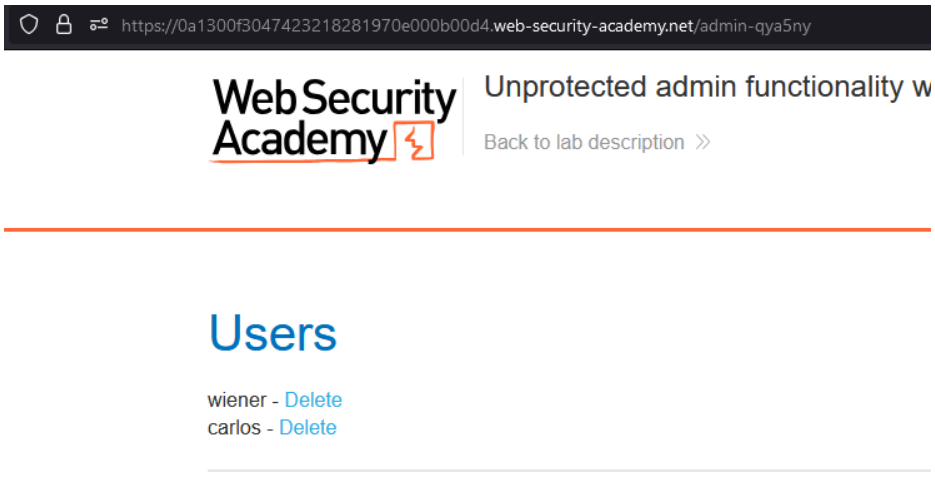
1) broken access control

```
<script>
var isAdmin = false;
if (isAdmin) {
   var topLinksTag = document.getElementsByClassName("top-links")[0];
   var adminPanelTag = document.createElement('a');
   adminPanelTag.setAttribute('href', '/admin-qya5ny');
   adminPanelTag.innerText = 'Admin panel';
   topLinksTag.append(adminPanelTag);
   var pTag = document.createElement('p');
   pTag.innerText = '|';
   topLinksTag.appendChild(pTag);
}
```

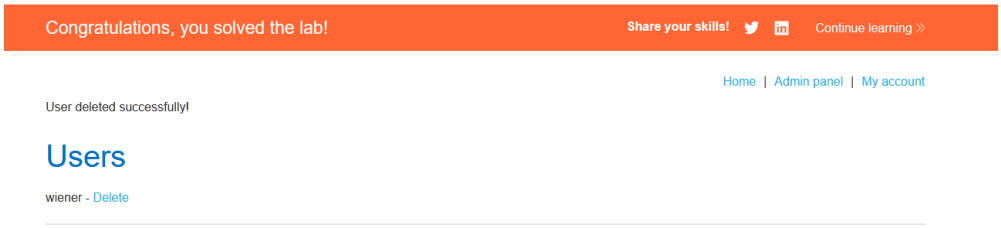
Normal kullanıcı ile giriş yapıldıktan sonra source kod içerisinde **/admin-qyan5ny**

Adlı bir url bulundu. Bu url'e gidildiği zaman herhangi bir kontrol yapılmamaktadır. Aşağıdaki görselde görüldüğü üzere



2) broken access control

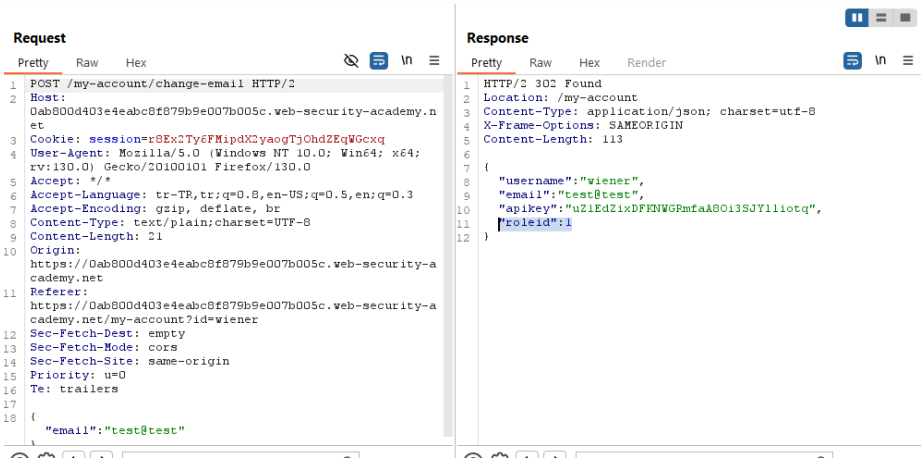
Yukarıdaki görselde görüldüğü üzere cookie header'ında **admin=false** adlı bir input alınmaktadır. Bu input true ile değiştirldiğinde aşağıdaki admin-panel url'i gözükmekte.



