Security Advisory

Title	SPBAS Business Automation Software
Risk	HIGH
Discovery	ph33r_ me@ph33r.co

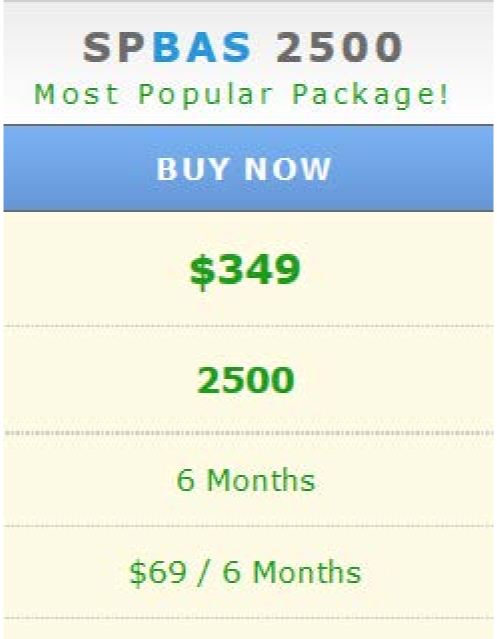
Affected Product:
SPBAS Business Automation Software 3.3

Introduction:
SPBAS is an eStore and Licensing Management System for selling and managing Script, Applications or any digital goods, SPBAS also has another futures like Knowledge Database, Please refer to vendor’s main website https://www.spbas.com

Impact:
SPBAS categorize every product as a package, and the Admin can preset Licensing system and connected to product (package), since SPBAS is Licensing Management System, advertised as Business Automation
Software, when a customer buy a product, he will get redirected to PayPal, after the payment is made, PayPal will redirect the customer back to the SPBAS store, then he will find his package ready to download with activated license, the customer can manipulate the http packets, and set any price, after paying PayPal will accept the payment because the request came from SPBAS without any interruption before PayPal handles
The request.

Technical Approach:

SPBAS doesn’t filter, or encrypt GET/POST requests, which gives the attacker the ability to change POST parameters, for example the attacker can change the price parameter, and when it send to PayPal it will be processed as valid transaction, this can be done easily by crafting HTTP request, and since everything is automated from the Seller part there is no need to human interaction till this point, now SPBAS will send the transaction to the seller to validate it, but since the attacker already marked as “paid” he will be provided with a customer portal, in order to get the download link the attacker needs to check the page source, and he will be able to find the download link.



SPBAS 2500

Most Popular Package!

$349

2500

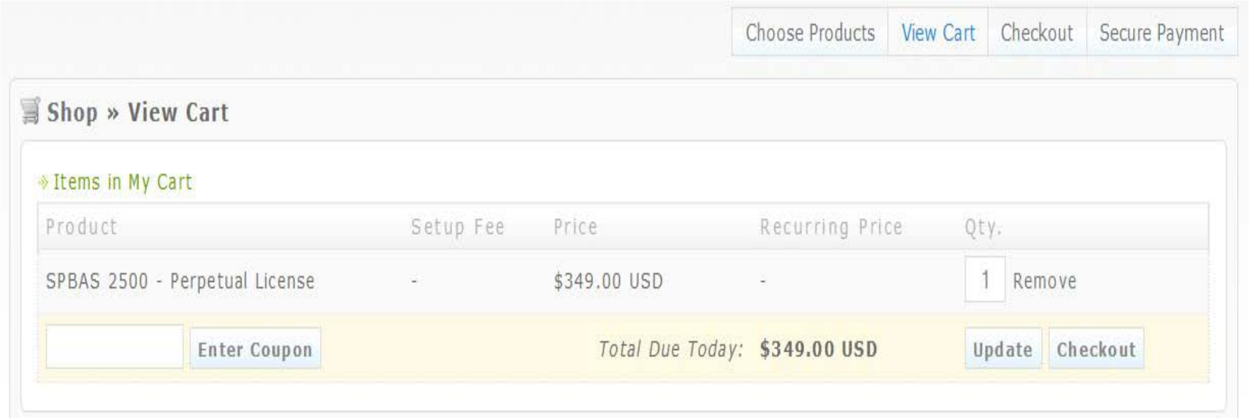
6 Months

$69 / 6 Months

SPBAS price source: (www.spbas.com)

Proof of Concept:

In this scenario we will try to craft HTTP request to change the real price and set our own.

