Financira
Evropska unija
NextGenerationEU

THE RECOVERY AND RESILIENCE PLAN

VARNOST PROGRAMOV

Predavanja #5
Matevž Pesek

DANAŠNJE TEME

- XSS, CSRF
- Sanitizacija, CORS
- SSRF
- Avtentikacija

Od prejšnjič

- Kakšni so tipični napadi?
- Zakaj je vzdrževanje pomembno?
- Kako izkoriščamo nedelovanje sistema?

RANLJIVOSTI Z NAPADI PREKO KLIENTA

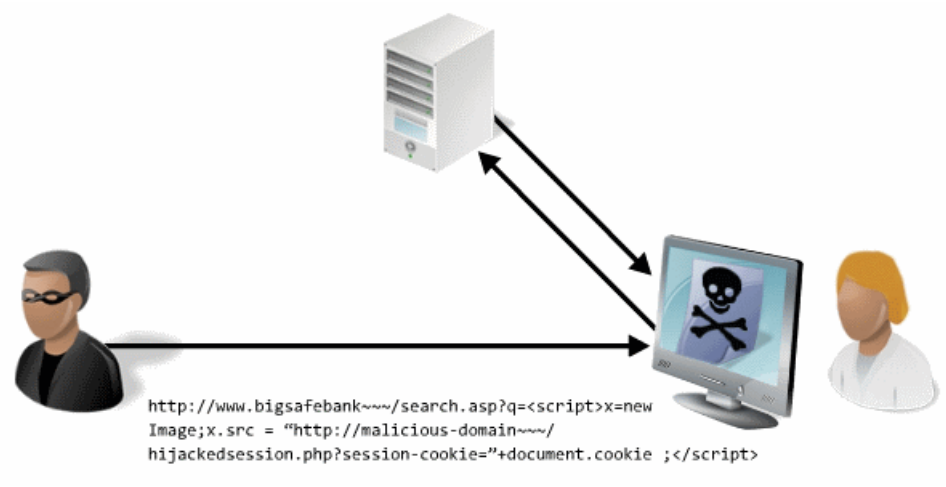
XSS - Primeri

- Pogosto:
  - JS + HTML koda
  - Izvršljive datoteke
  - Vtičniki, multimedijska gradiva ...
- Zaščita je nepopolna zaradi zaupanja sistemu/strani

Tipi XSS

- Reflected XSS
  - Napadalec pošlje ostalim uporabnikom povezavo do “varne” strani, ki naloži dodatno kodo
  - Strežnik servira dodatne parametre (npr. GET) ostalim uporabnikom
- Tipični sistemi
  - Širši napadi, emaili, …

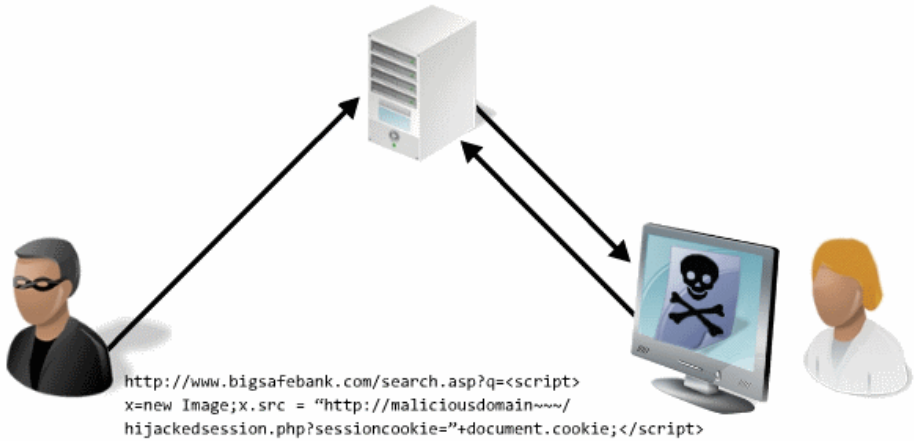
- Primer [levo]



https://www.veracode.com/security/xss#:~:text=Publicly%20visible%20profile%20pages%2C%20like,will%20execute%20the%20code%20automatically.

