III IZDANJE

Gilberto Najera-Gutierrez,
Juned Ahmed Ansari

Kali Linux

Testiranje neprobojnosti veba

Istražite motode i alatke etičkog hakovanja pomoću Kali Linuxa

kompjuter biblioteka

Packt>

Gilberto Najera-Gutierrez
Juned Ahmed Ansari

Kali Linux

Testiranje neprobojnosti veba

kompjuter biblioteka

Packt›

Izdavač:

kompjuter biblioteka

Obalskih radnika 4a, Beograd

Tel: 011/2520272

e-mail: kombib@gmail.com

internet: www.kombib.rs

Urednik: Mihailo J. Šolajić

Za izdavača, direktor:
Mihailo J. Šolajić

Autori: Gilberto Najera-Gutierrez
Juned Ahmed Ansari

Prevod: Slavica Prudkov

Lektura: Miloš Jevtović

Slog: Zvonko Aleksić

Znak Kompjuter biblioteke:
Miloš Milosavljević

Štampa: „Svetlost“, Čačak

Tiraž: 500

Godina izdanja: 2018.

Broj knjige: 502

Izdanje: Prvo

ISBN: 978-86-7310-525-3

Web Penetration Testing with Kali Linux Third Edition

Gilberto Najera-Gutierrez

Juned Ahmed Ansari

ISBN 978-1-78862-337-7

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд,
се добија на захтев

UVOD

Veb aplikacije, kao i veb servisi, postali su deo svakodnevnog života – koriste se u vladinim procedurama, društvenim medijima i aplikacijama za bankarstvo, a pronaći ćete ih i u mobilnim aplikacijama koje šalju i primaju informacije korišćenjem veb servisa. Kompanije i ljudi generalno koriste veb aplikacije svakodnevno. Sama ova činjenica čini veb aplikacije privlačnom metom za krađu informacija i druge kriminalne radnje. Stoga, zaštita ovih aplikacija i njihove infrastrukture od napada je veoma važna za programere i vlasnike.

U poslednje vreme učestale su vesti iz raznih krajeva sveta o masovnom kompromitovanju podataka i zloupotrebama funkcionalnosti aplikacija za generisanje dezinformacija ili sakupljanje korisničkih informacija, koje su zatim prodavane marketinškim kompanijama. Ljudi počinju da brinu kako kompanije koriste i štite njihove informacije. Dakle, kompanije treba da preduzmu aktivne mere za sprečavanje takvog „curenja“ ili napada. To se radi na mnogim frontovima, od strože kontrole kvaliteta u toku razvojnog procesa, do PR-a i obaveštavanja medija kada je detektovan incident.

Pošto su razvojni ciklusi kraći i dinamičniji zbog upotrebe aktuelnih metodologija, povećanje složenosti u mnoštvu tehnologija je potrebno za kreiranje moderne veb aplikacije. Osim toga, zbog nasleđene loše prakse, pojedini programeri ne mogu u potpunosti da testiraju svoje veb aplikacije sa aspekta bezbednosti, s obzirom da im je prioritet da svoje proizvode isporuče na vreme. Ova složenost u veb aplikacijama i u samom razvojnom procesu stvara potrebu za profesionalcima koji su specijalizovani za testiranje bezbednosti i koji se uključuju u razvojni proces i preuzimaju odgovornost testiranja aplikacije u pogledu bezbednosti sa tačke gledišta napadača. Ovi profesionalci su penetracioni testeri.

U ovoj knjizi govorićemo o osnovnim konceptima veb aplikacija i penetracionog testiranja, opisujući sve faze u metodologiji, od dobijanja informacija za identifikovanje mogućih slabih tačaka, do eksploatisanja ranjivosti. Ključni zadatak penetracionog testera je da, kada pronađe i verifikuje ranjivost, posavetuje programere kako da isprave uočenu grešku i spreče da se ona ponovo javi. Prema tome, sva poglavlja u ovoj knjizi koja su posvećena identifikaciji i eksploatisanju ranjivosti uključuju i odeljak u kojem je ukratko opisano kako se sprečavaju i izbegavaju takvi napadi.

