Cross Site Scripting (XSS) in Action

زانکۆی هەڵەبجە ، کۆلێژی زانست ، بەشی کۆمپیوتەر

ئامادەکردن : بڕوا نعمان محمد

پوختە

XSS باوترین لاوازی ئاسایشە کە دەتوانرێ بدۆزرێتەوە لە بەرنامەی (کاربەرنامەی) وێب لە ئەمڕۆدا.

هەربەرنامەیەکی وێب بەرهەمێک دروست دەکات لەسەربنەمای ئەو زانیاریەی کە بەکارهێنەر داخڵی دەکات بەڵام بەبێ ڕاست کردنەوەی ناوەڕۆکەکە بە شێوەیەکی ڕاستەقینە ئەوا ئاماژەیە بۆ XSS.

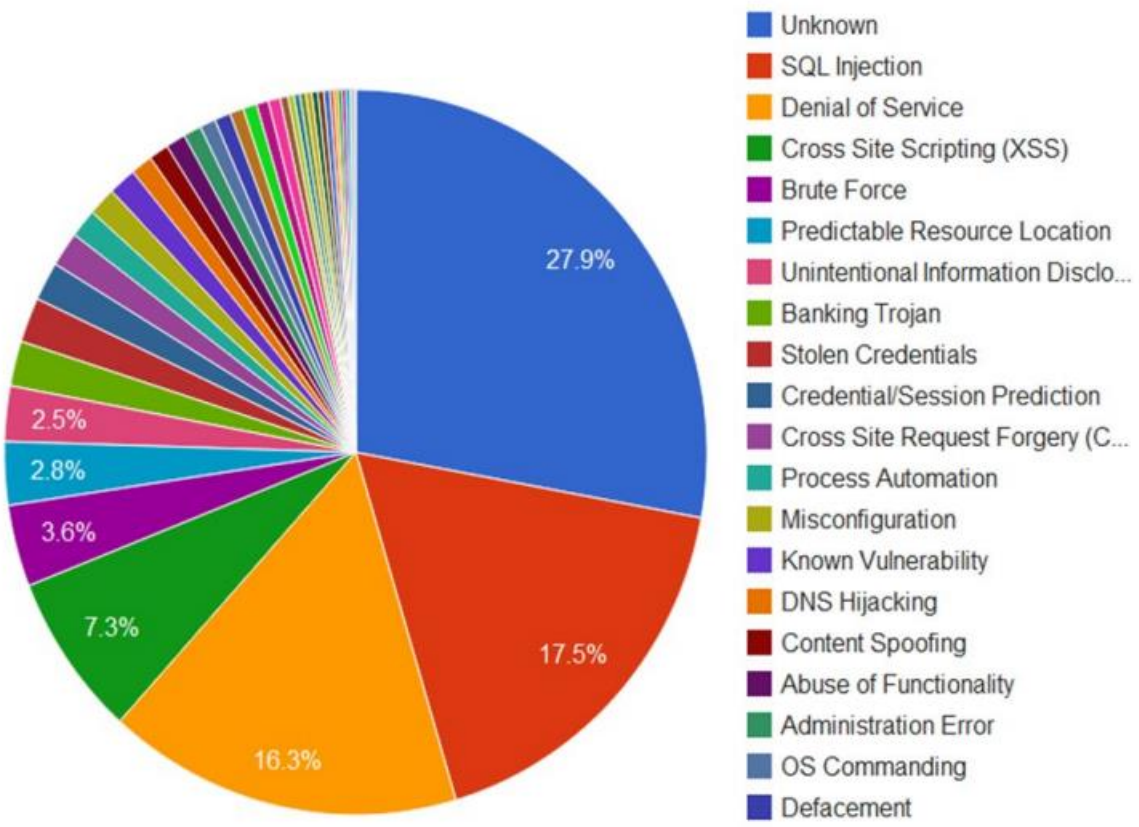
سەلماندنی ئەو زانیاریانەی کە بەکارهێنەر داخڵی دەکات لە ڕێگەی فلتەرکردن و لابردنی داتای نەخوازراو کە کاریگەرترین ڕێگایە بۆ ڕێگرتن لە هێرشەکانی XSS .

وشەسەرەکیەکان

XSS ، فلتەرکردن ، لابردنی داتای نەخوازراو ، هێرشی XSS ، نموونەی XSS.