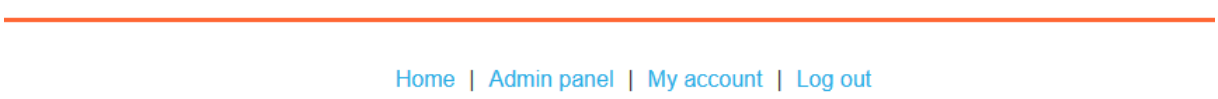
Admin panele girildiği zaman gene aynı şekilde **admin=false** değeri true ile değiştirilerek carlos kullanıcısı silinmekte

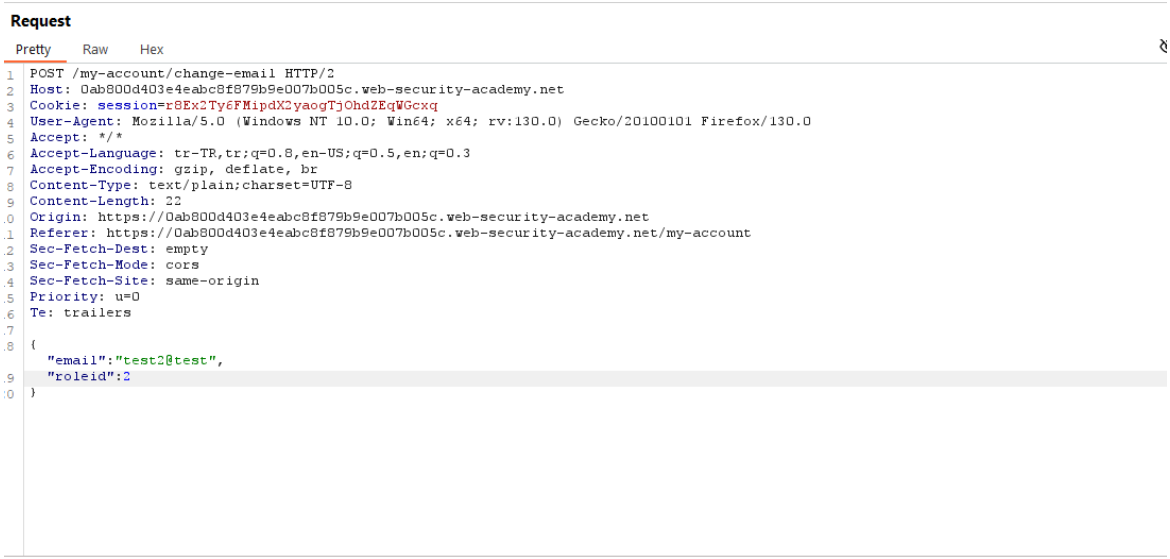
dir.

