗
- Model understanding of the issue ✓
- Using the model to find vulnerabilities ✓

State of the Art

- Automatic gathering data ✗
- Model understanding of the issue ✓
- Using the model to find vulnerabilities ✓
- Automatic testing of vulnerabilities ✗

State of the Art

- Automatic gathering data ✗
- Model understanding of the issue ✓
- Using the model to find vulnerabilities ✓
- Automatic testing of vulnerabilities ✗
- Automatic validation of tests ✗

Our Goals

- Automatic gathering data ✗
- Model understanding of the issue ✓
- Using the model to find vulnerabilities ✓
- Automatic testing of vulnerabilities ✗
- Automatic validation of tests ✗

Our Goals

- Automatic gathering data ✓
- Model understanding of the issue ✓
- Using the model to find vulnerabilities ✓
- Automatic testing of vulnerabilities ✗
- Automatic validation of tests ✗

Our Goals

- Automatic gathering data ✓
- Model understanding of the issue ✓
- Using the model to find vulnerabilities ✓
- Automatic testing of vulnerabilities ✓
- Automatic validation of tests ✗

Our Goals

- Automatic gathering data ✓
- Model understanding of the issue ✓
- Using the model to find vulnerabilities ✓
- Automatic testing of vulnerabilities ✓
- Automatic validation of tests ✓

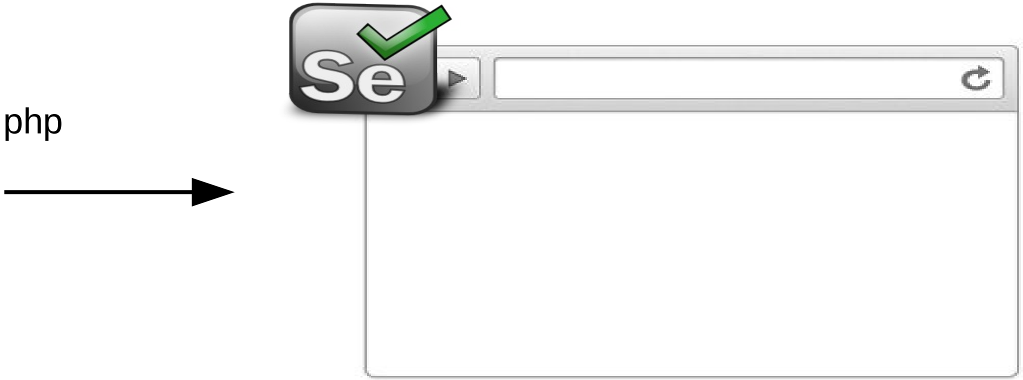
A Simple Use Case

A Simple Use Case

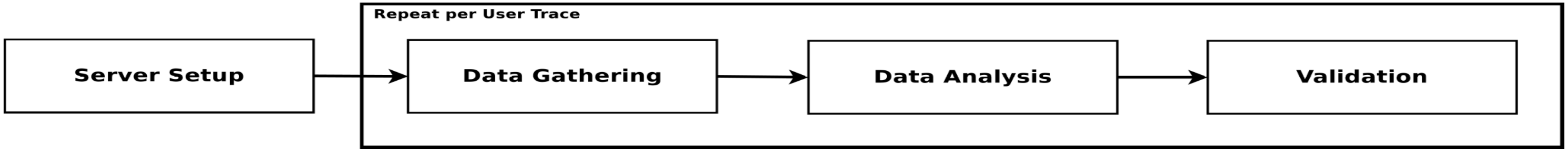
A Simple Use Case

1. open url http://www.shop.com/use_coupon.php
2. click on button ‘coupon’
3. click on field id=‘coupon_id’
4. click on button id=’submit’

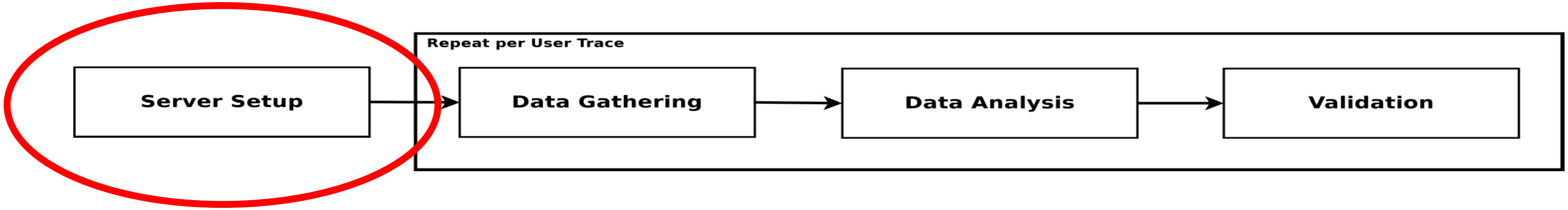
(user trace)



