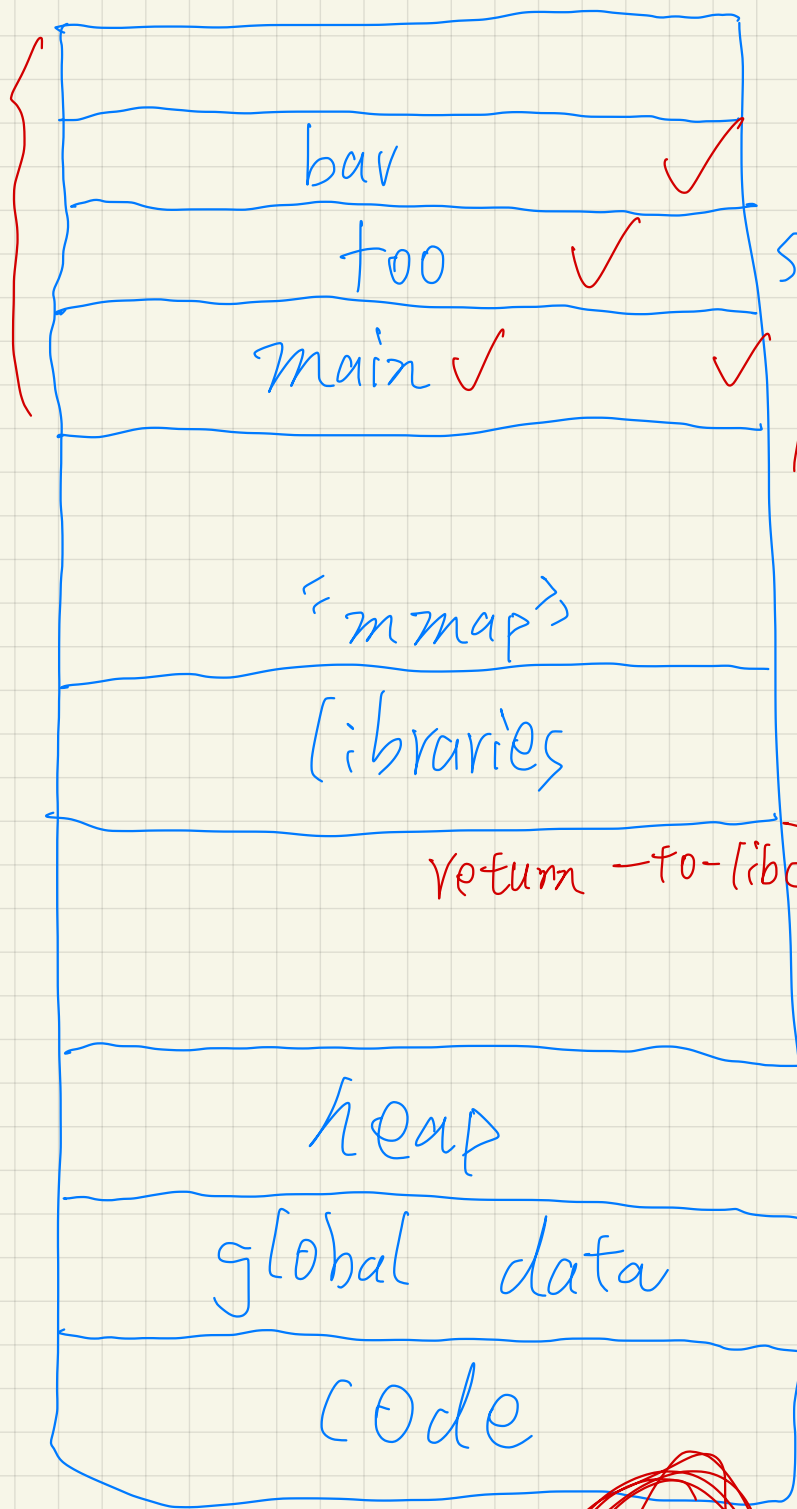


memory layout:



stack

(1) *
1988 }

fooC

(2) *
2005 }

return -to-libc

barC

(3) *

(4)