KOME JE NAMENJENA OVA KNJIGA

Napisali smo ovu knjigu imajući na umu nekoliko vrsta čitalaca. Studenti računarstva, programeri i administratori sistema koji žele da obogate svoje znanje o bezbednosti informacija ili oni koji žele da imaju karijeru u ovoj oblasti upoznaće neke osnovne koncepte i instrukcije koje su jednostavne, što će im omogućiti da izvrše prvo penetraciono testiranje u sopstvenim laboratorijama, a pronaći će i osnove i alatke za nastavak rada i učenja.

Programeri aplikacija i administratori sistema će takođe naučiti kako se napadači ponašaju u stvarnom svetu, koji aspekti treba da budu razmotreni za izgradnju bezbednijih aplikacija i sistema i kako se detektuje zlonamerno ponašanje. Iskusni stručnjaci na polju bezbednosti će u ovoj knjizi pronaći neke srednje teške i napredne tehnike eksploatacije i ideje kako da kombinuju dve ili više ranjivosti da bi izvršili sofisticiranije napade.

ŠTA OBUHVATA OVA KNJIGA?

Poglavlje 1, „Uvod u penetraciono testiranje i veb aplikacije“, obuhvata osnovne koncepte penetracionog testiranja, Kali Linuxa i veb aplikacija. Poglavlje započinje samom definicijom penetracionog testiranja i drugih ključnih koncepata, a zatim slede razmatranja pre uključivanja profesionalnog penetracionog testa, kao što je definisanje oblasti važenja i pravila primene. Zatim ćete pregledati Kali Linux i videti kako funkcionišu veb aplikacije, fokusirajući se na aspekte koji se više odnose na penetracionog testera.

U Poglavlju 2, „Podešavanje laboratorije pomoću Kali Linuxa“, naći ćete tehnički pregled okruženja testiranja koje će biti upotrebljeno u ostalim poglavljima. Započećemo poglavlje objašnjenjem šta je Kali Linux i opisom alatki koje on uključuje za namenu testiranja bezbedosti veb aplikacija, a zatim ćemo pogledati ranjive veb aplikacije koje će biti upotrebljene u narednim poglavljima za demonstraciju ranjivosti i napada.

U Poglavlju 3, „Izviđanje i profilisanje veb servera“, prikazane su tehnike i alatke koje koriste penetracioni testeri i napadači za preuzimanje informacija o tehnologijama koje su upotrebljene za razvoj, hostovanje i podršku ciljne aplikacije i identifikaciju prve slabe tačke koja može da bude dalje eksploatisana, jer je, ako se prati standardna metodologija za penetraciono testiranje, prvi korak sakupljanje informacija o ciljevima.

Poglavlje 4, „Nedostaci provere identiteta i upravljanja sesijom“, kao što i naslov govori, namenjeno je detekciji, eksploataciji i smanjenju ranjivosti koja se odnosi na identifikaciju korisnika i razdvajanje dužnosti unutar aplikacije. Počećemo objašnjenjem različitih mehanizama za proveru identiteta, a zatim ćemo objasniti kako ovi mehanizmi mogu da imaju nedostatke u dizajnu ili implementaciji i kako zlonamerni akteri ili penetracioni testeri mogu da iskoriste ove nedostatke.

U Poglavlju 5, „Detektovanje i eksploatacija nedostataka zasnovanih na injektiranju“, opisani su detekcija, eksploatacija i smanjenje najčešćih nedostataka injektiranja, jer je jedna od najvećih briga programera u pogledu bezbednosti da aplikacije ne budu ranjive

u bilo kojoj vrsti napada injektiranjem, bez obzira da li je to SQL injektiranje, injektiranje komande ili bilo koji drugi napad, jer to može da predstavlja veliki rizik za veb aplikaciju.