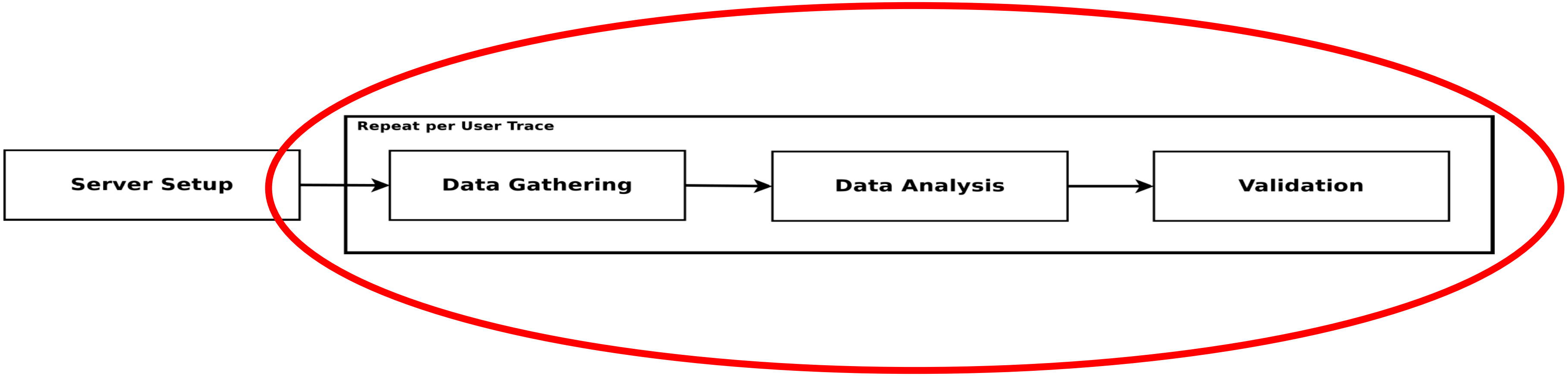
Testing and Validation Pipeline



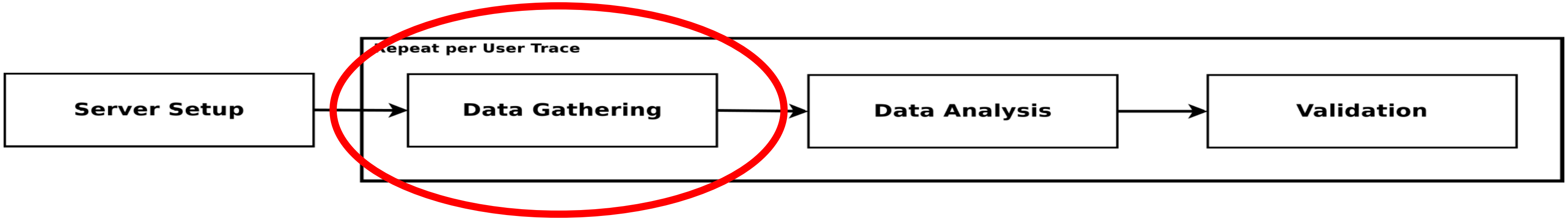
Testing and Validation Pipeline



Testing and Validation Pipeline



Testing and Validation Pipeline



Repeat per User Trace

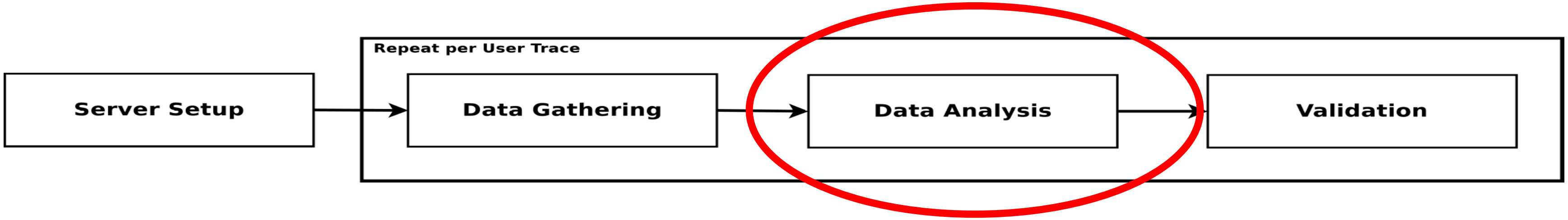
Server Setup

Data Gathering

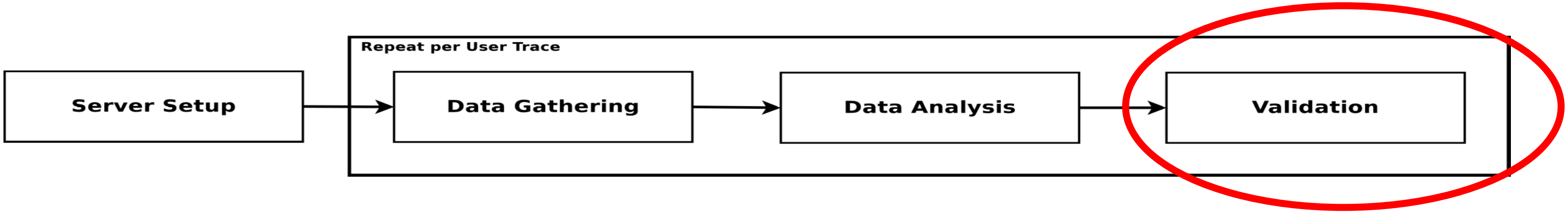
Data Analysis

Validation

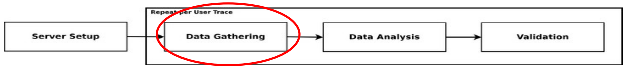
Testing and Validation Pipeline



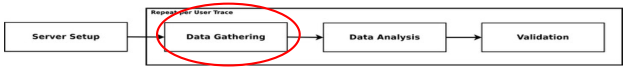
Testing and Validation Pipeline

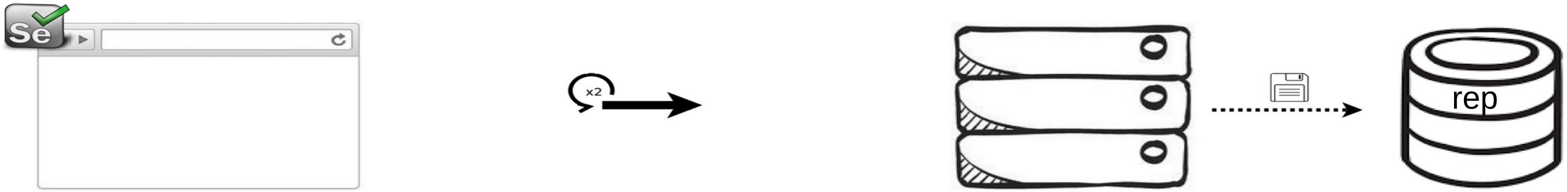


Data Gathering



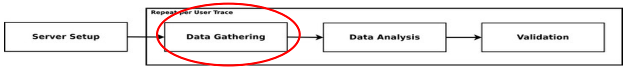
Data Gathering

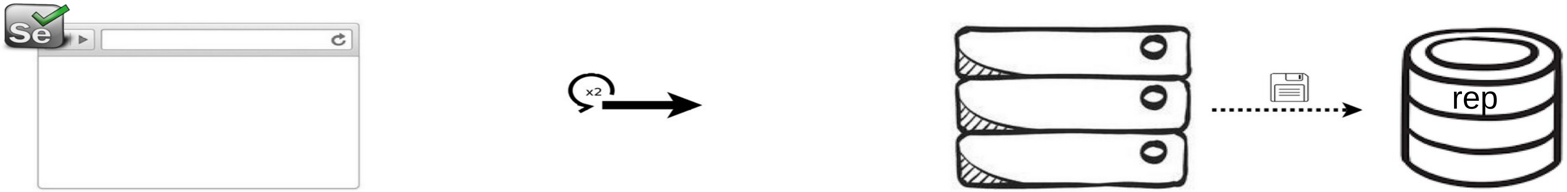




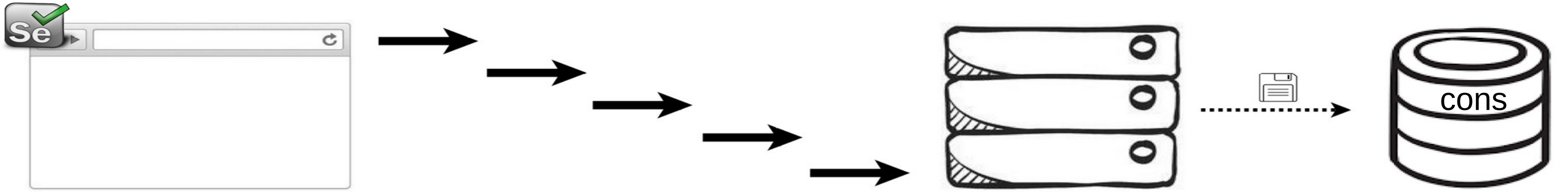
Repeated User Trace Execution (x2)

Data Gathering





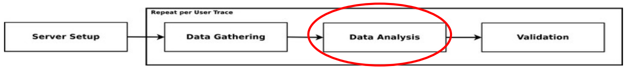
Repeated User Trace Execution (x2)



Consecutive User Trace Execution

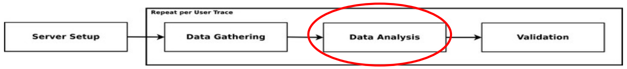
Data Analysis

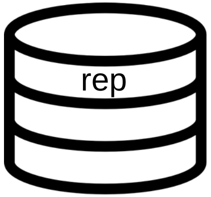
(noisy URL Parameters)



Data Analysis

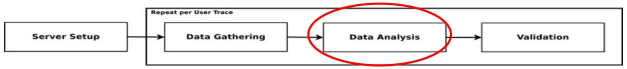
(noisy URL Parameters)

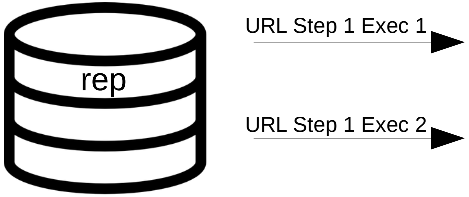




Data Analysis

(noisy URL Parameters)



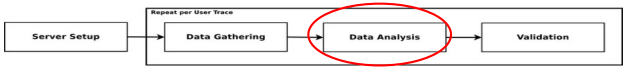


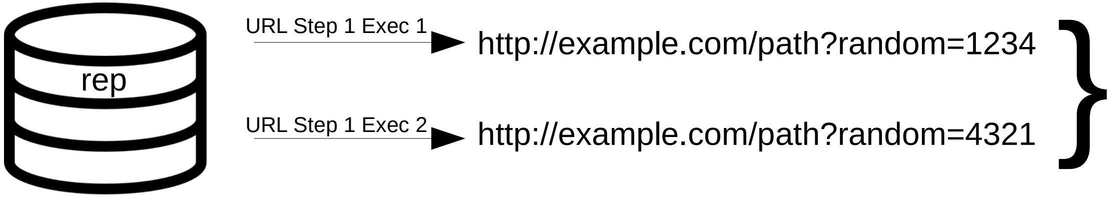
http://example.com/path?random=1234

http://example.com/path?random=4321

Data Analysis

(noisy URL Parameters)





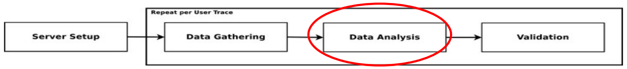
URL Step 1 Exec 1 → http://example.com/path?random=1234

URL Step 1 Exec 2 → http://example.com/path?random=4321

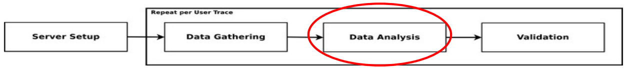
URL Step 1: http://example.com/path?random=<rnd>

Data Analysis

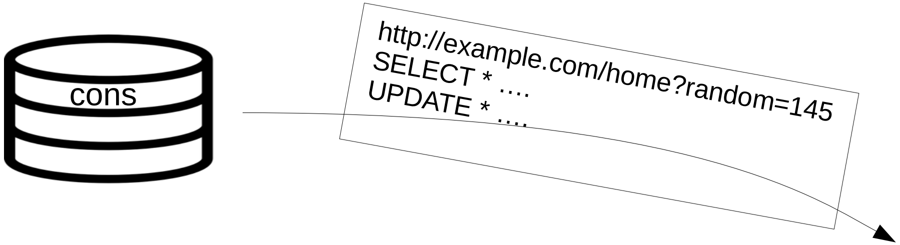
(Bucketing)



