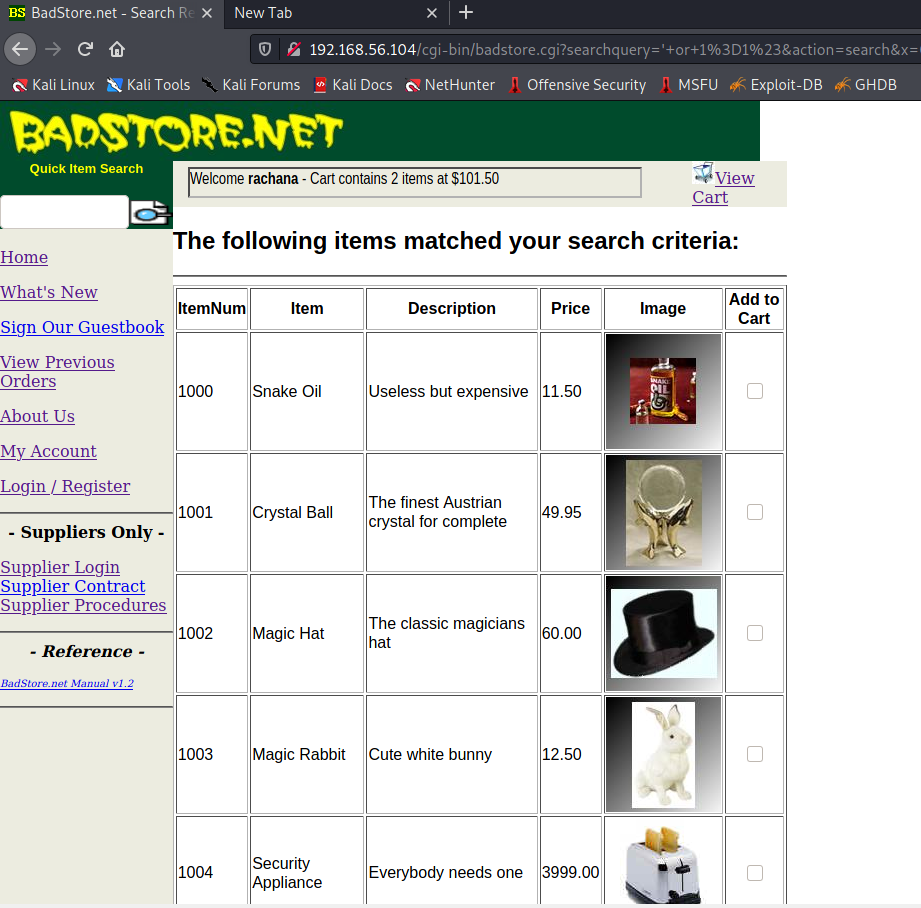
**BAD STORE report**

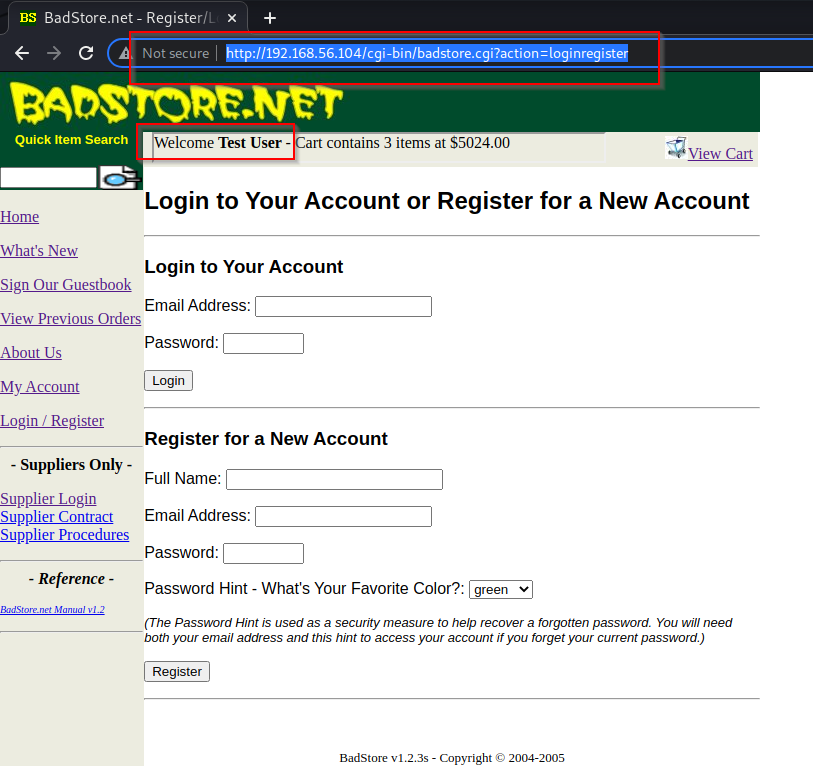
Bad store is a machine where you can shop products. Here we have found some of the vulerabilites.

* Successfully registered and logged in as a rachana.
* Now I can see products which are avilable and purches them.

