SECURITY
TALK
SERIES

Using Standards-Based Internet Explorer Features to Protect Your Web Apps

Pete LePage
Senior Product Manager
Microsoft Corporation

Agenda

- **A Little History**
- Securing Your Infrastructure
- Trust User Input at Your Own Peril
- SQL Injection Attacks
- Cross-Site Scripting (XSS) Attacks
- ClickJacking Attacks
- Native JavaScript Object Notation (JSON)
- Building Mashups

PROPRIETE CERN
CERN
This machine is a
DO NOT POWE
DOWN!!
Information Management: A Proposal
PROPRIETE CERN

The security architecture of the Web platform, until recently, was largely an afterthought

We could block nearly 100% of exploits by removing one component from the system…

Or, we could block a majority of exploits by removing a different component from the system…

Making the Correct Tradeoffs Is Hard

Internet Explorer 8 Security Vision

Windows® Internet Explorer® 8: secure by default.

- Security Feature Improvements
  - Create security features that address the top vulnerabilities today and in the future
- Secure Features
  - Reduce attack surface of existing code by closing legacy holes
  - Apply security-focused rigors against new code
- Provide Security and Compatibility
  - Users understand that improved security is a reason to upgrade

Agenda

SECURITY
TALK
SERIES

A Little History

▶ **Securing Your Infrastructure**

Trust User Input at Your Own Peril

SQL Injection Attacks

Cross-Site Scripting Attacks

ClickJacking Attacks

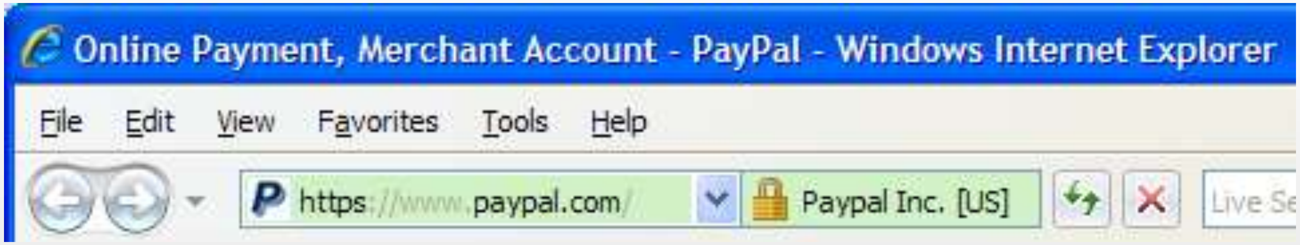
Native JSON

Building Mashups

Creating Secure Connections

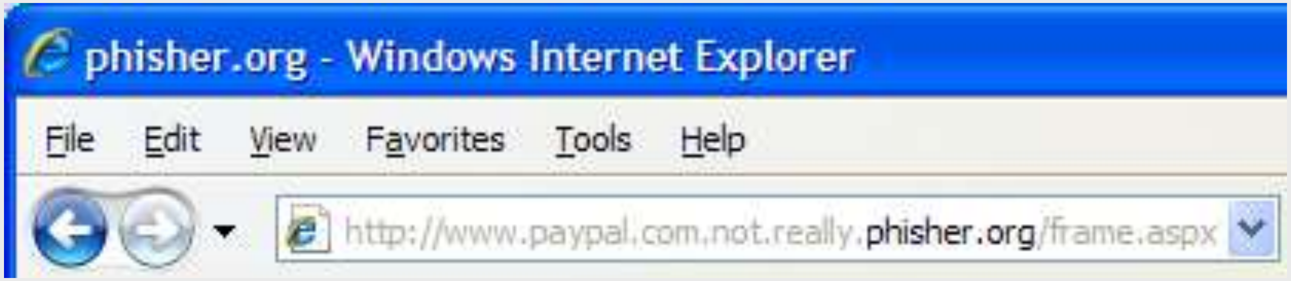
Domain Highlighting

Help users to quickly and accurately determine whether or not they are visiting the expected site


Online Payment, Merchant Account - PayPal - Windows Internet Explorer

https://www.paypal.com/

Paypal Inc. [US]


phisher.org - Windows Internet Explorer

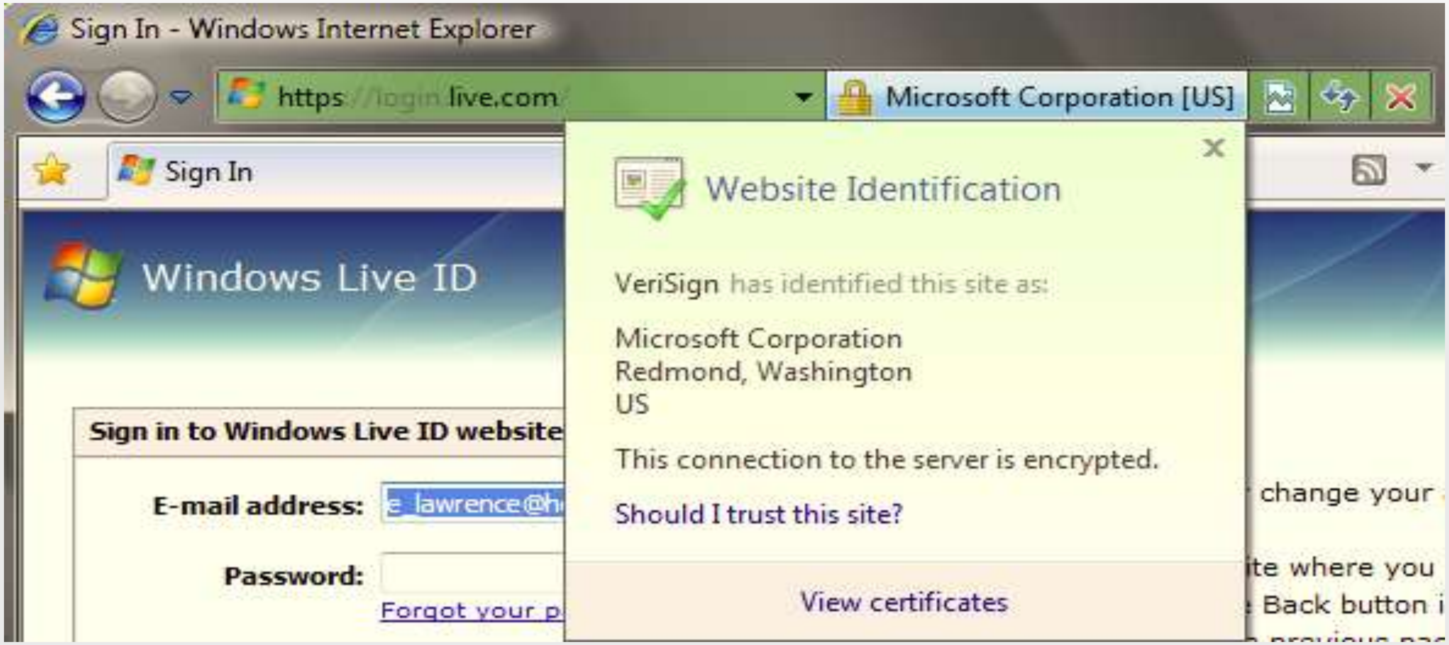
http://www.paypal.com.not.really.phisher.org/frame.aspx

