**Hazirlayanlar-Əliyev Sənan,Əlizadə Araz,Əlizadə Xəyyam,Əsgərov Həbib**

**Qrup-641a2**

**Fənn-Veb təhlükəsizlik**

**Lab-6**

**Tapşırıq aşağıdakıdır:**

Bu tapşırıqda siz kukiləri “oğurlamaq”la məşğul olacaq və bu cür hücumların qarşısının alınmasını öyrənəcəksiniz.

Sizə iki kompüter lazım olacaq. Tapşırığın hər bir elementinə xüsusi diqqət verməniz çox önəmlidir. Kompüterlərdən birinin Linux əsaslı olması yaxşı olardı.

Kompüterləri şərti olaraq “İstifadəçi” və “Dələduz” adlandıracağıq. Tapşırıq əsasında “Dələduz” adlı kompüterin sahibi “İstifadəçi”nin kukilərini oğurlayacaq.

“İstifadəçi” kompüterində:

* <http://lab6.adil.az/> saytına daxil olun.
* Sayta ilk dəfə daxil olduqda istifadəçi adı və şifrə istəyəcək. İstənilən istifadəçi adı və şifrəni daxil edin.
* Fərz edin ki, hansısa bir xidmətin login formasıdır. Bu sayt nümunə üçün olduğundan istənilən istifadəçi adı və şifrə ilə daxil olmaq mümkündür.

Yuxarıdakı addımları yerinə yetirdikdən sonra həmin sayt “İstifadəçi”nin kompüterində kukiləri yadda saxlayır.

İndi növbə “Dələduz” kompüterindədir.

“Dələduz” istəyir ki, “İstifadəçi”nin kukiləri oğurlasın. Bunun üçün hücum planı hazırlamaq lazımdır. İlk olaraq öz kompüterində bir veb-server quraşdırmalıdır. Apache serveri yükləməklə əvvəlki dərslərdə olduğu kimi bunu yerinə yetirə bilərsiniz.

Biz elə etmək istəyirik ki, “İstifadəçi” <http://lab6.adil.az/> saytına gələn dəfə daxil olanda hansısa şəkildə “Dələduz” serverinə qoşulmuş olsun.

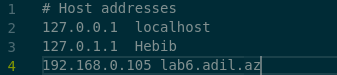
Fərz edək ki, hansısa virus vasitəsilə, və ya “İstifadəçi”nin kompüterinə fiziki olaraq əl vurmaq imkanı olan kiminsə vasitəsilə bu planı yerinə yetirdiniz. Tapşırıq üçün biz bu hadisəni sadəcə simulyasiya edəcəyik (öyrənmək xarakteri daşıdığından). “İstifadəçi”nin kompüterində hosts faylını dəyişməklə lab6.adil.az-nı DNS vasitəsilə “Dələduz”-un kompüterinə yönləndirin. Bunun üçün onlar eyni şəbəkədə olmalıdırlar.

İndi “İstifadəçi” <http://lab6.adil.az/> saytına daxil olduqda saxta bir sayta “Dələduz”un serverinə qoşulacaq. “Dələduz” kukiləri oğurlamaq üçün JavaScriptdən istifadə edə bilər. JavaScriptdə document.cookie dəyişəni bütün cookieləri özündə cəmləşdirir. Serverin sahibi siz olduğunuzdan səhifədə bir skript yazmaqla bu hücumu həyata keçirə bilərsiniz. İndiyədək öyrəndiyimiz alətlərdən istifadə etməklə belə bir hücumu yerinə yetirin.

Tapşırıqdan 10 bal almaq üçün aşağıdakılar yerinə yetirilməlidir: “Dələduz” serverində istifadə olunan skriptlər hər biri GitHub-a yüklənməlidir. Kukilərdə olan şifrəni açmalısınız. Kukilərdə olan secret\_message adlı məlumatı deşifrə edib oxumalısınız və bunu hesabatınızda qeyd etməlisiniz. Kukiləri oğurlamaq üçün etdiyiniz bütün addımlar hər biri hesabat kimi sənədləşdirilməlidir.

<http://lab6.adil.az/> saytının orijinal kodları vulnarable-app qovluğunda yerləşdirilib. İpucu tapmaq üçün ondan yararlana bilərsiniz.

İndi biz tapşırığın ilk şərtini yerinə yetiririk və sayta daxil oluruq <http://lab6.adil.az/> saytına. Sayt işləyir biz indi bu sayta hücum etməliyik. Biz saytın dns adresində bəzi dəyişiklik edirik , bu sayta daxil olmaq istəyən bütün istifadəçilər bizim dələduz sayta gəlməlidir. DNS adresində dəyişiklik etməliyik. Aşağıdaki şəkildə biz linux istifadə edirik deyə /etc/hosts-da dəyişiklik etməliyik əgər windows -da isə bu fərqli qovluqdadır. Bizim dələduz saytının ip adresinin qarşısına saytın domen adresini yazırıq. İndi isə lab6.adil.az saytına daxil olmaq istəyərkən bizim dələduz sayta gələcəklər və bizim istədiyimiz kimi cookie-ləri oğurlayacayıq. Biz yəni dələduz bu saytda cookie-ləri oğurlamaq üçün Javascript kodları vasitəsi ilə ələ keçiriləcək və bu cookie-lər dələduzun əlinə keçəcək. Aşağıdaki şəkildə isə hosts-da dəyişiklik edirik.



Biz daxil olmaq istəsək error verəcək çünki biz apache serverini qurmamışıq hələki. Bizim dələduz saytı apache serverinə yükləməliyik. Bunu aşağıdaki kimi edirik. Burdada bizim kodlarımız yer alır ilk öncə bu react kodunu **npm run build** edirik ki apache2 serverinə yükləyə bilək.

Npm run build etdikdə bizim fayllarımızın içinə bir fayl yüklənəcək adı build olan . Bu faylı biz daxil etməliyik apache2 serverinə.

Aşağıdaki kodlarla bunu etmək mümkündür.

**1)npm run build**

**2)cp –r /home/Hebib/Desktop/Facebook/build /var/www/html**

Bizim fayllar artıq apache serverinə yüklənmiş oldu son olaraq aşağıdakı kodu yazaraq apache serverinin html qovluğuna köçürürük.

