Zraniteľnosti webových aplikácií - útoky na server

Kód kurzu: GOC542

Toto školeníie vás zasvätí do tajov webhackingu a zraniteľností webových aplikácií, ktoré umožňujú útočiť na aplikačné servery a na nich uložené dáta. Školenie vám umožní do detailov pochopiť a v praxi si vyskúšať metódy, ktoré bežne používajú útočníci. Zraniteľnosti webových aplikácií umožňujúce útoky na server patria medzi najzávažnejšie hrozby a dôkladne by s nimi mali preto byť zoznámení všetci vývojári a prevádzkovatelia webových aplikácií. Vzhľadom na to, že zneužitie tohto typu zraniteľností vedie často ku kompletnému prevzatiu kontroly nad cieľovým systémem, mali by ste sa s nimi zoznámiť a otestovať si bezpečnosť svojich webových aplikácií skôr než to za vás urobí nevítaný votrelec. Všetko, čo k tomu budete potrebovať, vás naučíme na tomto praktickom kurze.

Pre koho je kurz určený

Kurz je určený vývojárom a prevádzkovateľom webových aplikácií, ktorí chcú porozumieť postupom útočníkov pri napádaní webových aplikácií. Na mnohých praktických ukážkach si vyskúšame postupy útočníkov, pri ktorých dochádza ku kompromitácii serveru a databáz.
Postupy preberané na tomto kurze cielia primárne na technológie Apache, PHP a MySQL. Pretože sa ale dajú predstavené princípy často aplikovať aj na iné technológie, odporúčame návštěvu kurzu každému, kto sa chce zoznámiť s praktikami útočníkov a chce získať správne bezpečnostné návyky pri vývoji a prevádzke webových aplikácií a serverov.

Čo vás naučíme

Náš jedinečný kurz Webhacking v praxi 2 – útoky proti serverom vám umožní do detailov pochopiť a hlavne si na praktických príkladoch vyskúšať metódy, ktoré bežne využívajú útočníci počas útokov na webové servery a aplikácie. V priebehu kurzu si postupne vysvetlíme všetko, čo potrebujete poznať pre obranu proti týmto útočným technikám.

Požadované vstupné znalosti

Kurzu sa môže zúčastniť každý, kto má základné znalosti technológií HTTP, HTML a SQL.

Osnova kurzu

Prieskum prostredia

- Identifikácia použitých technológií
- Web Crawling/Spidering
- Hľadanie neverejných zdrojov
- Repozitáre
- Open Directory listing
- IIS Tilde File Enumerate
- Apache Multiviews File Enumerate
- HTTP metódy

Exploitácua použitých technológií

- Guessing
- Hľadanie exploitov
- Použitie exploitov
- Post exploitácia
- Shelly

Zraniteľnosti a útoky na SSL

- Zraniteľnosti jednotlivých šifrovacích algoritmov

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Heartbleed
- Poodle
- BEAST
- CRIME
- BREACH
- ďalšie

Útoky na dáta

- Chýbajúca/nedostatočná autorizácia
- Priamy prístup k objektom
- Únik dát pri redirekte
- Forced Browsing

Útoky na databázu

- Union-Based SQL injection
- Boolean-Based SQL injection
- Error-Based SQL injection
- Time-Based SQL injection
- Stacked SQL injection
- Stored/Second-order SQL injection
- DNS exfiltration
- Multibyte SQL injection
- SQL injection via binary hash
- Local File Disclosure via SQL injection
- Command execute via SQL injection
- SQL Truncation

Crackovanie hashov

- Hashovacie algoritmy
- Solenie
- Crackovanie hashov
- Brute Force/Dictionary attack/Rainbow tables

Zraniteľnosti XML parserov

- Denial of Services via XML
- Local File Disclosure via XML
- Command Execution via XML
- XML injection
- LDAP injection
- XPATH injection

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Code Execution

- Nezabezpečený upload
- Nezabezpečený download
- Local File Disclosure
- Remote File Inclusion (RFI)
- Local File Inclusion (LFI)
- LFI via file upload
- LFI via session storage
- LFI via environment
- LFI via log
- LFI via phpinfo
- Function Injection
- PHP Object Injection
- Code Execution
- Command Execution
- WebDav a zneužitie HTTP metód
- PHP-CGI vulnerability
- SSI Injection

Pozrieme sa aj na ďalšie útoky...

- Zneužitie webserveru ako proxy
- HTTP request smuggling
- Privilege escalation/autorization bypass prostredníctvom cookie
- HTTP Request hlavičky
- Host Header Injection
- Napadení Session Storage
- Local Session Injection
- Session Puzzling
- ZIP bomby a DoS
- Útoky na zdieľaných serveroch
- Server-Side Request Forgery (SSRF)
- Zraniteľnosť Shellshock

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk