

**Bilgi Güvenliği ve Penetrasyon**

**(Teknik Seçmeli Ders VII)**

**PROJE ÖDEVİ**

**2022-2023 Güz Dönemi**

**21/12/2022**

**HAZAR HASCAN – 201913172016**

1- Siteye kayıt aşaması : ctf.hacker101.com sitesinde sayfa kaynağını

görüntüle yaptım orada register metnine tıkladım ve çıkan sitede kayıt olup

siteye giriş yaptım.

---------------------------------------------------------------------------

A little something to get you started

* : Açılan sayfa da sağ tıkla sayfanın kaynağını görüntüle yapıyoruz. Background.img ‘den sonra

Url’si yazıyordu o urlyi kopyalayıp sitenin sonuna ekliyoruz. Flag’ı alıyoruz.

-----------------------------------------------------------------------------

Micro-CMS v1

4-1 : Açılan sayfada testing’e tıklıyoruz sonrasında edit this page’e tıklıyoruz, edit de url’deki id’yi

değiştiriyoruz ve flagı alıyoruz.

4-2 : Create Page’e tıklayıp script yazıyoruz, ( “><script>document.cookie</script ) title ve

aşağıdaki alana’da aynı şeyi yazıp ana sayfaya gidip sayfayı yeniliyoruz. Flag’ı alıyoruz.

4-3 : Ana sayfada herhangi bir post’a tıklıyoruz editleme girdikten sonra url’nin sonuna ‘ işareti ekleyip

açılan sayfadaki flag’ı alıyoruz.

4-4 : Ana sayfada create post’a tıklıyoruz, başlık kısmına <button>some r</button> yazıyoruz.

Alt kısmına <img src=x onerror=alert(document.cookie) /> yazıyoruz. Ana sayfaya buton eklenmiş

oluyor. Sayfaya sağ tık yazıp sayfa kaynağını görüntülüyoruz, oradaki buton scriptinde flag’ı alıyoruz.

---------------------------------------------------------------------------

Photo Gallery

3-1: açılan sitede sayfa kaynağını görüntüle diyoruz oradan fetch?id=1'e tıklıyoruz.

açılan sayfadaki url kısmını sqlmap'e yazıp işlemi başlatıyoruz. çıkan yes/no sorularına

n yazıp cevapladıktan sonra işlem devam ediyor. 25-30dk sonra flag değerini aldım ama

site invalid flag diyor. aldığım flag kodu aşağıda:

\*

[06:05:54] [INFO] retrieved: files/purrfect.jpg

[06:09:37] [INFO] retrieved: 2

[06:09:53] [INFO] retrieved: 1

[06:10:02] [INFO] retrieved: Purrfect

[06:11:34] [INFO] retrieved: 1900286e063bf6d0aad89d7c6cc1a25665415cb82ea6779f762d4363e (flag değeri bu normalde)

[06:22:38] [INFO] retrieved: 3

[06:22:55] [INFO] retrieved: 1

[06:23:04] [INFO] retrieved: test

Database: level5

Table: photos

[3 entries]

\*

3-2 : view image'e tıklıyoruz. sırasıyla sql komutları yazıyoruz. union select

'main.py' sonrasında update photos SET title="test" WHERE id=3; commit; sonrasında

UPDATE photos SET filename="\*||ls ./files >test.txt" WHERE id=3; commit; sonrasında

ls ./files yerine env yazıyoruz. union select "test.txt" ile flagı görüyoruz.

3-3 : sayfa kaynağına gidip fetch 1'e gidiyoruz. union select 'files/adorable.jpg' yi

1,2,0 idlerde aratiyoruz 0'da devam ediyoruz. files/adorable.jpg'yi uwsgi.ini olarak

degistiriyoruz, sonrasında main.py olarak güncelleyip flagı alıyoruz.

--------------------------------------------------------------------------------

MicroCMS v2

3-1 : burp'ümüzü açıyoruz, açılan sayfada changelog bölümüne tıklıyoruz. forward'a

tıklayıp sayfaya gidiyoruz. edit'e tıkladığımızda çıkan yazıları repeater'a

yolluyoruz. repetearda GET kısmını POST yapıp send'e tıklıyoruz, flag'ı alıyoruz.

