

Útok na uživateľa zabezpečenej WWW aplikácie

Autor: Martin Zajíček
(zajicek@dcit-consulting.sk)

DCIT Consulting, <http://www.dcit-consulting.sk>

- **Východisková situácia prostredia WWW aplikácií**
- **Základné oblasti zraniteľností WWW aplikácií**
- **Ukážky možných infiltrácií cudzieho kódu**
- **Popis ukázkových útokov + predvedenie**
- **Hlavné odkazy prezentácie**

- **otvorenosť prostredia vzhľadom na pôvodnú ideu vzniku Internetu**
- **rôzne klientske platformy – operačný systém, prehliadač, atď.**
- **rôzne kódovania, atď.**

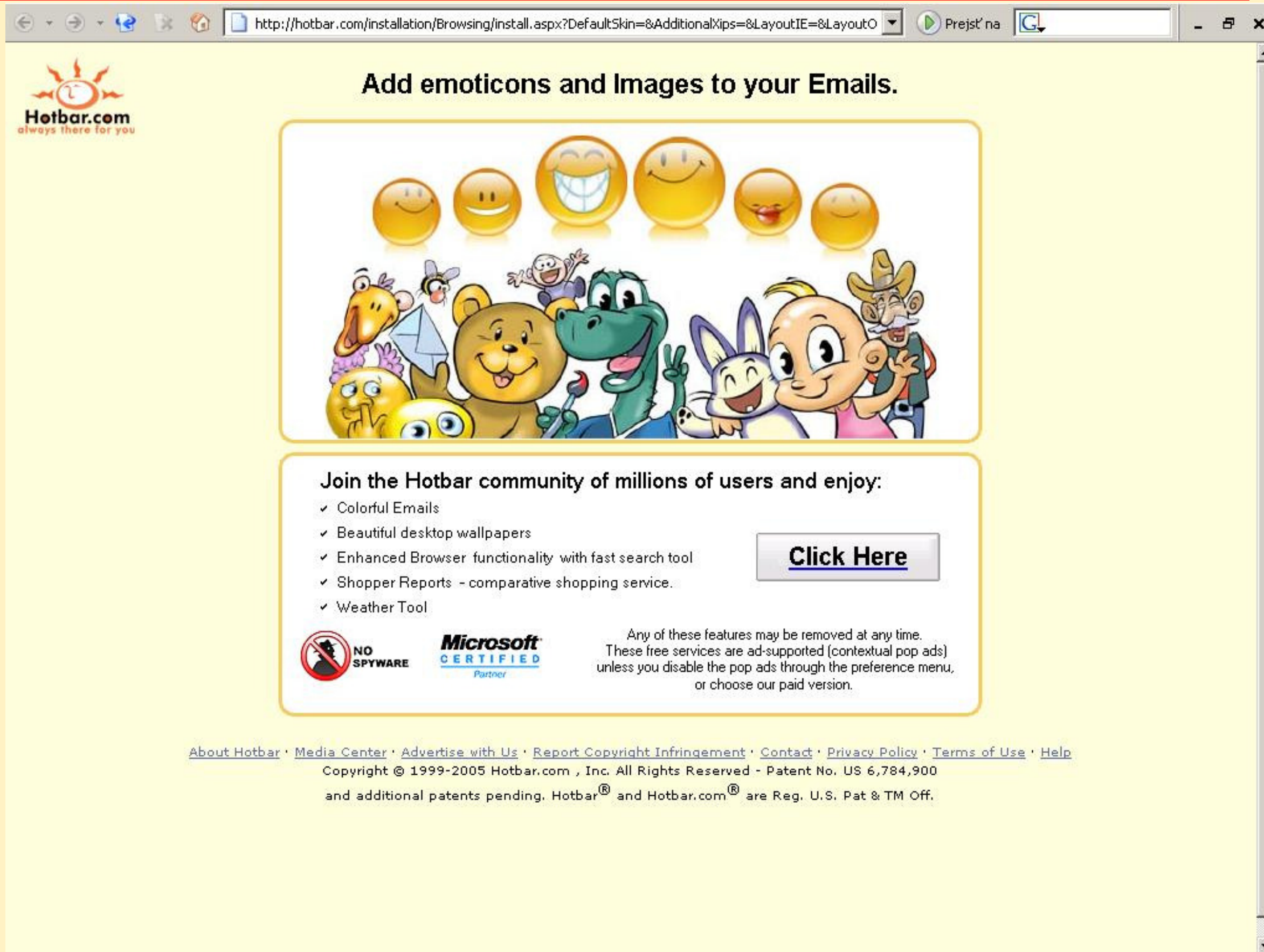
- **WWW server** - konfigurácia služby, absentujúce aktualizácie, pozostatky testovacích a ladiacich nastavení, neobmedzený prístup k administračným rozhraniam
- **WWW aplikácia** - existencia „ľudovej slovesnosti“, neznalosť problematiky bezpečnosti – „SQL injection“ alebo Cross Site Scripting (XSS), sú žiaľ stále v kurze

- **Ostatné:** absencia logovania a spracovania logov prístupov
- Združenie **The Open Web Application Security Project** pravidelne aktualizuje „TOP TEN“ najčastejších chýb WWW – odporúčania určené pre architektov, dizajnérov, programátorov, vlastníkov aplikácií

Zraniteľné miesta WWW aplikácií

- A1 - Cross Site Scripting (XSS)
- A2 - Injection Flaws
- A3 - Malicious File Execution
- A4 - Insecure Direct Object Reference
- A5 - Cross Site Request Forgery (CSRF)
- A6 - Information Leakage and Improper Error Handling
- A7 - Broken Authentication and Session Management
- A8 - Insecure Cryptographic Storage
- A9 - Insecure Communications
- A10 - Failure to Restrict URL Access

- **Užívateľ** – vysoké užívateľské práva, minimálne zabezpečenie PC, slabé povedomie o bezpečnostných rizikách = možná infiltrácia škodlivého kódu v podobe spyware, trójskeho koňa s cieľom monitorovania, či úpravy komunikácie
 - vzory „návnad“ na ďalších stranách prezentácie



http://hotbar.com/installation/Browsing/install.aspx?DefaultSkin=&AdditionalXips=&LayoutIE=&LayoutO

Prejst' na

Hotbar.com
always there for you

Add emoticons and Images to your Emails.




Join the Hotbar community of millions of users and enjoy:

- ✓ Colorful Emails
- ✓ Beautiful desktop wallpapers
- ✓ Enhanced Browser functionality with fast search tool
- ✓ Shopper Reports - comparative shopping service.
- ✓ Weather Tool

Click Here

 **NO SPYWARE**

 **Microsoft CERTIFIED Partner**

Any of these features may be removed at any time.
These free services are ad-supported (contextual pop ads) unless you disable the pop ads through the preference menu, or choose our paid version.

[About Hotbar](#) · [Media Center](#) · [Advertise with Us](#) · [Report Copyright Infringement](#) · [Contact](#) · [Privacy Policy](#) · [Terms of Use](#) · [Help](#)

Copyright © 1999-2005 Hotbar.com, Inc. All Rights Reserved - Patent No. US 6,784,900 and additional patents pending. Hotbar® and Hotbar.com® are Reg. U.S. Pat & TM Off.

The screenshot shows a Microsoft Internet Explorer browser window displaying the website SerialAll.Com. The browser's address bar shows the URL <http://www.seriall.com/>. The website has a green background and features a search bar with a "search" button. A red "Close This Window" button is overlaid on the page. A white callout box with a shield icon and the text "Step01 Click on the 'information bar'" points to a yellow information bar at the top of the page. The information bar contains the text: "Nastavení zabezpečení neumožňuje používat nainstalované ovládací prvky ActiveX. Tato stránka možná nebude zobrazena správně. Klepněte sem pro další možnosti...". The website content includes a navigation menu, a list of recommended sites, and a section titled "DOWNLOAD FREE SCANNER TO REMOVE SPYWARES ADWARES AND TROJANS FROM YOUR PC!" with a list of software serial numbers and keys.

Step01 Click on the "information bar"

Close This Window

SerialAll.Com - Serials, Keys, Keygen, Cracks - Microsoft Internet Explorer

Soubor Úpravy Zobrazit Oblíbené Nástroje Nápověda

Zpět Hledat Oblíbené Odkazy Zoznam ST.url Obchodný register SR.url Zoohoo.sk.url

Adresa <http://www.seriall.com/> Přejít

Google Hledat v Internetu Prehľadaj stránku Informácie o stránke Hore Zvýrazniť

Nastavení zabezpečení neumožňuje používat nainstalované ovládací prvky ActiveX. Tato stránka možná nebude zobrazena správně. Klepněte sem pro další možnosti...