3) broken access control



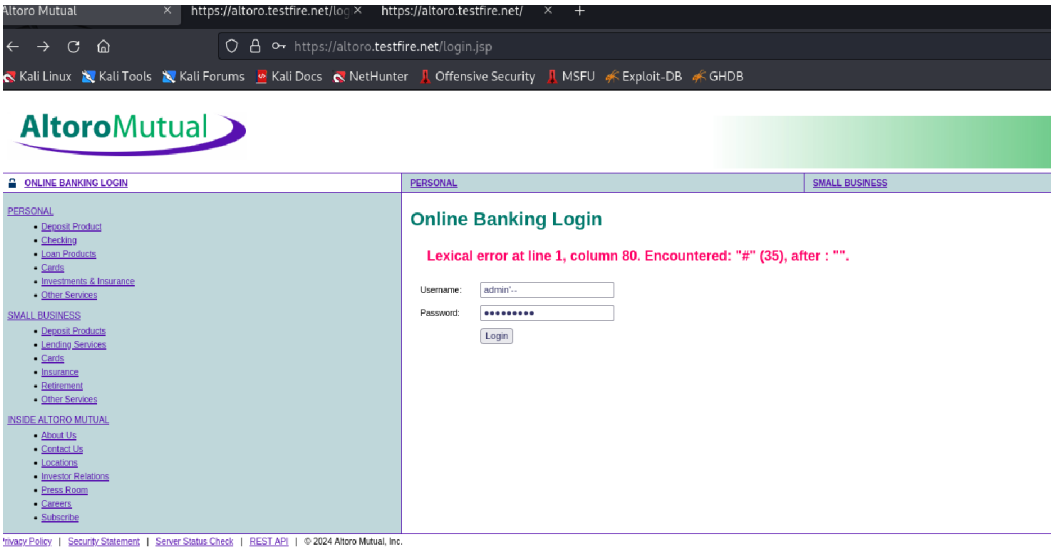
Kullanıcı email adresi düzenleme apisinden dönen cevapta **roleid:1** adlı bir json parametresi dönmekte mevcut kullanıcımın yetkisi 1 ‘ i temsil ettiği için yeniden bir email değişikliği isteği yollanıp bu sefer **roleid:2** değeri gönderildiği zaman aşağıdaki görsellerde görüldüğü gibi admin yetkisine sahip olunmuştur.

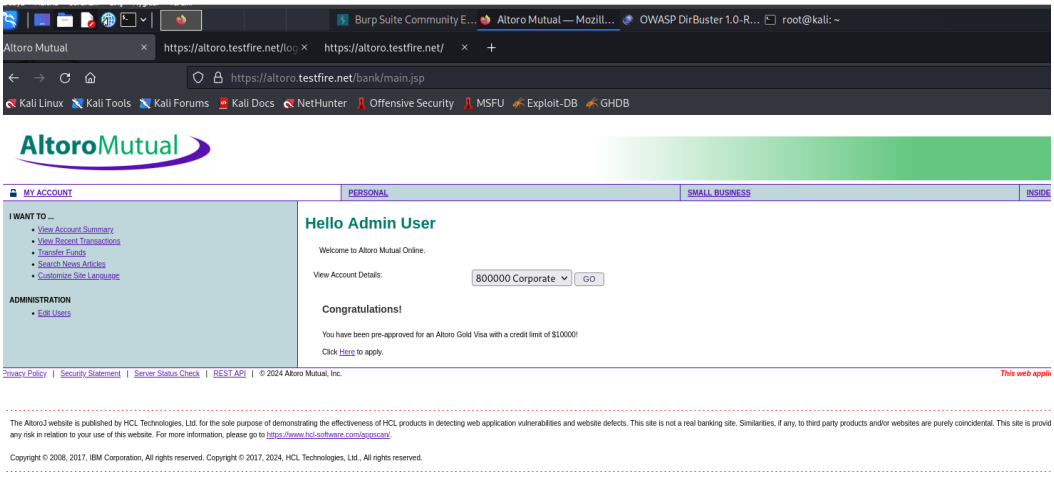




4) sql injection

Admin kullanıcısıyla giriş yapmak için sql injection denedim ve sisteme giriş elde ettim.