Data Analysis

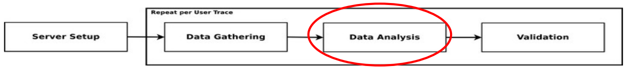


(Bucketing)

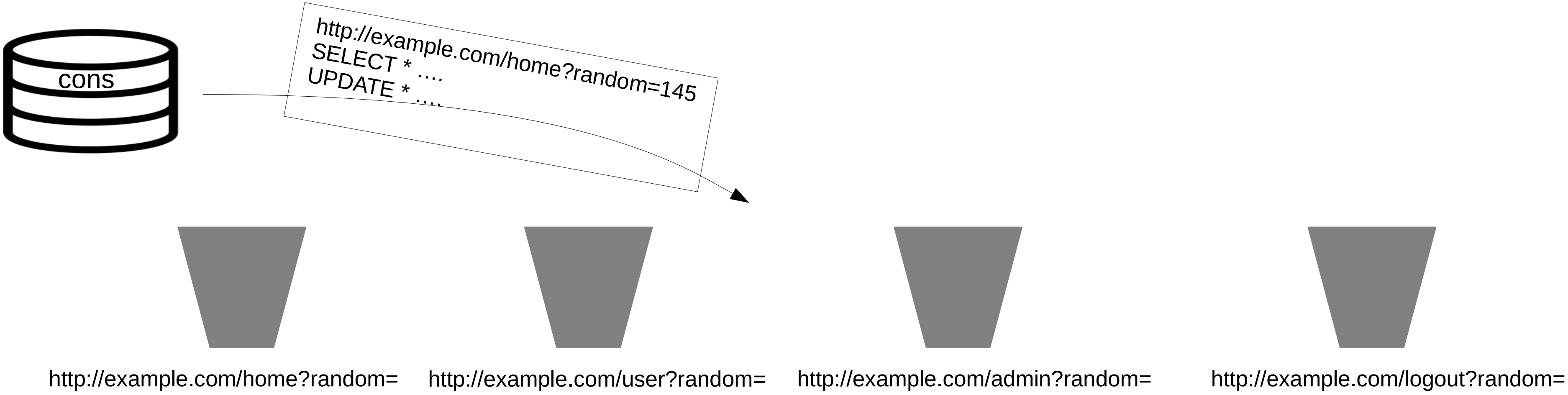


http://example.com/home?random=145
SELECT * ….
UPDATE * ….

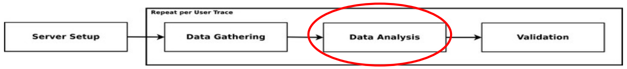
Data Analysis



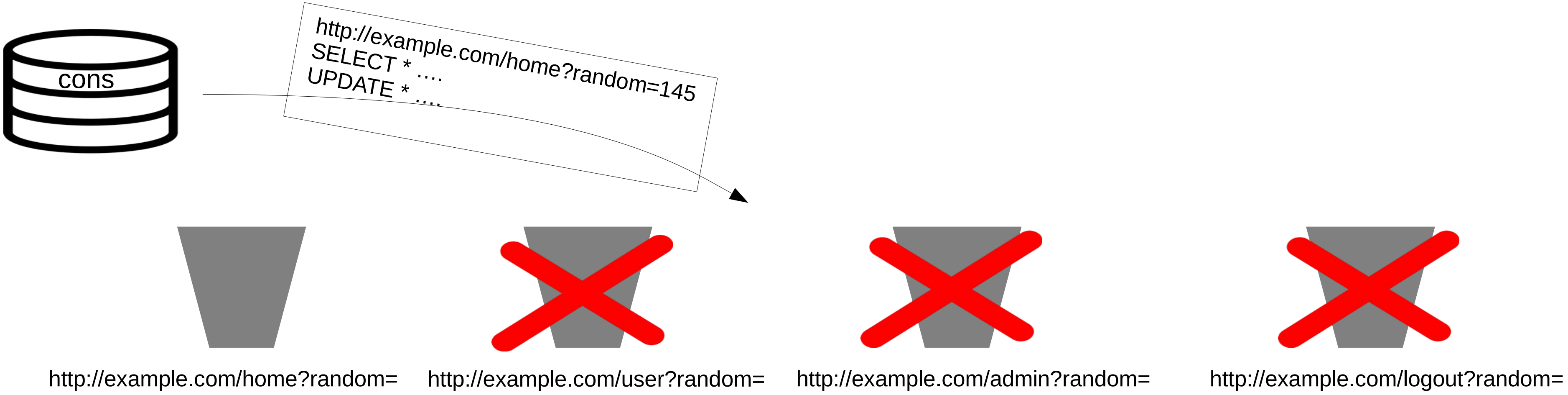
(Bucketing)


cons
http://example.com/home?random=145
SELECT * ….
UPDATE * ….
http://example.com/home?random=
http://example.com/user?random=
http://example.com/admin?random=
http://example.com/logout?random=

Data Analysis



(Bucketing)



http://example.com/home?random=145
SELECT * ....
UPDATE * ....

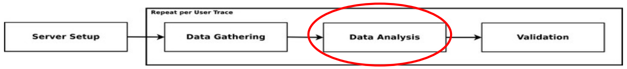
http://example.com/home?random=

http://example.com/user?random=

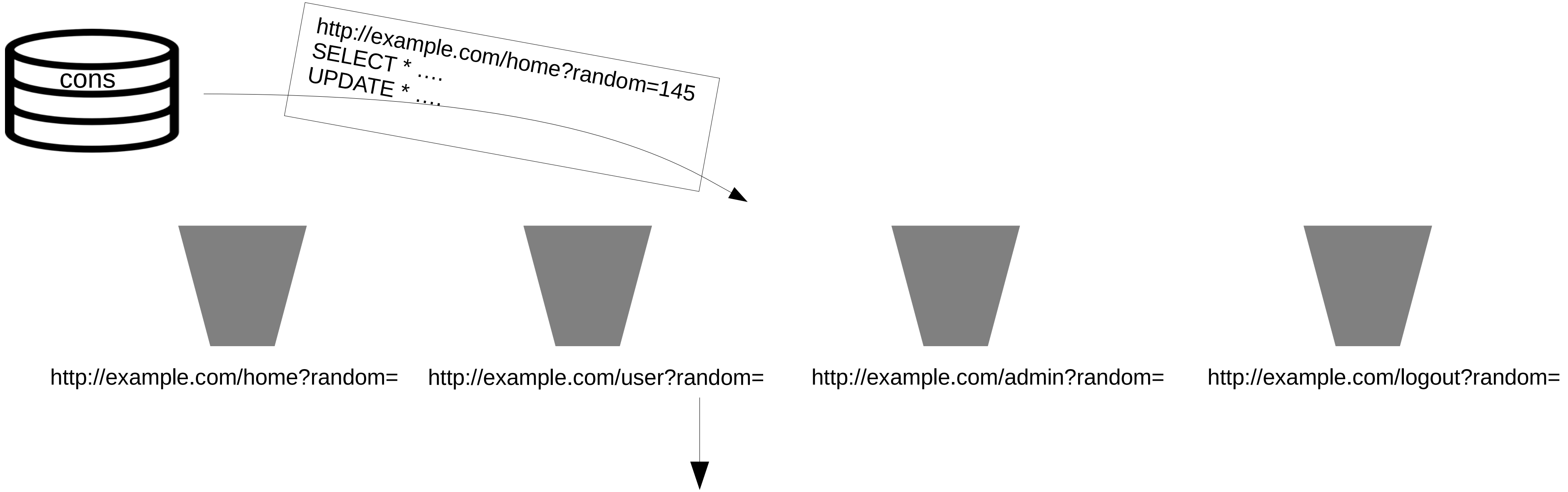
http://example.com/admin?random=

http://example.com/logout?random=

Data Analysis



(counting writing queries)



cons

http://example.com/home?random=145
SELECT * ….
UPDATE * ….

http://example.com/home?random=

http://example.com/user?random=

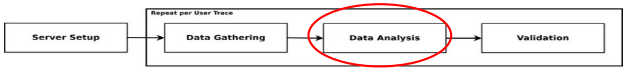
http://example.com/admin?random=

http://example.com/logout?random=

COUNT writing_query IN bucket

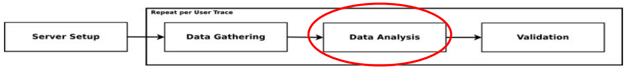
Data Analysis

(Interdependent Query Pairs)



