JavaScript API Misuse Detection by Using TypeScript

Jihyeok Park

KAIST

jhpark0223@kaist.ac.kr

JavaScript

- Client-side scripting language of web pages

JavaScript

- Client-side scripting language of web pages
- Most prevalent for client-side programming

JavaScript

- Client-side scripting language of web pages
- Most prevalent for client-side programming
- Become used outside of client-side

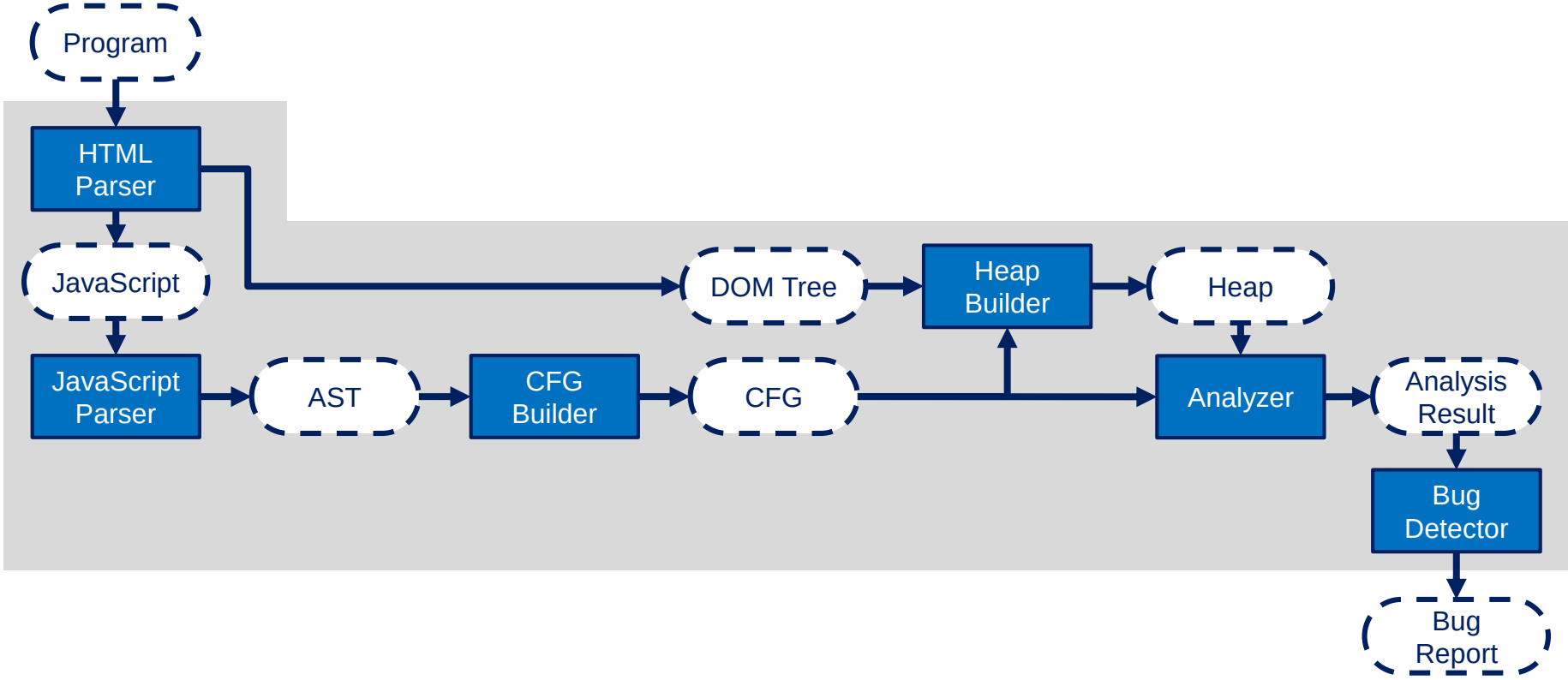
JavaScript

- Client-side scripting language of web pages
- Most prevalent for client-side programming
- Become used outside of client-side

MORE IMPORTANT

Analysis of JavaScript

- More challenging than other programming languages
- SAFE



TypeScript

- Strict superset of JavaScript with a type system
- Type checking at compile time
- TypeScript declaration files
  - *Interface*, *class*, *enum*
  - DefinitelyTyped project

My Idea

- Develop a tool to detect misuses of JavaScript APIs
  - Use TypeScript declaration files
  - Extend SAFE

JavaScript API Misuses

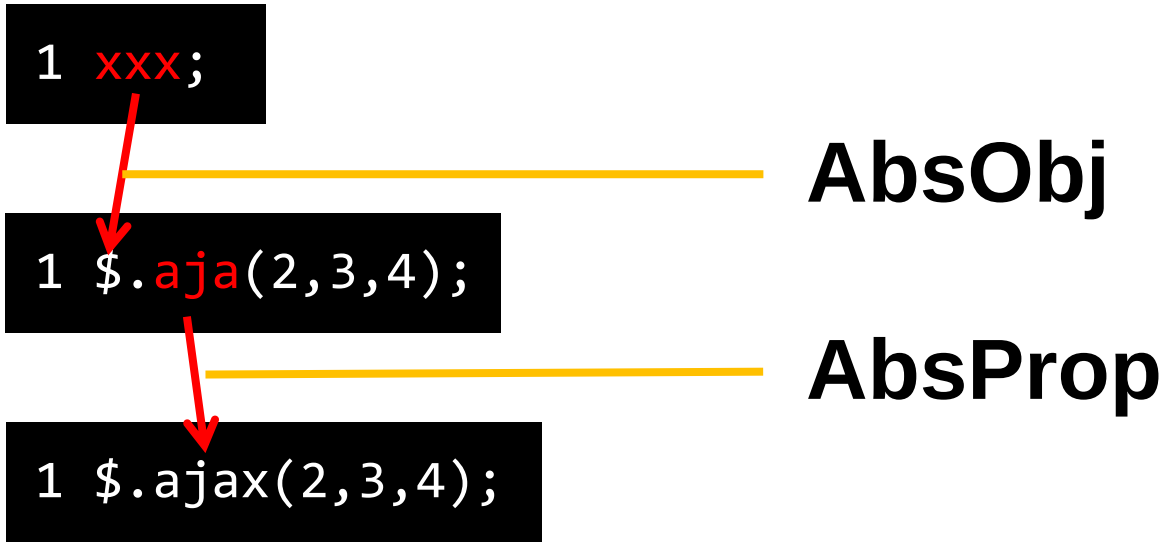
1. Accesses to absent objects or functions in APIs (**AbsObj**)
2. Accesses to absent member properties of API objects (**AbsProp**)
3. Wrong number of arguments to function calls (**WrongArgNum**)
4. Wrong types of arguments to function calls (**WrongArgTyp**)

