Hacking E.S.P.

Disclaimer

The views and opinions expressed in this presentation are solely those of the speakers and do not necessarily reflect opinions of their employers, Defcon, the Riviera, residents of Las Vegas, residents of Nevada, anyone in the United States or on the Planet Earth. Nothing we are saying should be construed as legal advice. Don't rely on anything that we say, do your own research.

Who We Are!

- Joe Cicero is currently a Network Specialist Instructor for Northeast Wisconsin Technical College, he specializes in teaching Linux, Network Security, and Computer Forensics Courses. Joe has had positions covering every aspect of computers including: Help Desk Support, Technician, Programmer, Network Administrator, Directory of Technology, Columnist and of course Instructor. He is most passionate about teaching and enjoys having the time to "tinker" with all types of technology.

- Michael Vieau is a independent security researcher located in United States where he conducts security assessments & penetration tests on new and existing technology for various customers (and sometimes just for fun). His main focus is on *NIX security, mobile devices, and wireless security. He comes from a wide technical background ranging from network infrastructure, to programming, instructing, & of course security.

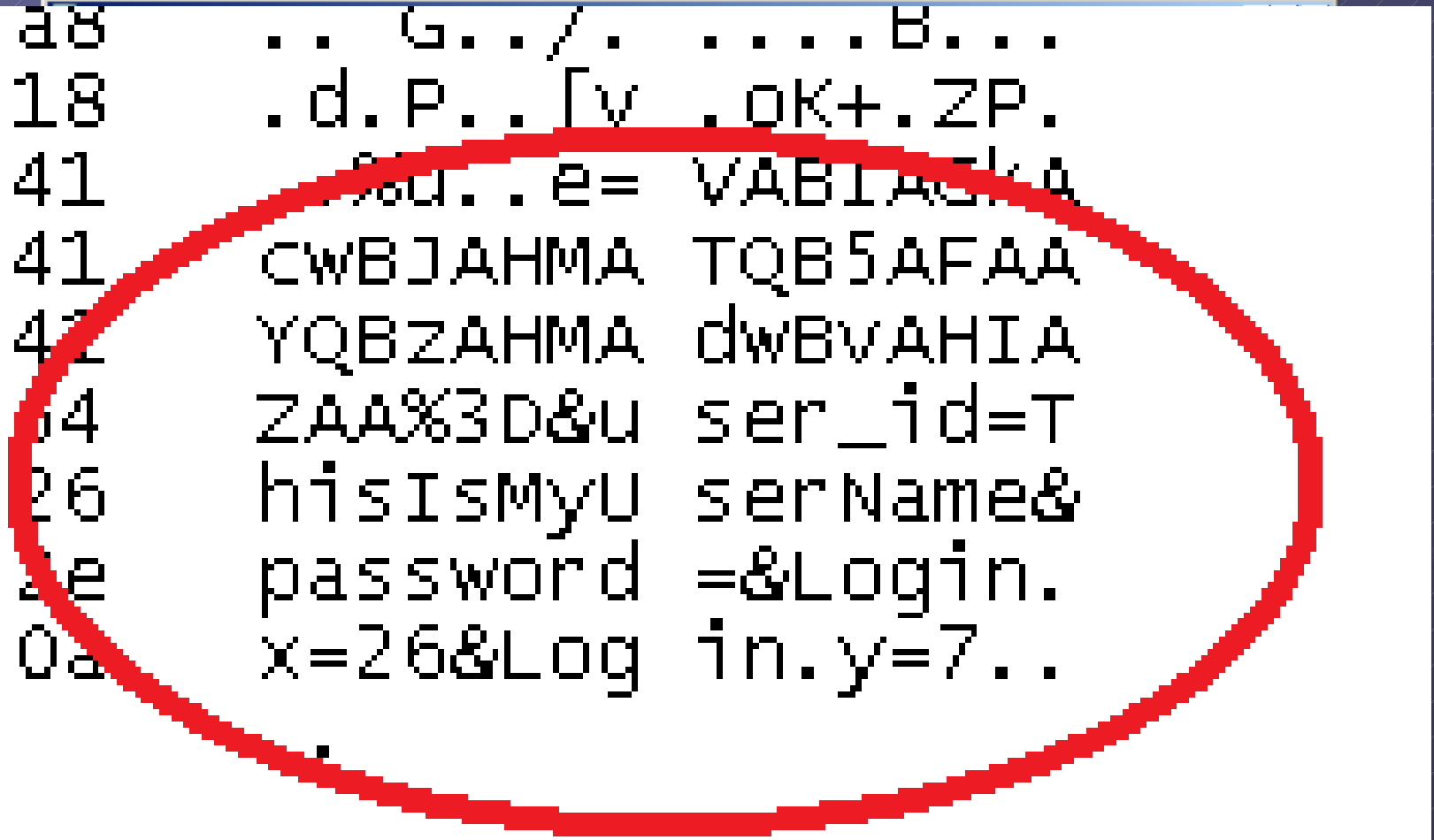
Why we did the research

- Almost everyone has dealt with an educational institution some time in their life.
- Educational Institutions must keep your personal / confidential information.