Extended Validation

Supported by all major browsers

- Windows® Internet Explorer® 7+, Firefox 3+, Opera 9+, Chrome 3+, and Safari 3+.

Over 10,000 sites with extended validation certificates.



Website Identification

VeriSign has identified this site as:

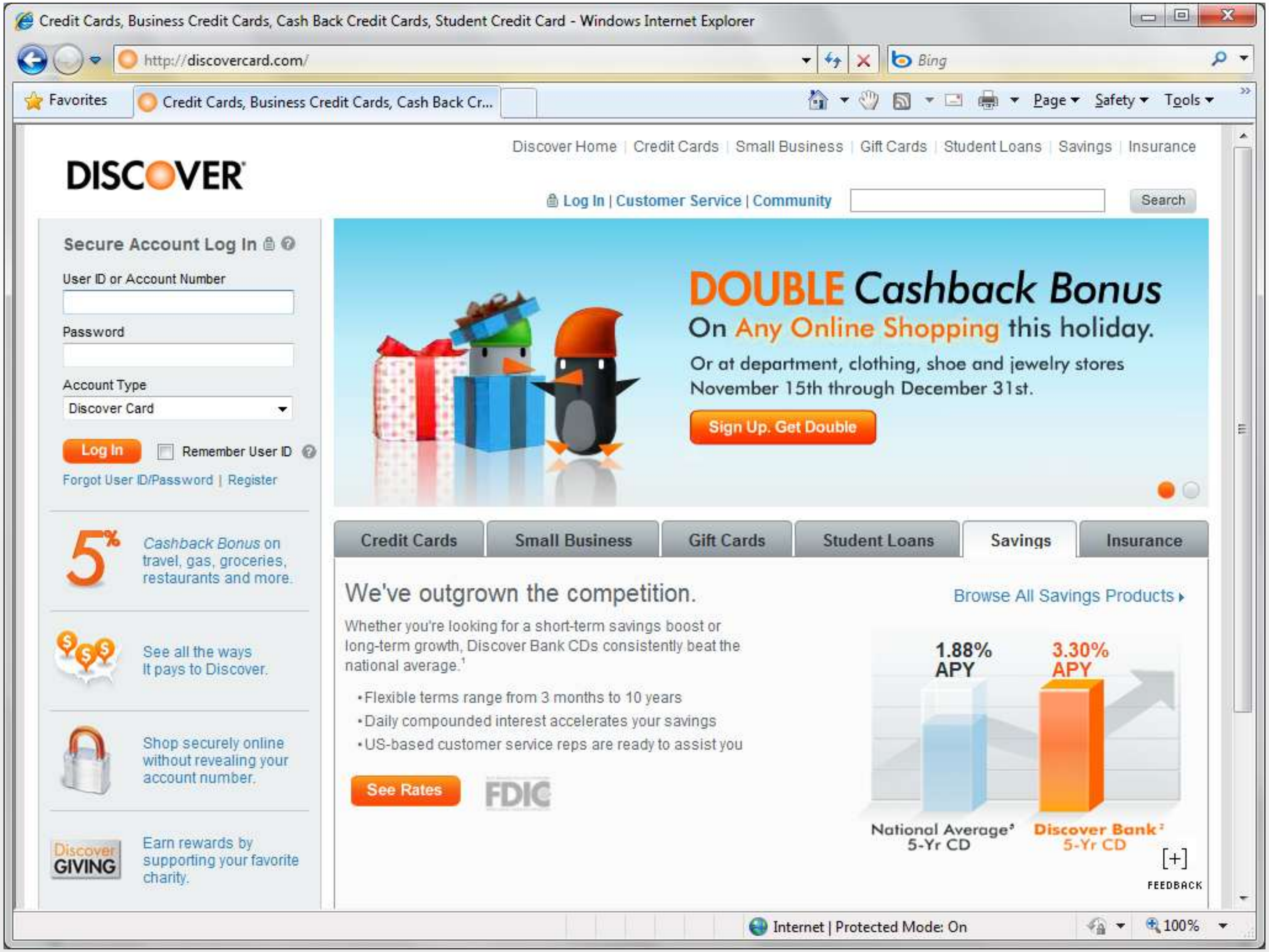
Microsoft Corporation
Redmond, Washington
US

This connection to the server is encrypted.

Should I trust this site?

View certificates

Insecure Login Form?