کورتەیەکی گشتی دەربارەی XSS

XSS یەکێکە لە باوترین هەڕەشەکانی ئاسایش لە بەرنامەی (کاربەرنامەی) وێب لە ئەمڕۆدا ، بەپێی داتابەیسی (بنکەی زانیاری) ڕووداوی هاککردنی وێب بۆ ساڵی ٢٠١١ ، XSS پلەی سێیەم داگیردەکات (٧.٣٪) هەروەها لە ساڵانی (١٩٩٩-٢٠١١) یەکێک بوە لە باوترین شێوازەکانی هێرش کردن. وەک لە خشتەی خوارەوەدا ڕوون کراوەتەوە



XSS شێوازێکە بەکاردێت بۆ دزینی داتا لە بەکارهێنەران بە توشبونی لاپەڕەکانی وێب بە سکریپتی بەدکار (سکریپتی زیانبەخش) (VBScript, JavaScript, ActiveX, Flash) ، بۆ ئەوەی زانیاری هەستیار و گرنگ لە سەردانیکەر (قوربانی) کۆبکاتەوە .

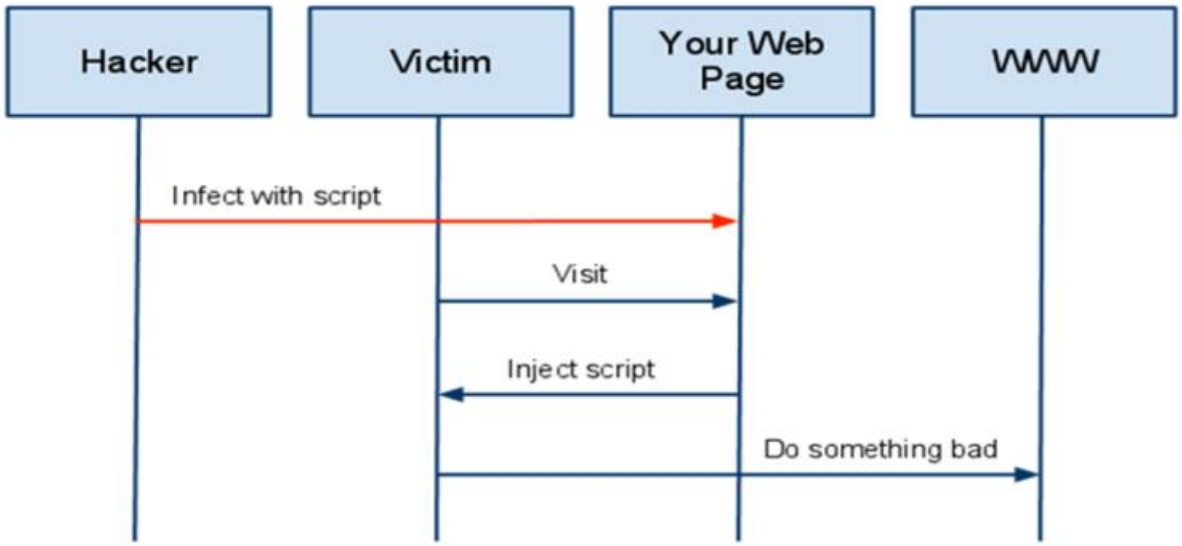
XSS خەریکی بە ئامانج گرتنی لاپەڕەکانی وێبی داینەمیکیە کە لەلایەن وێبگەڕەکانەوە لێکدەدرێنەوە ، بۆیە سکریپتە زیانبەخشەکان بە شێوەیەکی ناوخۆی لەسەر ئامێری بەکارهێنەر جێبەجێدەکرێن و زانیاریە هەستیارەکان بەم شێوەیە کۆدەکرێنەوە و لە کۆمپیوتەری قوربانیەکەوە دەگوازرێتەوە (دەنێردرێت) بۆ شوێنی هێرشبەرەکە ، عادەتەن هیرشبەرەکان لینکی زیانبەخش لەسەر ئینتەرنێت بڵاو دەکەنەوە ، چاوەڕێی ئەوەدەکەن کە بەکارهێنەرەکان کرتە بکەن.

