IJON

Exploring Deep State Spaces via Fuzzing

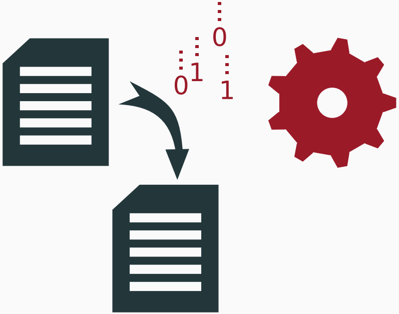
Cornelius Aschermann, Sergej Schumilo, Ali Abbasi, and Thorsten Holz
Ruhr University Bochum

Modern Fuzzers

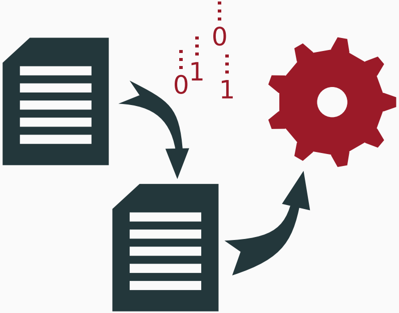
Modern Fuzzers

Modern Fuzzers

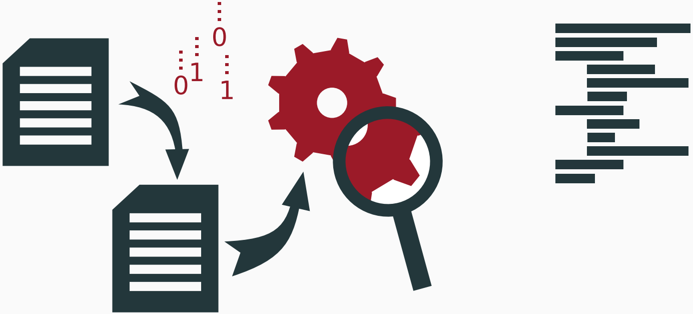
Modern Fuzzers



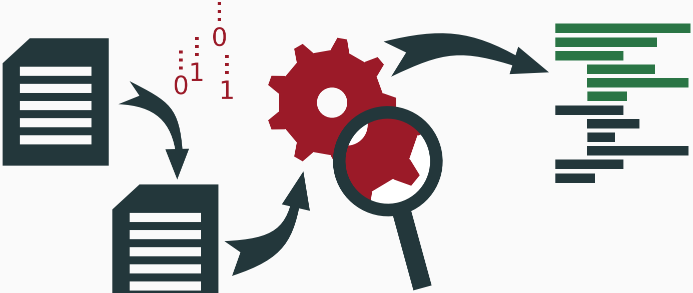
Modern Fuzzers



Modern Fuzzers

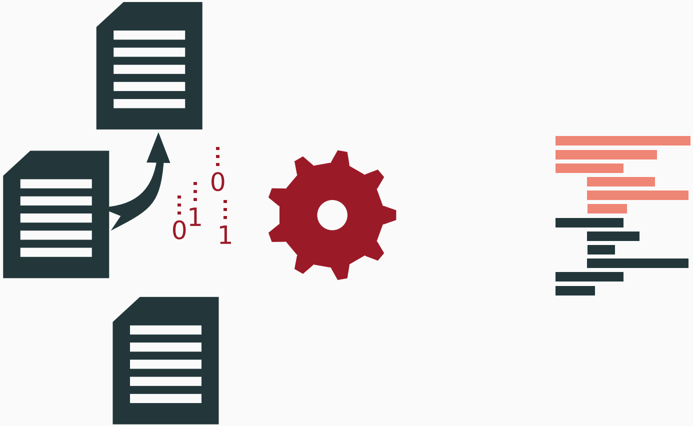


Modern Fuzzers

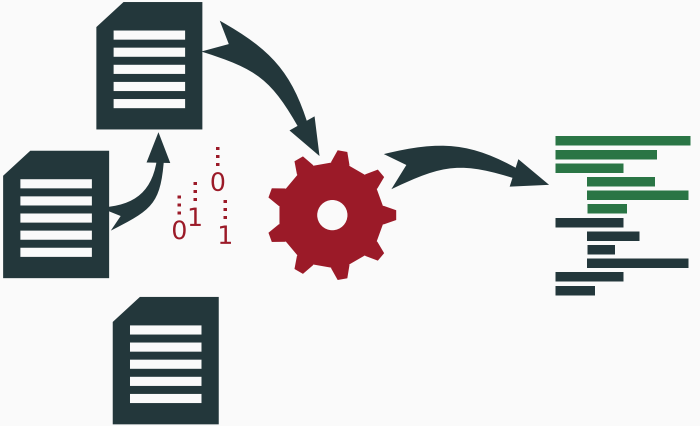


Modern Fuzzers

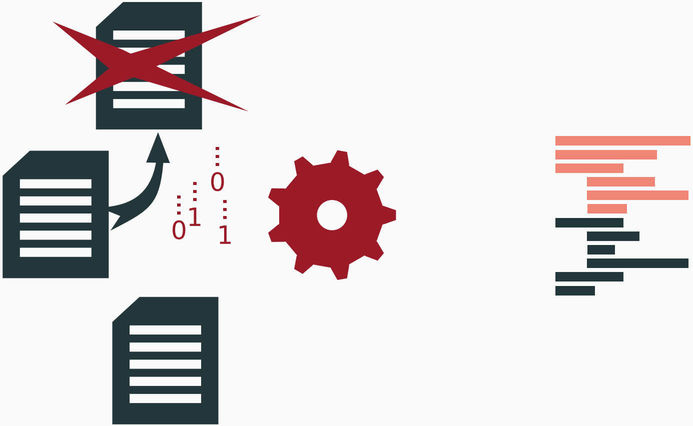
Modern Fuzzers



Modern Fuzzers

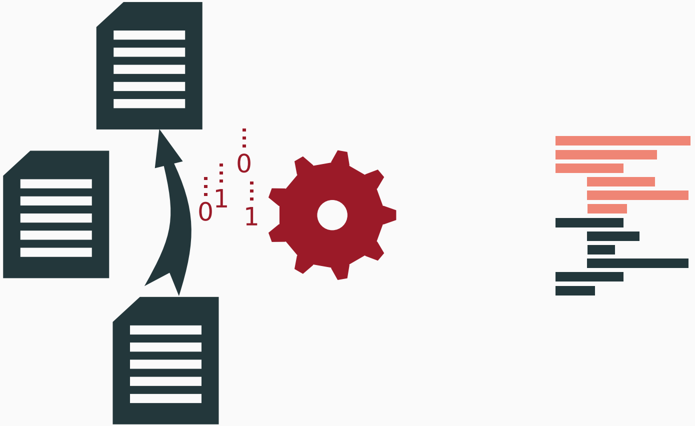


Modern Fuzzers

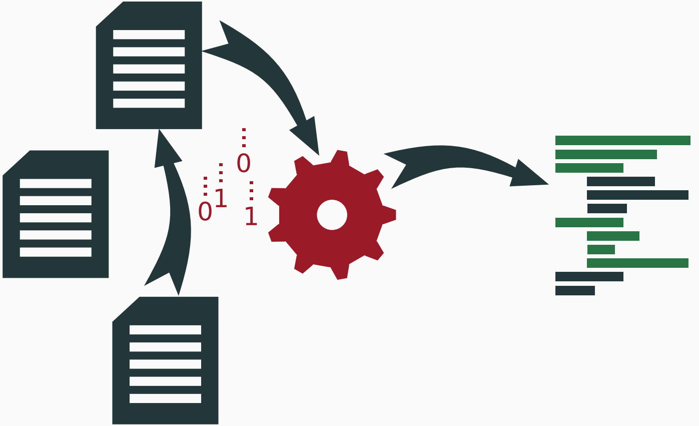


Modern Fuzzers

