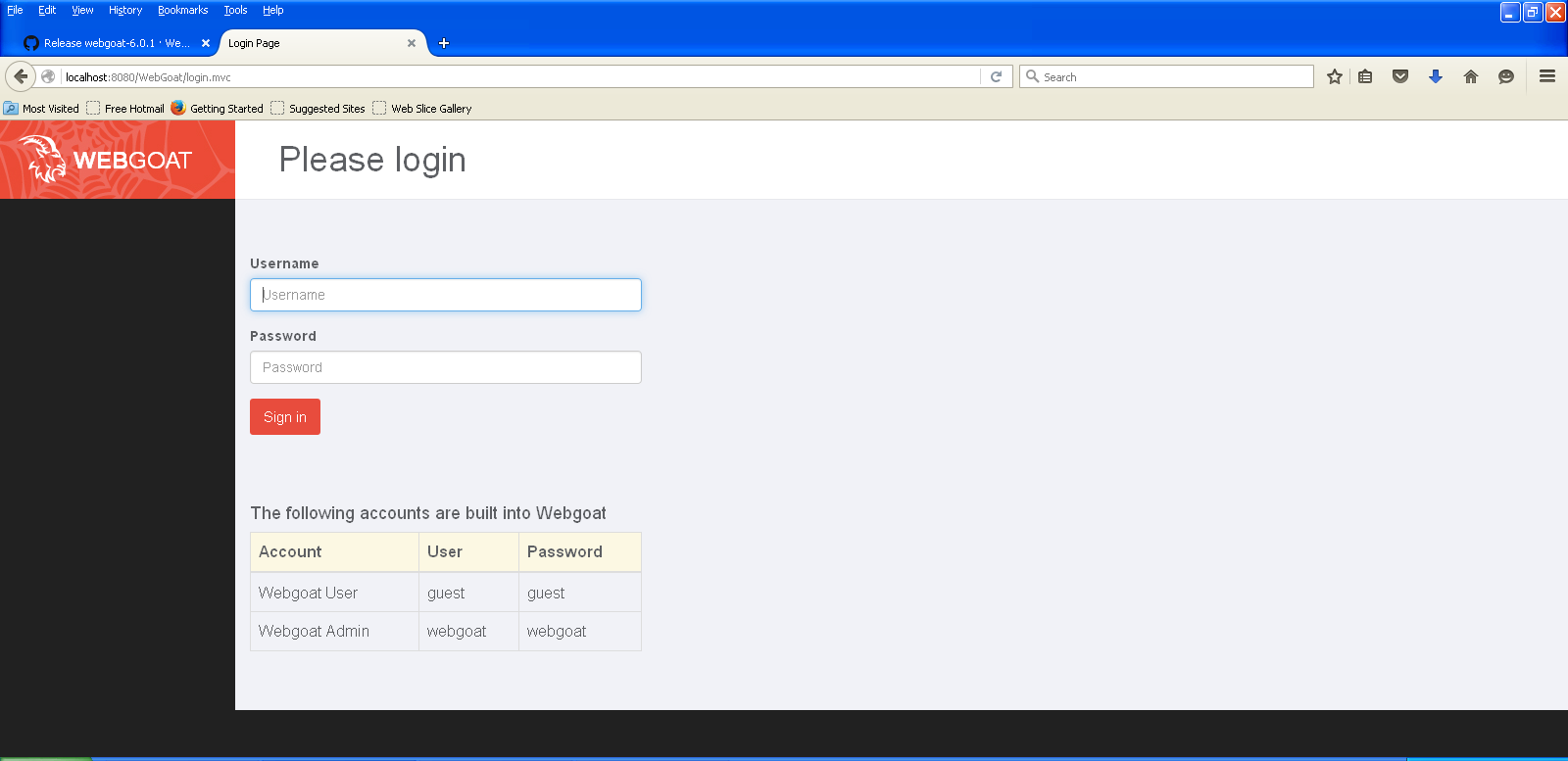
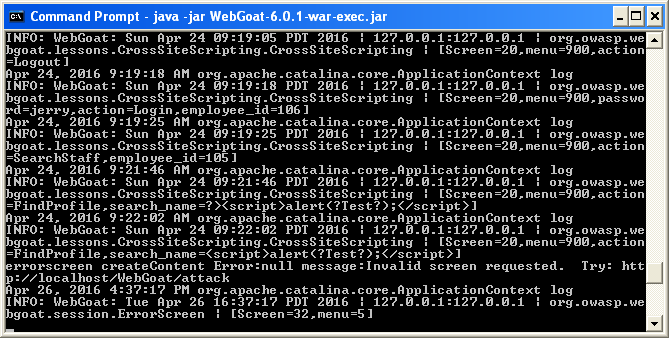