Data Analysis

(Interdependent Query Pairs)



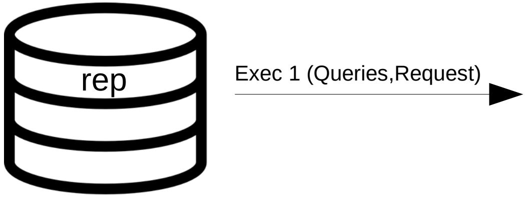
Repeat per User Trace

Server Setup

Data Gathering

Data Analysis

Validation

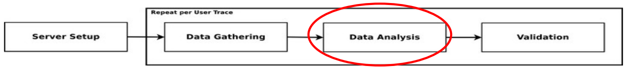


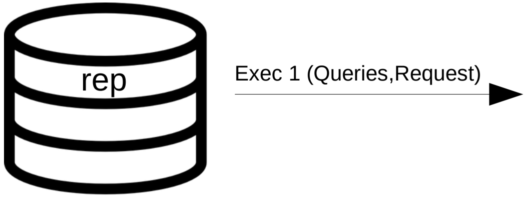
rep

Exec 1 (Queries,Request)

Data Analysis

(Interdependent Query Pairs)

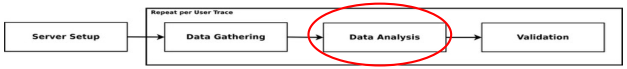




```
**Input**: Q = $\{q_1, q_2, ..., q_n\}$, a list of queries
**Output**: R = $\{..., (p,q)_i, ...\}$ a list of paired queries
R = $\emptyset$
for i = 1,2,...,n do
    q = Q[i]
    D = def(q)
    for j = i - 1, i - 2, ... , 1 do
        p = Q[j]
        U = use(p)
        if D ∩ U then
           R = R ∪ {(p,q)}
```

Data Analysis

(Interdependent Query Pairs)



rep

Exec 1 (Queries,Request) →

```
Input: Q = $\{q_1, q_2, ..., q_n\}$, a list of queries
Output: R = $\{..., (p,q)_i, ...\}$ a list of paired queries
R = $\emptyset$
for i = 1,2,...,n do
    q = Q[i]
    D = def(q)
    for j = i - 1, i - 2, ... , 1 do
        p = Q[j]
        U = use(p)
        if D ∩ U then
           R = R ∪ {(p,q)}
```

→

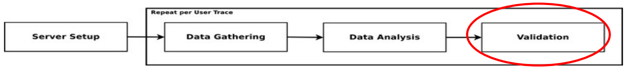
(Q1, Q2)

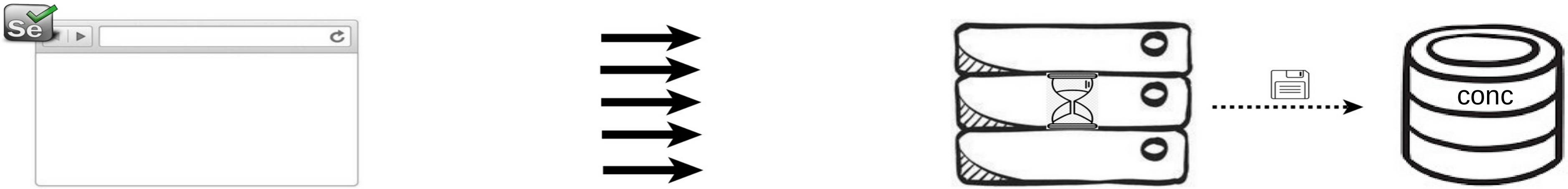
(Q1, Q3)

(Q5, Q8)

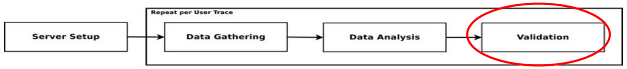
….

Testing


Server Setup
Repeat per User Trace
Data Gathering
Data Analysis
Validation


Se
conc

Validating



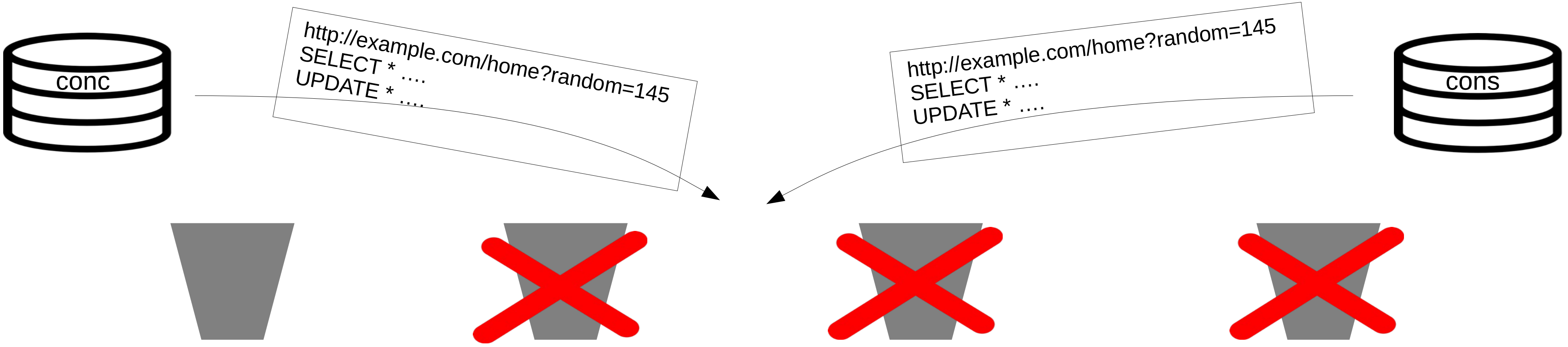
Repeat per User Trace

Server Setup

Data Gathering

Data Analysis

Validation



conc

http://example.com/home?random=145
SELECT * ….
UPDATE * ….

http://example.com/home?random=145
SELECT * ….
UPDATE * ….

cons

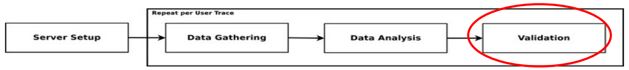
http://example.com/home?random=

http://example.com/user?random=

http://example.com/admin?random=

http://example.com/logout?random=

Validating



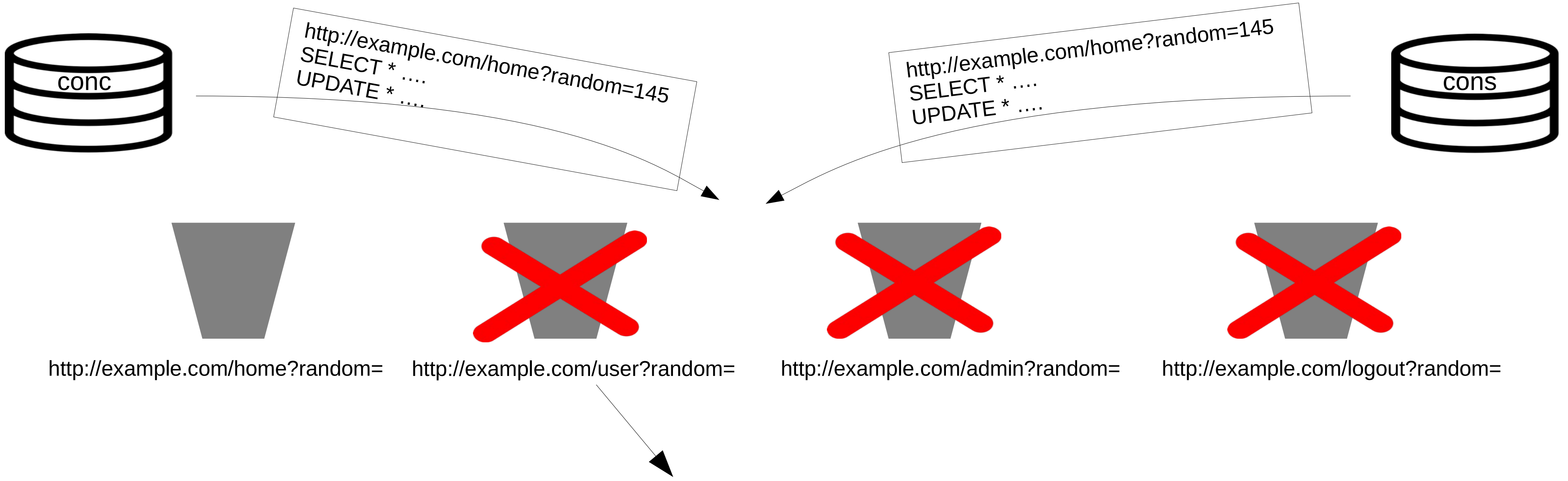
Repeat per User Trace

Server Setup

Data Gathering

Data Analysis

Validation



conc

http://example.com/home?random=145
SELECT * ….
UPDATE * ….