Credit Cards, Business Credit Cards, Cash Back Credit Cards, Student Credit Card - Windows Internet Explorer
http://discovercard.com/
Bing
Favorites
Credit Cards, Business Credit Cards, Cash Back Cr...
Page
Safety
Tools
DISCOVER
Discover Home | Credit Cards | Small Business | Gift Cards | Student Loans | Savings | Insurance
Log In | Customer Service | Community
Search
Secure Account Log In
User ID or Account Number
Password
Account Type
Discover Card
Log In
Remember User ID
Forgot User ID/Password | Register
Sign Up. Get Double
Credit Cards
Small Business
Gift Cards
Student Loans
Savings
Insurance
Browse All Savings Products
See Rates
FDIC
[+]
FEEDBACK
Internet | Protected Mode: On
100%

5% Cashback Bonus on travel, gas, groceries, restaurants and more.

See all the ways It pays to Discover.

Shop securely online without revealing your account number.

Earn rewards by supporting your favorite charity.

DOUBLE Cashback Bonus

On Any Online Shopping this holiday.

Or at department, clothing, shoe and jewelry stores November 15th through December 31st.

We've outgrown the competition.

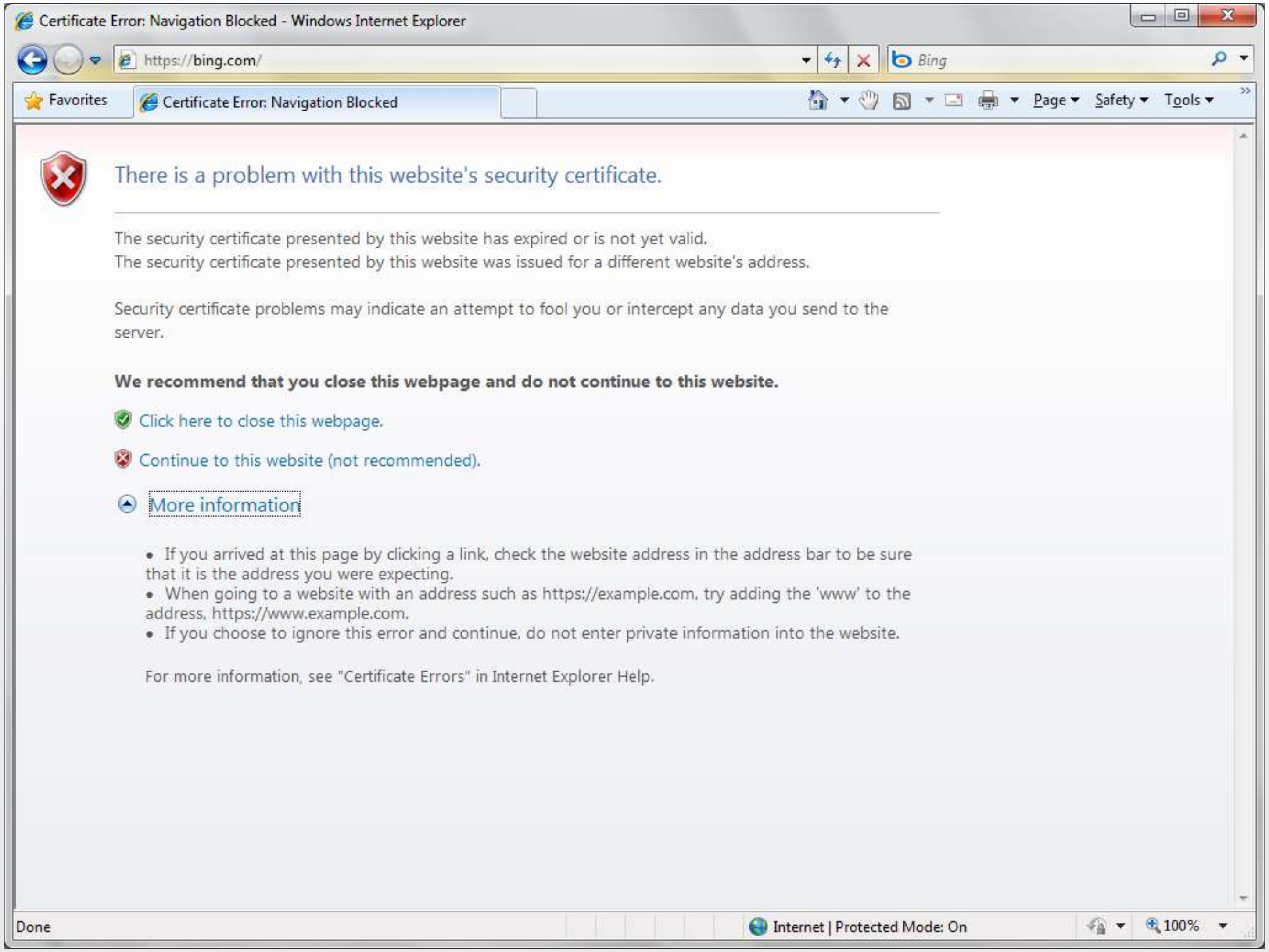
Whether you're looking for a short-term savings boost or long-term growth, Discover Bank CDs consistently beat the national average.[1]

- Flexible terms range from 3 months to 10 years
- Daily compounded interest accelerates your savings
- US-based customer service reps are ready to assist you

1.88% APY National Average[3] 5-Yr CD

3.30% APY Discover Bank[2] 5-Yr CD

Certificate Mismatch



Certificate Error: Navigation Blocked - Windows Internet Explorer
https://bing.com/
Bing
Favorites
Certificate Error: Navigation Blocked
Page ▾
Safety ▾
Tools ▾

There is a problem with this website's security certificate.

