Lista tehnika i alata koje koristimo

- Zloupotreba funkcionalnosti (Korišćenje funkcija web aplikacije za zaobilaženje mehanizama kontrole pristupa)
- Brute force napad (jednostavne i standardne lozinke)
- Spoofing sadrzaj (vrednost sadrzaja web stranice)
- Predvidjanje sesije (dostupna vrednost identifikatora sednica vam omogućuje presretanje sesija drugih korisnika. Slični napad izveden predviđanjem ili pogađanjem jedinstvenog identifikatora korisnika sesije)
- Crosssite skripte. Napad na webprodukciju na stranicu izdate web stranice, zlonameran kod (što će biti napravljeno na korisnikovom računaru prilikom otvaranja ove stranice) I interakcija ovog kodeksa sa napadačevim web serverom.
- Zahtev za križanje krivotvorina. Falsifikovanje zahteva za unakrsne stranice. Napad na posetioce web stranice koristeći nedostatke HTTP protokola.
- "HTTP EMPACT kriumčarenje". Napadi na osnovu netačnog prenosa http odgovora.
- "CHTTP reakcija." Napadi sa podelom Odgovora HTTP-a.
- "HTTP zahteva kriumčarenje". Napadi pogrešan prenos HTTP zahteva.
- "HTTP zahtev za cepanje." Napadi sa podelom upita http.
- "LDAP injekcija". Provedba LDAP operatora na web poslužitelju, kreiranje zahteva za uslugu LDAP-a na osnovu unesenih podataka korisnika.
- "NULL BYTE INJEKCIJA". Zaobiđujući Filter za web infrastrukturu dodavanje u URL simbol nula bajta, kako biste promenili logiku web aplikacije i primanje NSD datoteka.
- Zaređivanje OS-a. Izvođenje naredbi OS manipulacije aplikacija za unos podataka.
- "PATH PREDALJA". Dobijte pristup datotekama, direktorijima i timovima,
- smešten izvan glavnog direktorija web servera.
- "Predvidljiva lokacija resursa." Predvidljiva lokacija resursa,

Lista tehnika i alata koje koristimo

- omogućava vam pristup skrivenim podacima ili funkcionalnim
- prilike.
- "Uključivanje daljinskog datoteka" (RFI). Napad patovima koji omogućava daljinska datoteka na strani poslužitelja, putem skripte na web poslužitelju.
- Usmeravanje skretanja. Poruke sapuna za usmeravanje.
- Fiksacija sesije. Sednica za pričvršćivanje. Koristeći ovu klasu napada,napadač dodeljuje identifikator set sesije korisničke vrednosti.
- "Zloupotreba niza sapuna". Definicije ubrizgavanja skupova podataka u sapunu.
- SSI injekcija. Provedba proširenja servera. Umetnite naredbe servera u HTML kod ili ih pokrenite direktno sa servera.
- "SQL injekcija". Implementacija na zahtjv proizvoljnog SQL kodeksa.
- Zloupotreba preusmjeravanja URL-a. Preusmjerava bez provjere za neželjenu poštu.
- "Xpath injekcija". Implementacija XPath operatora napada na cilj
- web server kreiranje XPATH zahtjeva na osnovu unesenih podataka
- korisnika.
- "XML puhanje atributa". Parametri na naduvavanje.
- "XML vanjski entici". Uključujući vanjsku datoteku.
- "XML ekspanzija entiteta". Uvođenje varijabli iz tela za poruke.
- "XML injekcija". Implementacija na zahtev proizvoljnog xmlcoda.
- "XQuery ubrizgavanje". Implementacija na zahtev proizvoljnog XQuery kodeksa.