Content disposion ufak olmadığı vakit farketmek zor olduğu için ufak dosya atılır.
(Upload.php üzerinden post et) 1x1 png at

X-Platform :Android
s
Broken access Control

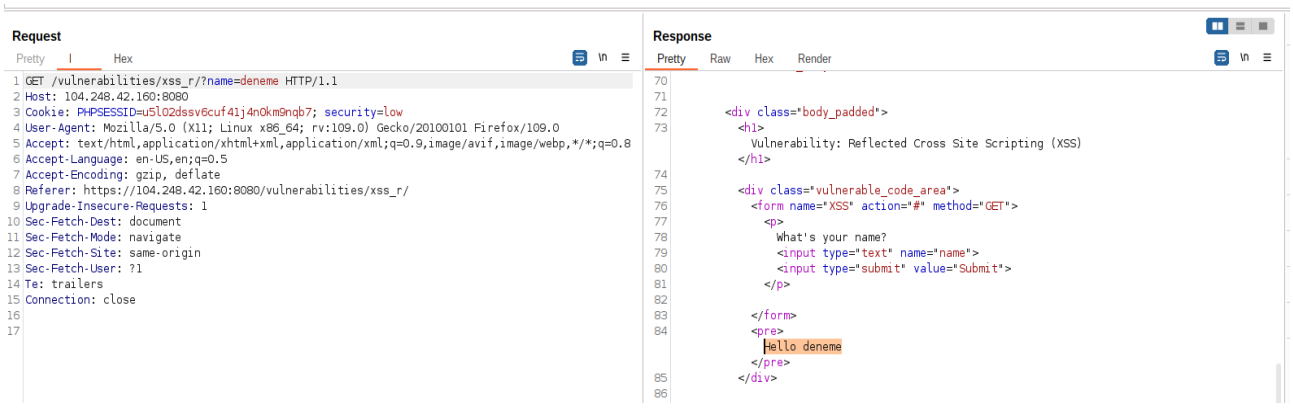
https://owasp.org/www-project-top-ten/
nessus,sqlmap,wiffiDVWA
 En çok Broken Access Control hatalarına dikkat

---
interpreter(yorumlanan)/compileed languages
en büyük fark compiled dillerde executable olmasıdır.

Php App-server ayağı kaldırma php -S 0.0.0.0:8090

#argsv phpde terminalde ön tanımlıdır.
Querystringden veri gönder,Rss

http://0.0.0.0:8090/upload.php?name=%3Cscript%3Ealert(%27denem%27);%3C/script%3E



http://0.0.0.0:8090/upload.php?name=%3Cscript%3Ealert(document.cookie);%3C/script%3E

sonuçları fishing mining yapılır .

XSS olup olmadığını test edilmek için bir inputta ,ilk olarak bad char kullanarak <>0/""; bad charları kontrol et.

Aşağıda ise dvwa için bypass örnekleri mevcuttur.

https://104.248.42.160:8080/vulnerabilities/xss_r/?name=assadas%3Cscri%3Cscript%3Ept%3Ealert%28%27deneme%27%29%3C%2Fscript%3E#

https://104.248.42.160:8080/vulnerabilities/xss_r/?name=%3CscripT%3Ealert%28%27son%27%29%3C%2Fscript%3E#

https://104.248.42.160:8080/vulnerabilities/xss_r/?name=%3Cscript+%3Ealert%28%27son%27%29%3C%2Fscript%3E#

<script >bıraktığında attribute eklendi.

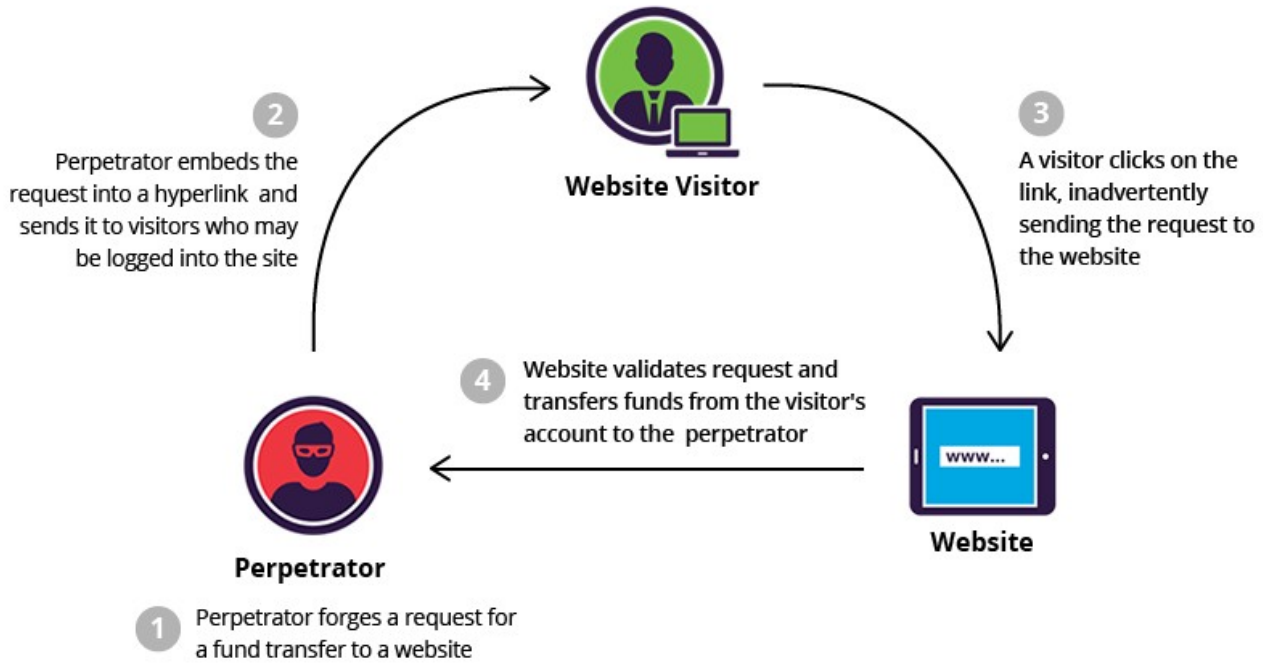
Htmlspecialchars html encode yapar.
context based output encoding

blindxss

Reflected Cross Site Scripting (XSS)

hard bypass
<img src=xxx onerror=alert(1)>

Cross Site Request Forgery (CSRF)istek sahteciliği



Burada en basit mantık şu ,alakasız bir website atarak,istemsizce ana siteye request etmemizi sağlar
---

EN TEMEL LOG YAPISI NASIL OLUŞTURULMALIDIR.:
tarih ip:host http:status:code post
---
cvss score:zafiyetin önem skorunu hesaplatır.

https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L

Scope (S):ortam değişebilirmi

En basit csrf örneği ,burada kullanıcılardan cookieleri alarak ,tarayıcının bağlı bulunduğu websitelerden çıkış yapar.

https://logmeout.co/ deneme

---

csrf korunma yöntemleri

csrf token

eski parola

mail/ telefon controlü

captcha

tokeni sürekli değiştir.rediste yada sessionda tutar.

Tokenları 1.mutlaka expire et ,2.kullanıcı ile eşleştir
