**Hazirlayanlar-Veliyev Resad, Zeynalli Valeh, Rehimova Nuray, Residli Musa, Rustemzade Mustafa**

**Qrup-641a2**

**Fenn- Veb Tehlukesizlik**

**Lab-(6)**

Biz ilk öncə tapşırıq ilə tanış olmalıyıq tapşırıq aşağıdakidir:

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.

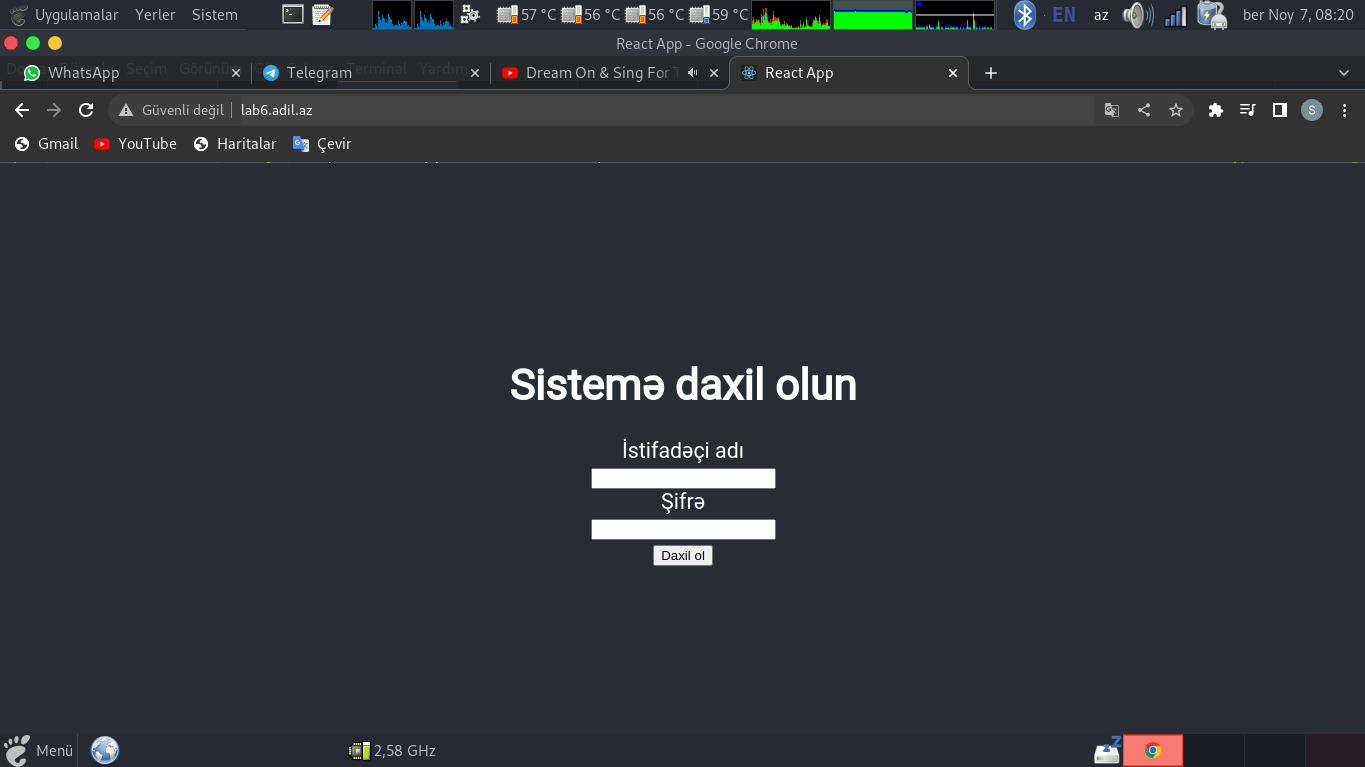
Biz elə etmək istəyirik ki, “İstifadəçi” <http://lab6.adil.az/> saytına gələn dəfə daxil olanda hansısa şəkildə “Dələduz” serverinə qoşulmuş olsun.

