



stopthehacker.com

“making the internet safer one website at a time”™

Jaal LLC ©

Script Vulnerabilities Leave Numerous Sites Effectuated

This public announcement is being made on behalf of Jaal LLC, an Internet security startup. Please read the disclaimer provided at the end of this document before proceeding.

More than 70,000 sites may have been compromised and become unwilling participants to cyber-crime in what could be a major outbreak in the making. Visitors to these sites can be exposed to malicious content, redirected to other sites or even infected by viruses, though as of present, we have not identified the exact purpose of the attacker. JAAL LLC and collaborators have identified the outbreak and to the best of our knowledge, this is the first public announcement of this specific vulnerability.

The list of sites and the associated “compromised” links are listed at the end of this announcement. A majority of these links were found to be active at 7 AM PST Friday the 6th of June 2008.

For more up-to-date information, visit: www.stopthehacker.com

If you found this announcement useful, please consider posting an acknowledgement in our newsgroup:

<http://jaalcheck.com/viewtopic.php?f=1&t=6>

Your feedback can keep us going.

External resources on the Internet where a detailed commentary may be found of this problem have also been listed below. In all these commentaries, a member of JAAL was involved.

Details of the Exploited Sites

On Thursday, Jun 5th 2008, one of the members of JAAL was informed about the behavior of the search functionality on the highly popular site pba.com, which caters to Pro-bowling enthusiasts. Team members followed upon this request and soon it was discovered that the ASP code which was being used to power the search functionality was the culprit.

Team members from JAAL have informed the webmaster of this site about this issue and have also notified security groups, stopbadware, of this issue.

The problem: When users search for simple items like [oil patterns](#) users are presented with a web page which displays adult material, This content is hardly suitable for the site in question.

Analysis: The JAAL Team has identified the following rationale for this exploit. We would like to thank members of stopbadware who have expressed their support in this regard.

The exploit on the pba.com site occurs because the input string, which is entered for the search, is incorrectly formatted before processing it. The process of safely escaping and removing unwanted/dangerous characters and commands from input on a web form is called "sanitization". It appears there are coding errors in pba.com's search script. Again, we do not claim that pba.com has been compromised, we simply state that there are errors in pba.com's "feature.asp" code which could potentially allow malicious entities to cause harm to the site, its reputation and to its visitors.

Therefore, any raw HTML code which is entered as input into the search form is pushed back on the output page as raw HTML and hence presents the user with a screen full of questionable material which links to conesfree.com, an adult content site. Simply put, pba.com needs to re-write/audit its sanitization policy or scripts.

Translating the query from its native format to simple text (ascii), we see:

```
<h1>download+porn+sex</h1><p>new+porn+starlets</p><a+href=conesfree . com><img + src=// conesfree . com/i.php><br>
```

This injection points to conesfree.com, an adult website. Team members from JAAL have included information about the owner of this site in this report and have sent the information to pba.com too. As of now, Google/stopbadware/McAfee don't flag either pba.com or conesfree.com as unsafe. However, it is a well known fact that once an exploitable script is found on a site, malicious entities can employ it to infect browsers viewing the page.

Interestingly, a large number of websites seem to have been affected by this kind of script vulnerability. They are listed below. In fact some arguably high profile sites seem to have been affected. JAAL lists only 100 odd sites out of the nearly 71300 results that were obtained by searching for specific terms on Google. JAAL is in the process of contacting the site administrators for these sites to inform them about the vulnerabilities in their scripts.

Again, we would like to extend our thanks to Steve and Erica from Stopbadware. An example of the kind of questionable content is provided at the very end, PLEASE BE WARNED, IT IS NOT SAFE FOR WORK!

More information can be found on

<http://banerjee-anirban.blogspot.com/2008/06/helping-out-on-stopbadwareorg.html>

