XSS

...

Cross-Site Scripting
OWASP TOP-10

JavaScript

...

Javascript, HTML, CSS

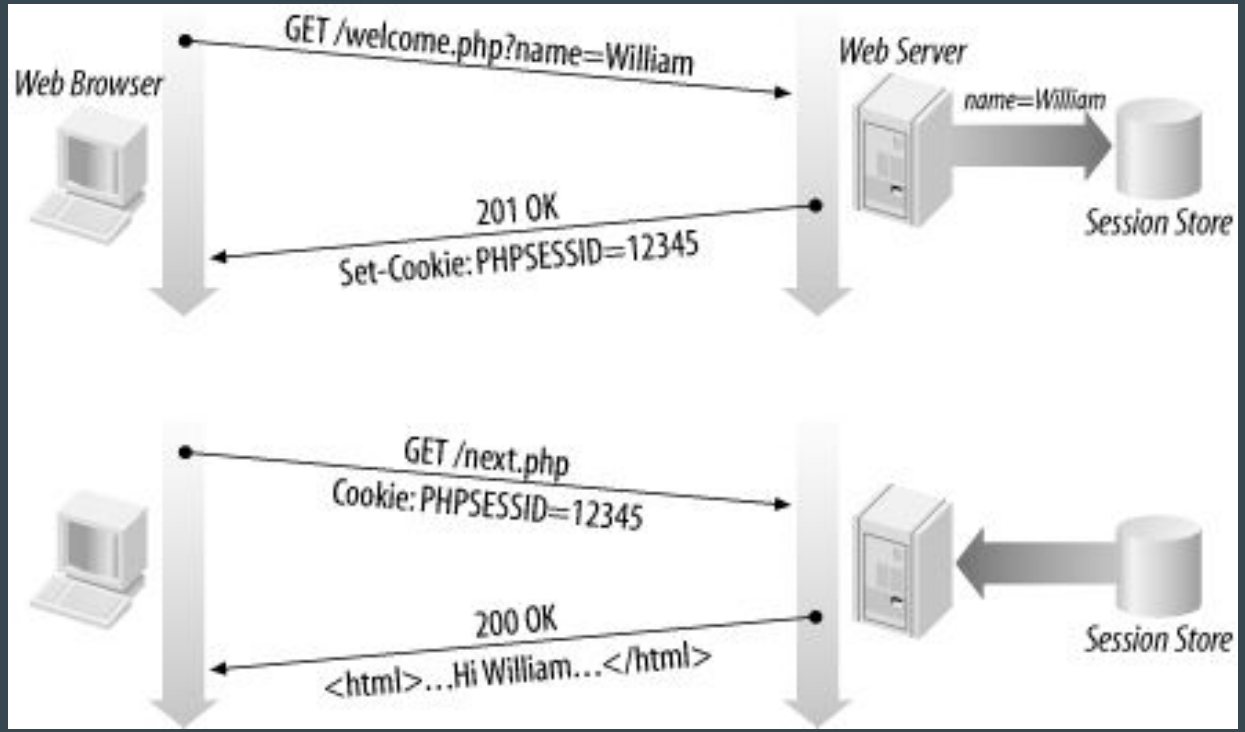
Authentication

...


We got both kinds of authentication factors
username AND password
quickmeme.com

Cookie

Session


Web Browser
GET /welcome.php?name=William
Web Server
name=William
Session Store
201 OK
Set-Cookie: PHPSESSID=12345
GET /next.php
Cookie: PHPSESSID=12345
Session Store
200 OK
<html>…Hi William…</html>

Saldırı ?

...

Hepsi JavaScript'in suçu

Tarayıcılar web sitelerinin kaynak kodu içerisindeki JS kodlarını render eder ve çalıştırır.

```
<html>

<script >alert("AU|Cyber")</script>

</html>
```

Server XSS & Client XSS

...