هێرشی ئاسای XSS

تائێستە زۆر ڕوونە کە هێرشبەرەکە پێویستی بە چوونە ژورەوە یاخود دەستگەشتن بە وێب سێرڤەری بەرنامەکەناکات بەڵکو تەنها بە گۆڕینی پەڕەی وەڵامدانەوەکە بە هەندێک سکریپتی تایبەت لەناوەوە ، سەرەڕای ئەوەش ، بەکارهێنەرەکە گێڵە(وشیارنیە) ئەم سکریپتانە لەسەر ئامێرەکەی جێبەجێدەکات .

بەم شێوەیە هێرشبەرەکە دەستی دەگاتبە ناوەڕۆکی زانیارییە هەستیارە خوازراوەکان ، هە پەڕەیەک کە فۆڕم یاخود داینەمیک لینک لەخۆ دەگرێت لاوازە بۆ ئەم جۆرە شێوازی هێرش کردنە .

وێنەی داهاتوو وەسفی شێوازی هێرشی XSS دەکات



زۆربەی هێرشەکانی XSS تاگی <Script> بەکاردێنن بۆ چالاککردنی ناوەڕۆکە زیانبەخشەکان لەسەر پەڕەی وێبی بەکارهێنەر کەبە شێوەیەکی ناوخۆی لیکدەدرێنەوە ، تاگەکە لەوانەیە دەقێکی چەسپێنراو یان دەقێکی دەرەکی چالاک بکات .

- Embedded, <Script>alert(“XSS-Cross site scripting”)</Script>
- External, <Script>src=http://some.evil.site.com/xss.js </Script>

تاگی تری HTML مان هەیە کە دەتوانرێ سکریپتەکەی پێ ئینجێکت بکرێت وەک BODY, IMG, LINK, INPUT, TABLE, DIV, OBJECT, EMBED وە زۆری تر.

نموونەی هێرشی XSS

بەرنامەی ئاشکرا بۆ XSS چیە ؟

لە ڕاستیدا هەربەرنامەیەکی وێب کە بەرهەمێک دروست دەکات لەسەربنەمای داخڵکردنی زانیاریە لە بەکارهێنەرەوە بەڵام بەبێ راستکردنەوەی ناوەڕۆکەکە بەشێوەیەکی ڕاستەقینە ئاماژە بۆ XSS دەکات .

نمونەی ئە بەرنامانەی کوێری بەکاردێنن لەگەڵ پارامیتەرەکان کەڕێگە بە کرداری بووک مارکینگ (نیشانەکردن) دەدەن هەمیشە نرخی پارامیتەرەکە شوێنەکەی ناو URL کەیە .

باوێنای بزوێنەرێکی گەڕانی سادە بکەین کاتێک بەکارهێنەرەکە بۆکسی نوسینەکە بەکاردێنێت بۆ نوسینی دەقێک و پاشان فشاردەخاتە سەر دوگمەی گەڕانەکە بەرنامەکە دەقەکەو لیستێک لە ئەنجام پیشان دەدات کە پەیوەند دارە بەو دەقەی کە داخڵمان کردبوو.

http://www.mysearchtool.org/locate.php?searchstring=XSS

بە دروست کردنی لینکێک کە سکریپتی تێدایە و دانانی لە شوێنی گەڕانی دەق دا ، کاتێک پەڕەکە هەوڵدەدات دەقەکە پیشان بدات ، ئەوا لە ڕاستیدا سکریپتەکە جێبەجێ دەبێت بۆیە هێرشبەرەکە دەتوانێت داتای هەستیار کۆبکاتەوە کە هەڵگیراوە لەسەر کۆمپیوتەری باکارهێنەری بێتاوان (نێچیر)

http://www.mysearchtool.org/locate.php?searchstring=<script>alert("XSS")</script>