<http://jaalcheck.com/viewtopic.php?f=1&t=6>

and on stopbadware.org

EFFECTED SITES

1 <http://www.modthesims2.com>
2 <http://www.anagramgenius.com>
1 <http://www.movieweb.com>
1 <http://www.marketingvox.com>
1 <http://www.qwikcast.com>
1 <http://www.isound.com>
1 <http://www.reedfirstsource.com>
1 <http://www.filter-mag.com>
1 <http://www.onsemi.com>
1 <http://www.garnethill.com>
1 <http://www.marthastewart.com>
1 <http://www.filter-mag.com>
1 <http://www.atlantafalcons.com>
1 <http://www.solvaychemicals.com>
1 <http://www.solvay-fluor.com>
1 <http://www.usg.com>
1 <http://www.nashbar.com>
1 <http://www.guiasenor.com>
1 <http://www.drawerb.com>
1 <http://www.ebags.com>
1 <http://www.marthastewart.com>
1 <http://www.atlantafalcons.com>
1 <http://www.thesmedleylog.com>
1 cleaning101.com
1 <http://www.cartoondollemporium.com>
1 <http://www.euclidchemical.com>
1 <http://www.bitlaw.com>
1 <http://www.cartype.com>
1 <http://www.dclab.com>
1 <http://www.guiasenor.com>
1 <http://www.almaz.com>
1 <http://www.verdictoncars.com>
1 <http://www.drawerb.com>
1 <http://www.safariwest.com>
1 <http://www.dinewise.com>
1 <http://www.ebags.com>
1 <http://www.visitpensacola.com>
1 <http://www.shelldorado.com>
1 <http://www.solsem.com>
1 <http://www.macminute.com>
1 <http://www.eyeonbooks.com>
1 <http://www.pain.com>
1 <http://www.iweiss.com>
1 <http://www.linuxmanpages.com>
1 <http://www.download3k.com>
1 <http://www.blastro.com>
1 cleaning101.com
1 <http://www.thesmedleylog.com>
1 <http://www.rickbayless.com>
1 <http://www.ccamatil.com>
1 <http://www.cortlandreview.com>
1 <http://www.windfinder.com>
1 <http://www.silkwormink.com>

1 <http://www.projekt.com>
1 <http://www.woodenshoe.com>
1 <http://www.scientificindustries.com>
1 <http://www.pridetoronto.com>
1 <http://www.cortina-systems.com>
1 <http://www.unreliablewitness.com>
1 <http://www.cottoninc.com>
1 <http://www.ezinedirector.com>
1 <http://www.classbuilder.com>
1 <http://www.radiantsystems.com>
1 <http://www.rms.com>
1 <http://www.scourstop.com>
1 <http://www.cooperlighting.com>
1 <http://www.creative-weblogging.com>
1 <http://www.jackstackbbq.com>
1 <http://www.dailyom.com>
1 <http://www.investors.sage.com>
1 <http://www.playscripts.com>
1 <http://www.faraday.com>
1 <http://www.vmetro.com>
1 <http://www.solsem.com>
1 <http://www.fistofblog.com>
1 <http://www.homeenvy.com>
1 <http://www.blastro.com>
1 <http://www.cartype.com>
1 <http://www.safariwest.com>
1 <http://www.bitlaw.com>
1 <http://www.classbuilder.com>
1 <http://www.projekt.com>
1 <http://www.rms.com>
1 <http://www.scourstop.com>
1 <http://www.cooperlighting.com>
1 <http://www.silkwormink.com>
1 <http://www.creative-weblogging.com>
1 <http://www.faraday.com>
1 <http://www.ozbedandbreakfast.com>
1 <http://www.almaz.com>
1 <http://www.rickbayless.com>
1 <http://www.layersmagazine.com>
1 <http://www.insound.com>
1 <http://www.opticsplanet.com>
2 <http://www.grindtv.com>
2 <http://www.aceticket.com>
1 <http://www.electronicbookreview.com>
1 <http://www.insound.com>
2 <http://www.oracle.com>
1 <http://www.electronicbookreview.com>
1 <http://www.pointstreak.com>
1 <http://www.france.com>
1 <http://www.darla.com>
2 <http://www.ratebeer.com>
1 <http://www.pba.com>
1 <http://www.tennisweek.com>

Domain Name: CONESFREE.COM

Registrant:

house

villi vilson (villisupport@gmail.com)

