Financira
Evropska unija
NextGenerationEU

THE RECOVERY AND RESILIENCE PLAN

VARNOST PROGRAMOV

Predavanja #4

Matevž Pesek

Teme?

- Do nedelje izbira teme
  - Preverite prej (med predavanji/vajami) s prof.
- Izberite temo, ki vas zanima
  - Čeprav je težka!
- Vprašanja?

DANAŠNJE TEME

Uporabniški vnos in problematike

- Podatkovne zbirke in problematike delovanja
- Izkoriščanje ranljivosti v zbirkah

Od prejšnjič

- SQL vrivanje
  - Zakaj je nevarno? Kaj je namen?
- Kakšne tipe SQL vrivanja poznamo?
- Kaj so časovno odvisni napadi?

Baze in sistemi

- Tipični napadi niso nujno kompleksni
- Vzdrževanje je kritičnega pomena
- Zmožnosti so lahko tudi ranljivosti
- Konfiguracija!
- (Ne)delovanje kot cilj
- Varnostne kopije

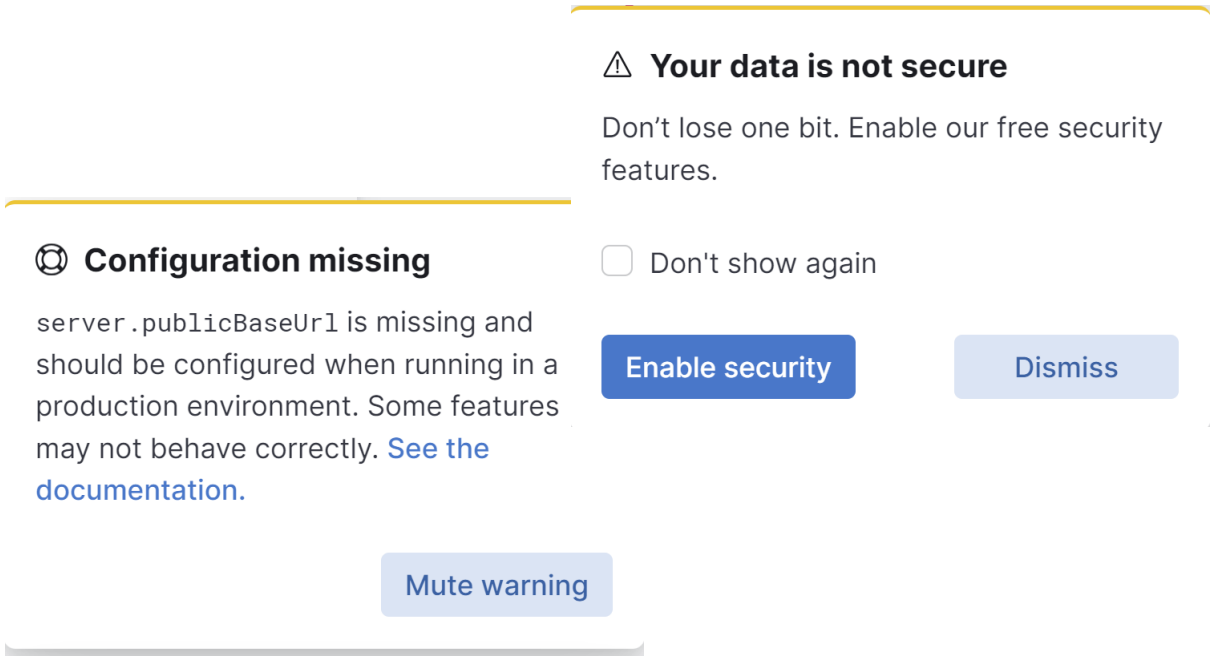
Nekompleksni napadi

- Izkoriščanje ranljivosti uporabnika
  - Omejitve privilegijev
  - Dostopnost login podatkov

- Primeri:
  - “šef ima admin dostop”
    - Omejujemo ljudi po funkciji, ne po hierarhiji
  - Vpeljava (pre)kompleksne zaščite
    - Geslo na tipkovnici
    - Gesla v GIT/repozitorijih
  - (nezazumno) omejevanje dostopa
    - Vpeljava backdoor tehnik za optimizacijo procesa (VPN)