چۆن ڕێگە لەم جۆرە دۆخانەبگرین ؟

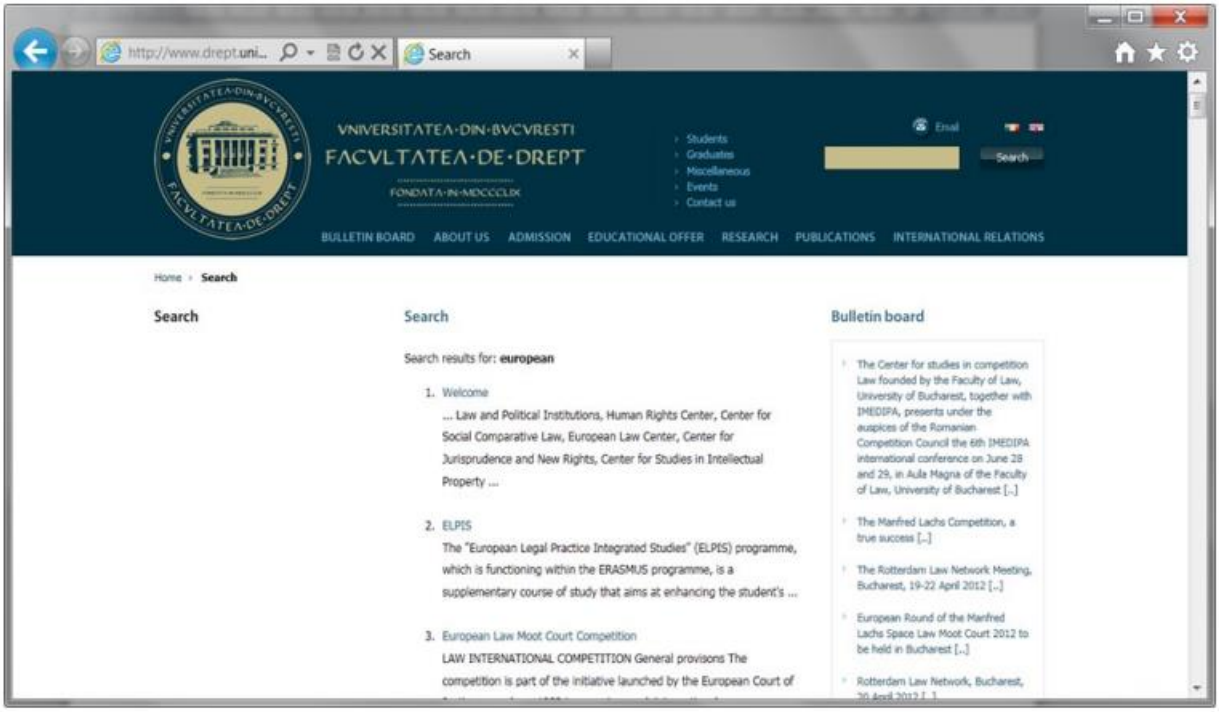
وەڵامەکە زۆر سادەیە: هەربەرنامەیەکی وێب کە زانیاری داخڵ کراوی بەکارهێنەر پیشان بدەدات دەبێت ناوەڕۆکەکەی بسەلمێنرێت پێش ئەوەی داخڵی پەڕەی بەرهەمبێت ، بە شێوەیەکی ئاسای سێرڤەری وێب پێویستە فلتەری ئەو زانیاریانە بکات کە بەکارهێنەر داخڵی دەکات بۆ سڕینەوەی ئەو ناوەڕۆکانەی کەلەوانەیە کێشەدروست بکەن.

هێرشی XSS – نموونەی ژیانی ڕاستەقینە

بۆ ئەوەی نموونەیەکی ژیانی ڕاستەقینە دابین بکەین ، من هەوڵمداوە ماڵپەڕێکی ڕۆمانی بدۆزمەوە کە بەشێکی ئینگلیزیشی هەیە ، بۆیە من قوتابخانەی یاسام هەڵبژارد لە زانکۆی بوخارست . گرنگترین قوتابخانەی یاسا لە ڕۆمانیا http://www.drept.unibuc.ro/index-en.htm .