**1) cd /var/www/html/build**

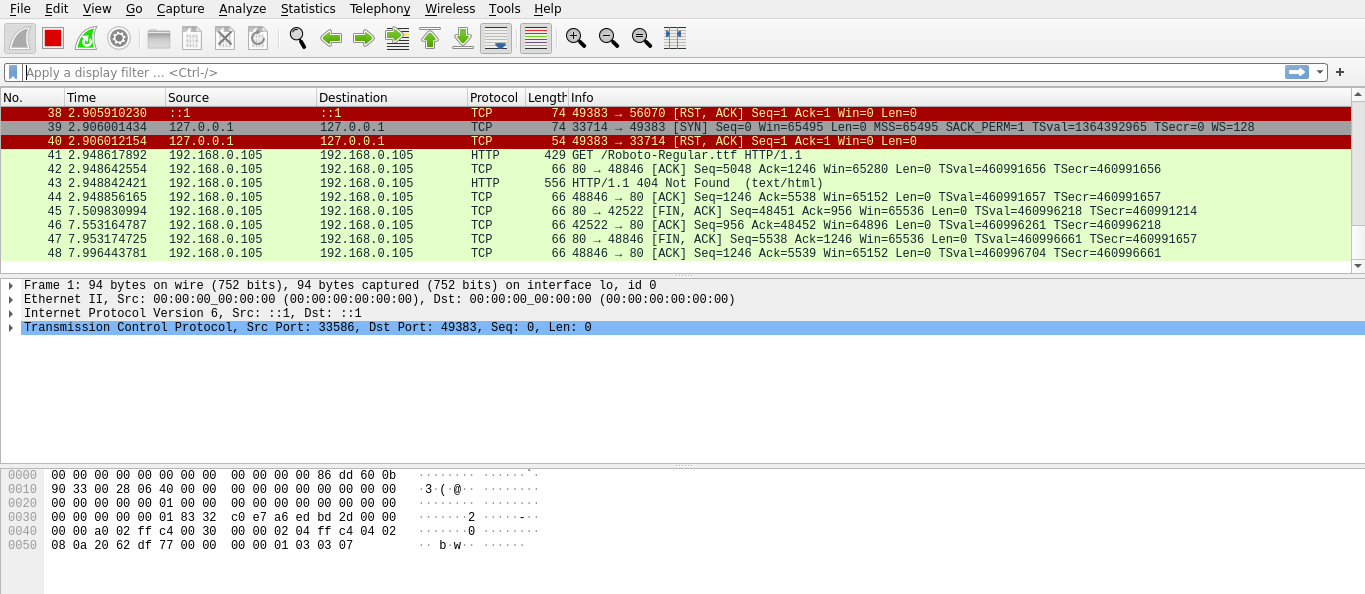
**2) mv \* ../**

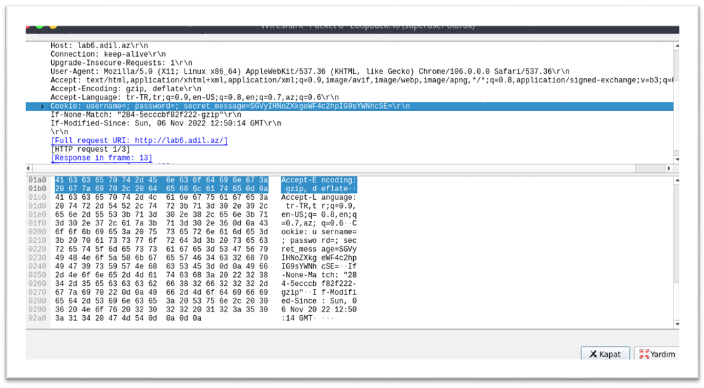
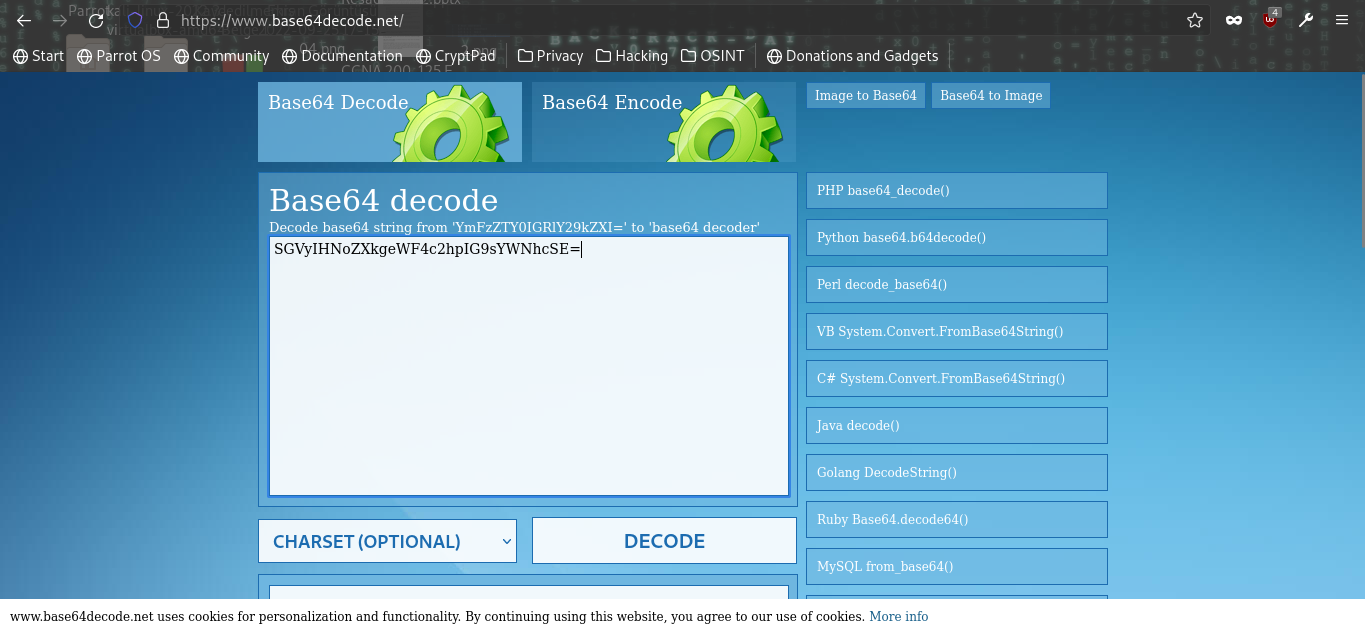
Artıq bizdə belə bir görüntü alınmalıdır.