JavaScript API Misuses

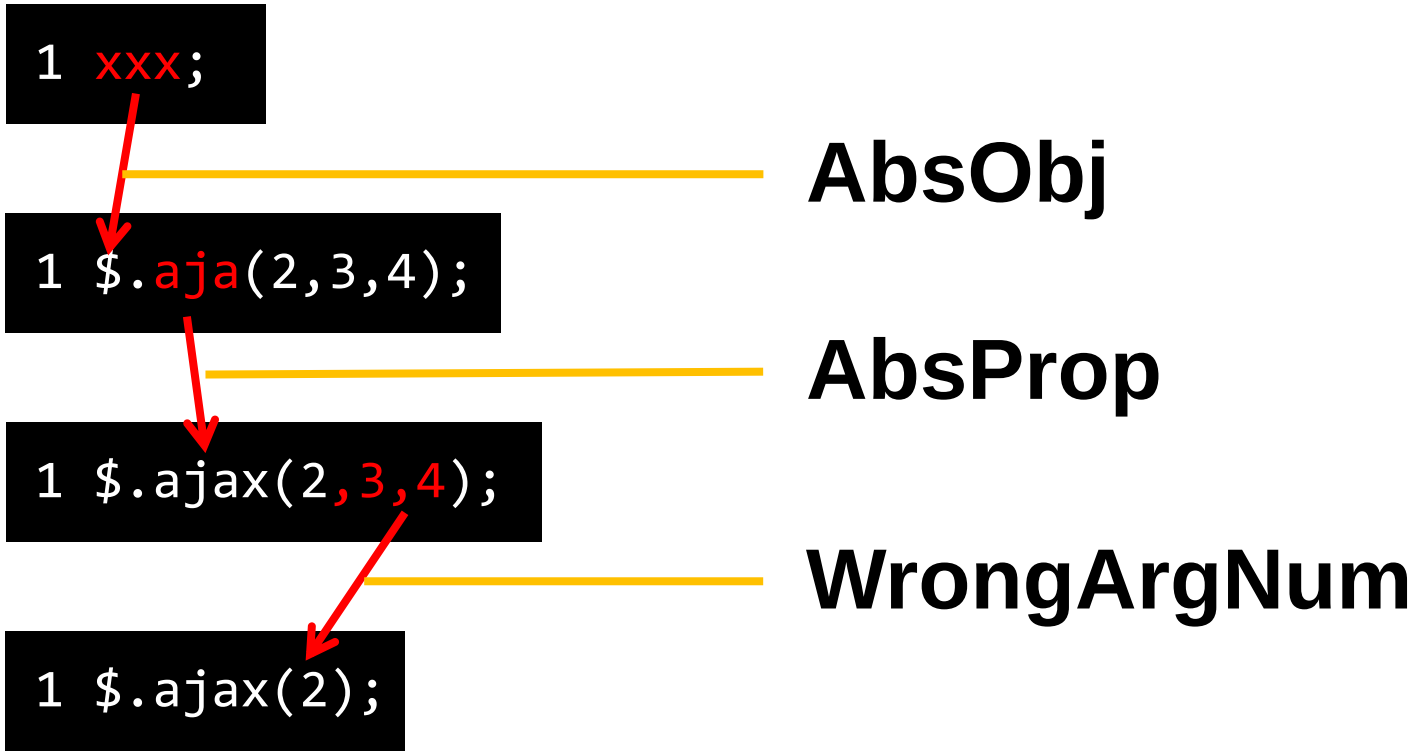
```
1 xxx;
```

JavaScript API Misuses

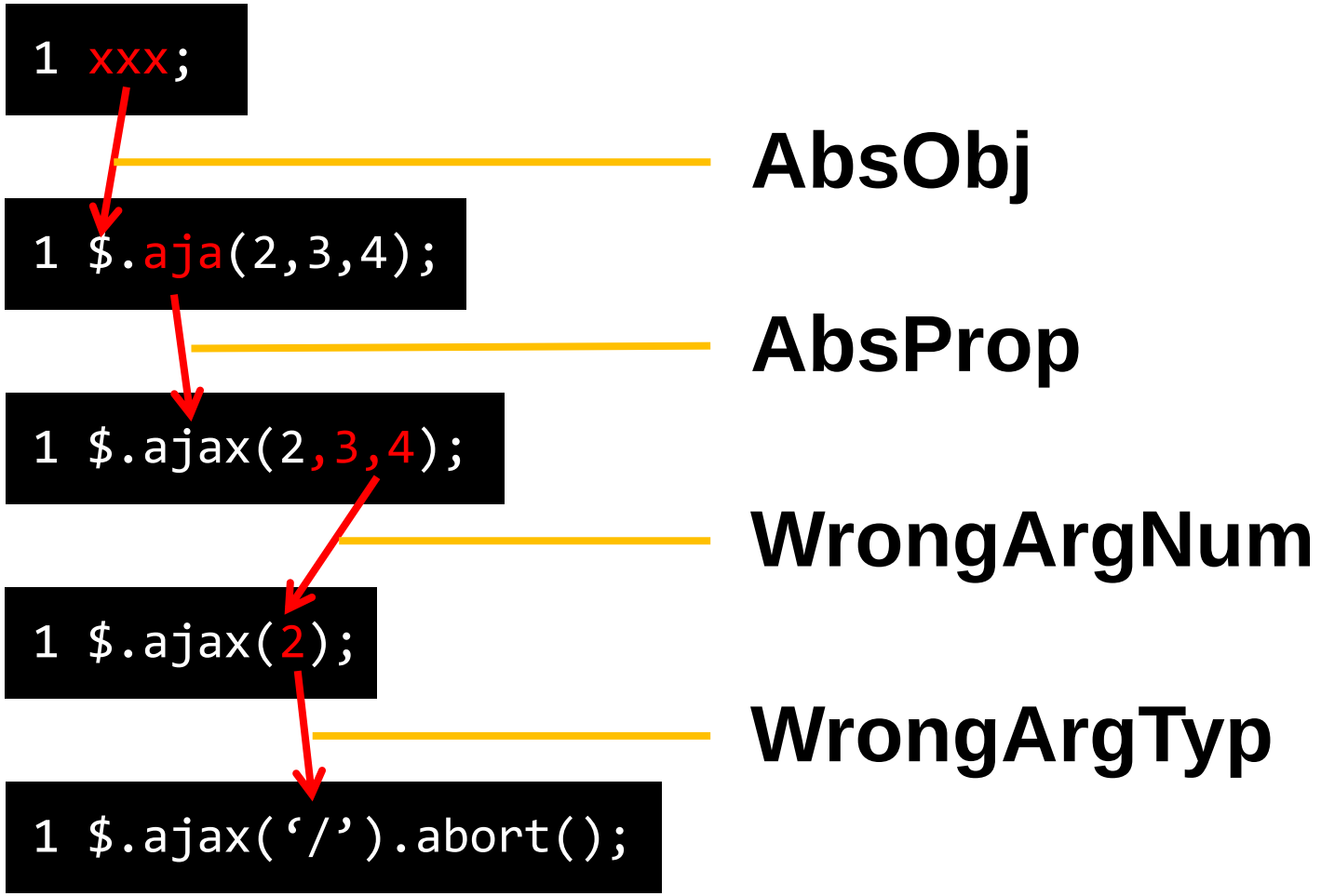