The security certificate presented by this website has expired or is not yet valid.
The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

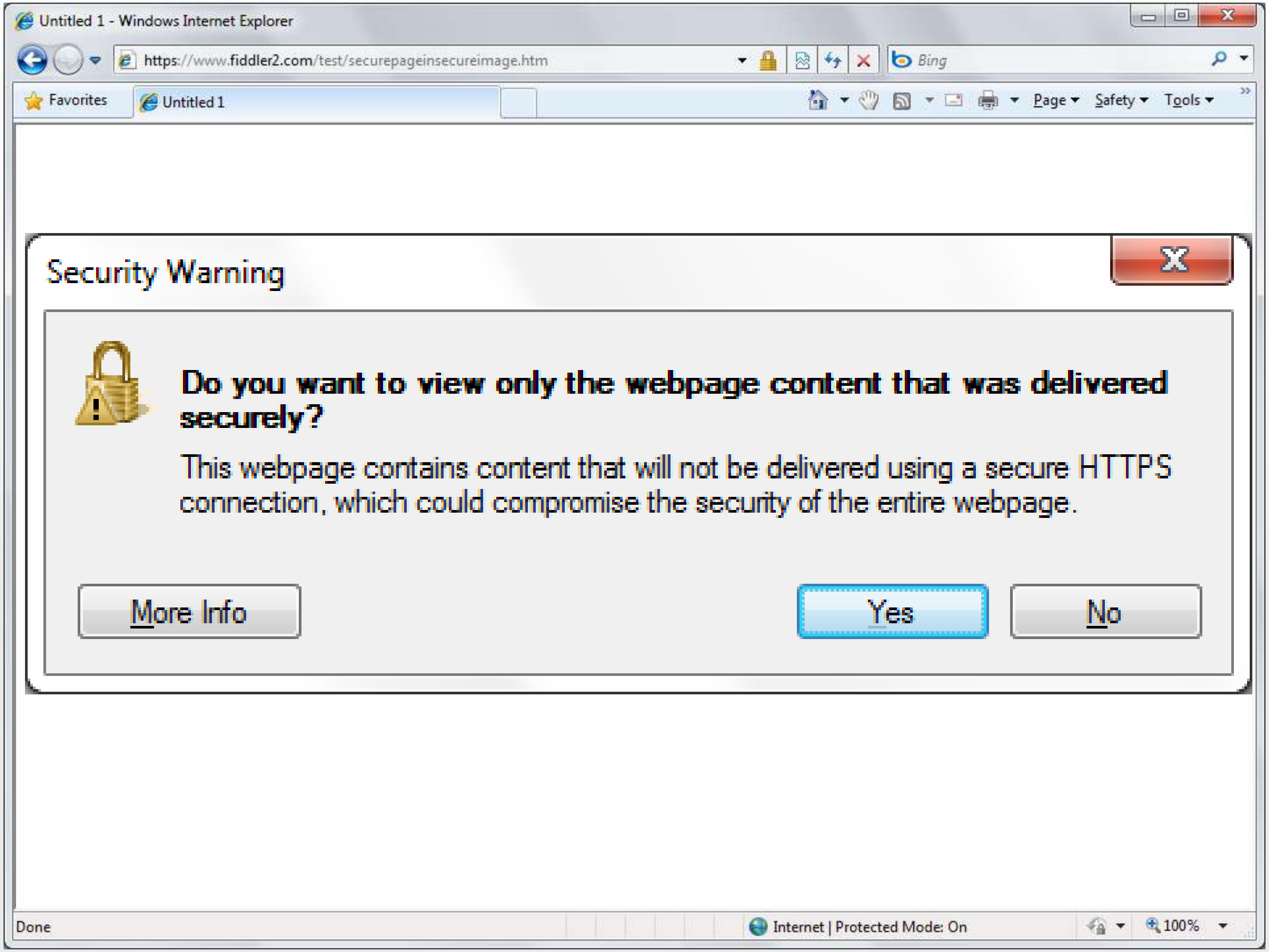
Continue to this website (not recommended).

More information

- If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
- When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.
- If you choose to ignore this error and continue, do not enter private information into the website.

For more information, see "Certificate Errors" in Internet Explorer Help.

Be Aware of Mixed Content



Untitled 1 - Windows Internet Explorer
https://www.fiddler2.com/test/securepageinsecureimage.htm
Bing
Favorites
Untitled 1
Page
Safety
Tools

Security Warning

Do you want to view only the webpage content that was delivered securely?

This webpage contains content that will not be delivered using a secure HTTPS connection, which could compromise the security of the entire webpage.