Površnost

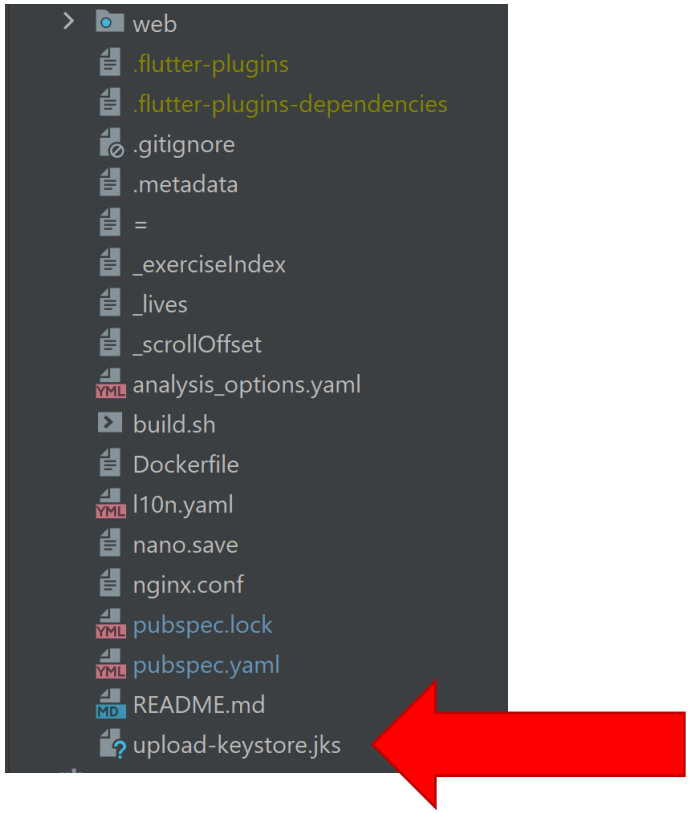
- Izkoriščanje ranljivosti Sistema
  - Default računi (admin/admin)
  - Default konfiguracije



- SQL
  - Root/nopassword
- Sistemi
  - avtenta22 (HSE)
  - srcadmin (JU)
- Elastic/Kibana
  - Popolnoma odprt dostop do različice 7.x
  - Kasneje opcijsko omejitve

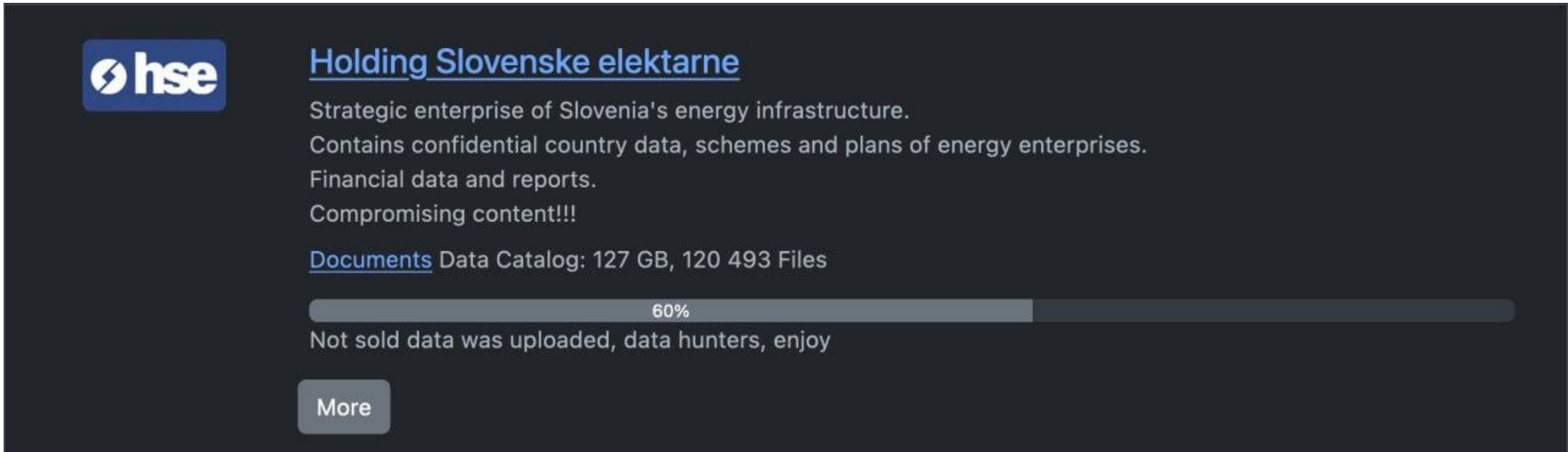
Problematične omejitve

- Google Play store
  - Ključ za aplikacijo – le en
  - Izguba ključa – nezmožnost posodobitve
- Rešitev?
  - Shranjevanje v Git repozitorij
  - Alternative?