http://example.com/home?random=145
SELECT * ….
UPDATE * ….

cons

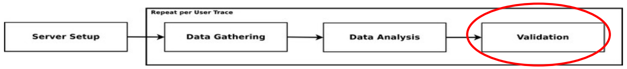
http://example.com/home?random=

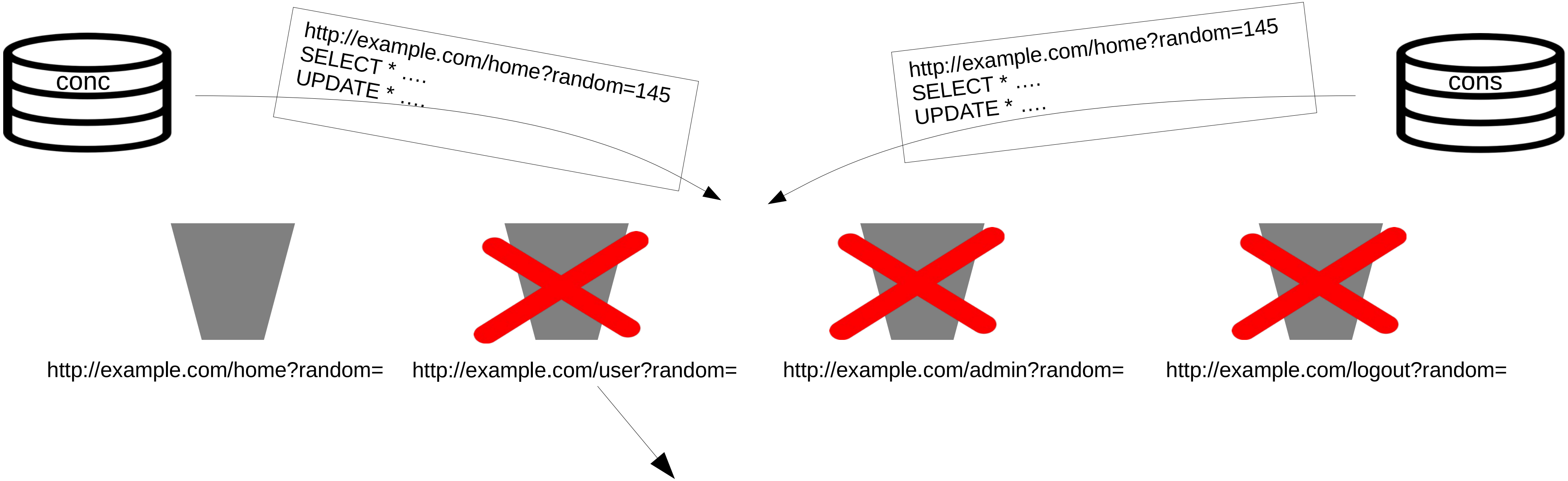
http://example.com/user?random=

http://example.com/admin?random=

http://example.com/logout?random=

Validating




conc

http://example.com/home?random=145
SELECT * ….
UPDATE * ….

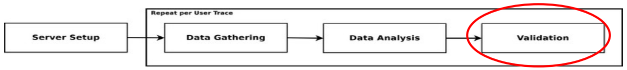
http://example.com/home?random=145
SELECT * ….
UPDATE * ….

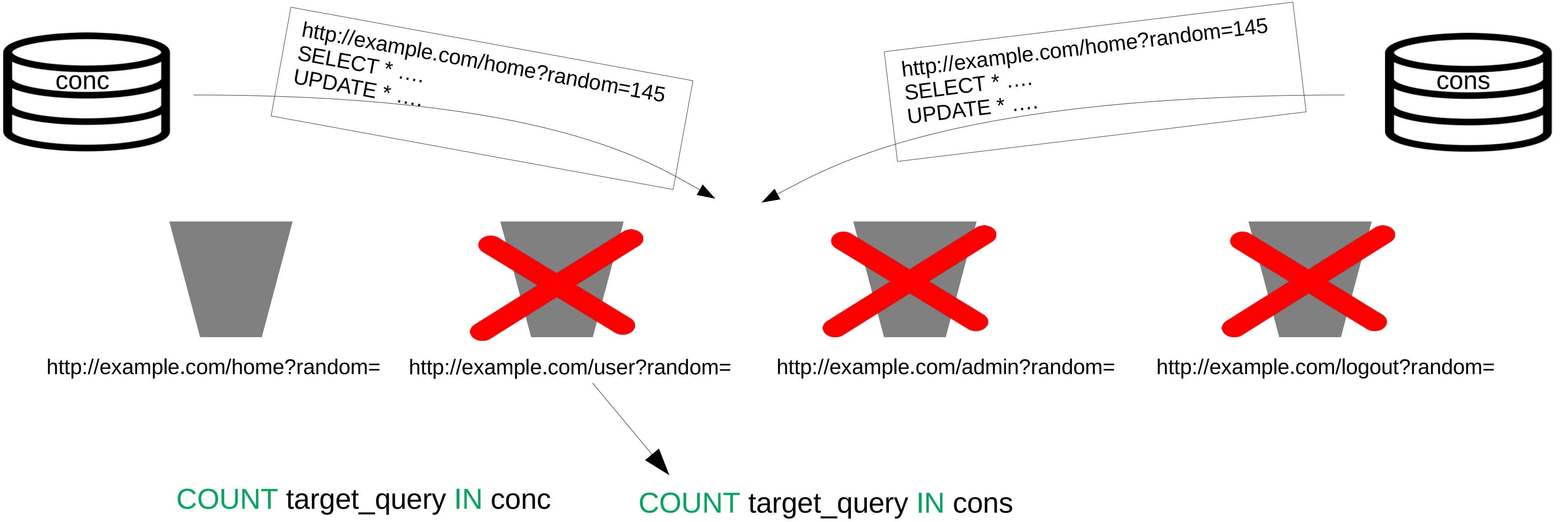
cons

http://example.com/home?random= http://example.com/user?random= http://example.com/admin?random= http://example.com/logout?random=

COUNT target_query IN conc

Validating

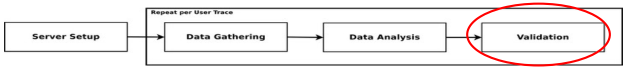


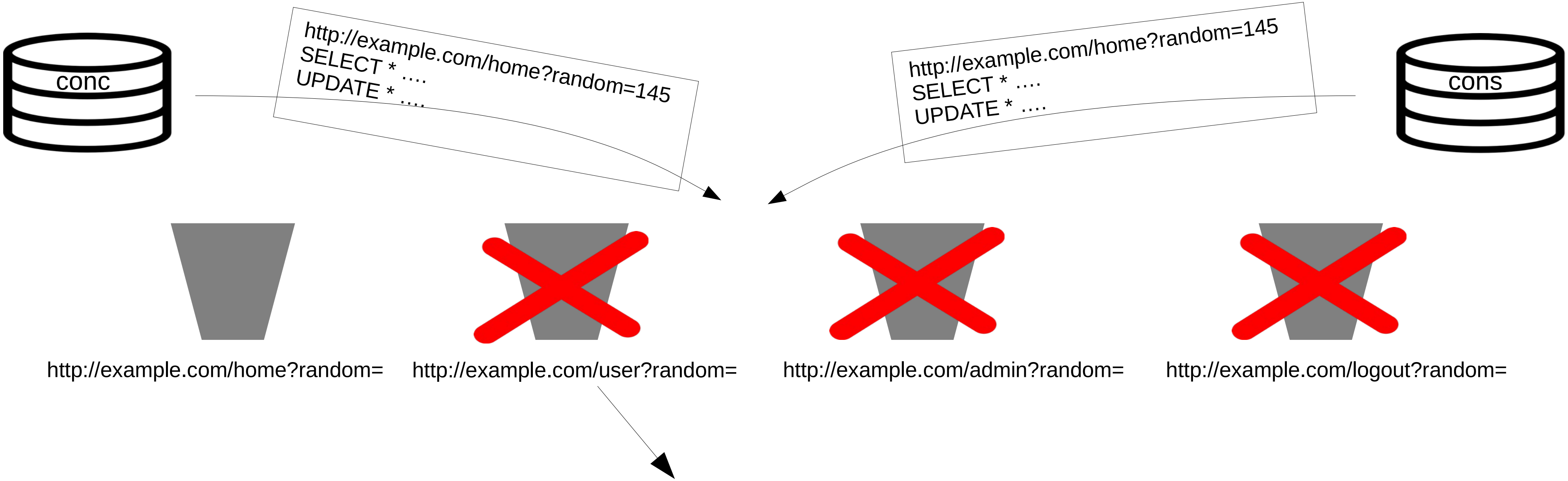

conc
http://example.com/home?random=145
SELECT * ….
UPDATE * ….
http://example.com/home?random=145
SELECT * ….
UPDATE * ….
cons
http://example.com/home?random=
http://example.com/user?random=
http://example.com/admin?random=
http://example.com/logout?random=