Tipi XSS

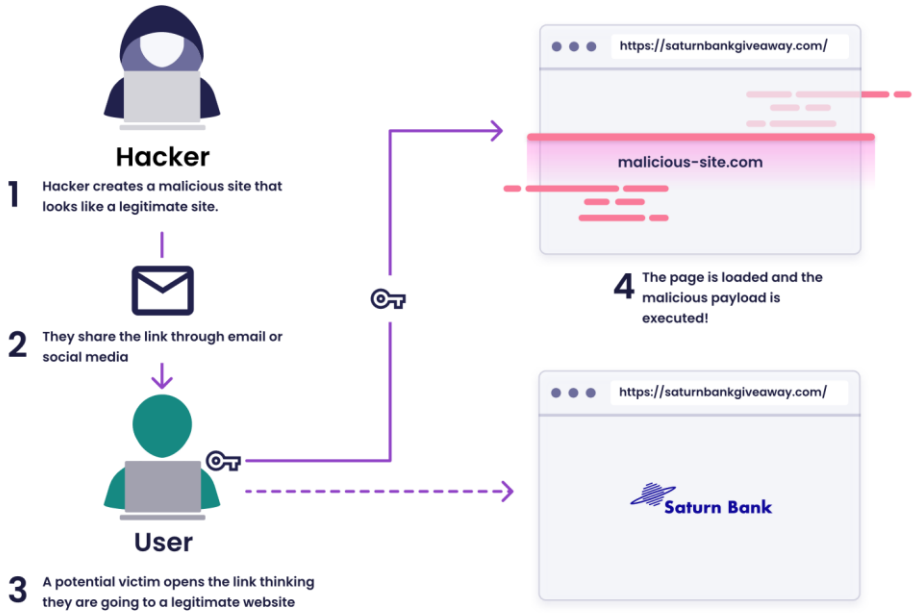
- Stored XSS
  - Napadalec shrani uporabniški vnos na strežnik
  - Strežnik servira uporabniški vnos ostalim uporabnikom
- Tipični sistemi
  - Profili, forumi, družbena omrežja, skupine …
- Primer [levo]



https://www.veracode.com/security/xss#:~:text=Publicly%20visible%20profile%20pages%2C%20like,will%20execute%20the%20code%20automatically.

Cross-site request forgery

- Z domene B delamo poizvedbo na domeno A
- Primer:
  - Dostopamo do napadalčeve spletne strani (B)
  - Na spletni strani (B) se v ozadju izvede poizvedba na legitimno stran (A)
  - Pri poizvedbi uporabi brskalnik poverilnice uporabnika (A) skozi stran (B)



Resnost zlorabe

- Zgodi se zaradi slabe zaščite sistema
- Naprimer:
  - Najdemo stran, ki je zlorabljiva
  - Lahko:
    - ukrademo poverilnice,
    - zlorabimo aktivno sejo za izvedbo akcij,
    - Kraja podatkov iz seje
    - Pošiljanje zbranih podatkov drugam
      - K sebi, na druge sisteme, ...

ZAŠČITA

Minimalne higienične osnove

Zaščita

- Minimalne osnove
  - Sanitizacija nizov (html escaping)
  - CORS
  - HttpOnly piškotki

- Lahko naredimo še mnogo več ...