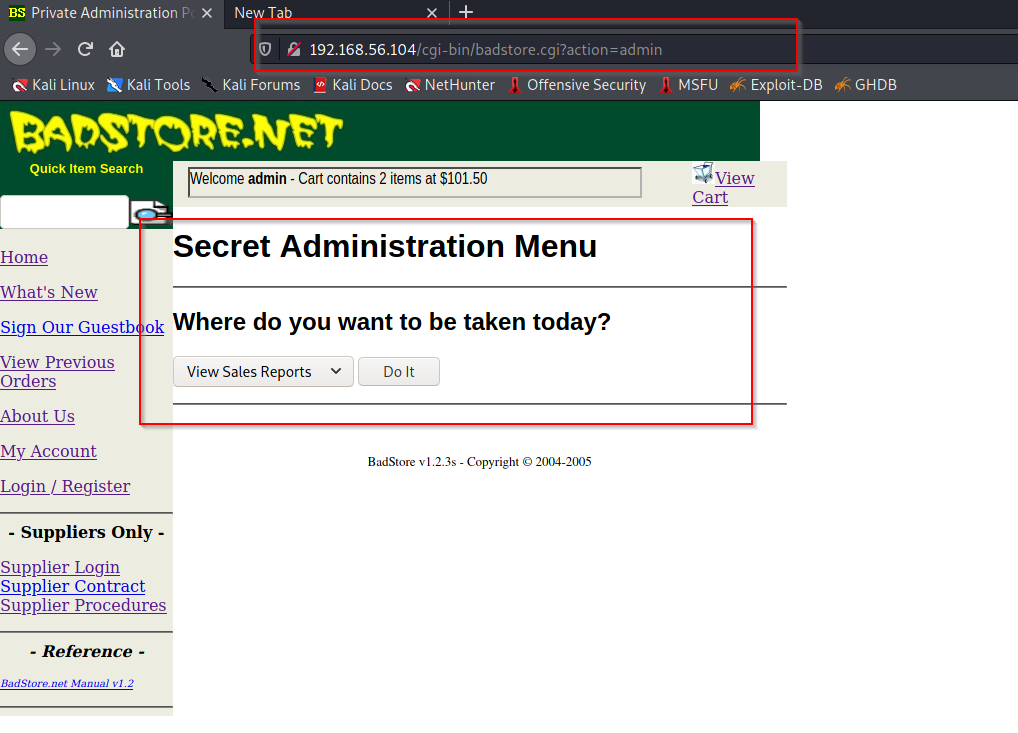


Let’s try logging in as an admin.

* URL path traversal- <http://192.168.56.104/cgi-bin/badstore.cgi?action=loginregister>

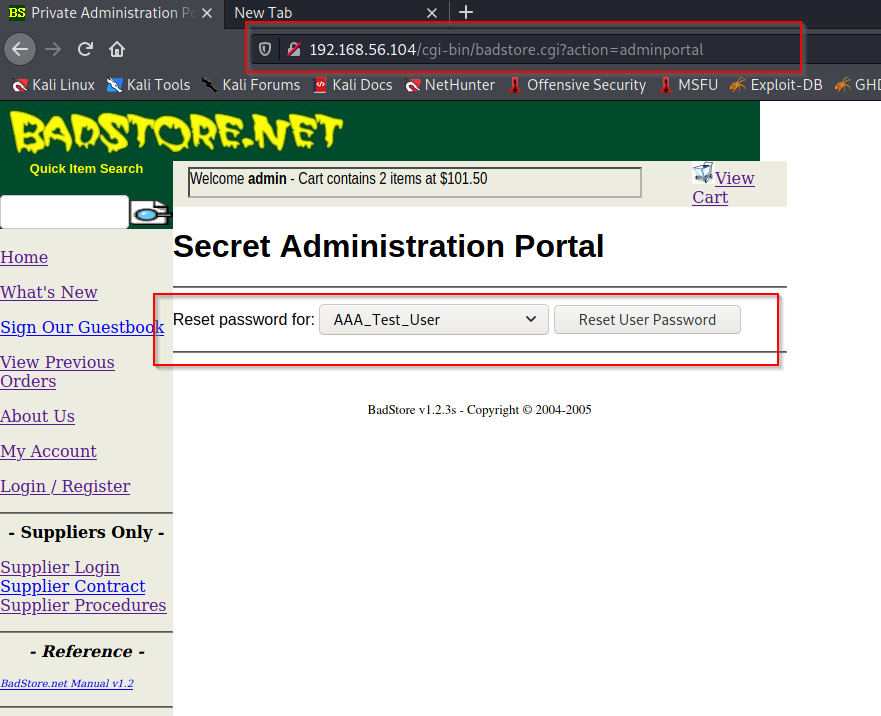


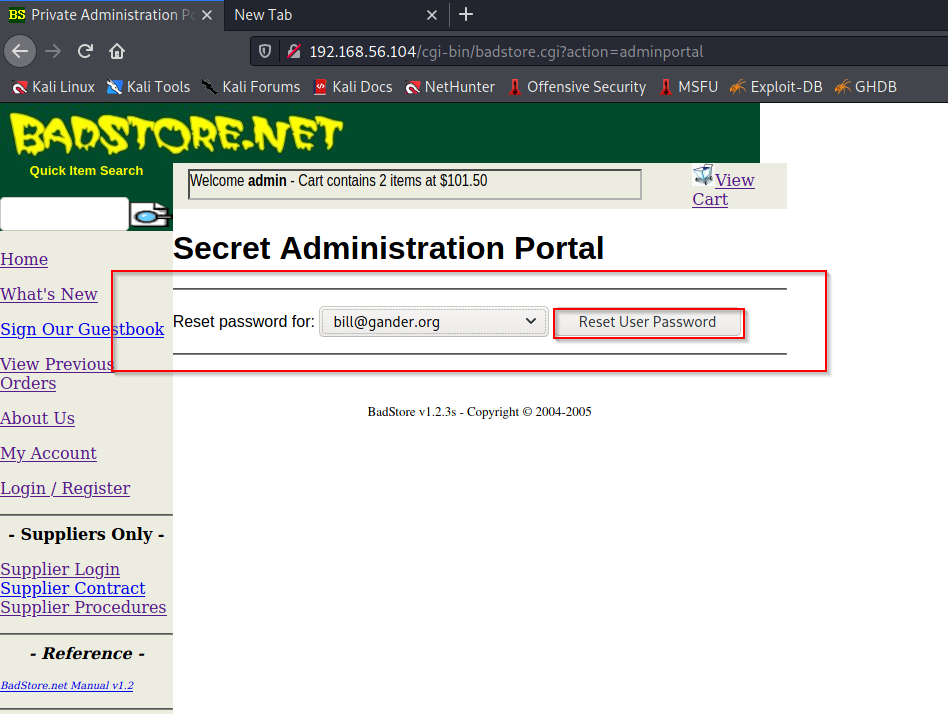
* <http://192.168.56.104/cgi-bin/badstore.cgi?action=admin>
* Successfully got an admin access. Here I can edit any user details I want.
* I can view sales report also I ca change password for particular user.