U Poglavlju 6, „Pronalaženje i eksploatisanje ranjivosti, prenosa i izvršenja skripta kroz sajt (XSS)“, opisano je šta je ranjivost prenosa i izvršenja skripta kroz sajt, šta predstavlja bezbednosni rizik, kako se identifikuje kada je veb aplikacija ranjiva i kako napadač može da iskoristi ovu ranjivost da preuzme osetljive informacije od korisnika ili da ih natera da nesvesno izvrše neke akcije.

U Poglavlju 7, „Cross-Site Request Forgery, identifikacija i eksploatacija“, saznaćete šta je Cross-Site Request Forgery napad i kako funkcioniše. Zatim ćemo opisati ključni faktor za detektovanje nedostataka koji ga omogućavaju i tehnike za eksploataciju. Poglavlje ćemo završiti savetima o prevenciji i izbegavanju ovih napada.

Poglavlje 8, „Napadi na nedostatke u kriptografskim implementacijama“, započinje uvodom u koncepte kriptografije koji su korisni iz perspektive penetracionog testera, kao što je način na koji SSL/TLS funkcioniše. Predstavićemo koncepte i algoritme enkripcije, kodiranje i heširanje, a zatim ćemo opisati alatke koje se koriste za identifikaciju slabih SSL/TLS implementacija, zajedno sa eksploatacijom dobro poznatih oblika ranjivosti. Zatim ćemo opisati detekciju i eksploataciju ranjivosti u uobičajenim kriptografskim algoritmima i implementacijama. Poglavlje ćemo završiti savetom kako da sprečite ranjivost kada koristite šifriranu komunikaciju ili kada skladištite osetljive informacije.

U Poglavlju 9, „AJAX, HTML5 i napadi na strani klijenta“, opisana je strana klijenta penetracionog testiranja veb aplikacije, počev od procesa analize sadržaja AJAX aplikacije i opisa programerskih alatki koje su uključene u modernim veb pretraživačima. Takođe ćemo predstaviti inovacije koje su unete u HTML5 i nove izazove za napadače i penetracione testere. Zatim, sledi odeljak u kojem je opisana upotreba programerskih alatki za zaobilaženje bezbednosnih kontrola koje su implementirane na strani klijenta, a poglavlje se završava savetima za prevenciju i izbegavanje ranjivosti AJAX-a, HTML-a 5 i strane klijenta.

U Poglavlju 10, „Ostali uobičajeni nedostaci u veb aplikacijama“, biće reči o direktnom pristupu neadekvatno zaštićenim objektima, uključivanju fajlova, „zagađenju“ HTTP parametra i ranjivosti otkrivanja informacija i njihovoj eksploataciji. Poglavlje ćemo završiti savetom kako da sprečite i otklonite ove nedostatke.

U Poglavlju 11, „Upotreba automatizovanih skenera u veb aplikacijama“, opisani su faktori koje treba uzeti u obzir kada se koriste automatizovani skeneri i fuzeri u veb aplikacijama. Takođe ćete saznati kako ovi skeneri funkcionišu i šta je fuzing. Zatim ćemo predstaviti primere upotrebe alatki za skeniranje i fuzing, koje su uključene u Kali Linux. Završićemo poglavlje predstavljanjem akcija koje penetracioni tester treba da izvrši nakon automatskog skeniranja veb aplikacije da bi programeru aplikacije isporučio rezultate ranjivosti.

ŠTA VAM JE POTREBNO ZA OVU KNJIGU?

Da biste dobili maksimum iz ove knjige

Da biste uspešno iskoristili ovu knjigu, treba da imate osnovno znanje o sledećim temama:

- instalacija Linux OS-a
- upotreba Unix/Linux komandne linije
- HTML jezik
- programiranje PHP veb aplikacije
- Python programiranje

Jedini hardver koji vam je potreban je računar sa operativnim sistemom koji može da pokrene VirtualBox ili drugi virtuelizacioni softver. Za specifikaciju preporučujemo sledeću konfiguraciju:

- Intel i5, i7 ili sličan CPU
- hard drajv od 500 GB
- 8 GB RAM-a
- internet konekcija