JavaScript API Misuses



JavaScript API Misuses



JavaScript API Misuses

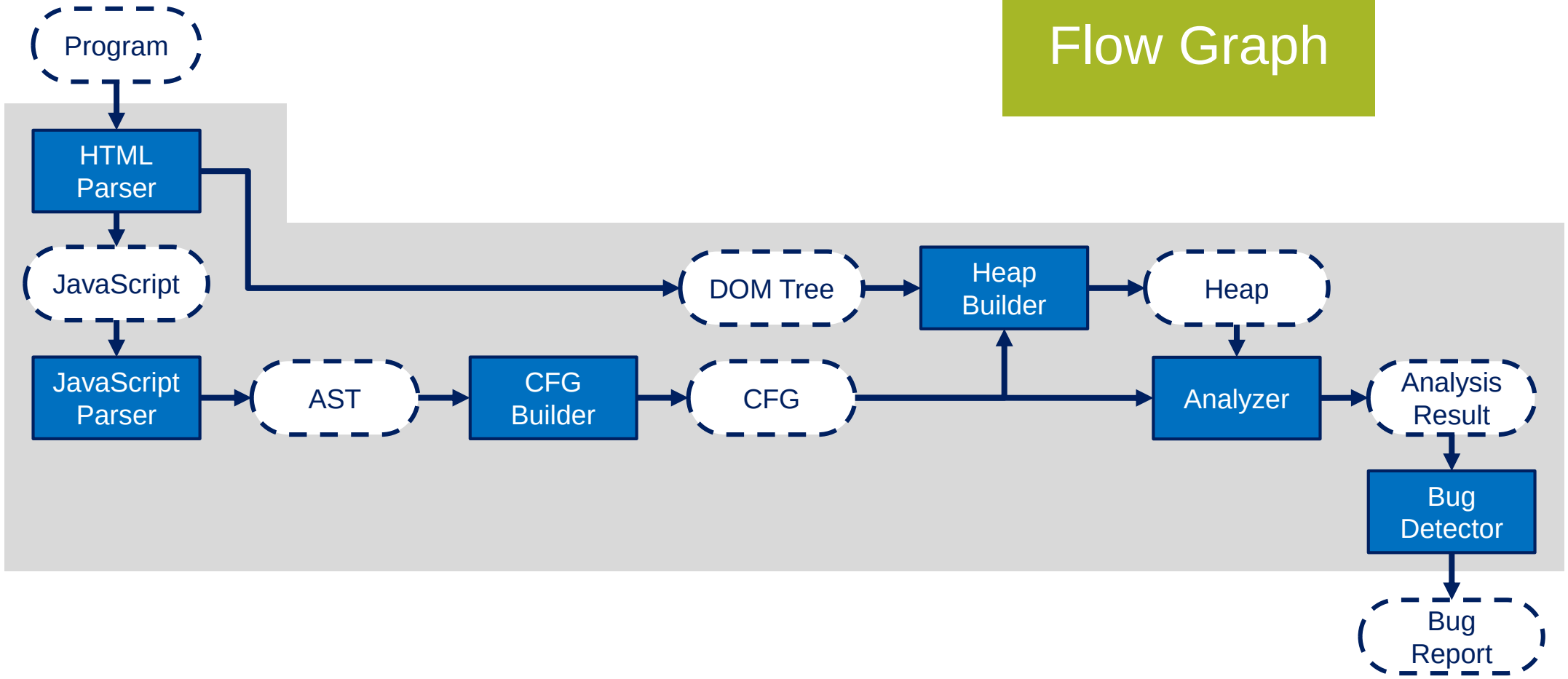


