CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

# Hakiranje Google tražilicom

## CCERT-PUBDOC-2008-05-228

+CERT.hr u suradnji s LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom CARNet CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

## CARNet CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

## LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

# Sadržaj

# 1. Uvod

Hakiranje tražilicom je pojam koji se odnosi na umijeće stvaranja kompleksnih upita tražilici kako bi prikazala informacije vezane uz računalnu sigurnost kroz velike količine pretraživanih podataka. U zlonamjernom obliku može ga se koristiti za otkrivanje web stranica koje su ugrožene brojnim ranjivostima, kao i privatnih, osjetljivih informacija. Ovo filtriranje podataka izvodi se pomoću naprednih Google operatora pretraživanja. Iako je Google osnovni alat u Google hakiranju, mnoge od taktika i operatora mogu se koristiti na drugim pretraživačima, kao što su MSN Search i Yahoo.

Sama riječ hakiranje (eng. hack) označava pojam vezan uz razbijanje bilo kakvih računalnih ili telekomunikacijskih sustava. Postoji terminologija koja navodi da bi hakere koji provaljuju u računalne sustave trebao zvati "crackers", a u telefonske sustave "phreaks".

U ovom dokumentu dan je opis osnovnih i naprednih Google operatora pretraživanja. Ukazano je i na način pretraživanja ranjivih stranica, osjetljivih podataka te dokumenata. Zatim su opisane osnovne ranjivosti koje su vezane uz hakiranje Google tražilicom, te navedeni načini zaštite od njih.

## *1.1. Hakiranje kroz povijest*

Razvoj prve mreže počinje 1969. godine kada je osnovan Arpanet, predak Interneta, sa samo četiri čvora. Godine 1971 Ray Tomlinson je napisao prvi program za elektroničku poštu koji se koristi na Arpanet mreži koja tada ima 64 čvora. Zahvaljujući slučajnoj distribuciji virusa 1980. g. dolazi do pada sustava na mreži Arpanet te do formiranja mreže Internet 1983. Godine 1989. na CERN laboratoriju za istraživanja u fizici visokih energija u Genevi, Tim Berners-Lee počinje razvijati protokole koji će postati World Wide Web, a godinu dana kasnije pridružuje mu se i Robert Cailliau.

1972. god John Draper, također poznat kao Captain Crunch, čini besplatni međugradski poziv puštajući precizni ton u telefon kao uputu telefonskom sustavu kako bi otvorio kanal. Na ideu je došao kada je pronašao zviždaljku kao poklon u žitaricama koju je iskoristio za imitaciju tona (frekvencije 2600 Hz) koji koristi telefonski sustav za uspostavljanje međugradskih poziva.

U kolovozu 1986.g., nalazirajući male pogreške u evidenciji korisničkog korištenja računalnih resursa na računalu u Lawrence Berkeley Lab na University of California, Berkeley, administrator sustava (eng. System Administrator) Clifford Stoll razotkriva dokaz o provali hakera. Dugogodišnji rezultati istrage rezultirali su uhićenjem pet odgovornih hakera iz Njemačke.

Godine 1988.g. Robert Morris, diplomski student na Cornell University, neovlašteno je pristupio računalu koje se koristi isključivo od strane Savezne vlade ili financijskih institucija. Morris je uhićen i ubrzo nakon toga je kažnjen novčanom kaznom od 10 000 dolara te osuđen na tri godine uvijetno i 400 sati dobrovoljnog rada.

Kevin Mitnick je, 1989.g., osuđen za krađu softvera iz Digital Equipment i kodova za međugradske linije iz telefonske tvrtke MCI u SAD-u. On je prva osoba osuđena pod novim zakonom protiv dobivanja pristupa na računalne mreže u kaznjive svrhe te je odslužio godinu dana zatvora.

1993.g. Kevin Poulsen, Ronald Austin i Justin Peterson su na radio-telefonskom natjecanju preuzeli kontrolu nad telefonskim linijama na radio stanici kako bi se osiguralo propuštanje samo njihovih poziva. Grupa je navodno dobila dva automobila Porsche, 20 000 dolara u gotovini i ljetovanje na Havajima.

Šesnaestogodišnji student glazbe Richard Pryce, poznatiji po nadimku Datastream Cowboy, je 1994.g. uhićen i optužen za provalu u stotine računala, uključujući i one na Griffiths Air Force bazi, NASA-i te korejski Atomic Research Institute. Njegov internetski mentor, "Kuji", nikad nije pronađen.

Iste godine, grupa ruskih hakera provaljuje u računala Citibank i prebacuje više od 10 milijuna dolara s računa klijenata. Na kraju, Citibank je vratila sve osim 400 000 dolara ukradenog novca.

U veljači 1995.g., Kevin Mitnick je uhićen drugi put, a optužen je za krađu 20 000 brojeva kreditnih kartica. Proveo je četiri godine u zatvoru, a pušten je pod uvjetom da izbjegava kontakt s računalima i mobilnim telefonima.

Dana 15 studenog 1995.g., Christopher Pile postaje prva uhićena osoba zbog pisanja i distribuiranja računalog virusa. Gospodin Pile, koji sebe naziva Black Baron, bio je osuđen na 18 mjeseci pritvora.

Kasnije, US General Accounting Office otkriva da su US Defense Department računala kontinuirano napadnuta 250 000 puta u 1995.

1996.g. napadnute su popularne web stranice u znak protesta zbog tretmana Kevina Mitnicka.

U ožujku 1999.g., pojavljuje se Melissa virus na računalima širom svijeta. Nakon kraće istrage, FBI je uhitio pisca virusa, 29-godišnjeg programera, Davida L Smitha iz New Jerseya.

Godine 2000 u veljači, neke od najpopularnijih web stranica u svijetu, kao što su Amazon i Yahoo, su gotovo srušene preplavljivanjem s lažnim zahtjevima za podacima.

U svibnju iste godine, virus ILOVEYOU je poharao računala u svijetu. Tijekom narednih mjeseci, razne inačice ovog virusa su nađene u računalima tvrtki koje nisu dovoljno učinile kako bi se zaštitile. A u listopadu iste godine Microsoft priznaje da je njegova korporacijska mreža bila hakirana te je otkriven izvorni kod za buduće Windows sustave.