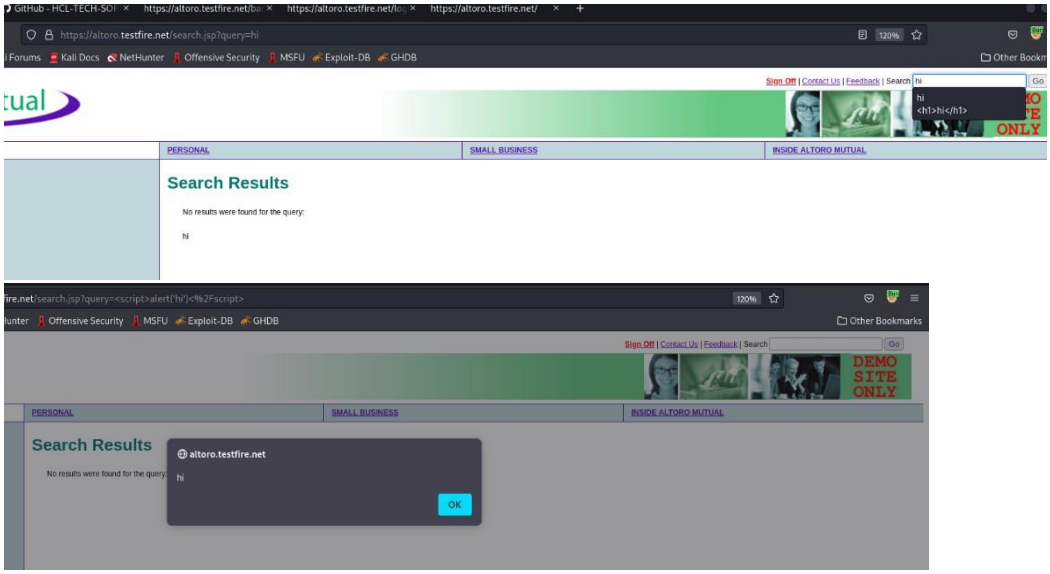




5) XSS İNJECTİON

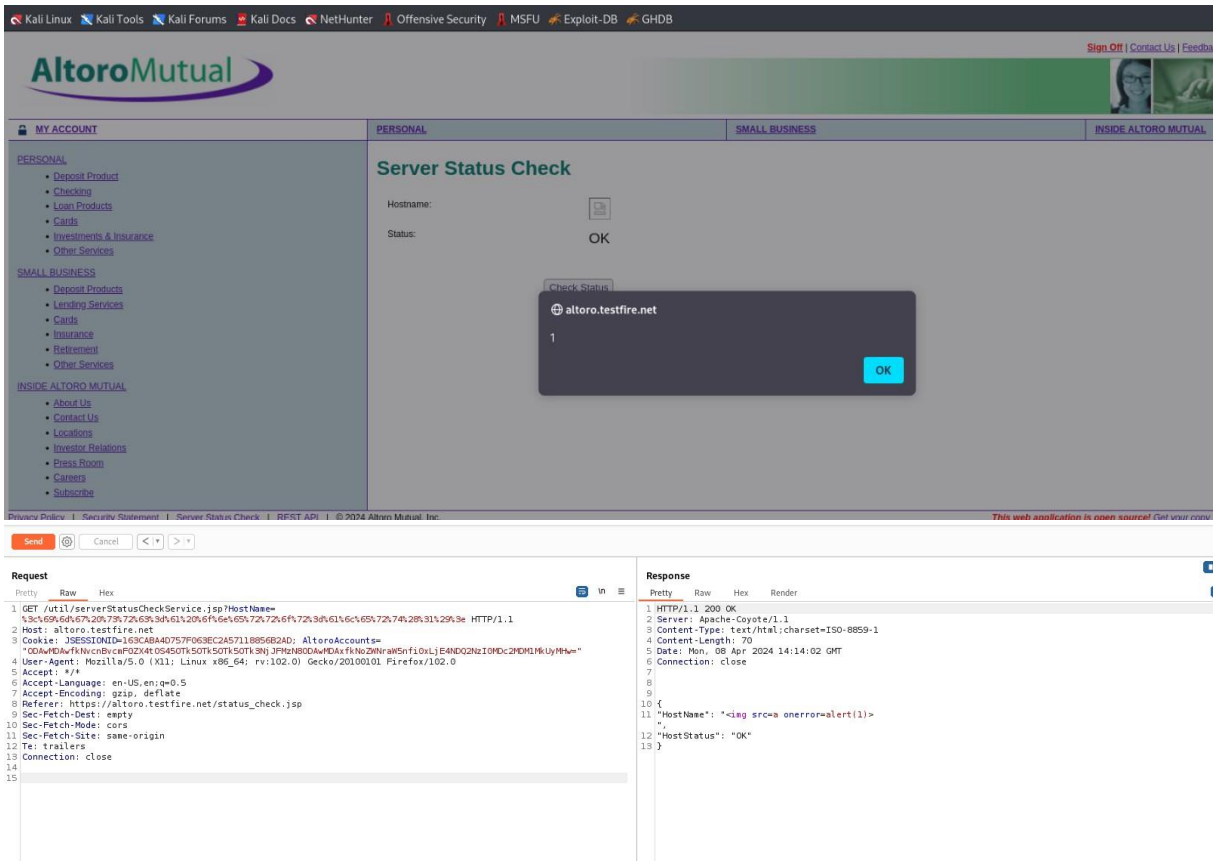
Arama bölümde aşağıda görüldüğü gibi arama sekmesine yazılan input html içerisine gömülüyor. Eğer bir filteleme yoksa xss açığı olabilir diye düşündüm ardından