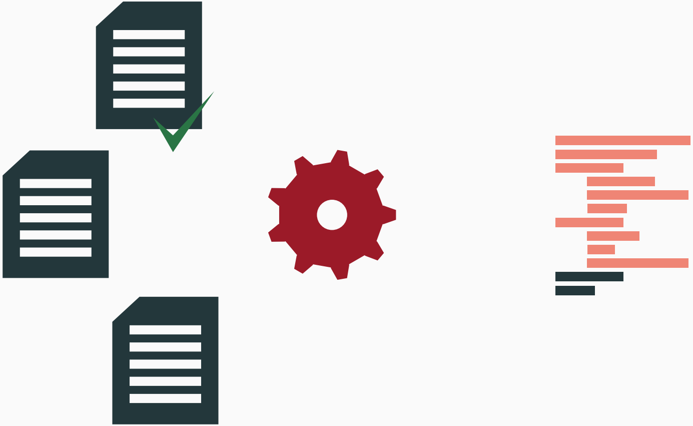
Modern Fuzzers



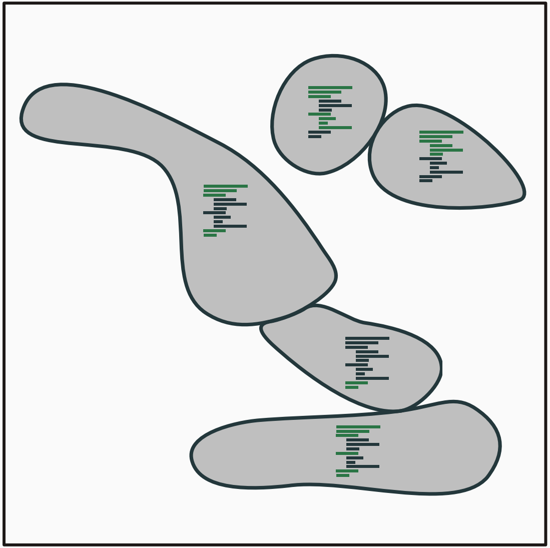
Modern Fuzzers



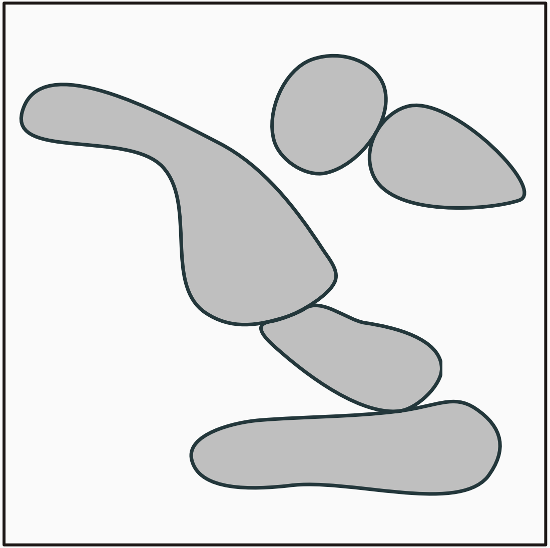
Modern Fuzzers



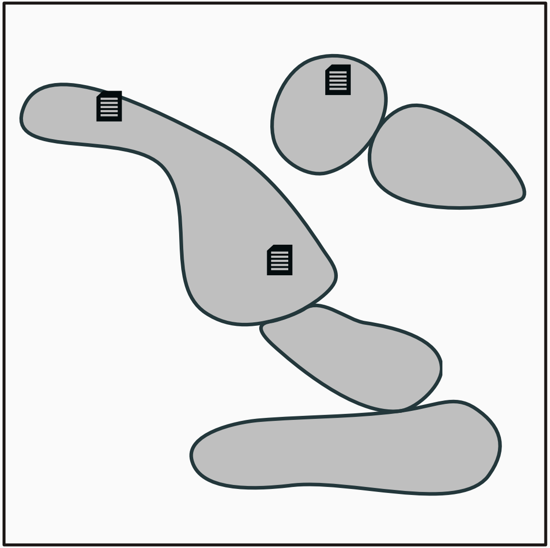
High-Level Mutation Fuzzing



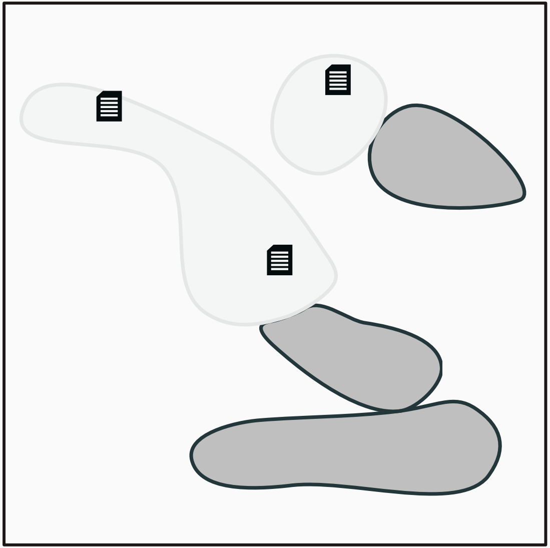
High-Level Mutation Fuzzing



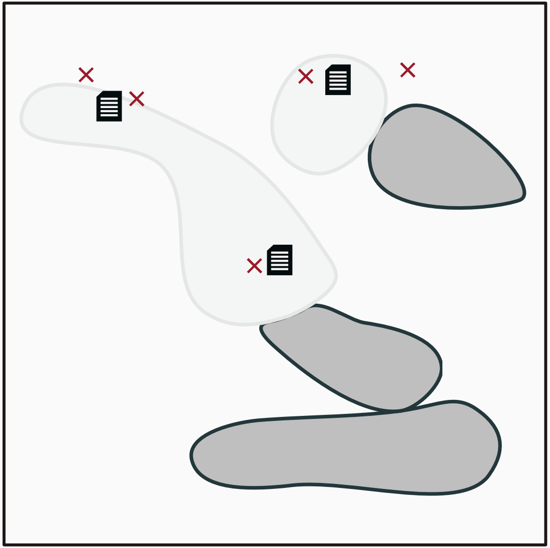
High-Level Mutation Fuzzing



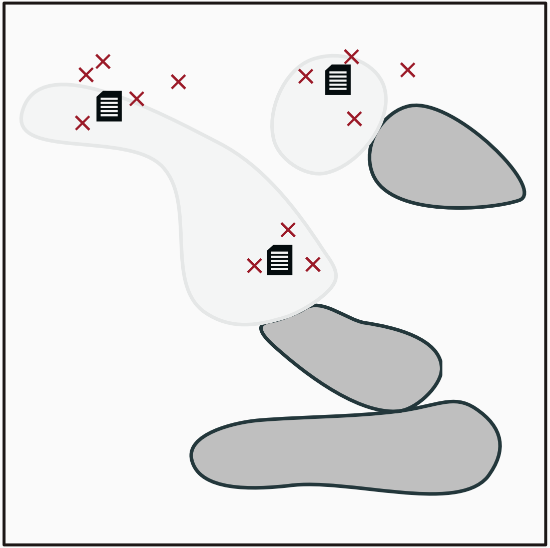
High-Level Mutation Fuzzing



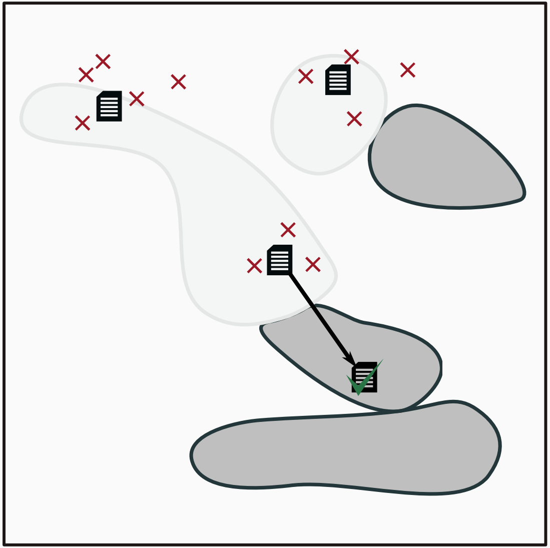
High-Level Mutation Fuzzing



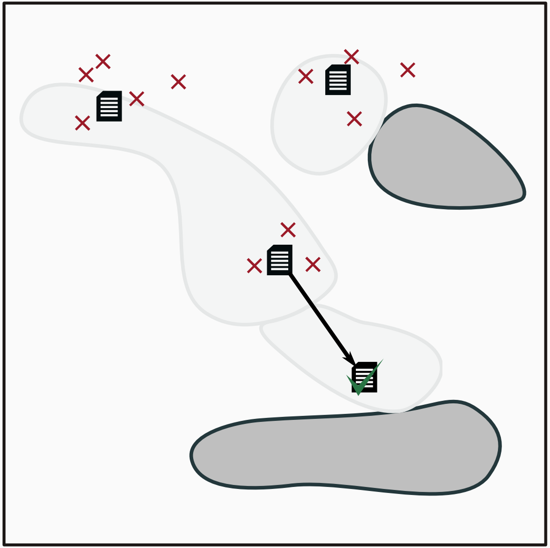
High-Level Mutation Fuzzing



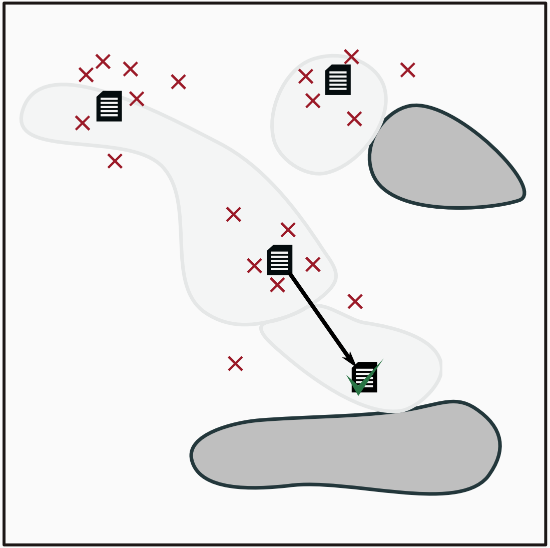
High-Level Mutation Fuzzing



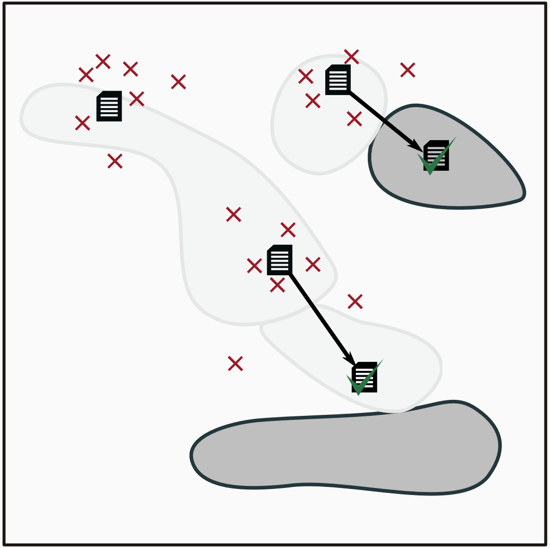
High-Level Mutation Fuzzing