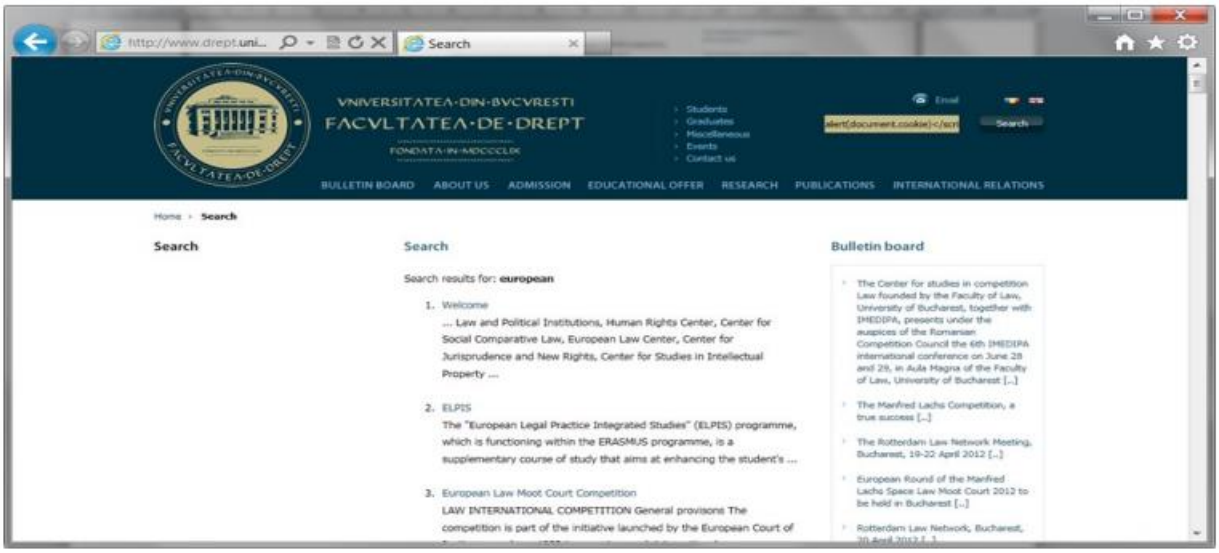
بەکارهێنەرەکان لەوانەیە بچنەژورەوە بۆ وێب سایتەکە بۆ دەست گەیشتن بە هەندێک ناوچەی سنوردار کراو (خشتە – دەرەجە – باج – هتد...) ، کەواتە بەرنامەی وێب بە شێوەیەکی ناوخۆی کوکیز هەڵدەگرێت (خەزندەکات) کە بەکاردێت بۆ ناسینەوەی ناسنامەی قوتابی بۆ سەردانەکانی داهاتوو لە هەمان ئامێرەوە

لەبەشی ڕاستی سەرەوەی لاپەڕەکە ، بۆکسی گەڕان هەیە کە دەتوانرێت بەکاربێت بۆ خێرا دۆزینەوەی ناوەڕۆکێکی دیاریکراو ، بۆ نموونە ئەگەر بەکارهکراو ، بۆ نموونە ئەگەر بەکارهێنەر حەزی لە دۆزینەوەی سەرچاوەی پەیوەندیدار بە یاسادانانی ئەوروپاوە بوو ئەوا بۆکسی گەڕان لەوانەیە بژاردەیەکی زۆر گونجاو بێت