<script>alert(“deneme”)</script> payload’ını kullandım.



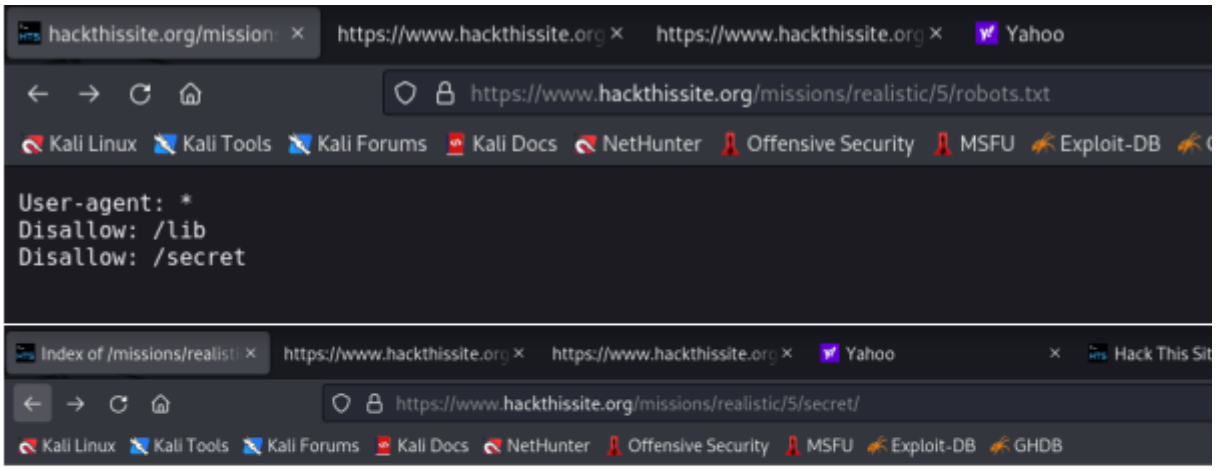
6) xss injection

/Status_check url'inde hostname değeri parametre olarak alınıyor. Ben de burpsuite yardımıyla paketi tuttum ardında ise hostname değerini manipüle ederek <img src=a onerror=alert(1) > payload'ını kullandım.



7) **Cryptographic Failures** -Damn Telemarketers Ctf

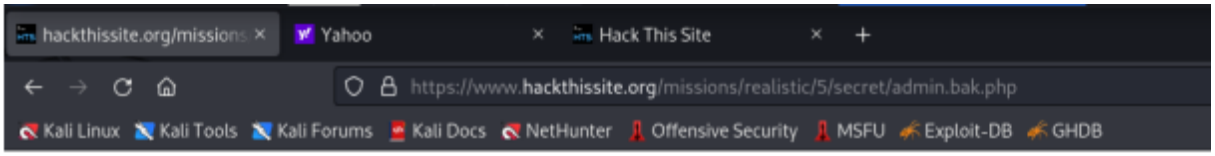
Robots.txt dosyasına baktığımda 2 uzantı gördüm bunlardan secret olana girdiğimde beni 2.resimdeki görsel karşıladı.