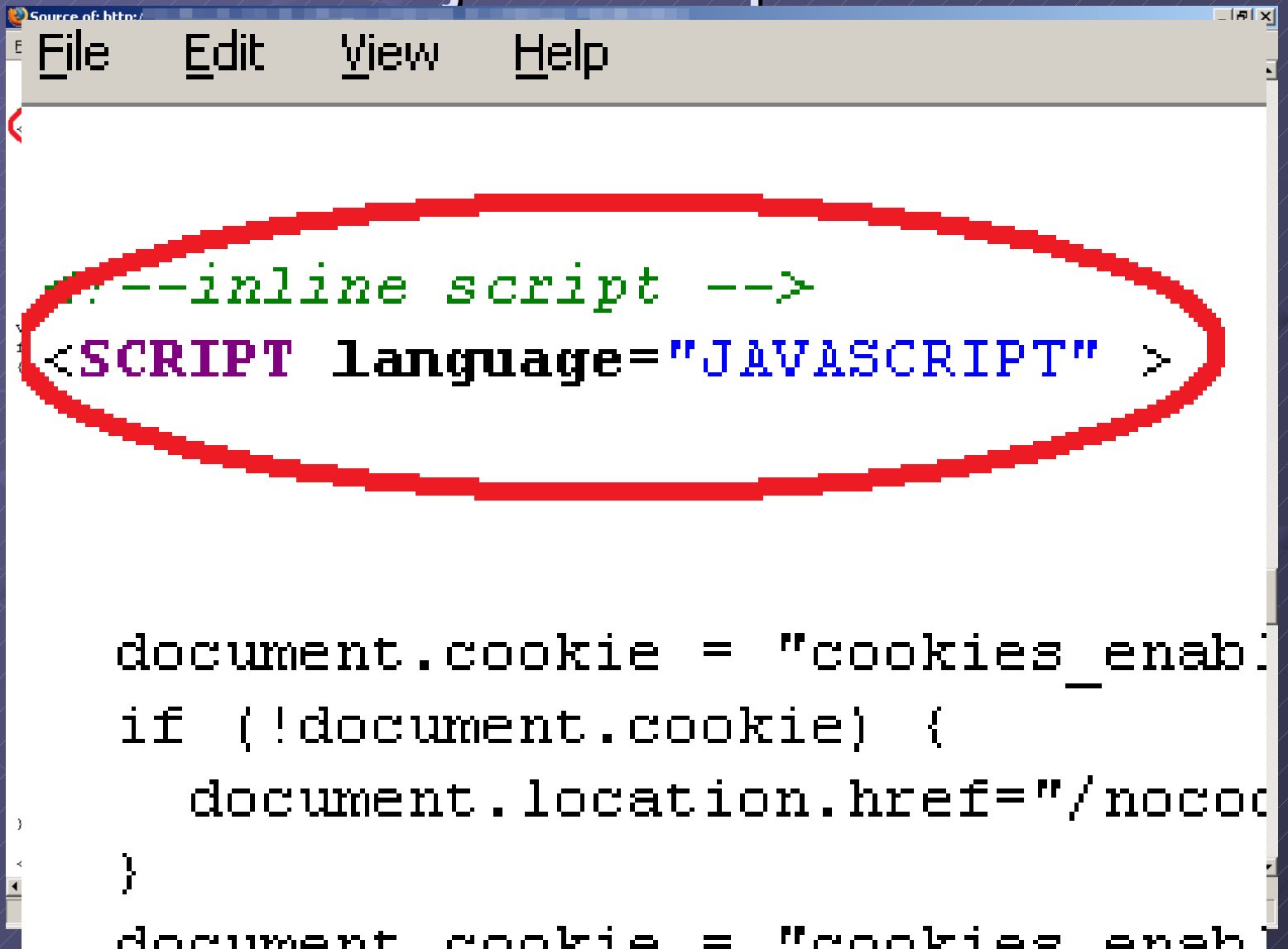
ESP login



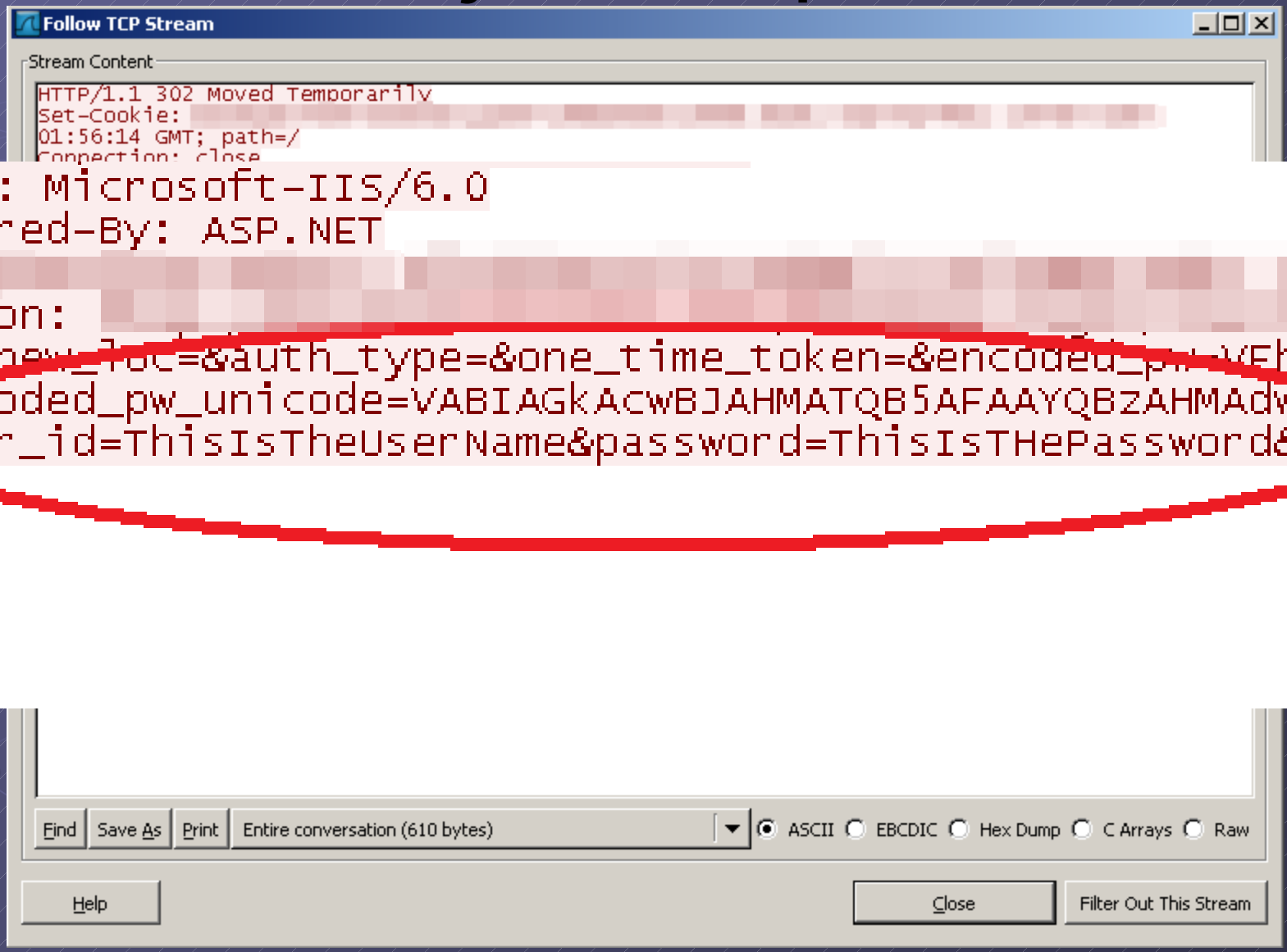
Wireshark Capture Of Login



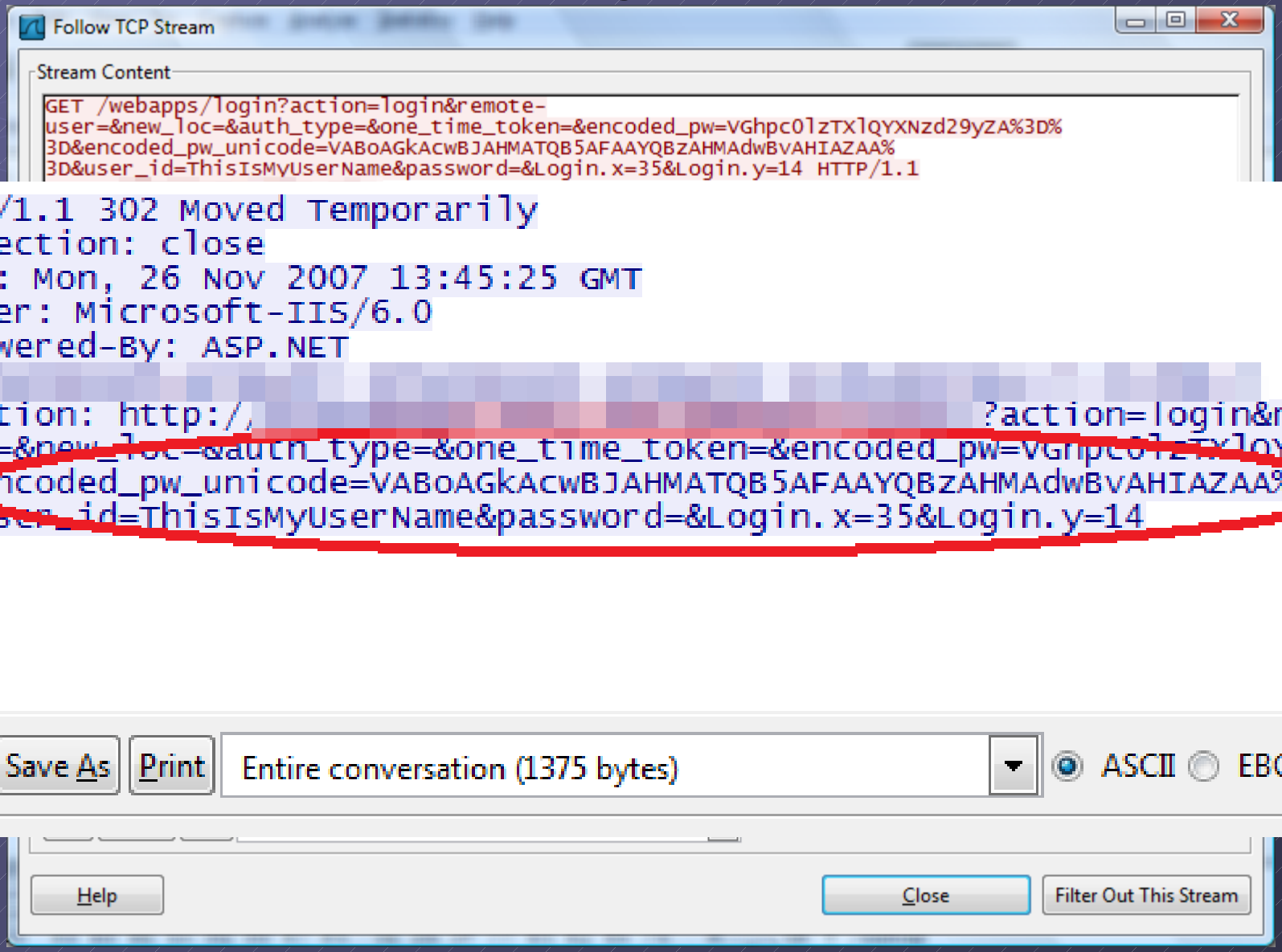
Login page code – Oh, it's using javascript!



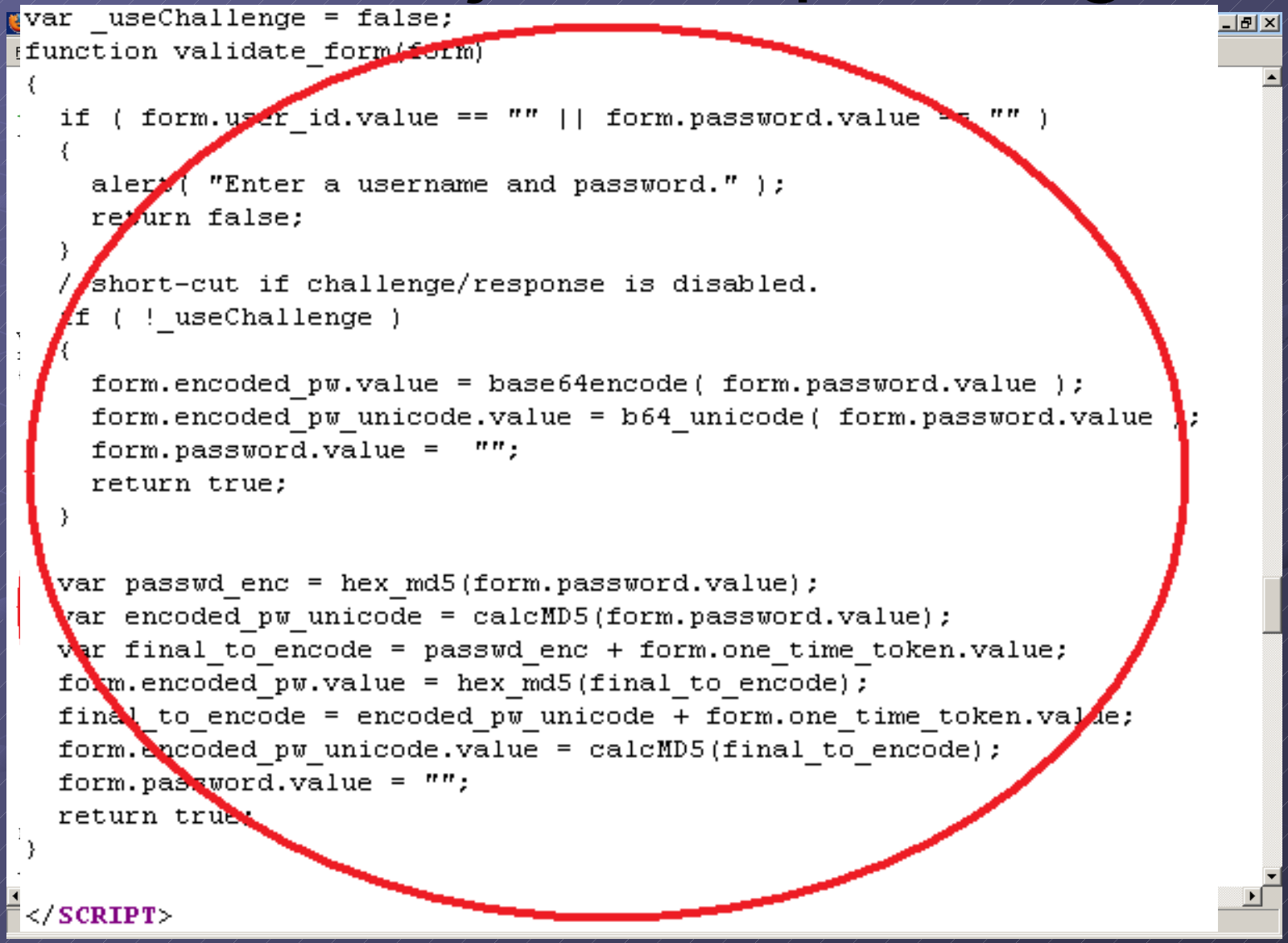
What if javascript is off?



Capture with javascript on…

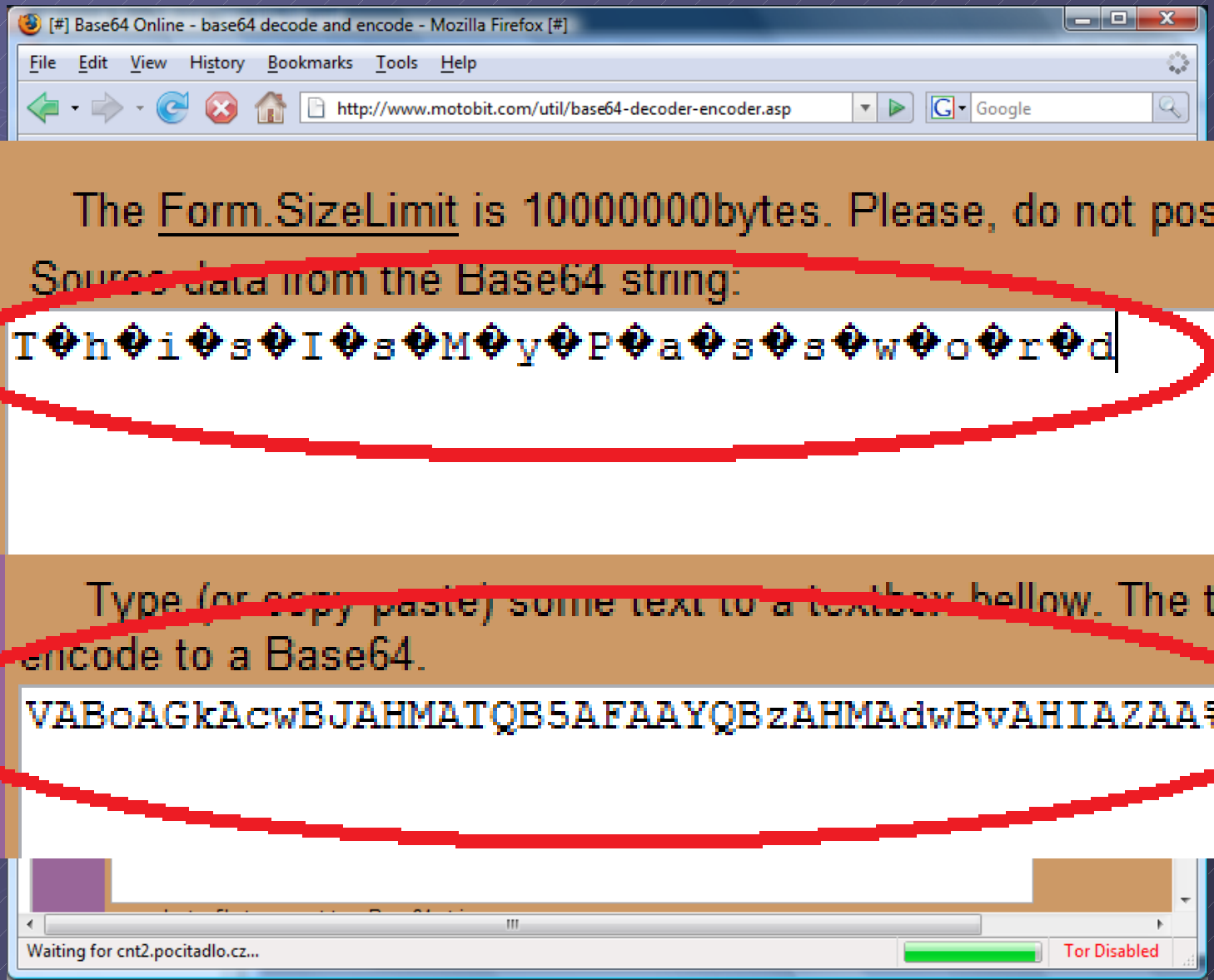


What is javascript doing?