# 2. Hakiranje Google tražilicom

Google je vjerojatno najmoćniji alat za pretraživanje na Internetu dostupan bilo kome. Temelji se na algoritmu koji rangira stranice prema zadanom upitu tako da korisnici mogu pretraživati informacije po želji, pomoću ključnih riječi i operatora. Google indeksira i sprema ne samo web stranice već u svoje pretrage uključuje i PDF i Word dokumente, Excel proračunske tablice, Flash SWF animacije, *čiste* (eng. plain) tekstualne datoteke i mnoge druge sadržaje.

Google je također stvorio usluge i alate za širu javnost i poslovno okruženje, uključujući i Web aplikacije, mreže za oglašavanje te rješenja za poslovne subjekte. Osim kao tražilica može se koristiti i kao kalkulator, pretvarač valuta, rječnik te na mnoge druge korisne načine.

Pored svojih alata za pretraživanje web stranica, Google pruža i druge usluge i alate uključujući Google News, Google Suggest, Google Product Search, Google Maps, Google Co-op i Google Desktop Search. Tu su i proizvodi koji nisu izravno vezani uz pretraživanje. Gmail, na primjer, je webmail aplikacija, ali još uvijek uključuje i mogućnosti pretraživanja, dok Google Browser Sync ne pruža pretragu objekata, iako ima za cilj uskladiti postavke preglednika na korisničkom računalu.

Mnogi proizvodi su dostupni kroz Google Labs, zbirku aplikacija koje su u testnoj fazi za korištenje u javnosti.

## *2.1. Osnove pretraživanja tražilicom*

Pretraživanje pomoću Google tražilice radi se zadavanjem korisničkih upita. Google tražilica prihvaća upite kao jednostavan tekst i razbija ih u niz uvjeta za pretraživanje (zadane riječi), fraza, osnovnih te naprednih operatora. Operatori pretraživanja osiguravaju funkcionalnost tražilice pružajući bolje filtriranje rezultata.

Drugi način je nepredno pretraživanje korištenjem Web stranice "Advanced Search", koja nudi pretraživanje po raznim kriterijima, koji se upuisuju u ponuđena - dodatna polja.

### 2.1.1. Osnovni operatori pretraživanja

Značenje osnovnih operatora pretraživanja:

( + ) - uključivanje pojma

( - ) - isključivanje pojma

( " ) - fraze

( . ) - zamjenski znak za za bilo koji znak (eng. character)

( * ) - bilo koja riječ

( | ) - logički operator *ili* (eng. 'OR')

( ) - zagrade grupiraju upite

Potrebno je napomenuti da Google ignorira sljedeće riječi: a, about, an, and, are, as, at, be, by, from, how, i, in, is, it, of,on, or, that, the, this, to, we, what, when, where, which, with (pa je njihovo zadavanje u pretragama nepotrebno).

### 2.1.2. Napredni operatori pretraživanja

Uz osnovne operatore pretraživanja Google podržava mnoge parametre za napredno pretraživanje i filtriranje rezultata prema korisničkim upitima. Google tražilica može otkriti mnoge osobne podatke kada se koriste napredni operatori pretraživanja.

Napredni operatori za pretraživanje podataka mogu dohvaćati:

1. **podatke za identifikaciju** - povezani uz osobni identitet korisnika (ime, adresa, telefonski broj, adresa elektroničke pošte)
2. **osjetljive podatke** - javni podaci, ali mogu sadržavati i osobne podatke te njihovo otkrivanje može smetati vlasniku (adresa elektroničke pošte, postovi na forumu).
3. **povjerljive podatke** - privatni podaci za skupinu korisnika (lozinke za chat, korisnička imena i lozinke).
4. **tajne podatke** - tajni ključevi, privatni ključevi, kriptirane poruke napravljene od tajnih podataka koji trebaju biti dostupni samo vlasniku.

Slijedi abecedni popis naprednih operatora za pretraživanje uz navedene primjere korištenja:

**allinanchor**:

Google tražilicca ograničava rezultate na stranice koje sadrže sve pojmove koji su određeni u upitu u anchor tekstu. Anchor text je tekst na stranici koji je poveznica na drugu web stranicu ili neko drugo mjesto na trenutnoj stranici.

Primjer: *allinanchor: najbolji muzej Sydney*

Rezultat pretrage: stranice koje sadrže riječi "najbolji", "muzej" i "Sydney" u anchor tekstu

**allintext**:

Rezultat pretrage su one stranice koje sve pojmove određene upitom sadrže u tekstu stranice.

Primjer: *allintext: ponuda putovanja*

Rezultat pretrage: stranice koje sadrže riječi "ponuda" i "putovanja" bilo gdje u tekstu

**allintitle**:

Pretraga ograničava rezultate na one stranice koje sve pojmove koji su određeni upitom sadrže u naslovu. U pretraživanju slika pronaći će datoteke čija imena sadrže nevedene pojmove, a pri pretraživanju Google News vratit će članak čiji naslov uključuje određene pojmove.

Primjer: *allintitle: zdrava prehrana*

Rezultat pretrage: stranice koje sadrže riječi "zdrava" i "prehrana" u nsalovu stranice

**allinurl**:

Stranice koje se pojavljuju u rezultatu su ograničene na one koje sadrže sve navedene pojmove u svojoj URL adresi.

Primjer: *allinurl: Google faq*

Rezultat pretrage: stranice koje sadrže riječi "Google" i "faq" u URL adresi

( npr. www.google.com/help/faq.html )

**author:**

Google pretraga će ograničiti svoje Google Groups rezultate samo na članke navedenog autora. Pri tome, autor može biti potpuno ili djelomično ime te adresa elektroničke pošte.

Primjer: *jutro author:marko author:maric*

Rezultat pretrage: članci koje sadrže riječ "jutro", a napisao ih je Marko Maric

**cache:** URL

Prikazat će se spremljena verzija web stranice koju Google ima pohranjenu u svojoj memoriji, umjesto trenutne verzije stranice.

Primjer: *cache: cache:www.eff.org*

Rezultat pretrage: prikazuje inačicu početne stranice Electronic Frontier Foundation koju Google ima spremljenu u memoriji

**daterange:**

Pretraga vraća stranice indeksirane od Google tražilice u zadanom vremenskom razdoblju koji je potrebno izraziti u obliku Julianskog datuma.

