

# YAVUZLAR WEB GÜVENLİĞİ & YAZILIM TAKIMI

## OWASP TOP 10 WRITE-UPS

### 1. TryHackMe - Corridor

Odanın açıklamasında IDOR zafiyeti (OWASP TOP 10 kategorilerinden A01:2021 - Broken Access Control'e karşılık geliyor) bulundurduğu belirtilmişti (<https://tryhackme.com/r/room/corridor>). Siteye girdiğimde Şekil 1.1'deki koridor görseli ile karşılaştım.



Şekil 1.1. Koridor Görseli

Görseldeki 13 adet kapının üzerine geldiğimde ayrı ayrı sayfalara yönlendirmeler yapıldığını gözlemledim. Bu kapıları teker teker açtığımda her bir sayfada, boş bir oda görseliyle karşılaştım. Boş oda görselleri aynıydı. Görseli ve sayfaları incelediğimde herhangi bir şey bulamadım o yüzden koridor görselinin bulunduğu ana sayfaya geri döndüm. Ana sayfanın kaynak kodlarını incelediğimde Şekil 1.2.'deki gibi yönlendirmelerin bulunduğu linkleri gözlemledim.

```

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css"
Integrity="sha384-9aIt2nRpC12Uk95S99aT6vr2U+dr54V64GKRxHyp7cf81896d222Y" crossorigin="anonymous">
<title>Corridor</title>
<link rel="stylesheet" href="/static/css/main.css">
</head>
<body>

<map name="image-map">
<area target="" alt="c4ca4238a0b923820dcc509a6f75849b" title="c4ca4238a0b923820dcc509a6f75849b" href="/c4ca4238a0b923820dcc509a6f75849b" coords="257,893,258,332,325,351,325,860" shape="poly">
<area target="" alt="c81e728d9d4c2f636f067f89cc14862c" title="c81e728d9d4c2f636f067f89cc14862c" href="/c81e728d9d4c2f636f067f89cc14862c" coords="469,766,583,747,581,405,474,394" shape="poly">
<area target="" alt="eccbc87e4b5c2f28388f1d2f2a7baf3" title="eccbc87e4b5c2f28388f1d2f2a7baf3" href="/eccbc87e4b5c2f28388f1d2f2a7baf3" coords="585,698,598,691,593,429,584,421" shape="poly">
<area target="" alt="a07f692232e71b1031a67b7542122c" title="a07f692232e71b1031a67b7542122c" href="/a07f692232e71b1031a67b7542122c" coords="658,668,644,437,658,652,655,437" shape="poly">
<area target="" alt="e4da3b7fbce2345d772b0674a318d5" title="e4da3b7fbce2345d772b0674a318d5" href="/e4da3b7fbce2345d772b0674a318d5" coords="692,637,698,455,695,628,695,467" shape="poly">
<area target="" alt="1679891c5a880faf6b5e687eb1b2dc" title="1679891c5a880faf6b5e687eb1b2dc" href="/1679891c5a880faf6b5e687eb1b2dc" coords="719,628,719,458,728,471,728,689" shape="poly">
<area target="" alt="8f14e45fcee167a5a36dedd4bea2543" title="8f14e45fcee167a5a36dedd4bea2543" href="/8f14e45fcee167a5a36dedd4bea2543" coords="857,612,933,618,936,456,852,455" shape="poly">
<area target="" alt="c9f8f895fb98ab9159f51f0b297e236d" title="c9f8f895fb98ab9159f51f0b297e236d" href="/c9f8f895fb98ab9159f51f0b297e236d" coords="1476,857,1478,354,1537,335,1541,901" shape="poly">
<area target="" alt="45c48cc2e2a077fbdea13f61c7669d26" title="45c48cc2e2a077fbdea13f61c7669d26" href="/45c48cc2e2a077fbdea13f61c7669d26" coords="1124,766,1380,752,1383,481,1325,397" shape="poly">
<area target="" alt="d3944688244259755d38e6d163828" title="d3944688244259755d38e6d163828" href="/d3944688244259755d38e6d163828" coords="1102,695,1217,784,1222,423,1283,423" shape="poly">
<area target="" alt="0512bd43d9caae02c998ba82652dca" title="0512bd43d9caae02c998ba82652dca" href="/0512bd43d9caae02c998ba82652dca" coords="1154,668,1146,661,1144,442,1157,442" shape="poly">
<area target="" alt="c28ad4d76fe97759aa27a8c99bffe718" title="c28ad4d76fe97759aa27a8c99bffe718" href="/c28ad4d76fe97759aa27a8c99bffe718" coords="1185,628,1116,633,1113,447,1182,447" shape="poly">
<area target="" alt="c51ce418c124a18e0b5e4b97fc2af39" title="c51ce418c124a18e0b5e4b97fc2af39" href="/c51ce418c124a18e0b5e4b97fc2af39" coords="1073,689,1081,628,1082,459,1073,463" shape="poly">
</map>
</body>
</html>