Server XSS

Sunucuda depolanan verinin son kullanıcıya döndürülmesi ve tarayıcıda render edilmesi sonucu oluşan saldırı tipi

<%=firstName %>

First Name = <script>alert(1)</script>

<%=Request.Form[“FirstName”] %>

Client XSS

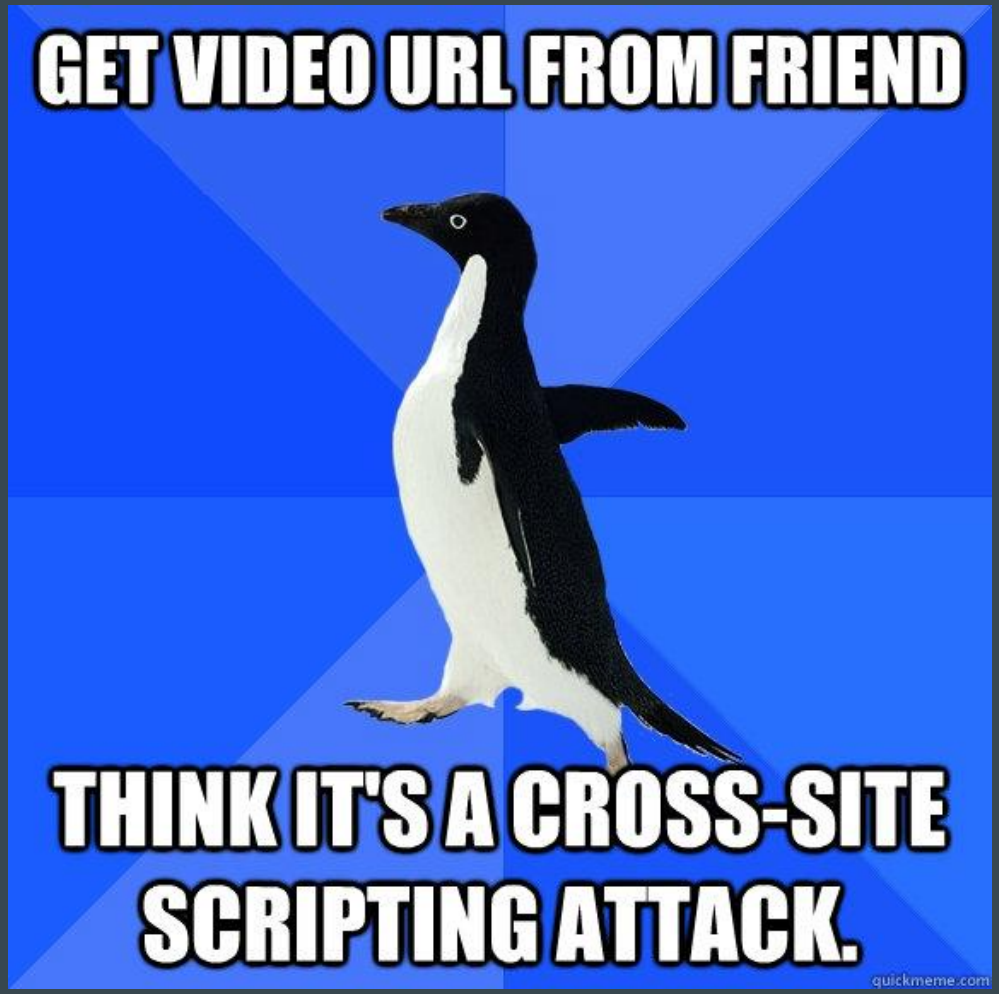
Son kullanıcının, uygulamayı zararlı JavaScript kodu ile manipüle ettiği sadırı tipi

```
<script type=”text/javascript”>

...

   xmlhttp.open("GET", "get_first_name.aspx", true);

   xmlhttp.send(); }

</script>
```