Primjer: *književnost daterange: 2452774-2452803*

Rezultat pretrage: stranice o književnosti indeksirane od strane Google tražilice tijekom mjeseca svibnja 2003

**define:**

Google prikazuje definicije za pojam koji slijedi, što ovaj operator pretraživanja čini korisnim za pronalaženje definicija riječi, fraza i akronima.

Primjer: *define:blog*

Rezultat pretrage: definicije za pojam blog

**ext:**

Nedokumentirani alias za filetype:.

**filetype: sufiks**

Rezultati su ograničeni na stranice čija imena završavaju na sufiks. Kada se ne navede format dokumenata, Google pretražuje različite formate datoteka.

Primjer: *hakiranje filetype:pdf*

Rezultat pretrage: Adobe Acrobat pdf dokumenti o hakiranju

**group:**

Google pretraga će ograničiti svoje Google Groups rezultate na grupe sa člancima iz određene grupe ili područja.

Primjer: *spavati group:misc.kids*

Rezultat pretrage: članci iz područja misc.kids koji sadrže riječ "spavati"

**id:**

Nedokumentirani alias za info:.

**inanchor:**

Stranice koje se nalaze u rezultatu su stranice koje sadrže riječ nazančenu u upitu u anchor tekstu na stranici. Stavljanje inanchor: ispred svake riječi u upitu je ekvivalentno stavljanju allinanchor: ispred upita.

Primjer: *meksički inanchor:restoran*

Rezultat pretrage: stranice koje sadrže u anchor tekstu riječ "restoran" te riječ "meksički" bilo gdje na stranici

**info: URL**

Predstavit će se neke informacije o odgovarajućoj web stranici. Ova funkcionalnost može se dobiti upisivanjem URL web stranice izravno u Googleov okvir za pretraživanje.

Primjer: *info:gothotel.com*

Rezultat pretrage: informacije o stranici GotHotel.com

**insubject:**

Google tražilica će ograničiti članak u Google Groups na one koji sadrže pojmove koji su određeni u upitu.

Primjer: *insubject:zaspati*

Rrezultati pretrage: članci čiji naslov sadrži riječ "zaspati"

**intext: pojam**

Rezultati su ograničeni na dokumente koji sadrže pojam u tekstu. Stavljanje intext: ispred svake riječi u upitu je ekvivalentno stavljanju allintext: ispred upita.

Primjer: *Hamish Reid intext:pandemonia*

Rezultati pretrage: stranice koje sadrže rijč "pandemonia" u tekstu, a riječi "Hamish" i "Reid" bilo gdje na stranici uključujući i naslov, URL i slično

**intitle: pojam**

Pretraga ograničava rezultate na dokumente koji sadrže pojam u naslovu. Stavljanje intitle: ispred svake riječi u upitu je ekvivalentno stavljanju allintitle: ispred upita.

Primjer: *Google intitle:hakiranje*

Rezultati pretrage: dokumenti koji sadrže riječ "hakiranje" u naslovu te riječ "Google" bilo gdje u dokumentu

**inurl:**

Ispis rezultata je ograničen na dokumente koji sadrže prvu riječ navedenu u upitu u URL. Stavljanje inurl: ispred svake riječi u upitu je ekvivalentno stavljanju allinurl: ispred upita.

Primjer: *inurl:zdrava prehrana*

Rezultati pretrege: dokumenti koji sadrže riječ "zdrava" u URL adresi i "prehrana" bilo gdje u dokumentu

**link: URL**

Prikazuju se stranice koje upućuju na navedeni URL.

Primjer: *link:www.googleguide.com*

Rezultati pretrege: stranice koje upućuju na Google Guide

**location:**

Pri pretraživanju Google News upit vrati samo članke s navedene lokacije (država).

Primjer: *queen location:canada*

Rezultati pretrege: članci koji sadrže riječ "queen" (kraljica) sa web stranica iz Kanade

**movie:**

Google tražilica će pronaći informacije vezane uz navedeni film, ali moguće je pronaći i filmove koje u opisu sadrže zadane ključne riječi.

Primjer: *movie: awesome car chase*

Rezultati pretrege: ispis filmova koji u opisu sadrže riječi "awesome"," car" ili "chase"

**numrange:**

Korištenje operatora pruža rezultate koji sadrže broj iz zadanog raspona.

Primjer: *Willie Mays numrange:1950..1960*

Rezultati pretrege: stranice koje sadrže riječi "Willie" i "Mays" te broj između1950 i 1960

**phonebook:**

Pokazuje se ispis telefonskih unosa za navedeni upit.

Primjer: *phonebook:Krispy Kreme Mountain View*

Rezultati pretrege: telefonski unos za Krispy Kreme trgovinu u Mountain Viewu

**related: URL**

Upit daje popis web stranica koje su slične navedenoj web stranici. Rezultati pretraživanja mogu se dobiti preko "Similar pages" linka na Google glavnoj stranici s rezultatima.

Primjer: *related:www.consumerreports.org*

Rezultati pretrege: stranie koje su slične web stranici Consumer Reports

**rphonebook:**

Google tražilica prikazuje telefonske oglase za određeni upit.

Primjer: *rphonebook: John Doe NY*

Rezultati pretrege: prikaz telefonskih oglasa za John Doe u New Yorku

**site:**

Rezultati pretraživanja su ograničeni na stranicu ili domenu koja je navedena. Također, rezultati se mogu ograničiti na stranicu ili domenu preko izbornika na stranici za napredno pretraživanje.

Primjer: *mir site:gov ili mir site:.gov*

Rezultati pretrege: stranice o miru unutar .gov domene

**source: ID**

Google News će ograničavati pretragu na članke izvora vijesti s navedene ID.

Primjer*: izbori source:new_york_times*

Rezultati pretrege: članci o izborima objavljeni u New Yourk Times

**stocks:**

Otvoriti će se stranica koja prikazuje informacije o dionicama za simbole koji su određeni.

Primjer: *stocks:brcm brcd*

Rezultati pretrege: informacije o Broadcom Corporation i Brocade Communications System

**store: ID**

Froogle (online prodaja) ograničava pretragu na trgovinu navedenog ID-a.

Primjer: *polo shirt store:llbean*

Rezultati pretrege: ponuda za “polo” i “shirt” iz trgovine L. L. Bean.

**weather: okacija**

Ako Google prepoznaje lokaciju, prognoza će se pojaviti na vrhu stranice s rezultatima. U suprotnom, rezultati će sadržavati poveznice na web stranice s vremenskom prognozom za tu lokaciju.