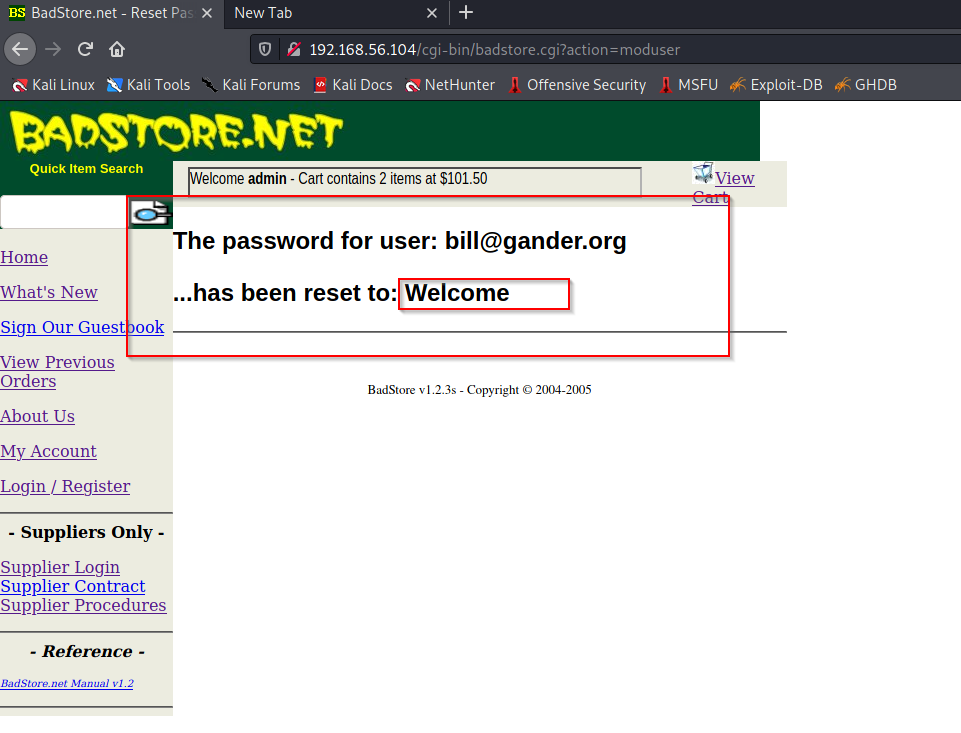


* Reset password for user.

Click on reset user password.

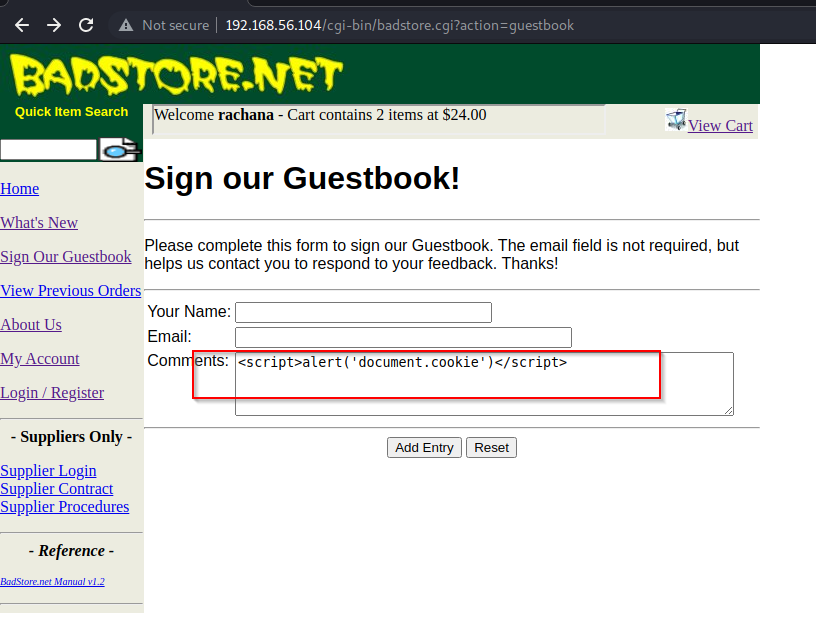


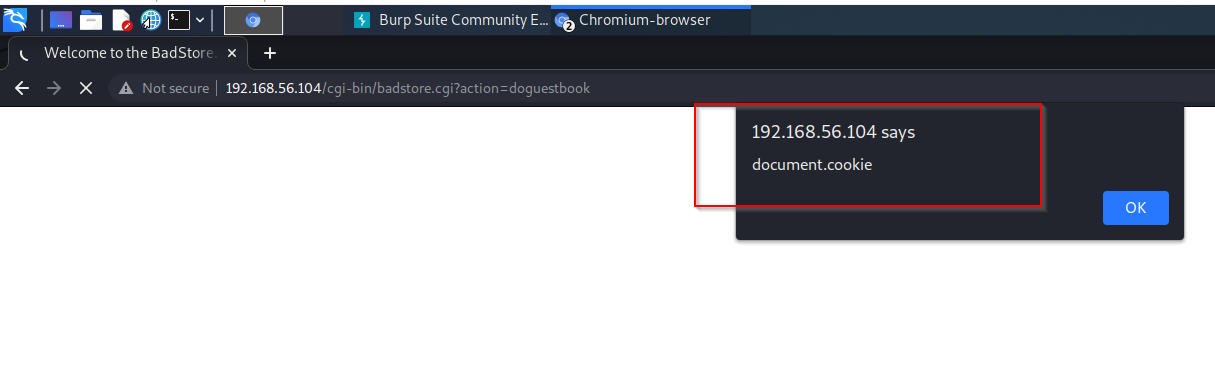




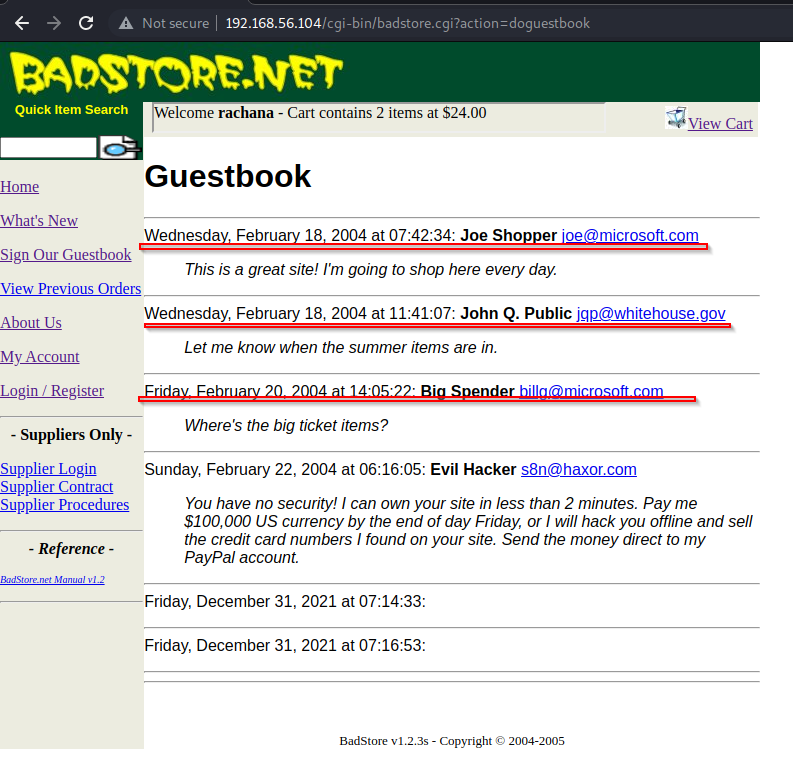
Here password is reset to **“Welcome”** for bill.