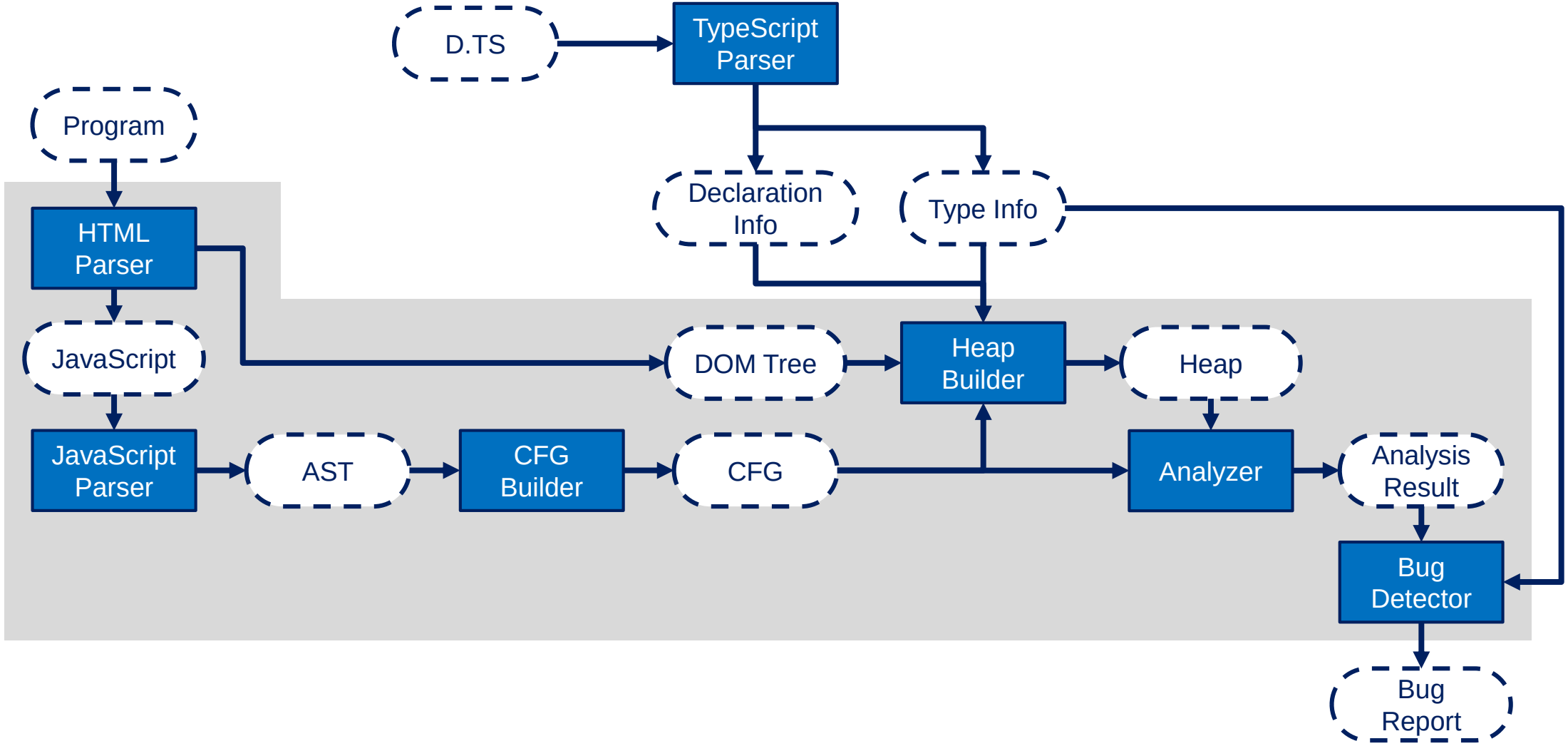
Methodology

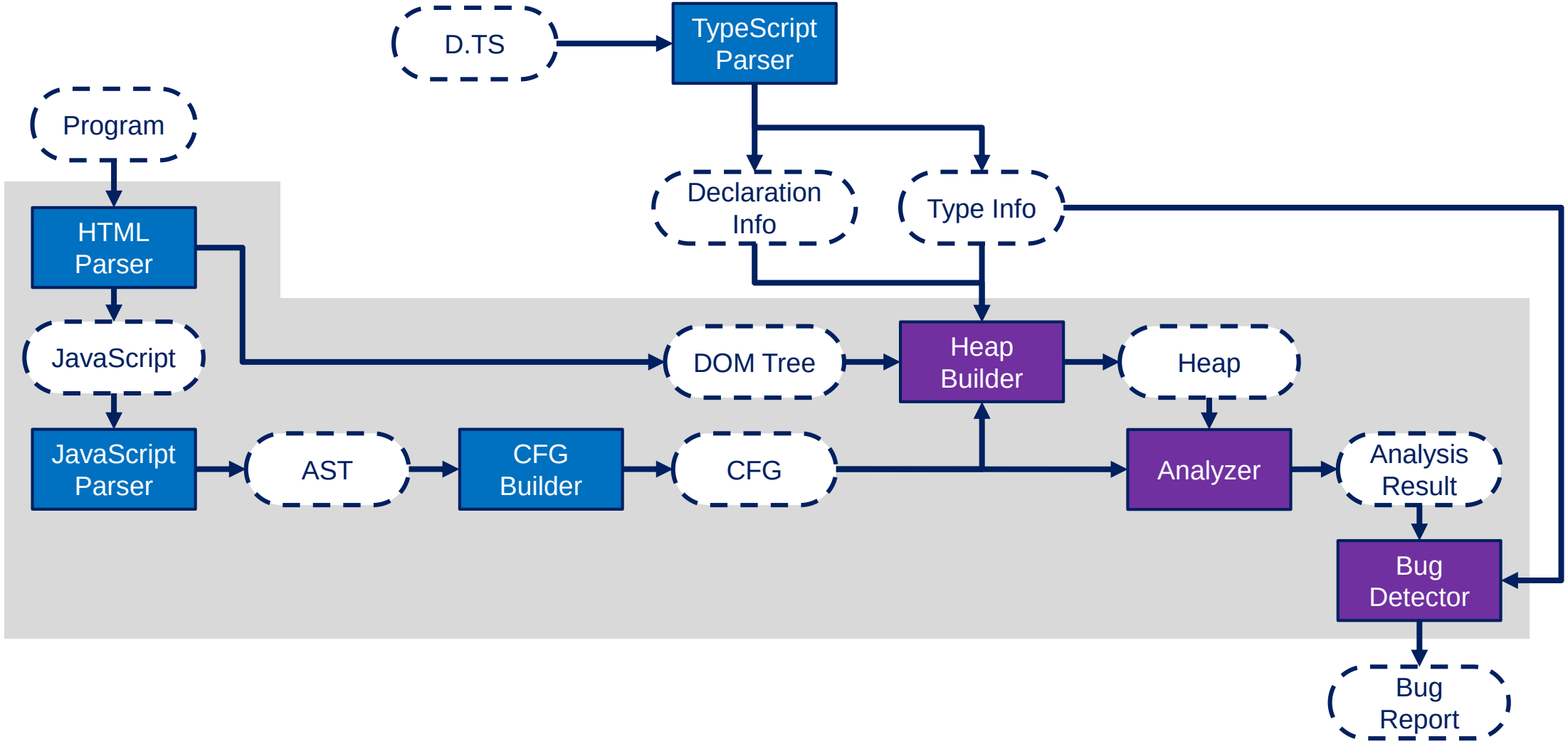
- Extend SAFE – Scalable Analysis Framework for ECMAScript

