Digital Interruption

Web Application Security

Web applications and the things that go wrong

Jahmel Harris

+44 (0)161-820-3056

www.digitalinterruption.com

jahmel@digitalinterruption.com

contact@digitalinterruption.com

MGH

Manchester Grey Hats

@mcrgreyhats

Hands on hacking….things!

Join our slack channel

Quiz!

Phreaking

31337

White Hat

Handle

0-day

Pwned

Black Hat

whoami

Security Consultant at Digital Interruption

@jayHarris_Sec

Mobile | Radio | Reverse Engineering

Why?

Proud of our software

Protecting our customers data

Reputational damage

Compliance

Release on time

(Do you know how expensive an external consultant is?)

What?

Hackazon

Sample of vulnerabilities

Questions? Ask!

Some technical content and explanation

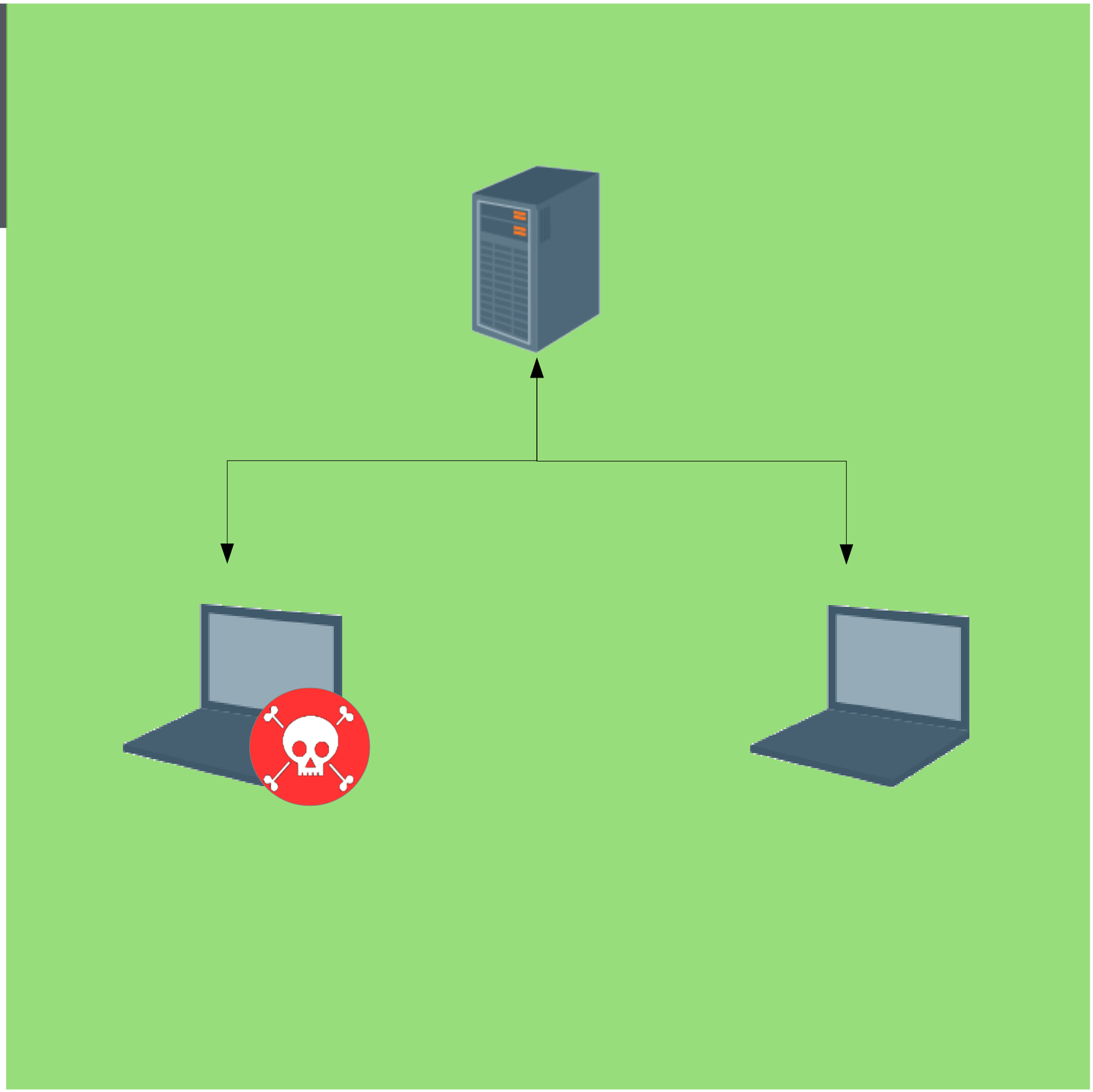
Disclaimer

ETHICAL hacking

Any actions and or activities related to the material contained within this presentation is solely your responsibility. The misuse of this information can result in criminal charges brought against the persons in question.