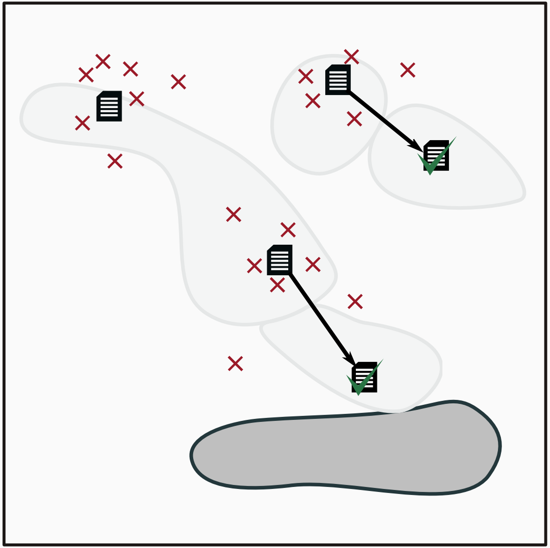
High-Level Mutation Fuzzing



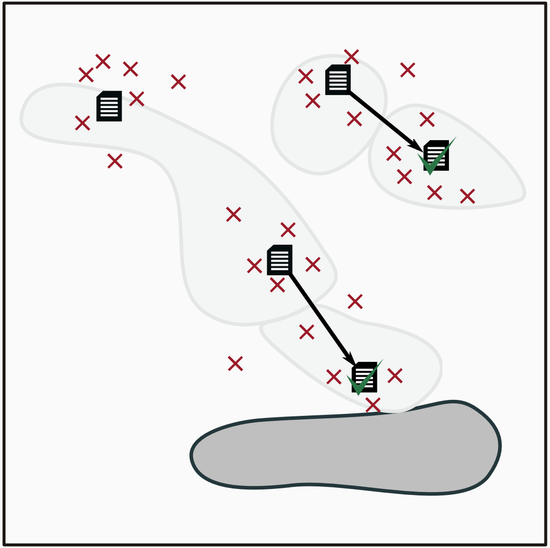
High-Level Mutation Fuzzing



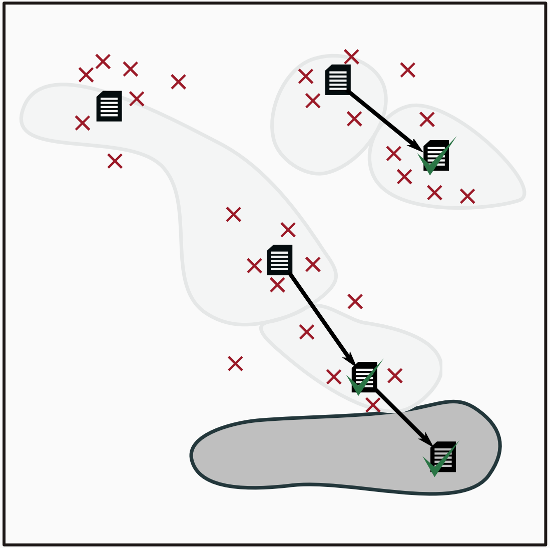
High-Level Mutation Fuzzing



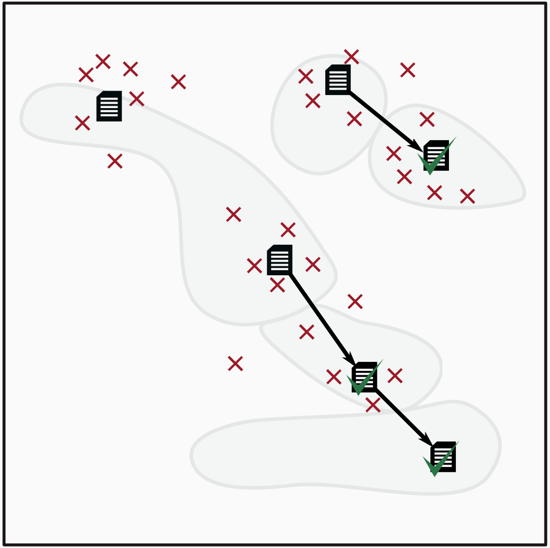
High-Level Mutation Fuzzing



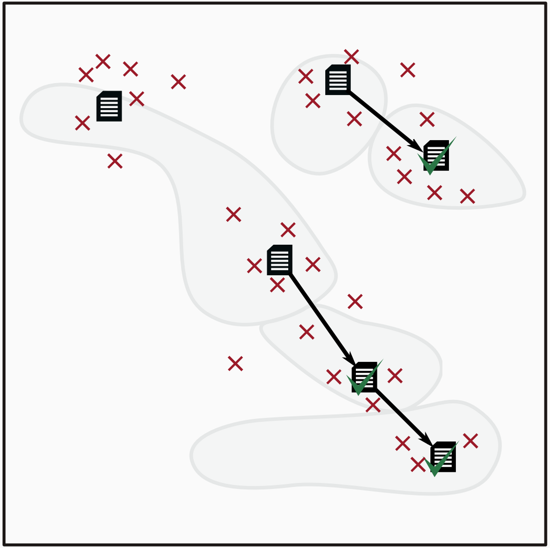
High-Level Mutation Fuzzing



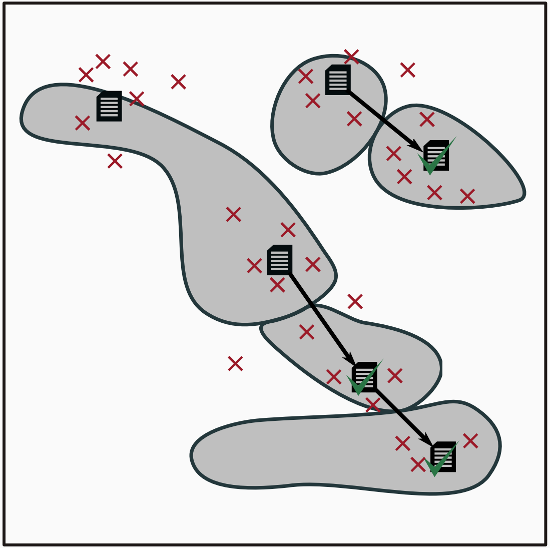
High-Level Mutation Fuzzing



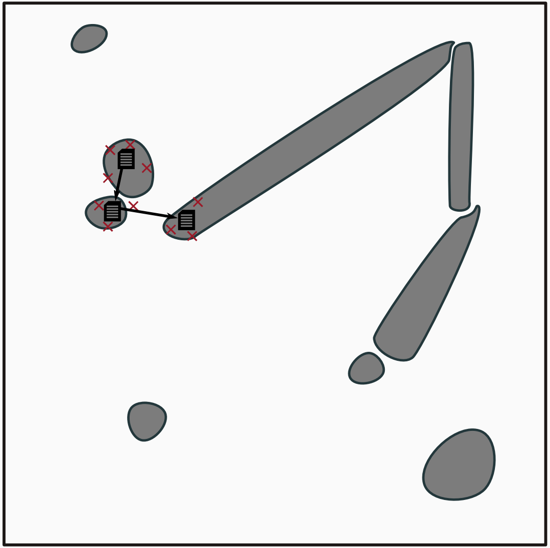
High-Level Mutation Fuzzing



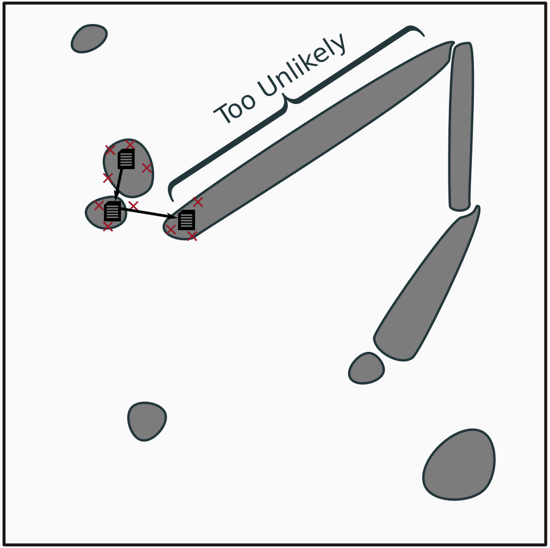
High-Level Mutation Fuzzing



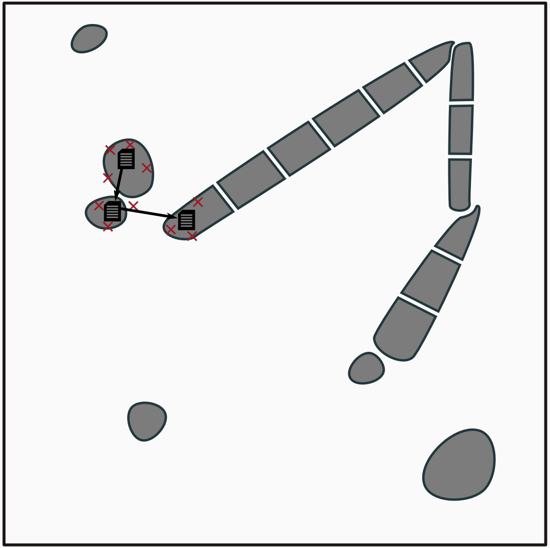
Limitations

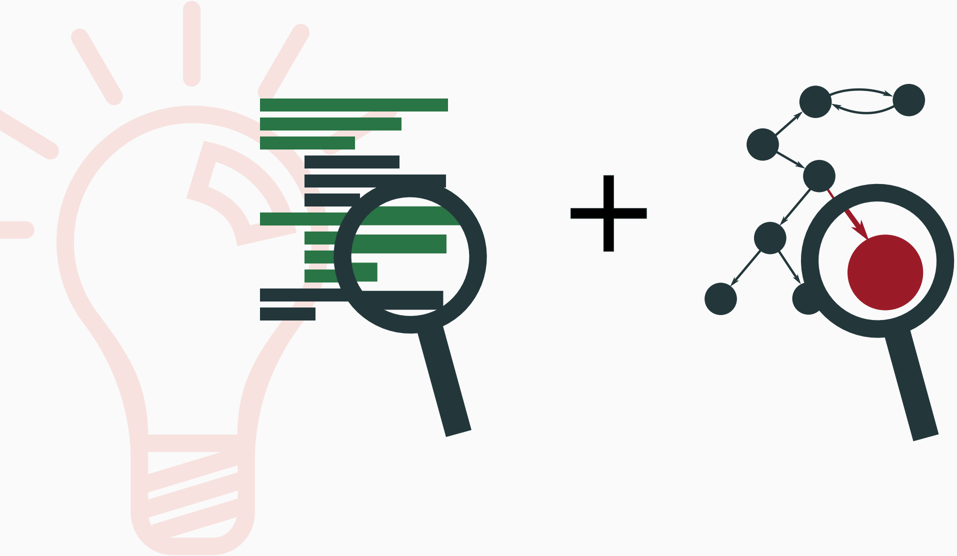


Limitations



Better Feedback