Sanitizacija nizov

- T.i. “escaping”
  - Podobno kot pri bazah
  - Dopolnilo – “textContent” na poljih (JS)

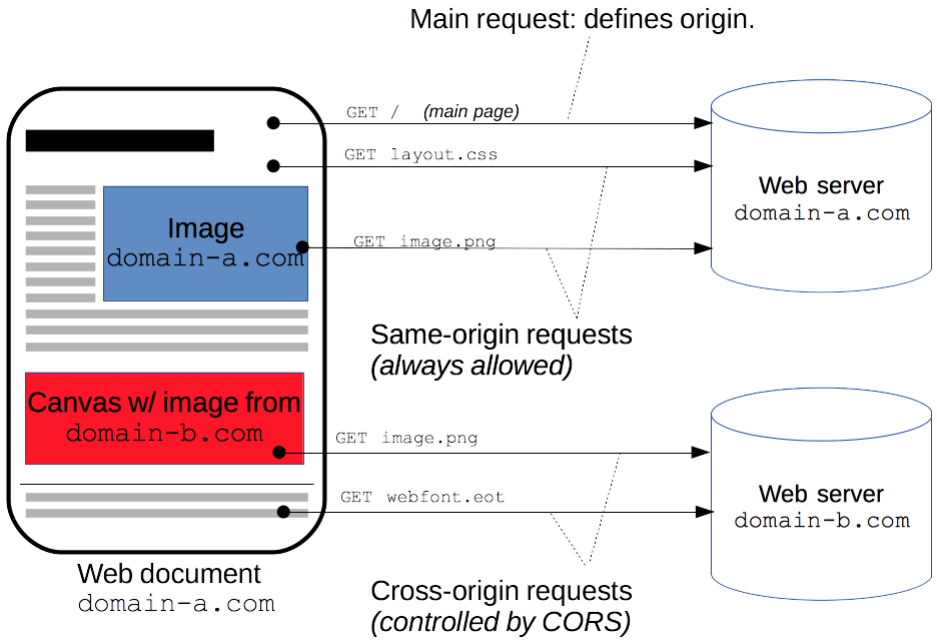
- Minimum:
  - Escaping HTML characters in a string means replacing the:
  - less than symbol (<) with <
  - greater than symbol (>) with >
  - double quotes (") with "
  - single quote (') with '
  - ampersand (&) with &

- Primer [levo]

CORS

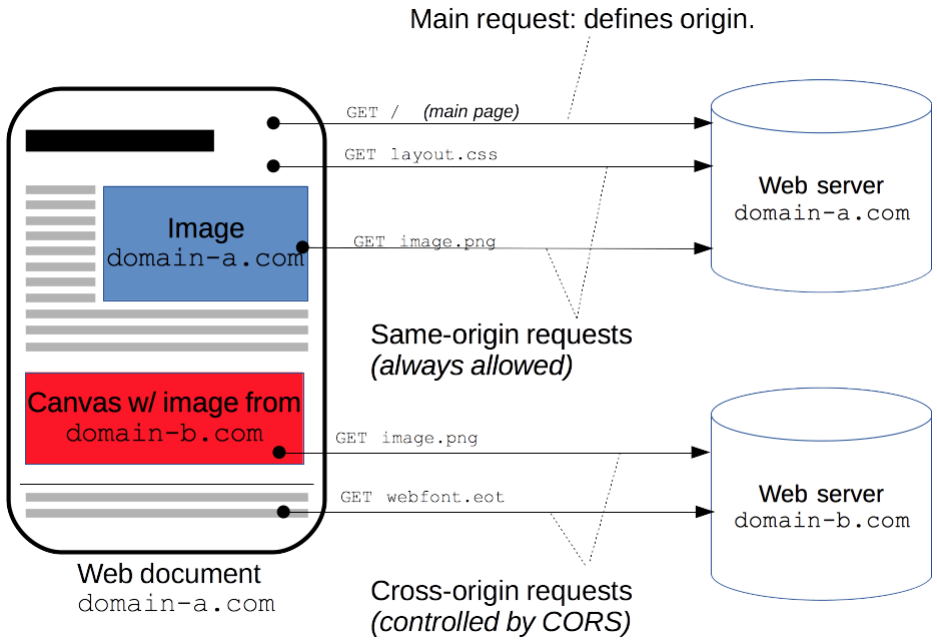
- Chrome in ostali brskalniki od ~ 2009
- Lahko ga zaobidemo
  - Primer slabe prakse!
  - Primeri: API dostopi, “začasne rešitve”