```

Şekil 1.2. Ana Sayfanın Kaynak Kodu

Yönlendirme linklerinin en başta Base64 ile şifrelendiğini düşündüm fakat deneyince öyle olmadığını anladım. Biraz araştırdıktan sonra linklerin MD5 ile şifrelendiğini öğrendim. Şifrelenmiş metinleri kırmak için “[www.cmd5.org](http://www.cmd5.org)” sitesini kullandım ve tek tek bütün linklerdeki metinleri çözdüm. Çözülen metinler birden on üçe kadar numaralandırılmıştı.

Hash: 
Type: 

decrypt
Encrypt

Result:
1

Şekil 1.3. Çözülmüş Linkin İçerik Görüntüsü

0

Generate
Clear All
SHA1
SHA256
SHA512
Password Generator

☐ Treat each line as a separate string
☒ Lowercase hash(es)

MD5 Hash of your string: [\[ Copy to clipboard \]](#)

cfcd208495d565ef66e7dff9f98764da

Şekil 1.4. “0” Sayısının MD5 ile Şifrlenmesi

Bunun üzerine 14 numaralı bir kapı olacağını düşünerek 14 sayısını MD5 ile şifreledim ve yönlendirmelerden birinin üzerinde denedim. 404 cevabıyla karşılaştım ve böyle bir sayfa olmadığını anladım. Şansımı 14 ile denedikten sonra 0 ile denemeye karar verdim ve Şekil 1.4.’teki gibi 0 sayısını MD5 ile şifreledim. Aynı şekilde yönlendirmelerin birinin üzerinde deneyince flag’in bulunduğu sayfayla karşılaştım ve odayı çözmüş oldum.



Şekil 1.5. Flag’in Bulunduğu Sayfa

## 2. PortSwigger - Excessive Trust in Client-Side Controls

Laboratuvar, açıklamasında Business Logic zafiyeti bulunduğu belirtiliyor (<https://portswigger.net/web-security/logic-flaws/examples/lab-logic-flaws-excessive-trust-in-client-side-controls>). Bu da OWASP TOP 10 kategorilerinden A01:2021 - Broken Access Control kategorisine karşılık geliyor.

Laboratuvarın başında “Lightweight l33t leather jacket” adlı ürünün satın alınması isteniyordu. Verilen bilgilerle kullanıcı girişi yaptığımda kullanıcının 100\$ bakiyesi olduğunu gördüm. Satın alınması istenen ürün ise 1337\$ olarak satışa konulmuştu. Burp Suite üzerinden intercepti açıp istekleri dinlemeye başladım. İstenen ürünü sepete ekledim ve gelen isteği inceledim. İstekte ürüne ait productId, quantity ve price değerleri bulunuyordu. Gelen istek üzerinden ürün fiyatını 133700 yerine 1 olarak değiştirdim ve isteği ilerletip ürünü sepete ekledim.

```
1 POST /cart HTTP/2
2 Host: 0ab5001104d0510f85baa0aa00c400ec.web-security-academy.net
3 Cookie: session=3C7d8KjnwTi0aHx2kYMISxPjqjPxTpsd
4 Content-Length: 49
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0ab5001104d0510f85baa0aa00c400ec.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0ab5001104d0510f85baa0aa00c400ec.web-security-academy.net/product?produ
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0, i
22
23 productId=1&redir=PRODUCT&quantity=1&price=1
```