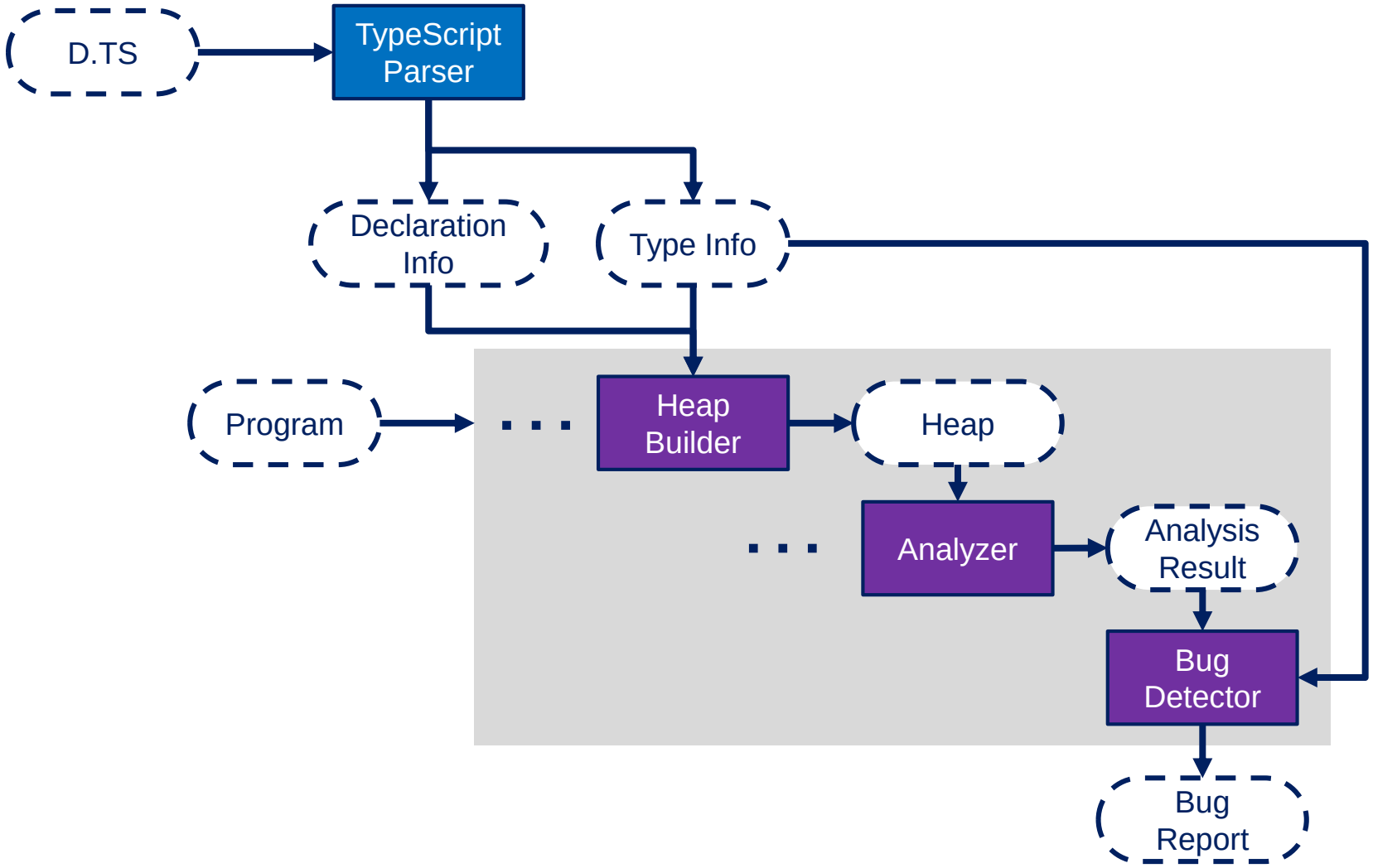
  - DefinitelyTyped
  - TypeScript parser
  - Mock-up object
  - Misuse detection

