# MOPS-2010-004: ClanSphere Captcha Generator Blind SQL Injection Vulnerability

May 3rd, 2010

A SQL Injection vulnerability was discovered in the Captcha generator of ClanSphere that allows retrieving all the data from the database.

### Affected versions

Affected is ClanSphere <= 2009.0.3

### Credits

The vulnerability was discovered by Stefan Esser during the Month of PHP Security SQL Injecton Marathon.

### About ClanSphere (translated)

ClanSphere is a modern and modular Web-CMS that allows to completely organise clans, clubs and other kinds of groups. It is a PHP script that is open source and free of costs for now. It is released under the new bsd license.

### Detailed information

This vulnerability was discovered during SQL Injection Marathon a PHP code auditing marathon performed by Stefan Esser. The basic idea of this initiative is to select random PHP applications and perform a short code audit on them. The maximum time spent on each application is 30 minutes and after the first found SQL injection usually the next application is audited.

During SQL Injection Marathon ClanSphere was also audited and within 30 minutes it was possible to find multiple SQL injection vulnerabilities. The first one is located in the Captcha generator. The captcha generator of ClanSphere contains the following code.

```
#$ip = cs_sql_escape($_SERVER['REMOTE_ADDR']);
$ip = cs_getip();
$timeout = cs_time() - 900;
$save_hash = isset($_GET['mini']) ? 'mini_' . $hash : $hash;

$where = "captcha_ip = '" . $ip . "' AND captcha_time &lt; '" . $timeout . "'";
$old = cs_sql_select(__FILE__,'captcha','captcha_id',$where,'captcha_time DESC');
```

One can see here that the output of the cs_getip() function is used directly in the captcha generator for an SQL query. One can also see that this was safe in earlier days because the SQL escaped remote addr was used instead. To see that it is a possible SQL injection vulnerability now it is necessary to look into the implementation of the cs_getip() function that is presented below.

```
function cs_getip () {

  if (getenv('HTTP_CLIENT_IP'))
    $ip = getenv('HTTP_CLIENT_IP');
  elseif (getenv('HTTP_X_FORWARDED_FOR'))
    $ip = getenv('HTTP_X_FORWARDED_FOR');
  elseif (getenv('HTTP_X_FORWARDED'))
    $ip = getenv('HTTP_X_FORWARDED');
  elseif (getenv('HTTP_FORWARDED_FOR'))
    $ip = getenv('HTTP_FORWARDED_FOR');
  elseif (getenv('HTTP_FORWARDED'))
    $ip = getenv('HTTP_FORWARDED');
  else
    $ip = isset($_SERVER['REMOTE_ADDR']) ? $_SERVER['REMOTE_ADDR'] : '';
  return $ip;
}
```

You can see here that the remote addr is only used as fallback nowadays. Instead the IP is taken from a number of HTTP headers. However HTTP headers are also user input and therefore cannot be trusted. Therefore each of the trusted HTTP headers can be used for a blind SQL injection attack on ClanSphere’s captcha generator.

**Proof of concept, exploit or instructions to reproduce**

No proof of concept exploit will be provided for this vulnerability.

**Notes**

The vendor already released a fixed version of ClanSphere 2009.3.1. However in his release announcement he claims that for MOPS we checked ClanSphere very deeply by using the german expression “auf Herz und Nieren geprÃ¼ft”. This is however not true. ClanSphere like any other application was only checked for less than 30 minutes. You should always remind that when looking at the vulnerabilities found during SQL Injection Marathon. Each of these vulnerabilities was found in less than 30 minutes so they were easy to find and therefore most probably long known by blackhats.

---