- Primer [levo]



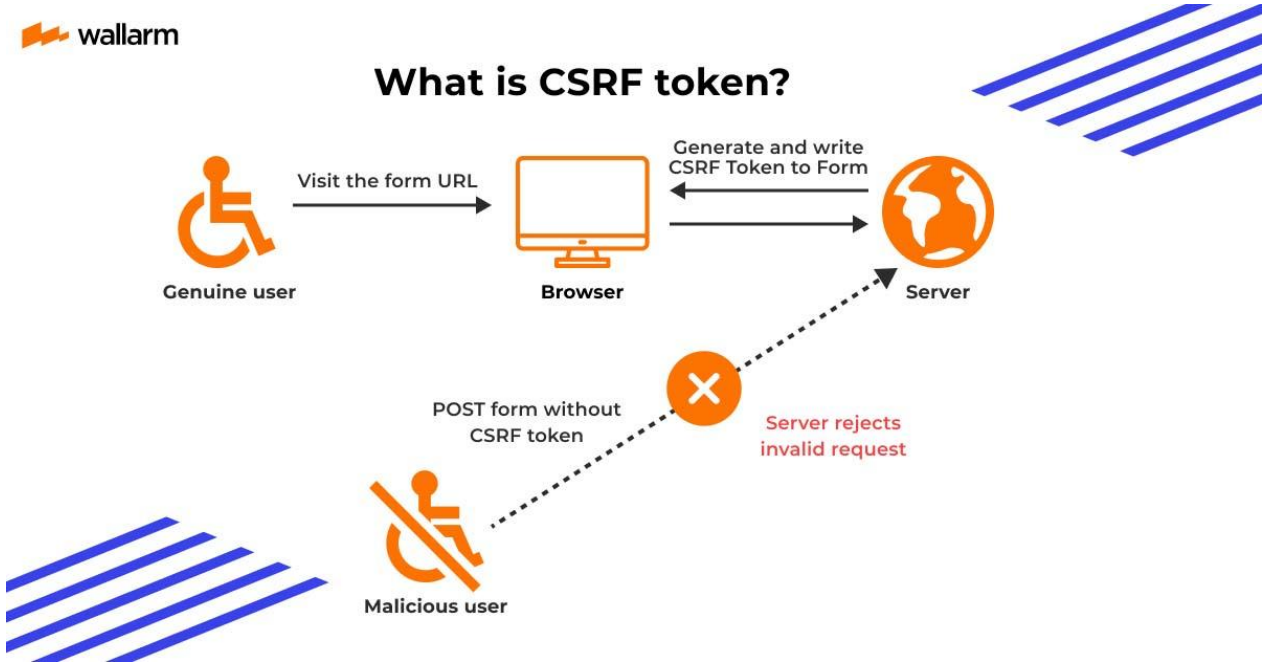
HttpOnly piškotki

- Tri variante:
  - HttpOnly
    - JavaScript nima nadzora nad piškotki
  - Secure
    - Pošiljamo zgolj preko https
  - SameSite
    - Ne dovoljuje drugih domen



CSRF Žeton

- Ob poizvedbi na spletno stran se najprej zgenerira CSRF žeton
- Ko naslednjič naredimo poizvedbo, z žetonom avtenticiramo sejo

