

# WEB HACKING: įveikti internetą

## Informacijos apsaugos mokymai

Lietuvoje vyrauja nuomonė, kad apsaugoti įmonės informacinių technologijų sistemas nuo kompiuterinių įsilaužėlių (hakerių) pakanka įdiegti ugniasienę ir antivirusines sistemas. Tačiau šios ir panašios priemonės visiškai neveiksmingos prieš tinklalapių saugumo problemas. O dažna įmonė jau nebeapsiriboja vien tik reprezentaciniu savo tinklalapiu, tačiau dažnai į internetą perkelia ir dalį savo verslo. Būtent dėl to įsilaužėlių taikiniu tampa tinklalapiai. Tyrimų kompanijos Gartner duomenimis, 75% įsilaužimų įvyksta pasinaudojant nesaugiais tinklalapiais. Kitaip nei kitai programinei įrangai, tinklalapiui dažnai tiesiog negalima atsisiųsti ir įdiegti saugumo spragos pataisymo. Kovodami su šia problema, pristatome "WEB HACKING: įveikti internetą" mokymus, nagrinėjančius tinklalapių, web servisų ir kitų HTTP protokolo pagrindu veikiančių sistemų saugumo problemas.

### Kas turėtų dalyvauti?

- web programuotojai;
- tinklo administratoriai;
- IT saugumo specialistai;
- IT vadovai;
- entuziastai, besidomintys IT saugumu.

### Reikalavimai dalyviams:

- tinklalapių kūrimo principų žinojimas;
- Windows arba Linux sistemų pagrindai;
- bendros žinios apie *HTML, JavaScript, SQL ir HTTP*.

### Ko išmoksite

Dalyvaudami šiuose kursuose Jūs perprasite įsilaužėlių naudojamą metodiką, išmoksite mąstyti kaip įsilaužėlis ir veikti kaip įsilaužėlis. Jūs sužinosite:

- kaip aptinkami įmonės interneto resursai;
- kaip surandamos spragos serveriuose ir kitoje įrangoje;
- kaip tyrinėti tinklalapius ir ieškoti trūkumų juose;
- kaip nustatyti pažeidžiamumus neaplankant tinklalapio;
- kaip išnaudoti aptiktas spragas (pigiau „apsipirkti“ interneto parduotuvėje ☺);
- kaip išgauti ar modifikuoti duomenis, pasiekti duomenų bazes;
- kaip sukelti atsisakymo aptarnauti (*Denial-of-Service*) atakas;
- sužinosite kas yra *CSRF, Blind SQL Injection, XSS, HTTP Splitting, Cookie Poisoning* bei kitokios kasdienės „baisybės“;
- kaip nuo viso to apsisaugoti.

Kursų metu daug dėmesio skiriama praktiniams užsiėmimams, todėl susipažinsite ne tik su teorija, bet ir įgausite praktikos.

### Kursų turinys

Kursus sudaro dvi dalys. Abiejų dalių metu pateikiama daug ne tik teorinės medžiagos, bet ir praktinių užduočių, kurias dalyviai atlieka savarankiškai arba kartu su dėstytoju. Mokymų metu pavyzdžiai pateikiami su Lietuvos kompanijomis ir sistemomis. Nors mokymai ir orientuoti į tinklalapius, tačiau jie negali veikti be operacinės sistemos, serverio, kompiuterinio tinklo, interneto, juos prižiūrinčių žmonių bei kitų reikalingų komponentų.

**Svarbu ⇒ Mokymų metu yra drąsiai peržengiamos tinklalapių apsaugos ribos ir nagrinėjamos operacinių sistemų bei kompiuterinio tinklo saugumo problemos, žmoniškojo faktoriaus klaidos, dalyviai mokosi atlikti kompiuterinio tinklo auditą, išnaudoti aptiktus įvairius pažeidžiamumus ir t.t.**

### Pirmoji dalis

Šioje mokymų dalyje dalyviai sužinos daug įvairios tinklalapių laužimo technikos: kaip iš naršyklės pasiekti duomenų bazes, kaip iš paprasto XSS pažeidžiamumo sukurti visą *botnet* tinklą, kaip serveryje vykdyti sisteminės komandas ir t.t.

#### Architektūra ir metodika:

- duomenų praradimas
- saugumo situacija Lietuvoje
- web architektūra ir komponentai
- kas yra web aplikacijos apsauga
- silpnosios web vietos
- įsilaužimo metodika

#### Sistemų identifikavimas:

- interneto resursai, paieškos sistemos
- programinė įranga
- intuicija



### Web serverio laužimas:

- populiariausios sistemos ir jų saugumas
- kur ieškoti naujienų
- kuo ieškoti pažeidžiamumų
- sukurti virusą yra paprasta
- slaptažodžių parinkimas
- Denial-of-Service
- sava galva
- naujų pažeidžiamumų paieška
- socialinė inžinerija
- kiti pažeidžiamumai

### Web aplikacijos analizė:

- tikslai
- gamintojo ir TVS nustatymas
- slaptų vietų aptikimas
- paieškos sistemos
- interneto resursai
- lokali kopija
- turinio analizė
- parametrų analizė
- programinė įranga

### Web aplikacijos laužimas:

- HTTP protokolas
- sesijos valdymas
- aplikacijų trūkumai
- viešai neteikiami resursai
- klaidingas autentifikavimas ir sesijos valdymas
- slaptažodžių spėjimas
- lietuviškų slaptažodžių top 10
- perteklinė informacija, netinkamas klaidų apdorojimas
- nesaugiai saugomi duomenys
- nesaugios komunikacijos
- tiesioginis objektų pasiekimas
- cross site scripting
- cross site request forgery
- injekcijos
- sesijos nuodijimas ir failų įterpimas
- web servais
- AJAX saugumas
- HTTP splitting
- Denial-of-Service

Pirmos dalies mokymų metu gausu praktinių užduočių. Dalyviai turės apie 30 praktinių užsiėmimų, savarankiškas užduotis, kartu su dėstytoju nagrinės įsilaužimus.

