Erich Viebrock

ECPE 178

Lab #8: Security Testing

1. **Inet addr:**

   10.0.2.15

2. **Directory name:**

   /badstore/

3. **File name:**

   Badstore_net_v1_2_Manual.pdf

4. **Briefly explain what information one might obtain by crawling a web site**

   One will obtain any files hosted by a web site. This should be used for both black hats and white hats, as one could look for confidential files, or malware.

5. **What is the potential risk for a web site being crawled?**

   Any confidential documents or files that should not be visible to the user are now visible.

6. **List two vulnerabilities from the report and explain the countermeasures to fix them.**

   Vulnerability 1: SQL Injection

   Countermeasure 1: Prevent using operators in search queries, and any other security tactics to prevent users from returning more hits than they should.

   Vulnerability 2: Cross Site Scripting

   Countermeasure 2: Prevent users from entering a client-side script into a web page.

7. **What do you think happens when you append admin to action=?**

   You'll gain admin access.

8. **What is the result of this URL?**

   I gained admin access.

9. **List 3 actions that administrators can take.**

   a. View Sales Reports

   b. Reset User Password

   c. Add User

10. **Select an action and click Do It. What happens?**

    I was notified I (Unregister User) am not an Admin.

11. **Write down your registration information below for reference.**

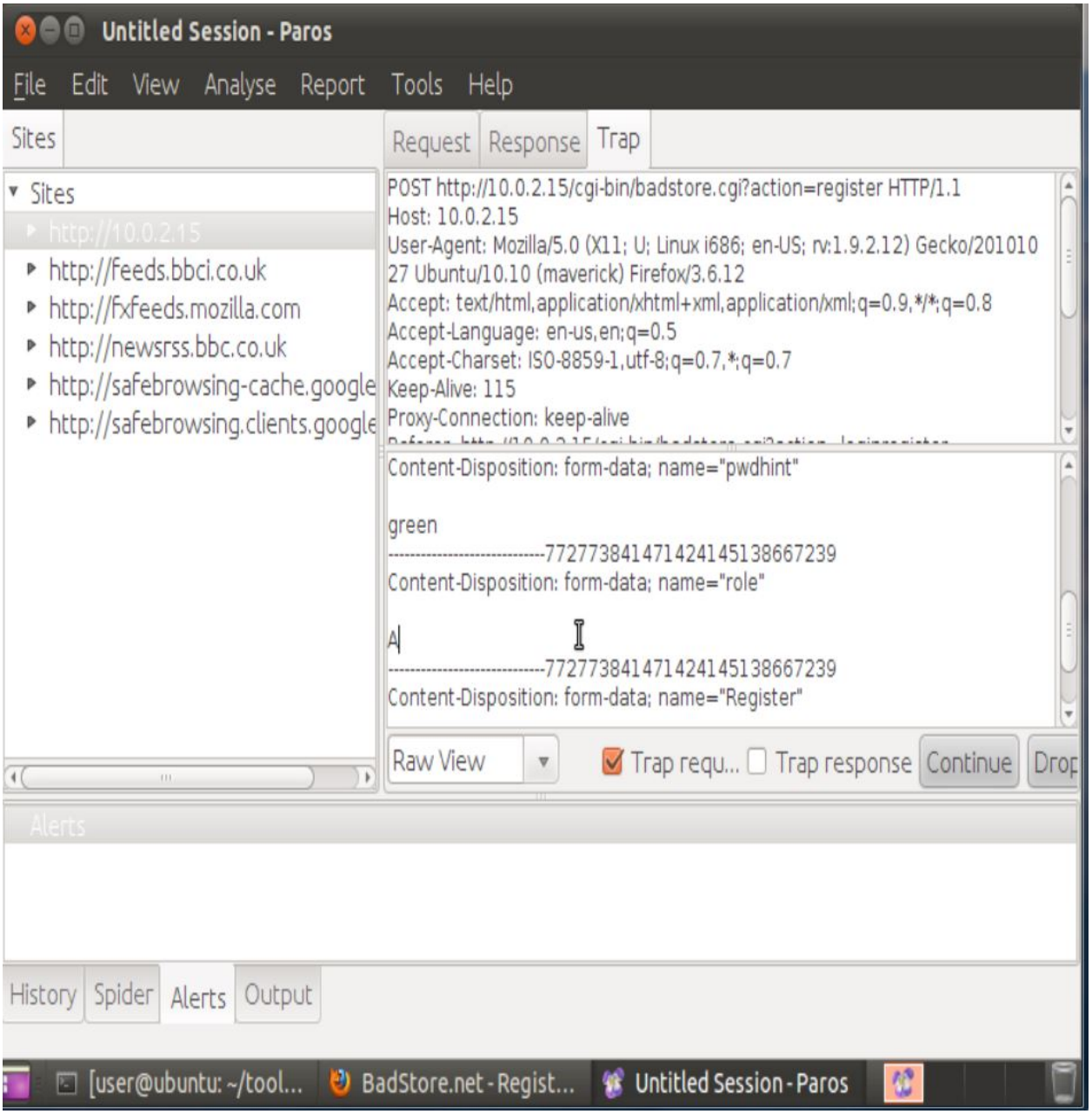
    Full Name: blah blah

    Email Address: blah@gmail.com

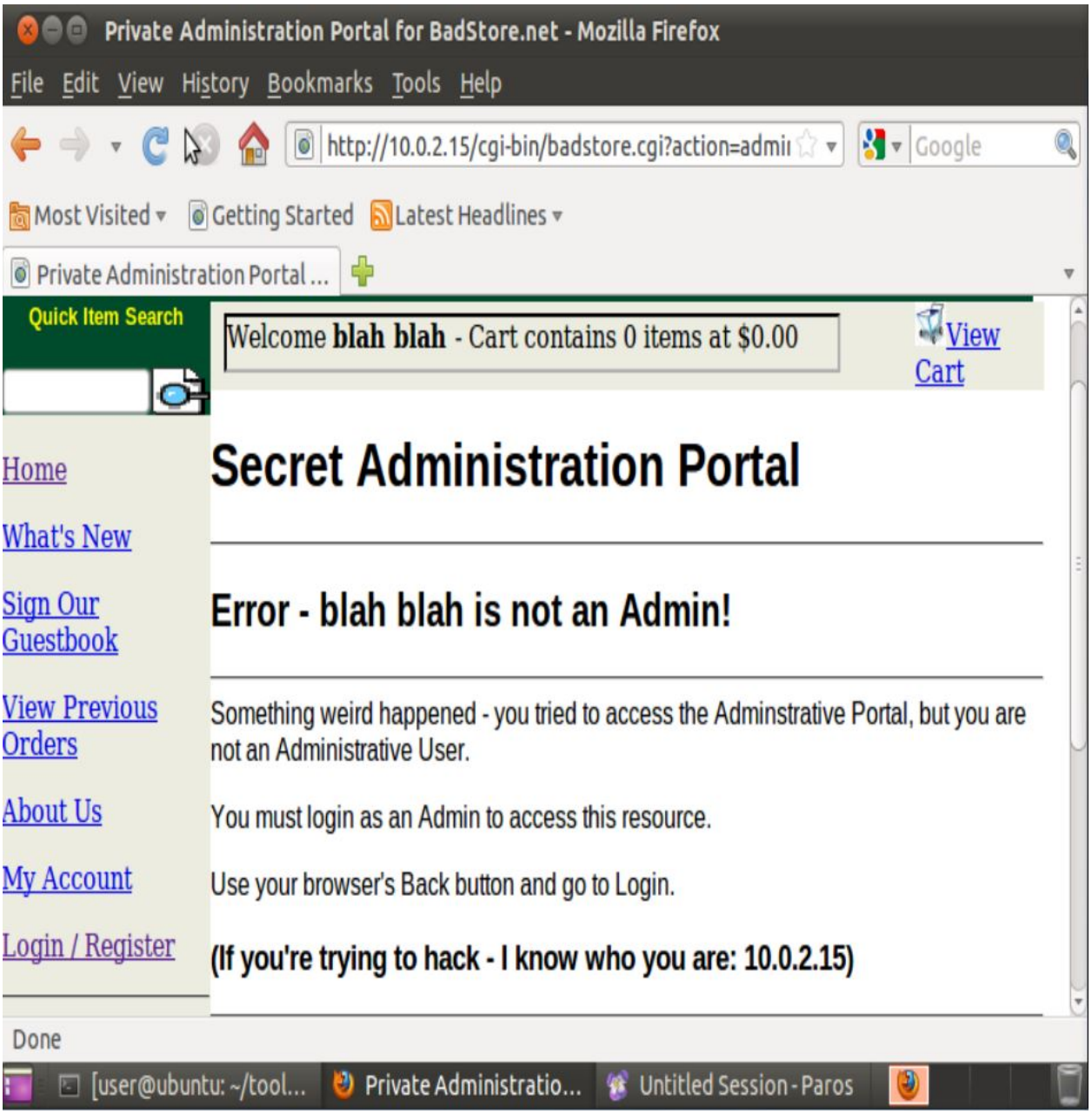
    Password: blah

12. List the password hash of the administrator.

Even though I changed the HTTP request from “U” to “A” in the proxy server, I was not granted admin access.



13. Paste a screenshot of your results.



14. Password Hash:

Can’t answer, because I was not granted admin access.

15. What is the password?

Can’t answer, because I was not granted admin access.

16. **Explain briefly how the MD5 cracker works in order to crack the above password.**

    The password is encoded in an MD5 hash. By decoding from the MD5 hash, we are able to discover what the password is and can use this password for login.

17. **Explain briefly the vulnerability of the web server which you have just exploited in this exercise.**

    We were able to compromise any account, including the master administrator. Essentially doesn't get any more exploitable from this.

18. **Explain briefly how you exploit the vulnerability in this exercise.**

    By changing an HTTP request, we were able to create an account with admin control. By decoding MD5 hash passwords, we then had any account's password, including the master administrator. From then, we had master admin control.

19. **Describe a method to exploit Badstore.net using SQL injection or XSS vulnerability.**

    By entering a search in the query like "Smith' OR '1'='1" could potentially return all information in the database, rather than information just about "Smith".

20. **Describe a method to fix the SQL injection or XSS vulnerability you identified above.**

    Do not allow users to use operators in search queries.