

Forum:[Hack Forums](#)

Thread: [CLI Bing Dorker](#)

Hieroglyphicz - February 12, 2016, 7:18 am

This allows you to enter a search term, a number of pages to scan and returns the SQLi vulnerable pages as best as it can. It's not super in depth and you could definitely expand a lot on it's tests but just something I wrote out of boredom earlier:

PHP Code

```
<?php
#!/usr/bin/php
<?php
set_time_limit(0);
$query = cin('Query to search? ');
$pages = cin('Pages to search? ');
$showAll = cin('Show non injectable links too [y/N]? ');
$showAll = (preg_match("#y#", $showAll))?true:false;
$jar = array();
$pages = (int) $pages;
$start = 1;
$query = urlencode($query);
?>
*****

Starting up
*****

> Scanning bing for results....
<?php
while($pages) {
    $curl = curl_init("http://www.bing.com/search?q={$query}&first={$start}");
    curl_setopt($curl, CURLOPT_USERAGENT,
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:34.0) Gecko/20100101 Firefox/34.0");
    curl_setopt($curl, CURLOPT_URL, "http://www.bing.com/search?q={$query}&first={$start}");
    curl_setopt($curl, CURLOPT_FAILONERROR, true);
    curl_setopt($curl, CURLOPT_FOLLOWLOCATION, true);
    curl_setopt($curl, CURLOPT_AUTOREFERER, true);
    curl_setopt($curl, CURLOPT_RETURNTRANSFER, 1);
    $result = curl_exec($curl);
    curl_close($curl);
    preg_match_all("#<h2><a(?:.*)</a></h2>#i", $result, $links);
    foreach($links[1] as $link) {
        preg_match("#href=\"(?:.*)\"#", $link, $match);
        $jar[] = $match[1];
    }
    $start += 14;
    $pages--;
}
echo "> Scanning links for SQLi...\n";
foreach($jar as $link) {
    $curl = curl_init("{ $link}");
    curl_setopt($curl, CURLOPT_USERAGENT,
```

```

"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:34.0) Gecko/20100101 Firefox/34.0");
curl_setopt($curl, CURLOPT_URL, "{$link}");
curl_setopt($curl, CURLOPT_FAILONERROR, true);
curl_setopt($curl, CURLOPT_FOLLOWLOCATION, true);
curl_setopt($curl, CURLOPT_AUTOREFERER, true);
curl_setopt($curl, CURLOPT_RETURNTRANSFER, 1);
if($pagedata = curl_exec($curl)) {
    if (preg_match("/Query Error/i", $pagedata)) {
        $valid = "injectable";
    }
    elseif (preg_match("/You have an error in your SQL syntax/i", $pagedata)) {
        $valid = "injectable";
    }
    elseif (preg_match("/SQL syntax/i", $pagedata)) {
        $valid = "injectable";
    }
    elseif (preg_match("/SQL/i", $pagedata)) {
        $valid = "injectable";
    }
    elseif ($pagedata == "Connection Error") {
        $valid = "<i>[Connection Error]</i>";
    }
    else {
        $valid = "clean";
    }
    if($valid != 'clean' || $showAll) {
        echo "{$link} : ".colorize($valid, $valid)."\n";
    }
} else {
    if($showAll) {
        echo "{$link} : link dead\n";
    }
}
}
}

```

```

function cin($prompt="") {
    echo $prompt;
    $handle = fopen("php://stdin","r");
    return fgets($handle);
}
function colorize($text, $status) {
    $out = "";
    switch($status) {
        case "clean":
            $out = "[42m"; //Green background
            break;
        case "injectable":
            $out = "[41m"; //Red background
            break;
        case "warning":
            $out = "[43m"; //Yellow background
            break;
        default:

```

```
        throw new Exception("Invalid status: " . $status);
    }
    return chr(27) . "{$out}{$text}" . chr(27) . "[0m";
}
?>
```

stackoverflowin - February 12, 2016, 8:45 am

Eh, the logic of this is fine. But the quality of the script is just horrible, check out the PHP standards: <http://www.php-fig.org/psr/psr-1/>

It'll improve your coding style -- right now it's just a jumbled mess. You might want to port this over to a class and use Guzzle for the HTTP requests.

PHP Code

```
<?php
$out . $text"
```

Please, no!

Hieroglyphicz - February 12, 2016, 9:23 am

(Feb 12, 2016 09:45 AM)StackOverlowin Wrote: [\[CITE\]](#) Eh, the logic of this is fine. But the quality of the script is just horrible, check out the PHP standards: <http://www.php-fig.org/psr/psr-1/>

It'll improve your coding style -- right now it's just a jumbled mess. You might want to port this over to a class and use Guzzle for the HTTP requests.

PHP Code

```
<?php
$out . $text"
```

Please, no!

Thanks yeah I'll read back up. I've been locked up and in rehab the last year or so, so I'm a little rusty but I probably should do a bit a re-reading. Thanks

stackoverflowin - February 12, 2016, 9:58 am

Also you've made a common mistake;

PHP Code

```
<?php
$showAll = (preg_match("#y#", $showAll))?true:false;
->
$showAll = (preg_match("#y#", $showAll));
```

Hieroglyphicz - February 12, 2016, 9:45 pm

(Feb 12, 2016 10:58 AM)StackOverlowin Wrote: [\[CITE\]](#) Also you've made a common mistake;

PHP Code

```
<?php
$showAll = (preg_match("#y#", $showAll))?true:false;
->
$showAll = (preg_match("#y#", $showAll));
```

Oh I've actually never thought about that, thanks