3-2 : login yapmamız gerekiyor, random username ve şifre giriyoruz burpden login'e

tıkladığımızdaki yazıyı kopyalıyoruz. kalide "nano sqlrequest.txt" kodunu çalıştırıp

yazıyı oraya yapıştırıyoruz. oluşturduğumuz txt dosyasını sqlmap'de calistiriyoruz.

sqlmap -r sqlrequest.txt --drop komutunu yazıp bayrağı ve kullanıcı bilgilerini

alıyoruz ama bende ne yaptıysam hata verdi uygulama 2 tane bayrağı alamadım...

[06:00:48] [CRITICAL] unable to connect to the target URL ('Connection refused'). sqlmap is going to retry the request(s)

[06:00:48] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--proxy', '--proxy-file'...)

3-2 2. yöntem denemesi: username kısmına ' işareti koyup login diyoruz. sqlmap'de

url ile çalıştırıcaz bu sefer." sqlmap --random-agent -u "<https://1ab35ed7901064f8c770a302ab9e44df.ctf.hacker101.com/login>" --data="username=adm&password=adm" --dbms=mysql --dbs "

gelen sorulara "n" yanıtını veriyoruz. sonucunda bizim isimize yarayacak

level2 cevabını alıyoruz. -D level2 --tables 'ı son komutumuzun sonuna ekliyoruz.

admin ve pages oldugunu ögrendik. -D level2 -T admins --dump kodunu yazıp bir daha

çalıştırıyoruz. ve kullanıcı bilgilerini aldık giriş yapıp flagı alıyoruz.

3-3 : page/edit/1 urlsini kopyalıyoruz. curl --request POST -v "<https://1ab35ed7901064f8c770a302ab9e44df.ctf.hacker101.com/page/edit/1>"

komutunu kalide çalıştırıyoruz. -D level2 -T pages --dump kodunu yazıp kalide bir daha

çalıştırıyoruz. ve kullanıcı bilgilerini aldık giriş yapıp flagı alıyoruz.

-----------------------------------------------------------------------------

CODY'S FİRST BLOG

3-1 : add comment kısmında sayfayı incele kısmına bakıyoruz edindiğimiz bilgiye göre

o bölgeye <?php include() ?> yazdıktan sonra flag'ı alıyoruz.

3-2 : sayfa kaynağı kısmında yazan admin auth kısmını buluyoruz ve url'ye ekleyip gidiyoruz

url'deki auth kısmını silip admin sayfasını görüyoruz flag en altta.

3-3 : <?php echo readfile("index.php") ?> komutunu yazıp sumbit'e basıyoruz. admin page'ine

geçip onaylıyoruz. url'de page'in sonuna <http://localhost/index'e> gidiyoruz, sayfa

kaynağını görüntüle dedikten sonra flag'ı alıyoruz.

----------------------------------------------------------------------------

POSTBOOK

7-1 : postbook sign in'e tıkladık,hintlere bakıp kullanıcı adının user şifrenin

ise very easy olduğunu söylüyor denemelerle "Password"ü buldum.

Bayrağı ele geçirdim.

7-2 : sayfadaki post'a tıklayıp gidiyoruz. sayfanın ıd'si 3 olarak gözüküyor.

bu id ile oynadığımızda bayrağa ulaşıyoruz.

7-3 : siteye kayıt oluyoruz. sonrasında kendi kullanıcımzla giriş yapıyoruz. sağ

tık incele yapıyoruz orada user\_id value kısmında 3 olan değeri 2 yapıyoruz.

create post olan bölüme yazıyı yazıp flagı alıyoruz.

7-4 : bu flagın ipucusunda 189\*5 olarak yazıyor sonucu alana yazıp create post'a

tıklıyoruz. edit'e basıyoruz title'ı da 945 olarak güncelliyoruz. home'a geri

dönüyoruz. hello everyone page'ine tıklayıp id'yi 945 yapıp flagı aldım.

7-5 : edit işini yapmak için edite tıklayıp id'mizi 3 olarak güncelliyoruz metine

edit yaptığımızı yazdıktan sonra savepost'a tıklıyoruz. çıkan sayfada bayrağımızı

alıyoruz.

7-6 : anasayfada sağ tık yapıp inceleye tıklıyoruz, storage'e gelip value değerini

kopyalayıp md5 decrypt da value değerinin 3 olduğunu öğreniyoruz. hintten ögrendi\_

gimiz 1 degerini md5 formatında oraya yapistiriyoruz. yeni post aciyoruz ve bayragi

aliyoruz.

7-7 : burp yüklüyoruz ve proxyden aldığımız ıd'yi md5 decrypt'de value değerinin

6 olduğunu öğreniyoruz. burada 3 değerini md5 encryptliyoruz ve delete bastığımızda

yolladığımız delete.php id'sini 3 değerinin md5'ini giriyoruz ve flag'i aldık.