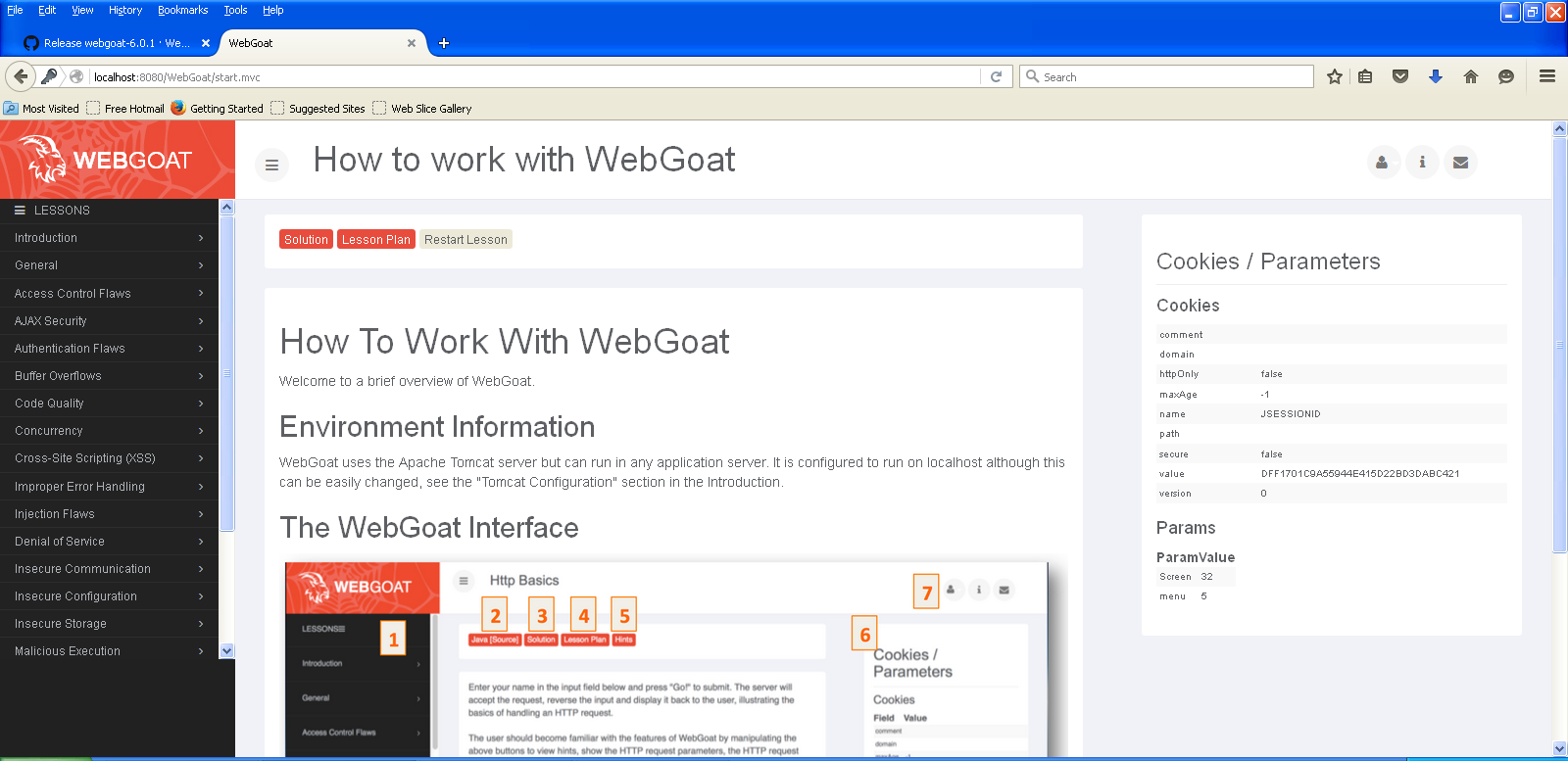
**Project 3**