* XSS- cross side scripting. (On the user side).
* Script added- <script>alert(‘document.cookie’)</script> .

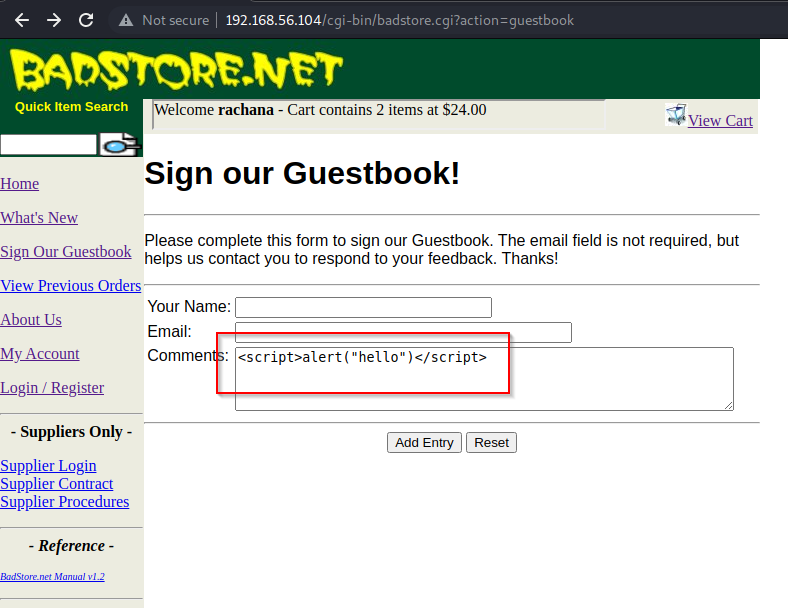


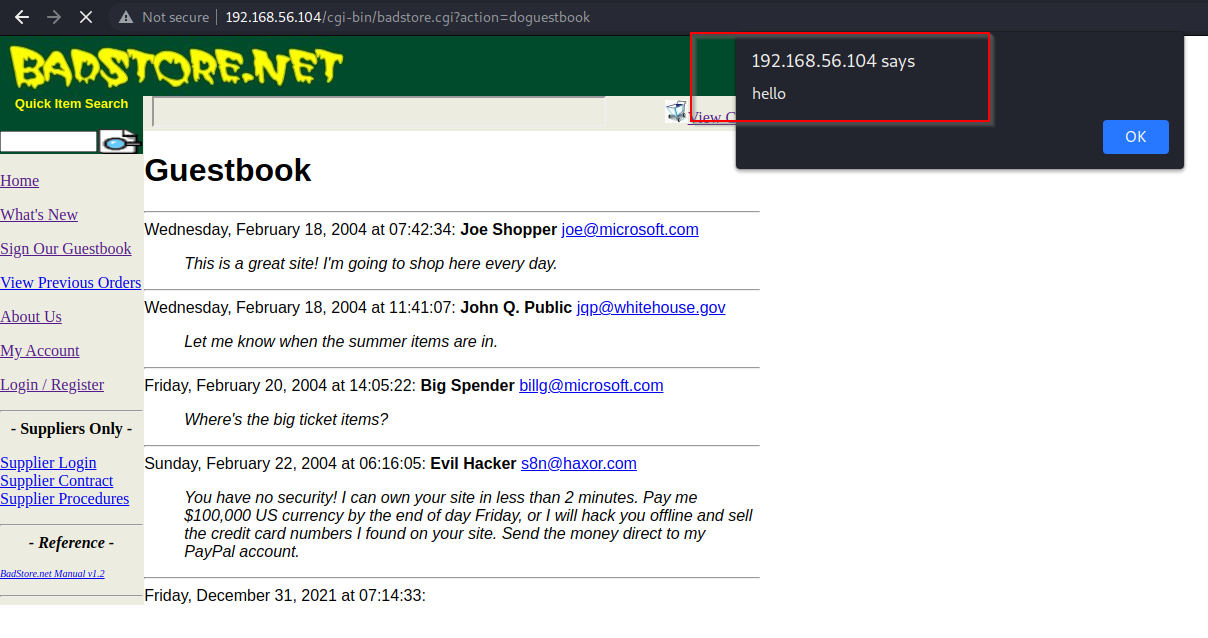


* After clicking on ok we get this guestbook.

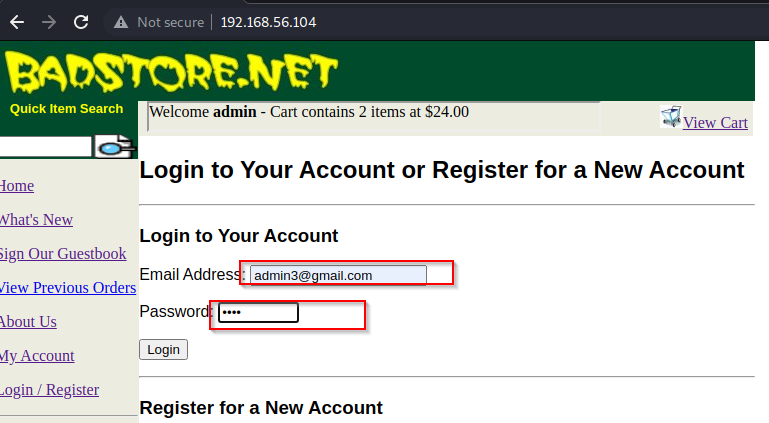


* Script added- <script>alert(‘hello’)</script>.