Primjer: *weather Sunnyvale*

Rezultati pretrege: vremenska prognoza za Sunnyvale

| Usluge pretraživanja | Operatori pretraživanja |
|---|---|
| Web Pretraga | allinanchor: , allintext: , allintitle: , allinurl: , cache: , define: , filetype: , id: , inanchor: , info: , intext: , intitle: , inurl: , phonebook: , related: , rphonebook: , site: , stocks: |
| Pretraga slika | allintitle: , allinurl: , filetype: , inurl: , intitle: , site: |
| Grupe | allintext: , allintitle: , author: , group: , insubject: , intext: , intitle: |
| Imenik | allintext: , allintitle: , allinurl: , ext: , filetype: , intext: , intitle: , inurl: |
| Novosti | allintext: , allintitle: , allinurl: , intext: , intitle: , inurl: , location: , source: |
| Froogle | allintext: , allintitle: , store: |

**Tablica 1.** Google pretrage i odgovarajući operatori

Kombiniranje naprednih operatora je moguće u nekim slučajevima, ali ga u pravilu treba izbjegavati. Neki od operatora za pretraživanje neće raditi ispravno ako se stavi razmak između dvotočke (:) i upita pa se preporuča njegovo izbjegavanje. Također, mnogi operatori za pretraživanje mogu se pojaviti bilo gdje u upitu, ali efikasije je postaviti ih na početak upita.

Napredni operatori daju manje rezultata, ali su zato rezultati bolje fokusirani na pretraživani upit. Također, pojedini operatori daju bolje rezultate za određene usluge Google pretraživanja kako je prikazano u tablici 1.

## *2.2. Osnove hakiranja*

Hakiranjem pomoću Google tražilice pronalazi se željeni tekstualni niz (niz znakova) unutar velikog broja rezultata pretraživanja. Haker zadaje posebni upit tražilici te preko rezultata dolazi do potrebnih podataka. Neki od popularnijih primjera su korištenje Google tražilice za pronalaženje određene verzije ranjive web stranice. Osim toga, moguće je pretraživati web poslužitelje, baze podataka i dokumente te pronaći razne povjerljive podatke (korisnička imena i lozinke).

### 2.2.1. Pretraživanje ranjivih stranica

Zadavanjem odgovarajućeg upita tražilica može pronaći stranice ranjive na određeni napad.

Primjeri upita koji traže stranice ranjive na:

1. Cross-Sites Scripting (XSS) napade:
   allinurl:/scripts/cart32.exe
   allinurl:/CuteNews/show_archives.php
   allinurl:/phpinfo.php
2. SQL injection napade:
   allinurl:/privmsg.php

### 2.2.2. Pretraživanje web poslužitelja

Kroz direktorije web poslužitelja moguće je kretanje kao kroz datoteke u Windows ili Linux operacijskom sustavu. Napadaču to omogućava lako prikupljanje informacija o poslužitelju, kao i otkrivanje ranjivosti.

Pregled propusta na web poslužiteljima moguć je koristeći sintaksu Index of/:

```
Index of /admin
Index of /passwd
Index of /password
```

Korištenje *operatora inurl:* ili *allinurl:* za otkrivanje ranjivosti:

```
allinurl:winnt/system32
inurl:.bash_history
```

Do propusta na web poslužiteljima moguće je doći koristeći i operatore *intitle:* ili *allintitle:*

```
allintitle: "index of /root
allintitle: "index of /admin
```

Google je moguće koristiti kao CGI skener ili web skener, program koji traži poznate ranjivosti u web poslužitelju. CGI skeneri su vrlo jednostavni alati koji traže osnovne ranjivosti u web aplikacijama i pokušaju ih iskoristiti. Nedostatak im je u tome što pretražuju samo osnovne ranjivosti pa se za ozbiljnije provjere sigurnosti koriste specijalizirani Web Application Security skeneri.

Primjer korištenja Google tražilice kao CGI skenera:

```
allinurl:/random_banner/index.cgi
```

Postoje razni alati koji obavljaju skeniranje, ali korisnik mora imati dozvolu za njihovo korištenje.

„Gooscan" je alat koji automatizira upite za Google tražilicu za UNIX operacijski sustav. Ovi upiti su posebno dizajnirani kako bi pronašli potencijalne ranjivosti na web stranicama. Za profesionalnu sigurnost, Gooscan služi kao pomagalo u prikupljanju informacija u fazi procjene ranjivosti. Administratoru poslužitelja pomaže otkriti što je već poznato o stranici zahvaljujući Google tražilici.

### 2.2.3. Pretraživanje dokumenata

Pri pretraživanju dokumenata Google omogućuje ograničavanja pretrage pomoću naprednog operatora pretraživanja *filetype:* na određene vrste dokumenata. Primjeri dokumenata koje možemo pronaći mijenjajući ekstenziju:

- Adobe Portable Document Format (pdf)
- Adobe PostScript (ps)
- Lotus 1-2-3 (wk1, wk2, wk3, wk4, wk5, wki, wks, wku)
- Lotus WordPro (lwp)
- MacWrite (mw)
- Microsoft Excel (xls)
- Microsoft PowerPoint (ppt)
- Microsoft Word (doc)
- Microsoft Works (wks, wps, wdb)
- Microsoft Write (wri)
- Rich Text Format (rtf)
- Text (ans, txt)

Primjer korištenja pretraživanja dokumenata:

```
filetype:doc site:gov confidential
```

ispisuje sve dokumente sa doc ekstenzijom, u svim domenama koje završavaju na .gov i sadrže riječ "confidential".

### 2.2.4. Pretraživanje korisničkih imena i lozinki

Gotovo sve stranice sadrže administratorske podatke, uključujući korisnička imena i lozinke. Formirajući ispravan upit pomoću odgovarajućih operatora pretrage moguće je na vrlo jednostavan način doći do tih podataka.

Ako tražilici zadamo upit:

```
intitle:index.of.etc
```

, pretraga daje pristup etc direktoriju, gdje se mogu naći mnoge datoteke s lozinkama. Moguće je pretraživati i "backup" datoteke zadavanjem upita:

```
filetype:bak inurl:"htaccess|passwd|shadow|htusers".
```

### 2.2.5. Zanimljive pretrage

Pretraga stranica sa mp3 datotekama:

```
Index of ftp/ +.mp3
Index of music/
Index of films/
Index of pjevač
```

# 3. Osnovne ranjivosti

Većina web stranica s dinamičkim sadržajem ranjiva je na razne napade. Pretraživanjem Google tražilicom napadač može otkriti ranjive stranice te iskoristiti te informacije za izvođenje napada.