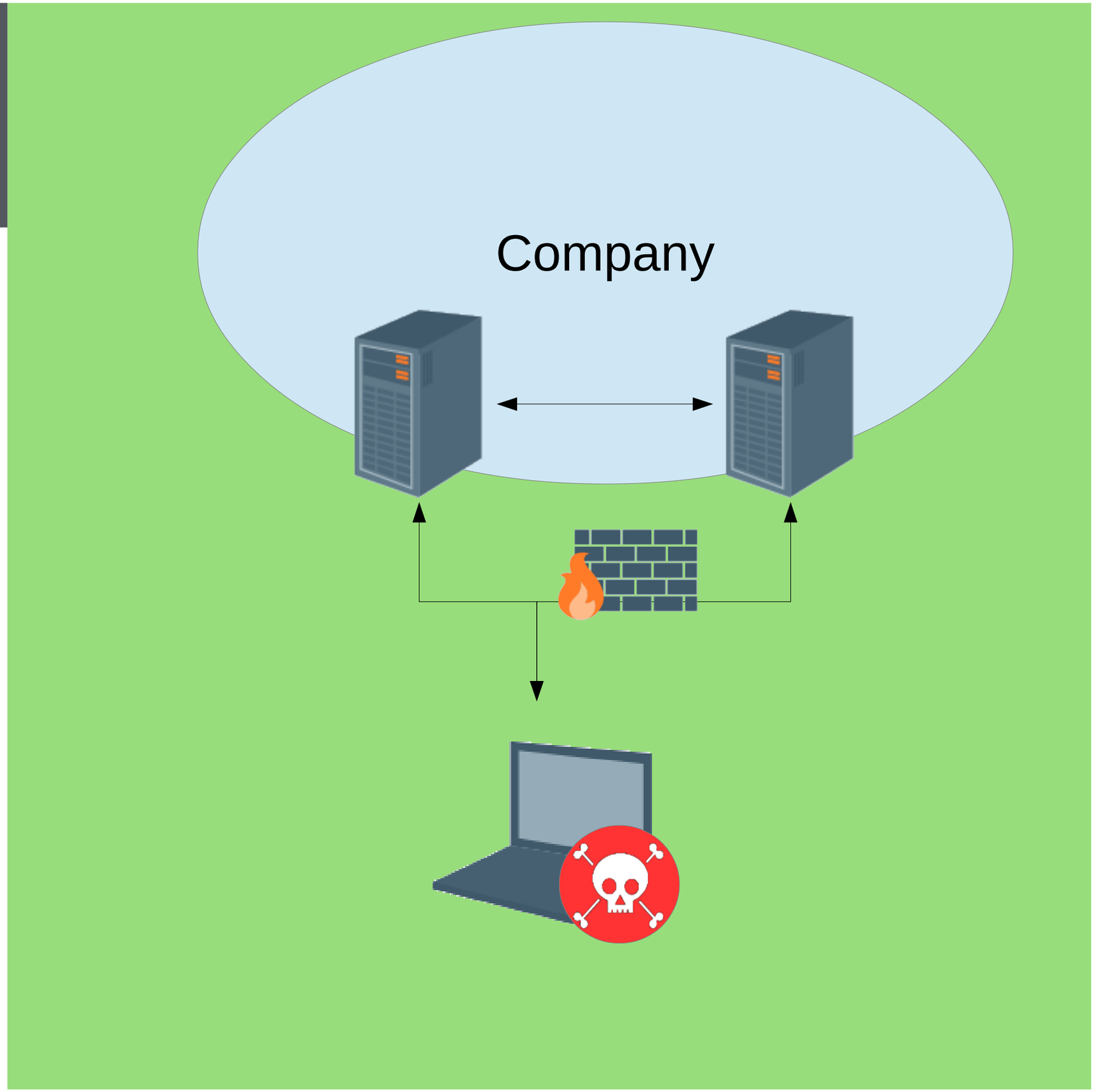
Hack to learn. Don't learn to hack.

Attacking user(s)



