Zajímavosti z penetračního testování

Martin Kunc • martin.kunc@nic.cz • 10. 11. 2021

CZ.NIC | SPRÁVCE DOMÉNY CZ

Střípky 1

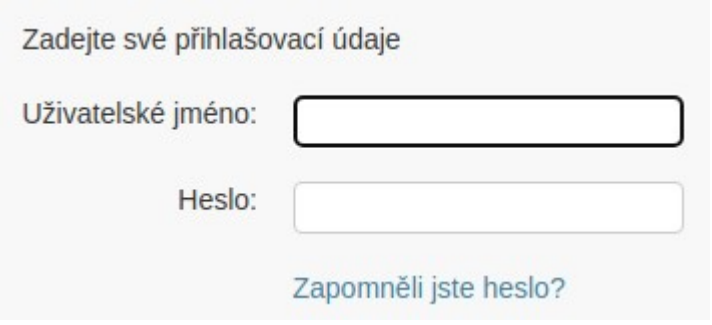
- SQL injection
- Čtení a zápis souborů (uživatel mysql)
- Složka /var/www/html/_uploads s povoleným zápisem pro všechny
- Webshell
- Profit

Střípky 2

- Hádání hesel je stále velmi silný nástroj
- Webmail – 1 uživatel – přihlášení s libovolným heslem

Phishing

- Nezájem ze strany klientů
- Letos první klient
- Více než 1/3 lapených zaměstnanců (přihlašovacích údajů)



Phishing - prequel

- Reakce na dřívější incident (bez dopadu na registr)
- Potřeba zvýšení povědomí o rizicích

Phishing - provedení

- Napodobení komunikace ředitele
- Ekvivalent kradenému účtu
- Navázání na předchozí hromadnou komunikaci
- Časově limitovaná soutěž – „prvních 10“

Phishing - chyby

- Jiné formátování textu
- Chyběl podpis
- URL vedoucí na „cizí“ stránky

Phishing - kudos

- Řešení dle postupů
- .. včetně změny hesla
- Admini připravili pravidlo na zablokování stránky

Pentest – případ

- Turris Omnia
- Minipoty
- Fuzzing
- Neúspěšné vnucení IP adresy do systému Sentinel

Pentest – případ

- MojeID
- aktuálně v řešení
- včetně podpůrných nástrojů

Děkuji za pozornost

Martin Kunc • martin.kunc@nic.cz