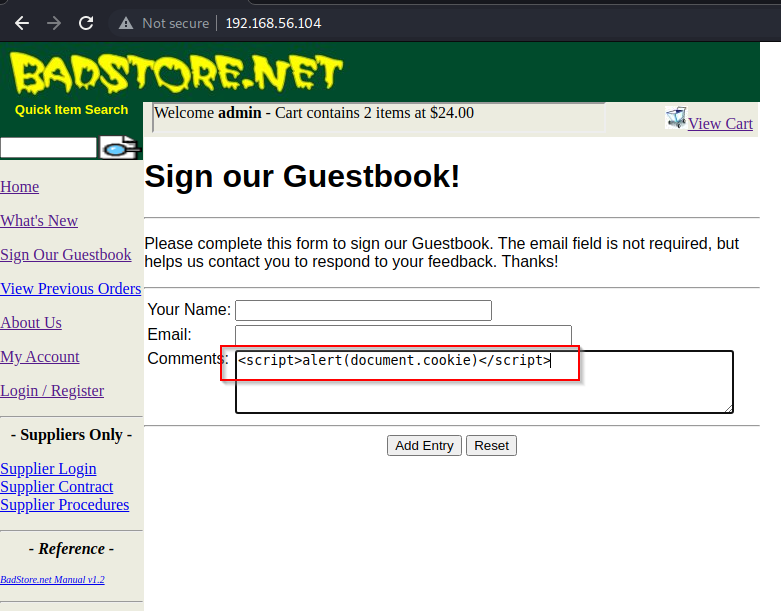


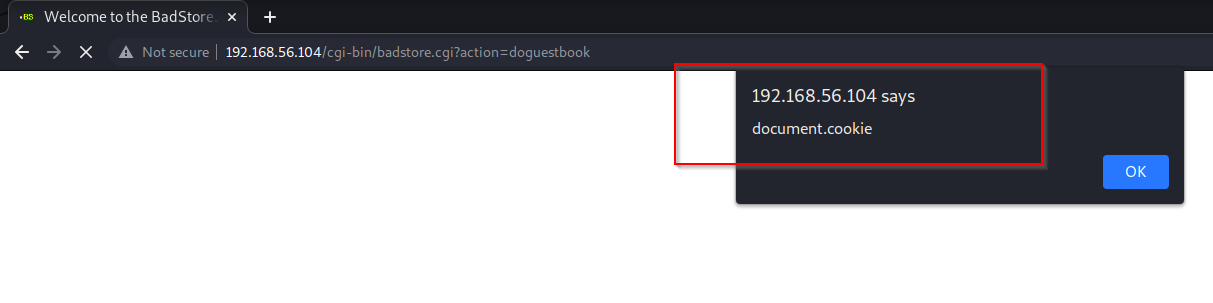
* **XSS- cross side scripting (with admin access)**
* Let’s try logging in with admin access.



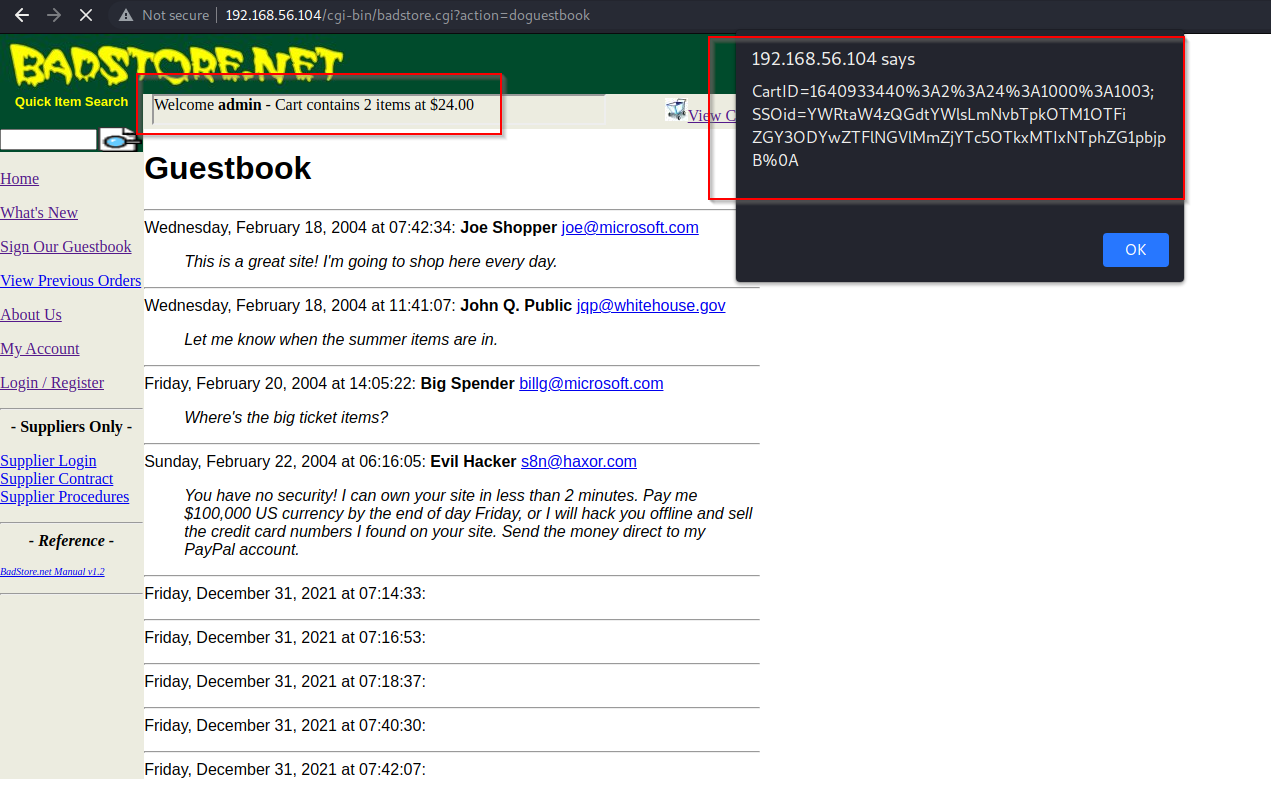
Here I’ve logged in as an admin.