Annotations

```
while(true) {
    // ...

    switch (input[i]) {
        case 'w': y--; break;
        case 's': y++; break;
        case 'a': x--; break;
        case 'd': x++; break;
    }
    // ...
}
```

```
+-+---+---+
|X|     |#|
| | --+ | |
| |   | | |
| +-- | | |
|     |   |
+-----+---+
```

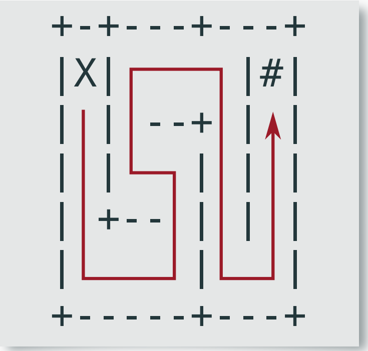
Annotations

```
while(true) {
    // ...
    IJON_SET(hash(x,y));
    switch (input[i]) {
        case 'w': y--; break;
        case 's': y++; break;
        case 'a': x--; break;
        case 'd': x++; break;
    }
    // ...
}
```

```
+-+---+---+
|X|     |#|
| | --+ | |
| |   | | |
| +-- | | |
|     |   |
+-----+---+
```

Annotations

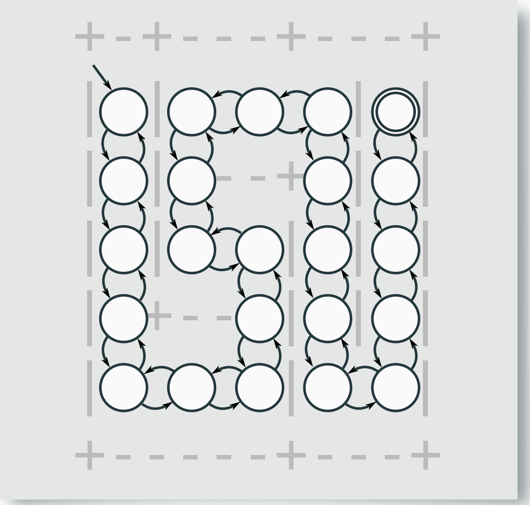
```