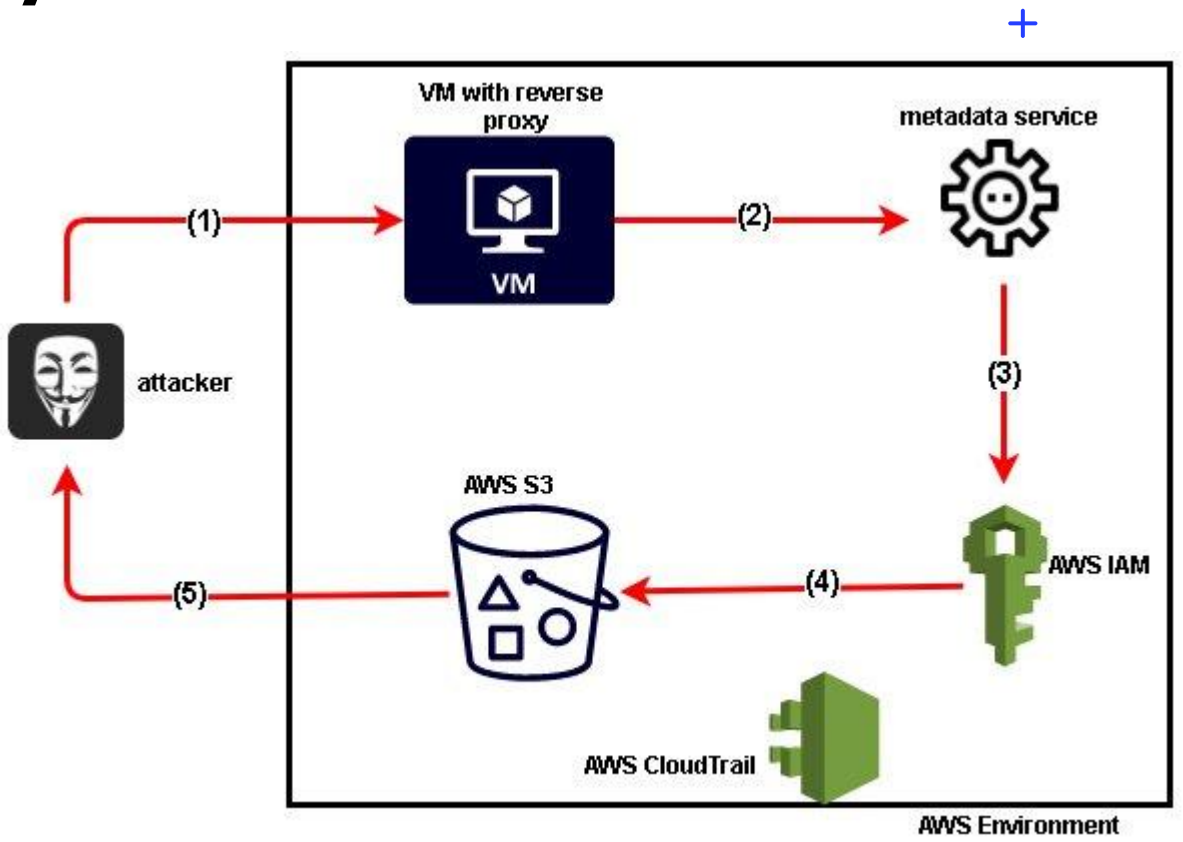


https://www.wallarm.com/what/csrf-token

SSRF NAPADI

Napad preko proxy strežnika

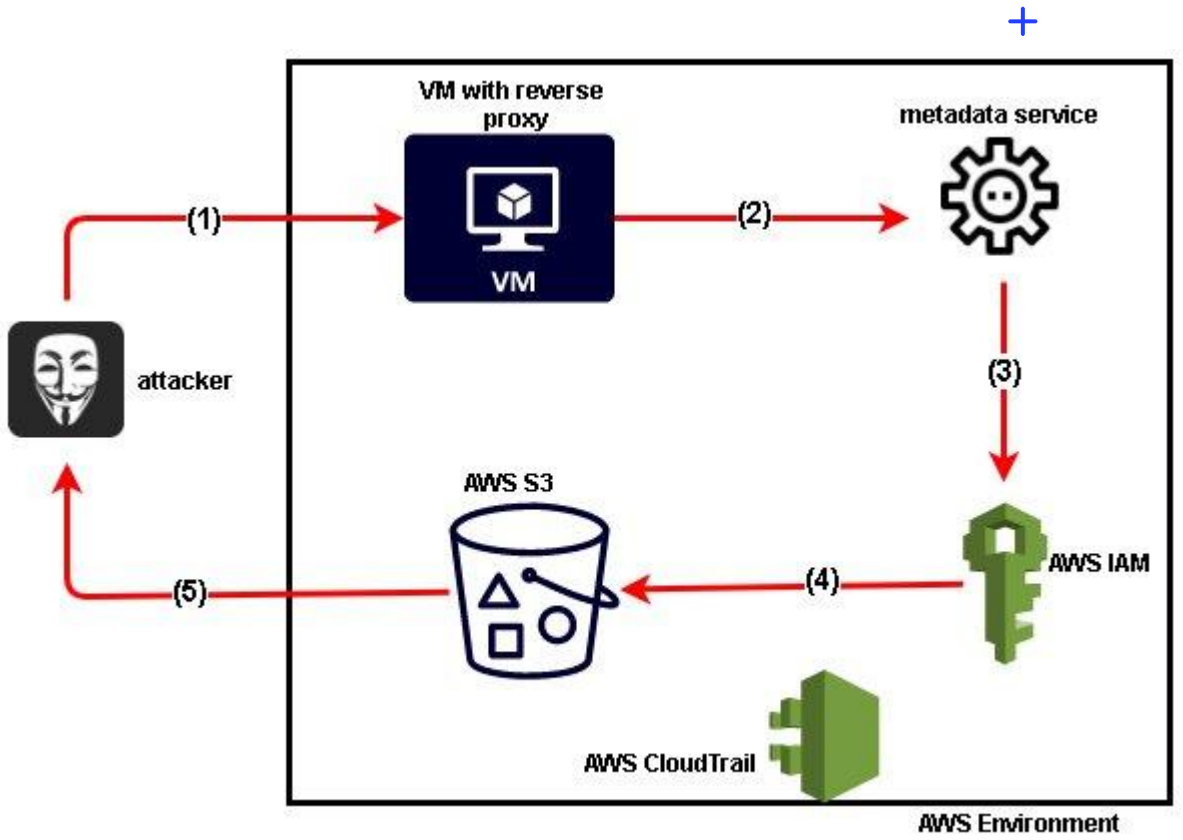
- Dostop do proxy strežnika
- Dostop do zalednih sistemov
- Napad preko absolutizacije relativnih poti
  - /images/abc.png -> https://example.com/...
  - /images/abc.png -> https://localhost/...
  - /images/abc.png -> file:///etc/passwd
- Napadi so možni na različnih protokolih
- Primer [levo]



https://www.researchgate.net/publication/342140502_Cloudstrike_Chaos_Engineering_for_Security_and_Resiliency_in_Cloud_Infrastructure/figures?lo=1

Zaščite SSRF

- Izogibanje uporabe proxy-jev z dinamičnimi poizvedbami
  - https://example.com/url=images/slika.png
- Uporaba prevedenih poti namesto uporabniških poti
  - V bazi hranimo pot do slike in prevedemo /images/{id}.png v to pot
- Politika omrežnega dostopa
  - Samo določeni interni strežniki
  - Samo izhodni promet



https://www.researchgate.net/publication/342140502_Cloudstrike_Chaos_Engineering_for_Security_and_Resiliency_in_Cloud_Infrastructure/figures?lo=1

PRIMERI

Don’t try this at home ;)

Primer: Capital One

Napad

- Reverse proxy z dinamičnimi povezavami
- Dostop do internih strežnikov
  - AWS metadata strežnik
  - IAM service account podatki
- Javni dostop do AWS S3
- Ukradenih 100M+ podatkov o uporabnikih
  - Številke kreditnih kartic
  - SSN

Zaščita

- Popravljen/sanitiziran reverse proxy
- AWS POST poizvedba na do metadata strežnika
- Omejen dostop in pravice service account-ov
- Samo interno dostopna S3 instanca

HVALA

Vaje

- XSS primeri v okolju
- Izdelava popravka in namestitev popravljene kode sistema