* Script added - Script added- <script>alert(‘document.cookie’)</script> .

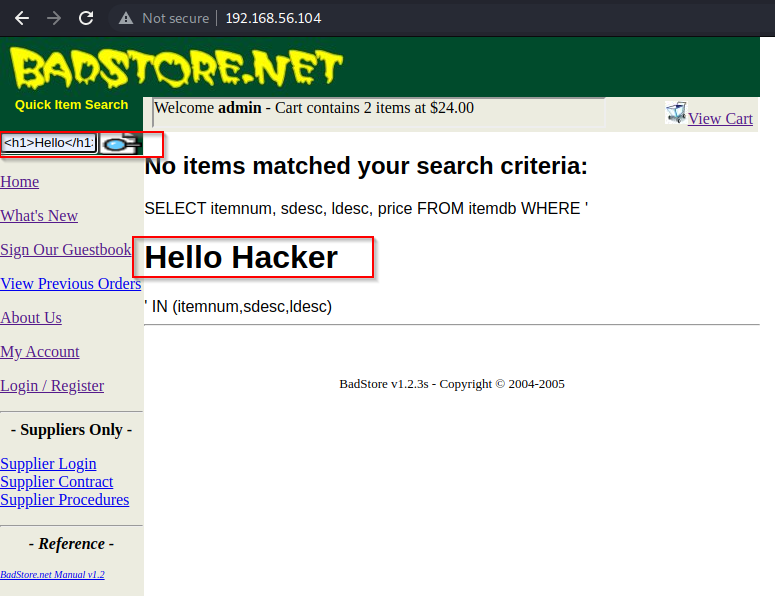




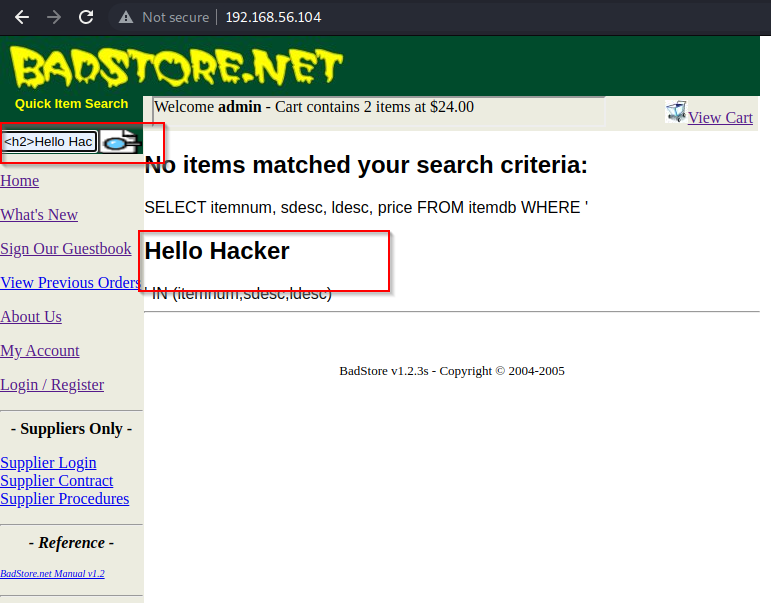
* Successfully got the cookie information.