Jedne od najčešćih ranjivosti su *Cross Site Scripting* ranjivosti web stranica te SQL ranjivosti baza podataka. Također, veliku štetu poslužitelju ili računalom sustavu može prouzročiti napad uskraćivanja usluga (eng. Denial of Service). Ostali poznati načini iskorištavanja ranjivosti su: povećanje ovlasti, pokretanje proizvoljnog koda*, CRLF injection* te *Directory Traversal* napad.

U nastavku su opise osnovne ranjivosti, način njihovog iskorištavanja te odgovarajuća zaštita.

## *3.1. Cross Site Scripting napad*

Cross Site Scripting (XSS ili CSS) napad se općenito smatra kao jedna od najčešćih ranjivosti aplikacijskog sloja pri hakiranju pomoću tražilice. Općenito, radi se o tehnici koja, koristeći ranjivosti u kodu web aplikacija, omogućuje napadaču da umetne posebno oblikovani programski kod među podatke koji se razmijenjuju između poslužitelja i klijenta, a da korisnik toga nije niti svjestan (nema vidljivih znakova da je umetnut bilo kakav kod u ranjivu web aplikaciju).

Napadač koristeći XSS ranjivost može pomoću web aplikacije proslijediti korisniku zlonamjernu JavaScript, VBScript, ActiveX, HTML ili Flash skriptu. Kako preglednik ne može prepoznati da je skripta došla iz nepouzdanog izvora ona se učitava i izvršava u korisnikovom web pregledniku.

Upotreba XSS napada može ugroziti privatne informacije, manipulirati ili ukrasti kolačiće (cookies), stvoriti pogrešne zahtjeve za korisnika ili omogućiti izvršavanje zloćudnog koda na sustavu krajnjeg korisnika.

Svaka stranica koja omogućuje korisniku unos nekih podataka može biti ranjiva na XSS napad, a ranjivost je obično prisutna u obliku poveznica (Login, Zaboravili ste lozinku i sl.).

XSS napad se pojavljuje u tri oblika: XSS temeljen na DOM modelu te neustrajni i ustrajni XSS napad.

### 3.1.1. XSS ranjivost temeljena na DOM (tip 0)

Ovaj oblik XSS ranjivosti u početku je bio nazvan kao lokalna cross-site scripting ranjivost, a kasnije se naziva ranjivost temeljena na DOM (eng. Document Object Model) modelu. Pri ovoj XSS ranjivosti, problem postoji kada propust u web pregledniku omogućuje da se prikazana stranica tretira kao da je smještena na lokalnom računalu korisnika.

U praksi, iskorištavanje ove ranjivosti slično je iskorištavanju neustrajne XSS ranjivosti, osim u jednom važnom slučaju. Zbog načina na koji starije inačice preglednika Internet Explorer (IE) tretiraju "client-side" skriptu u lokalnim zonama, XSS rupe ove vrste u stranici mogu rezultirati udaljenim iskorištavanjem ranjivosti. Ovo nadilazi ograničenja koja su normalno prekoračena s XSS ranjivosti.

### 3.1.2. Neustrajni XSS napad (tip 1)

Neustrajna (eng. Non-Persistent) XSS ranjivost je najčešći tip ranjivosti, a javlja se kada korisnici posjećuju posebno oblikovane poveznice za koje je vezan zlonamjerni programski kod.

Napadač može uvjeriti korisnika da slijedi zlonamjerni URL koji je umetnut kodom na stranici s rezultatima, čime se izvršava programski kod koji je pohranjen unutar URL polja. Da bi prikrili štetni kod, napadači *maskiraju* (tj. skrivaju) zlonamjerni programski kod koristeći Hex model kodiranja.

### 3.1.3. Ustrajni XSS napad (tip 2)

Ustrajna (eng. Persistent) XSS ranjivost navodi se kao pohranjena ranjivost ili ranjivost drugog reda te omogućuje najmoćniju vrstu napada. Često je nazivana kao HTML injekcija, a javlja se kada je štetni programski kod pohranjen unutar web aplikacije.

Klasični primjer za ovaj tip ranjivosti je ostavljanje aktivnih HTML formiranih poruka za više korisnika (web portali), a za iskorištavanje ranjivosti dovoljno je da korisnik pregleda sadržaj stranice koja sadrži štetni kod.