while(true) {
    // ...
    IJON_SET(hash(x,y));
    switch (input[i]) {
        case 'w': y--; break;
        case 's': y++; break;
        case 'a': x--; break;
        case 'd': x++; break;
    }
    // ...
}
```



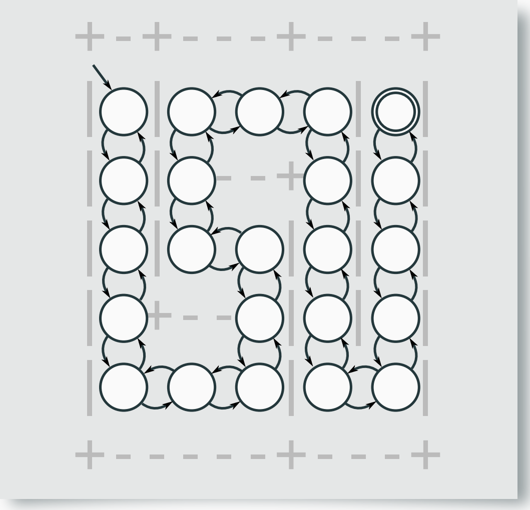
```
+-+---+---+
|X|     |#|
| | --+ | |
| |   | | |
| +-- | | |
|     |   |
+-----+---+
```

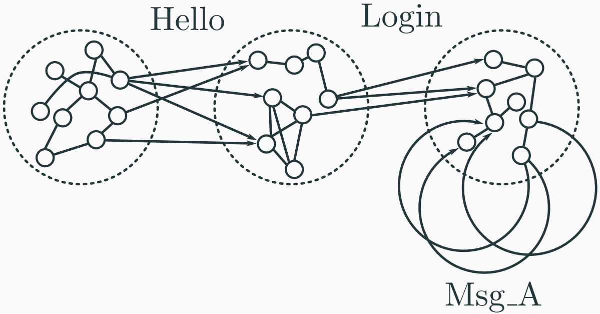
Real World?

Implicit State Machine



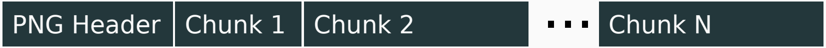
Implicit State Machine





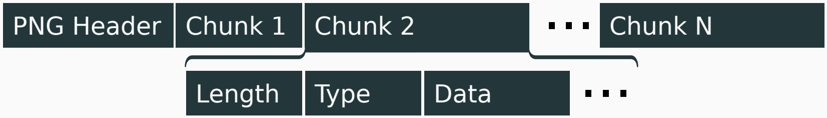
libpng

libpng



PNG Header | Chunk 1 | Chunk 2 | ... | Chunk N

libpng



PNG Header

Chunk 1

Chunk 2

...

Chunk N

Length

Type

Data

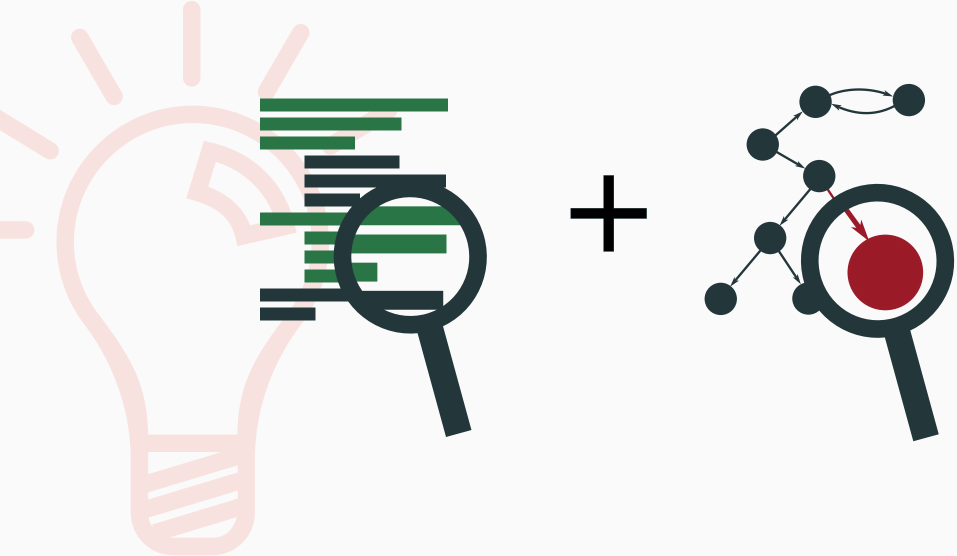
...