* **HTML injection**
* Code injected- <h1>Hello Hacker</h1>



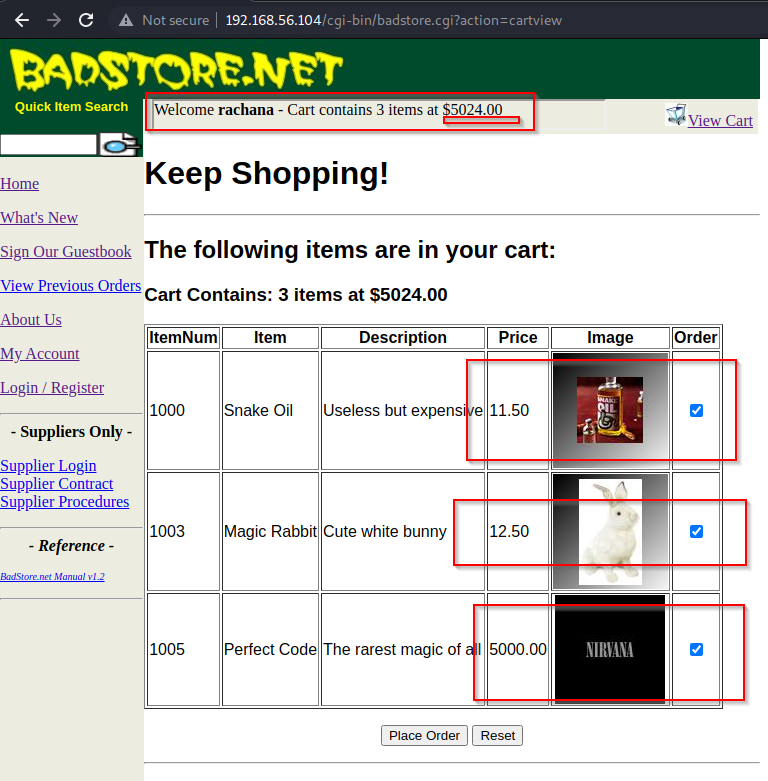
* Code injected- <h2>Hello Hacker</h2>



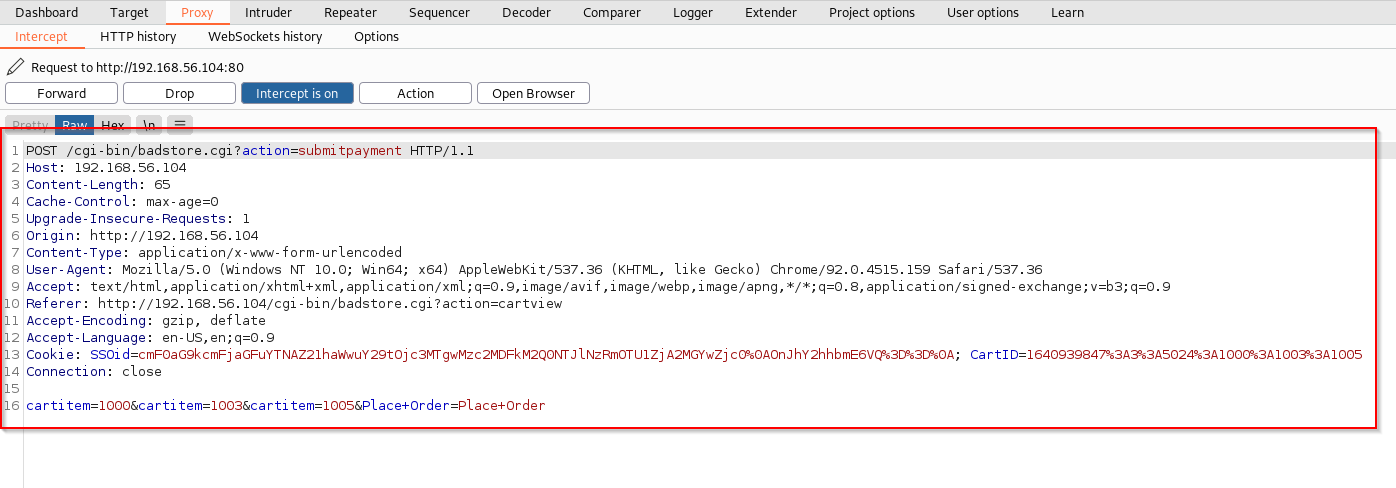
* **IDOR –**

I’ve added few products in the cart which will cost me 5024.00 $.

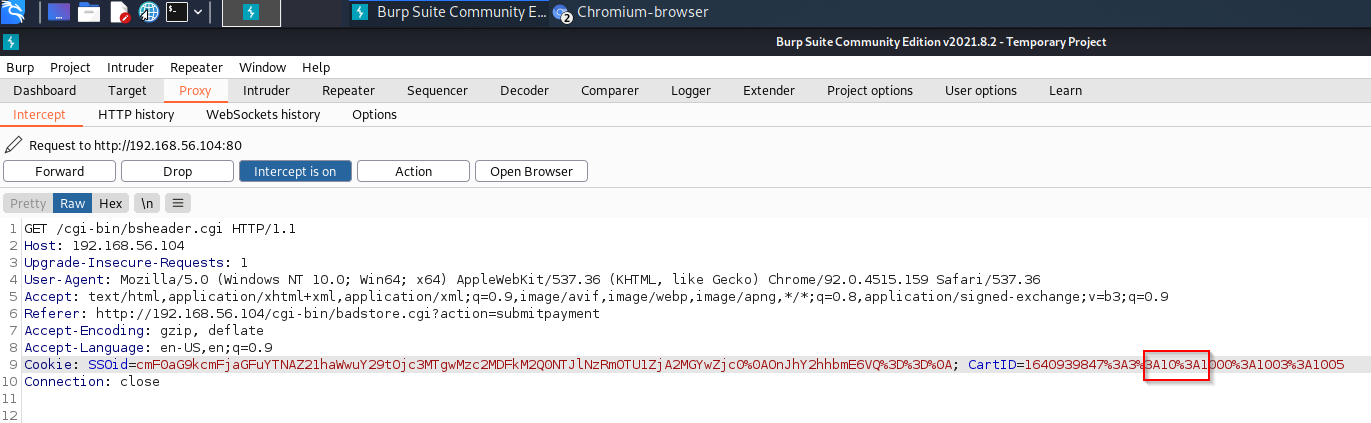
* Click on place order.



* Let’s catch the request using burpsuite.

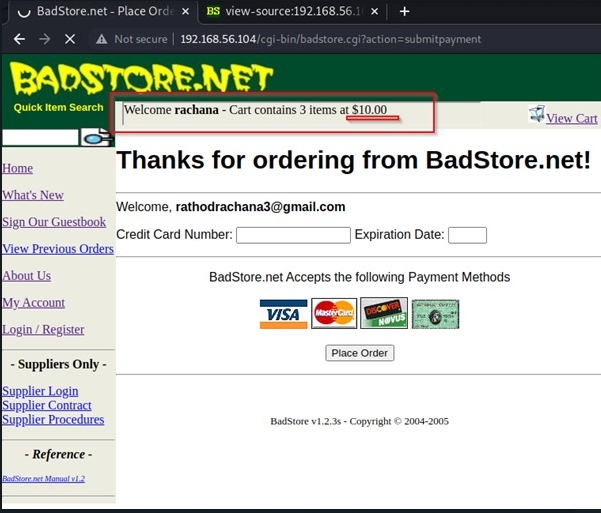


* We’ve caught the request. Edit the changes and forward the request.

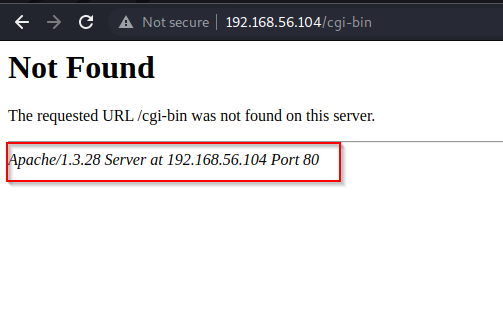


* Their product was for $5024 for 3 items.

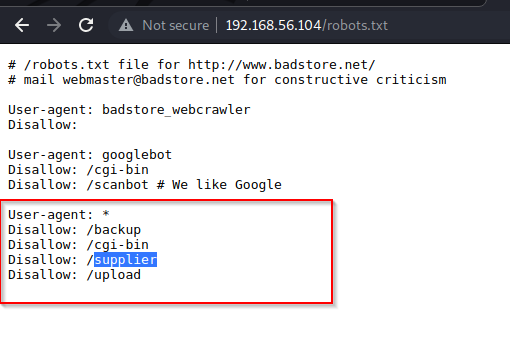
Now we can buy 3 products for $ 10.00.