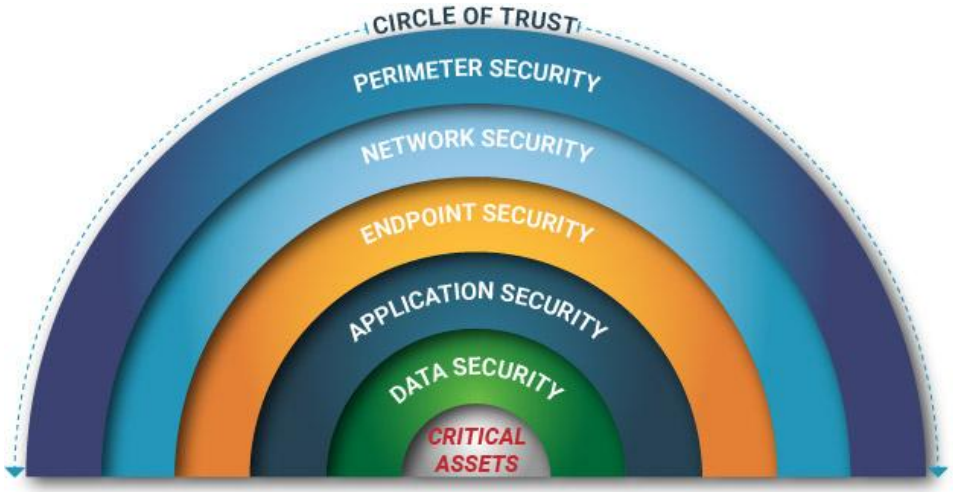
Zakaj pride do teh napadov?

- Dokumentacija
  - Ki to ni
- Odlaganje varnostnih kopij in konfiguracij (dump)
- Krog zaupanja



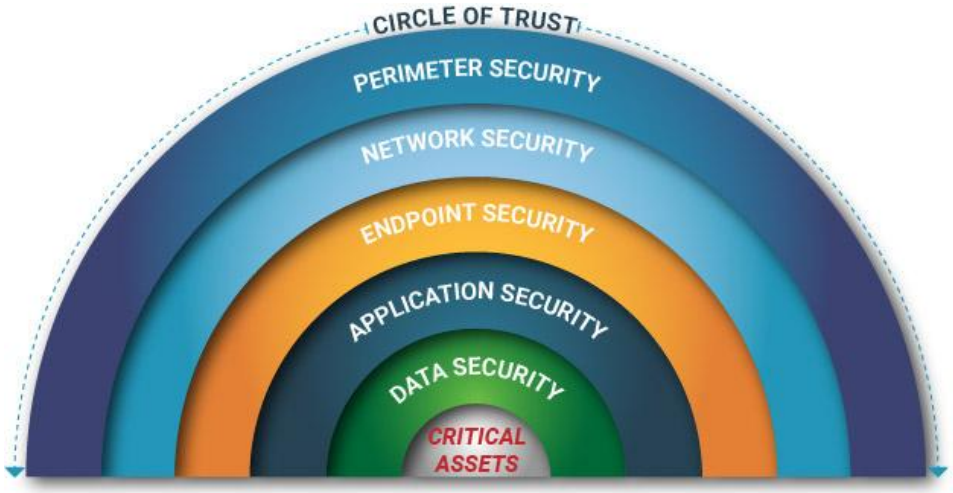
Krog zaupanja (Circle of trust)

- Ne zaupaj nikomur
  - Sploh pa ne uporabniku
  - T.i. “zero-trust model”
- Problem deljenja podatkov z drugimi
  - Sodelovanje med organizacijami/državami
- Kam spadajo e-maili, priponke itd?
  - Tipičen način dostopa do sistema!
- Kaj bomo s “šefom”?