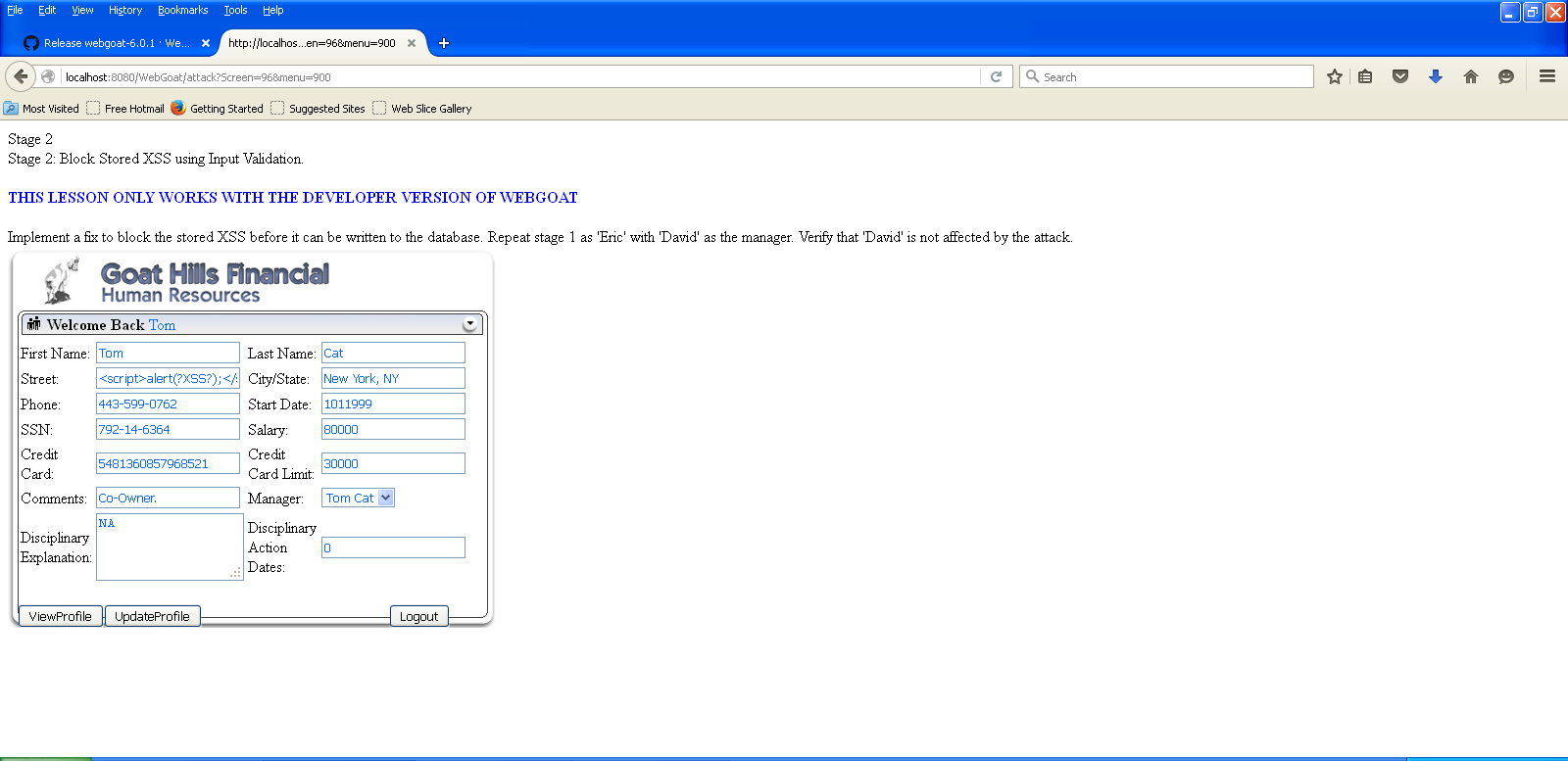