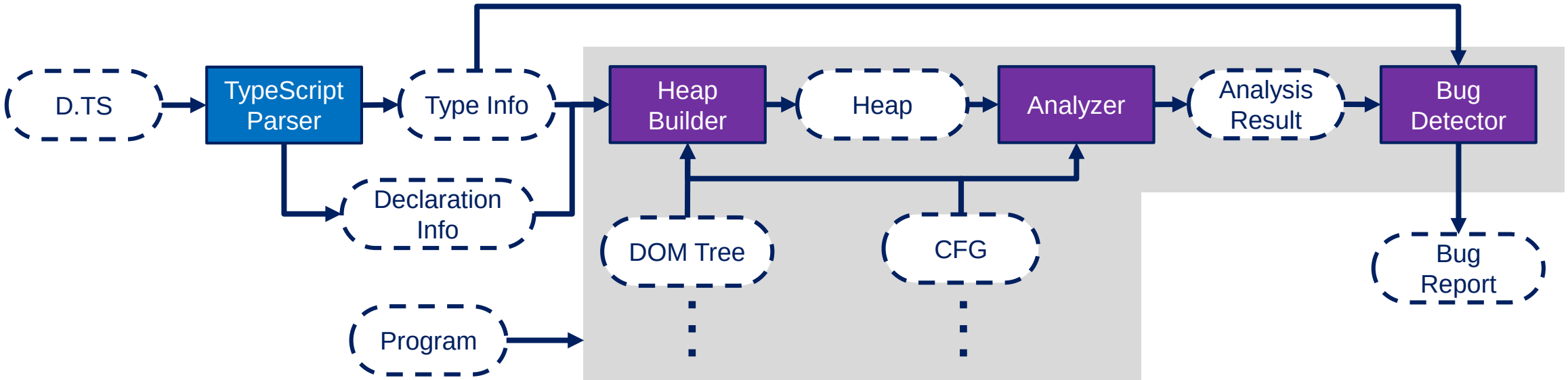
SAFE Flow Graph



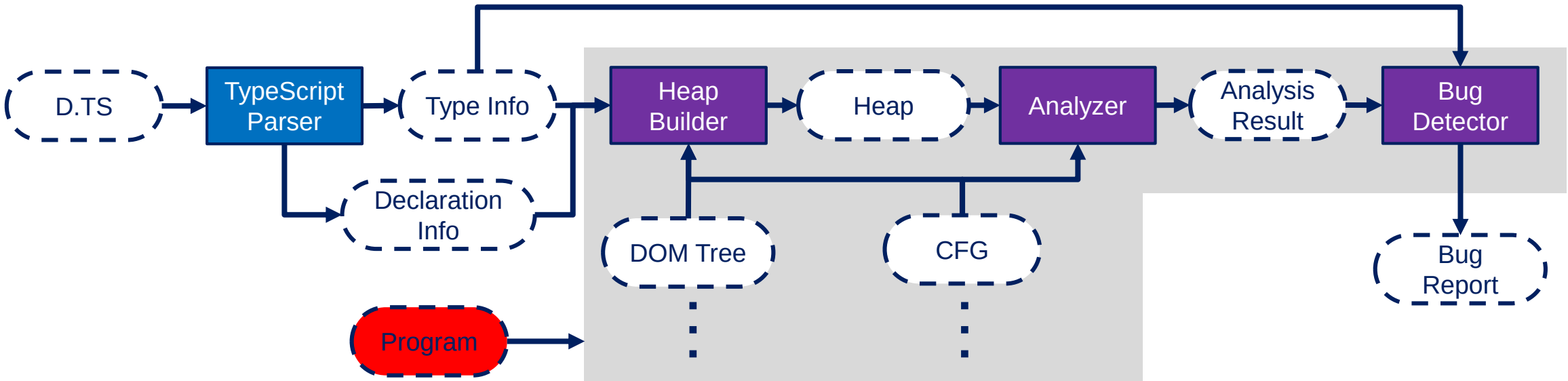

D.TS
TypeScript Parser
Program
HTML Parser
Declaration Info
Type Info
JavaScript
DOM Tree
Heap Builder
Heap
JavaScript Parser
AST
CFG Builder
CFG
Analyzer
Analysis Result
Bug Detector
Bug Report


D.TS
TypeScript Parser
Program
HTML Parser
Declaration Info
Type Info
JavaScript
DOM Tree
Heap Builder
Heap
JavaScript Parser
AST
CFG Builder
CFG
Analyzer
Analysis Result
Bug Detector
Bug Report

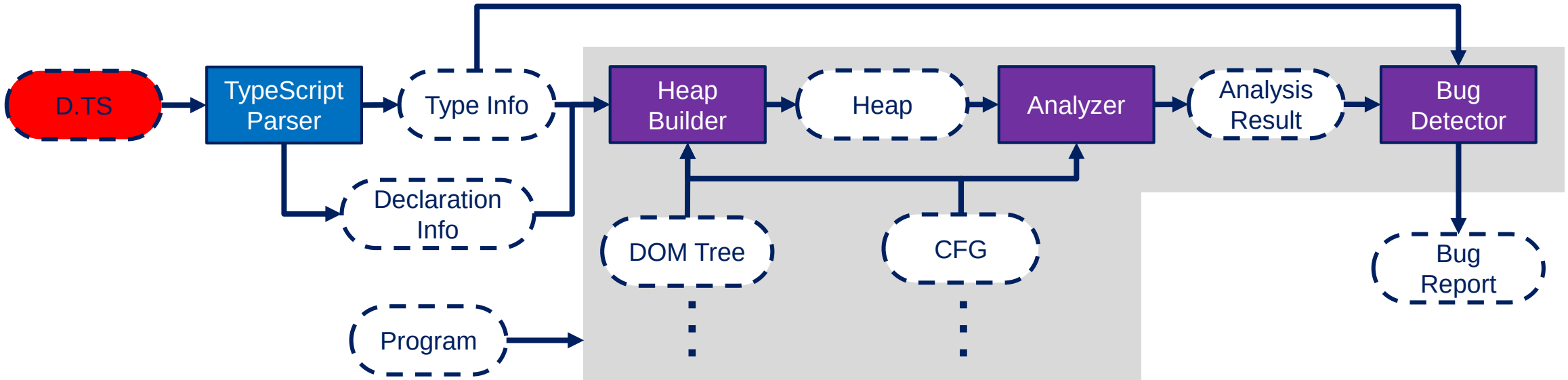

D.TS
TypeScript Parser
Declaration Info
Type Info
Program
Heap Builder
Heap
Analyzer
Analysis Result
Bug Detector
Bug Report