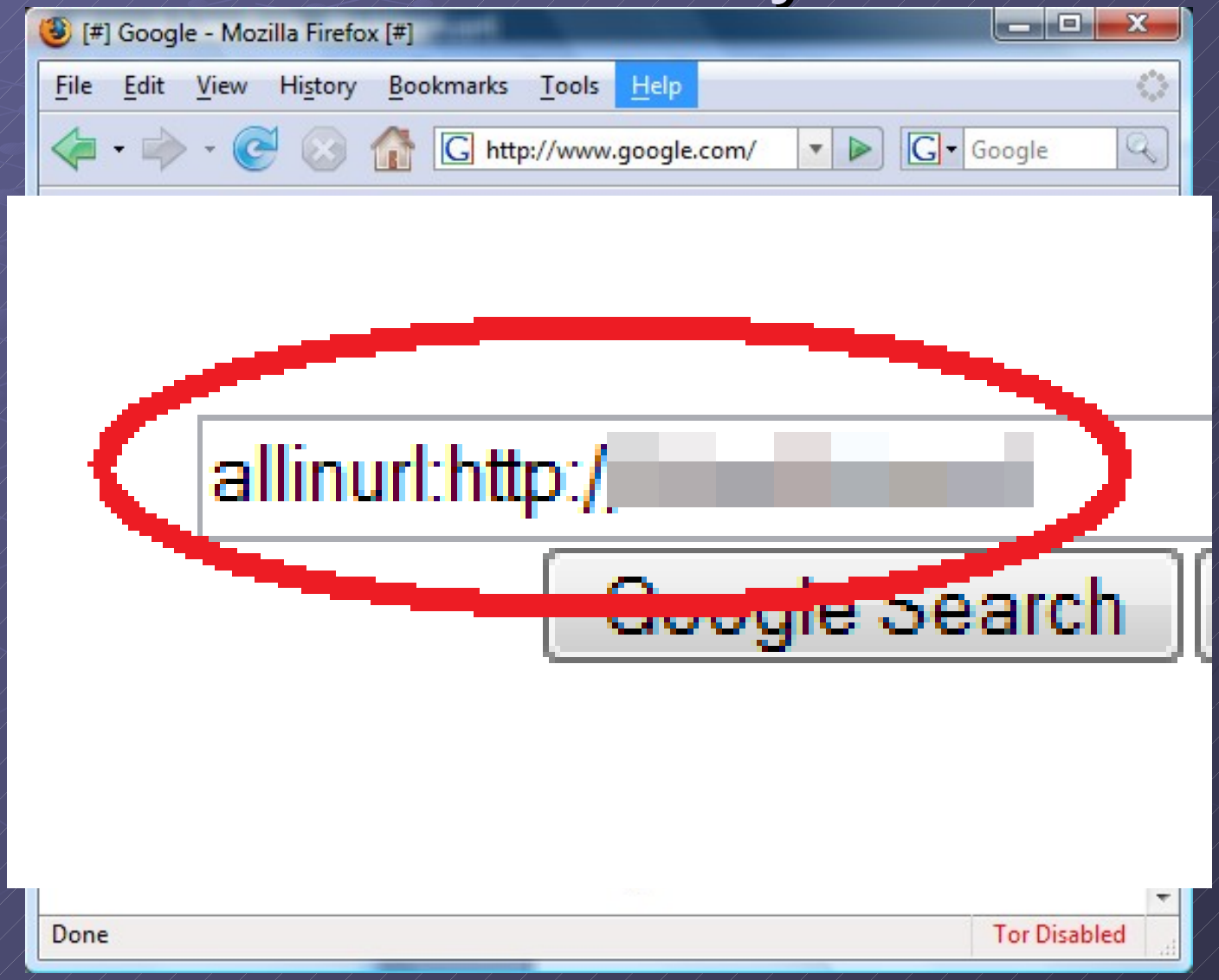


```
var _useChallenge = false;
function validate_form(form)
{
  if ( form.user_id.value == "" || form.password.value == "" )
  {
    alert( "Enter a username and password." );
    return false;
  }
  // short-cut if challenge/response is disabled.
  if ( !_useChallenge )
  {
    form.encoded_pw.value = base64encode( form.password.value );
    form.encoded_pw_unicode.value = b64_unicode( form.password.value );
    form.password.value =  "";
    return true;
  }

  var passwd_enc = hex_md5(form.password.value);
  var encoded_pw_unicode = calcMD5(form.password.value);
  var final_to_encode = passwd_enc + form.one_time_token.value;
  form.encoded_pw.value = hex_md5(final_to_encode);
  final_to_encode = encoded_pw_unicode + form.one_time_token.value;
  form.encoded_pw_unicode.value = calcMD5(final_to_encode);
  form.password.value = "";
  return true;
}

</SCRIPT>
```

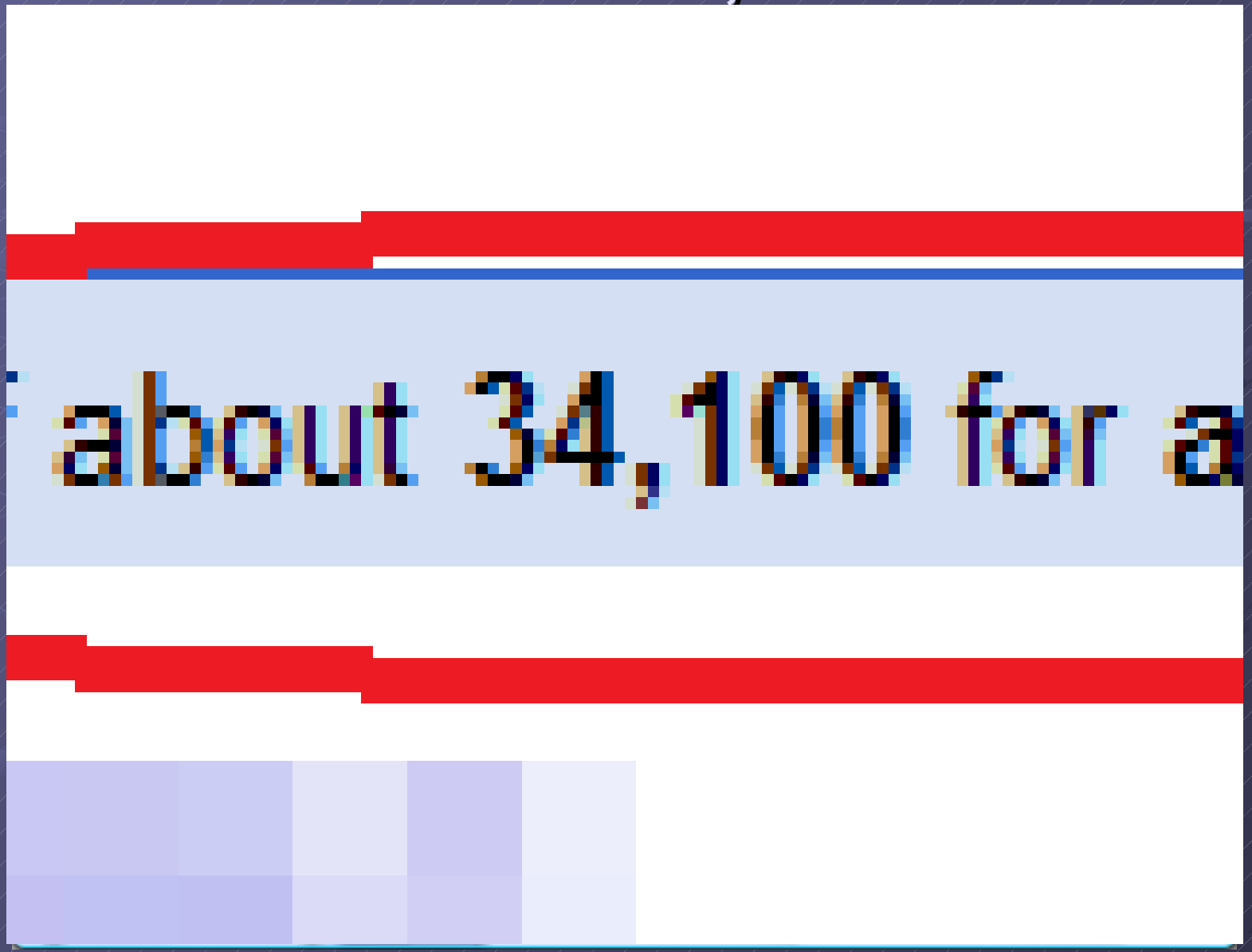
Can we decode it? – Yes!



How many schools use this ESP insecurely?



Over 34,000!



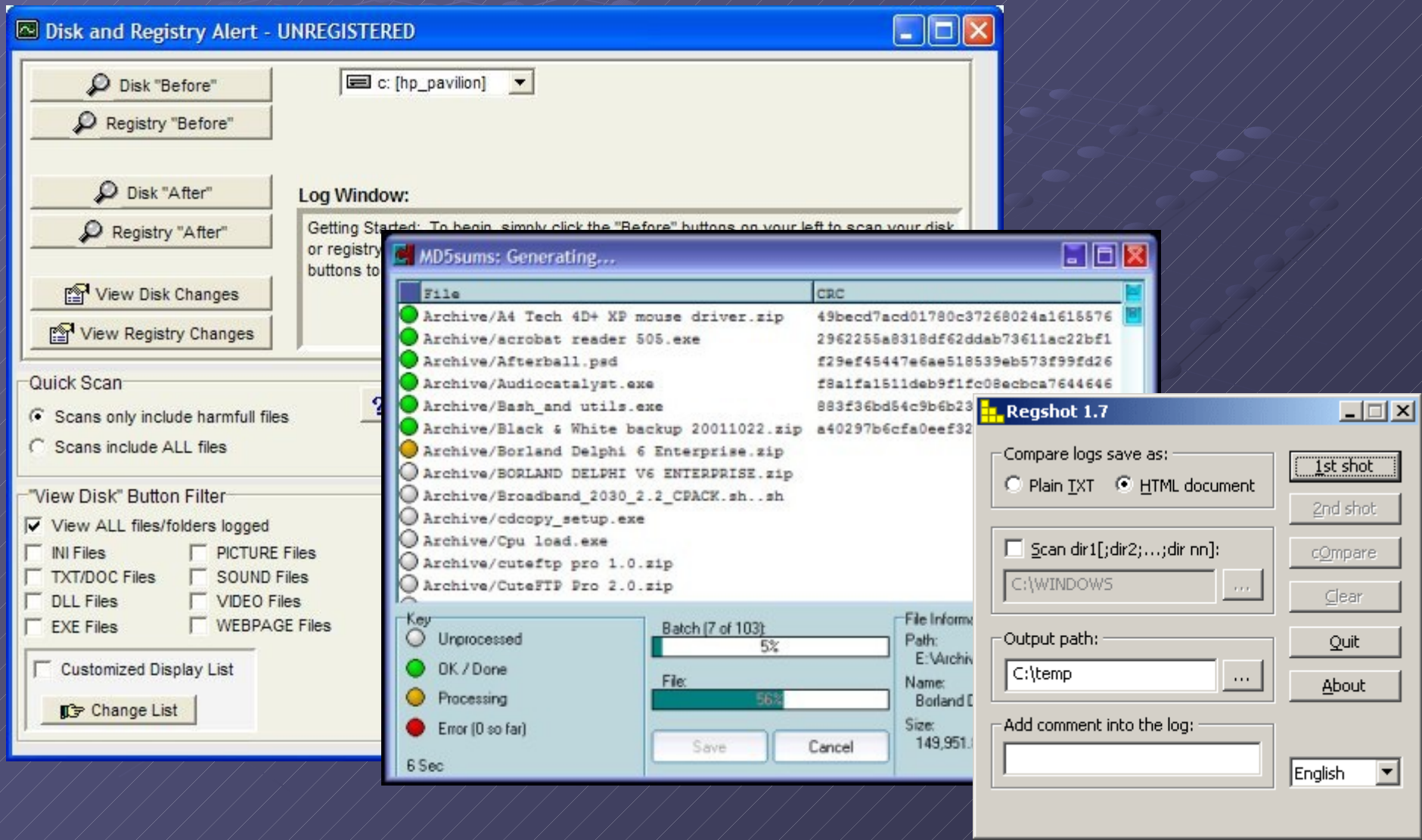
What we know now…

- It is possible to steal a username and password…
  - on a network with hubs
  - on a network with switches (arp poison)
  - on a wireless network
- This username and password is used for other accounts.
- However, there might be a log of an attackers activity.

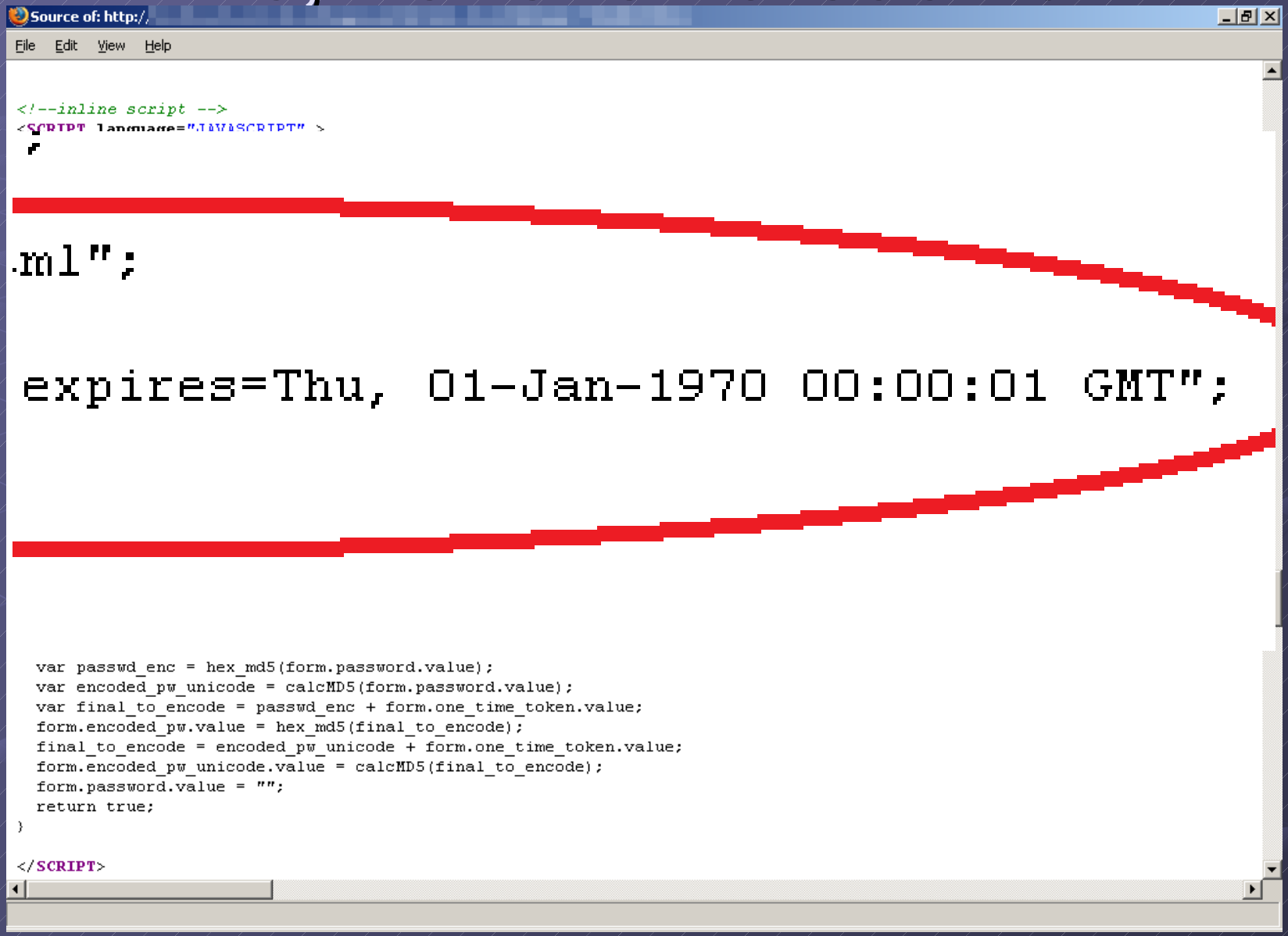
Sidejacking…

- How can we hide our activity?
- Instead of Hijacking the login and password – Sidejack it by piggybacking on the users session.