More Info
Yes
No
Done
Internet | Protected Mode: On
100%

Mixed Content Example

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en"
  lang="en">

<head>
  <meta http-equiv="X-UA-Compatible"
  content="IE=EmulateIE8" />
  <meta http-equiv="Content-Type" content="text/html;
  charset=iso-8859-1" />
  <link rel="shortcut icon" href="/favicon.ico" />
  <link href="http://example.com/CssReset.css"
  rel="stylesheet" type="text/css" />
  <link href="styles.css" rel="stylesheet" />
  <title>
...
```

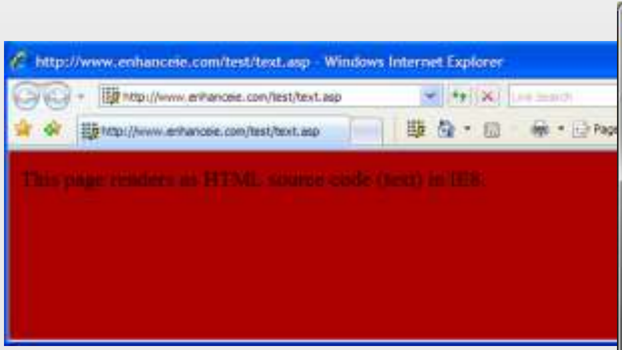
MIME-Sniffing

No upsniff from image/*

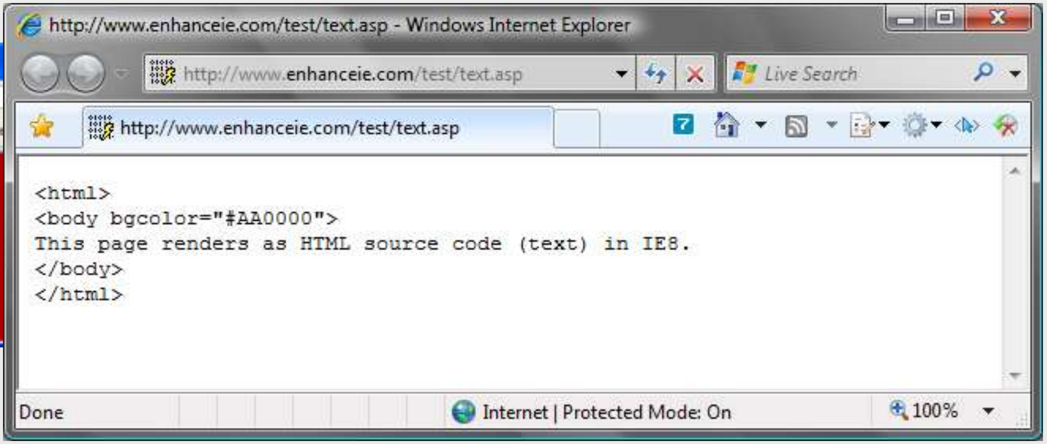
X-Content-Type-Options: nosniff

Option to force file save:

```
Content-Disposition:
attachment;filename=“foo.doc”;
X-Download-Options: NoOpen
```

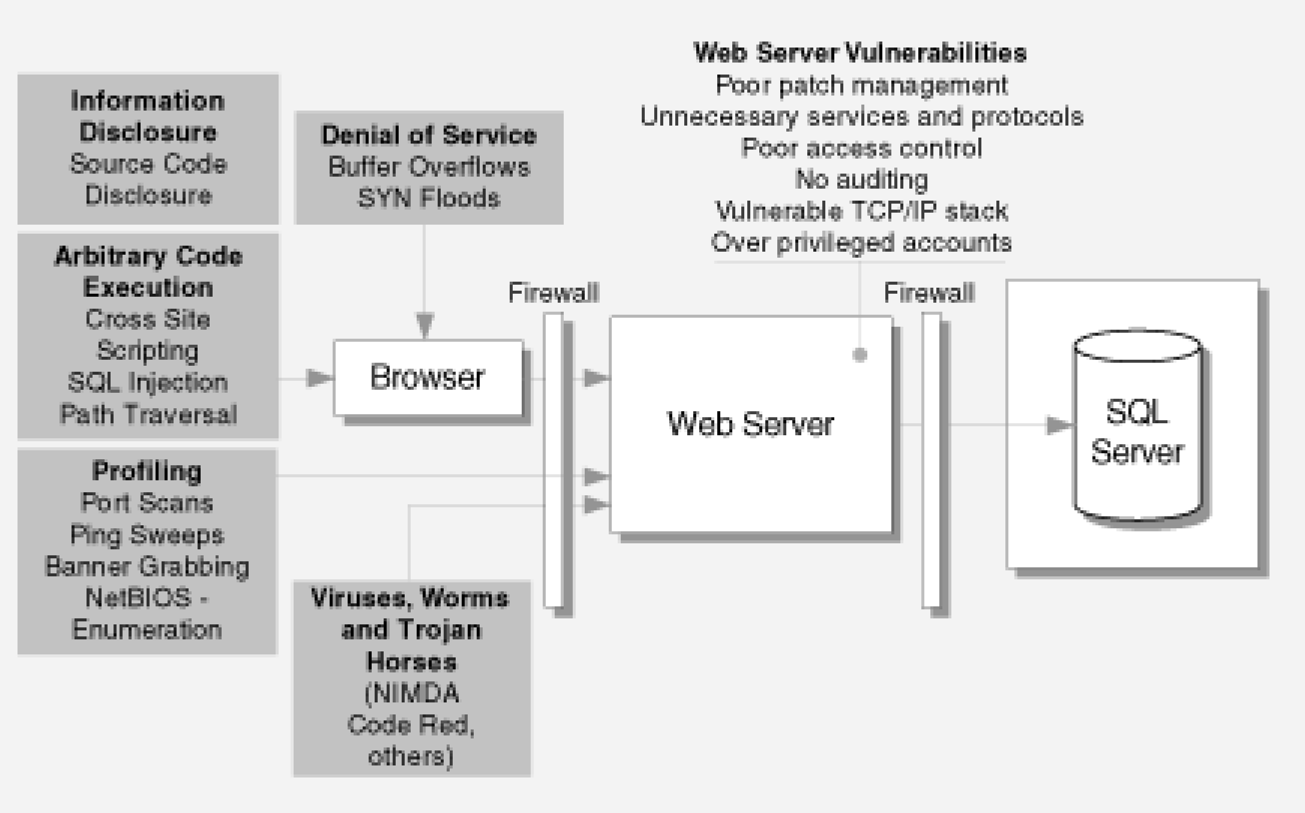

http://www.enhanceie.com/test/text.asp - Windows Internet Explorer
http://www.enhanceie.com/test/text.asp

This page renders as HTML source code (text) in IE8.


http://www.enhanceie.com/test/text.asp - Windows Internet Explorer
http://www.enhanceie.com/test/text.asp
Live Search
http://www.enhanceie.com/test/text.asp
Done
Internet | Protected Mode: On
100%

```
<html>
<body bgcolor="#AA0000">
This page renders as HTML source code (text) in IE8.
</body>
</html>
```

Keep Your Servers Secure



Best Practices

- Ensure you're using Secure Sockets Layer (SSL) when appropriate
- Check users aren't being prompted for mixed content?
- Make sure your servers up to date
- Use best-practices for user accounts and passwords

Agenda

- A Little History
- Securing Your Infrastructure
- **Trust User Input at Your Own Peril**
- SQL Injection Attacks
- Cross-Site Scripting Attacks
- ClickJacking Attacks
- Native JSON
- Building Mashups

Assume All User Input Is Evil

toStaticHTML() function

Client-side string sanitization, based on the Microsoft Anti-XSS Library.

