```
contract Attacker {
  Victim v;

  function exploit() {
    v = Victim(0x123);
    v.??;
  }

  function () payable {
    v.??;
  }
}
```

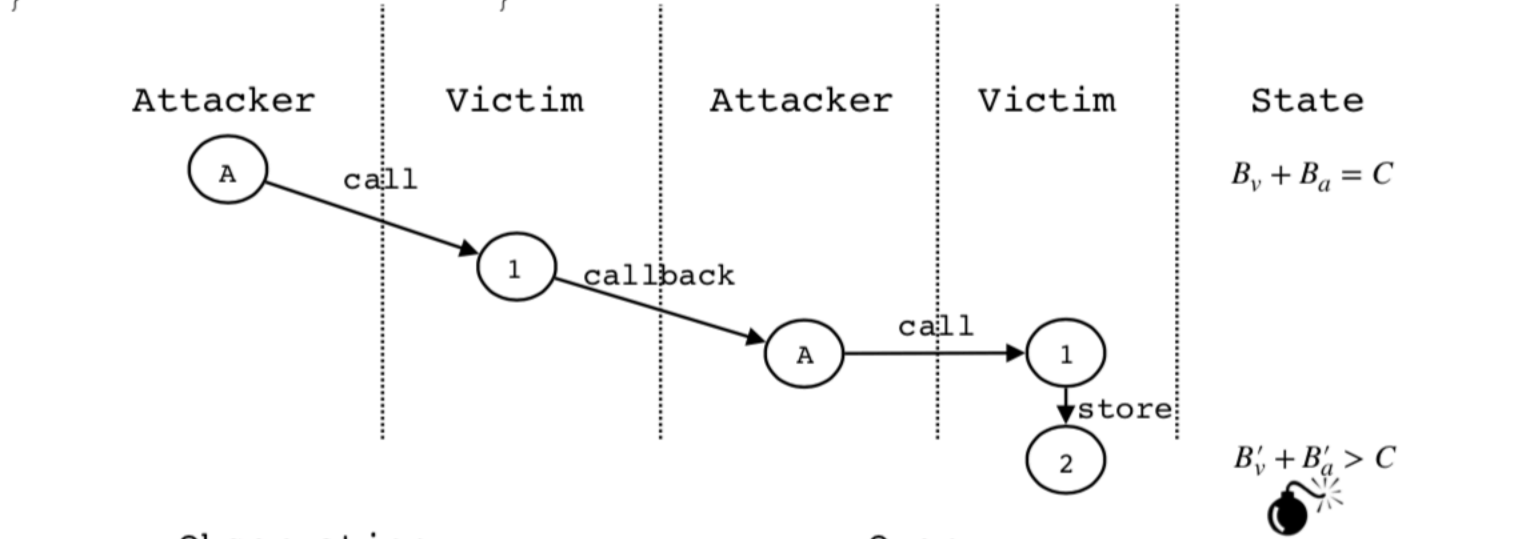
(1) attack template

```
contract Attacker {
  Victim v;

  function Attacker() {
    v = Victim(0x123);
    v.withdraw(10);
  }

  function () payable {
    v.withdraw(10);
  }
}
```

(2) attack program

```
contract Victim {
  ...
  function withdraw(uint a){
  1 msg.sender.call.value(a);
  2 bal[msg.sender] -= a;
  }
}
```

(3) victim program



Observation:

call+call*…store

Query:

$$\exists\, i, j, k, call, call', store .\ \ i < j < k \ \wedge call_{loc} = i \wedge call'_{loc} = j \wedge\ store_{loc} = k \ \wedge\ call.gas > 2300$$