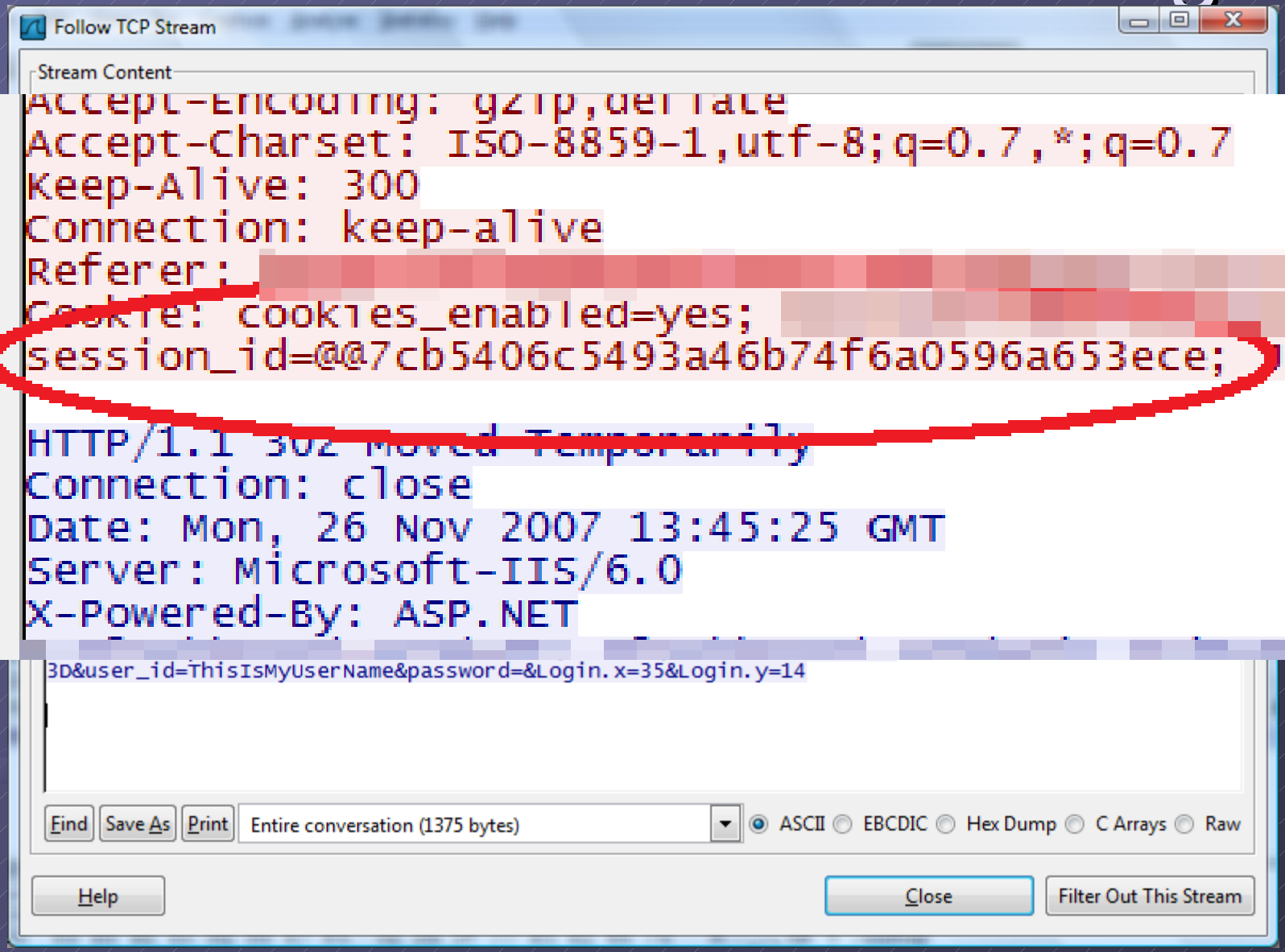
Is anything left on PC – file, file modification, registry entry?



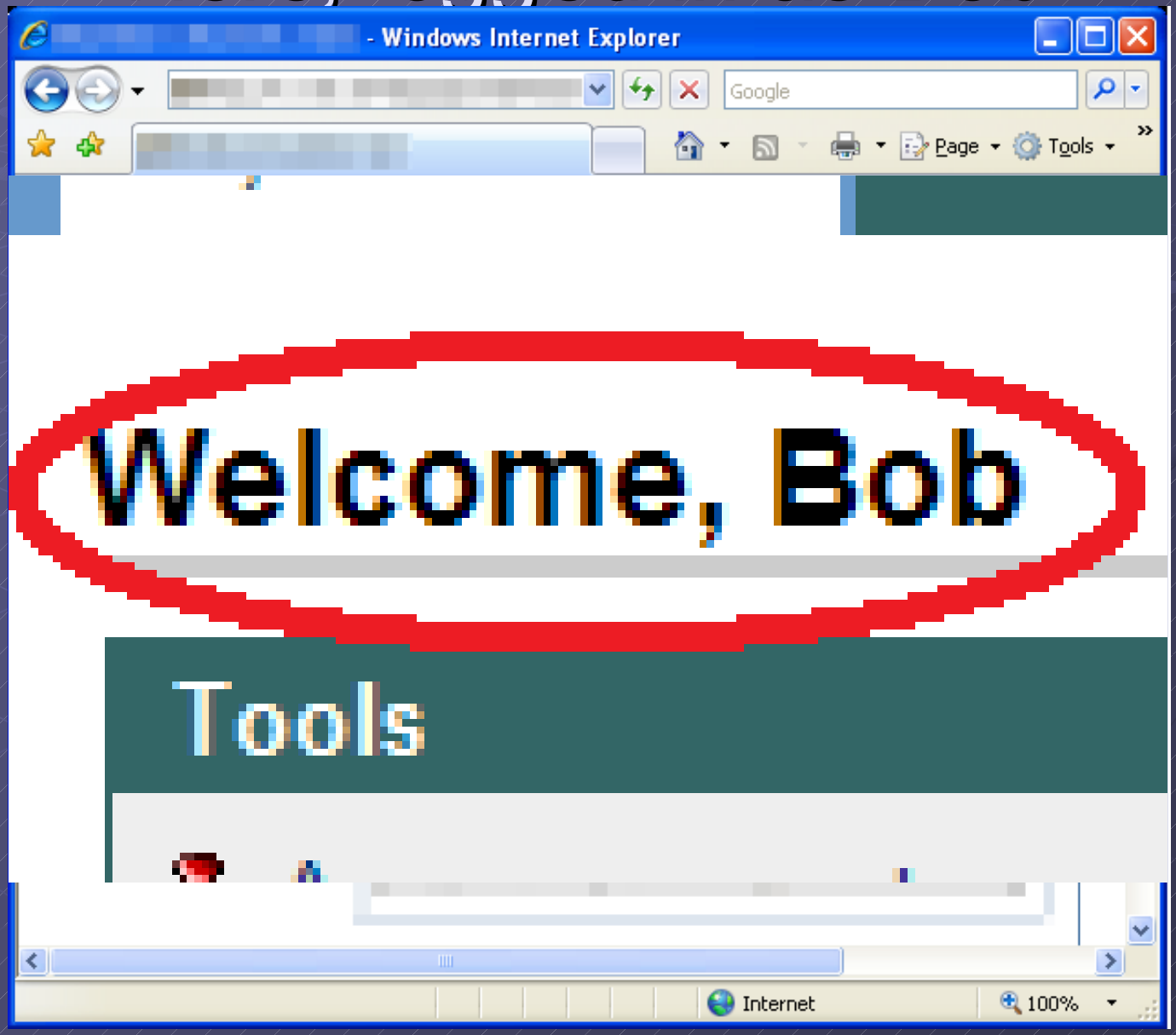
No, not even a cookie?



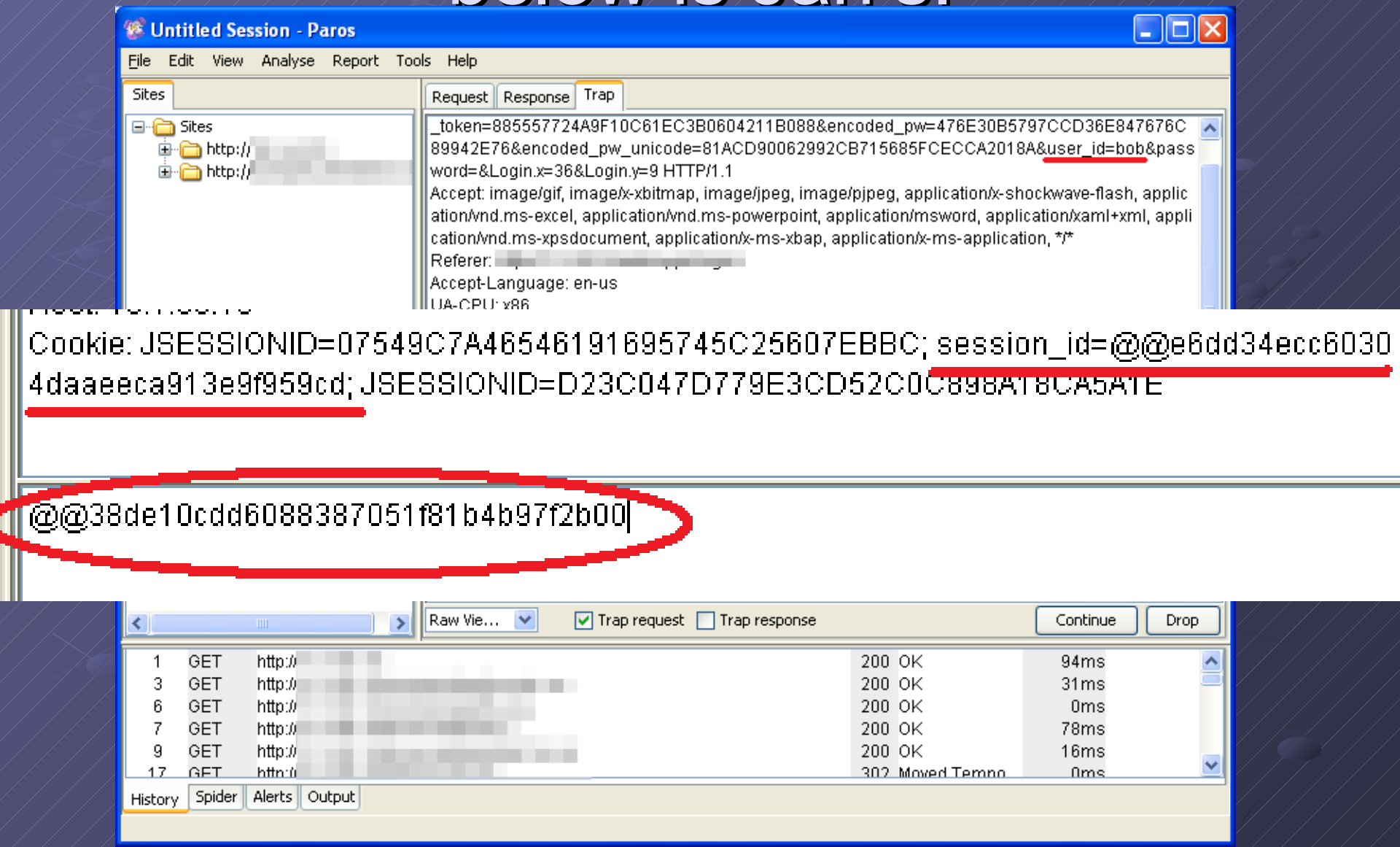
What's this session ID doing?