COUNT target_query IN conc

COUNT target_query IN cons

Validating





http://example.com/home?random=145
SELECT * ….
UPDATE * ….

http://example.com/home?random=145
SELECT * ….
UPDATE * ….

http://example.com/home?random=

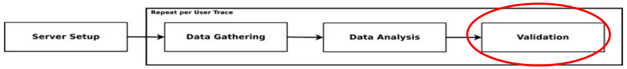
http://example.com/user?random=

http://example.com/admin?random=

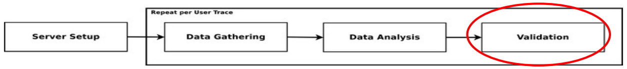
http://example.com/logout?random=

IF (COUNT target_query IN conc > COUNT target_query IN cons) THEN verified GRC

Validating


Repeat per User Trace
Server Setup
Data Gathering
Data Analysis
Validation

Validating



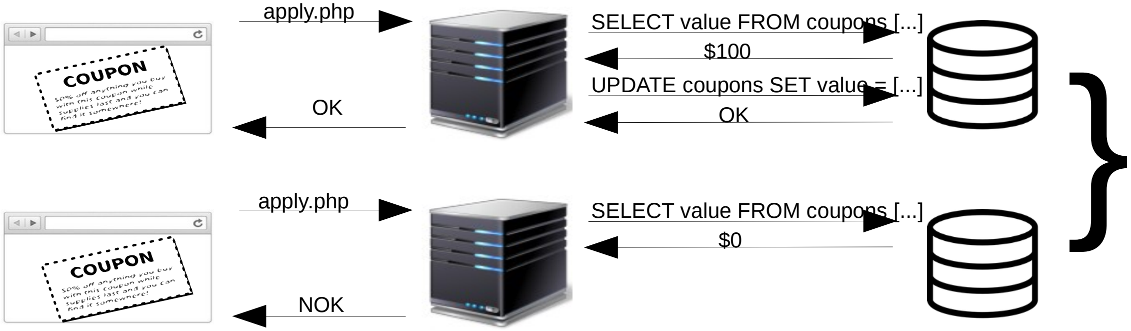
Server Setup

Repeat per User Trace

Data Gathering

Data Analysis

Validation



apply.php

SELECT value FROM coupons [...]

$100

UPDATE coupons SET value = [...]

OK

OK

apply.php

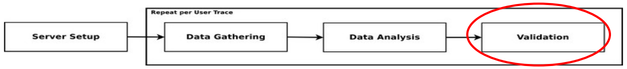
SELECT value FROM coupons [...]

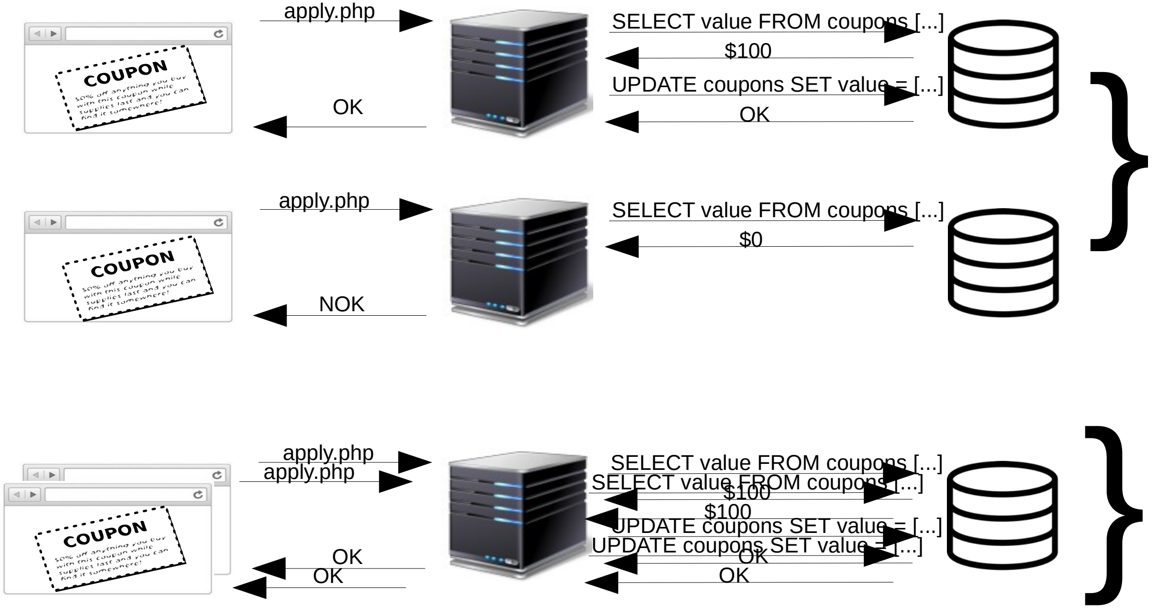
$0

NOK

count(UPDATE coupons …) = 1

Validating




COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!

apply.php

SELECT value FROM coupons [...]

$100

UPDATE coupons SET value = [...]

OK

OK

apply.php

SELECT value FROM coupons [...]

$0

NOK

count(UPDATE coupons …) = 1

apply.php

apply.php

SELECT value FROM coupons [...]

SELECT value FROM coupons [...]

$100

$100

UPDATE coupons SET value = [...]

UPDATE coupons SET value = [...]

