By: webDEViL
Email: w3bd3vil [at] gmail [dot] com
Written: 20th Oct, 2008
Discovered: Somwhere in March, 2008

Internet Banking Flaws in India

This paper talks about the primitve POST manipulation vulnerabilities that still exist in the Indian Banking Sector. I will be highlighting on how this becomes an issue and is a serious problem to online stores. This vulnerability has a huge effect, all related to Indian Banks. This could be applicable to banks elsewhere if a similar banking system is used.

```
POST /index.asp HTTP/1.1
Host: 192.168.9.231
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9) Gecko/2008061015 Firefox/3.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://192.168.9.231/
Cookie: ASPSESSIONIDCARADCQD=NBAFPHOAIECLLFGDIDNIGJFI
Content-Type: application/x-www-form-urlencoded
Content-Length: 43

x=165&y=134&Username=test&Password=test
```

Lets start off with the an example of how Internet Banking works.
You have a bank account with which you get a online id, password and a transaction password. With that you have your debit card of which certain details are required while doing a purchase online.

Suppose I browse off to xxxx.in, start shopping and search for and buy a candy. ;) I will skip to the part that is the most important. The payment!

While paying you have options to select from credit card, cheque etc. but what I am going to be focusing on is the “Payment through online banking” part. So, one selects the Online Banking option and is redirected to the banks site.

The interesting part is the POST data that gets passed on. The data is all the details of the purchase that you make. All in encrypted format, but instead its only encoded to base64. So we could very well manipulate the data and set the price value to like Rs 1 (US $ 0.02). Upon changing the values the bank raises no question marks and our payment gets accepted and we are redirected back to xxxx.in, our shopping site.

POST /BANKAWAY?IWQRYTASKOBJNAME=bay_mc_login&BAY_BANKID=ICI HTTP/1.1
*Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, */**
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)
Host: infinity.icicibank.co.in
Connection: Keep-Alive
Cache-Control: no-cache
Referer: http://www.esevaonline.com/epay/payICICI.jsp
Content-Length: 172

bank=ICICI&SBMTTYPE=POST&MD=P&PID=000000000xxx&PRN=xxxxxxx&ITC=xxxxxxxx&AMT=3322.00&CRN=INR&RU=http%3A%2F%2Fwww.esevaonline.com%2Fepay%2FEftPay.jsp&CG=Y&RESPONSE=AUTO&PIQ=S

The good thing here is that the site accepts our payment and says the payment has been recieved and the order is under processing. But our payment never gets accepted as the payment is actually not made and the rejection mail comes in after a few days. You are refunded the amount and you have your precious money back!

Ok, so whats new about that? Some sites offering PayPal are effected by that even now!
True, but thats not the end. There is more to it.

Now here is a different case, I got to another shopping site yyyyy.in the site doesnt have integration directly with a bank but they still offer payment through online banking, How? Easy, by being a merchant at one of the payment gateways like ccavenue.com etc. There are quite a few, I cannot remember the others. But things change here a bit.

I browse off to yyyyy.in and buy an air ticket. Jumping to the payment we have an option of Online Banking and asusual I select that. This time instead of redirecting me to the bank's site I get redirected to the payment gateway, the payment gives me a form to fill and that inturn takes me to the bank page. DOING DOING DOING!

Ok, so there is a clear cut difference on how things operate in the two cases.
1- xxxxx.in --> Bank
2 ▪ yyyyy.in --> Payment Gateway --> Bank

In our first case our payment gets rejected because there is a direct contact between the site and the bank. In case two thats not the case ;). The bank is in contact with the Payment Gateway and the Payment Gateway with the site.

Now, if I were to modify the POST (sometimes its GET also) data being sent from the shopping site yyyyy.in the result would be the same. My payment would get accepted but the transaction would be rejected after a few days. But, if I were to modify the POST details that the Payment Gateway sends

to the Bank the shopping site wouldnt know anything about it.
The direct realtion here is between
yyyyy.in <--> Payment Gateway
Payment Gateway <--> Bank
So there is no direct relation between the site and the Bank.

Now, I buy a ticket from yyyyy.in and move on to the Payment gateway and while moving on to the bank's site I change the POST data to change the price. The bank accepts it and redirects me to the payment gateway which says the payment is done. The Payment gateway then passes on this information to the site which says the payment is done and voila! My order gets accepted and I am off to Kashmir!

The only reason why this works is because of the Payment Gateway. The payment gateway acts as the MiTM ;) The POST header being passed from the Payment Gateway to the Bank is modified. The Payment Gateway just generates a transaction passed without the amount being passed through. Even if the amount is passed through, like in some sites like ebay.in you could modify the POST data from the Payment Gateway to the shopping site to reflect the exact amount. Your payment does get accepted with the yellow bar appearing below your order, but ebay(.in) probably has a manual verification in place. So, tough luck. But in general most Indian shopping sites that are accepting Online Banking through a Payment Gateway are vulnerable.

I have confirmed its existence on Spicejet.com with ICICIBank.com and using the Ccavenue.com gateway, with Sify Shopping, and a few more ;)

Final notes, a few of the Indian Banking sector seems to be using the software developed by InfoSys, so if you were to find a vulnerability in the application you will find quite a few targets. The security in our Banking sector might be good enough but there they miss out on the basics, I guess!

Another example of how things go about in the Banking Sector here is a look at Jammu and Kashmir Bank. A reverse ip check shows this

jkbank.net has the IP address: 68.178.156.75
53 found with the IP 68.178.156.75

1) (cut)
2) BURNHALLSCHOOL.COM
3) LOTUSTECHNOLOGIES.NET
4) (cut)
5) (cut)
6) (cut)
7) albasons.com
8) albasons.com
9) bioinfoku.org
10) bsnlatmchq.net
11) habibcomputers.com
12) hotelbroadway.com
13) hotellidder.com
14) hotellidder.com
15) jammuandkashmirbank.com

16) jkbank.net
17) jkccc.com
18) jkccc.com
19) jkwdc.com

A shared host with 53 ugly sites! I could easily buy an account on the shared hosting server. Well, after that there is nothing much to tell.

Another stupidty being done until recently by ICICI bank was that the content of the CAPTCHA image was being sent in the Response Header. This happened on the form where you enter your credit card details. It definitely made no sense having the CAPTCHA.
Probably some bot spoiled the fun for them and then they realised their mistake and changed the way that operates.

Anyhow, thats how things are over here. Hopefully we will develop soon enough. :)