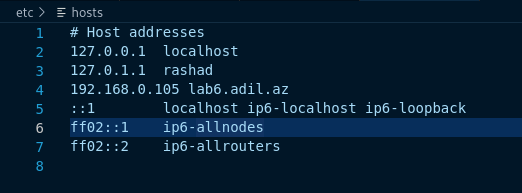
Fərz edək ki, hansısa virus vasitəsilə, və ya “İstifadəçi”nin kompüterinə fiziki olaraq əl vurmaq imkanı olan kiminsə vasitəsilə bu planı yerinə yetirdiniz. Tapşırıq üçün biz bu hadisəni sadəcə simulyasiya edəcəyik (öyrənmək xarakteri daşıdığından). “İstifadəçi”nin kompüterində hosts faylını dəyişməklə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

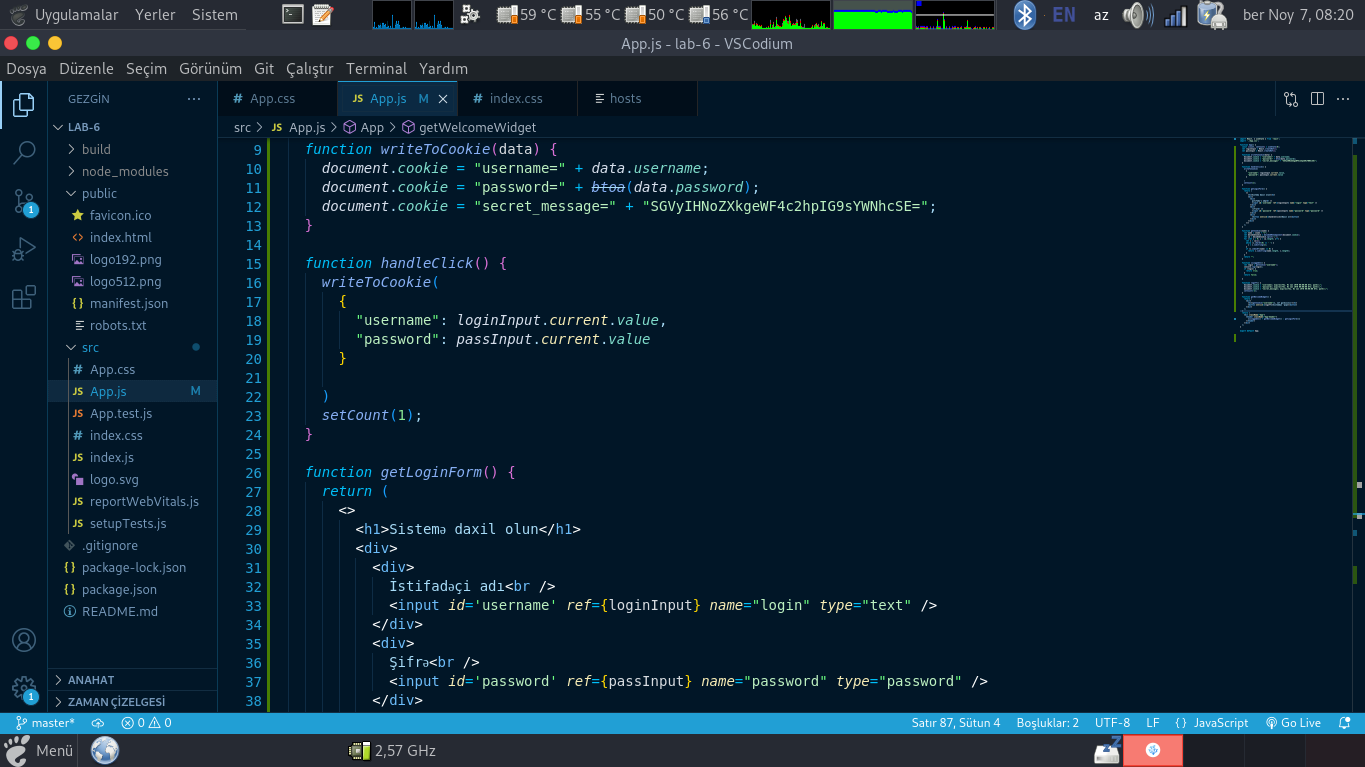
İndi “İstifadəçi” <http://lab6.adil.az/> saytına daxil olduqda saxta bir sayta “Dələduz”un serverinə qoşulacaq. “Dələduz” kukiləri oğurlamaq üçün JavaScriptdən istifadə edə bilər. JavaScriptdə document.cookie dəyişəni bütün cookieləri özündə cəmləşdirir. Serverin sahibi siz olduğunuzdan səhifədə bir 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 isə biz tapşırığın ilk şərti olan səhifəyə daxil olmalıyıq.Sayta daxil olduq saty işlək vəziyyətdədir və biz bu sayta hücum etməliyik. Bəs necə? İlk öncə biz saytın dns adresində bəzi dəyişiklik edirik və bu sayta daxil olmaq istəyən bütün istifadəçilər bizim dələduz sayta düşməlidir bunun üçün kiçik bir simulyasiya yaradaq. İlk öncə DNS adresində dəyişiklik edək. Aşağıdaki şəkildə biz linux istifadə edirik deyə /etc/hosts-da dəyişiklik edirik və bizim dələduz saytının ip adresinin qarşısına saytın domen adresini yazırıq.