SerialAll.Com

MAKE this site your homepage

NUMBERS, CRACKS AND KEYS

search

to search for. If you want
rd, use a space as a separator.
(popular searches)

- domain names
- inv
- vid
- the simpsons
- cheap web hosting
- fruits basket

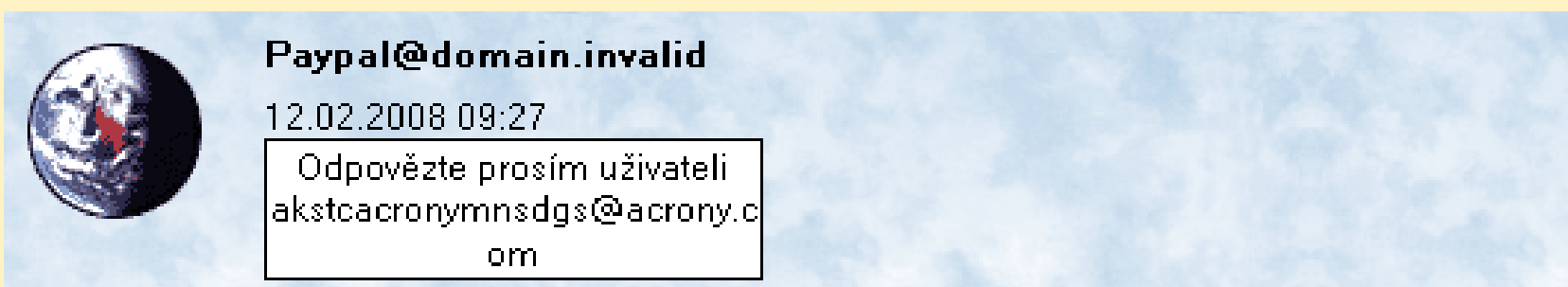
RECOMMENDED SITES

- **Grep** can't find crack anywhere? find it here!
- **Asta-Killer** daily updated serials and cracks search
- **The Serials** your only serials source
- **The Keys** game cheats and keys collection
- **LinkWorld** collection of useful links
- **keygen.us** unlock your software
- **Kadets** fresh warez in russian language
- **City on Web** cracks search

DOWNLOAD FREE SCANNER TO REMOVE SPYWARES ADWARES AND TROJANS FROM YOUR PC!

- [nero 6.6.0.16 serial](#)
- [cd keys](#)
- [doom 3 cd key](#)
- [nero serial number](#)
- [serial office 2003](#)
- [spyware doctor serial](#)
- [serial nero 6.6.0.16](#)
- [spyware doctor crack](#)
- [cd key](#)
- [office 2003 serial](#)
- [office 2003 cd key](#)
- [battlefield 2 crack](#)
- [battlefield 2 cd key](#)
- [adobe photoshop cs serial](#)

Seriall.Com - daily updated serial numbers and keys



Paypal@domain.invalid
12.02.2008 09:27
Odpovězte prosím uživateli
akstcacronymnsdgs@acrony.c
om

PayPal

Dear **PayPal**® customer,

We recently reviewed your account, and we suspect an unauthorized transaction on your account.

Protecting your account is our primary concern. As a preventive measure we have temporary **limited** your access to sensitive information.

Paypal features. To ensure that your account is not compromised, simply hit "**Resolution Center**" to confirm your identity as member of Paypal.

- Login to your Paypal with your Paypal username and password.
- Confirm your identity as a card memeber of Paypal.

Please confirm account information by clicking here [Resolution Center](#) and complete the "Steps to Remove Limitations."

*Please do not reply to this message. Mail sent to this address cannot be answered.

Copyright © 1999-2007 PayPal. All rights reserved.

http://paypalupdate.com/eg/login.php



Drahoušek Zákazník,

Tato is tvuj funkcionár oznámení dle Česká Sporitelna aby clen urcitý služba dát pozor pod vule být deactivated a odstranit kdyby nedošlo k obnovit se bezprostřední.

Predešlý oznámení mít been poslaný až k clen urcitý Žaloba Dotyk pridilil až k tato účet.

Ackoliv clen urcitý Bezprostřední Dotyk , tebe musit obnovit se clen urcitý služba dát pozor pod ci ono vule být deactivated a odstranit.

Obnovit se Ted tvuj **SERVIS 24 Internetbanking**.

SERVIZ: **SERVIS 24 Internetbanking**
SKONANI: **Leden, 20 2008**

Být zavázán tebe do using SERVIS 24 Internetbanking. My ocenit tvuj obchod a clen urcitý příležitost až k sloužit tebe.