Index of /missions/realistic/5/secret

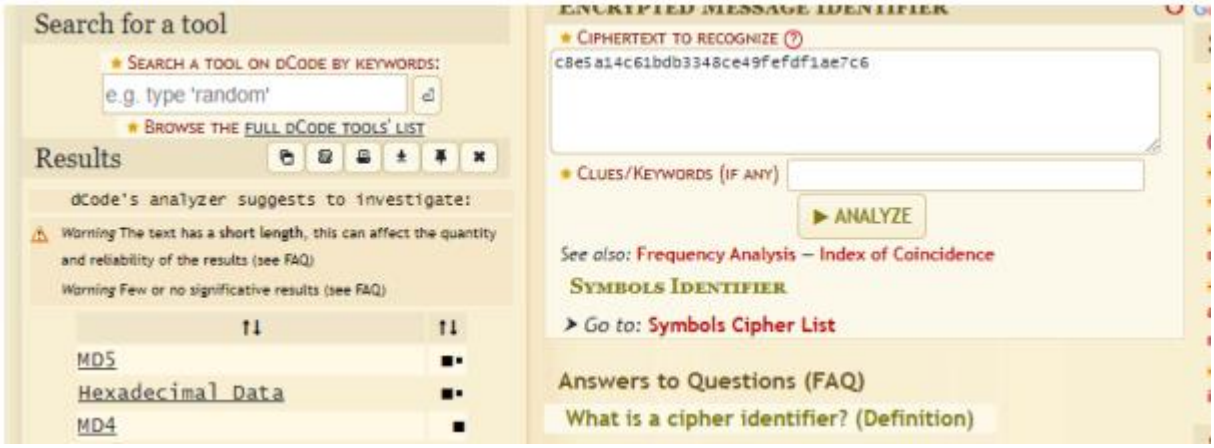
Name	Last modified	Size	Description
Parent Directory		-	
admin.bak.php	2013-12-30 05:28	230	
admin.php	2013-12-30 05:28	621	

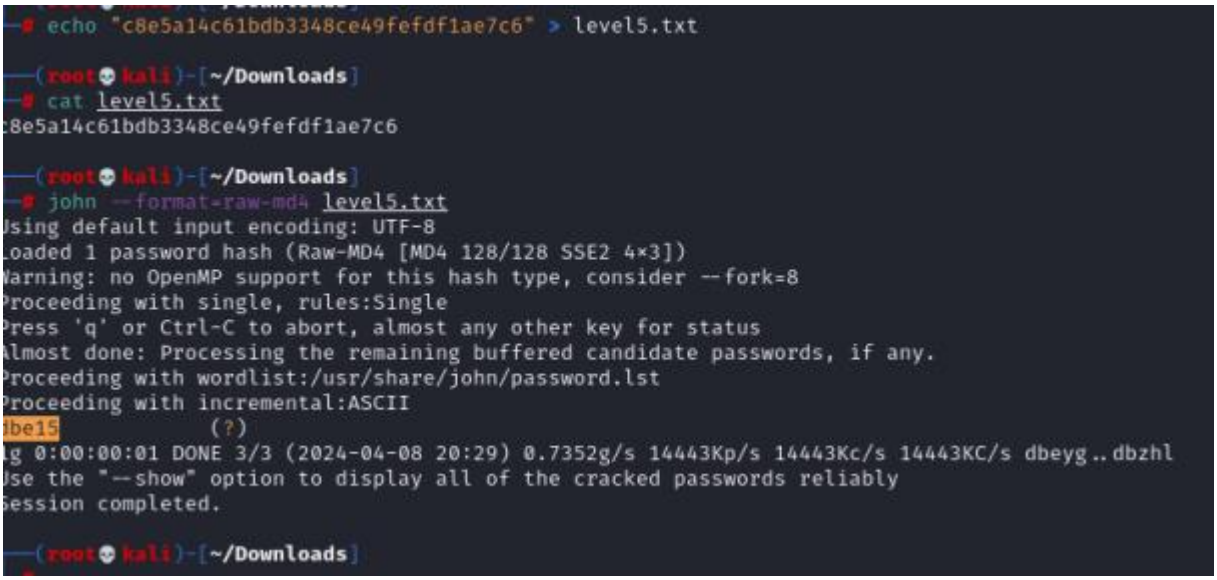
Admin.bak.php dosyasına girdiğimde ise bir hash ile karşılaştım.



error matching hash c8e5a14c61bdb3348ce49fefdf1ae7c6

Hangi algoritma ile hashlendiğini bulmak için dcode.fr web sitesinden yararlandım. İlk üç en yüksek sonuç için teker teker denedim.en sonunda ise md4 ile hashlenm iş olduğunu tespit ettim.