Bu sayta daxil olmaq istəyən istifadəçilər yanlış adresə gələcək yəni dələduz sayta. Dələduz sayta daxil olan kimi cookie-lər dələduz saytında javascript kodları vasiəsi ilə ələ keçiriləcək və bu cookie-lər dələduzun əlinə keçəcək. Biz indi daxil olmaq istəsək error verəcək çünki biz kodu apache2 serverinə daxil etməliyik apache2 serveri dedikdə gerçək həyatda etsə idik başqa bir sayt açıb oranın serverinə yükləyəcəkdik kodları amma dediyimiz kimi simulyasiya edirik deyə apache2 serverinə yükləməliyik ilk öncə kodlarımız ilə tanış olaq.



Burdad 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 build adlı. Bu faylı biz daxil etməliyik apache2 serverinin içinə bunun üçün aşağıda göstərilmiş kodu yazırıq terminala.

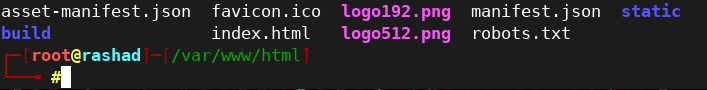


İndi bizim fayllar apache2 serverinə yüklənmiş oldu. Daha sonra biz **/var/www/html/build** -ə daxil olaraq orda aşağıdakı kodu yazaraq içindəki faylları atırıq **var/www/html/** -ə.



İlk öncə aşağıdakı cd ilə başlayan kodu yazırıq çünki fayla daxil olmamış içindəki faylları çıxarmaq olmaz daha sonra is içindəki faylları çıxarırıq.

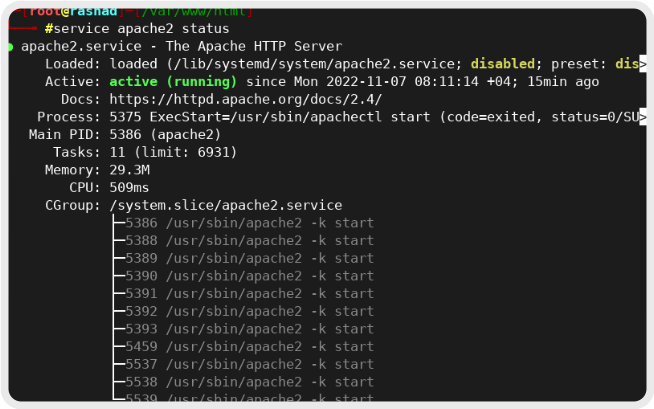
Daha sonra isə biz **service apache2 start** yazraq serveri başladırıq.





