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 an 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

http://
### Wireshark Capture Of Login

<table>
<thead>
<tr>
<th>a8</th>
<th>.. G../.. .....B...</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>.d.P..[v .OK+.ZP.</td>
</tr>
<tr>
<td>41</td>
<td>%u..e= VABIAcKAA</td>
</tr>
<tr>
<td>41</td>
<td>CWBJAHMA TQB5AFAA</td>
</tr>
<tr>
<td>41</td>
<td>YQBZAHMA dwBVAHIA</td>
</tr>
<tr>
<td>54</td>
<td>ZAA%3D&amp;user_id=T</td>
</tr>
<tr>
<td>26</td>
<td>hisIsMyUserName&amp;</td>
</tr>
<tr>
<td>26</td>
<td>password =&amp;Login.</td>
</tr>
<tr>
<td>26</td>
<td>x=26&amp;Login.in.y=7..</td>
</tr>
</tbody>
</table>

This table includes captured data from a Wireshark analysis of a login process, showing hexadecimal values and strings that were transmitted or received during the login attempt.
Login page code – Oh, it’s using javascript!

```javascript
<script language="JAVASCRIPT">

document.cookie = "cookies_enab:
if (!document.cookie) {
    document.location.href="/nocoo

document.cookie = "cookies_enab
```
What if javascript is off?
Capture with javascript on...
What is javascript doing?

```javascript
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!

The Form.SizeLimit is 10000000 bytes. Please, do not post source data from the Base64 string:

The displayed string is not legible.

Type (or copy paste) some text to a textbox hellow. The text encode to a Base64.

The displayed string is not legible.
How many schools use this ESP insecurely?
Over 34,000!

about 34,100 for a
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?

```html
</script>

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;
```
What’s this session ID doing?
Here, logged in as Bob.
Here is Bob’s session Id, pasted below is Jan’s.

@@@38de10cdd6088387051f81b4b97f2b00|
Bob’s session ID replaced with Jan’s.

Host: 10.1.60.10
Cookie: JSESSIONID=07549C7A46546191695745C25607EBBC; session_id=@@38de10cdd6088387051f81b4b97f2b00] JSESSIONID=D23C047D779E3CD52C0C898A18CA5A1E
I became Jan!
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?

```html
<script>alert('XSS Vulnerable?')</script>
```
Yes!

[!] The page at http://example.com says: [!]

XSS Vulnerable?

OK

You are not currently participating in any courses.

My Tasks
No tasks due.

Search the Web
Google Search

Find: cookie  Next  Previous  Highlight all  Match case
Done
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.

- Remember the session hijacking!
Surely there are no other issues!

- How do these applications work?
- What else can we do?
Find some hidden capabilities!

Welcome Page
- Notes
  Displays notes user can edit.
- Report Card
  Displays total grades.
- Search the Web
  Search the Web with the Google search engine.
- SOLO Orientations
- Technical Support
- Thesaurus
- Thesaurus
- Time
  Weekly news and features from Time magazine.
- Travel
  Make reservations for flights, hotels, and car rentals.
- Weather
  Look up weather information for any city from Weather.com.

Submit
Click Submit to finish. Click Cancel to quit.
Hmmm - 131 not listed
Can we add it?

&addModule=1311
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!

Login Information

Your **username** is the letter *w* followed by your Student ID# or Employee ID#.

- If you do not know your student ID# or employee ID#, [click here to get it](#).

Your **default password** is your birth date in the MMDDYYYY format. For example: if you were born on July 4, 1976, your default password is **07041976**.
Register for a class? – No!

Click the Create button below to create an account.
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...
Are breaches that common?

How often do these breaches happen?

What type of information is leaked?

The biggest data disaster ever

posted: Friday, November 30 at 05:15 am CT by Bob Sullivan

Bates College reveals alumni data breach

By Matt Hines
Staff Writer, CNET News.com
Published: March 17, 2005, 9:22 AM PST
Symantec Global Internet Security Threat Report

Data breaches
- Education: 16%
- Government: 14%
- Health care: 24%
- Financial: 20%
- Retail/wholesale: 16%
- Telecommunications: 4%
- Military: 2%
- Computer software: 2%
- Biotech/pharmaceutical: 1%

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