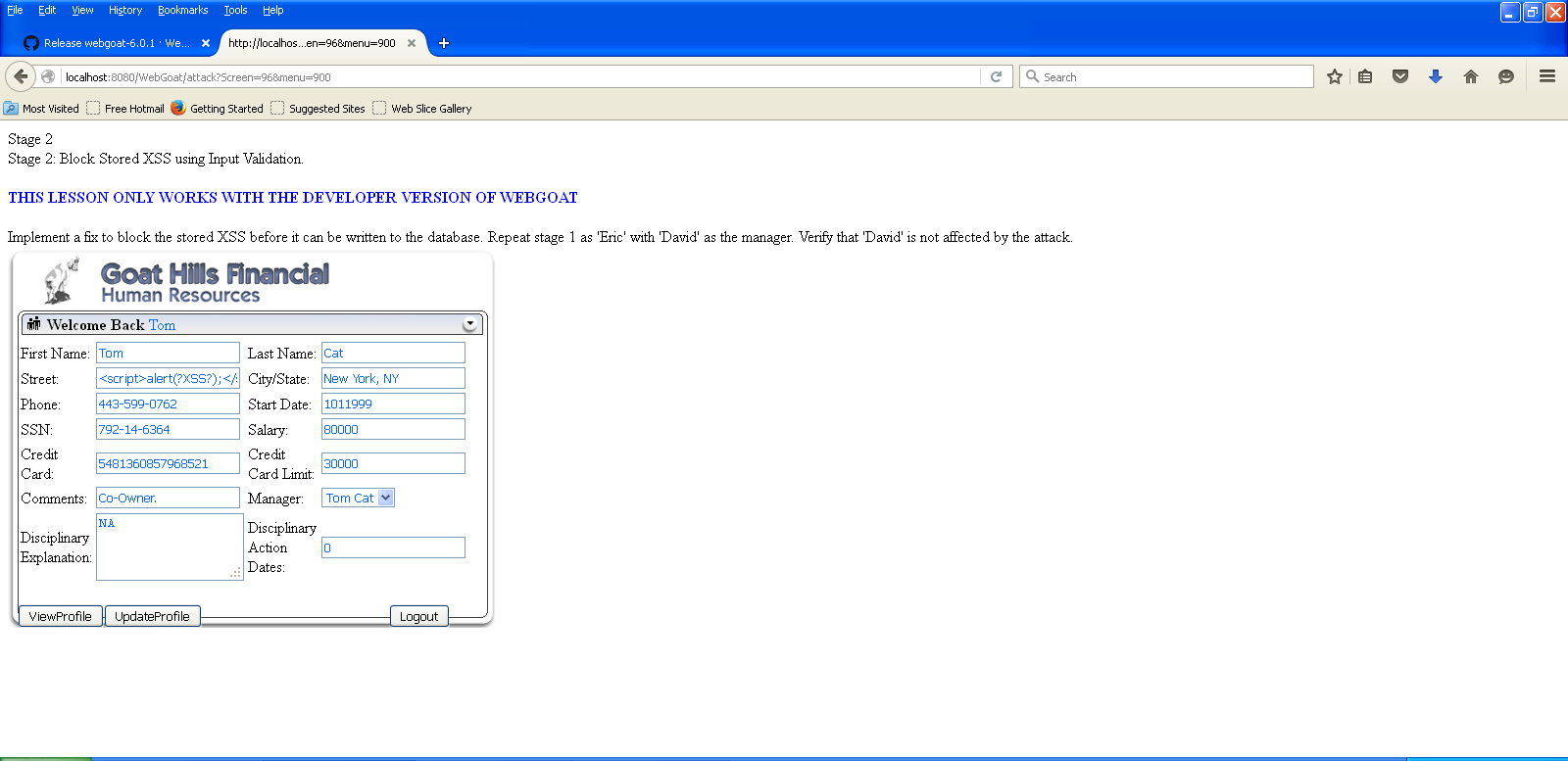
Stage 0:



**Stage 1 – Stored XSS Attack**

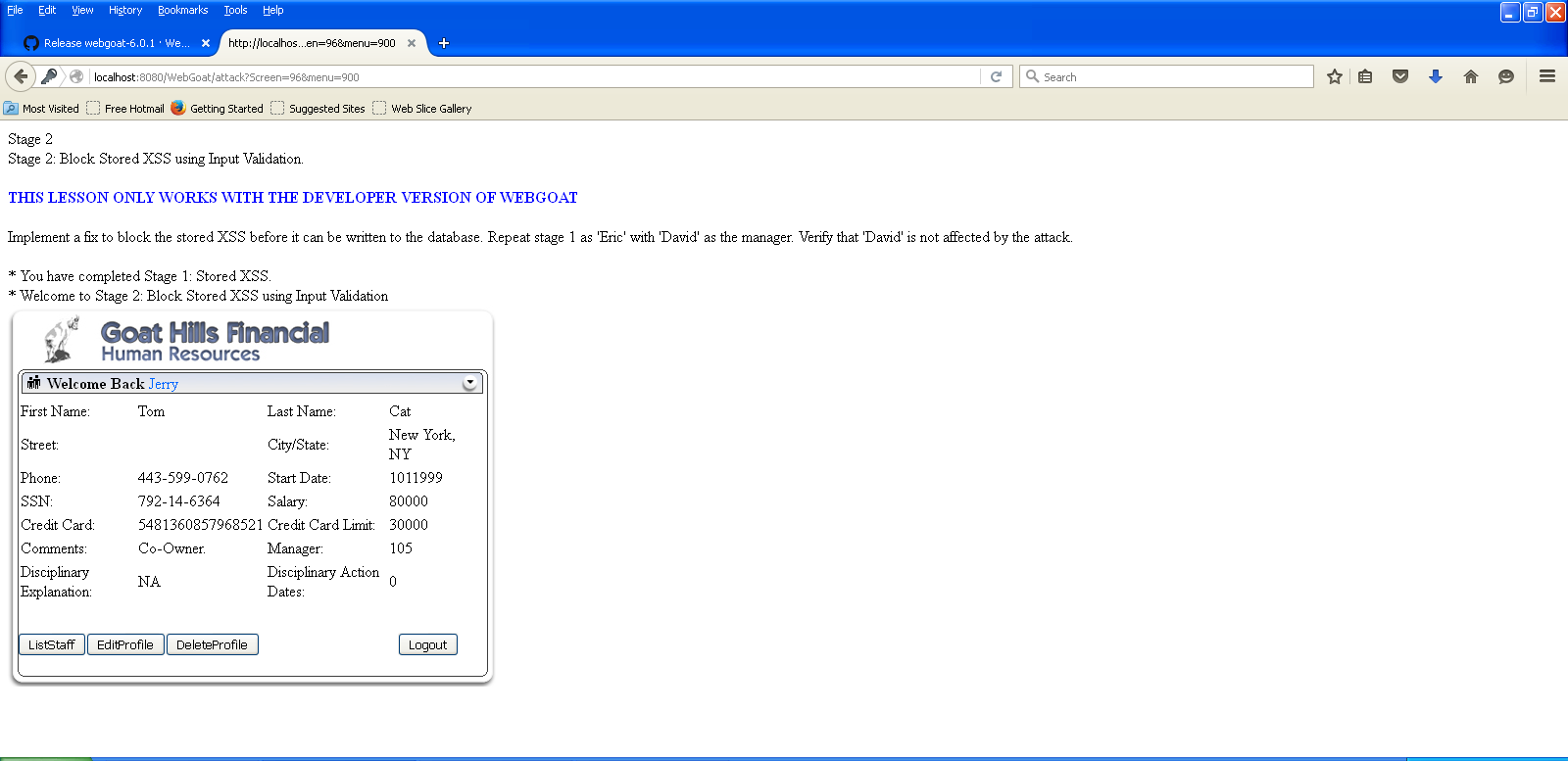
1. Using the drop-menu, you can login with ‘Tom Cat’ as Employee and password as tom
2. Click on View Profile.
3. Click on Edit Profile.
4. Change the text in the street field to **<script>alert(“XSS”);</script>**
5. Click on update profile.
6. Observe what happens.
7. Logout from Tom Cat