DIGITAL INTERRUPTION

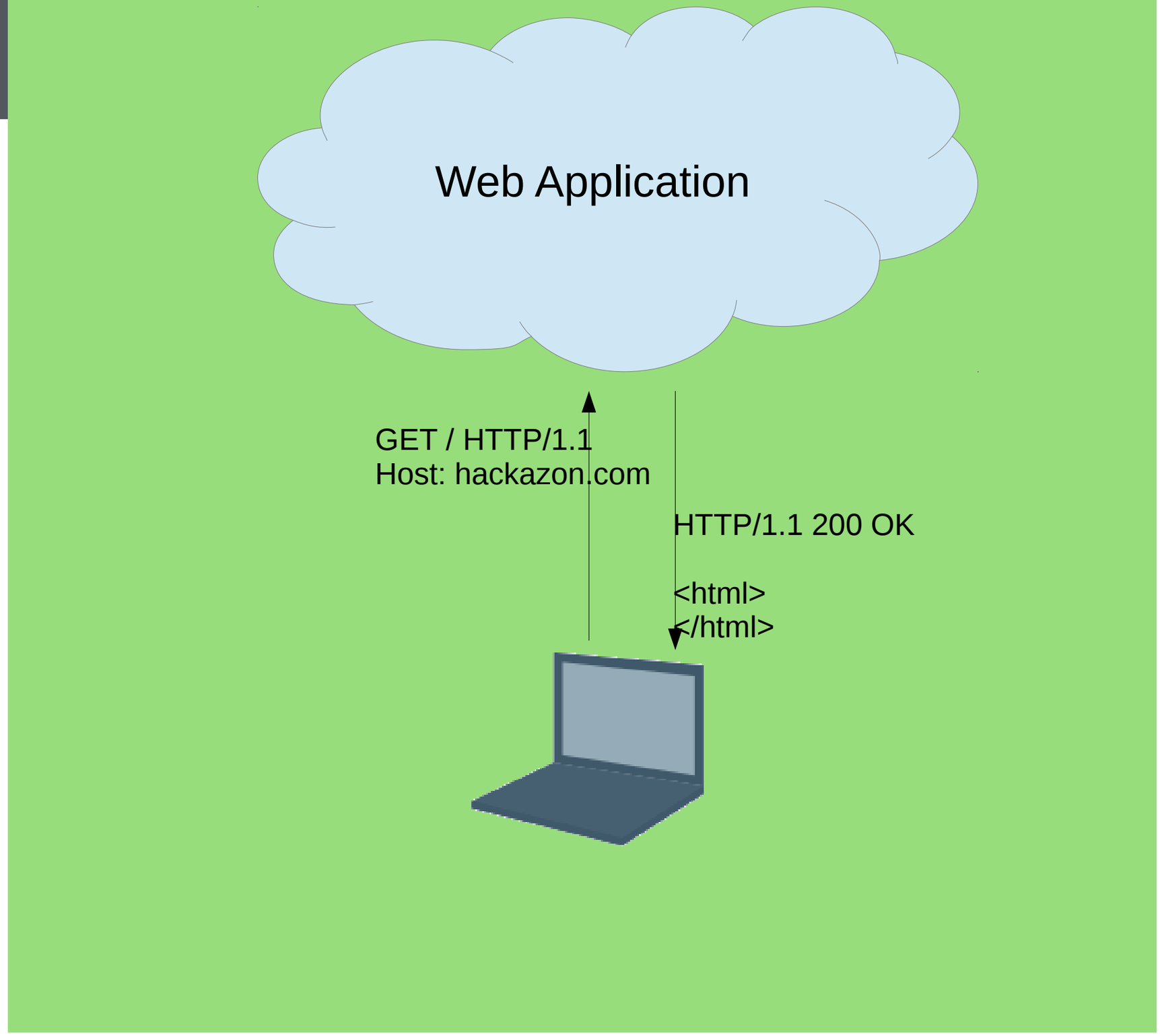
Attacking Servers



DIGITAL INTERRUPTION

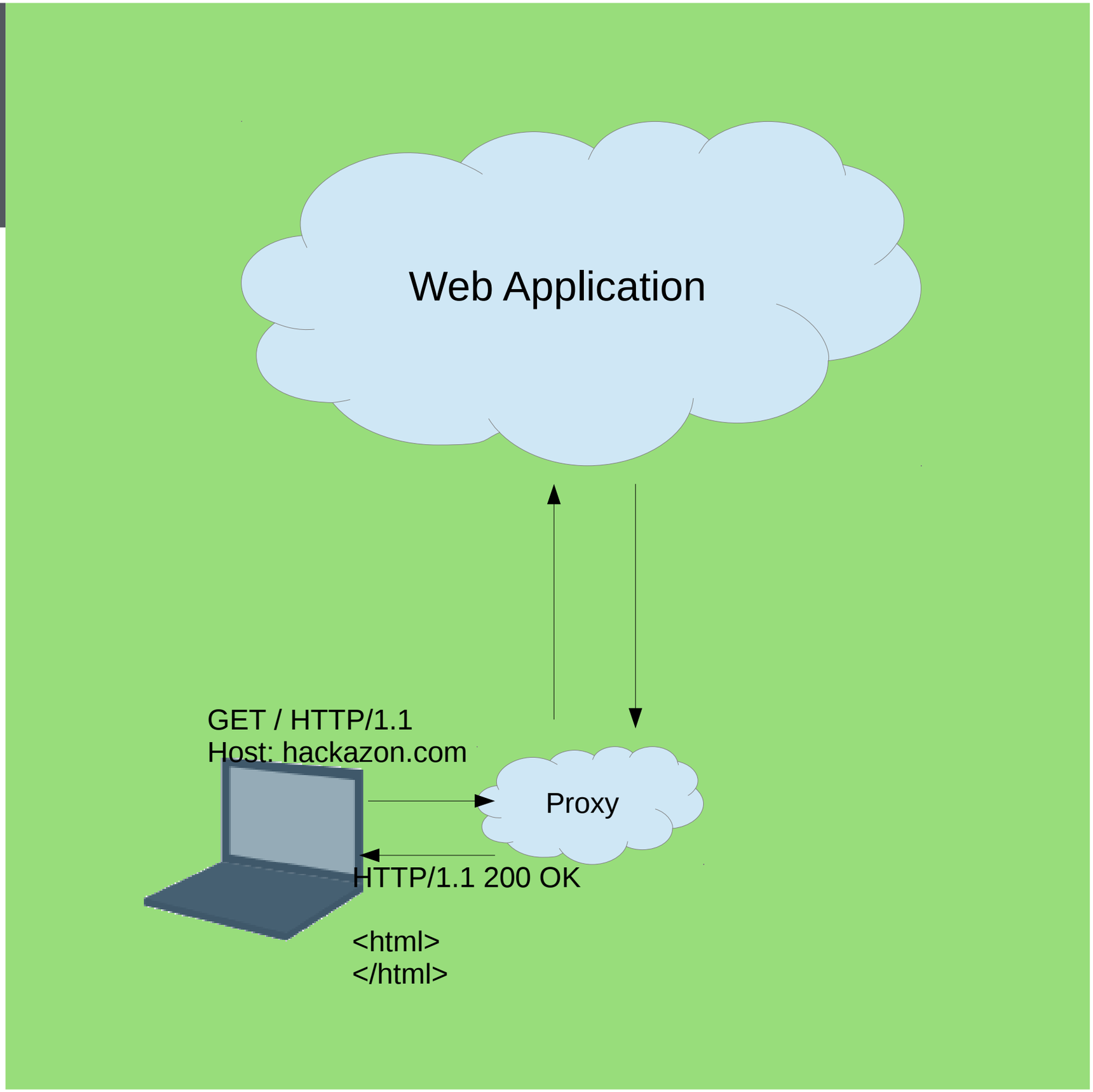
Let’s get hacking

Attacking Servers



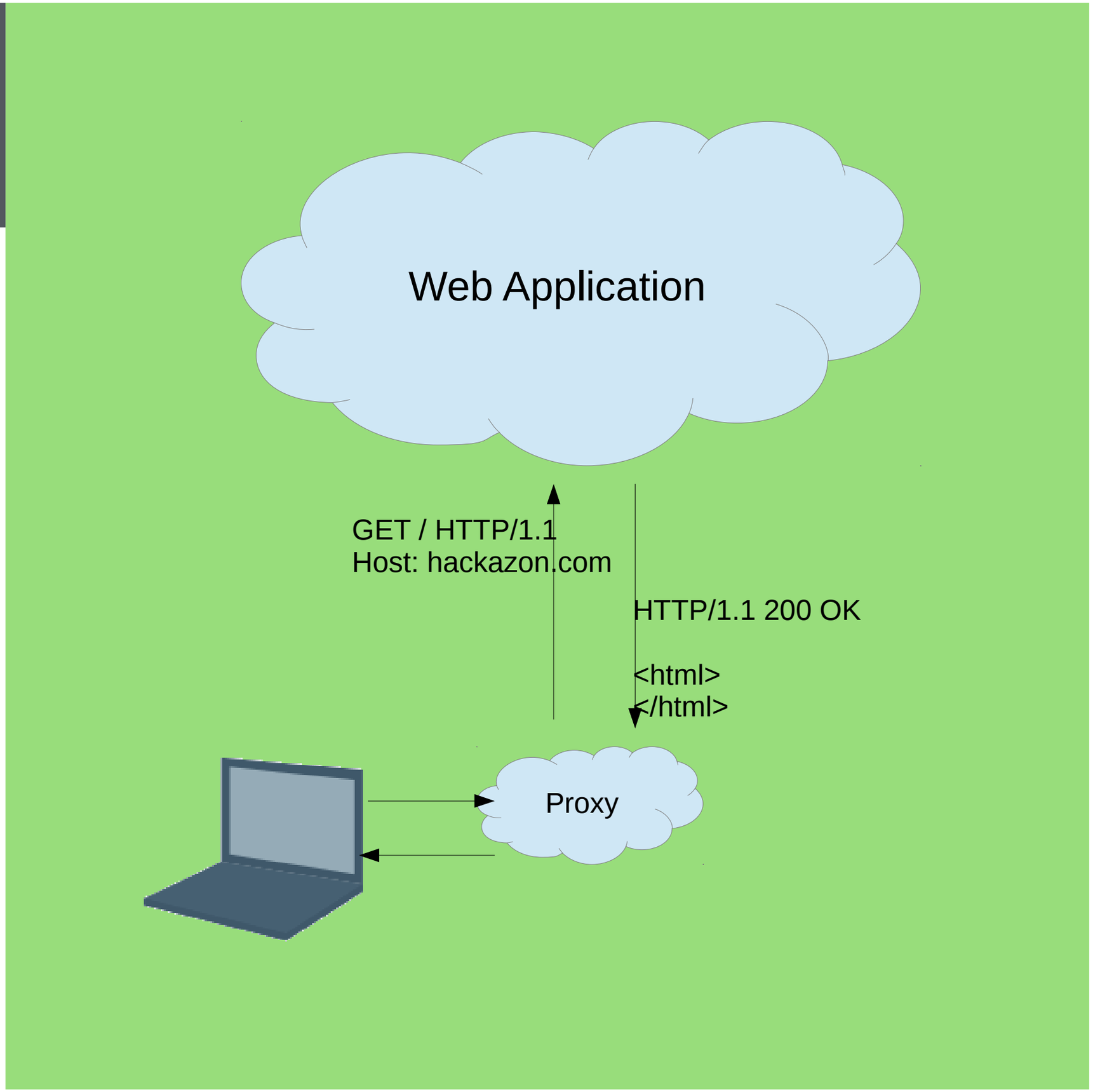
DIGITAL INTERRUPTION

Attacking Servers



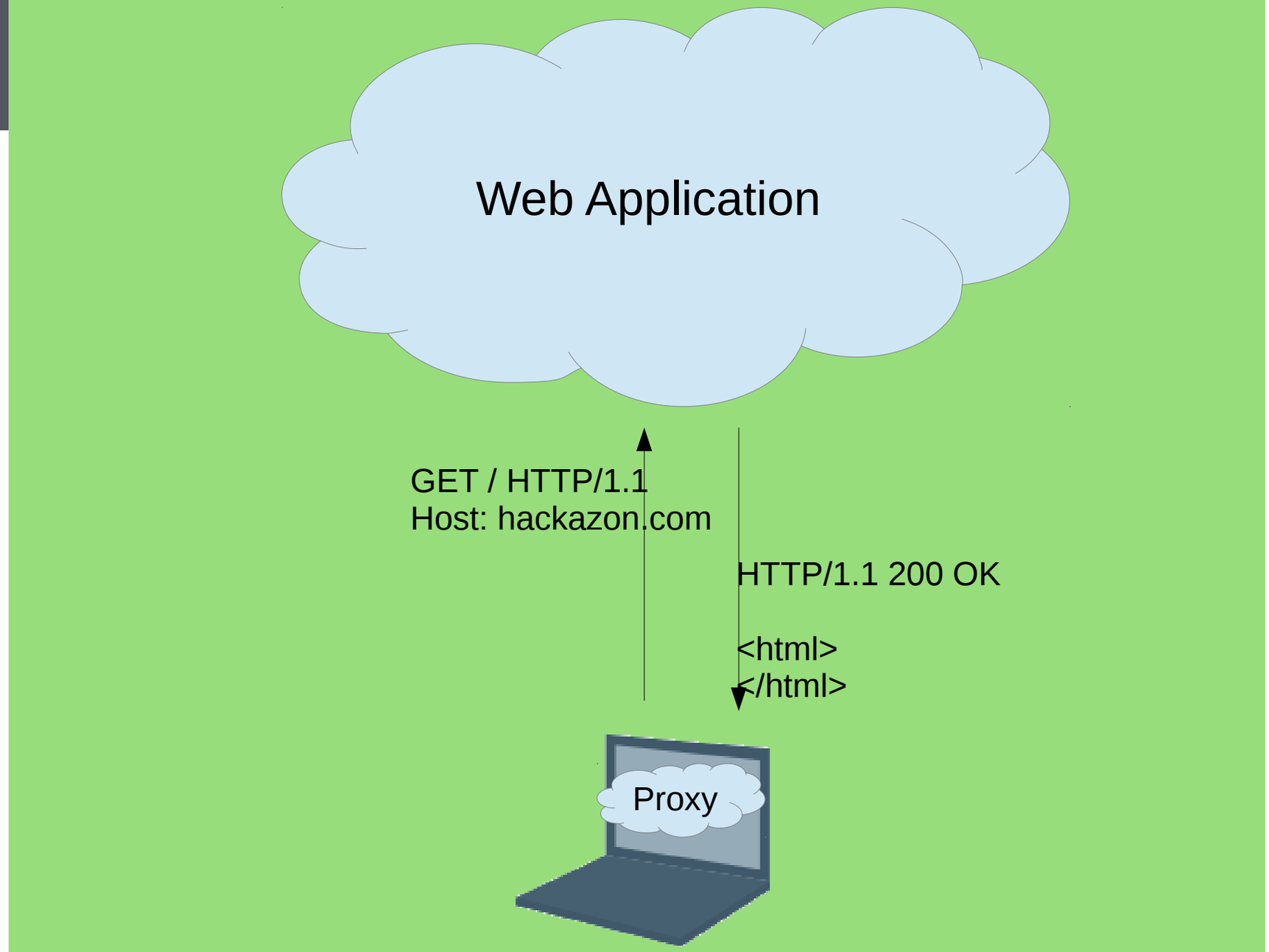
DIGITAL INTERRUPTION

Attacking Servers



DIGITAL INTERRUPTION

Attacking Servers