libpng

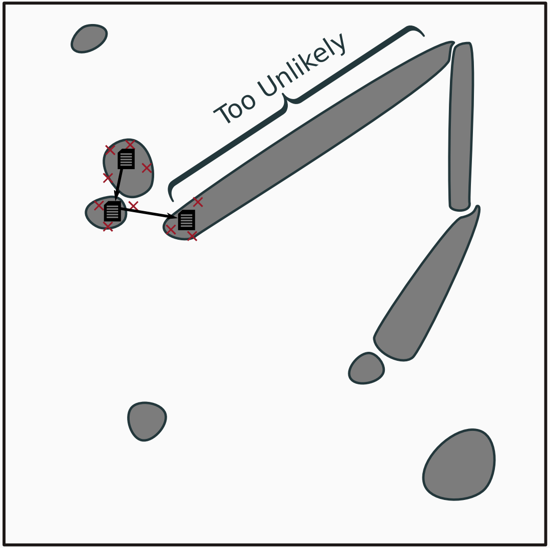
```
while(true) {
    hdr = read_chunk_hdr();
    switch (hdr.type) {
        case png_oFFs: handle_oFFs(); break;
        case png_IDAT: handle_IDAT(); break;
        // ...
    }




}
```

libpng

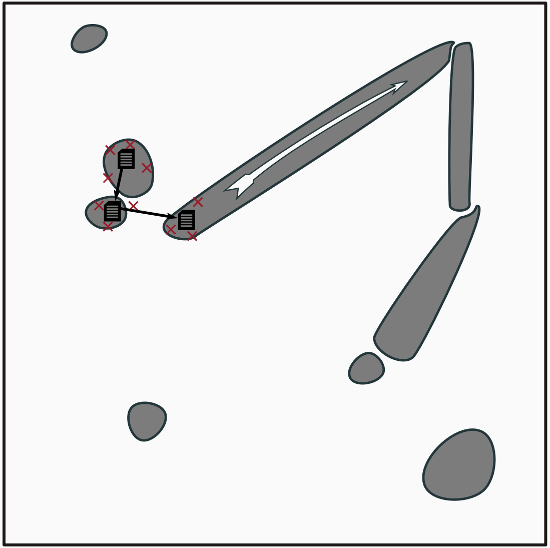
```
uint32_t log = 0;
while(true) {
    hdr = read_chunk_hdr();
    switch (hdr.type) {
        case png_oFFs: handle_oFFs(); break;
        case png_IDAT: handle_IDAT(); break;
        // ...
    }
    if( no_parse_error() ){
        log = log << 8 | hash(hdr.type)&0xff;
        IJON_SET(log)
    }
}
```



Limitations

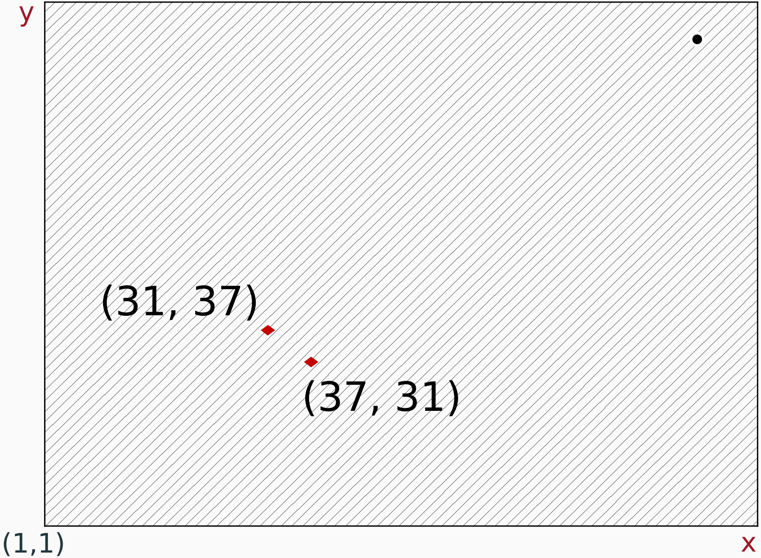


Better Feedback



High Level Mutation Fuzzing

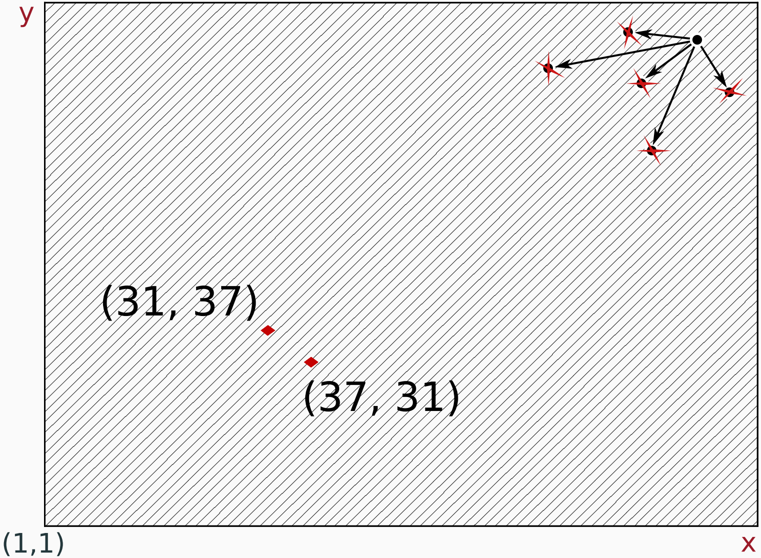
```
if(x > 1 && y > 1)

  if( x * y == 1147 )
    bug(1);
```



High Level Mutation Fuzzing

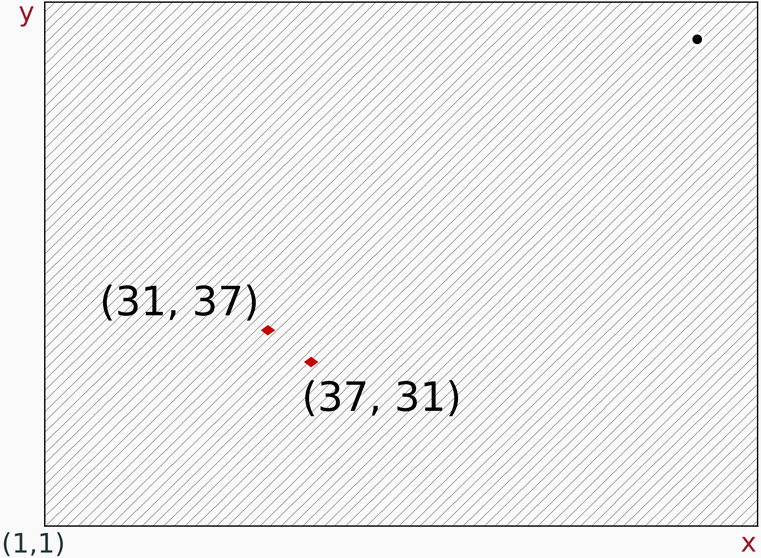
RUHR UNIVERSITÄT BOCHUM

```
if(x > 1 && y > 1)

  if( x * y == 1147 )
    bug(1);
```



