

DNS rebinding (Edhem Avdagić)

Zadatak

Zadatak je:

1. istražiti vrstu napada/ranjivosti poznatu pod imenom DNS rebinding,
2. jasno objasniti kako taj napad funkcionira
3. i pripremiti demonstraciju napada.

Seminarski rad treba kroz tekst odgovoriti na sljedeća pitanja te dati primjere i jasne ilustracije:

1. Što je to IP adresa, što je domena/domensko ime, može li više domena pokazivati na jednu IP adresu?
2. Može li se više Web stranica na različitim domenama nalaziti na istoj IP adresi?
3. U takvoj situaciji, kako Web poslužitelj zna koju Web stranicu treba poslužiti? Kako tada funkcioniraju drugi Web mehanizmi, primjerice HTTP kolačići?
4. Što je to "same-origin policy", za što služi, kako funkcionira?
5. Što je to DNS rebinding napad/ranjivost, kako funkcionira?
6. Koji su primjeri DNS rebinding ranjivosti iz prakse (npr. u nekom poznatom softveru)?
7. Pripremiti demonstraciju napada za prezentaciju seminarskog rada.
8. općeniti savjet za ovu temu: prvo proučite napad i pripremite demonstraciju, pa kada Vam je jasno kako funkcionira, krenite na pisanje

Neki korisni izvori:

1. općenito o DNS rebindingu:
<https://medium.com/@brannondorsey/attacking-private-networks-from-the-internet-with-dns-rebinding-ea7098a2d325>
2. korisna stranica za izradu demonstracije ranjivosti: <https://lock.cmpxchg8b.com/rebinder.html>

Plan rada

Vremenski plan rada

Datum	Aktivnost

Dnevnik rada

Datum (tjedno)	Aktivnost	Utrošak vremena	Daljnji rad
25. 3. - 31. 3.	Upoznavanje sa osnovama tematike (IP, domene, DNS)		Upoznavanje sa samim napadom
1. 4. - 7. 4.	Sakupljanje literature i video-predavanja o DNS rebindingu, upoznavanje sa detaljima same-origin policy-ja, pronalazak alata za demonstraciju napada		Izrada demonstracije napada

Rezultat

Zaključak

Prijedlog za daljnje istraživanje

From: <http://studentski-izvjestaji.zesoi.fer.hr/> - **Studentski izvještaji**

Permanent link: http://studentski-izvjestaji.zesoi.fer.hr/doku.php?id=studenti:edhem_avdagic:ea_ps_I_2018&rev=1554289625

Last update: **2023/06/19 16:21**