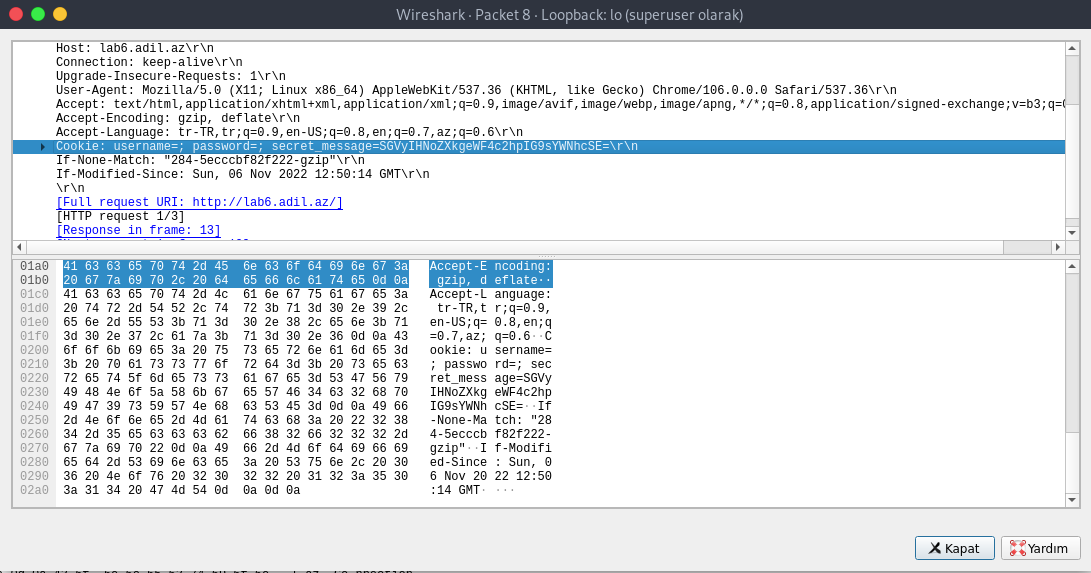
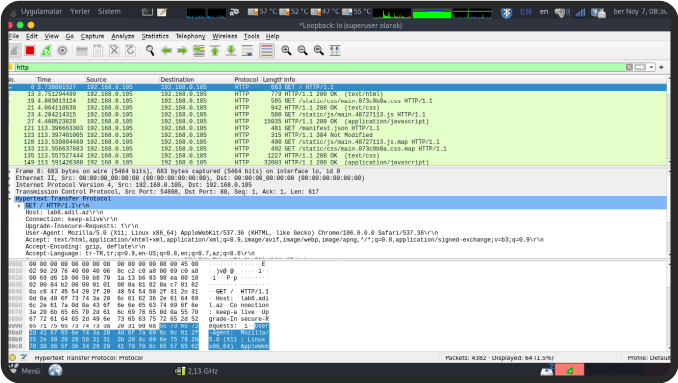
Daha sonra işlədiyindən əmin olmaq üçün **service apache2 status** yazırıq aktiv yazırsa deməli işləyir.

Artıq hər şey hazırdır lab6.adil.az saytına daxil olan kimi bizim sayta yönləndiriləcək və bizim saytda istifadəçilərin cookie-si əlimizə keçəcək.