Reflected XSS

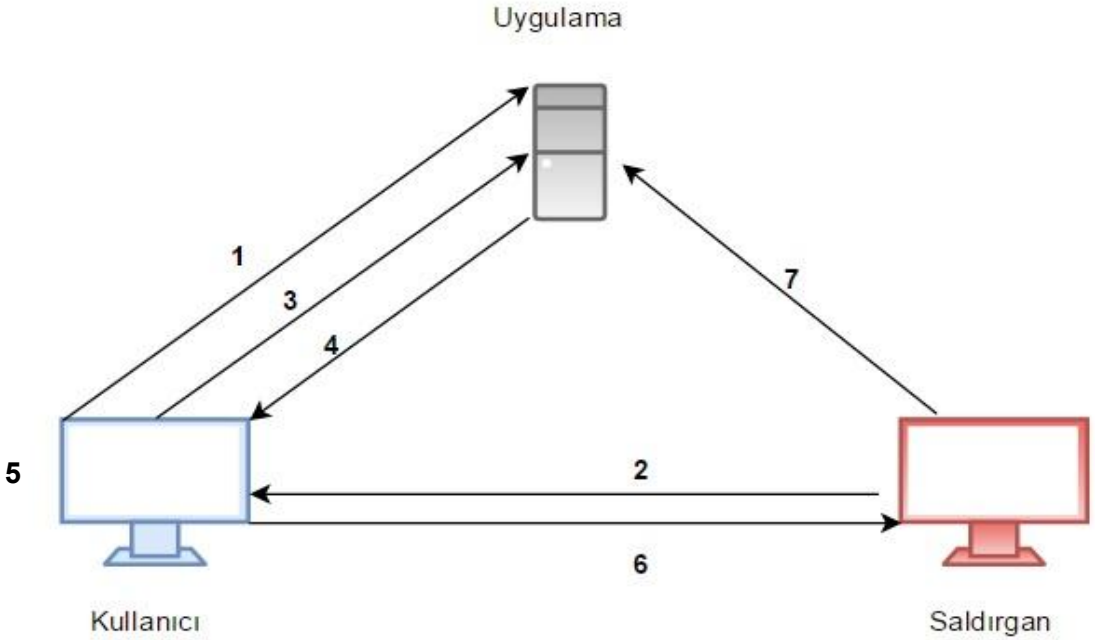
...

Son kullanıcıdan alınan verinin, filtreleme işlemi yapılmadan sonuç olarak döndürülmesinden kaynaklıdır


GET VIDEO URL FROM FRIEND
THINK IT'S A CROSS-SITE SCRIPTING ATTACK.
quickmeme.com

Reflected

```
<?php
$name = $_GET['name'];
echo "Welcome $name<br>";
echo "<a href="http://saldirgan.com/">Click
to Download</a>";
?>
```


Uygulama
1
3
4
7
5
2
6
Kullanıcı
Saldırgan

Reflected

- Kullanıcı oturum açar
- Saldırgan kullanıcıya kendi oluşturduğu URL'i gönderir
- Kullanıcı saldırganın URL'ini talep eder
- Sunucunun dönüşü zafiyetli JavaScript kodu ile olur
- JavaScript kodu kullanıcının tarayıcısında çalışır
- Kullanıcının session token'ı saldırgana gönderilir
- Saldırgan session'ı ele geçirir

Reflected

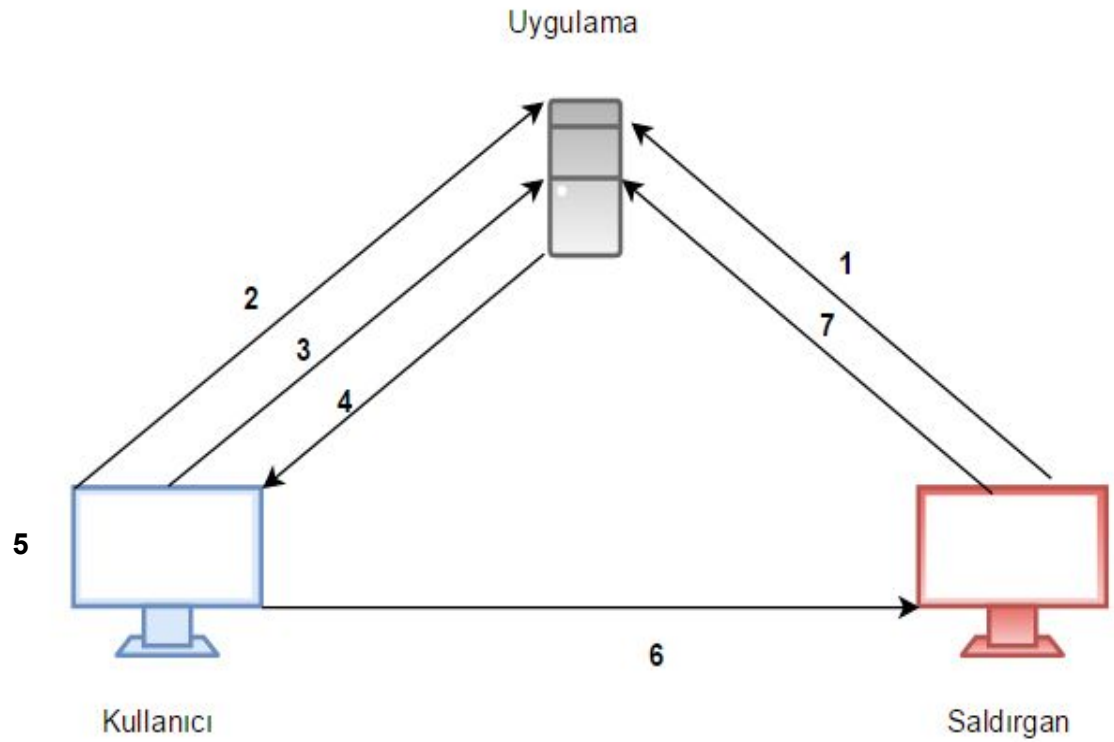
Kullanıcıdan girdi alıp basan ekranlar
Hata ekranları

