Sigurnost web aplikacija

Trajanje treninga: 5 dana (08h-16h ili 09h-17h, petak 08h-13h) – 6h30min + pauze
(pauza za ručak– 1 sat, pauze za kavu– 15 min x 2)

Potrebno predznanje: Trening „Pogled na sigurnost računalnih sustava s „tamne“ strane“, poželjno je imati znanje i iskustva s treninga: „Praktična primjena tehnika napada na računalne sustave“

Na treningu se kroz 5 dana obrađuje sljedeće:

Sigurnosni koncepti – ukratko će biti pokriveni osnovni koncepti sigurnosti, kao što su CIA i DAD trokut i sveobuhvatna zaštita. Raspravljat će se i o trenutnim prijetnjama i rizicima kojima su izložene web aplikacije.

Koncepti web tehnologija i framework-ova – Ovaj je modul baza za ostatak predavanja, Obradit će se web tehnologije koje se danas najčešće koriste, kao što su: Java, .NET, PHP i Flash, te sam HTTP protokol i *cookies*. Spomenut će se osnovni problemi vezani uz web aplikacije, te će se proći kroz OWASP top 10 ranjivosti, koje će u kasnijim modulima biti detaljno obrađene.

Koncepti i razlike web servera – Modul obrađuje osnovne koncepte i ranjivosti vezane uz najpopularnije web servere (Apache, Tomcat, MS IIS).

Alati – kako bi bili u mogućnosti ispitati sigurnost web aplikacija potrebno je razumjeti protokole i i alate pomoću web debugger proxy-a koji nam mogu pomoći u identificiranju ranjivosti u ulaznim točkama aplikacije i u pronalaženju grešaka. Korištenjem web debugger proxy-a kao što su: Burp, ZAP, Web Scarab, Fiddler isl., jednostavno je mapirati aplikaciju i identificirati parametre koji se koriste. Najbolji način učenja je praktični dio, pa će polaznici u vježbi koristiti BURP i ZAP proxy kako bi otkrili jednostavne ranjivosti poput file/directory enumeracije isl.

Obilaženje kontrola na klijentskoj strani – Jedna od bitnijih stvari koje treba testirati u modernim web aplikacijama je unos na klijentskoj strani. Problem je u tome što aplikacija ne smije vjerovati ničemu što je poslano s klijentske strane, jer može biti manipulirano. Polaznici će kroz vježbu imati priliku modificirati podatke koje klijentska strana šalje serverskoj i na taj način mijenjati ponašanje same aplikacije.

Napadi na autentikaciju – Polaznici će se upoznati s različitim autentikacijskim mehanizmima, kao što su: HTML form bazirana autentikacija, multifaktorska autentikacija, klijentski i serverski certifikati, HTTP basic i digest autentikacija, te windows integrirana autentikacija. Budući je PKI (public key infrastructure) jedna od najbitnijih komponenti sigurnosti web aplikacija, bit će detaljno objašnjena. Demo će pokazati kako je moguće koristiti automatizirani pristup i podesiti *brute force* napad pomoću BURP alata.

Napadi na web aplikacije: Injection (A1) – U ovom će se modulu polaznici upoznati s SQL i LDAP injection napadima. Biti će objašnjeno koliko duboko napadači mogu prodrijeti korištenjem navedenih napada. Polaznici će isprobati razne SQL injection napade kroz vježbe predviđene za ovaj modul.

Napadi na web aplikacije: XSS/CSRF (A3/A8) – Polaznici će se upoznati s različitim XSS napadima (pohranjeni, reflektirani i DOM bazirani). Dodatno ćemo se pozabaviti CSRF napadima i načinima zaštite od istih. Pomoću BeeF alata biti će demonstrirano koliko opasni mogu biti XSS napadi. Kroz vježbu, polaznici će imati priliku iskoristiti pohranjenu XSS ranjivost i preko nje ukrasti informacije o *session*-u, te je iskoristiti u narednom modulu za impersonaciju administratora i krađu njegovog *session*-a.