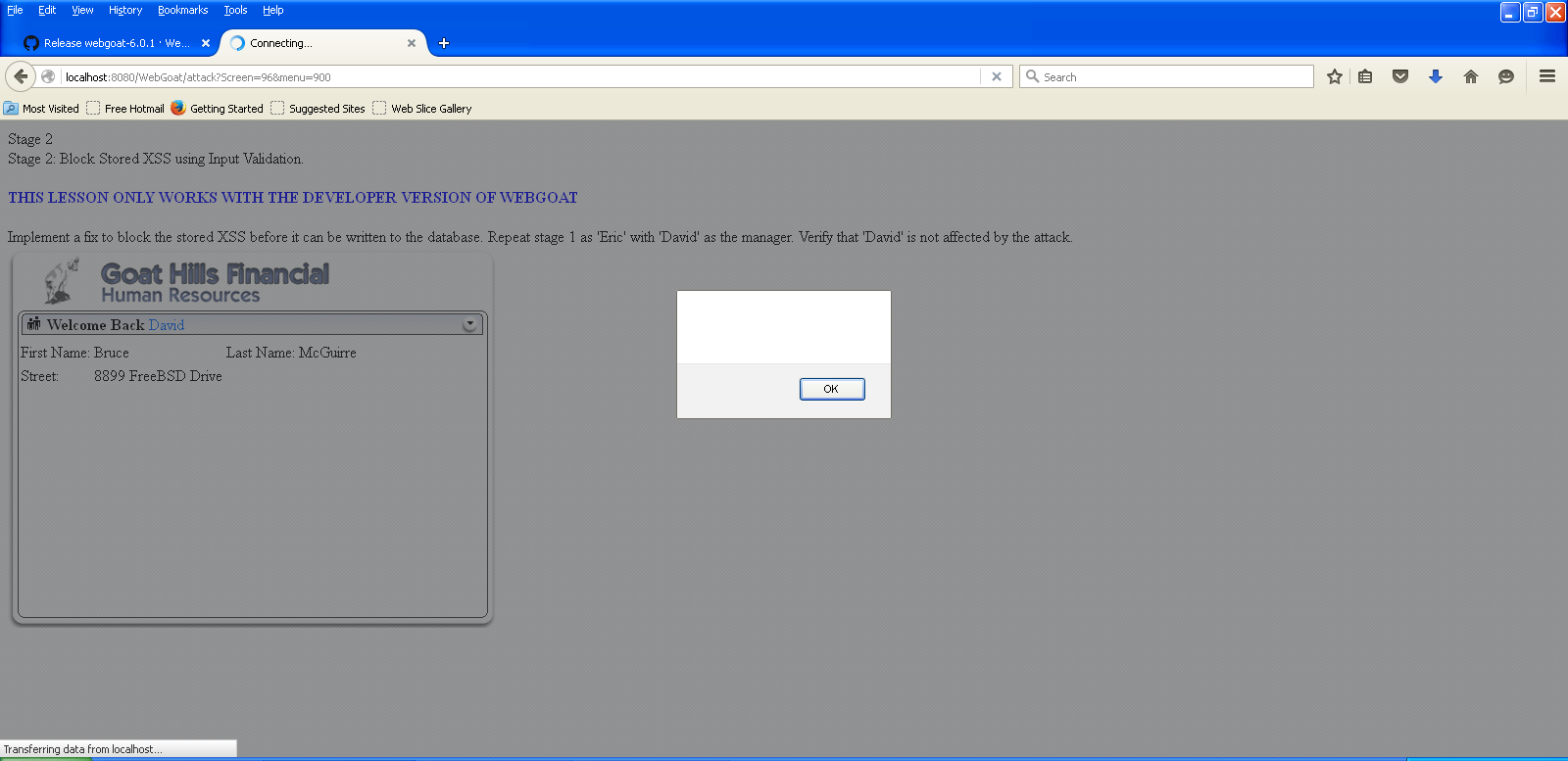
**Infecting Jerry with the script:**

1. Login with ‘Jerry Mouse’ as Employee and password as jerry
2. Click on Tom in left pane and then click on view profile in the right pane.
3. Observe what happens.