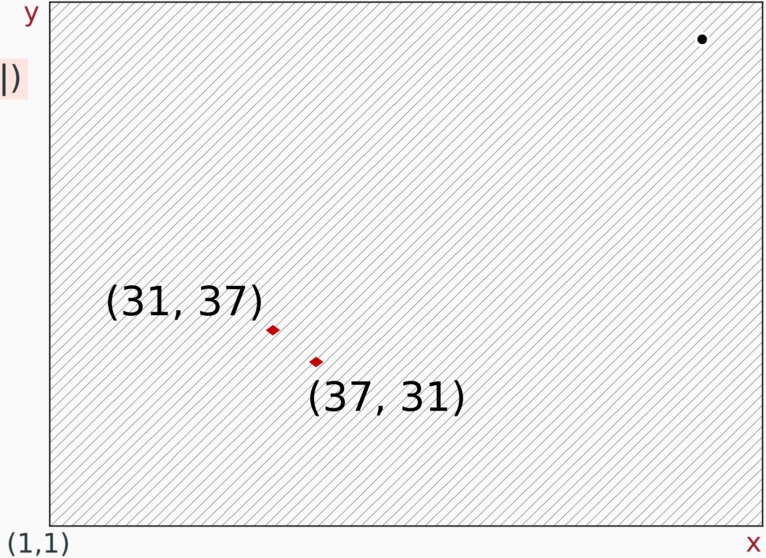
High Level Mutation Fuzzing

```
if(x > 1 && y > 1)

  if( x * y == 1147 )
    bug(1);
```



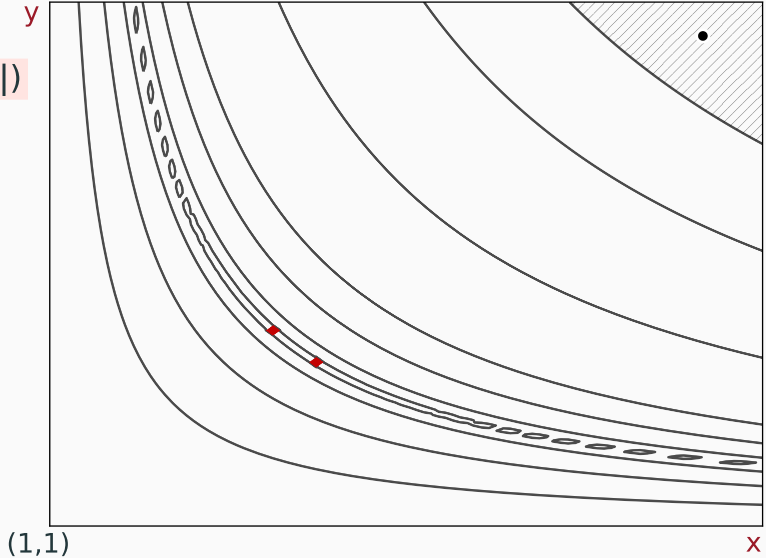
High Level Mutation Fuzzing

```
if(x > 1 && y > 1)
minimize(|x*y - 1147|)
  if( x * y == 1147 )
    bug(1);
```



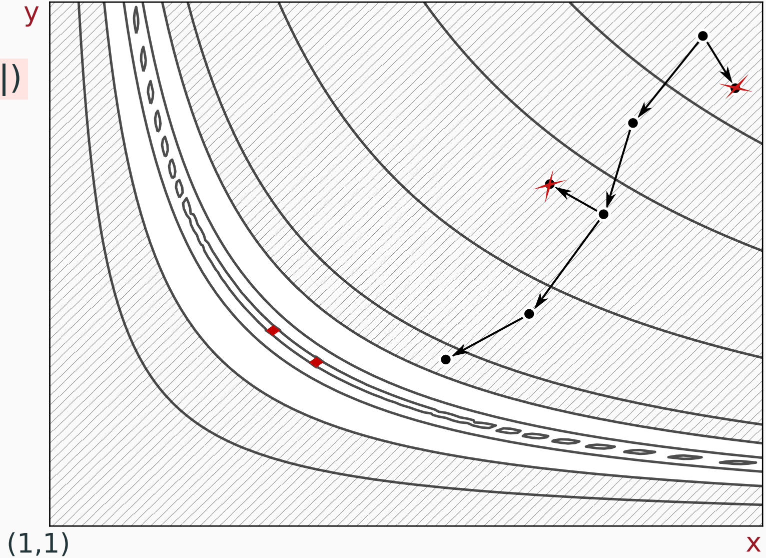
High Level Mutation Fuzzing

```
if(x > 1 && y > 1)
minimize(|x*y - 1147|)
  if( x * y == 1147 )
    bug(1);
```



High Level Mutation Fuzzing

```
if(x > 1 && y > 1)
minimize(|x*y - 1147|)
  if( x * y == 1147 )
    bug(1);
```

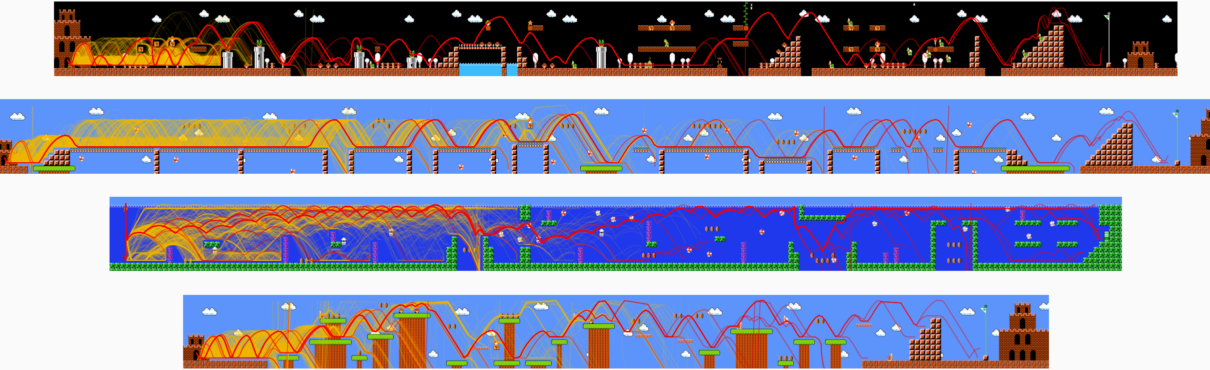


Super Mario Bros.

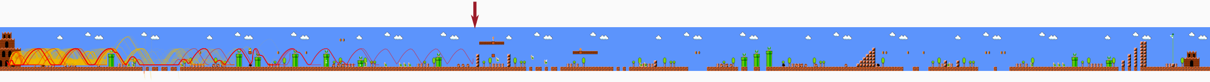
```
IJON_MAX(player_x);
```

+

Super Mario Bros.



Super Mario Bros.