```
window.toStaticHTML("This is some <b>HTML</b> with
embedded script following...
<script>alert('bang!');</script>!");
```

Returns:

```
This is some <b>HTML</b> with embedded script
following... !
```

Best Practices

- Don’t rely on client-side validation for input
- Use toStaticHTML() as one method to sanitize data

Agenda

SECURITY
TALK
SERIES

A Little History

Securing Your Infrastructure

Trust User Input at Your Own Peril

SQL Injection Attacks

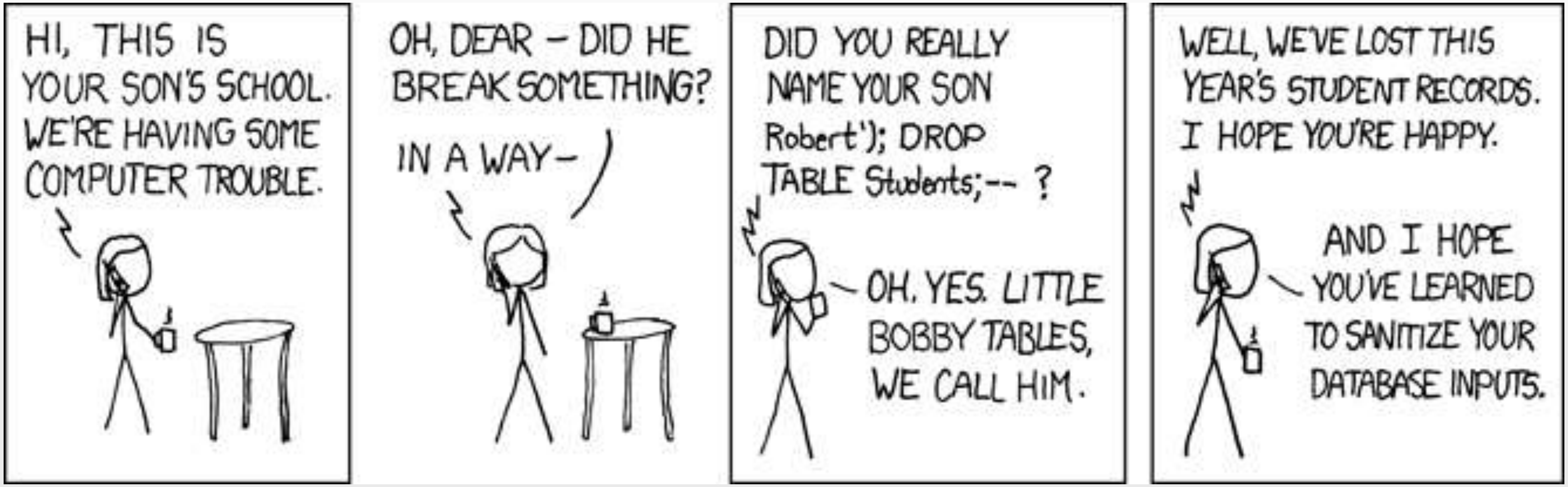
Cross-Site Scripting Attacks

ClickJacking Attacks

Native JSON

Building Mashups

SQL Injection Attacks


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Source: http://xkcd.com/327/

Protecting Against SQL Injection

Constrain User Input

- Use Type-Safe SQL Parameters

```
SqlDataAdapter myCommand = new SqlDataAdapter("AuthorLogin", conn);
myCommand.SelectCommand.CommandType = CommandType.StoredProcedure;
SqlParameter parm = myCommand.SelectCommand.Parameters.Add("@au_id",
SqlDbType.VarChar, 11);
parm.Value = Login.Text;
```

Using Escape Routines