**Stage 3 – Stored XSS Revisited**

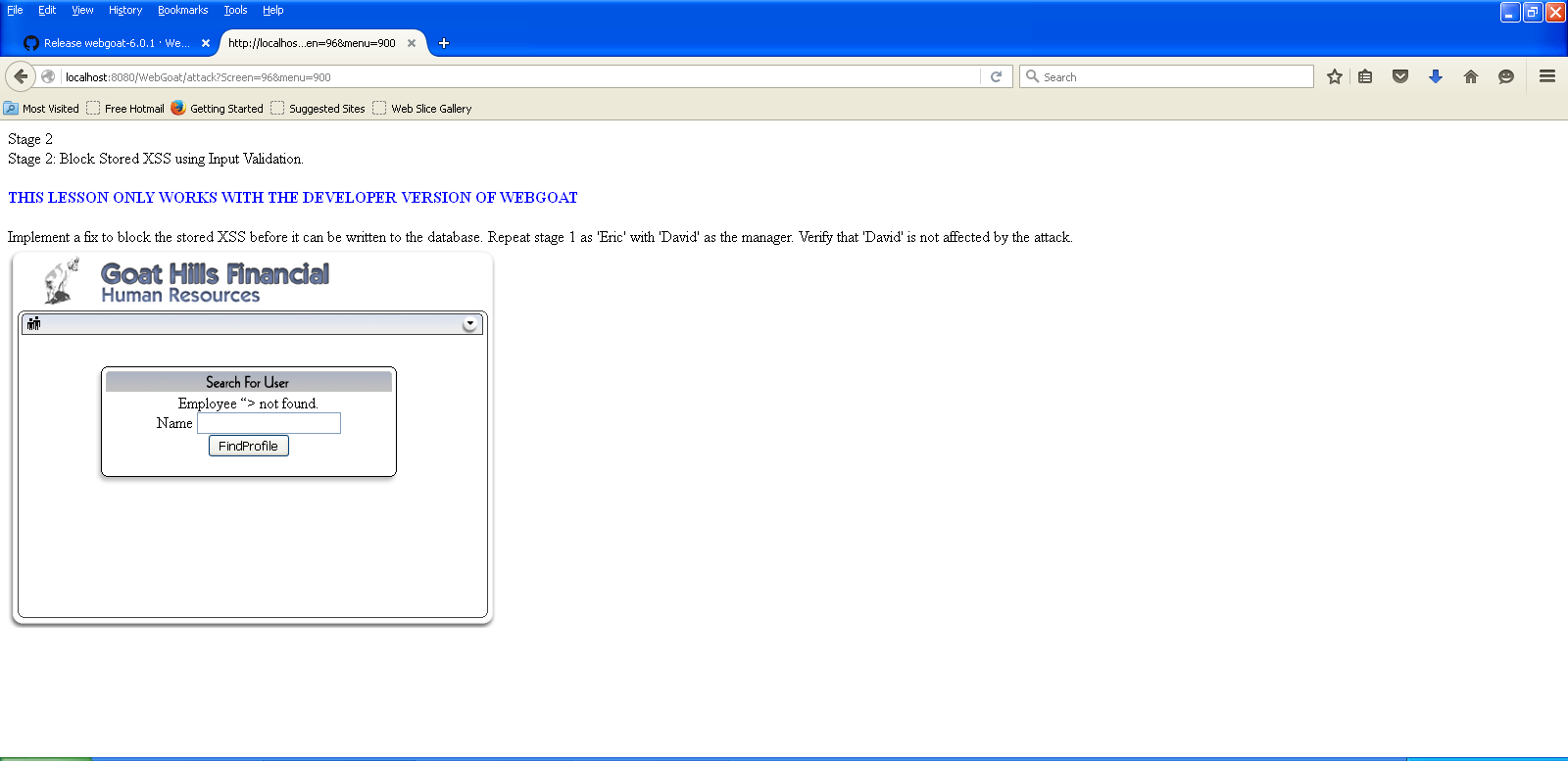
1. Login with ‘David Glambi(manager)’ as Employee and password as david.
2. Click on Bruce from the list and then click on view profile.
3. Observe what happens.