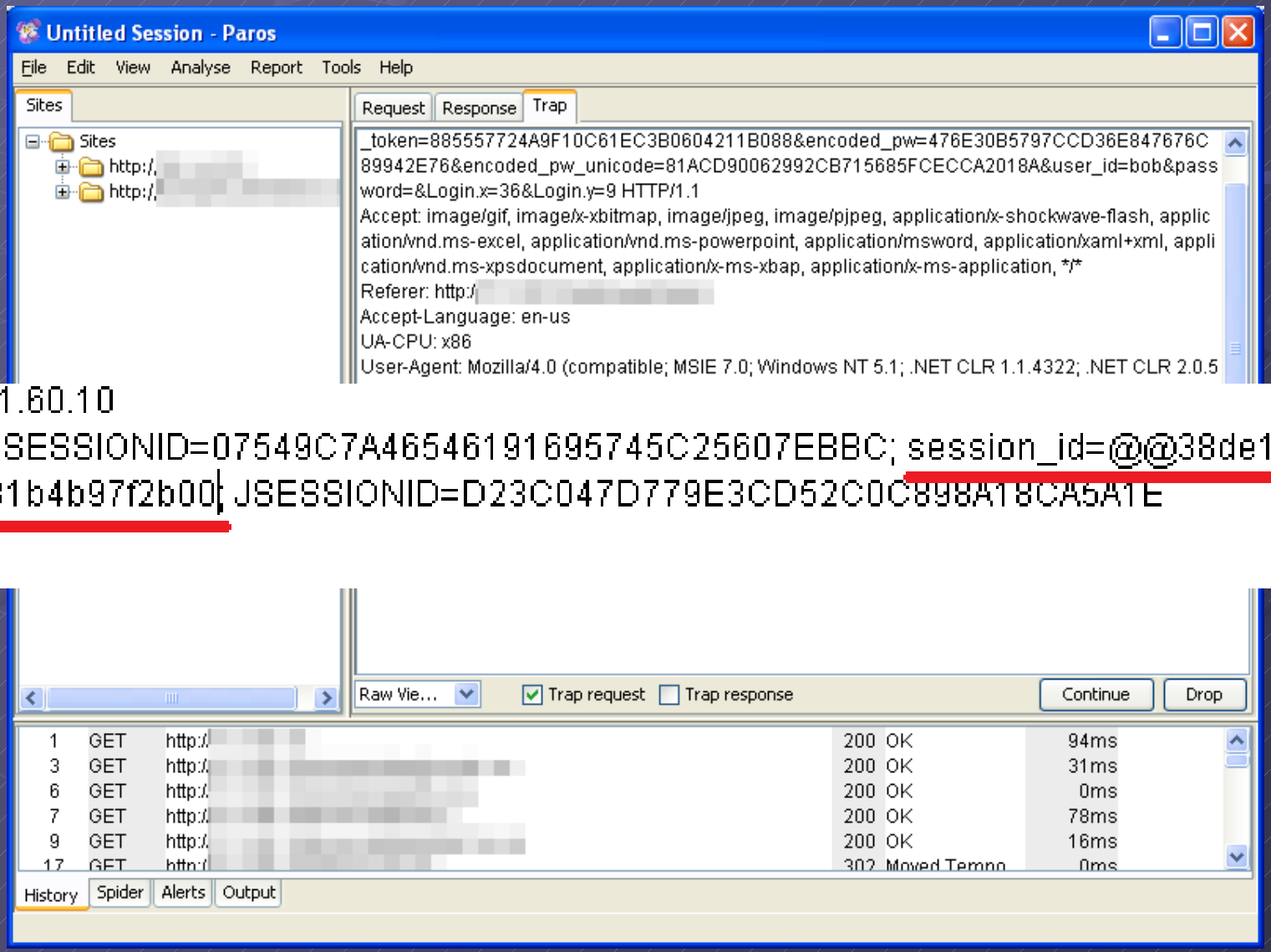
Here, logged in as Bob.



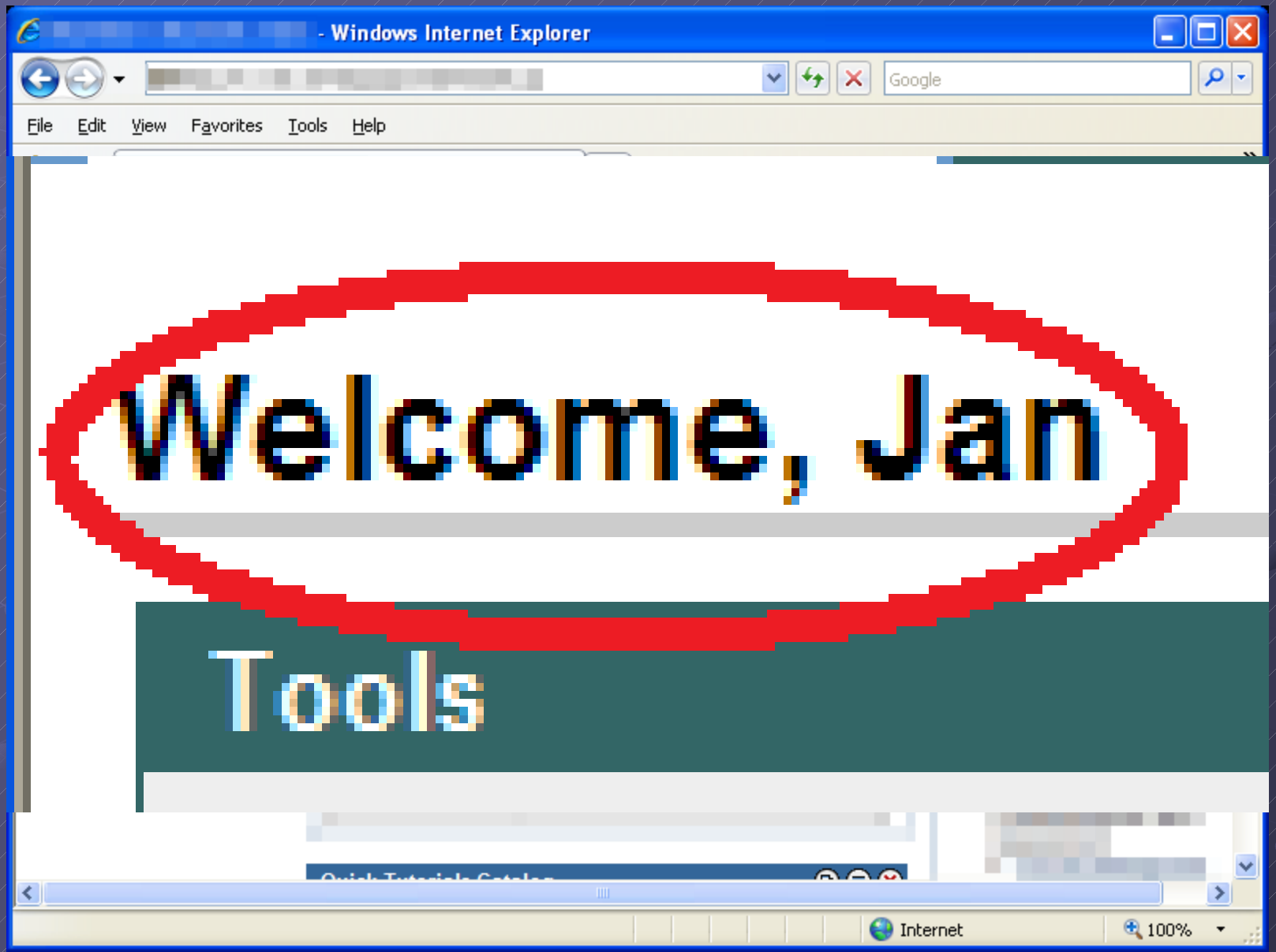
Here is Bob's session Id, pasted below is Jan's.



Bob's session ID replaced with Jan's.



I became Jan!


- Windows Internet Explorer
Google
File Edit View Favorites Tools Help
Welcome, Jan
Tools
Internet
100%

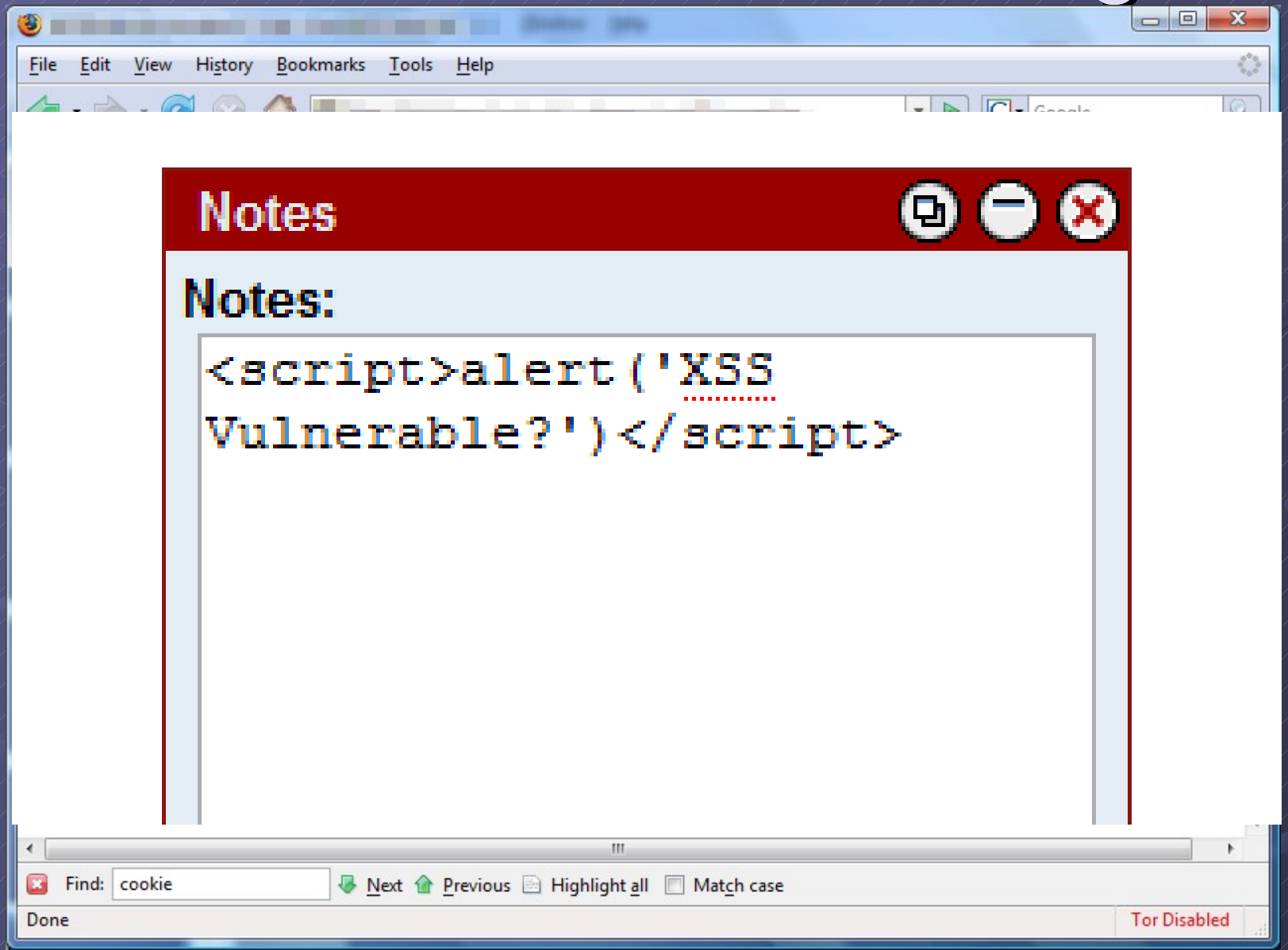
When do you get the Session ID?

- Before login!
- Why is this dangerous…
  - Could lead to a local exploit where user copies session id before someone logs in.
  - Remote exploit that captures this info and sends it off.