D.TS
TypeScript Parser
Type Info
Declaration Info
Program
Heap Builder
Heap
Analyzer
Analysis Result
Bug Detector
DOM Tree
CFG
Bug Report

```
<html>
    <head>
        <script src="…/jquery.min.js"></script>
        <script>
            $.get('abc');
        </script>
    </head>
…
```



```
...
interface JQeuryStatic {
    ...
    get(index?: number): any;
    ...
}
declare var $: JQueryStatic;
```

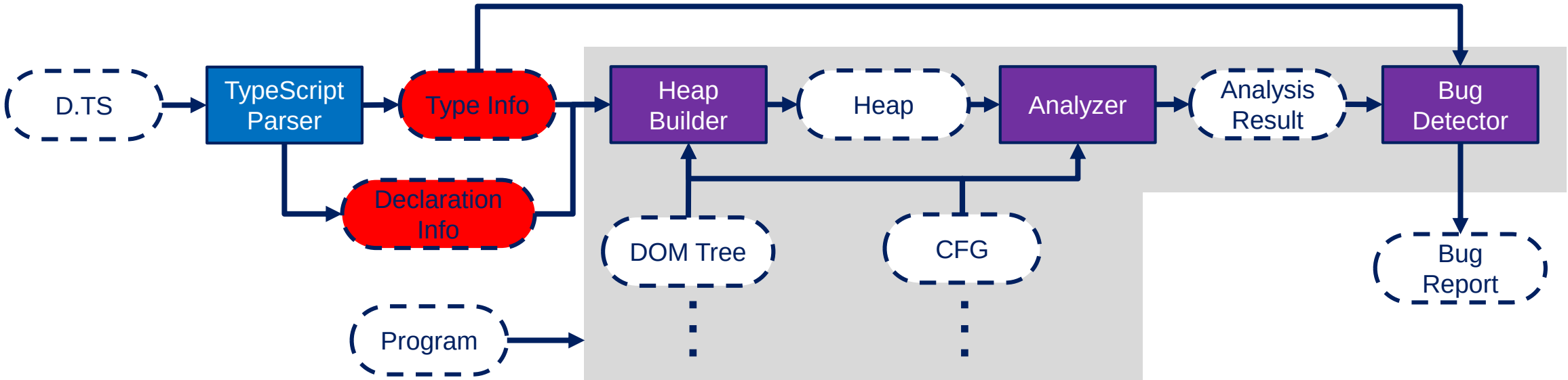


Type Info

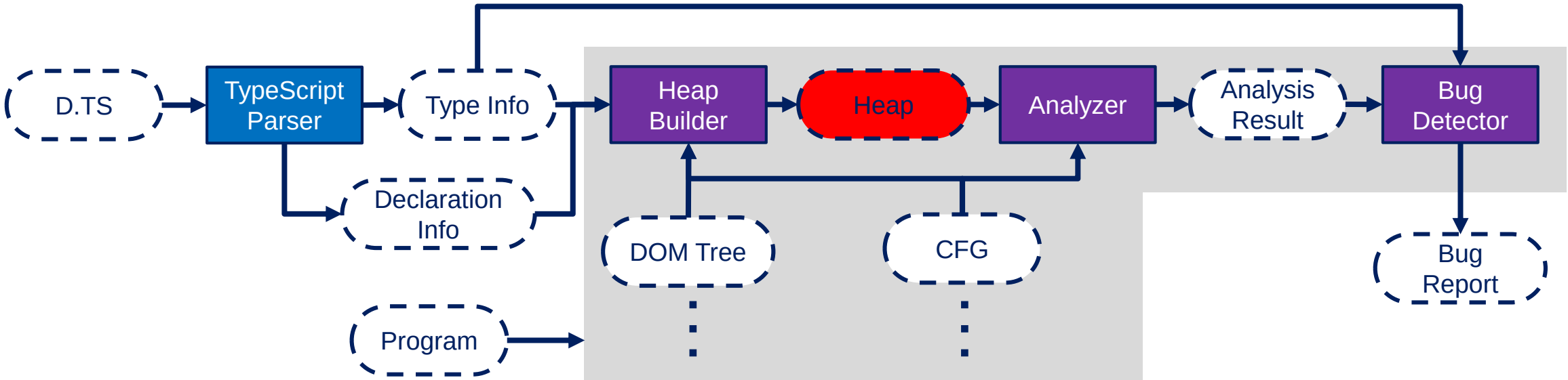
<NAME>		<AST NODE>
JQueryStatic	→	<InterfaceNode>
JQueryParam	→	<InterfaceNode>
...		

Declaration Info

<NAME>		<AST NODE>
$	→	<VarNode>
jQuery	→	<VarNode>
...		