-----------------------------------------------------------------------------

OSU CTF

1-1 : sistemdeki "admin' or '1'='1" username ve password'a yazarak giriş yapıyoruz.

sonrasında natasha\_drew'in base64 formatı için cyberchef'i kullanıp değeri alıyoruz.

url'ye update-student ekleyip / koyduktan sonra değeri verip tüm notları A yapıyoruz.

onayladıktan sonra flag'i alıyoruz.

----------------------------------------------------------------------------------

Y2FuIHlvdSByZWNvbj8/

3-1/2/3 : siteye girdikten sonra sadece jpg yüklenebileceğini söylüyor fakat biz

php denedik olmadı sonrasında phtml denedik ve oldu. burp'ü çalıştırıyoruz, phtml

dosyasını yüklerken post metodunu repeater'a atıyoruz. repeaterdan php kodları

yazarak send ediyoruz. en sonunda ls'de admine gidiyoruz, admin içinde flag var cat

ile ona gidip 3 flag'ıda alıyoruz.

------------------------------------------------------------------------------

H1 Thermostat

2-1 : apk dosyası hazırlandıktan sonra indiriyoruz. indirdiğimiz apk dosyasını

herhangi bir apk decompiler sitesinde işledikten sonra oluşan rar dosyasını

indirip java "payloadrequest.java" dosyasını buluyoruz. vscode ile açtıktan sonra

flagı alıyoruz.

2-2 : üstteki işlemleri yaptıktan sonra elde ettiğimiz dosyada 2. flag'da mevcut.

-------------------------------------------------------------------------------

Encrypted Pastebin

4-1 : açılan sayfadaki yerlere test test girip post'a tıklıyoruz. url'nin sonundaki

"~~" işaretlerini silip enter'a bastığımızda flag'ı alıyoruz.

4-2 : url'yi not defterine kopyalıyoruz "~" >> "=" , "!" >> "/" ve "-" >> "+"

işaretleri yanındakiler olacak şekilde değiştiriyoruz. sonra kalide padbuster'ı

çalıştırıyoruz. padbuster hata verdiği için flag'ı alamadım

-----------------------------------------------------------------------------

BugDB v1

1-1 : açılan sayfadaki graphiql'ye tıklıyoruz. açılan alana sırasıyla node id:1 ve

id:1 yazıp yolluyoruz. findUser(username:"admin") id yazıp yolluyoruz. sonrasında

sırasıyla user, edges, node, bugs, edges, node, id yazıp yolluyoruz. en sonunda

query ile başlayan satırlarıda yolladıktan sonra flagı alıyoruz.

-----------------------------------------------------------------------------

BugDB v2

1-1 : açılan sayfadaki graphiql'ye tıklıyoruz. açılan alana sırasıyla query,user

,edges,node, id ve username yazıp karşı tarafa yolluyoruz. sonrasında allbugs, reporter

, private, reportedid ve id yazıp yolluyoruz. en sonunda mutation ve modify bug yapıp

historyden bi önceki koda dönüp flagı alıyoruz.

-------------------------------------------------------------------------------

Ticketastic

2-1 : submit ticket denedim ilk önce test test diye olusturdum. sonra admin logine

tıkladım username ve passwordu aynıymış "admin". yeni kullanıcı oluştururken burp'ü

açıyoruz, creat'e bastığımızda önümüze düşen yazıdan newUser metodunu kopyalıyoruz.

sql kodunu yazdıktan sonra olustudugumuz kullanıcıyla giris yapiyoruz ve flagi aliyoruz.

2-2 : flag'in id'li olan mesajını sqlmapde çalıştırıyoruz -u ile urlyi verip --dump

ile kodu bitiriyoruz. bir kaç dk süren işlemden sonra

------------------------------------------------------------------------------

HACKHOLIDAYS CTF

12-1 : ipucundan elde ettiğimiz bilgiye göre url'ye gidip /robots.txt ekliyoruzve flagı alıyoruz.

12-2 : /robots.txt sayfasindan aldigimiz url'yi sonuna ekliyoruz. gittiğimiz sayfadasağ tıkla insepctor'a tıklıyoruz içinde gezerken flag'ı görüyoruz.

12-3 : açılan sayfada /people-rater/ ‘ı url’ye ekleyip gidiyoruz. 2. sıradaki butona tıklayıp burp’den id

kısmını kopyalıyoruz. Bu ıd’yi cyberchefte frombase64 ile çevirdikten sonra id:3 olduğunu öğreniyoruz.