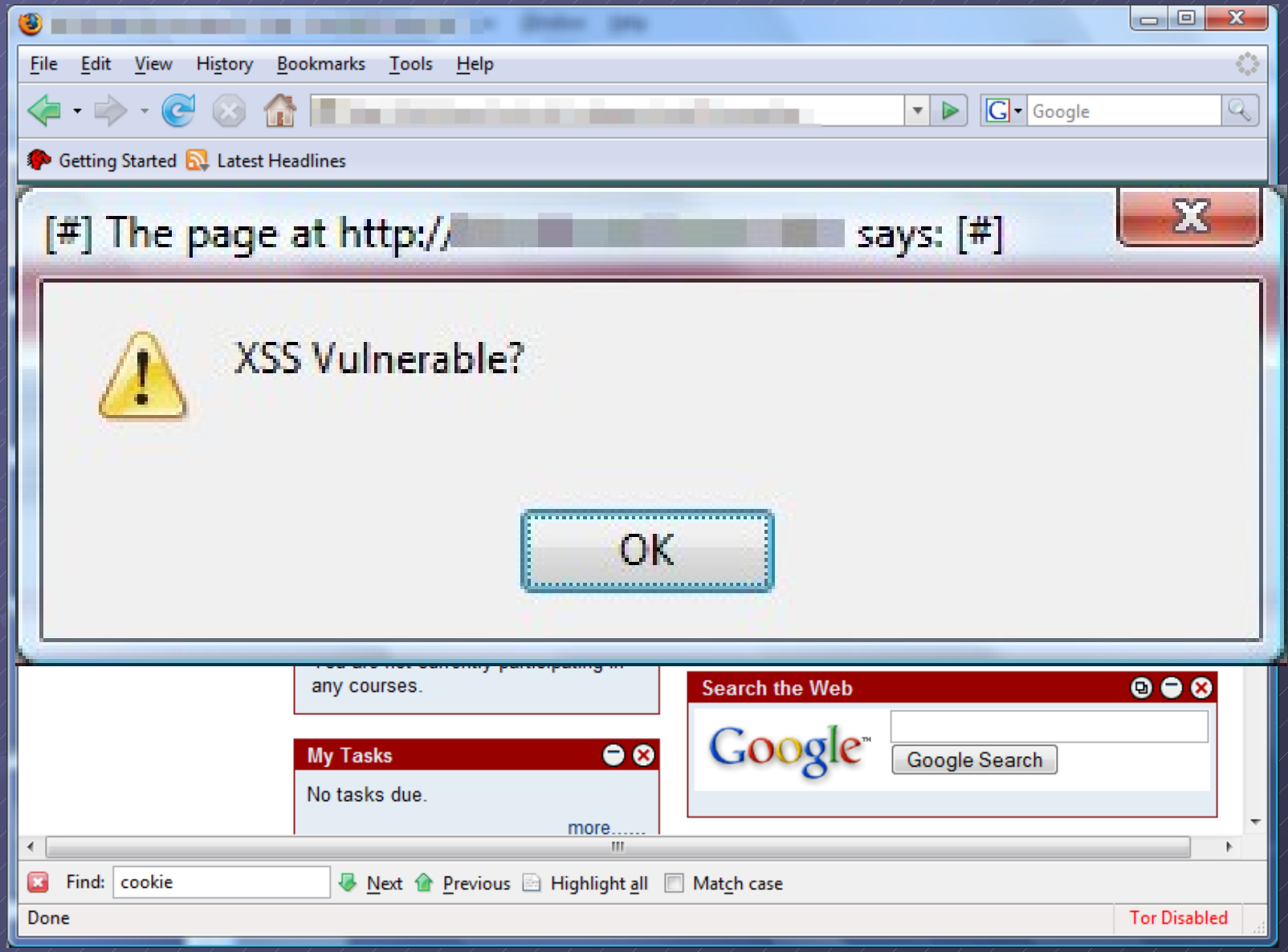
What other vulnerabilities can we find?

- XSS?
- Can we insert code?
- What can we do with the code?
- What else can we do?

Does it allow us to use tags?



Yes!


File Edit View History Bookmarks Tools Help
Google
Getting Started
Latest Headlines
[#] The page at http:// says: [#]
XSS Vulnerable?
OK
any courses.
My Tasks
No tasks due.
more.....
Search the Web
Google
Google Search
Find: cookie
Next
Previous
Highlight all
Match case
Done
Tor Disabled

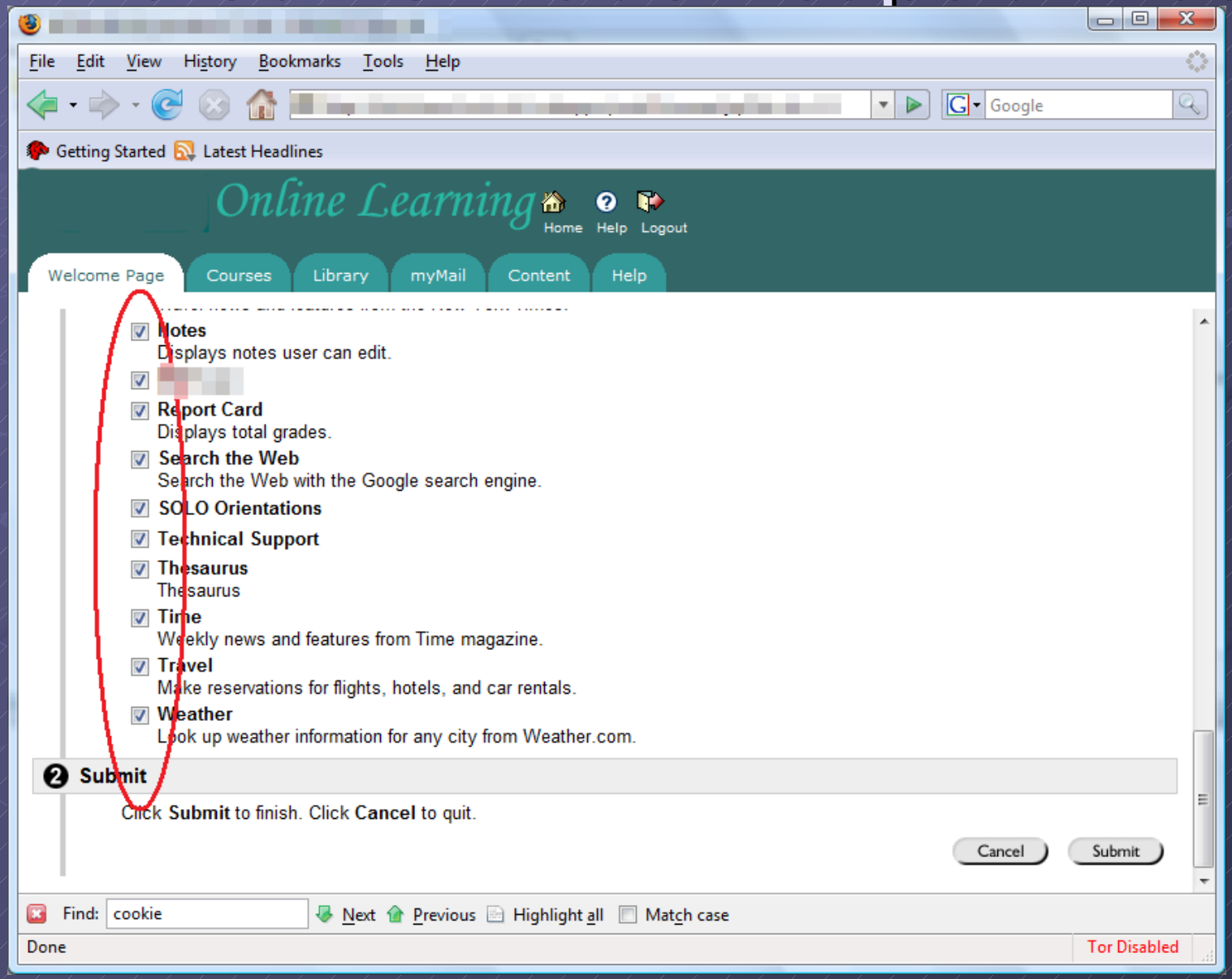
So what?

- After you have found an XSS hole in a web application on a website, check to see if it issues cookies. If any part of the website uses cookies, then it is possible to steal them from its users.
  - http://www.cgisecurity.com/articles/xss-faq.shtml
  - Remember the session hijacking!

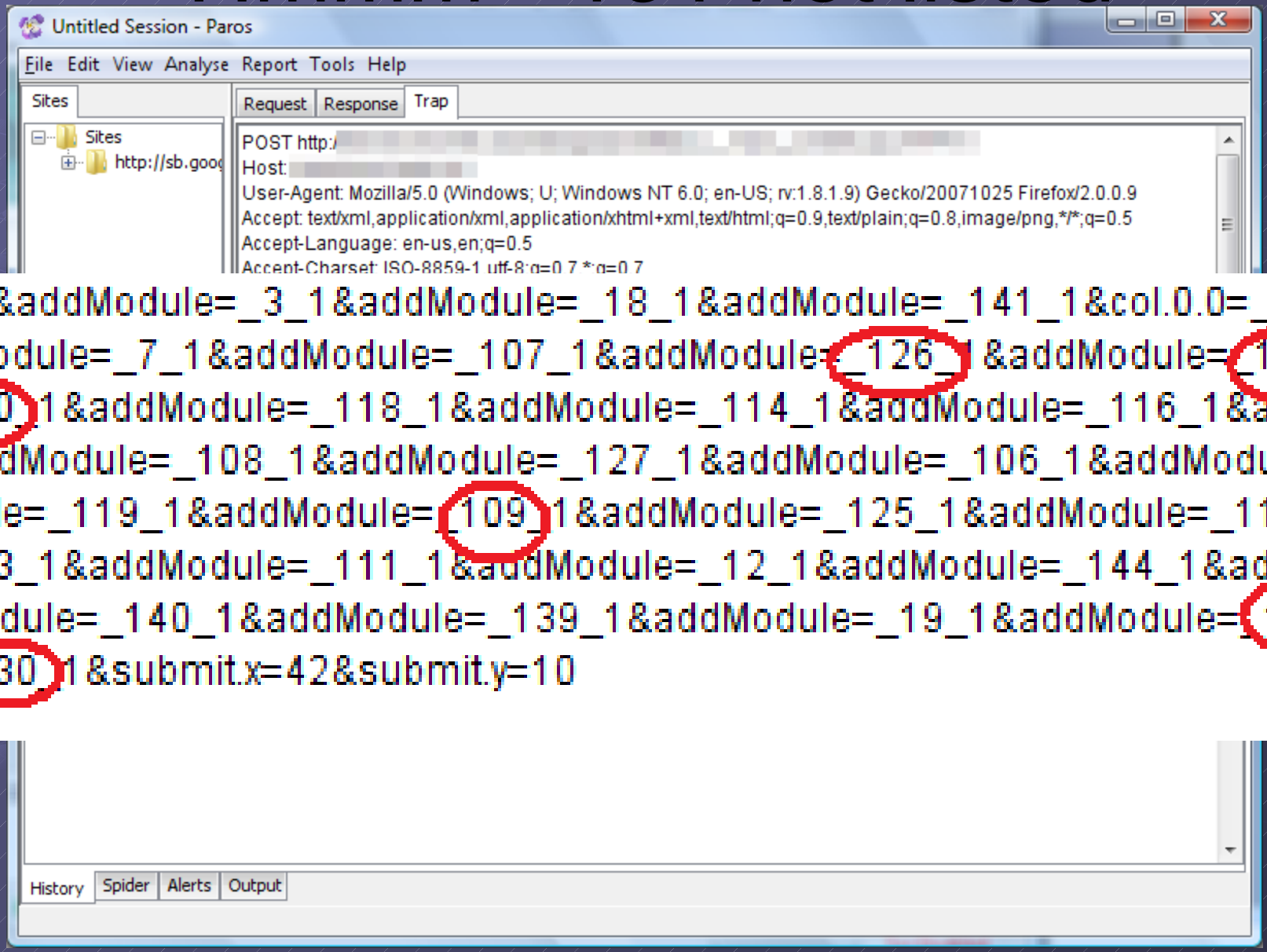
Surely there are no other issues!

- How do these applications work?
- What else can we do?

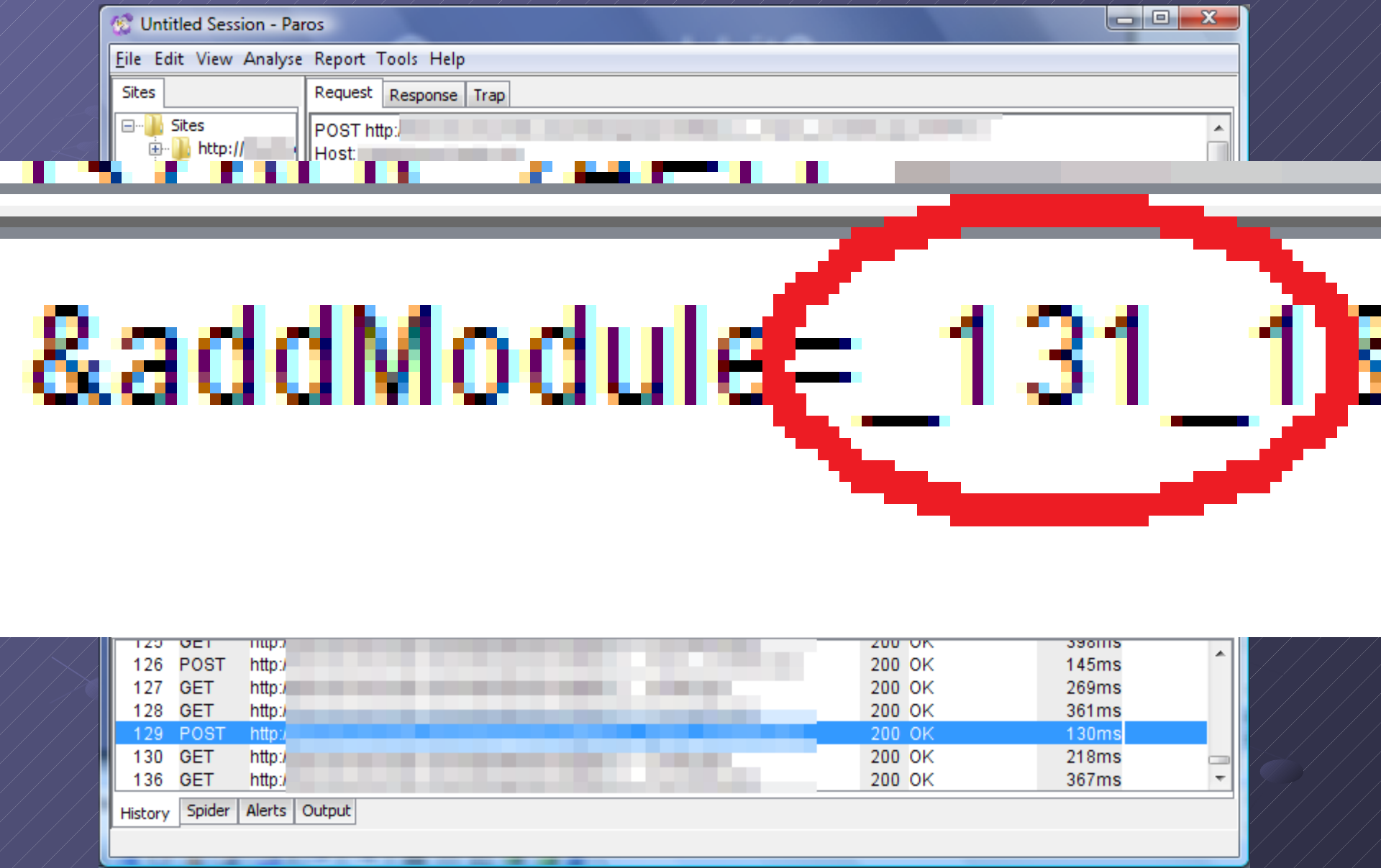
Find some hidden capabilities!