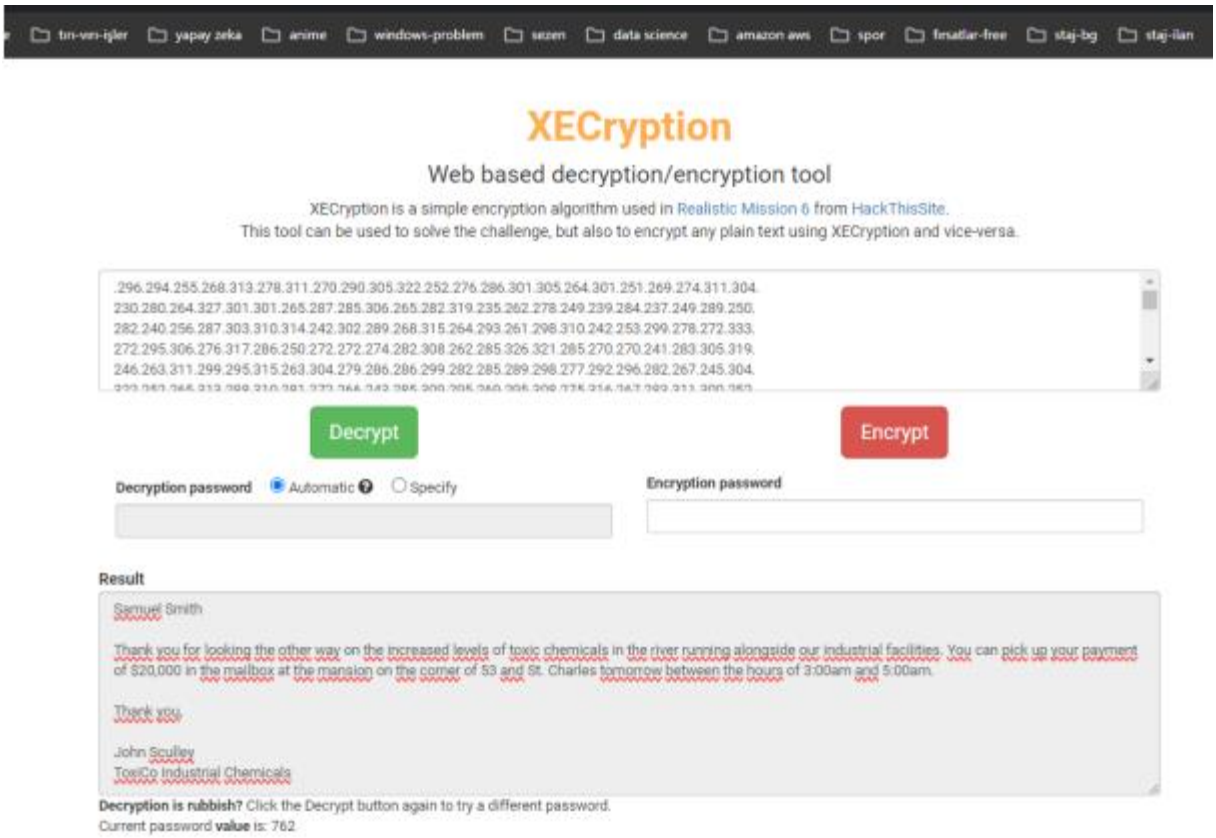


8) **Cryptographic Failures – Basic challenge soru 6**

İlk başta sezar şifreleme methodu kullanıyor diye düşündüm fakat oradan bişey çıkmadı ben de denemeler yapmaya başladım 1234567890 girdisini yolladığımda 13579;=?A9 çıktısı geldi asci olarak ilk karakter hariç 1 er fazlası ile şifrelendiğini fark ettim. ardından ascii tablosunda baka baka şifreyi çözdüm.

9) **Cryptographic Failures - ToxiCo Industrial Chemicals**

Bırakılan ip ucunda XECryption algorithm kullanılarak şifrelendiği söylenmiş. Biraz araştırmayla bu algoritmanın online decoder ını buldum (https://telmo.pt/xecryption/) ve mesajı çözdüm.



Kullanılan ctf platformları:

1)portswigger

2) http://altoro.testfire.net

3) https://www.hackthissite.org