**Stage 5 – Reflected XSS**

1. Login with ‘Jerry Mouse’ as Employee and password as jerry.
2. Click on search staff.
3. Type **“><script>alert(“Test”);</script>** in the input field.

Click on find and observe what happens



1. What happens in a stored XSS attack? Explain using the project result.

A Stored XSS attack is a dangerous variant of XSS flaws. Stored attack occurs when the data is saved by server and then displayed under the privilege of the web application.

In our case, user Tom-Cat login in and modifies the Street field with a javascript code.The street field is infected and passes this code to user Jerry.When Jerry logs in and selects Tom’s profile,He sees the street textbox with the information.

1. What are some measures that can be taken to block a stored XSS attack?

**Restrict Untrusted JavaScript:**

* Allow JavaScript code to run from the trusted domains.
* Installing noscript XSS addon to safeguard against XSS attacks

• **Use Built-In Browser Protections:** Most modern webbrowsers have bult in protection against XSS attacks.

• **Restrict External Websites from Requesting Internal Resources**: The NoScript plug-in has a feature called the Application Boundary Enforcer (ABE) that can be configured to disallow external websites from requesting internal resources.

• **Maintain Good System Hygiene**: It is important to keep systems and applications up-to-date with updates and patches, protected from malware and securely configured

* **HTML encode special characters:** HTML characters like <,> etc should be encoded to prvent XSS attacks

1. Explain your observation and understanding about the vulnerability from stage 5.

In Reflected XSS, the attacker’s payload script has to be part of the request which is sent to the web server and reflected back in such a way that the HTTP response includes the payload from the HTTP request. Using Phishing emails and other social engineering techniques, the attacker lures the victim to inadvertently make a request to the server which contains the XSS payload and ends-up executing the script that gets reflected and executed inside the browser. Since Reflected XSS isn’t a persistent attack, the attacker needs to deliver the payload to each victim – social networks are often conveniently used for the dissemination of Reflected XSS attacks.

Jerry logs in and injects a script to the fields.When another employee logs in and searches for an employee,The script injected will be reflected in the dialogue box.