Şekil 2.1. Düzenlenmiş İsteğin Ekran Görüntüsü

Store credit:  
\$100.00

Cart

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$0.01	<div><div>-</div><div>1</div><div>+</div></div> <div>Remove</div>

Şekil 2.2. Ürünün Sepetteki Görüntüsü

İsteği ilerlettikten sonra sepeti kontrol ettiğimde ürün fiyatının beklediğim gibi değiştiğini gördüm. Buradan sonra sepeti normal bir satın almaymış gibi onayladım ve satın almayı gerçekleştirdim. Tebrik mesajı ile karşılaştım ve böylelikle laboratuvarı bitirmiş oldum.

Congratulations, you solved the lab!

Store credit:  
\$99.99

Your order is on its way!

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	1
Total: \$0.01		

Şekil 2.3. Laboratuvar Tebrik Görüntüsü

### 3. PortSwigger - High-Level Logic Vulnerability

Bir önceki laboratuvardaki ile aynı isteklerde bulunan bu laboratuvarın açıklamasında da aynı şekilde Business Logic zafiyeti bulunduğu belirtiliyor (<https://portswigger.net/web-security/logic-flaws/examples/lab-logic-flaws-high-level>). Aynı şekilde OWASP TOP 10 kategorilerinden A01:2021 - Broken Access Control kategorisine karşılık geliyor.

Önceki laboratuvarıda yaptığım gibi Burp Suite üzerinden intercepti açıp istekleri dinlemeye başladım. Satın almam istenen ürünü sepete ekledim ve isteği inceledim. İstek içeriğine baktığımda önceki laboratuvarın aksine ürün fiyatı istek üzerinden gönderilmiyordu. Bunu fark ettiğimde ürün sayısını değiştirmeye karar verdim. Ürün sayısını -1 olarak düzenledim ve sepete ekledim. Sepet kısmında satın alma işlemini gerçekleştirmeye çalıştığımda “Cart total price cannot be less than zero” hata mesajı ile karşılaştım.

```
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,in
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a4d00da03cfd505844cb44a00180023.web-security-academy.net/product?pro
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0, i
22
23 productId=1&redir=PRODUCT&quantity=-1
```

Şekil 3.1. Düzenlenmiş İstek İçeriği

Bunun üzerine hedef ürünün fiyatını karşılayacak kadar negatif sayıda ürün eklemeye karar verdim. Bakiyeyi aşmamak için düşük ücretli bir üründen -66 adet sepete ekledim.

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	- 1 + Remove
Giant Pillow Thing	\$19.84	- -66 + Remove

Şekil 3.2. Sepet İçeriğinin Ekran Görüntüsü

Sepet sayfasını incelediğimde 1 adet 1337\$ ve -66 adet 19.84\$ ürünle birlikte toplam 27.56\$'lık tutarla karşılaştım. Sepeti normal bir satın almaymış gibi onayladım ve satın almayı gerçekleştirdim. Satın almadan sonra tebrik mesajı ile karşılaştım ve böylelikle laboratuvarı bitirmiş oldum.

Congratulations, you solved the lab!

Store credit:  
\$6.94

Your order is on its way!

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	1
Giant Pillow Thing	\$19.84	-66