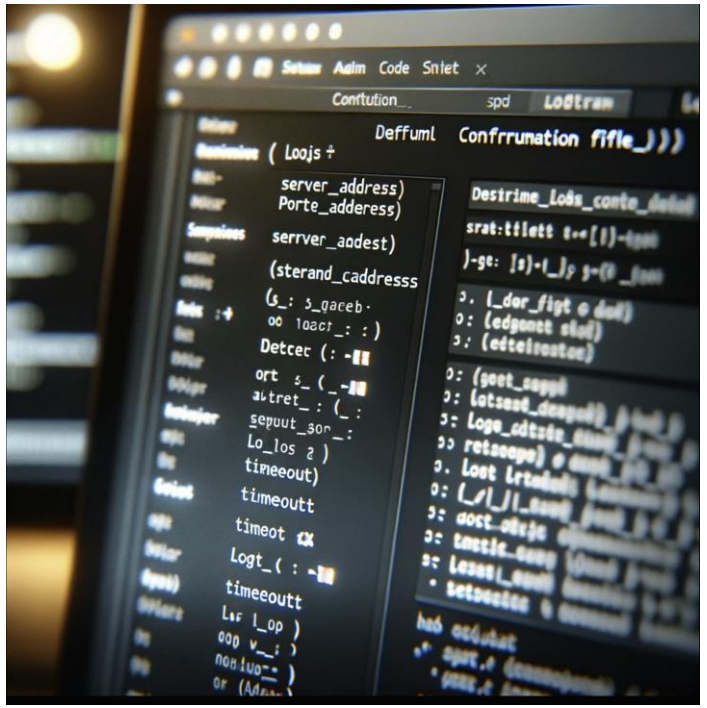
Kje najpogosteje odtekajo podatki?

- Interno
  - Preveč dostopa
  - Premalo samozaščite (uporabnik)
- Eksterno
  - Druge entitete,
  - ne/omejevanje dostopa
  - Naljučni dejavniki
    - Usb ključki, odpisana oprema itd



Super dodatki!

- Omogočanje zmožnosti podatkovne baze/Sistema
  - Default vklopljene zmožnosti
- Izklop zmožnosti, ki jih ne uporabljamo
  - Apache/SQL moduli
  - Dostopi, prikazi, vizualizacije
    - Kibana!
  - Zmanjševanje kompleksnosti



Onemogočanje storitve

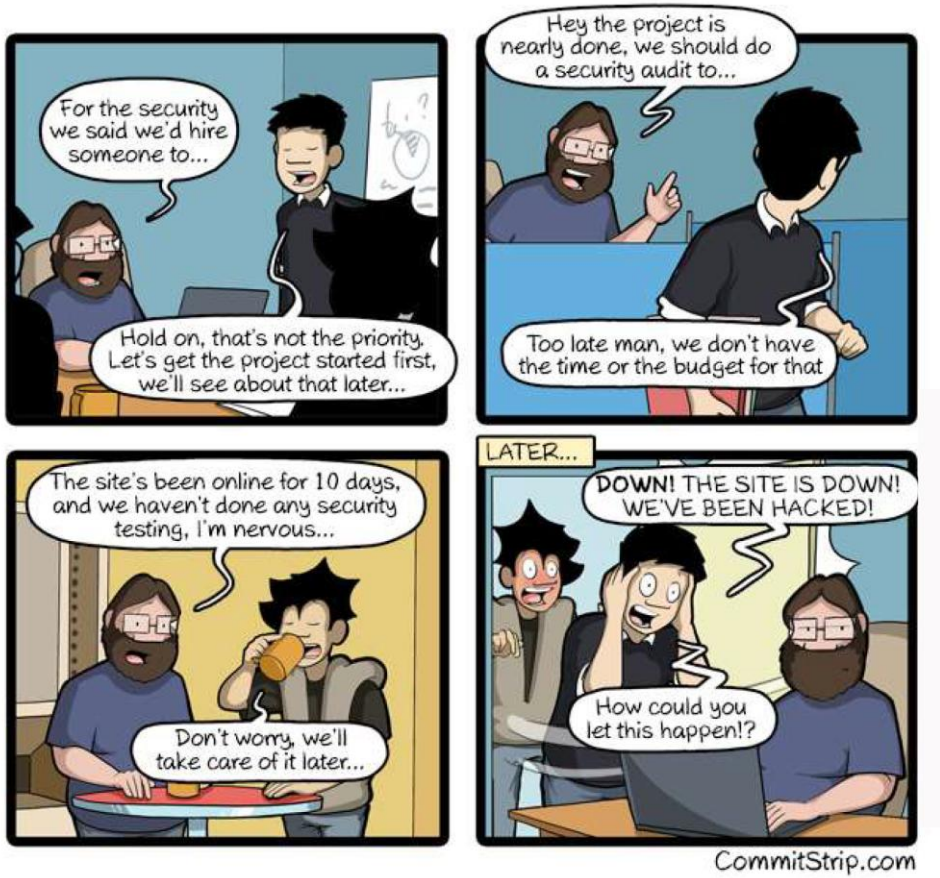
- Na nivoju sistema ali baze
  - Izvedba kompleksnih poizvedb
    - Kompleksni ERP sistemi (SAP, Navision ipd)
  - Izvedba mnogih izvedb (DDoS)
    - Državna infrastruktura
- Lahko je rezultat povzročanje stroškov
  - npr. nakup letne vozovnice in google maps
- Podrobnosti izvedbe
  - Ni nujno tako kompleksno kot se sliši
    - Večina infrastructure nima dobre redundance (single point of failure)
  - Ne potrebujemo nujno velikega števila naprav
    - Primer JU in 1 prenosnika