Napadi na web aplikacije: Broken authentication and session management (A2) – HTTP protokol je po dizajnu nesiguran protokol koji nije orijentiran prema konekciji.U ovom modulu, polaznici će se upoznati s klasičnim problemima vezanim uz upravljanje *session*-om. Vježba pokazuje kako se može ukrasti korisnikov *session* krađom *cookie*-a, te zašto je upravljanje *session*-om preko parametara problematično.

Ostali učestali napadi – većina sigurnosnih problema danas vezana je uz nesigurne direktne reference prema objektima i neadekvatne kontrole pristupa. DOR (Direct Object Reference) problemi opisani su u ovom modulu, a vježba pokazuje kako neispravno implementirane kontrole prilikom pristupa fileovima mogu narušiti sigurnost aplikacije. Svaka aplikacija ovisi o infrastrukturi na kojoj je implementirana. Ukoliko je softver nepatchiran ili su uključene nepotrebne, a potencijalno ranjive funkcije, napadač to može iskoristiti u svoju koristi te ostvariti pristup aplikaciji. Često će neispravno upravljanje greškama dovesti do curenja osjetljivih podataka, koje napadač može iskoristiti u slučaju pojave dodatnih propusta. U ovom modulu bit će obrađeni primjeri koji pokazuju neke od osjetljivih informacija kojima je moguće pristupiti na ovakav način. Redirekcije i prosljeđivanja (engl. *forwards*) moguće je iskoristiti u maliciozne svrhe raznim načinima. Polaznici će se upoznati s HTTP Response Splitting napadima. Također će biti obrađene redirekcije između HTTP i HTTPS protokola, te *Secure cookie flag*. Bit će demonstriran alat SSLStrip.

Logički propusti– Logički propusti spadaju u jednu od najopasnijih kategorija kad su web aplikacije u pitanju. Mnogo puta se dogodilo da je kvalitetno napisana i osigurana web aplikacija kompromitirana upravo zbog greške u logici, što je napadačima omogućilo stvari koje developer nije planirao. Uz to, logičke greške najčešće napadaču dozvoljavaju privilegirani pristup podacima i/ili aplikaciji, te se na taj način obilazi sigurnost sustava. Ovaj modul objašnjava spomenute greške i vodi polaznike kroz primjere viđene na produkcijskim aplikacijama.

BoF (Buffer Overflow) - Sigurnost aplikacija općenito nije zaokružena dok se ne razumiju uzroci i posljedice BoF-a, pa je zadnji dan ovog treninga dediciran upravo toj tematici. Polaznici će se upoznati s osnovama registara i asemblerom, te će imati priliku napisati svoj prvi BoF u python skripti baziran na jednostavnoj ranjivoj aplikaciji. Za onr koji nemaju nikakvog programerskog iskustva, demo će pokriti sve što je potrebno znati kaj je u pitanji osnova BoF-a.

Sadržaj treninga:
DAN 1

1. **Sigurnosni koncepti**
   - Općenito o sigurnosti
   - Razni napadi na web aplikcaije
   - Statistika napada na web aplikacije (Verizon DBIR, AKAMAI state of the Internet, ...)
2. **Koncepti web tehnologija**
   - Povijest
   - Multi-tier arhitektura
   - HTTP protocol
   - Enkodiranje
   - Metode i statusni kodovi HTTP protokola
   - Cookies i zaštita session-a
   - HTML, XML, SOAP
   - Parameter tampering koncepti
   - OWASP (top 10, testing guide, ESAPI)
   - Razni Web debuging alati
   - VJEŽBADEMO: Mapiranje web aplikacije
   - VJEŽBA/DEMO: Automatizirano skeniranje web aplikacije
   - VJEŽBA/DEMO: forced browsing
   - Kako se zaštititi?

3. **Koncepti frameworkova**
   - ASP.NET / Silverlight (NOT TO BE USED ANYMORE)
   - PHP
   - JAVA
   - Flash

4. **Koncepti i razlike web servera**
    - MS IIS
    - Apache
    - Tomcat
    - Ranjivosti web servera
    - LAB: Hakiranje Tomcat servera