OK

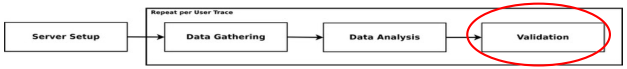
OK

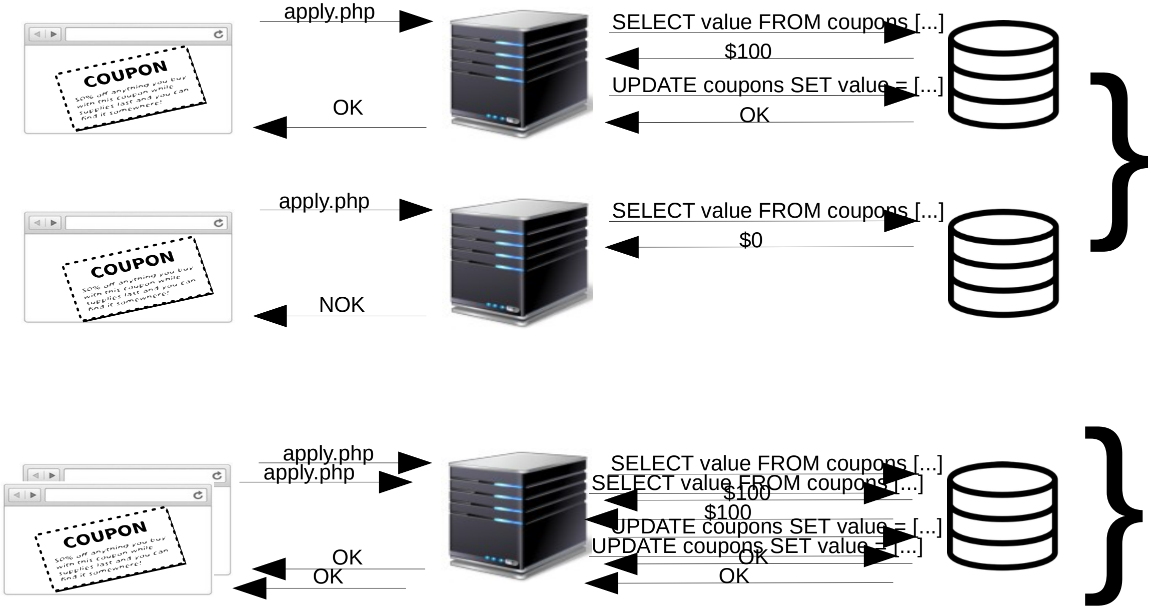
OK

OK

count(UPDATE coupons …) = 2

Validating





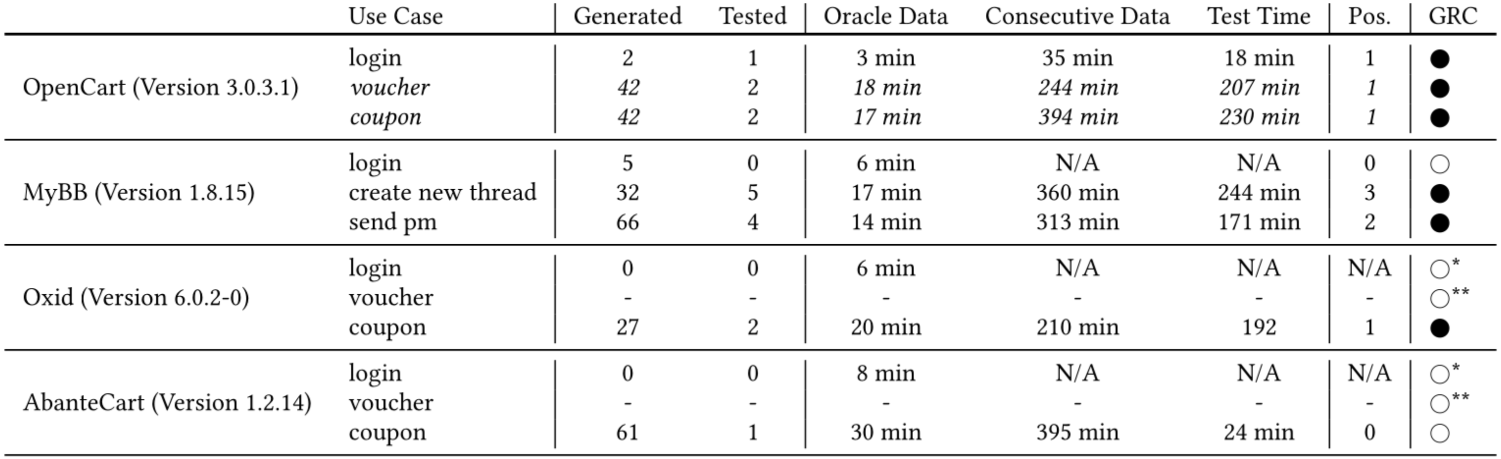
COUPON
50% off anything you buy with this coupon while supplies last and you can find it somewhere!
apply.php
OK
SELECT value FROM coupons [...]
$100
UPDATE coupons SET value = [...]
OK
apply.php
NOK
SELECT value FROM coupons [...]
$0
apply.php
apply.php
OK
OK
SELECT value FROM coupons [...]
SELECT value FROM coupons [...]
$100
$100
UPDATE coupons SET value = [...]
UPDATE coupons SET value = [...]
OK
OK

count(UPDATE coupons …) = 1

```
def use_voucher(cur_price, voucher_id):
    cur_value = get_voucher_value(voucher_id)
    if cur_value > 0:
        if cur_value >= cur_price:
            new_v = cur_value - cur_price
            new_price = 0
        else:
            new_v = 0
            new_price = cur_price - cur_value
        end
        update_voucher_value(new_v, voucher_id)
    return new_price
```

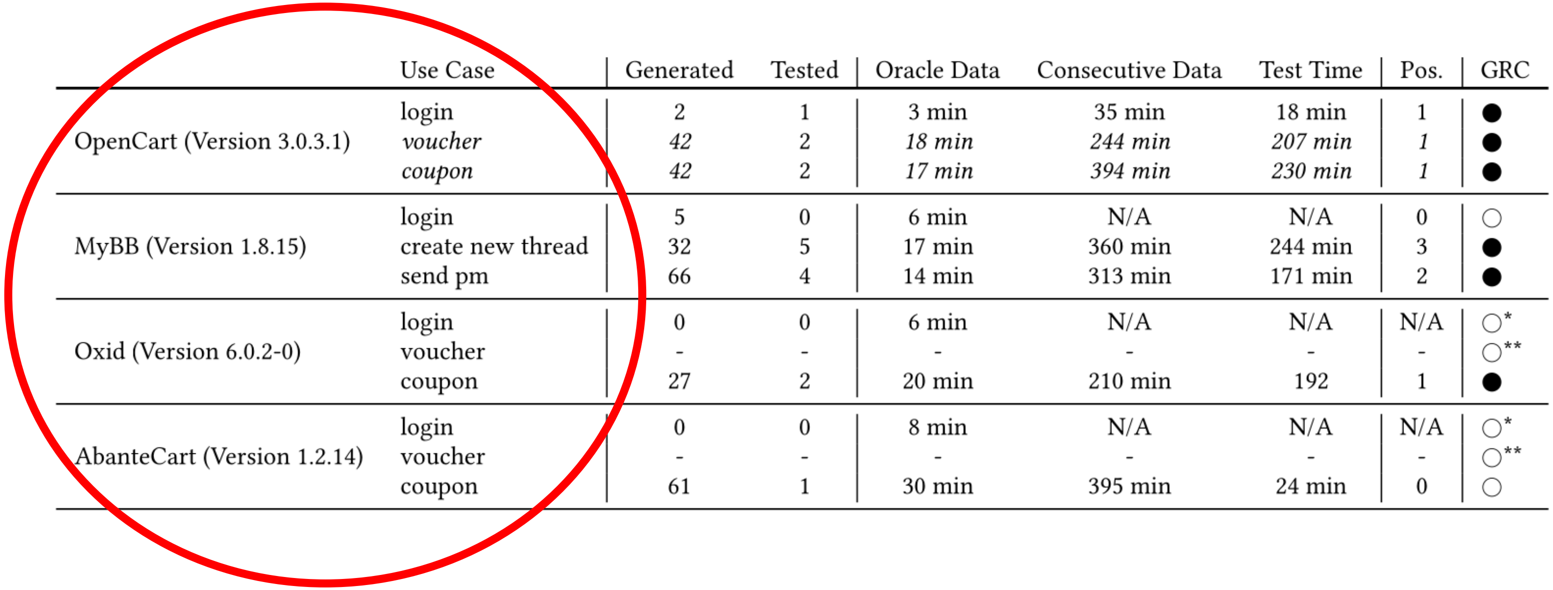
count(UPDATE coupons …) = 2

Evaluation



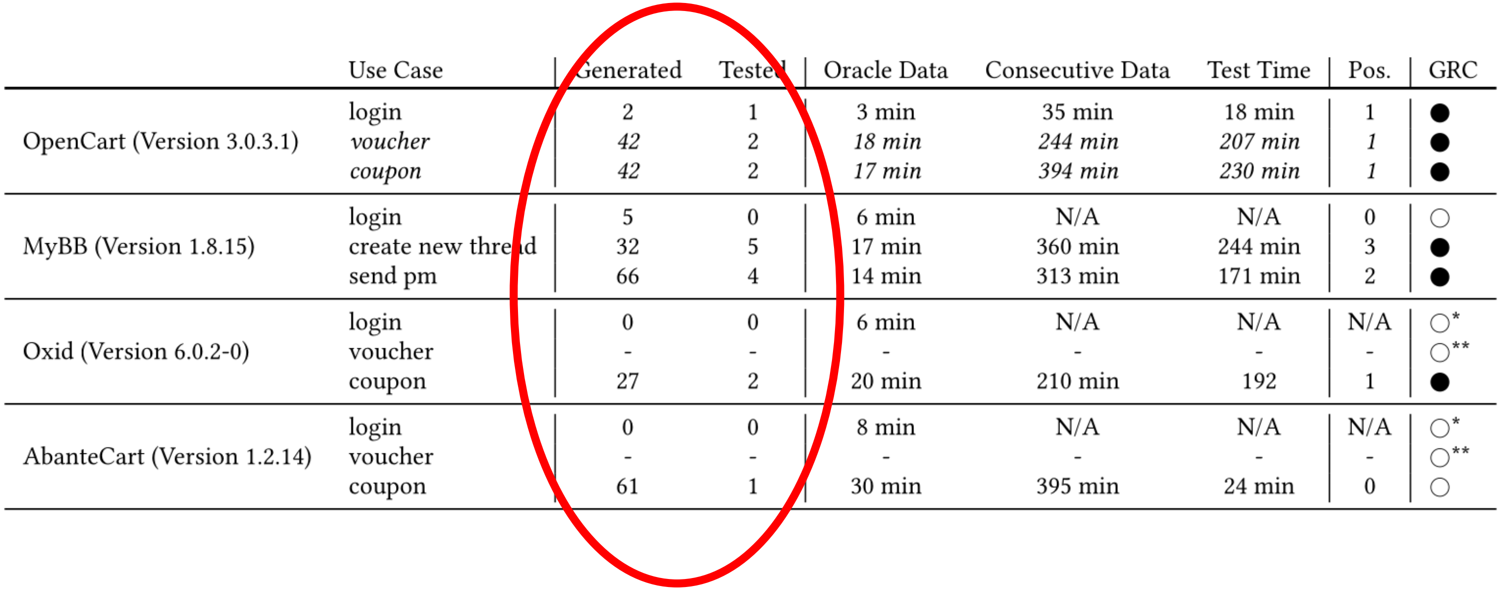
	Use Case	Generated	Tested	Oracle Data	Consecutive Data	Test Time	Pos.	GRC
OpenCart (Version 3.0.3.1)	login	2	1	3 min	35 min	18 min	1	●
	voucher	*42*	2	*18 min*	*244 min*	*207 min*	*1*	●
	coupon	*42*	2	*17 min*	*394 min*	*230 min*	*1*	●
MyBB (Version 1.8.15)	login	5	0	6 min	N/A	N/A	0	○
	create new thread	32	5	17 min	360 min	244 min	3	●
	send pm	66	4	14 min	313 min	171 min	2	●
Oxid (Version 6.0.2-0)	login	0	0	6 min	N/A	N/A	N/A	○*
	voucher	-	-	-	-	-	-	○**
	coupon	27	2	20 min	210 min	192	1	●
AbanteCart (Version 1.2.14)	login	0	0	8 min	N/A	N/A	N/A	○*
	voucher	-	-	-	-	-	-	○**
	coupon	61	1	30 min	395 min	24 min	0	○