## Antroji dalis

Kiekvienas dalyvis, vadovaudamasis pirmoje dalyje įgytomis žiniomis, turės tinkle aptikti paslėptą serverį, nustatyti jame veikiančias tarnybas, įvertinti serverio operacinės sistemos ir veikiančių tarnybų saugumą bei išnaudoti jų trūkumus. Vėliau dalyvis turės pasirinkti kuo būti – įsilaužėliu ar saugumo auditoriumi. Ir vienam, ir kitam teks ištyrinėti nesaugų banką, surinkti įvairią informaciją ir rasti kuo daugiau pažeidžiamumų arba gauti pinigus iš svetimos sąskaitos ir pakeisti tinklalapio išvaizdą (angl. deface). Taip pat dalyviai detaliau susipažins su socialinės inžinerijos psichologiniais spąstais bei informacijos vadybos sistema kaip apsaugos priemone. Šios dalies didžiąją dalį sudaro praktiniai užsiėmimai.

### Praktinis tinklo auditas:

- serverių ir aplikacijų aptikimas
- serverių ir aplikacijų pažeidžiamumų nustatymas
- web sistemų aptikimas
- pažeidžiamumų išnaudojimas

### Informacijos saugos vadybos sistema:

- Informacija, informacinės vertybės
- Informacijos apsauga
- Informacijos apsaugos principai
- Informacijos apsaugos ISO standartai

### Socialinė inžinerija:

- Tikslas
- Prasmė
- Būdai ir metodai
- Apsaugos priemonės

### Web Hacking banko laužimas:

- aplikacijos analizė
- silpnų vietų aptikimas
- pažeidžiamumų išnaudojimas

## Kita informacija



Kiekvienas dalyvis gaus kursams pritaikytą Linux distribuciją DVD diske ir kursuose dėstomos medžiagos skaidres. Dalyvis diske ras ne tik mokymų metu naudojamą programinę įrangą, bet ir papildomos video medžiagos. Taip pat visiems išklausiems šį kursą bus įteikti kursų dalyvio pažymėjimai.

Kavos pertraukėlėmis ir pietumis dalyviams taip pat bus pasirūpinta.



**Trukmė:** 3 dienos

**Laikas:** - liepos mėn. 1-3 dienomis **Vilniuje**

**Kalba:** - kursai vedami lietuvių kalba  
- mokymų medžiaga pateikiama lietuvių kalba

**Grupės dydis:** iki 12 dalyvių.

**Kaina:** - 1950 Lt

Mokymams taikomas 0% PVM tarifas.

## Registracija ir kontaktinė informacija:

- telefonu: +370 615 20288, (8 5) 2030 828
- el. paštu adresu: mokymai@isec.lt

**UAB „Informacijos saugos sprendimai“**

www.isec.lt



## Apie dėstytoją

### **Audrius Lučiūnas**

Specializacija. Internetinių (WEB) sistemų saugumas, programinės įrangos saugumas, kompiuterinio tinklo saugumas, socialinė inžinerija, IT sistemų saugumo vertinimas, planavimas ir įgyvendinimas. IT saugumo patirtis ~ 10 metų

Darbinė patirtis. Informacinių sistemų auditai, saugios IT sistemų architektūros projektavimas, tinklų ir IT sistemų pažeidžiamumų analizė AB „Lietuvos Geležinkeliai“, AB „Lietuvos Radijo Televizijos Centras“, įvairiose LR ministerijose, AB „Lietuvos Paštas“, AB „Rytų skirstomieji tinklai“ ir t.t. Užsienio bankų Web sistemų, programų ir tinklų auditai, respublikinio masto CERT (tinklų ir informacijos saugumo) tarnybos kūrimas, saugumo pažeidimų rezultatų koreliavimo sistemos kūrimas, DDoS atakų tyrimai.

## Dalyvių atsiliepimai

**Antanas K.** Labai retai sakau komplimentus kursų organizatoriams, tačiau šiuo atveju noriu pasakyti, kad tai buvo labiausiai pateisinę lūkesčius kursai per pastaruosius keletą metų. Jie suteikė impulsą ir pradines būtinas žinias tolimesniam savarankiškam... hakinimui. :-)

**Kęstutis B.** Kadangi turėjau labai mažai žinių apie Web Hacking, man šis kursas buvo labai naudingas. Po šių kursų visai kitaip žiūriu į Web aplikacijų kūrimą. Ačiū.

**Rimvydas T.** Tai unikalūs ir labai reikalingi kursai. Būtų gerai dar daugiau tokių kursų, kurie leistų patikrinti programinio kodo patikimumą.

**Viačeslav Š.** Kursų tema labai aktuali tiek žmonėms profesionaliai užsiimantiems Web bei tinklo administravimu, tiek ir paprastiems šių sričių vartotojams. Medžiaga buvo pateikta informatyviai ir profesionaliai.

**Tomas L.** Labai įdomu ir naudinga. Nemažai ką jau žinojau, bet nebuvo susidūręs su praktiniu laužimu, nežinojau programinės įrangos.

**Darius K.** Geri ir naudingi kursai. Dėstytojas savo srities žinovas.

**Tomas P.** Kursas ir medžiagos dėstymas puikūs.

**Rolandas G.** Labai geras linux'as. :)

**Robertas S.**