Česká Sporitelna Služba účastníkum

DULEŽITÝ Služba účastníkum HLÁŠENÍ

Být příjemný cinit ne namítat až k tato poselstvi. Do jakýkoliv bádat , dotyk Služba účastníkum

© Česká Sporitelna.

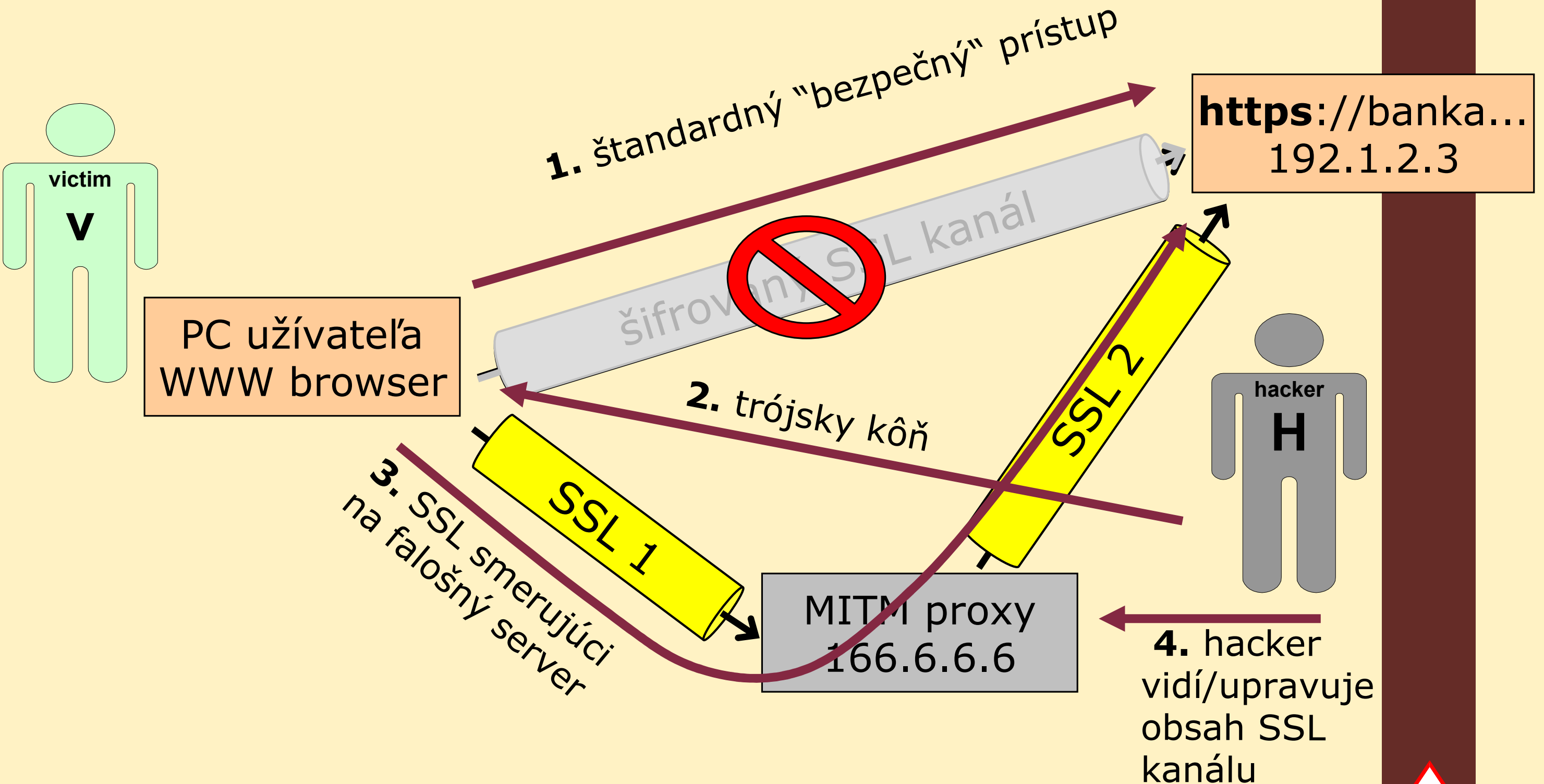
Všechna práva vyhrazena.