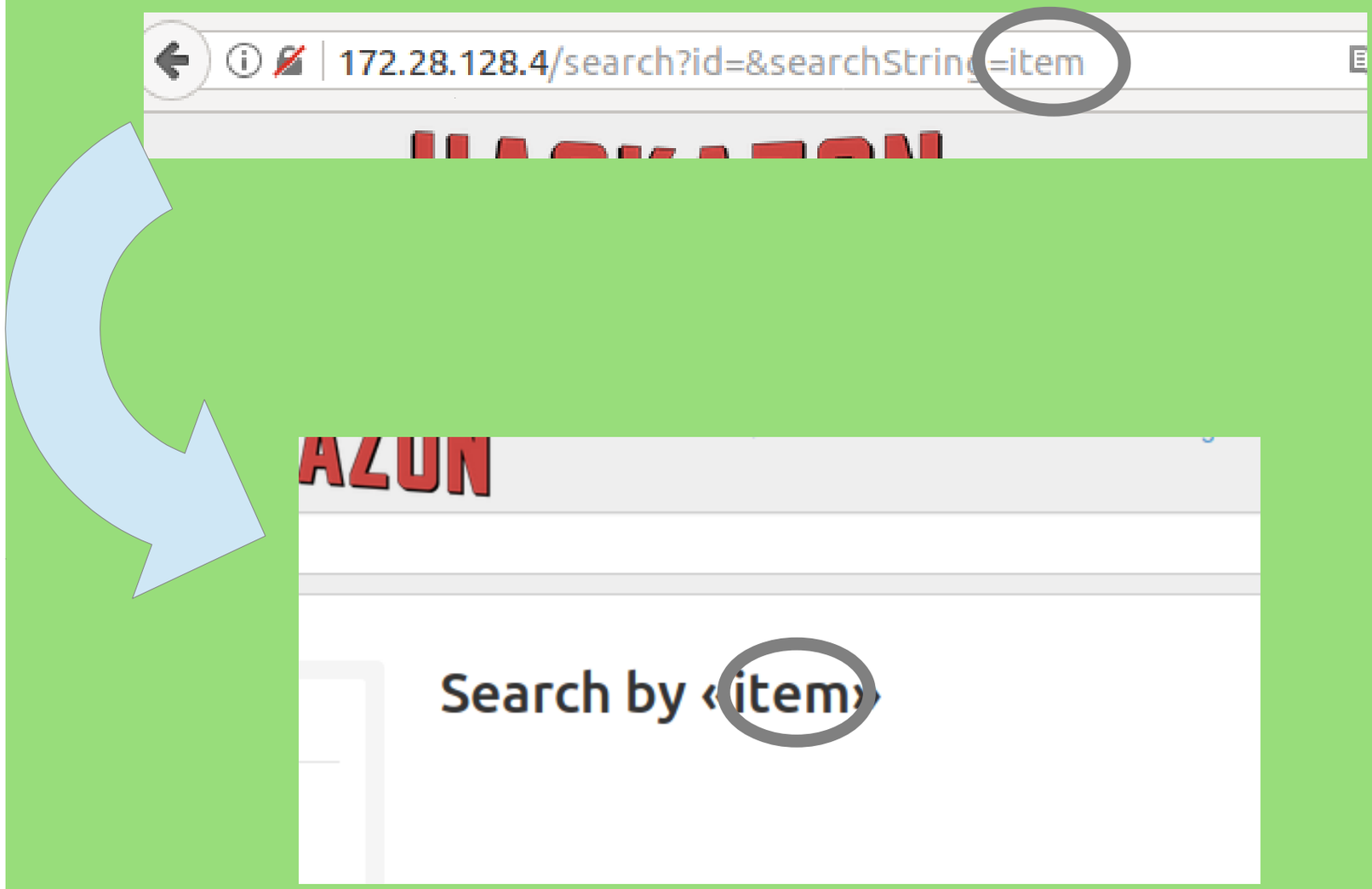


DIGITAL INTERRUPTION

Exercise 0
configuring the environment

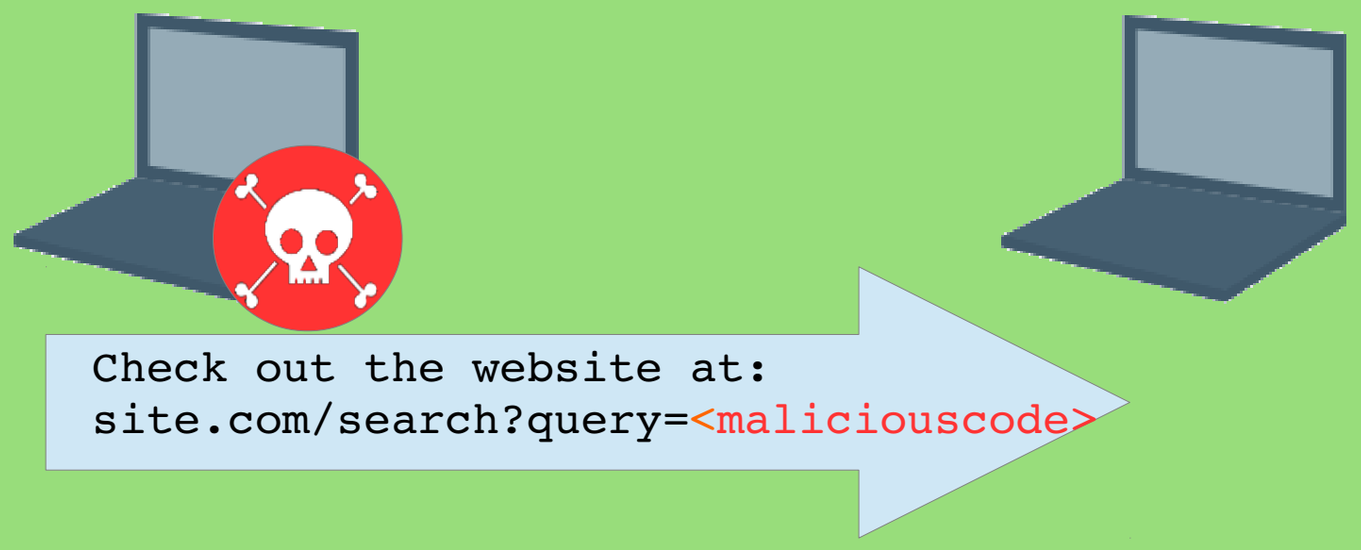
Exercise
Brute Force Attacks

Reflected XSS



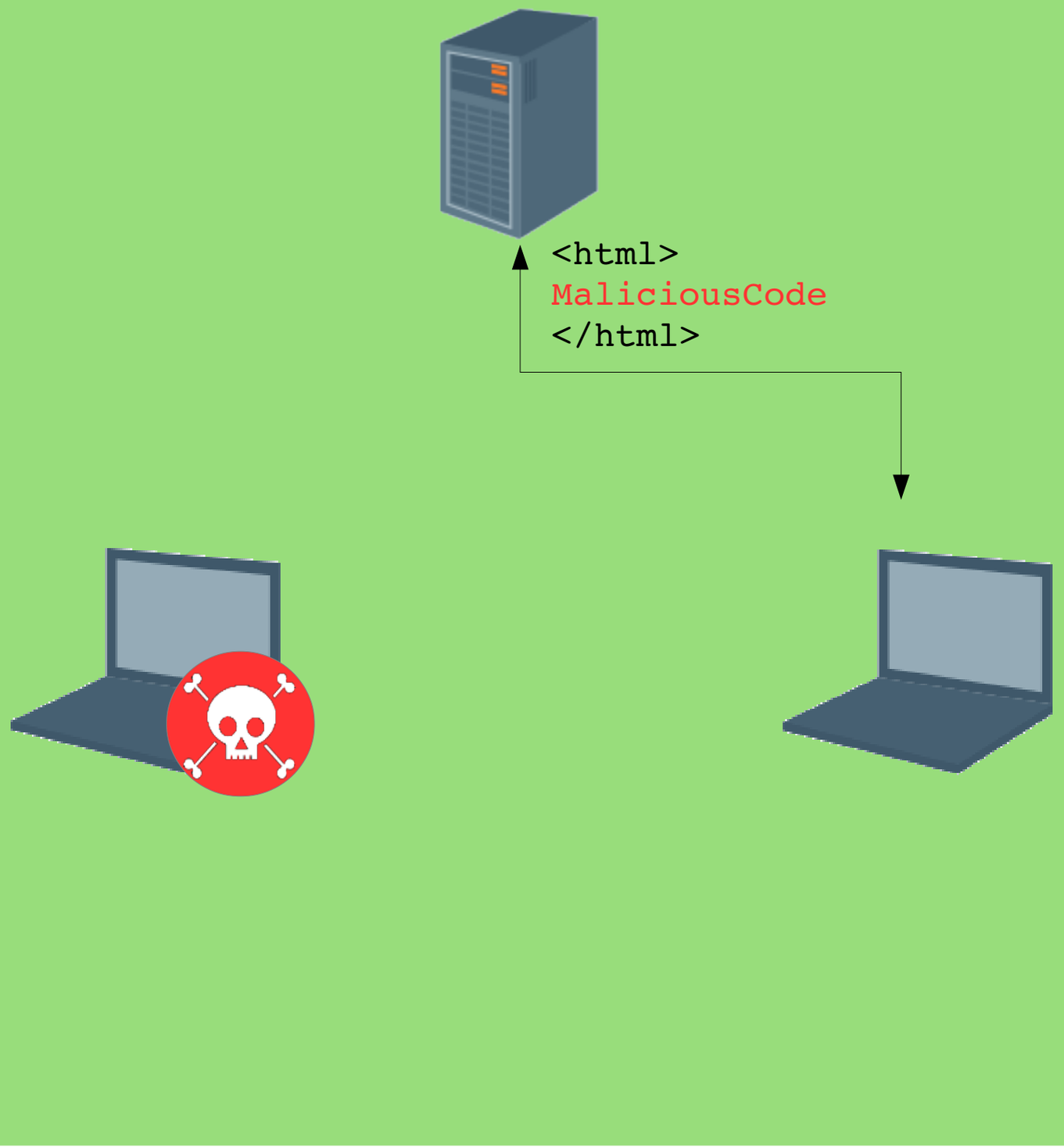
DIGITAL INTERRUPTION

Reflected XSS

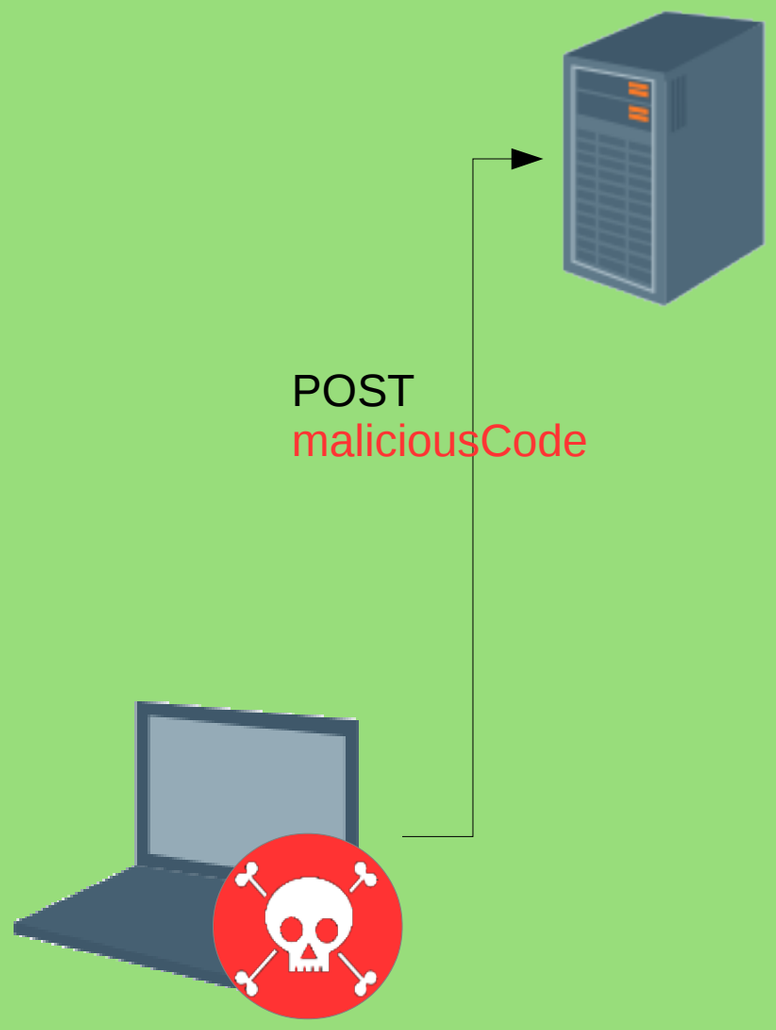


DIGITAL INTERRUPTION

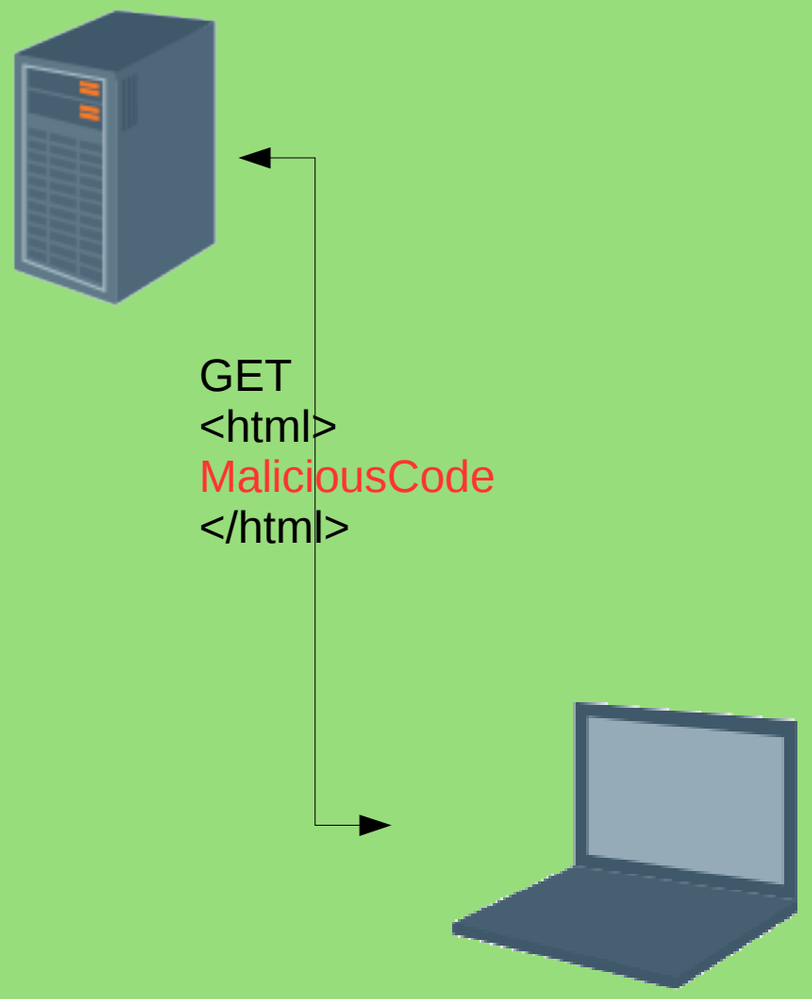
Reflected XSS



Stored XSS