Večina (vaših) podatkov je že na spletu!

- Varnostne kopije
  - Na varnem mestu
  - V varni obliki (ki je kriptirana)
- Problematika enega uporabnika in mnogih sistemov
  - Isto uporabniško ime in geslo pri mnogih storitvah
- Polnjenje poverilnic (“Credential-stuffing”)
  - poverilnice, pridobljene z vdorom podatkov v eni storitvi, uporabimo za poskus prijave v drugo nepovezano storitev
- Primeri:
  - 23andMe, twitter/X, Norton Life Lock, …

Kako se zavarovati?

- Kot uporabnik:
  - Raznolikost računov (vključno z emaili)
  - Različna gesla, passkey, autogenerate
  - Nikoli ne zaupaj nobeni organizaciji (npr. EU vs. ZDA)
- Kot podjetje:
  - Odvisno od upravljanja na projektu/podjetju
  - Papir prenese vse, pomembna je implementacija
  - Uporabnik je nevešč, programer je len!

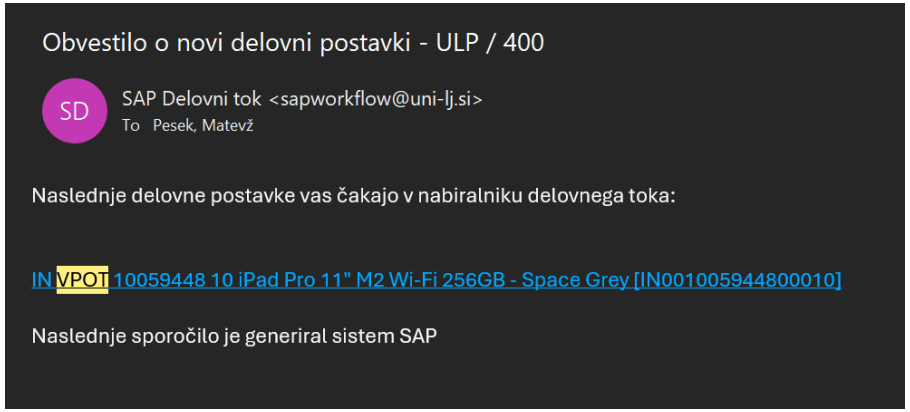


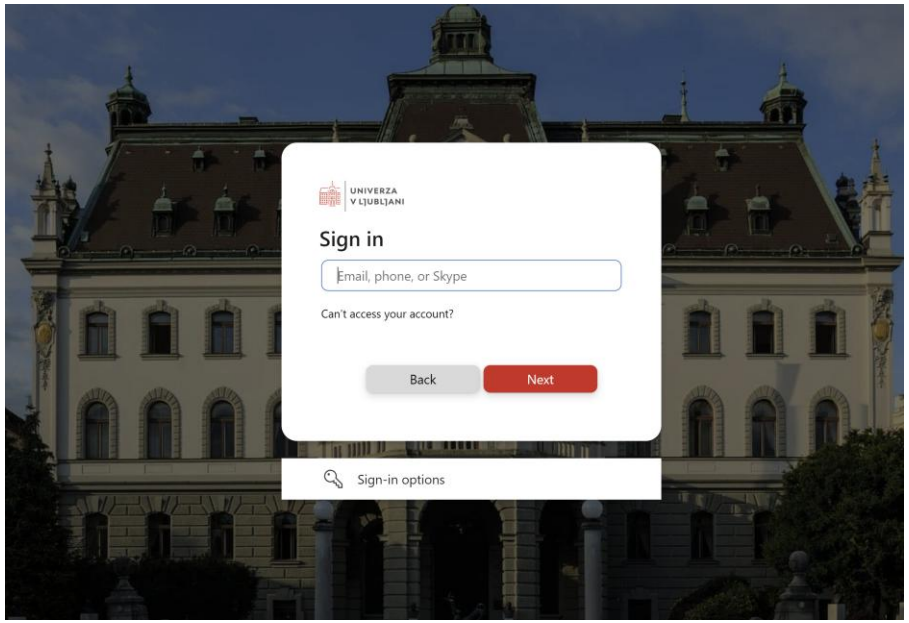
PRIMERI

Don’t try this at home ;)

SAP

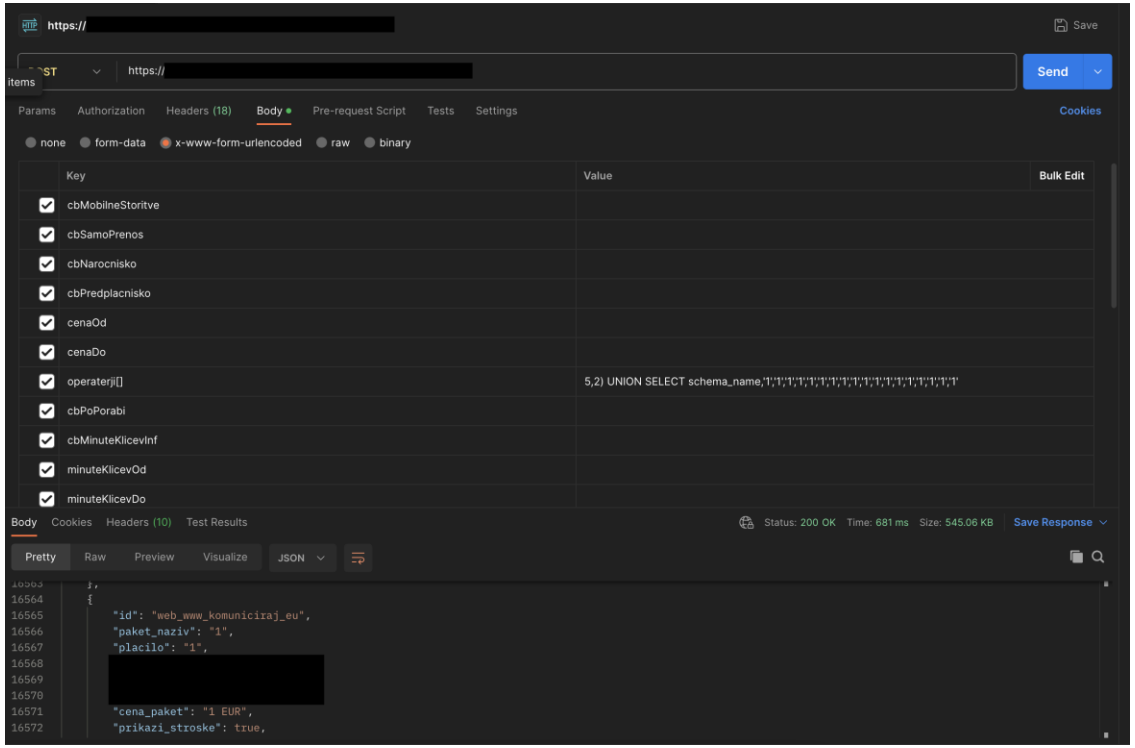
- SAP dostop
  - Email za potrjevanje
  - V 12 urah 550 vpisanih računov
  - Odziv USI - (pre)počasen
    - Email sporočilo je sedelo v nabiralnikih 10+dni
    - Profesorji pregledujejo maile z zamudo po FIFO principu
- Primer postopka (hipotetičen)





Javne agencije

- “Nek hipotetični primer neke javne Agencije”
  - PHP 5.6
  - Manjkala sanitizacija podatkov v seznamih
  - Ekstrakcija podatkov o bazi, tabelah in podatkih s pomočjo UNION stavka
  - Potencialno lahko od tu delamo datoteke, naložimo webshell, sprožimo RCE, itd.



https://book.hacktricks.xyz/network-services-pentesting/pentesting-mysql

TESTNO OKOLJE

Na vajah