

SADRŽAJ

1. UVOD	1
1.1. Web napad.....	1
1.1.1. Ciljevi i motivi napadača.....	2
2. VRSTE NAPADA NA WEB SADRŽAJ	4
2.1. SQL Injection (SQLi).....	4
2.1.1. Alati i tehnike SQL Injection (SQLi).....	7
2.2. Cross-Site Scripting (XSS).....	7
2.2.1. Alati i tehnike Cross-Site Scripting (XSS).....	9
2.3. Cross-Site Request Forgery (CSRF)	9
2.3.1. Alati i tehnike Cross-Site Request Forgery (CSRF)	11
2.4. Denial of Service (DoS) i Distributed Denial of Service (DDoS)	11
2.4.1. Denial of Service (DoS)	11
2.4.2. Distributed Denial of Service (DDoS)	12
2.4.3. Sličnosti i razlike	13
2.4.4. Alati i tehnike Denial of Service (DoS) i Distributed Denial of Service (DDoS)	14
2.5. Man-in-the-Middle (MitM) napadi	14
2.5.1. Alati i tehnike Man-in-the-Middle (MitM) napadi	16
2.6. Clickjacking	17
2.6.1. Alati i tehnike Clickjacking.....	18
2.7. Session Hijacking.....	18
2.7.1. Alati i tehnike Session Hijacking	20
2.8. Path traversal	21
2.8.1. Alati i tehnike Path Traversal.....	22
2.9. Command Injection	23
2.9.1. Alati i tehnike Command Injection	25
3. ALATI I TEHNIKE ZA NAPAD	26
4. POSLJEDICE NAPADA NA WEB SADRŽAJ	29
5. METODE ZAŠTITE I PREVENCIJE	32
6. ANALIZA NAJPOZNATIJIH NAPADA	34
7. ANALIZA TRENUTNIH SIGURNOSNIH STANDARDI I PRAKSA	36
8. NAJNOVIJI TRENDVI U OBLASTI WEB SIGURNOSTI.....	38
8.1. Studije slučaja i primjeri iz prakse	38
9. ZAKLJUČAK	40
10. LITERATURA.....	41