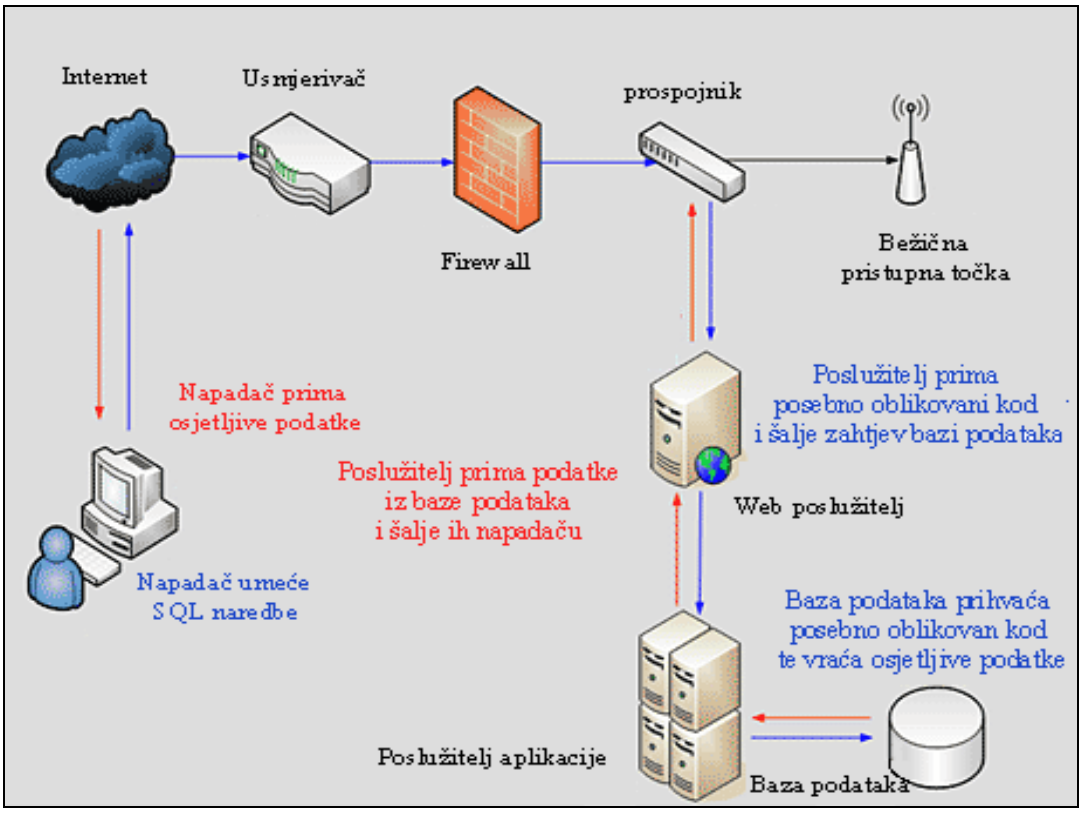
### 3.1.4. Zaštita od XSS napada

Pouzdano izbjegavanje Cross Site Scripting ranjivosti ranjivosti danas se može postići kodiranjem svih HTML specijalnih znakova. To se obično radi samo prije prikaza u web aplikaciji, a mnogi programski jezici imaju ugrađene funkcije ili biblioteke koje pružaju ovakvo kodiranje. Ostali načini zaštite su onemogućavanje izvršavanja JavaScript programskog koda, filtriranje korisničkih zahtjeva te sprječavanje krađe sjednica vezanjem *cookie* datoteka za IP adresu korisnika.

## *3.2. SQL injection napad*

SQL (eng. Structured Query Language) injection je tehnika koja iskorištava sigurnosnu ranjivost prilikom pristupa web aplikacije bazi podataka. Ranjivost nastaje kad web aplikacija prikazuje korisniku dinamički generirane web stranice za koje podatke dobiva SQL upitom, a kojeg formira ugrađujući u njega podatke koje unosi sam korisnik. Javlja se zato što aplikacija ne filtrira znakove posebne namjene od kojih se kreira SQL upit ako ih (zlonamjerni) korisnik upiše u polje za pretragu. Ukoliko napadač uspije po volji izmijeniti SQL upit, kojeg će aplikacija proslijediti internoj, skrivenoj bazi podataka, aplikacija će u ime (zlonamjernog) korisnika pretraživati cjelokupan sadržaj baze, uključujući i one podatke koji nisu namijenjeni vanjskim korisnicima. Posljedica napada je preuzimanje kontrole nad bazom podataka i izvršavanje naredbi nad ranjivim sustavom. Scenarij izvršavanja SQL napada prikazan je na slici 1.

Jedan od poznatijih oblika SQL injection ranjivosti je slijepi SQL napad, ali javljaju se i drugi oblici ove ranjivosti.




**Slika 1.** Scenarij izvršavanja SQL napada

### 3.2.1. Slijepi SQL injecton napad

Slijepi napad je napad pri kojem je web aplikacija ranjiva na SQL injection, ali rezultati injekcije nisu vidljivi za napadača. Izvođenje napada vrši se zadavanjem određenog SQL upita koji poziva stranicu. Povratna informacija o pogrešci dobije se u obliku web stranice s opisom pogreške pa potencijalni napadač može približno odrediti sintaksu SQL izjava nad određenom bazom podataka i izvesti SQL injection napad.

Vrste slijepog SQL injection napada:

1. **Uvjetovani odgovorom** – navodi bazu podataka da procjeni logičku izjavu prikazom stranice na zaslonu
2. **Uvjetovani pogreškom** –navodi bazu podataka da procjeni izjavu kao pogrešnu ako je izjava "WHERE" istinita te prema tome može odrediti SQL izjave
3. **Vremenska kašnjenja** – uzrokuje predugu obradu upita te preveliko kašnjenje izjave što napadač može iskoristiti za procjenu valjanosti upita.

### 3.2.2. Ostale vrste SQL ranjivosti

Osim slijepih SQL napada, postoje ranjivosti koje se javljaju kada aplikacija ne filtrira ono što se umeće za "escape" znakove koji se pretvaraju u SQL upit. Tada napadač može umetnuti upit koji će rezultirati kao istinit te upravljati odgovorima baze podataka. Neke implementacije SQL jezika ne podržavaju izvođenje višestrukih upita što napadaču omogućava samo izmjenu postojećih upita.

Rukovanje neodgovarajućim tipom podataka se javlja kada nisu postavljena pravilna ograničenja za polja u koja korisnik unosi podatke.

Ponekad postoje ranjivosti u poslužiteljima (npr. funkcija mysql_real_escape_string za MySQL poslužitelj) što omogućava napadaču da izvede napad pomoću loših "Unicode" znakova.

### 3.2.3. Zaštita od SQL napada

Kako bi se zaštitili od SQL injection napada korisnički podaci ne smiju biti izravno ugrađeni u SQL upit, već treba provesti provjeru ulaznih podataka. Osim ispitivanja veličine, tipa i sadržaja ulaznih podataka, moguće je upotrebljavati pohranjene procedure te testirati i ne prihvaćati određene nizove znakova.

## *3.3. DoS napad*

Napad uskraćivanja usluga (eng. Denial of Service - DoS) je napad koji napadaču ne omogućava neovlašten pristup podacima već čini računalo nedostupno legitimnom korisniku. Općenito, sastoji se u nastojanju napadača da učini neki poslužitelj ili uslugu privremeno ili trajno nedostupnim korisniku.

Pet osnovnih tipova DoS napada su:

1. Potrošnja računalnih resursa, kao što su kapacitet komunikacijskog kanala, diskovni prostor ili procesorsko vrijeme
2. Prekid zbog usmjeravanja (eng. routing) informacija.
3. Poremećaj informacija o stanju, kao što su nasilna resetiranja TCP sjednice.
4. Poremećaj fizičke komponente mreže.
5. Poremećaj medija namijenjen komunikaciji između korisnika tako da oni više ne mogu komunicirati na odgovarajući način.

### 3.3.1. ICMP poplave

Posebna varijanta DoS napada na javni Internet preplavljivanjem je *smurf napad,* koji omogućuje slanje paketa mrežom svim računalima putem adrese razašiljanja.