pokilas st 45

nikosat

aurot,11212

AM

Tel. +671.8928262123

Creation Date: 29-May-2008

Expiration Date: 29-May-2009

The raw links ****WARNING**** EXPLICIT CONTENT

<http://www.modthesims2.com/download.php> ... br%3E&f=38
<http://www.anagramgenius.com/agasearch>. ... 3E%3Cbr%3E
<http://www.anagramgenius.com/agasearch>. ... 3E%3Cbr%3E
<http://www.movieweb.com/search/?search=> ... 3E%3Cbr%3E
<http://www.marketingvox.com/subscriptio> ... TopSubform
<http://www.qwikcast.com/cgi-bin/forecas> ... 3E%3Cbr%3E
<http://www.isound.com/find.php?fi=%3Ch1> ... 3E%3Cbr%3E
<http://www.reedfirstsource.com/members/> ... 3E%3Cbr%3E
<http://www.filter-mag.com/index.php?sea> ... Cbr%3E&c=s
<http://www.onsemi.com/PowerSolutions/se> ... rFilters=Y
<http://www.garnethill.com/mercadoSearch> ... earch=true
<http://www.marthastewart.com/portal/sit> ... earch_home
<http://www.filter-mag.com/index.php?sea> ... Cbr%3E&c=s
<http://www.atlantafalcons.com/Search/Si> ... 3E%3Cbr%3E
<http://www.solvaychemicals.com/search/0> ... nguage=EN
<http://www.solvay-fluor.com/search/0,0>, ... nguage=EN
http://www.usg.com/USGSearch/search_res ... sPerPage=5
<http://www.nashbar.com/results.cfm?sear> ... 3E%3Cbr%3E
<http://www.guiasenor.com/cgi-bin/searc> ... 3E%3Cbr%3E
<http://www.drawerb.com/?s=%3Ch1%3Ebaren> ... 3E%3Cbr%3E
<http://www.ebags.com/search/index.cfm?N> ... decasearch
<http://www.marthastewart.com/portal/sit> ... chtype=web
<http://www.atlantafalcons.com/Search/Si> ... 3E%3Cbr%3E
<http://www.thesmedleylog.com/?s=%3Ch1%3> ... 3E%3Cbr%3E
http://cleaning101.com/search/search_fo ... ton=Search
<http://www.cartoondollememporium.com/doll> ... 3E%3Cbr%3E
http://www.euclidchemical.com/atomz_sea ... m=1&sp-s=0
<http://www.bitlaw.com/cgi-bin/search.cg> ... 3E%3Cbr%3E
<http://www.cartype.com/search.cfm?keywo> ... 3E%3Cbr%3E
http://www.dclab.com/searchresults_new. ... 3E%3Cbr%3E
<http://www.guiasenor.com/cgi-bin/searc> ... 3E%3Cbr%3E
<http://www.almaz.com/nobel/cgi-bin/sear> ... 3E%3Cbr%3E
<http://www.verdictoncars.com/jsp/vocmai> ... 3E&lnk=010
<http://www.drawerb.com/?s=%3Ch1%3Esmall> ... 3E%3Cbr%3E
<http://www.safariwest.com/?q=%3Ch1%3Ena> ... omp=search

http://www.dinewise.com/search.php?sear ... 3E%3Cbr%3E
http://www.ebags.com/search/index.cfm?N ... decasearch
http://www.visitpensacola.com/mainsearc ... 3E%3Cbr%3E
http://www.shelldorado.com/cgi-bin/subs ... helldorado
http://www.solsem.com/interest.asp?emai ... s-interest
http://www.macminute.com/search.php?key ... 3E%3Cbr%3E
http://www.eyeonbooks.com/search.php?q= ... 3E%3Cbr%3E
http://www.pain.com/sections/pain_resou ... 3E%3Cbr%3E
http://www.iweiss.com/search.src?Key=%3 ... 3E%3Cbr%3E
http://www.linuxmanpages.com/search.php ... ubmitted=1
http://www.download3k.com/googlesearch. ... FORID%3A11
http://www.blastro.com/search.html?sear ... 3E%3Cbr%3E
http://cleaning101.com/search/search_fo ... ton=Search
http://www.thesmedleylog.com/?s=%3Ch1%3 ... 3E%3Cbr%3E
http://www.rickbayless.com/search/?q=%3 ... 3E%3Cbr%3E
http://www.ccamatil.com/search.asp?srch ... &pgcount=1
http://www.cortlandreview.com/subscribe ... =subscribe
http://www.windfinder.com/wind-cgi/sear ... 3E%3Cbr%3E
http://www.silkwormink.com/pages/search ... 3E%3Cbr%3E
http://www.projekt.com/projekt/find.asp ... pe=keyword
http://www.woodenshoe.com/browse.cgi?ke ... rchresults
http://www.scientificindustries.com/cgi ... &action=sw
http://www.pridetoronto.com/search.php? ... 3E%3Cbr%3E
http://www.cortina-systems.com/products ... 3E%3Cbr%3E
http://www.unreliablewitness.com/?s=%3C ... fa1fc255a4
http://www.cottoninc.com/PowerSearch/?q ... 3E%3Cbr%3E
http://www.ezinedirector.com/subscriber ... =956605042
http://www.classbuilder.com/cgi-bin/sig ... 3E%3Cbr%3E
http://www.radiantsystems.com/search/se ... e=allwords
http://www.rms.com/SiteSearchResult.asp ... 3E%3Cbr%3E
http://www.scourstop.com/search.asp?pag ... 3E%3Cbr%3E
http://www.cooperlighting.com/search/se ... 3E%3Cbr%3E
http://www.creative-weblogging.com/cgi- ... wsletter=1
http://www.jackstackbbq.com/search.asp? ... 3E%3Cbr%3E
http://www.dailyom.com/cgi-bin/search/s ... 3E%3Cbr%3E
http://www.investors.sage.com/search/?q ... 3E%3Cbr%3E
http://www.playscripts.com/mainsearchre ... isfilled=1
http://www.faraday.com/cgi-bin/search.p ... boolean=OR
http://www.vmetro.com/category361.html? ... 3E%3Cbr%3E
http://www.solsem.com/interest.asp?emai ... s-interest
http://www.fistofblog.com/index.php?s=% ... 3E%3Cbr%3E
http://www.homeenvy.com/cgi-bin/home/in ... &what=list
http://www.blastro.com/search.html?sear ... 3E%3Cbr%3E
http://www.cartype.com/search.cfm?keywo ... 3E%3Cbr%3E
http://www.safariwest.com/?q=%3Ch1%3Ehe ... omp=search
http://www.bitlaw.com/cgi-bin/search.cg ... 3E%3Cbr%3E
http://www.classbuilder.com/cgi-bin/sig ... 3E%3Cbr%3E
http://www.projekt.com/projekt/find.asp ... pe=keyword
http://www.rms.com/SiteSearchResult.asp ... 3E%3Cbr%3E
http://www.scourstop.com/search.asp?pag ... 3E%3Cbr%3E
http://www.cooperlighting.com/search/se ... 3E%3Cbr%3E
http://www.silkwormink.com/pages/search ... 3E%3Cbr%3E
http://www.creative-weblogging.com/cgi- ... wsletter=1
http://www.faraday.com/cgi-bin/search.p ... boolean=OR
http://www.ozbedandbreakfast.com/result ... 3E%3Cbr%3E