PREUZIMANJE FAJLOVA PRIMERA KODA

Fajlove sa primerima koda možete da preuzmete za ovu knjigu sa našeg sajta:
http://bit.ly/2HaoZyp

PREUZIMANJE KOLORNIH SLIKA

Takođe smo obezbedili PDF fajl koji ima kolorne snimke ekrana/dijagrama koji su upotrebljeni u ovoj knjizi. Možete da ga preuzmete na adresi:

http://bit.ly/2vuBVub

UPOTREBLJENE KONVENCIJE

Postoji veliki broj konvencija teksta koje su upotrebljene u ovoj knjizi.

CodeInText: ukazuje na reči koda u tekstu, nazive tabele baze podataka, nazive direktorijuma, nazive fajlova, ekstenzije fajlova, nazive putanje, skraćene URL-ove, korisnički unos i Twitter postove. Evo i primera: „Mnoge organizacije će osluškivati port koji nije deo fajla nmap-services.“

Blok koda je prikazan na sledeći način:

```
<?php if(!empty($_GET[,k‘])) {
    $file = fopen(,keys.txt‘, ,a‘);
    fwrite($file, $_GET[,k‘]);
    fclose($file);
  }
?>
```

Kada želimo da privučemo pažnju na određeni deo bloka koda, relevantne linije ili stavke će biti ispisane zadebljanim slovima:

```
<?php if(!empty($_GET[,k‘])) {
    $file = fopen(,keys.txt‘, ,a‘);
    fwrite($file, $_GET[,k‘]);
    fclose($file);
  }
?>
```

Svaki unos komandne linije ili ispis će biti prikazan na sledeći način:

```
python –m SimpleHttpServer 8000
```

Zadebljana slova: Ukazuju na novi termin, važnu reč ili reči koje vidite na ekranu. Na primer, reči u menijima ili okvirima za dijalog prikazane su u tekstu na sledeći način: „Ako otvorite karticu **Logs** unutar **Current Browsera**, videćete da veza registruje sve što korisnik radi u pretraživaču, od klikova i otkucaja, do promena prozora ili kartica.“

Upozorenja ili važne napomene će biti prikazivani u ovakvom okviru.

Dobra praksa
Preporuke kako da programirate kao stručnjak prikazne su ovako.

POVRATNE INFORMACIJE

Povratne informacije od naših čitalaca su uvek dobrodošle.

Osnovne povratne informacije: Pošaljite e-mail na adresu informatori@kombib.rs i u naslovu poruke napišite naslov knjige. Ako imate bilo kakva pitanja o bilo kom aspektu ove knjige, pošaljite nam e-mail na adresu informatori@kombib.rs.

Štamparske greške: Iako smo preduzeli sve mere da bismo obezbedili tačnost sadržaja, greške mogu da se potkradu. Ako pronađete grešku u ovoj knjizi, bili bismo zahvalni ako biste nam to prijavili. Posetite stranicu http://bit.ly/2H8K7oA, kliknite Ostavite komentar i unesite detalje.

Piraterija: Ako na Internetu pronađete ilegalnu kopiju naših knjiga, u bilo kojoj formi, molimo vas da nas o tome obavestite i pošaljete adresu lokacije ili naziv web sajta. Kontaktirajte sa nama na adresi informatori@kombib.rs i pošaljite nam link ka sumnjivom materijalu.

Ako ste zainteresovani da postanete autor: Ako postoji tema za koju ste specijalizovani i zainteresovani ste da pišete ili sarađujete na nekoj od knjiga, pogledajte vodič za autore na adresi www.packtpub.com/authors.

RECENZIJA

Kada pročitate i upotrebite ovu knjigu, zašto ne biste napisali vaše mišljenje na sajtu sa kojeg ste je poručili? Potencijalni čitaoci tada mogu da upotrebe vaše mišljenje da bi odlučili o kupovini, mi u „Packtu“ možemo da razumemo šta mislite o našim proizvodima, a naši autori mogu da vide povratne informacije o svojoj knjizi. Hvala!