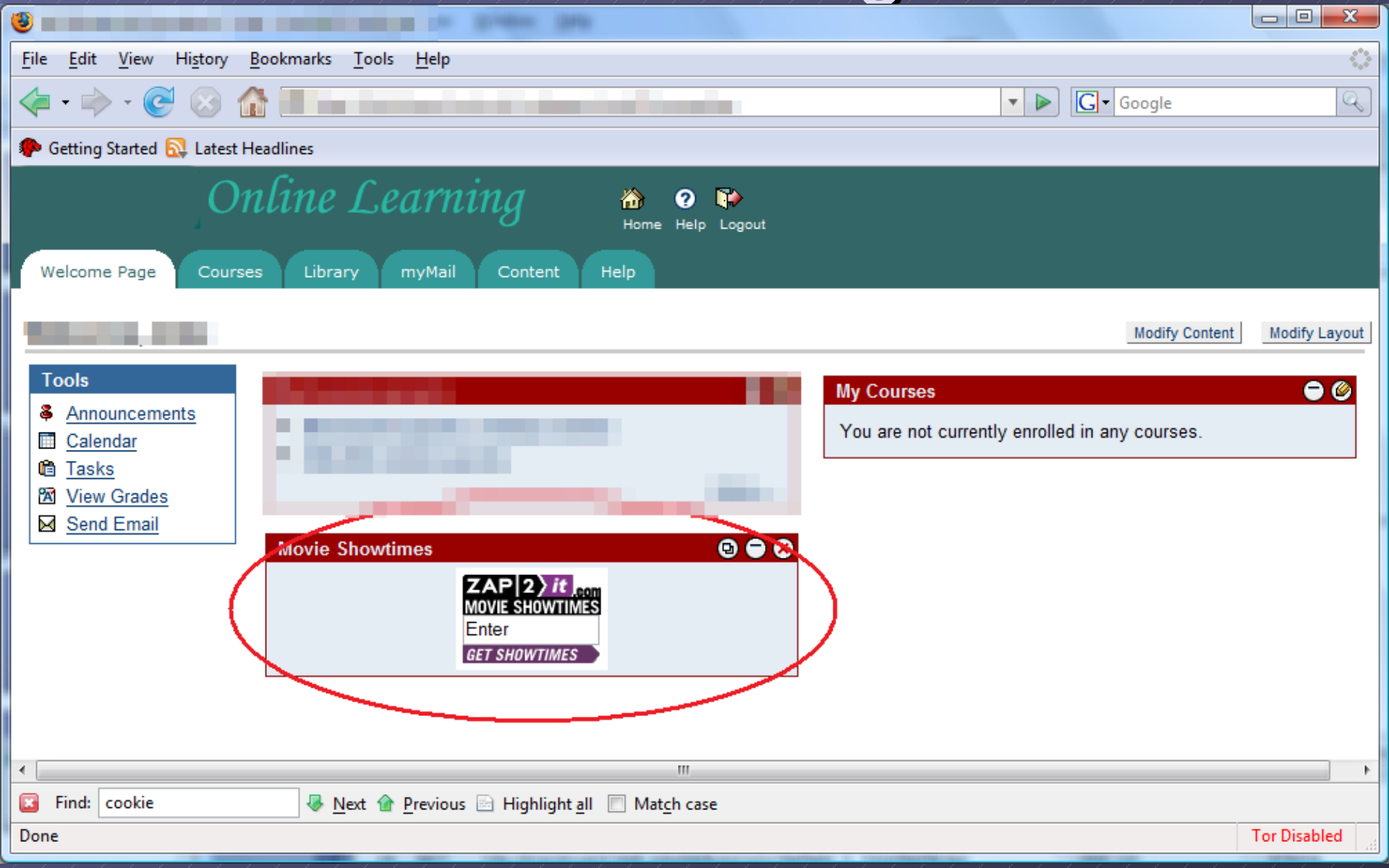
Hmmm - 131 not listed



Can we add it?


Untitled Session - Paros
File Edit View Analyse Report Tools Help
Sites
Request Response Trap
POST http:
Host:
&addModule=_131_1
126 POST
127 GET
128 GET
129 POST
130 GET
136 GET
200 OK
145ms
269ms
361ms
130ms
218ms
367ms
History Spider Alerts Output

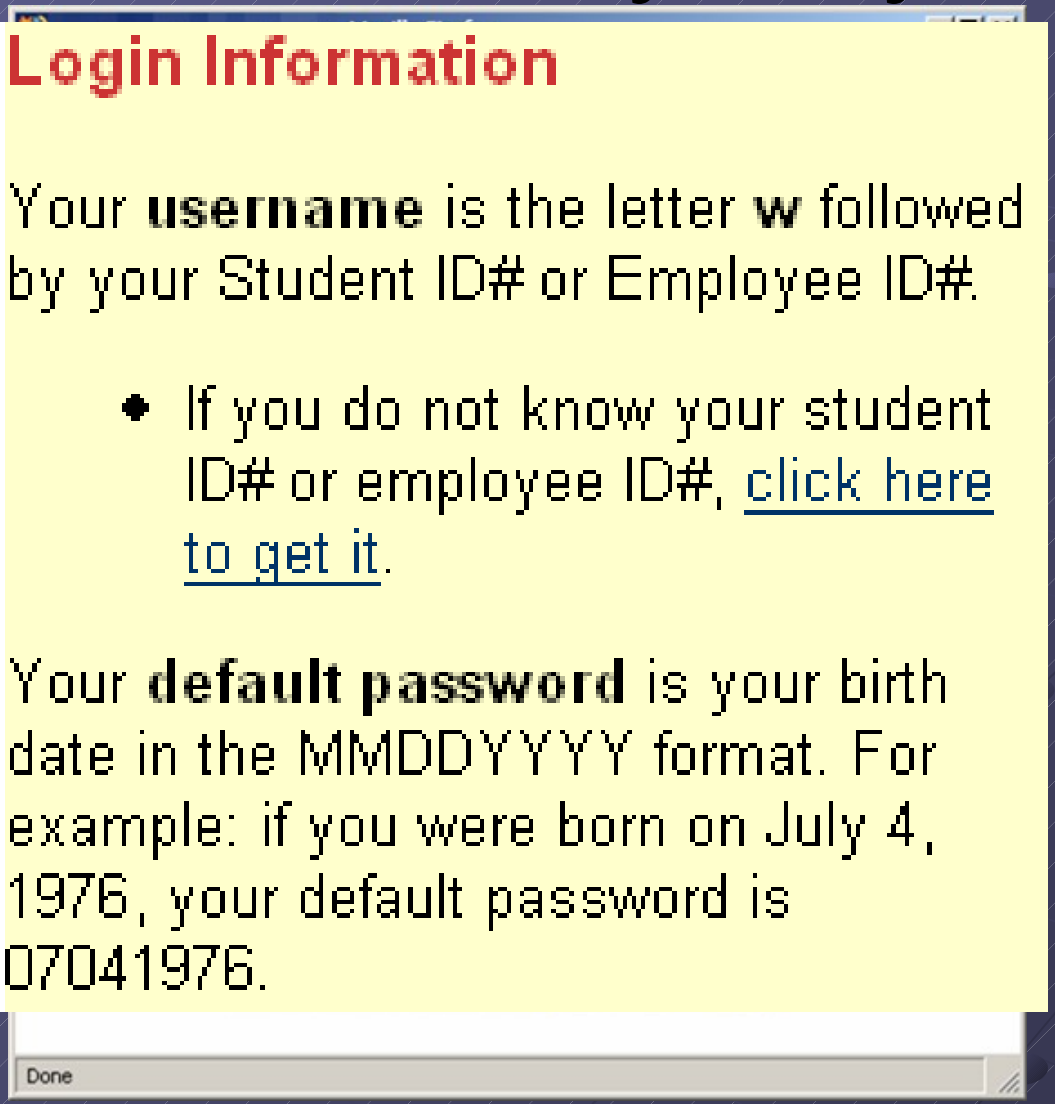
What did we get?



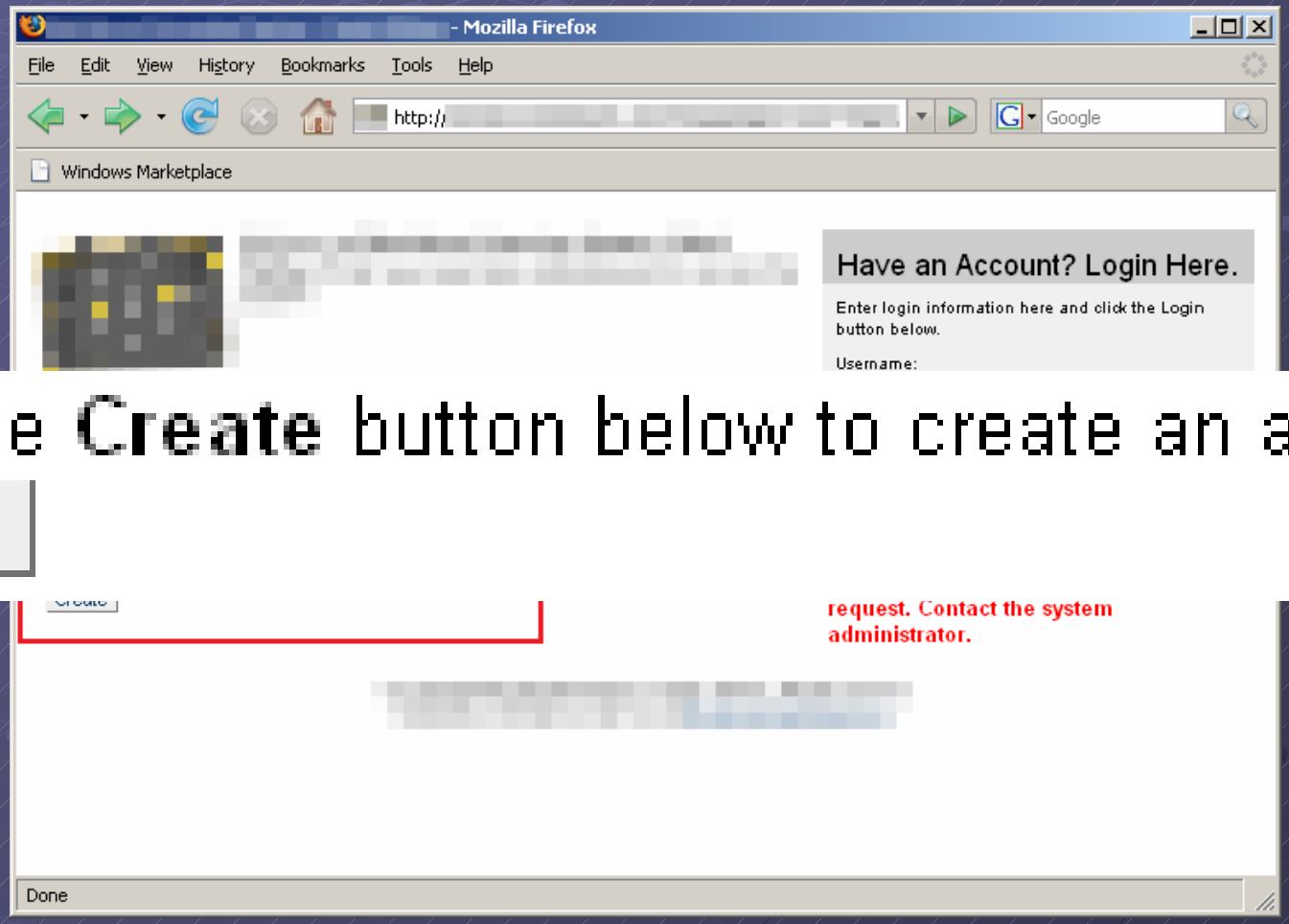
But testing requires an account – right?