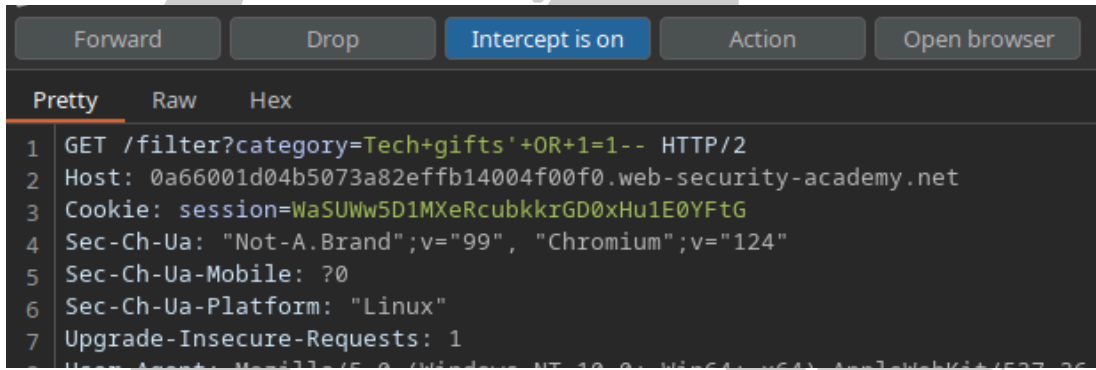
Total: \$27.56

Şekil 3.3. Laboratuvar Tebrik Görüntüsü

#### 4. PortSwigger - SQL Injection Vulnerability in WHERE Clause Allowing Retrieval of Hidden Data

Açıklamasında SQL Injection zafiyeti barındırdığı belirtilen bu laboratuvar haliyle A03:2021 - Injection kategorisine giriyor. Laboratuvarın çözülmesi için daha yayınlanmamış ürünlerin görüntülenmesine neden olan SQL Injection gerçekleştirilmesi bekleniyor (<https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data>).

İlk olarak Burp Suite üzerinden intercepti çalıştırdım. Laboratuvardaki kategori filtrelerinden herhangi birine tıkladım ve gelen isteği inceledim. Filtrelemenin GET metodu ile URL üzerinden gerçekleştirildiğini fark ettim ve URL sonuna basit bir SQL Injection payloadı ekledim.



Şekil 4.1. Düzenlenmiş İstek İçeriği

İsteği ilerlettikten sonra yayınlanmamış ürün kartlarıyla ve laboratuvar tebrik mesajıyla karşılaştım.

Congratulations, you solved the lab! Share your skills!



Tech gifts' OR 1=1--

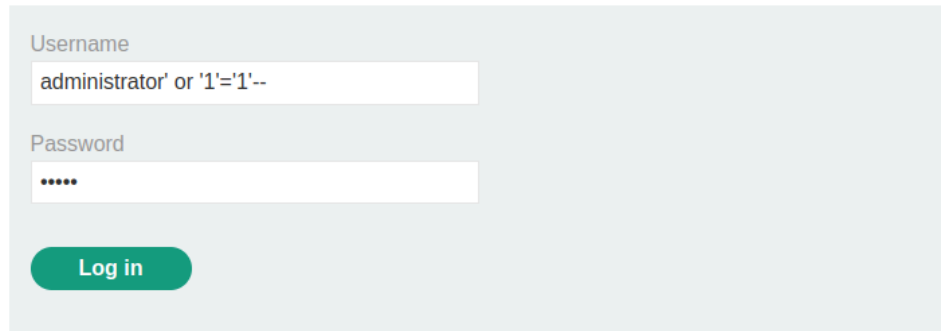
Şekil 4.2. Laboratuvar Tebrik Mesajı

## 5. PortSwigger - SQL Injection Vulnerability Allowing Login Bypass

A03:2021 - Injection kategorisindeki SQL Injection barındırdığı belirtilen bu laboratuvarın çözülmesi için administrator olarak giriş yapılması bekleniyor (<https://portswigger.net/web-security/sql-injection/lab-login-bypass>).

Bunun için laboratuvarın giriş sayfasına geçtim. Giriş sayfasında username kısmına basit bir SQL Injection payloadı, parolaya ise “falan” yazdım ve giriş butonuna tıkladım.

### Login



The screenshot shows a login form with two input fields: 'Username' and 'Password'. The 'Username' field contains the payload 'administrator' or '1'='1'--'. The 'Password' field contains five dots. Below the fields is a green 'Log in' button.

Şekil 5.1. Laboratuvar Giriş Ekranı

Yerleştirdiğim payloaddaki “administrator”dan sonra bulunan “ ' or '1'='1' “ kısım, sisteme herhangi bir şifre girmeden sisteme administrator olarak giriş yapmamı sağladı. Böylelikle tebrik mesajı ile karşılaştım ve laboratuvarı bitirmiş oldum.

Congratulations, you solved the lab!

### My Account

Your username is: administrator

Şekil 5.2. Laboratuvar Tebrik Mesajı



## 6. PortSwigger - OS Command Injection, Simple Case

Laboratuvar açıklamasında, ürün stok denetleyicisinde OWASP TOP 10 A03:2021 - Injection kategorisindeki OS Command Injection zafiyeti bulunduğu belirtilmiş (<https://portswigger.net/web-security/os-command-injection/lab-simple>).