Ping napad se sastoji od slanja velikog broja ping paketa do računala, a primarni uvjet za izvođenje napada je da napadač posjeduje veći kapacitet komunikacijskog kanala nego žrtva.

Syn poplava temelji se na slanju TCP/SYN paketa s nepoznatom adresom pošiljatelja.

### 3.3.2. Teardrop napad

Teardrop napad uključuje slanje oštećenih IP fragmenata s preklapanjem. Propust u TCP / IP fragmentaciji uzrokuje nepropisno obrađivanje fragmenata, te pad sustava kao rezultat toga. Ugroženi operacijski sustavi u tom napadu su: Windows 3.1x, Windows 95, Windows NT te Linux prije inačice 2.0.32 i 2.1.63.

### 3.3.3. DDoS i DRDoS napadi

Distribuirani DoS napad nastaje kada više sustava poplavi komunikacijski kanal ili resurse ciljanih sustava, obično jednog ili više web poslužitelja.

Glavne prednosti korištenja distribuiranih DoS napada su da više računala može generirati više prometa od jednog te da je teže isključiti više napada nego napad s jednog računala.

DRDoS (eng. Distributed Reflected DoS) napad uključuje slanje zahtjeva na vrlo velik broj računala koja će odgovoriti na zahtjeve. U napadačkom paketu koji provocira njihov odgovor, postavlja se lažna izvorišna adresa koja pokazuje na uređaj koji se napada. To znači da će žrtva biti preplavljena velikim brojem odgovora legitimnih računala koja pogrešno misle da im je žrtva poslala upit.

### 3.3.4. Peer-to-peer napad

Napadači su otkrili način za iskorištavanje nedostataka u peer-to-peer poslužiteljima za pokretanje DDoS napada. Prilikom iskorištavanja ranjivosti napadač ne mora komunicirati sa korisnicima, nego nalaže korisnicima zajedničkih peer-to-peer čvorišta da se spoje na web stranicu žrtve. Kao rezultat toga veliki broj računala može pokušavati uspostaviti vezu s poslužiteljem.

### 3.3.5. Zaštita od DoS napada

Ako je napad bio usmjeren na samo jedno računalo, najbolje je promijeniti IP adresu tog računala. Velika količina podataka može dolaziti od specifičnog davatelja Internet usluga ili usmjeritelja. U

tom slučaju može se privremeno blokirati sav promet koji dolazi sa tih izvora. Alternativna opcija je dodavanje novog sklopovlja ili povećanje širine prijenosnog pojasa i čekanje da napad prođe. Ovo možda nije najbolje rješenje, ali može pružiti privremenu zaštitu. Zadnja metoda bi bila fizičko isključivanje poslužitelja sa mreže, što administratoru daje vremena da riješi problem, ali u tom slučaju niti jedna usluga neće biti dostupna legalnim korisnicima.

## 3.4. Povećanje ovlasti

Povećanje ovlasti je akt iskorištavanja propusta u aplikaciji za pristup resursima koji su inače zaštićeni od aplikacije ili korisnika. Rezultat napada je obavljanje radnje s više ovlasti nego što je administrator dodijelio.

Oblici povećanja ovlasti:

1. *Vertikalno povećanje ovlasti* - legitimni korisnik s manjim ovlastima pristupa funkciji ili sadržaju rezerviranom korisnicima s većim ovlastima
2. *Horizontalno povećanje* ovlasti - korisnik pristupa funkciji ili sadržaju rezerviranom za korisnika koji ima iste olasti. Može se ostvariti na nekoliko načina: održavanjem predvidljive komunikacijske sjednice, XSS-om ili jednostavnim pogađanjem lozinki.

## 3.5. Pokretanje proizvoljnog programskog koda

Pokretanje proizvoljnog programskog koda se koristi za opisivanje napadačeve sposobnosti za pokretanje bilo koje naredbe na ciljanom računalu ili sustavu. Mogućnost da se aktivira izvršavanje proizvoljnog koda s jednog stroja na drugi se naziva udaljeno pokretanje programskog koda. To je najgori učinak koji ranjivost može prouzročiti jer omogućuje napadaču u potpunosti preuzimanje ugroženog računala.

Izvršavanje proizvoljnog koda se obično postiže kroz kontrolu nad pokazivačem procesora (eng. PC=program counter) koji predstavlja programsko brojilo te pokazuje na sljedeću naredbu koja procesor treba izvesti. Napadač umeće proizvoljni kod te mijenja vrijednost PC pokazivača tako da pokazuje na umetnuti kod koji se tada automatski pokreće. Najčešća metoda koja se koristi za ovu vrstu napada je prepisivanje spremnika (eng. buffer overflow).

## 3.6. CRLF injection napad

Pojam CRLF (eng. CR=Carriage Retur, LF=Line Feed) označava oznaku za kraj tekstualnog retka, a to su ACSII znakovi koji se ne prikazujeuna ekranu, ali se vrlo široko koriste u operacijskom sustavu Windows. Na Linux / UNIX operacijskim sustavima kraj retka je naznačen korištenjem samo LF-a..

CRLF injection napad se događa kada napadač umeće CRLF naredbe u sustav. Ova vrsta napada nije tehnološki sigurnosni propust u operacijskom sustavu ili poslužitelju, nego ovisi o načinu na koji je web stranica razvijena. Kada napadač pronađe aplikaciju ranjivu na CRLF, mogućnost iskorištavanja ranjivosti ovisi o strukturi aplikacije.

Najbolji način za obranu od CRLF napada je filtriranje svih ulaznih korisničkih podataka, a naročito posebnih (meta)znakova (onih koji se ne prikazuju na ekranu).

## 3.7. Directory Traversal napad

Directory Traversal napad omogućava pristup djelomično zaštićenom direktoriju i izvršavanje naredbi izvan web direktorija poslužitelja.

Web poslužitelji pružaju dvije glavne razine sigurnosnih mehanizma:

1. Access Control Lists (ACL) - popis korisnika ili grupa koje smiju pristupiti, promijeniti ili izvršiti određene datoteke na poslužitelju, te ostala prava pristupa
2. Korjenski direktorij – (eng. root directory) specifičan direktorij na poslužiteljskom datotečnom sustavu u kojem su korisnici zatovreni, tj. ne mogu pristupiti direktorijima iznad njega.