http://www.almaz.com/nobel/cgi-bin/sear ... 3E%3Cbr%3E
http://www.rickbayless.com/search/?q=%3 ... 3E%3Cbr%3E
http://www.layersmagazine.com/?keyword= ... age=search
http://www.insound.com/search/searchmai ... 3E%3Cbr%3E
http://www.opticsplanet.com/s/search.ph ... 3E%3Cbr%3E
http://www.grindtv.com/search/?term=%3C ... orm=videos
http://www.grindtv.com/search/?term=%3C ... orm=videos
http://www.aceticket.com/search.php?hea ... 3E&stage=1
http://www.aceticket.com/search.php?hea ... 3E&stage=1
http://www.electronicbookreview.com/act ... 3E%3Cbr%3E
http://www.insound.com/search/searchmai ... 3E%3Cbr%3E
http://www.oracle.com/pls/db102/print_h ... 3E%3Cbr%3E
http://www.oracle.com/pls/db102/print_h ... 3E%3Cbr%3E
http://www.electronicbookreview.com/act ... 3E%3Cbr%3E
http://www.pointstreak.com/search/index ... ort=hockey
http://www.france.com/search/results.cf ... ype=Hotels
http://www.darla.com/catalog/search.asp ... ion=Search
http://www.ratebeer.com/findbeer.asp?Be ... 3E%3Cbr%3E
http://www.ratebeer.com/findbeer.asp?Be ... 3E%3Cbr%3E
http://www.pba.com/news/feature.asp?sea ... 3E%3Cbr%3E
http://www.tennisweek.com/search/query. ... siteid=696

DISCLAIMER

The content in this file, including domain names, trademarks, monetization partners, and other information, is provided by stopthehacker.com and Jaal LLC and its third party content providers for your personal information only, and is not intended to be relied upon for any action or decision. This information is gathered through automated means and is subject to change. Content in this file is not appropriate for the purposes of making a determination to pursue legal claims regarding a particular domain or making any determination on whether a particular domain is confusingly similar to a registered trademark. Nor does Jaal LLC provide any form of advice amounting to legal advice, or make any recommendations regarding particular domains and whether they may violate any rule or regulation. Such a determination is complex and should be made with the advice of competent legal counsel.

Neither Jaal LLC nor its third party content providers shall be liable for any errors, inaccuracies or delays in content, or for any actions taken in reliance thereon.

JAAL LLC EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, AS TO THE ACCURACY OF ANY THE CONTENT PROVIDED, OR AS TO THE FITNESS OF THE INFORMATION FOR ANY PURPOSE.