Laboratuvar açıklamasını dikkate alarak önce rastgele bir ürün açıklama sayfasına geçtim. Ürün açıklama sayfasının aşağı kısmında stok kontrol kısmı bulunuyordu. Bunu görünce Burp Suite üzerinden intercept'i açtım ve normal bir şekilde stok kontrolü yaptım. Gelen isteği incelediğimde içeriğinde ürüne ait productId ve storeId değerleri bulunuyordu.

```
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Priority: u=1, i
19
20 productId=1&storeId=1|whoami
```

Şekil 6.1. Düzenlenmiş İstek İçeriği

İstekte bulunan storeId değerinin sonuna “[whoami]” payload’ı ekledim ve isteği ilerlettim. Bunun sonucunda ürün stok sayısının yazması gereken yerde “peter-w87sHX” yazıyordu. Bunu görünce payload’ın çalıştığını anladım ve sayfanın yukarısına çıktığımda laboratuvarı çözdüğüme dair tebrik mesajı ile karşılaştım.

**Web Security  
Academy**

OS command injection, simple case

[Back to lab description](#) >>

**Congratulations, you solved the lab!**

Şekil 6.2. Laboratuvar Tebrik Mesajı

## 7. PortSwigger - Reflected XSS Into HTML Context With Nothing Encoded

Laboratuvarın açıklamasında OWASP TOP 10 A07:2021 - Identification and Authentication Failures kategorisindeki Reflected XSS zafiyeti barındırdığı belirtilmiş (<https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded>). Laboratuvarın çözülmesi için “alert” fonksiyonunun tetiklenmesi gerekiyor.

Bu bilgiyle beraber laboratuvara girdiğimde karşıma blog araması yapılabilen bir searchbox çıktı. Direkt burada XSS denemeye karar verdim ve searchbox’ın içerisine “<script>alert(1);</script>” payload’ı yerleştirdim.



Şekil 7.1. Payload İçeren Searchbox Görüntüsü

Şekil 7.2. Tetiklenmiş Alert Fonksiyonu

Payload yerleştirilmiş searchbox aramasını gerçekleştirdiğimde alert fonksiyonunu tetikledim. Sonrasında ise laboratuvar tebrik mesajı ile karşılaştım.



Reflected XSS into HTML context with nothing encoded

[Back to lab description >>](#)

Congratulations, you solved the lab!

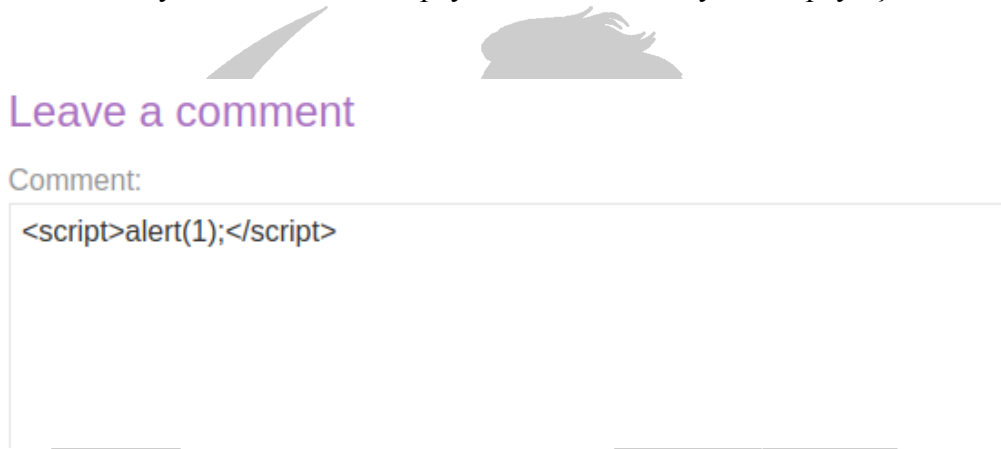
[Share your solution](#)