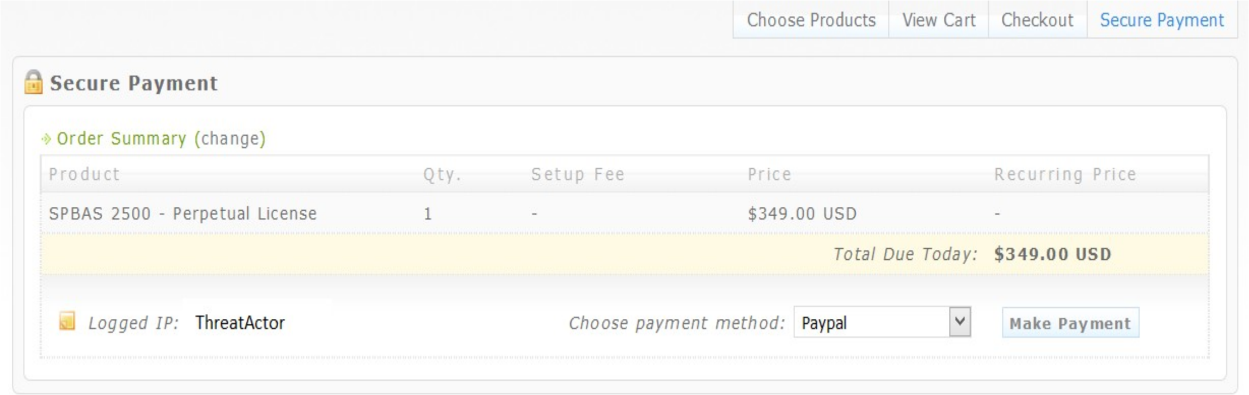


Shop » View Cart

Items in My Cart

Product	Setup Fee	Price	Recurring Price	Qty.
SPBAS 2500 - Perpetual License	-	$349.00 USD	-	1
		Total Due Today:	$349.00 USD	

This is SPBAS store, and we are buying a product cost $349, now in the next step we added the product to the Cart



Secure Payment

Order Summary (change)

Product	Qty.	Setup Fee	Price	Recurring Price
SPBAS 2500 - Perpetual License	1	-	$349.00 USD	-
			Total Due Today:	$349.00 USD

Logged IP: ThreatActor

Choose payment method: Paypal

By using PayPal as a gateway payment we will modify the HTTP request, after clicking on make Payment this the HTTP POST request will be sent to PayPal

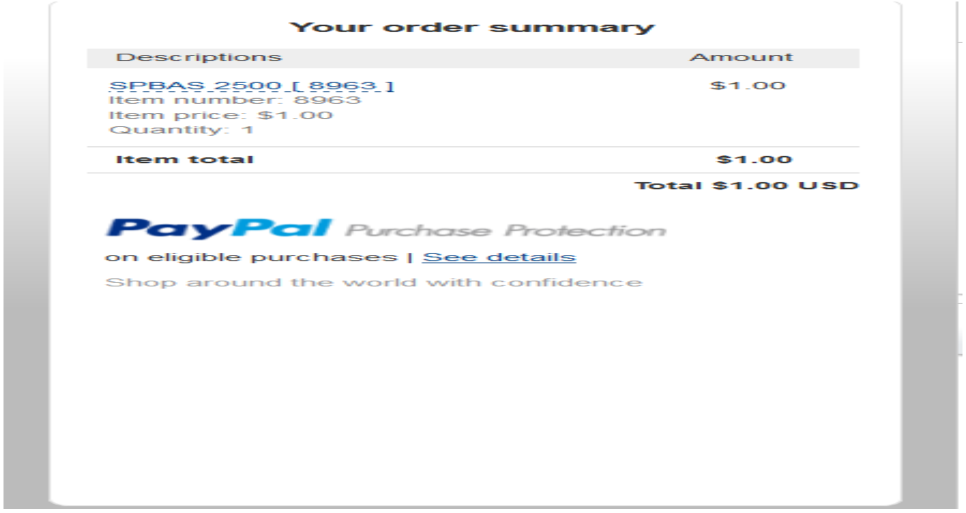
Normal payment process: User → SPBAS → PayPal → SPBAS

In our scenario it is like Man in the Middle

Attacker → SPBAS → Attacker Crafted request → PayPal → SPBAS

```
Host=www.paypa
l.com
User-Agent=Mozilla/5.0 (Windows NT 6.3; WOW64;
rv:38.0) Gecko/20100101 Firefox/38.0 this is the Post
parameters:
POSTDATA=cmd=_xclick&business=sales%40solidphp.com&item_name=SPBAS+2500+%5B+8963+%5D&ite
m_number=8963&custom=e519509
880844331c2b90b48fe665374&return=https%3A%2F%2Fwww.spbas.com%2Forders%2Findex.php%3Ftask%
3Dorder_process&notify_url=https
%3A%2F%2Fwww.spbas.com%2Forders%2Findex.php%3Ftask%3Dpayments%26gateway%3D1&cancel_retu
rn=https%3A%2F%2Fwww.spbas.
com%2Forders%2Findex.php%3Ftask%3Dpayment&amount=1.00&no_shipping=1&no_note=1&currency_code
=USD&rm=2
```

After making the payment, I changed the price from $349 to $1



Your order summary

Descriptions	Amount
SPBAS 2500 [8963] Item number: 8963 Item price: $1.00 Quantity: 1	$1.00
Item total	**$1.00**
	Total $1.00 USD

PayPal Purchase Protection
on eligible purchases | See details
Shop around the world with confidence

Tools used in this scenario:

1- Burp Proxy
2- Tamper Data
3- FireBug (for inspecting and find download links)

Date Disclosure:

- 5/25/2015 Vulnerability Discovery
- 5/27/2015 Advisory sent to US-CERT
- 5/27/2015 vendor been notified
- 7/15/2015 Vulnerability Disclosure

To this time the vendor didn’t release any updates

Discovery and Advisory:
Ph33r
me@Ph33r.co