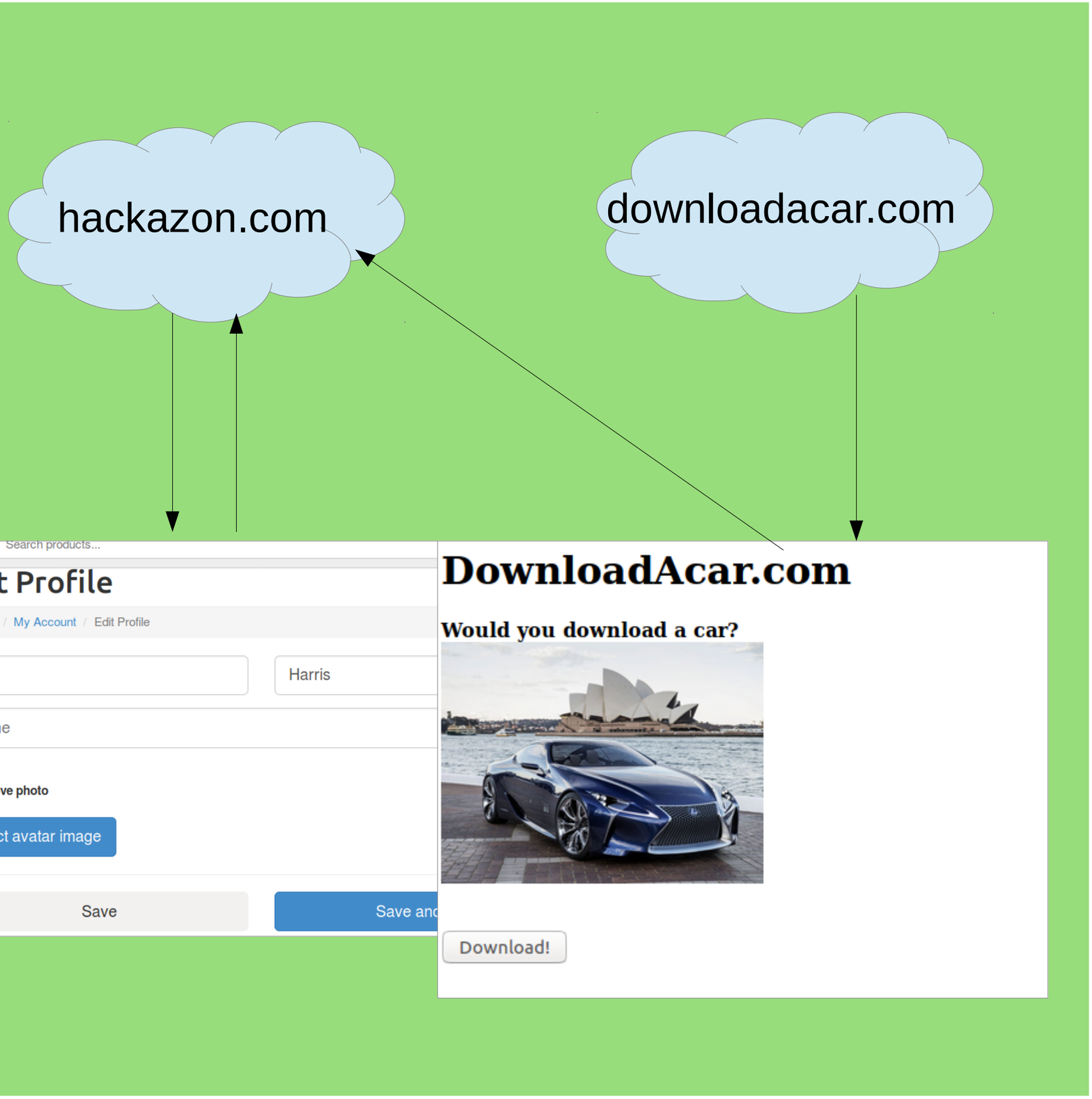


Stored XSS



Exercise
Cross Site Scripting

CSRF


hackazon.com
downloadacar.com
All
Search products...
Edit Profile
Home / My Account / Edit Profile
Jay
Harris
Phone
Remove photo
Select avatar image
Save
Save and
DownloadAcar.com
Would you download a car?
Download!

Exercise
Cross Site Request Forgery

SQL Injection

```
string command = 'do something