Web For Pentester 1

Stored XSS

...

Kullanıcı tarafından değiştirilebilir depolanmış verilerin meydana getirdiği açıklar


Uygulama
1
2
3
4
5
6
7
Kullanıcı
Saldırgan

Stored

Ziyaretçi mesajları
Üyelik ekranları
Veritabanına girdi verilen her yer

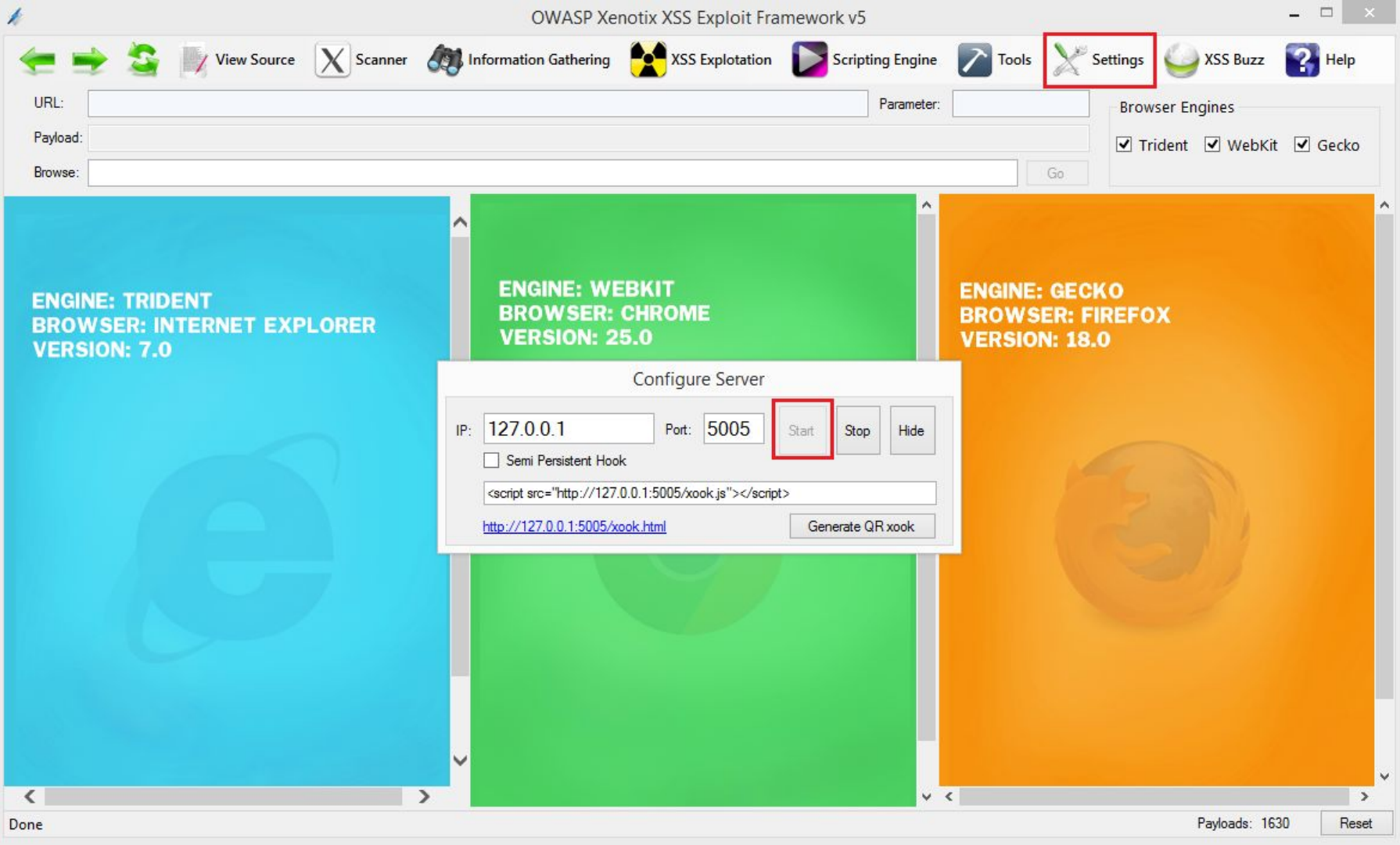
DVWA

Tools

...

Temel bilgisi olmayanlar için XSS uygulamada karışık olabilir.

- **Xenotix** (OWASP tarafından geliştirildi)
- Fiddler
- Netsparker Scanner (ücretli)


OWASP Xenotix XSS Exploit Framework v5
View Source
Scanner
Information Gathering
XSS Explotation
Scripting Engine
Tools
Settings
XSS Buzz
Help
URL:
Parameter:
Payload:
Browse:
Go
Browser Engines
Trident
WebKit
Gecko
ENGINE: TRIDENT
BROWSER: INTERNET EXPLORER
VERSION: 7.0
ENGINE: WEBKIT
BROWSER: CHROME
VERSION: 25.0
ENGINE: GECKO
BROWSER: FIREFOX
VERSION: 18.0
Configure Server
IP:
127.0.0.1
Port:
5005
Start
Stop
Hide
Semi Persistent Hook