- Do you have to brute force username and password scheme?
- Do you have to register for a class to learn these things?

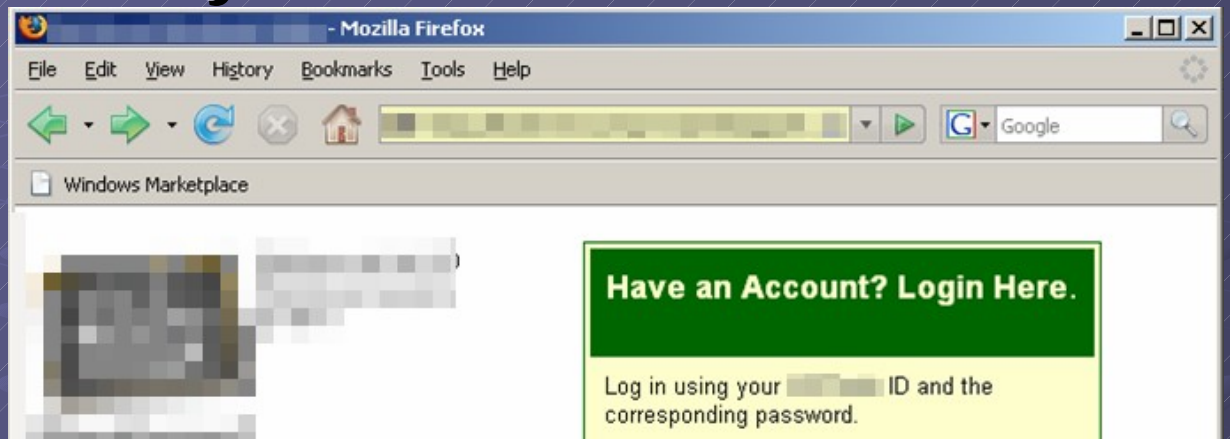
Brute Force – Why they tell you!



Register for a class? – No!

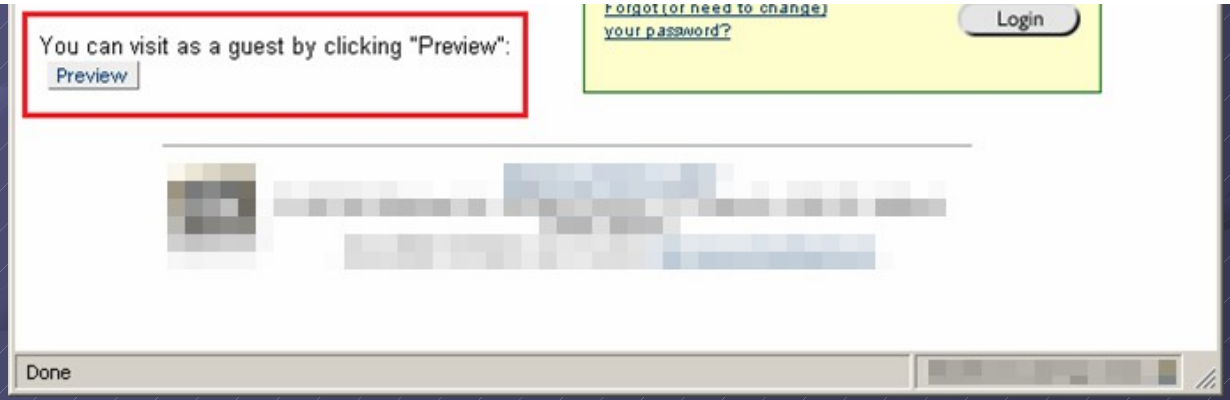


To lazy to create an account?



You can visit as a guest by clicking "Preview":

Preview



Other Applications.

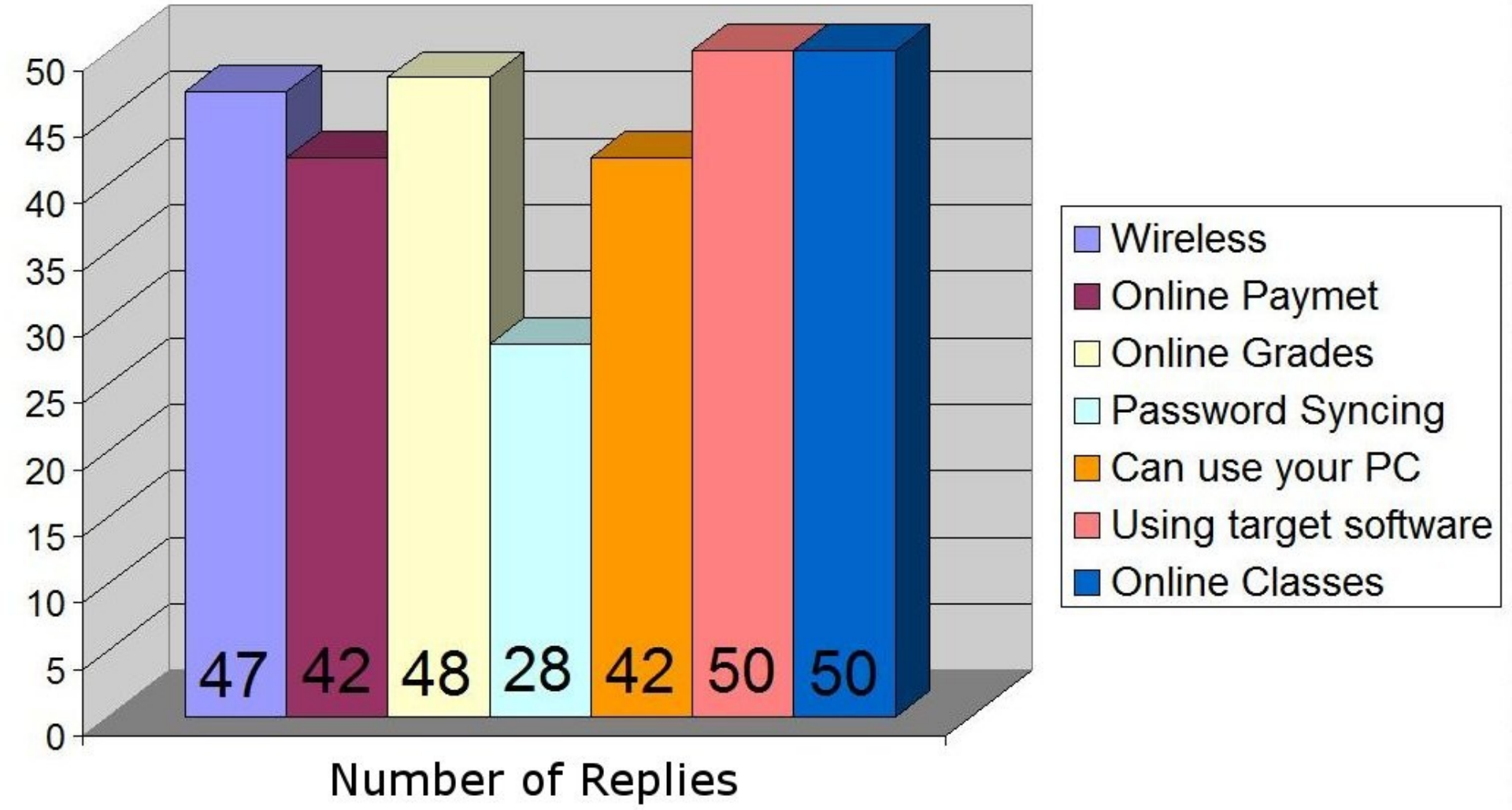
- How can you find other applications that these institutions are running?
- How do you know if they sync up the passwords?
- How do you know if they run wireless?

Ask them…

We sent them an Email!



E-mail Responses…




Japan military school raided over Aegis data
15-year-old Student Breaks into School Computer System
Downingtown school
By: Bogdan Popa, Security and Search Engines Editor
in Hiroshima on Saturday as part of an
about the Aegis missile
defense system.
Government agency exposes
Daily
University of Illinois Data Leak
"Well I just received an
Illinois. Apparent
attachm
ethnicity,
ber.
The Data Brea
Bates College s
Author: admin
00 students to delete and ignore
pen."
06
THE BIGGEST DATA DISASTER EVER
posted: Friday, November 30 at 05:13 am CT by Bob Sullivan
AHAHAHAHAHAHAHAHAHAHAHAHAHAHAHAHA.
this totally awesome screwup here.
on College reveals alumni data breach
By Matt Hines
Staff Writer, CNET News.com
Published: March 17, 2005, 9:22 AM PST

Apparently

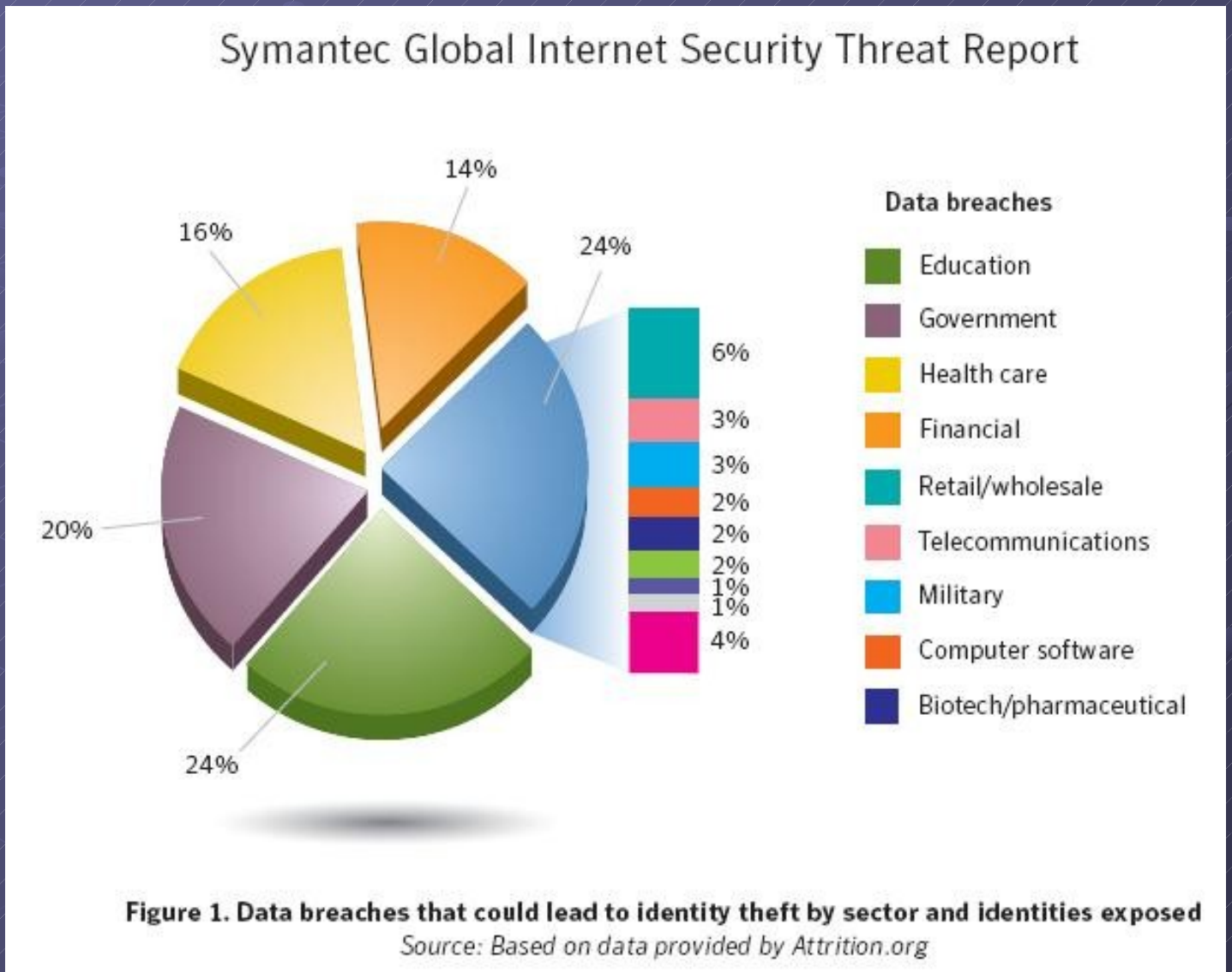


Figure 1. Data breaches that could lead to identity theft by sector and identities exposed

Source: Based on data provided by Attrition.org

What do we think is the cause?

- Educational institutions are fighting for your dollars.
- They feel the need to “keep up with the Jones’.”
- Security comes after functionality.
- Some colleges outsource their IT department and the company wants to standardize.

Many thanks to…

- Ben Dyer - researcher
- Samantha Ley – researcher
- Tom Burke - researcher
- Arcnet Dipswitch - researcher

Contact Us

hacking.esp@gmail.com