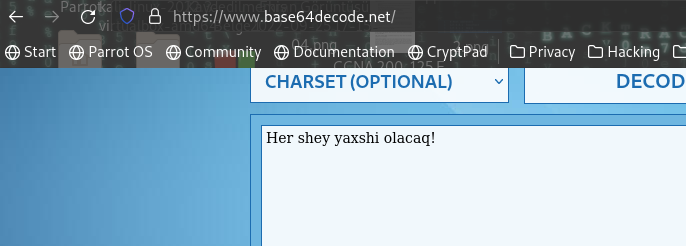
Daha sonra apache serverini başladırıq aşağıdakı kodu yazaraq.

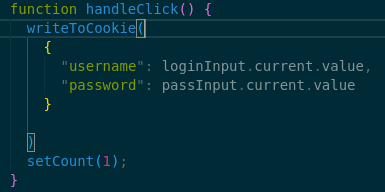
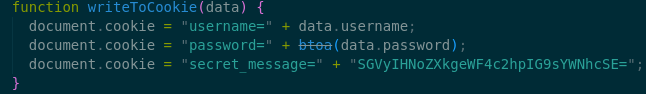
**1)service apache2 start (başladırıq)**

**2)service apache2 status( aktiv olub olmamasına baxmaq üçün status yazırıq.)**

Artıq hər şey hazırdır istifadəçinin cookie-sini oğurlamaq olar. Bunun üçün daha öncə istifadə etdiyimiz wireshark-dan istifadə edirik. Bunu etmək üçün tool-u açırıq və bizim əsas əməliyyat sistemində olduğu üçün linux biz Loopback-dən baxırıq protokollara. İstifadəçi daxil olan kimi bizə protokollar gəlir.Gördüyünüz kimi loopback-dən baxdıqda istifadəçi daxil olan kimi bizə protokollar gəlir və burdan cookie olanı tapıb seçirik. HTTP olaraq filtir edirik təbii ki ilk öncə.

Gördüyümüz kimi artıq cookie-ləri ələ keçirə bilirik. Hərhansı bir uername və şifrə daxil etsələr buraya gələcəkdir. İndi isə bizə secret mesaj bölməsindəki kodu həll etməliyik. Burda isə biz şifrəyə baxan kimi tipindən base64 olduğunu bilirik. Buna görə göstərdiyimiz sayta daxil oluruq. Decode etmək üçün bu səhifədən istifadə edə bilərik. Decode etdikdən sonra şifrəmiz aşağıdakı kimi olur.

Sonraki tapşırıq isə biz pis niyyətlə istifadə etdiyimiz cookie-ni oğurlamaq üçün istifadə etdiyimiz kodu aşağıdaki şəkildə göstəririk.



writeToCookie –də verilənlər username password və secret mesaj document.cookie-də cəm halında birləşir ümumiyyətlə document.cookie saytlarda cookie-ləri özündə birləşdirir.

HandleClick olan hissədə isə login olan hissədir bura yazılanlar cookie olaraq yadda saxlanılır writeToCookie funksyası ilə.

Bu şəkildə isə cookie-ni şifrələyirik.