<script src="http://127.0.0.1:5005/xook.js"></script>
http://127.0.0.1:5005/xook.html
Generate QR xook
Done
Payloads: 1630
Reset

Korunma Yolları

...

Tek kalıba uygun bir korunma yolu yok.
Ama...

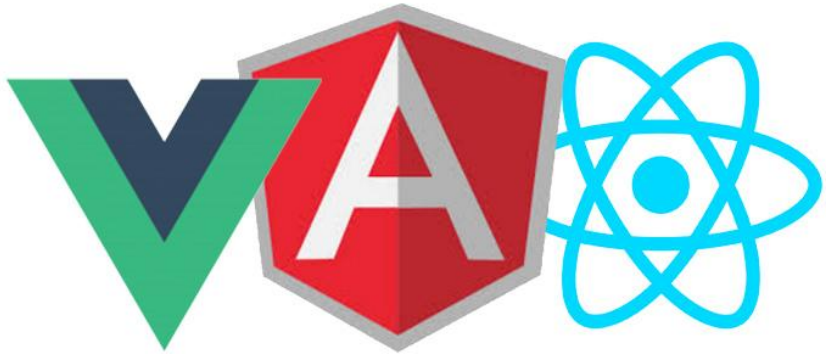
Paired Development

- Bir projede 2 veya daha fazla geliştirici çalışmalı.
- Geliştiriciler birbirinin kodunu review etmeli.

MVVC Javascript Frameworkleri

Javascript değişken manipülasyonu önüne geçmek için Frameworkler kullanılmalı.

- AngularJS (Google)
- React (Facebook)
- VueJS (Bağımsız)



HTML Purifier Kullanılmalı

htmlpurifier.org

HTML üzerindeki güvenilmeyen veri injection açığını en aza indirmek için oluşturulmuş bir **end-to-end purifier** framework.

Server-Side Encryption

- HTTP out
- HTTPS in!

API Güvenligi

Restful API kullanırken client-server cross-check yapılmalı.

API Kanalı manipülasyonunun önüne geçmek için **sunucudan bağımsız authentication** implement edilmeli.