on/with' + untrustedData;

execute(command);
```

SQL Injection

```
select * from tbl_users where
username=test_user and
password=123456
```

ID	username	password	Login Disabled
23	test_user	123456	no

SQL Injection

```
select * from tbl_users where
username='name' or 1=1 – and
password=<password>
```

ID	username	password	Login Disabled
1	admin	password	no
2	jsmith	p@55word	no
3	Amy	letmein	yes
..	..	..	..
23	test_user	password	no

DIGITAL INTERRUPTION

SQL Injection

```
select * from tbl_products
where productName like %product
union select * from tbl_users%
```

ID	username	password	Login Disabled
1	admin	password	no
2	jsmith	p@55word	no
3	Amy	letmein	yes
..	..	..	..
23	test_user	password	no

DIGITAL INTERRUPTION

Exercise
SQL Injection

Protections?

Follow good coding practices

Perform regular Penetration Testing and security code reviews

Encourage a “security champion”

Train developers & testers

Adopt Secure SDLC and/or DevSecOps

Involve everyone! Security should be embedded at all levels

DIGITAL INTERRUPTION

Digital Interruption

Questions?

Jahmel Harris

@JayHarris_Sec

@DI_Security

+44 (0)161-820-3056

www.digitalinterruption.com

contact@digitalinterruption.com