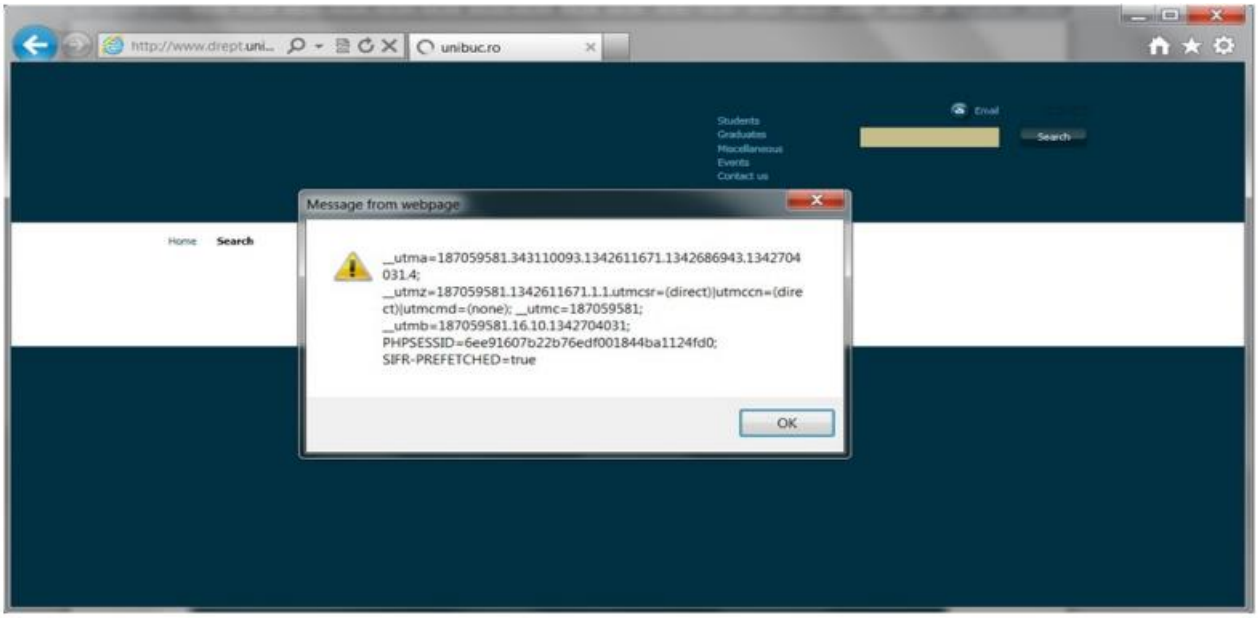


وەک چۆن دەتوانین تێبینی بکەین پەڕەکە تەنها ئەنجامەکان لە خۆ ناگرێت بەڵکو دەقە ئەسڵیەکەی داخڵمان کردبوو ئەویش لە خۆ دەگرێت بۆیە ئەمە پێدەچێت بژاردەیەکی زۆر باشبێت بۆ هێرشی XSS .

ئێمە بۆکسی گەڕان بەکاردێنین کە دەکەوێتە بەشی ڕاستی سەرەوەی پەڕەکە وە بۆ ئینجێکت کردنەکە سکریپتێکی جاڤا سکریپت بەکار دێنین کە بتوانێت ناوەڕۆکی کوکیزی بەکارهێنەرەکە ئاشکرابکات.



بەکەمترین هەوڵ بەرنامەکە وردەکاریە هەستیارەکان ئاشکرا دەکات وەک ڕوون کراوەتەوە لە شێوەی خوارەوەدا



وەک دەبینن ، ئەوە زۆر ئاسای دەردەکەوێت بۆ هێرشبەرێک بۆ دزینی ناسنامەی خوێندکارە تۆمارکراوەکانی ئێستا.

ئەنجامەکان

هێرشەکانی XSS لەمڕۆدا زۆر باون بەشێوەیەکی سەرەکی چونکە تەکنیکەکە زۆر سادەیە و ئەنجانەکان زۆر سادە دەردەکەون ، وەک بینیمان لە نموونەکەدا کەلەسەروە پیشاندراوە .

چۆن ڕێگری لەوهێرشانەبکەین ؟ وەڵامەکە سەلماندنی زانیری داخڵکراوە لەلایەن بەکارهێنەرەوە .

هانگاوی یەکەم بریتی دەبێت لە فلتەرکردنی ناوەڕۆک بە لابردنی هەر وشەیەکی مەترسی دار ، وەک تاگی <script> ، ئەمە دەکرێت بە زیادکردنی چەند کۆدێک بۆ بەرنامەی وێب یان بە بەکارهێنانی dedicated libraries ، بەدڵنیایەوە فلتەرەکان لەوانەیە هەندێک دەقی دروست و بڕوادار بسڕنەوە ، کەواتە ئەم فلتەرانە پێویستە بە ئاگای بەکار بهێنرێت .

دووەم ، هەڵاتن دەکرێت بەکاربهێنرێت بۆ ئاماژەدان بەو وێبگەڕە کە نابێت داتاکان بە هیچ شێوەیەک لێکبدرێنەوە ، کەواتە وێبگەڕەکە سکریپتەکە جێبەجێ ناکات تەنانەت ئەگەر بە دروستیش ئینجێکت بکات کۆدەکە،

لە کۆتایدا بەرنامەی وێب دەبێت بە شێوەیەکی گونجاو تاقیبکرێتەوە لە دژی XSS بۆ ئەم هۆکارە سکانەرێکی خۆکاری XSS پێشنیار دەکرێت بەکاربهێنرێت بۆ تێست کردنەکە.

سەرچاوەکان

1. XSS Attacks: Cross-site Scripting Exploits and Defense - http:// books.google.ro/books?id=Imt5Crr0jJcC&redir_esc=y
2. Cross Site Scripting Attack - http://www.acunetix.com/ websitesecurity/cross-site-scripting.htm
3. Felician Alecu, Securitatea în Internet, Informatică Economică, 3/2006, pp. 5 – 8, Editura ASE, București, 2006
4. The Law School of the University of Bucharest - http:// www.drept.unibuc.ro/index-en.htm
5. Preventing XSS Attacks - http://www.acunetix.com/blog/websecurity-zone/articles/preventing-xss-attacks/