rop

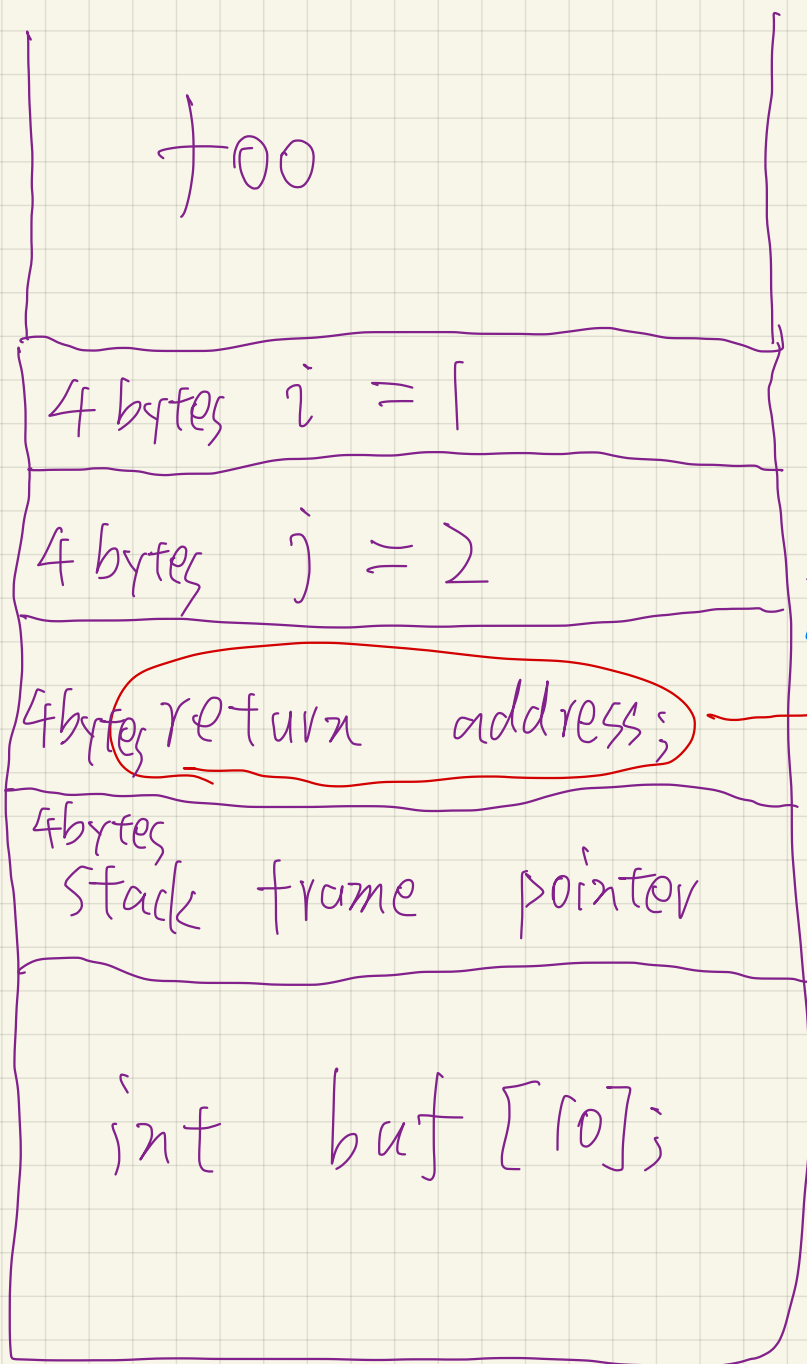
2012 }

*
main C
}
}

int a;
foo(a);

bar(); *
return;

return; *



```
int foo()
{
```

```
    bar(1, 2);
    int (= 13);
    return;
}
```

```
int bar(int i, int j)
```

```
int buf[10];
```

```
return 0;
```


tamper buf \Rightarrow 40 bytes + 4 bytes

tamper buf \Rightarrow 40 bytes + 4 bytes + 4 bytes

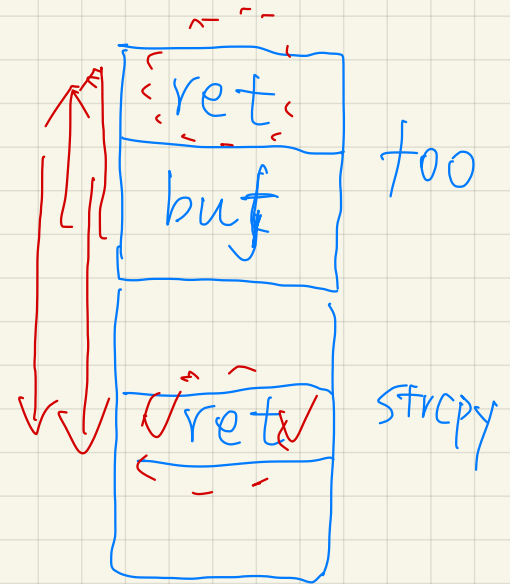
control flow hijacking

buf [40 bytes]