Uz sustav ranjiv na Directory Traversal napad, napadač može iskoristiti ovu ranjivost da bi izašao iz korjenskog direktorija i pristupio drugim dijelovima datotečnog sustava (kojima obično nema prava pristupa). To mu omogućava da pregleda zaštičene datoteke i/ili pokrene naredbe na web poslužitelju.

Učinkovita zaštiti od napada je, prije svega, instalirati najnoviju inačicu ranjive aplikacije ako je u istoj ispravljen uočeni propust. Zatim, učinkovito filtrirati korisnički unos (posebno *meta* znakove) te ukloniti sve nepoznate podatke.

# 4. Kako se braniti

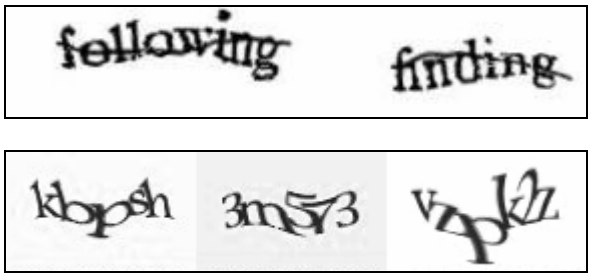
Hakiranje Google tražilicom može biti vrlo štetno za korisničku sigurnost i zato treba poduzeti odgovarajuće sigurnosne protumjere. Zaštita se može grupirati u zaštitu korisnika i zaštitu sustava.

Zaštita korisnika zahtjeva da se korisnik brani od mogućih prijetnji. Navedene su neki načini zaštite koje je potrebno napraviti:

- Ne ostavljati na Internetu osjetljive dokumente koji sadrže adresu, telefonske brojeve, dokumente o sigurnosnim kopijama (backup), tajne podatke poput lozinki, adrese privatne elektroničke pošte.
- Otkrivati samo minimalno potrebnu količinu osjetljivih informacija.
- Umjesto korištenja jednog korisničkog imena na svim sustavima koje koristi, predlaže se korisniku da koristiti više pseudonima.
- Pri ostavljanju postova i grupnih poruka ostati anoniman, te ne navoditi imena tvrtki ili organizacija ako se drukčije ne zahtjeva.
- Uključiti autentifikaciju za instalirane online uređaje (npr. pisače).

Zaštitom sustava bavi se administrator pomoću alata za automatsko skeniranje ranjivosti te pomoću *robots.txt* datoteke. Alati za automatsko skeniranje ranjivosti pretražuju moguće Google ranjivosti i testiraju rizike za sigurnost unutar sustava. Datoteka *robos.txt* sadrži ograničenja za operatore pretraživanja te korištenje iste sprečava indeksiranje osjetljivih podataka jer djeluje kao zahtjev za ignoriranjem navedenih datoteka ili direktorija prilikom pretraživanja (naputak google tražilici da iz rezultata pretrage isključi željene podatke).

Najnaprednija, ali i najkompleksnija metoda je instaliranje i upravljanje Google Honeypot sustavom te pokušati otkriti namjere napadača prije nego oni napadnu stvarni sustav. Ideja Google Honeypot sustava se sastoji od umetanja skrivene poveznice (eng. link) na web stranicu koja vodi hakera do PHP skripte kojom se prijavljuje njegova aktivnost umjesto otkrivanja podataka.




**Slika 2.** CAPTCHA testovi

Neke web stranice koje prikupljaju osjetljive sadržaje imaju posebne alate za zaštitu korisnika kao što je CAPTCHA test (eng. Completely Automated Public Turing Test to Tell Computers and Humans Apart) koji se koristi u računarstvu kako bi utvrdilo da odgovor ne generira računalo. Primjeri takve zaštite pomoću CAPTCHA testa prikazani su na slici 2.

Google Hacking DataBase (GHDB) je baza podataka upita koji identificiraju osjetljive podatke. Iako Google blokira neke od poznatijih upita, ništa ne zaustavlja hakera da indeksira stranice i pokrene GHDB upite direktno na pregledavani sadržaj.

Informacije koje Google Hacking DateBase identificira:

- Preporuke o ranjivosti
- Poruke o pogreškama koje sadrže previše podataka

- Datoteke koje sadrže lozinke
- Osjetljive direktorije
- Stranice koje sadrže portale za prijavu
- Stranice koje sadrže mrežne ili ranjive podatke kao što su firewall logovi

# 5. Zaključak

Pokazano je da hakiranje Google tražilicom pruža jednostavne i brze tehnike dobivanja osjetljivih informacija. Koristeći snažne pretraživače moguće je pretraživati razne vrste informacija pohranjene u ogromnom broju poslužitelja diljem svijeta. Dohvaćene informacije mogu biti iskorištene za otkrivanje ranjivosti te izvršavanje napada.

Spomenute su samo neke od brojnih ranjivosti koje se mogu otkriti i iskoristiti hakiranjem. Posljedice iskorištavanja navedenih ranjivosti mogu biti vrlo štetne za korisnika pa bi se zbog toga svi korisnici trebali pridržavati osnovnih načina zaštite podataka.

Iako se ulažu mnogi napori, a i mnogo novca u razvoj alata za zaštitu osjetljivih podataka, najprikladniji način zaštite je čuvanje tih podataka od izloženosti Internetu.

# 6. Reference


[1] Emin IslamTatli: Google Hacking Against Privacy http://www.cs.kau.se/IFIP-summerschool/papers/S01_P3_Emin_Islam.pdf,

[2] Don Doumakes, Matt Payne: Google Hacking 101, http://www.certconf.org/presentations/2005/files/WD4.pdf 2005

[3] Advanced Operators: http://www.googleguide.com/advanced_operators.html

[4] Google Hacking Database: http://johnny.ihackstuff.com/ghdb.php

[5] Google Hacking: http://en.wikipedia.org/wiki/Google_Hacking

[6] Website Security: http://www.acunetix.com/websitesecurity/google-hacking.htm

[7] Google Hacking: http://free-zg.t-com.hr/Davor-Sever/tekst/Google_hacking_by_UnDeAd.txt

[8] XSS (Cross Site Scripting): http://en.wikipedia.org/wiki/Cross-site_scripting

[9] SQL injection: http://en.wikipedia.org/wiki/SQL_injection

[10] Denial of Service: http://en.wikipedia.org/wiki/Denial-of-service_attack