İd değerlerini değiştirip repeaterden send ettikten sonra doğru id’nin 1 olduğunu öğrenip flag’ı alıyoruz.

12-4 : açılan sayfada /swag-shop/ ‘ı url’ye ekleyip gidiyoruz. Purchase’e tıkladım ama login istediği için farklı yerlere girmemiz lazım. Sayfa kaynağını görüntülüyoruz ve /api/stock diye bir yer görüyoruz, oraya giriyoruz. Sitenin url’sini kopyalayıp pentest-tools’daki online fuzzing tools’u kullanıyoruz. Session ve user’i öğreniyoruz. Sessions’daki metni kopyalayıp cyberchef’de frombase64 ile çevirip user’la ilgili metni kopyalıyoruz. Bunun uuid değeri olduğunu internetten öğrendikten sonra user?uuid=değer ‘ i yazıp flagı alıyoruz.

12-5 : internetteki forumdan öğrendiğim /my-diary/?template=entries.html sayfasını açıyoruz. Curl’de bu url’nin index.php’sini -s parametresi ile çalıştırıyoruz. Entries.html’de sayfa kaynağını görüntüleyip, urlden index.html yapıp sayfa kaynağına ulaşıyoruz, burada çeşitli ipuçlarından sonra secretadsecretaadmin.phpdmin.phpmin.php’yi bulduktan sonra yazıp oraya gidiyoruz. url’nin başındaki wievsource’u silip flagı alıyoruz.

12-6 : ipucu ve forumlardan öğrendiğim bir diğer alan /hate-mail-generator/ url’ye ekleyip giriyoruz. Örnek maili okudum sayfa kaynağına falan baktım pek bir şey görmediğim için, create new’e tıkladım. Test için oluşturduğum template hata verdi ama /templates yolunu öğrendik orayı inceliyoruz. Adminle alakalı adresle ilgili işlemleri yapıp inspectordan alice’i admin olarak değiştirip, kodu yazdıktan sonra flag’ı alıyoruz.

12-7 : ipucu ve forumlardan öğrendiğimiz bir diğer alan /forum url’ye ekleyip giriyoruz. Postlara tıkladığımızda you need to be admin view posts uyarısını alıyoruz. İnternette araştırmalar sonucu githubda grinch-networkde kullanıcı adı ve şifreyi öğreniyoruz. Forum/phpmyadmin sayfasına gidip bilgilerle giriş yapıyoruz, userda grinch isminin yanında admin 1 değerini görüyoruz, password’ü md5li olduğu için online bir şekilde decrpyt ettikten sonra şifreyi öğreniyoruz. Forum sayfasına gelip giriş yapıp secret plans’da flagı alıyoruz.

12-8 : ipucu ve forumlardan öğrendiğimiz bir diğer alan /r3c0n\_server\_4fdk59/ url’ye ekleyip gidiyoruz. Burada üstteki posta tıklayıp 3’lü resmi açıyoruz burada url’nin sonuna “ ‘ and 1=0 union all select “1’ and 1=0 union all select 4,5,6;--;--“,2,3;-- “ kodunu yazıp enter’a basıyoruz. Brute force işleminden sonra kullanıcı adı ve şifreyi öğrendikten sonra giriş yapıp flag’ı alıyoruz.

-----------------------------------------------------------------------------

PETSHOP PRO

3-1 : sayfaya girip kedi'yi sepete ekliyoruz. sağ tık inceleye basıp, checkout formunu

hidden'ı siliyoruz. orada ortaya çıkan yazıda price'ı 0 yapıp check out'a tıklıyoruz ve flagı alıyoruz.

------------------------------------------------------------------------------

TEMPLMAGE

2-1 : upload'a tıklıyoruz, oradan dosyayı seçtikten sonra burp'ü açıyoruz, burp

açıldıktan sonra yükleye basıyoruz, çıkan yerde dosya adlarını "../../" olarak

değiştirip forward ettikten sonra flagı alıyoruz.

2-2 : png formatında dosya indirip onu browse'dan ekliyoruz. burp'ü açıp upload'a

tıklıyoruz.send to repeater yapıp off yapıyoruz. <?php system ("cat index.php");?>

ekleyip dosyanın önüne /../../ ve uzantısını php yapıyoruz. fallow redirection'a

tıklayıp flag'ı aratıyoruz, çıkan flagı alıyoruz.