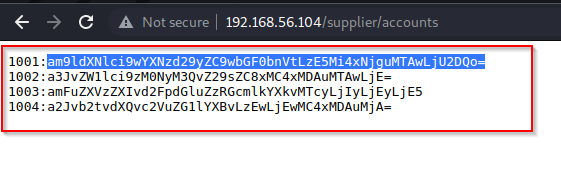
* **Banner grabbing**



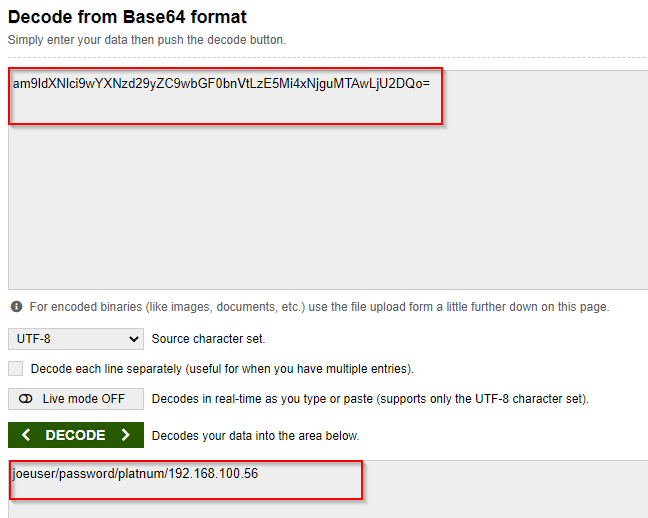
* **Robots.txt .**
* We have found few directories inside robots.txt.



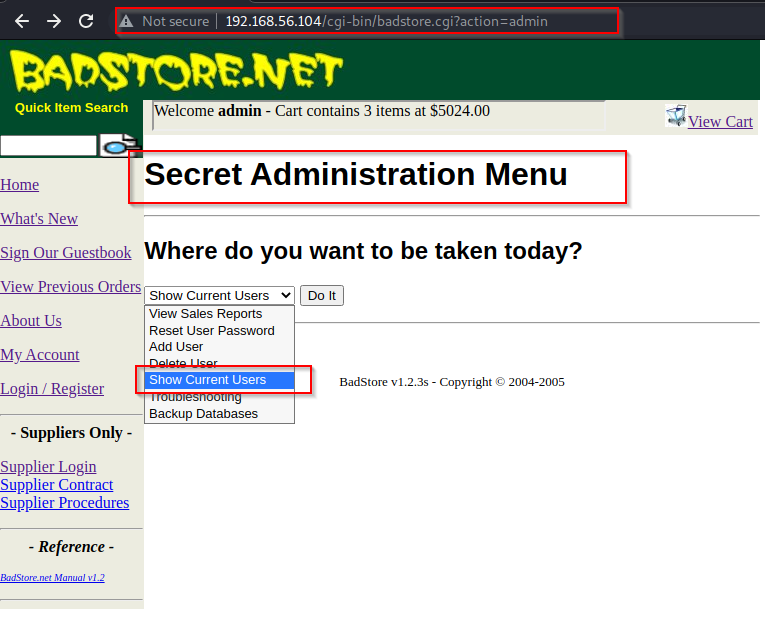
* We tried opening all of them from which we found username passwords under supplier.
* Base 64 code are found under supplier directory.

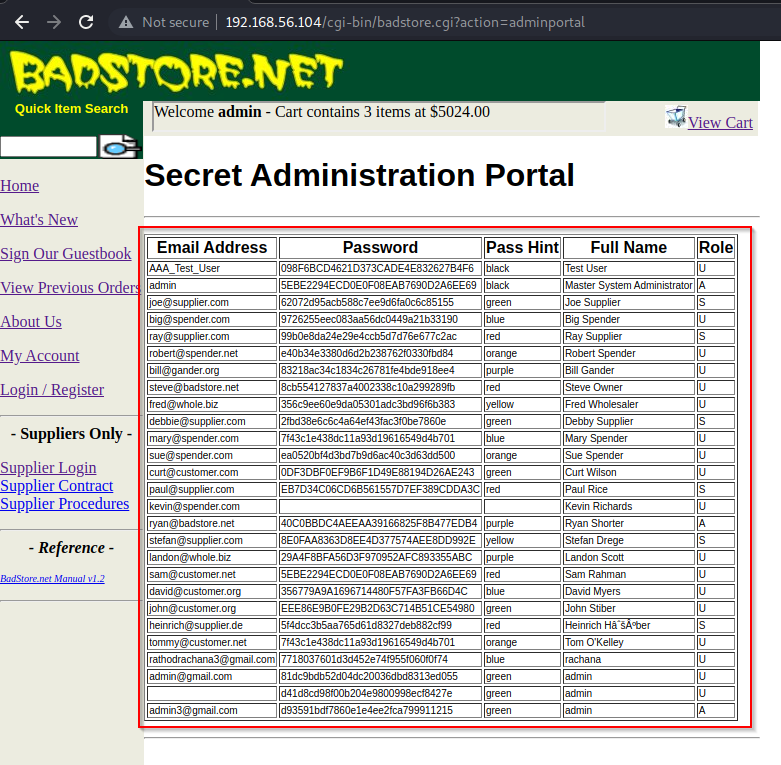


Let’s decode them and see what we found.



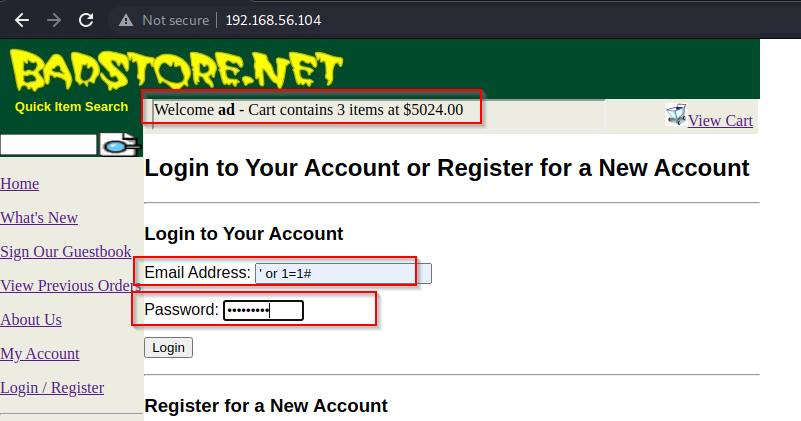
* **Admin control.**
* I’ve logged in as an administrator. Here I can see current users and their passwords.





Here we’ve found users and passwords.

* **SQL injection to get user access**
* Here I’m user named “ad”.
* Code injected-**‘ or 1=1#** (in both fields username and password)



* Got the login access as a user named **“Test User”.**