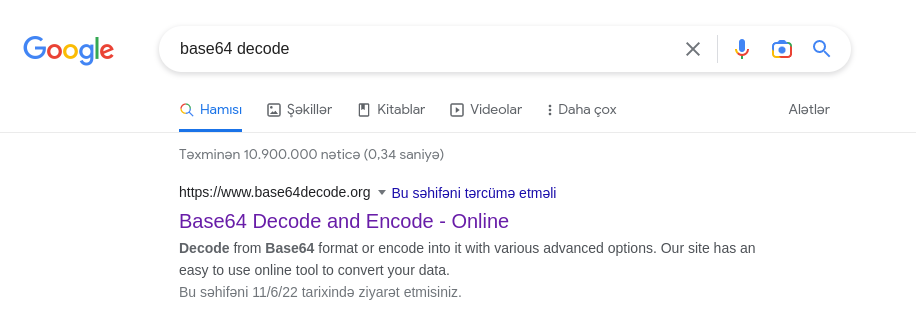


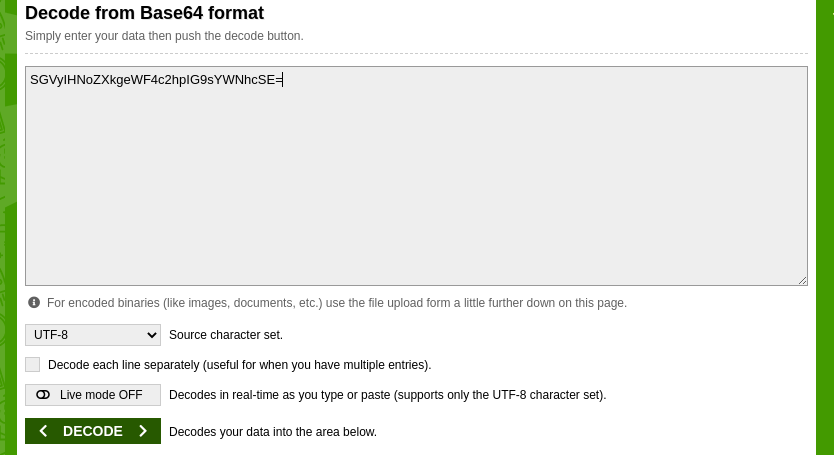
Biz bunu belə edə bilərik ki istifadəçi sayta daxil olan kimi biz wirshark-ı açırıq və cookie-lərini götürürük. Bunu etmək üçün tool-u açırıq və bizim əsas əməliyyat sistemində olduğu üçün linux biz Loopback-dən baxırıq protokollara. İstifadəçi daxil olan kimi bizə protokollar gəlir.

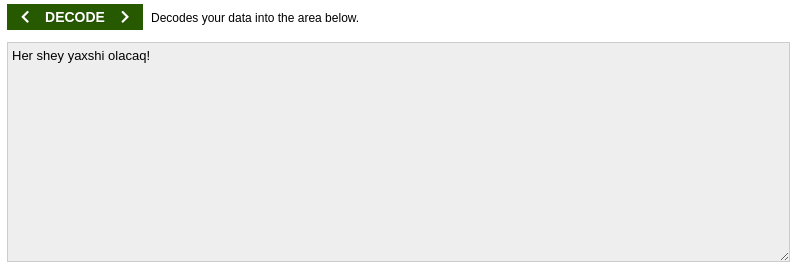
Daha sonra isə biz burdan HTTP protokollarına baxırıq birdə görürük ki cookie-nin olduğu protokol.Nə şifrə nə username daxil etsələr avtomatik burada görsənəcəkdir.



İndi isə bizə secret mesaj bölməsindəki kodu həll etməliyik. Burda isə biz şifrəyə baxan kimi tipindən base64 olduğunu bilirik. Onun üçün aşağıdaki sayta daxil oluruq.

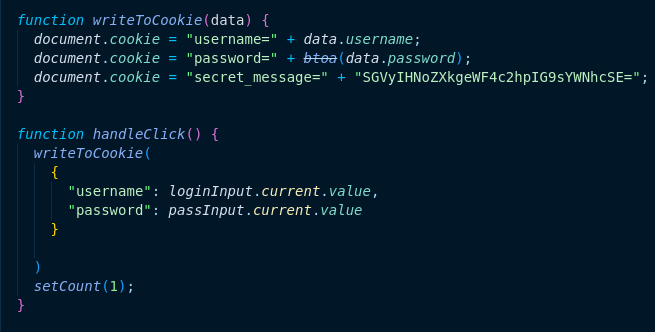
Sayta daxil olarkən bizi belə mənzərə qarşılayır. Biz decode etmək istədiyimiz şifrəni buraya daxil edirik.

 Daha sonra isə şifrəni tapırıq))

Müəllim bizə belə bir gözəl məsaj buraxıb və bizə də İNŞALLAH demək düşür.

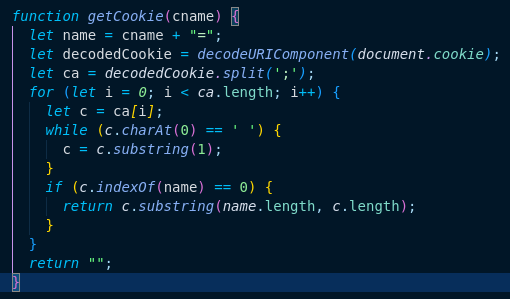
Daha sonra isə biz pis niyyətlə istifadə etdiyimiz cookie-ni oğurlamaq üçün istifadə etdiyimiz kodu aşağıdaki şəkildə göstəririk.

Burdada writeToCookie –də verilənlər username password və secret mesaj document.cookie-də cəm halında birləşir



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

Aşağıdakı şəkildə isə bu cookie-ni şifrələmək üçün istifadə olunur.



Diqqətiniz üçün minnətdaram!