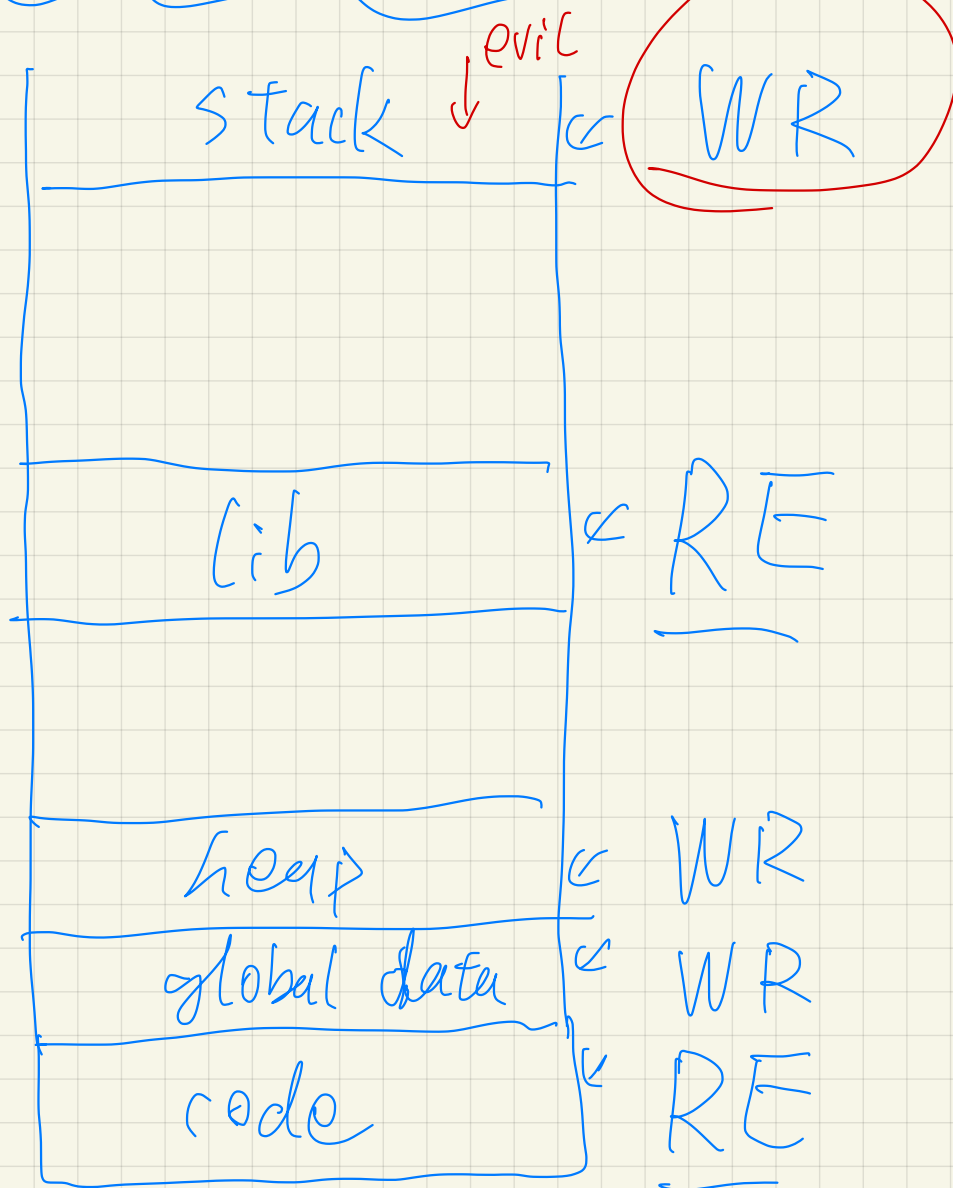
"payload" [evil code || 4 bytes || 4 bytes]



```
int foo ( char* s )  
{  
    int buf [10];  
    strcpy ( buf , s );  
}
```