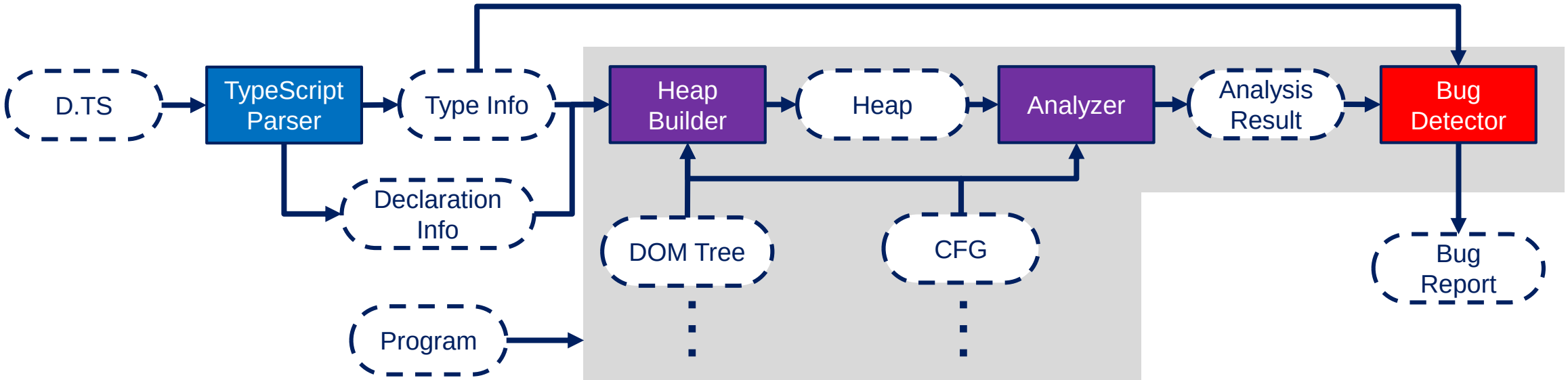
```
        <LOC>                          <Mock-up Object>

-2 (global)              →     { $ :  Loc(-1585)
                                 ... }
-1585 (JQueryStatic)     →     { get : Loc(-1586)
                                 ... }
-1586                    →     <FunctionObject>
                         ...
```

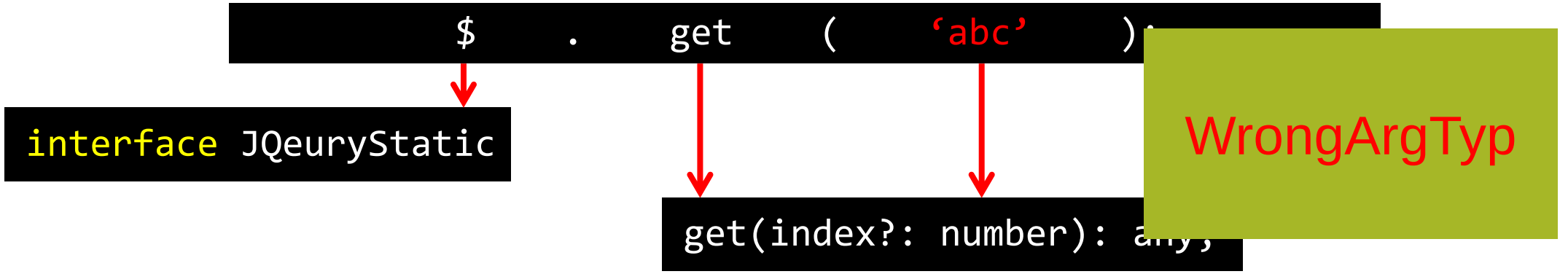


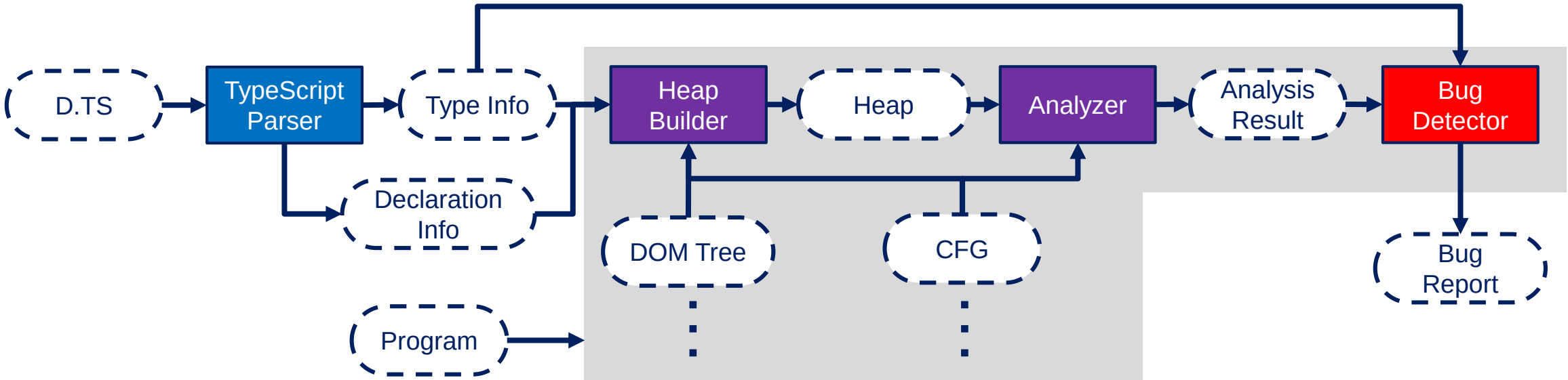
```
$ . get ( 'abc' );
```

```
interface JQeuryStatic
```

```
get(index?: number): any;
```




$. get ('abc'):
interface JQeuryStatic
get(index?: number): any;
WrongArgTyp


D.TS
TypeScript Parser
Type Info
Declaration Info
Program
Heap Builder
Heap
Analyzer
Analysis Result
Bug Detector
DOM Tree
CFG
Bug Report

Evaluation

- ExtJS 4.2 samples
  - http://docs.sencha.com/extjs/4.2.2/extjs-build/examples/

Name	Size (Kb)	Time (s)	Error
Feed Viewer	82.3	6.156	X
Ext JS Calendar	265.8	10.489	StatusProxy.js : AbsObj – Ext.baseCSSPrefix
Web Desktop	78.3	7.564	X
Portal Demo	30.9	6.072	X
Tiger	108.8	5.751	X
KitchenSink	33.7	6.716	X

Conclusion

- Developed a tool to detect misuses of JavaScript APIs by using TypeScript declaration files
- Found a “bug” in the ExtJS 4.2 documentation