Evaluation



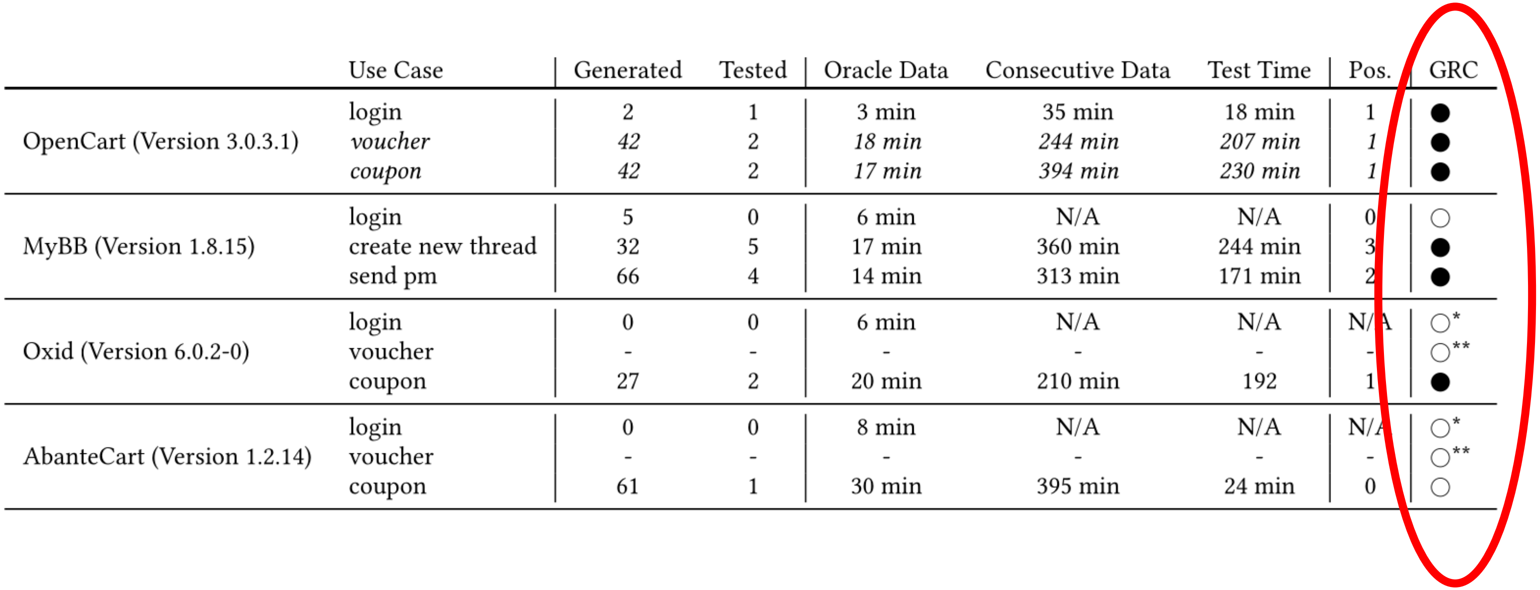
	Use Case	Generated	Tested	Oracle Data	Consecutive Data	Test Time	Pos.	GRC
OpenCart (Version 3.0.3.1)	login	2	1	3 min	35 min	18 min	1	●
	voucher	*42*	2	*18 min*	*244 min*	*207 min*	*1*	●
	coupon	*42*	2	*17 min*	*394 min*	*230 min*	*1*	●
MyBB (Version 1.8.15)	login	5	0	6 min	N/A	N/A	0	○
	create new thread	32	5	17 min	360 min	244 min	3	●
	send pm	66	4	14 min	313 min	171 min	2	●
Oxid (Version 6.0.2-0)	login	0	0	6 min	N/A	N/A	N/A	○*
	voucher	-	-	-	-	-	-	○**
	coupon	27	2	20 min	210 min	192	1	●
AbanteCart (Version 1.2.14)	login	0	0	8 min	N/A	N/A	N/A	○*
	voucher	-	-	-	-	-	-	○**
	coupon	61	1	30 min	395 min	24 min	0	○

Evaluation



	Use Case	Generated	Tested	Oracle Data	Consecutive Data	Test Time	Pos.	GRC
OpenCart (Version 3.0.3.1)	login	2	1	3 min	35 min	18 min	1	●
	voucher	*42*	2	*18 min*	*244 min*	*207 min*	*1*	●
	coupon	*42*	2	*17 min*	*394 min*	*230 min*	*1*	●
MyBB (Version 1.8.15)	login	5	0	6 min	N/A	N/A	0	○
	create new thread	32	5	17 min	360 min	244 min	3	●
	send pm	66	4	14 min	313 min	171 min	2	●
Oxid (Version 6.0.2-0)	login	0	0	6 min	N/A	N/A	N/A	○*
	voucher	-	-	-	-	-	-	○**
	coupon	27	2	20 min	210 min	192	1	●
AbanteCart (Version 1.2.14)	login	0	0	8 min	N/A	N/A	N/A	○*
	voucher	-	-	-	-	-	-	○**
	coupon	61	1	30 min	395 min	24 min	0	○

Evaluation



	Use Case	Generated	Tested	Oracle Data	Consecutive Data	Test Time	Pos.	GRC
OpenCart (Version 3.0.3.1)	login	2	1	3 min	35 min	18 min	1	●
	voucher	*42*	2	*18 min*	*244 min*	*207 min*	*1*	●
	coupon	*42*	2	*17 min*	*394 min*	*230 min*	*1*	●
MyBB (Version 1.8.15)	login	5	0	6 min	N/A	N/A	0	○
	create new thread	32	5	17 min	360 min	244 min	3	●
	send pm	66	4	14 min	313 min	171 min	2	●
Oxid (Version 6.0.2-0)	login	0	0	6 min	N/A	N/A	N/A	○*
	voucher	-	-	-	-	-	-	○**
	coupon	27	2	20 min	210 min	192	1	●
AbanteCart (Version 1.2.14)	login	0	0	8 min	N/A	N/A	N/A	○*
	voucher	-	-	-	-	-	-	○**
	coupon	61	1	30 min	395 min	24 min	0	○

Conclusion

Conclusion

- First automatic approach on testing and validating guarded race conditions in web applications

Conclusion

- First automatic approach on testing and validating guarded race conditions in web applications
- Implemented the approach as the tool Raccoon [1]

Conclusion

- First automatic approach on testing and validating guarded race conditions in web applications
- Implemented the approach as the tool Raccoon [1]
- Tested Raccoon against 4 different web applications

Conclusion

- First automatic approach on testing and validating guarded race conditions in web applications
- Implemented the approach as the tool Raccoon [1]
- Tested Raccoon against 4 different web applications
- Detected 6 Guraded Race Conditions 4 of them novel

[1]: https://github.com/simkoc/raccoon.git