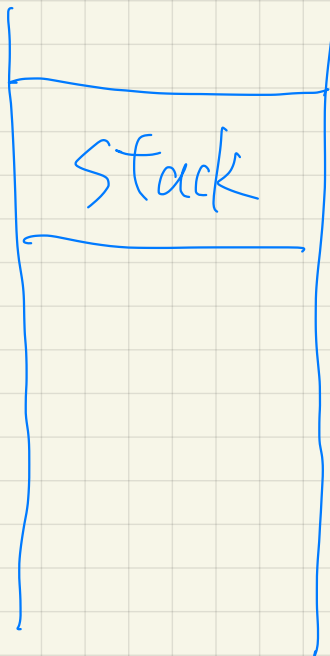
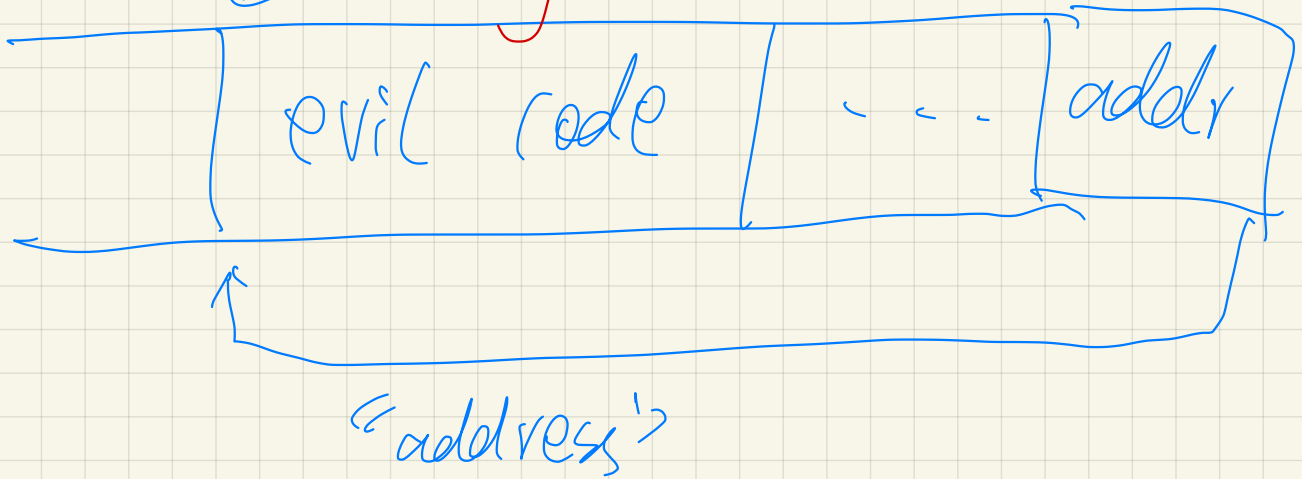
W XOR E:



R WE

ASLR:

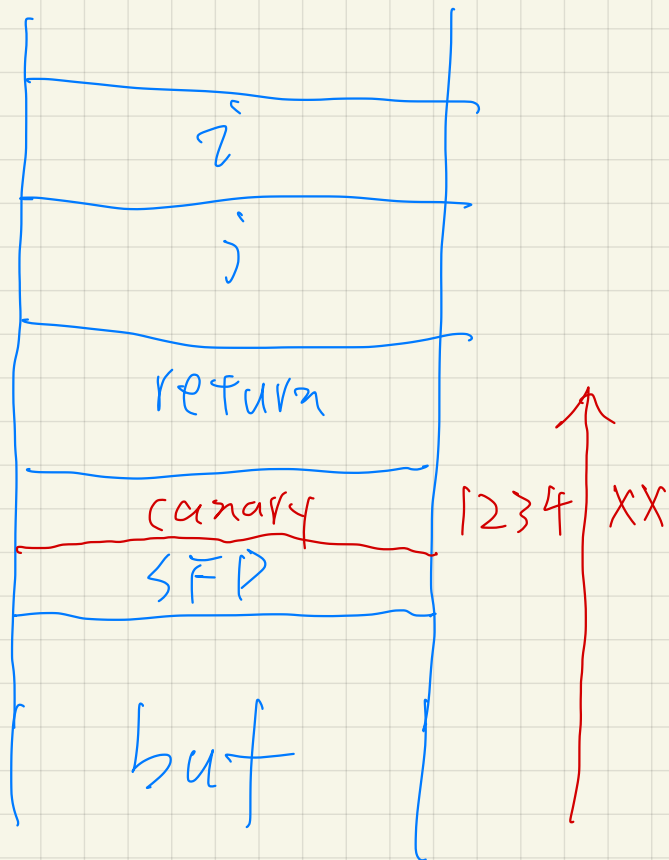
✓ changed



✓ beginning address

$2^6 \sim 2^8$

stack canary:



```
int foo( )
```

```
{
```

```
    allocate-canary;
```

```
    bar( );
```

```
}
```

```
int bar( )
```

```
{
```

```
    if (check-canary(1234))
```

```
    {
```

```
        abort;
```

