Testování bezpečnosti webových aplikací

Roman Kümmel

Obsah

- Průzkum prostředí
- Mapování aplikace
- Testování vstupů

Obsah

- **Průzkum prostředí**
  - **Identifikace OS**
  - **Identifikace webového serveru**
  - **Identifikace programovacího jazyka**
  - **Identifikace webové aplikace / autora**
  - **Identifikace Ostatních technologií**
  - **Identifikace známých zranitelností**
- Mapování aplikace
- Testování vstupů

Identifikace OS

- **Průzkum prostředí**
  - **Identifikace OS**
  - **Identifikace webového serveru**
  - **Identifikace programovacího jazyka**
  - **Identifikace webové aplikace / autora**
  - **Identifikace ostatních technologií**
  - **Identifikace známých zranitelností**
- Mapování aplikace
- Testování vstupů

- HTTP Response hlavičky
- Patička defaultních chybových stránek
  - 400 Znak % v URL
  - NULL char v URL
  - Dlouhý řetězec v HTTP request hlavičce
  - Neplatný protokol GET / FOO/1.1
  - Nevalidní request
  - 403 Pokus o výpis adresáře
  - 404 Přístup k neexistujícímu zdroji
  - 405 Použití neplatné HTTP metody
  - 414 Příliš dlouhá URL adresa
  - 501 Použití neplatné HTTP metody
  - 505 Neplatná verze HTTP protokolu HTTP/9.8
- Souvislost mezi webovým serverem a OS
- Zranitelnost Full Path Disclosure
- Case sensitivita
- Typické otevřené porty
- Odchylky v implementaci TCP protokolu
  - Nmap, XProbe2, p0f
- Rezervované názvy ve Windows LPT1, COM1, …

Identifikace webového serveru

- **Průzkum prostředí**
  - **Identifikace OS**
  - **Identifikace webového serveru**
  - **Identifikace programovacího jazyka**
  - **Identifikace webové aplikace / autora**
  - **Identifikace ostatních technologií**
  - **Identifikace známých zranitelností**
- Mapování aplikace
- Testování vstupů

- HTTP Response hlavičky (Server)
- Patička defaultních chybových stránek
  - Pro podrobnosti viz identifikaci OS
- Obsah a vzhled defaultních chybových stránek
- Rozdílné chování serverů při použití
  - dlouhých URL
  - neplatné HTTP metody
  - neplatného protokolu
  - nepodporované verze HTTP protokolu
- Pořadí HTTP response hlaviček
- Automatické nástroje
  - HTTPrint, HTTPrecon
- Defaultní uvítací stránka serveru
  - přístup z prohlížeče přes IP
  - přístup s neplatnou hodnotou hlavičky Host
- Typické pro Apache
  - zakázaný přístup k souborům .ht
  - alias na adresář icons
- Typické pro IIS
  - Speciální znaky v URL (*, ~)

Identifikace programovacího jazyka

- **Průzkum prostředí**
  - **Identifikace OS**
  - **Identifikace webového serveru**
  - **Identifikace programovacího jazyka**
  - **Identifikace webové aplikace / autora**
  - **Identifikace ostatních technologií**
  - **Identifikace známých zranitelností**
- Mapování aplikace
- Testování vstupů

- HTTP Response hlavičky (Sever, X-Powered-By)
- Patička defaultních chybových stránek
  - pro podrobnosti viz identifikaci OS
- Použitá přípona souborů
- Při nasazení hezkých URL
  - pokus o přístup k souboru index, default, home, apd.
  - přidání přípony k jednotlivým částem URL
  - dotaz na existenci přípon do vyhledávačů
- Defaultní název session cookie
- Zranitelnost Full Path Disclosure
- PHP: HTTP metody (FOO = GET)

Identifikace webové aplikace / autora

- **Průzkum prostředí**
  - **Identifikace OS**
  - **Identifikace webového serveru**
  - **Identifikace programovacího jazyka**
  - **Identifikace webové aplikace / autora**
  - **Identifikace ostatních technologií**
  - **Identifikace známých zranitelností**
- Mapování aplikace
- Testování vstupů

- HTTP Response hlavičky (Powered-By, Generator)
- META tagy ve zdrojovém kódu HTML stránky
- Komentáře ve zdrojovém kódu HTML, JS, CSS
- Patička webové stránky
- Přítomnost souborů
  - readme.txt, changelog.txt, version.txt, install.txt, license.txt, upgrade.txt
  - s / bez přípony txt
  - na Linuxu různé varianty velikosti písmen
- Typické názvy souborů a adresářů
- Typické komentáře
- Typické názvy cookies
- Defaultní vzhled přihlášení do administrace
- Defaultní vzhled chybových stránek
- Zranitelnost Full Path Disclosure
- Automatické nástroje
  - Wappalyzer, Whatweb, CMSdetector