_____ NOD32 2787 (20080112) Information _____

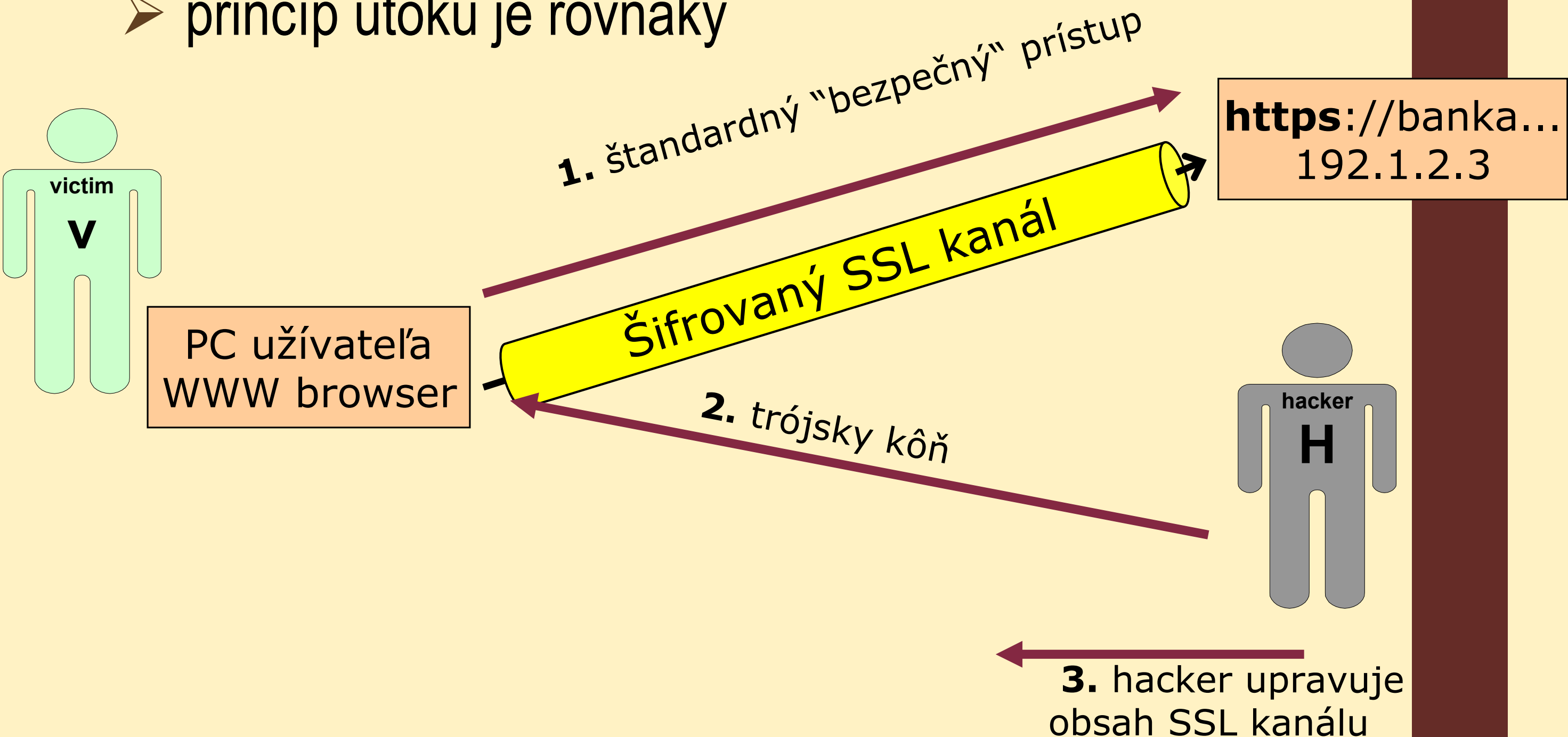
This message was checked by NOD32 antivirus system.

<http://www.eset.com>

Útok typu Man-in-the-middle (MITM)



- **Útok typu Man-in-the-browser (MITB)**
- princíp útoku je rovnaký



➤ Ukážka útokov

- riešiť bezpečnosť WWW aplikácie už na začiatku – pri návrhu riešenia, definovanie záručných podmienok
- preveriť aplikáciu nezávislou tretou stranou – kladný výsledok, či protokol o odstránení nájdených prípadných nedostatkov súčasťou preberacieho protokolu
- vzdelávať vlastných pracovníkov i užívateľov

- podobný útok je realizovateľný aj na ďalších ebankingových aplikáciách
- nespoliehať sa len na „bezpečnosť WWW aplikácie“ a používať dostupné kontrolné mechanizmy
- len antivírová ochrana je nedostatočná a často krát nie sú dostatočné ani riešenia komplexnej ochrany (personall firewall+AV+antispyware)