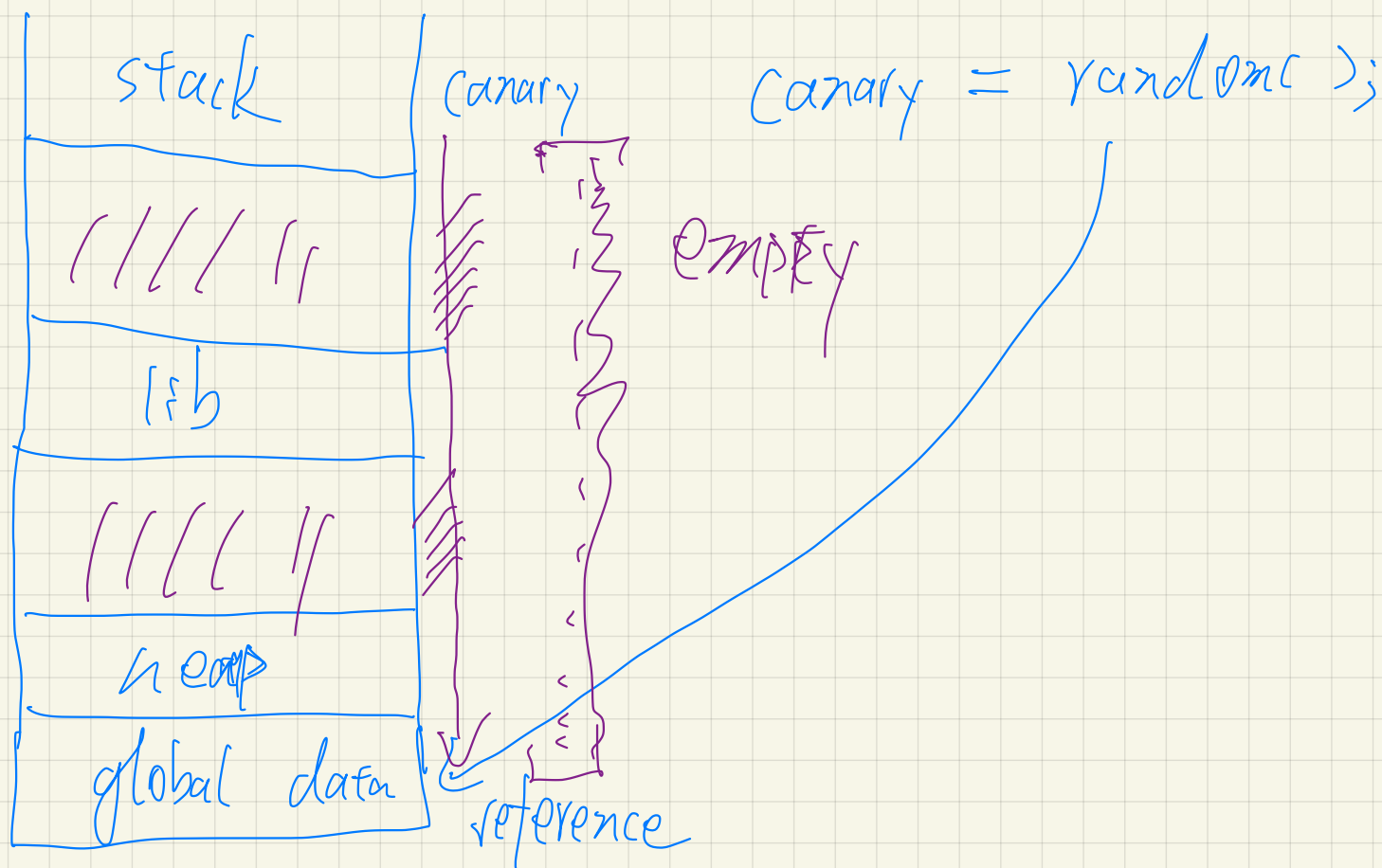
```
    }
```

```
    return;
```

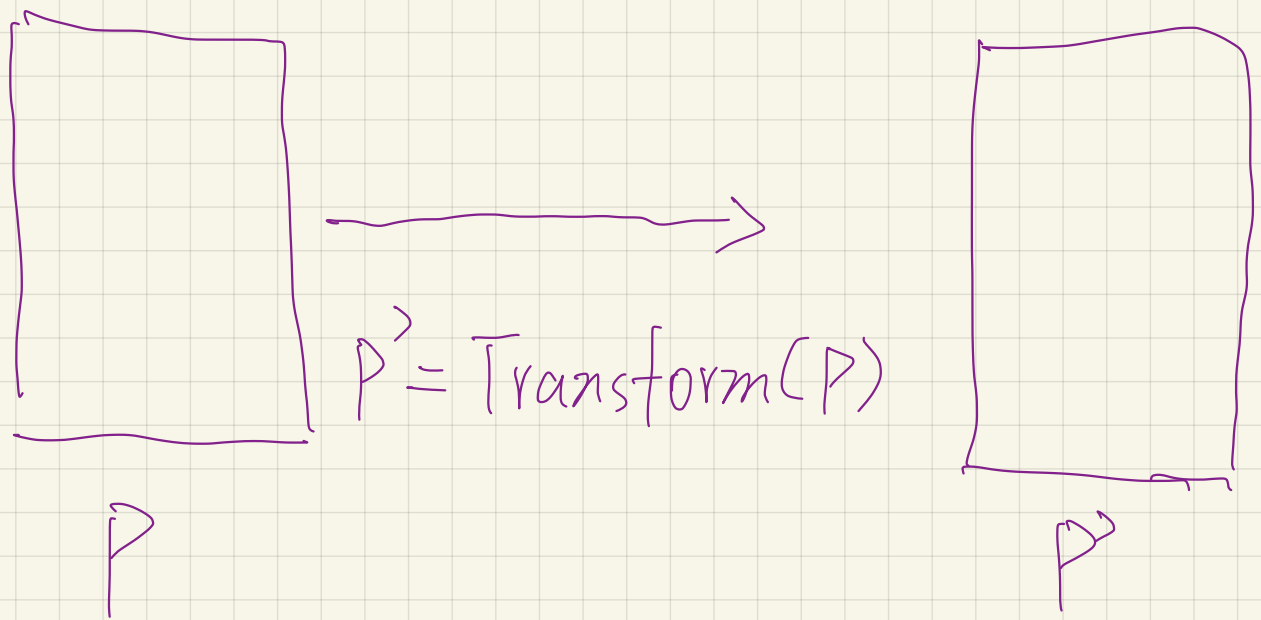
```
}
```

{evil || SFP || 1234 || addr}





// segment faults



$\left\{ \begin{array}{l} P \\ P' \end{array} \right. \Rightarrow \begin{array}{l} \textcircled{1} \text{ visually different} \\ \textcircled{2} \text{ identical functionality} \end{array}$

Obfuscation

software security analysis \Rightarrow similar
 $P \quad P'$

$\textcircled{1}$ malware $\begin{array}{l} \rightarrow \text{signature} \\ \rightarrow \text{clustering} \end{array}$

$\textcircled{2}$ vulnerability (mining)
 detection

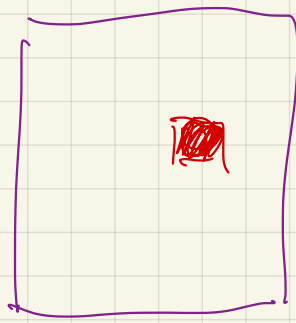
③

code clone

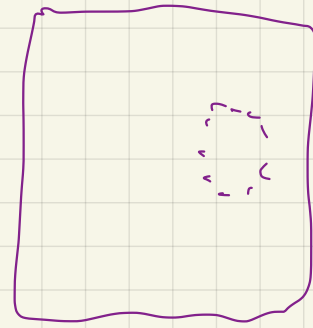
code plagiarism

④

patch-based attack



patched



unpatched

patched \Rightarrow obfuscated