Real World?

dmg2img

```
data = (char *)malloc(xml.len + 1);
if (!data)
   exit_with_error();
//....
data[xml.len] = '\0';
```

dmg2img

Overflow?

```
data = (char *)malloc(xml.len + 1);
if (!data)
   exit_with_error();
//....
data[xml.len] = '\0';
```

dmg2img

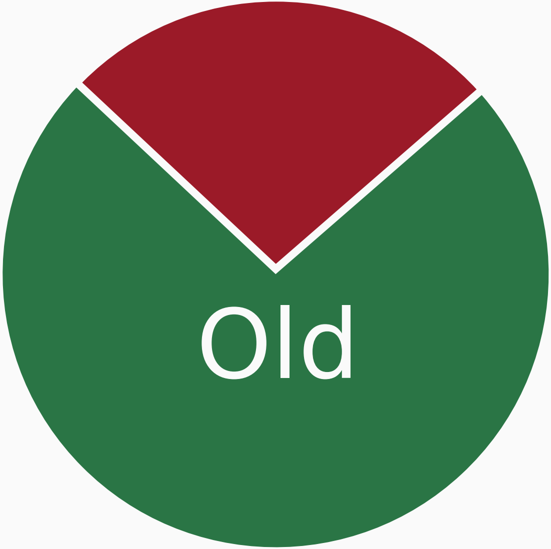
```
IJON_MAX(xml.len);
data = (char *)malloc(xml.len + 1);
if (!data)
   exit_with_error();
//....
data[xml.len] = '\0';
```

Eval

CGC

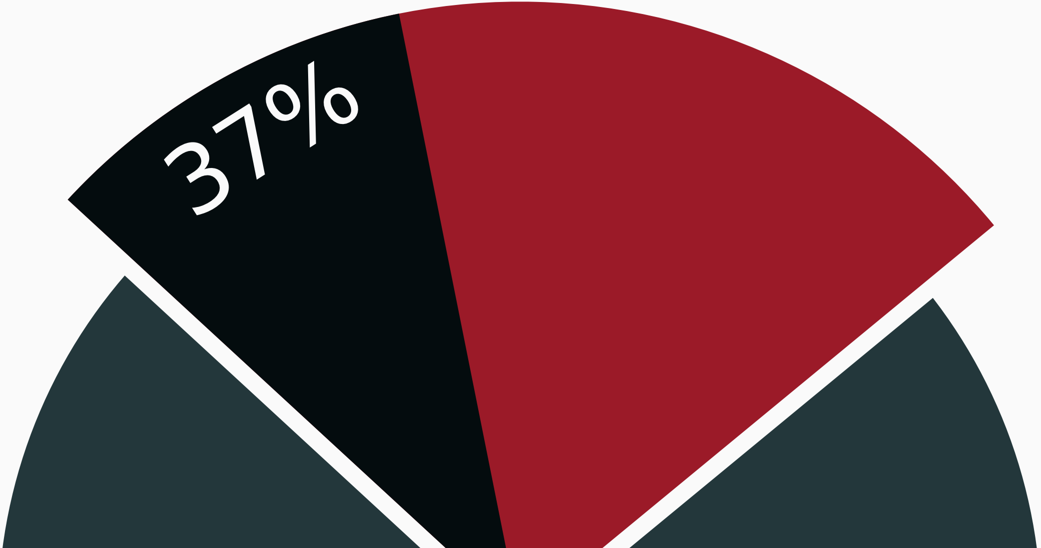
(226 Challenges)

Eval



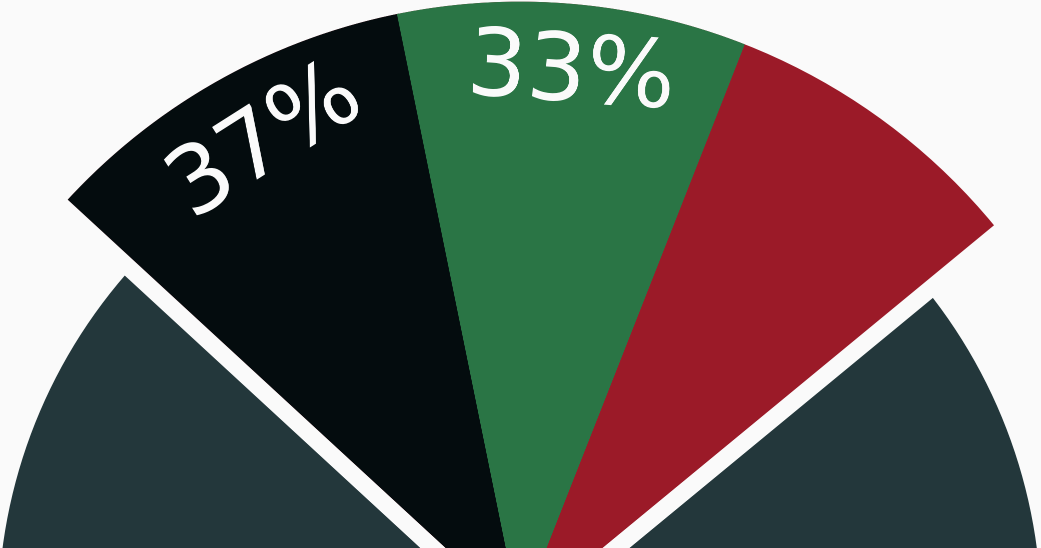
Eval

Eval

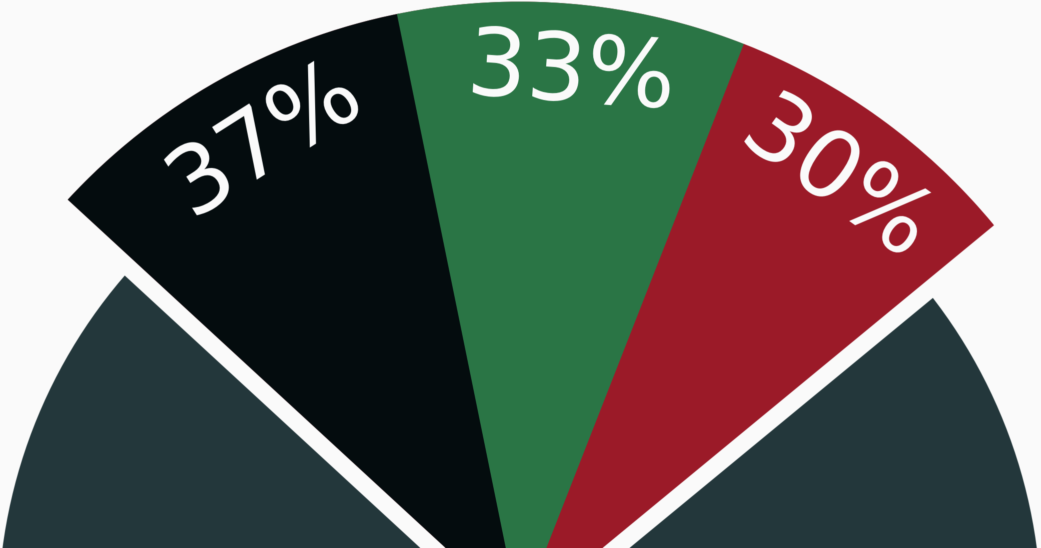


Eval

RUHR UNIVERSITÄT BOCHUM RUB



Eval



Future