Identifikace ostatních technologií

- **Průzkum prostředí**
  - **Identifikace OS**
  - **Identifikace webového serveru**
  - **Identifikace programovacího jazyka**
  - **Identifikace webové aplikace / autora**
  - **Identifikace ostatních technologií**
  - **Identifikace známých zranitelností**
- Mapování aplikace
- Testování vstupů

Identifikace modulů, pluginů, frameworku, WAF, LB

- HTTP Response hlavičky
- META tagy ve zdrojovém kódu HTML stránky
- Komentáře ve zdrojovém kódu HTML
- Typické názvy souborů a adresářů
- Typické komentáře
- Typické názvy cookies

Vyhledání rozhraní pro správu

- Scan portů
- Subdomény
- Cesty v URL

- Defaultní / slabé přístupové údaje - Guessing

Identifikace známých zranitelností

- **Průzkum prostředí**
  - **Identifikace OS**
  - **Identifikace webového serveru**
  - **Identifikace programovacího jazyka**
  - **Identifikace webové aplikace / autora**
  - **Identifikace ostatních technologií**
  - **Identifikace známých zranitelností**
- Mapování aplikace
- Testování vstupů

- Mezinárodní databáze zranitelností
  - CVE (cvedetails.com)
  - CWE
  - NVD
  - OSVD
- Webové stránky autora jednotlivých komponent
- Changelog jednotlivých komponent
- Dotaz na zranitelnosti pomocí vyhledávačů
- Vyhledávání exploitů
  - exploit-db.com (searchsploit)
  - 0day.today
  - exploitalert.com

Obsah

- Průzkum prostředí
- **Mapování aplikace**
  - **Nalezení vhostů**
  - **Nalezení subdomén**
  - **Nalezení všech součástí aplikace**
- Testování vstupů

Hledání vhostů

- Průzkum prostředí
- **Mapování aplikace**
  - **Nalezení vhostů**
  - **Nalezení subdomén**
  - **Nalezení všech součástí aplíkace**
- Testování vstupů

- Reverzní překlad IP adresy (PTR záznamy)
- Alternativní domény v SSL certifikátech
- Reference zveřejněné webhostingem
- Defaultní uvítací stránka serveru
- Zveřejněné statistiky serveru
  - Server-Status, status, stats, awstats, statistics
- Webové aplikace na nestandardních portech
- On-line služby umožňující zobrazit vhosty na konkrétní IP adrese
  - ipneighbour.com
  - pentest-tools.com
  - domaintools.com
  - kloth.com
  - virustotal.com
- Dotaz vyhledávačům na IP adresu

Hledání subdomén

- Průzkum prostředí
- **Mapování aplikace**
  - **Nalezení vhostů**
  - **Nalezení subdomén**
  - **Nalezení všech součástí aplíkace**
- Testování vstupů

- Dotazování se vyhledávačů
- Alternativní domény v SSL certifikátech
- Dotazování se cílového serveru
- Dotazování se DNS serveru
- Zone Transfer na DNS
- On-line služby
  - pentest-tools.com
  - domaintools.com
  - shodan.io
  - virustotal.com
- Automatické nástroje
  - Subbrute
  - Sublist3r
  - The Harvester

Hledání všech součástí aplikace

- Průzkum prostředí
- **Mapování aplikace**
  - **Nalezení vhostů**
  - **Nalezení subdomén**
  - **Nalezení všech součástí aplíkace**
- Testování vstupů

- Manuální crawling (spidering)
- Automatický crawling (spidering)
- Predikce názvů souborů
- Dotaz vyhledávačům
- Obsah souboru robots.txt
- Obsah souboru sitemap.xml
- Vyhledávání pomocí slovníků
  - záložních souborů (zálohy skriptů, databáze, aplikace)
  - konfiguračních souborů
  - logů
- Ověření otevřeného výpisu adresářů
- Ověření výskytu git repozitáře (.git)
- IIS Tilde Enumeration
- Apache Multiviews

Obsah

- Průzkum prostředí
- Mapování aplikace
- **Testování vstupů**
  - **Testování v rámci celé aplikace**
  - **Testování na každé stránce**
  - **Testování každého formuláře**
  - **Testování každého vstupu**
  - **Testování session managementu**
  - **Testování specifické pro konkrétní stránky**
  - **Testování podle konkrétního typu vstupu**

Děkuji za pozornost