DAN 2

5. **Obilaženje kontrola na klijentskoj strani**
    - Manipulacija podacima na klijentskoj strani (Prameter tampering)
    - Napadi na klijentskoj strani
    - DEMO: Primjer napada na klijentskoj strani (DLL injekcija)
    - Skrivena polja u formi
    - Session cookie i zaštita
    - DEMO: Analiza cooki-a
    - URL parametri
    - Referer header
    - LAB: naliza cookie-a i manipulacija podacima n klijentskoj strani
    - Kako se zaštititi?
6. **Napadi na autentikaciju**
    - Koncepti autentikacije i autorizacije
    - Autentikacijska metoda: Basic
    - Autentikacijska metoda: Digest
    - Autentikacijska metoda: Windows integrirana (NTLM, Kerberos)
    - Autentikacijska metoda: HTML form bazirana
    - Autentikacijska metoda: Klijentski certifikati (multifaktorska autentikacija)
    - Kritpografija 101
    - PKI 101
    - Napadi na autentikacijski proces
        - Brute force,
        - Dictionary,
        - Pre-computed hashes
    - VJEŽBA/DEMO: Automatizacija napada na web password-e pomoću BURP-a i hydra-e
    - Kako se zaštititi?
7. **Propusti u dizajnu i implementaciji**
    - Loš password
    - Autentikacijske metode podložne brute-force napadima
    - Opsežne poruke o greškama
    - Nezaštićen prijenos korisničkom imena i passworda
    - Funkcionalnosti zaboravljenog passworda i promjene passworda
    - Zapamti me funkcionalnost
    - Funkcionalnost impersonacije korisnika
    - I mnogi drugi propusti
    - Kako se zaštititi?

DAN 3

8. **Napadi na web aplikacije: Injection (A1)**
    - SQL injekcija
        - Razlike između baza: MySQL, MS SQL, Oracle …
        - Jednostavni i napredni primjer SQL injekcije
        - Napredni primjer SQL injekcije
        - Korištenje SQLMap alata

- VJEŽBA/DEMO: SQL injekcija (jednostavan i napredni primjer)
- VJEŽBA/DEMO: SQL injekcija (sqlmap)
- LDAP injekcija, OS command injekcija
- LAB: Od OS command injekcije do shell-a
- Kako se zaštititi?

9. Napadi na web aplikacije: XSS/CSRF (A3/A8)

- Pohranjeni (*persistent*) XSS
- Reflektirani XSS
- DOM bazirani XSS
- XSS – kako se može iskoristiti
- CSRF
- Framework za napad (BeEF)
- VJEŽBA/DEMO: Jednostavan reflektirani XSS
- VJEŽBA/DEMO: Krađa cookie-a korištenjem pohranjene XSS ranjivosti i session hijacking-a
  VJEŽBA/DEMO: Od XSS-a do shella – BeeF (Browser Exploatation Framework)
- Kako se zaštititi?

10. Napadi na web aplikacije: Broken authentication and session management (A2)

- Upravljanje session-om u web aplikacijama
- Tehnike krađe cookie-a
- VJEŽBA: korištenje ukradenog cookie-a za krađu session-a
- DEMO: Trace.axd, Elmah.axd
- Kako se zaštititi?

DAN 4

11. Ostali učestali napadi na web aplikacije

- Što je to *direct object reference*
- VJEŽBA: Pristup file-ovima korištenjem *direct object* referenci
- Kako se zaštititi?
- File inclusion Lokalni i udaljeni (LFI, RFI)
- Directory trsversal
- Null byte napadi
- VJEŽBA/DEMO: LFI, RFI, directory traversal
- Problemi vezani uz file upload
- VJEŽBA/DEMO: Od slike do root prava u nekoliko minuta
- Kako radi redirekcija
- HTTP Response Splitting
- Kako iskoristiti redirekciju u maliciozne svrhe
- VJEŽBA: SSL strip
- Kako se zaštititi?

12. Logički propusti

- Što su to logički propusti
- Primjeri
- VJEŽBA: iskorištavanje logičkih propusta
- Kako se zaštititi?

13. Baze

- MSSQL
- Oracle
- MySQL
- Najčešći napadi
- VJEŽBA/DEMO: Identifikacija i hakiranje baza podataka

DAN 5

14. BoF (Buffer Overlow)

- O asembleru i registrima
- Stack bazirani BoF
- DEMO/VJEŽBA: Stack bazirani overflow
- SEH bazirani overflow
- DEMO: SEH bazirani overflow