Şekil 7.2. Laboratuvar Tebrik Mesajı

## 8. PortSwigger - Stored XSS Into HTML Context With Nothing Encoded

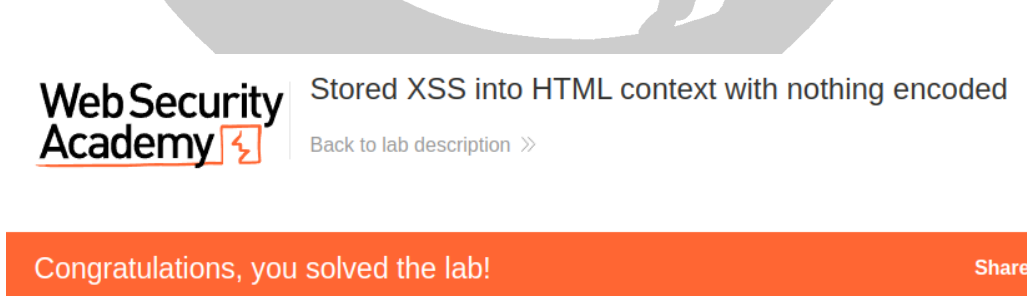
Laboratuvarın açıklamasında OWASP TOP 10 A07:2021 - Identification and Authentication Failures kategorisindeki Stored XSS zafiyeti barındırdığı belirtilmiş (<https://portswigger.net/web-security/cross-site-scripting/stored/lab-html-context-nothing-encoded>). Laboratuvarın çözülmesi için “alert” fonksiyonunun tetiklenmesi gerekiyor.

Laboratuvara girdiğimde listelenmiş blog postlarıyla karşılaştım. Rastgele girdiğim bir postun sayfasında yorum eklenebildiğini fark ettim. Yorum ekleme kısmına alert fonksiyonunu tetikleyecek basit bir XSS payload’ı ekledim ve yorumu paylaştım.



Şekil 8.1. Payload İçeren Yorumun Görüntüsü

Yorumum paylaştıktan sonra sayfayı yeniledim ve alert fonksiyonunu tetikledim. Alert fonksiyonunu tetikleyince laboratuvarı çözmüş oldum ve tebrik mesajı ile karşılaştım.



Şekil 8.2. Laboratuvar Tebrik Mesajı

## 9. PortSwigger - Stored DOM XSS

Laboratuvarın açıklamasında OWASP TOP 10 A07:2021 - Identification and Authentication Failures kategorisindeki Stored XSS zafiyeti barındırdığı belirtilmiş (<https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-dom-xss-stored>).

Laboratuvarın çözülmesi için “alert” fonksiyonunun tetiklenmesi gerekiyor.

Önceki laboratuvardaki gibi aynı şekilde laboratuvar da blog postları bulunuyordu. Rastgele bir posta girdim, yorum sekmesine “<><img src=’falan’ onerror=’alert(1);’/></>” XSS payloadı ekledim. Yorumu paylaştım ve sayfayı yeniledim.

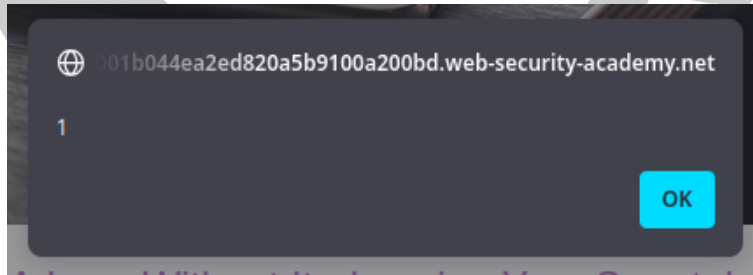
Leave a comment

Comment:

```
<></>
```

Şekil 9.1. Payload İçeren Yorumun Görüntüsü

Sayfayı yenileyince alert fonksiyonunun tetiklendiğini ve laboratuvar tebrik mesajını gördüm. Böylelikle laboratuvarı tamamladım.



Şekil 9.2. Tetiklenmiş Alert Fonksiyonu

Web Security  
Academy

Stored DOM XSS

[Back to lab description >>](#)

Congratulations, you solved the lab!

Şekil 9.3. Laboratuvar Tebrik Mesajı