```
private string SafeSqlLiteral(string inputSQL)
{
    return inputSQL.Replace("'", "''");
}
```

Best Practices

- Assume all user input is evil!
- Use parameterized statements instead of building queries

Agenda

A Little History

Securing Your Infrastructure

Trust User Input at Your Own Peril

SQL Injection Attacks

Cross-Site Scripting Attacks

ClickJacking Attacks

Native JSON

Building Mashups

“XSS is the new buffer overflow.”

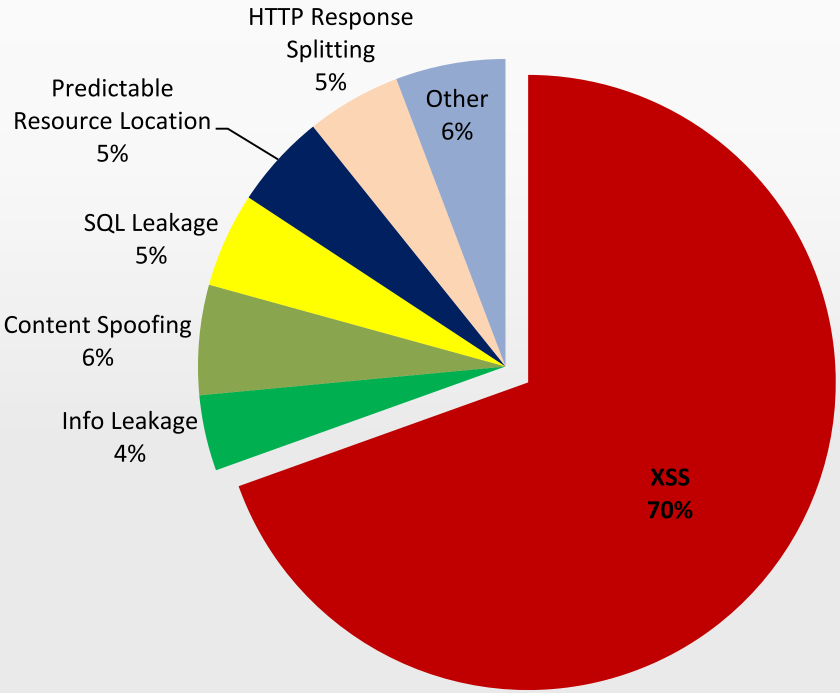
-Researcher Bryan Sullivan

- Steal cookies
- Log keystrokes
- Deface sites
- Steal credentials (of a sort)
- Port-scan the intranet

- Launch cross-site request forgery (CSRF)
- Steal browser history
- Abuse browser/AX vulnerabilities
- Evade phishing filters
- Circumvent HTTPS

Threat Landscape

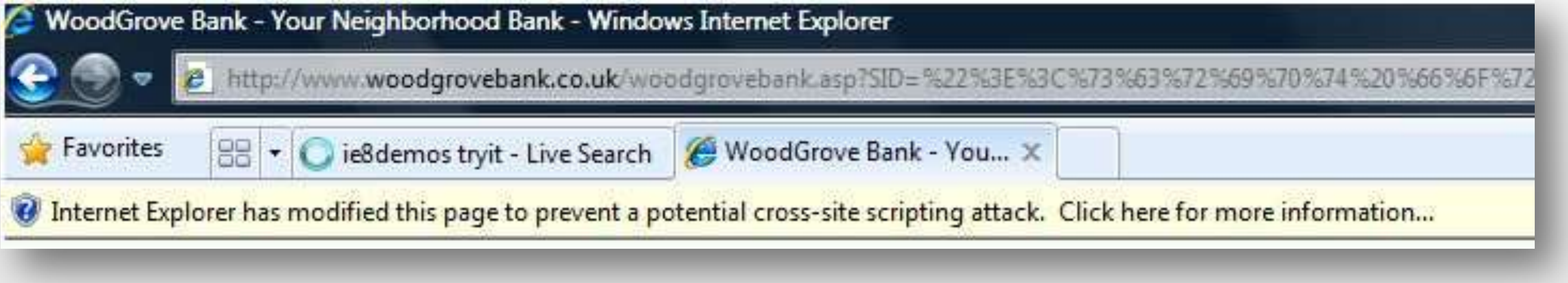
Web Site Vulnerabilities by Class



Source: Whitehat Security 8/08

Cross-Site Scripting Filter

Identifies and prevents majority of XSS reflection attacks


WoodGrove Bank - Your Neighborhood Bank - Windows Internet Explorer
Favorites
ie8demos tryit - Live Search
WoodGrove Bank - You...

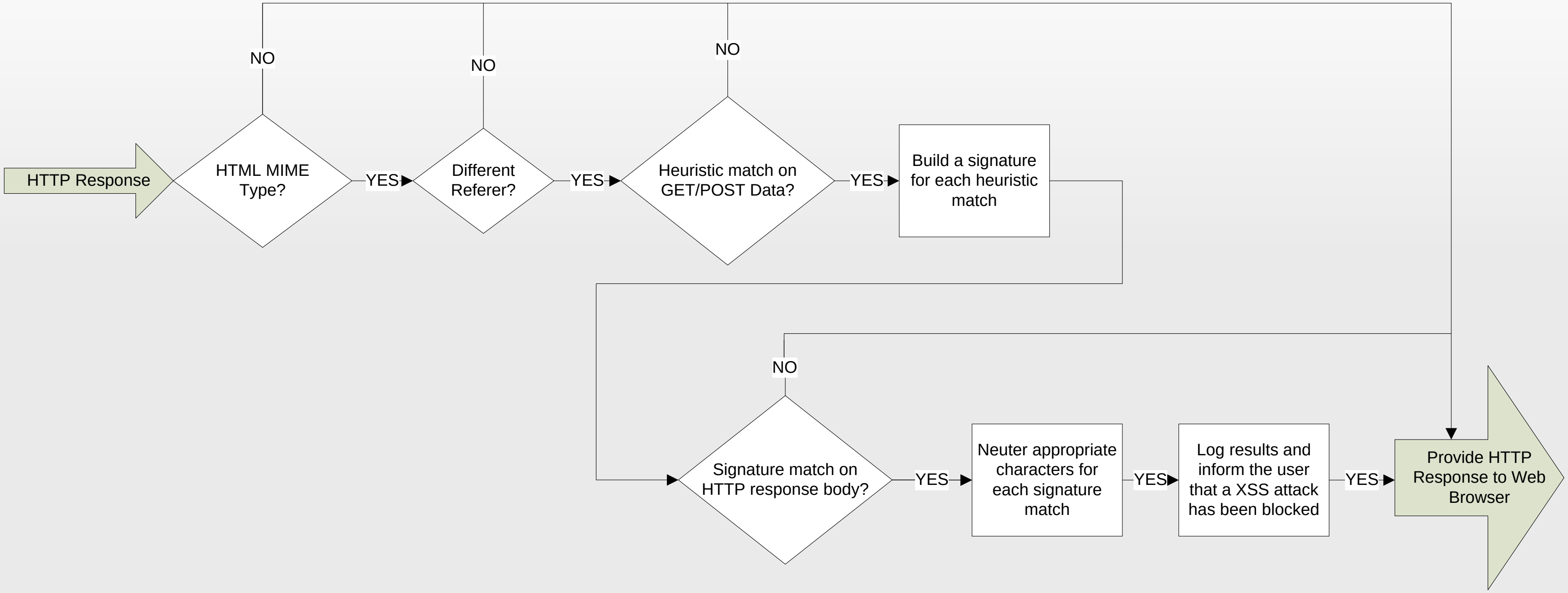
http://www.woodgrovebank.co.uk/woodgrovebank.asp?SID=%22%3E%3C%73%63%72%69%70%74%20%66%6F%72

Internet Explorer has modified this page to prevent a potential cross-site scripting attack. Click here for more information...

XSS Filter

Intercept and prevent majority of Type-1 XSS attacks

Great performance and site compatibility


HTTP Response
HTML MIME Type?
NO
YES
Different Referer?
NO
YES
Heuristic match on GET/POST Data?
NO
YES
Build a signature for each heuristic match
NO
Signature match on HTTP response body?
YES
Neuter appropriate characters for each signature match
YES
Log results and inform the user that a XSS attack has been blocked
YES
Provide HTTP Response to Web Browser

XSS Filter

Original script:

```
<SCRIPT src=http://hackersite.ie8demos.com/snoop.js>
```

Generated Signature:

```
<SC{R}IPT¤src¤=>
```

Neutered Script

```
<SC#IPT src=http://hackersite.ie8demos.com/snoop.js>
```

Best Practices

- Use the ASP.NET Anti-Cross-Site Scripting Library
  - http://msdn.microsoft.com/en-us/security/aa973814.aspx
- Disable US-ASCII codepage
- Disable sniffing of UTF-7 codepage
- Fix other codepage-related bugs
- Disable Cascading Style Sheets (CSS) expressions in Standards mode

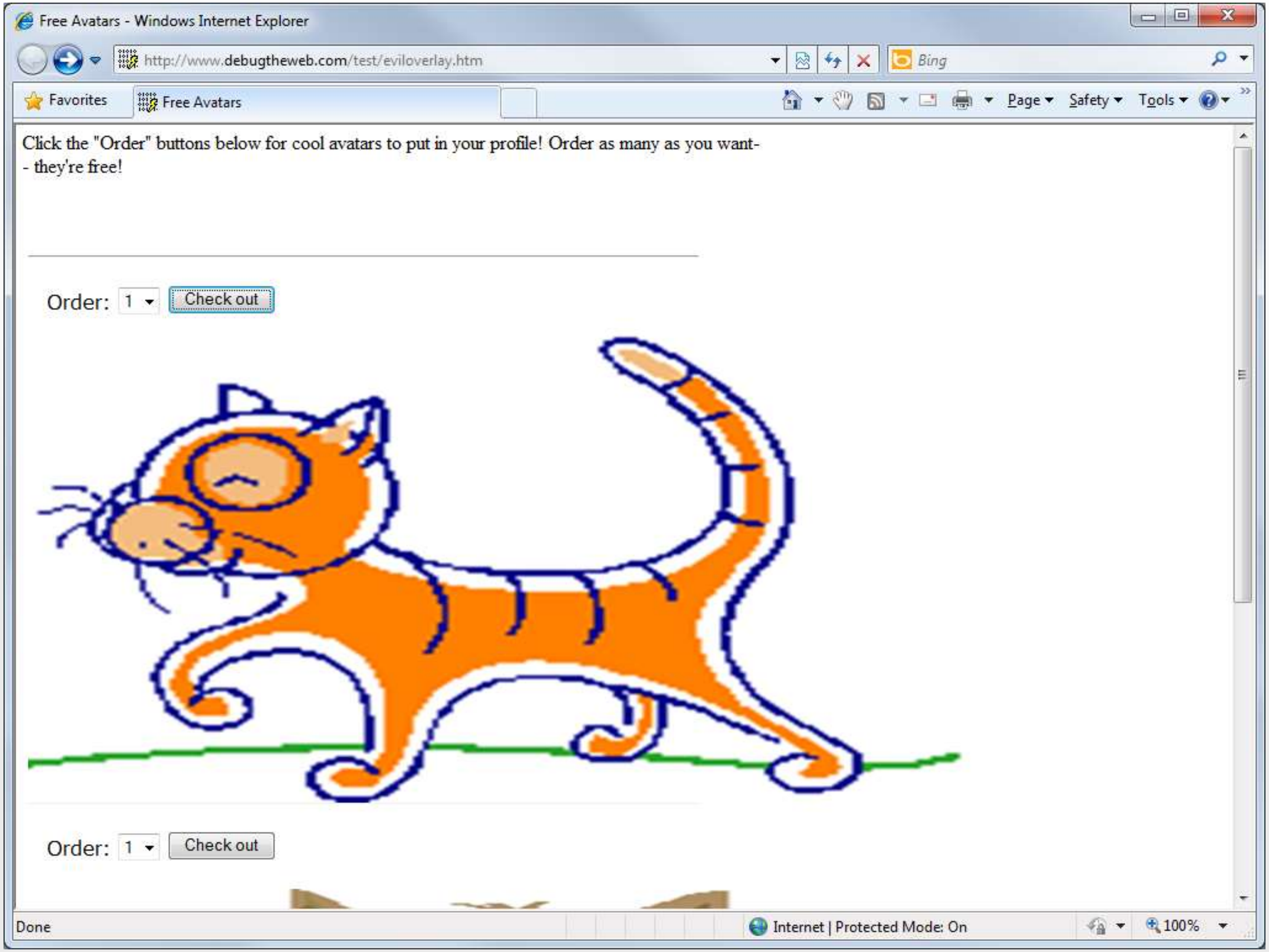
Agenda

- A Little History
- Securing Your Infrastructure
- Trust User Input at Your Own Peril
- SQL Injection Attacks
- Cross-Site Scripting Attacks
- **ClickJacking Attacks**
- Native JSON
- Building Mashups

ClickJacking

ClickJacking Demo

ClickJacking – Free Avatars?



Free Avatars - Windows Internet Explorer
http://www.debugtheweb.com/test/eviloverlay.htm
Bing
Favorites
Free Avatars
Page ▾ Safety ▾ Tools ▾

Click the "Order" buttons below for cool avatars to put in your profile! Order as many as you want--they're free!

Order: 1 ▾ Check out

Order: 1 ▾ Check out

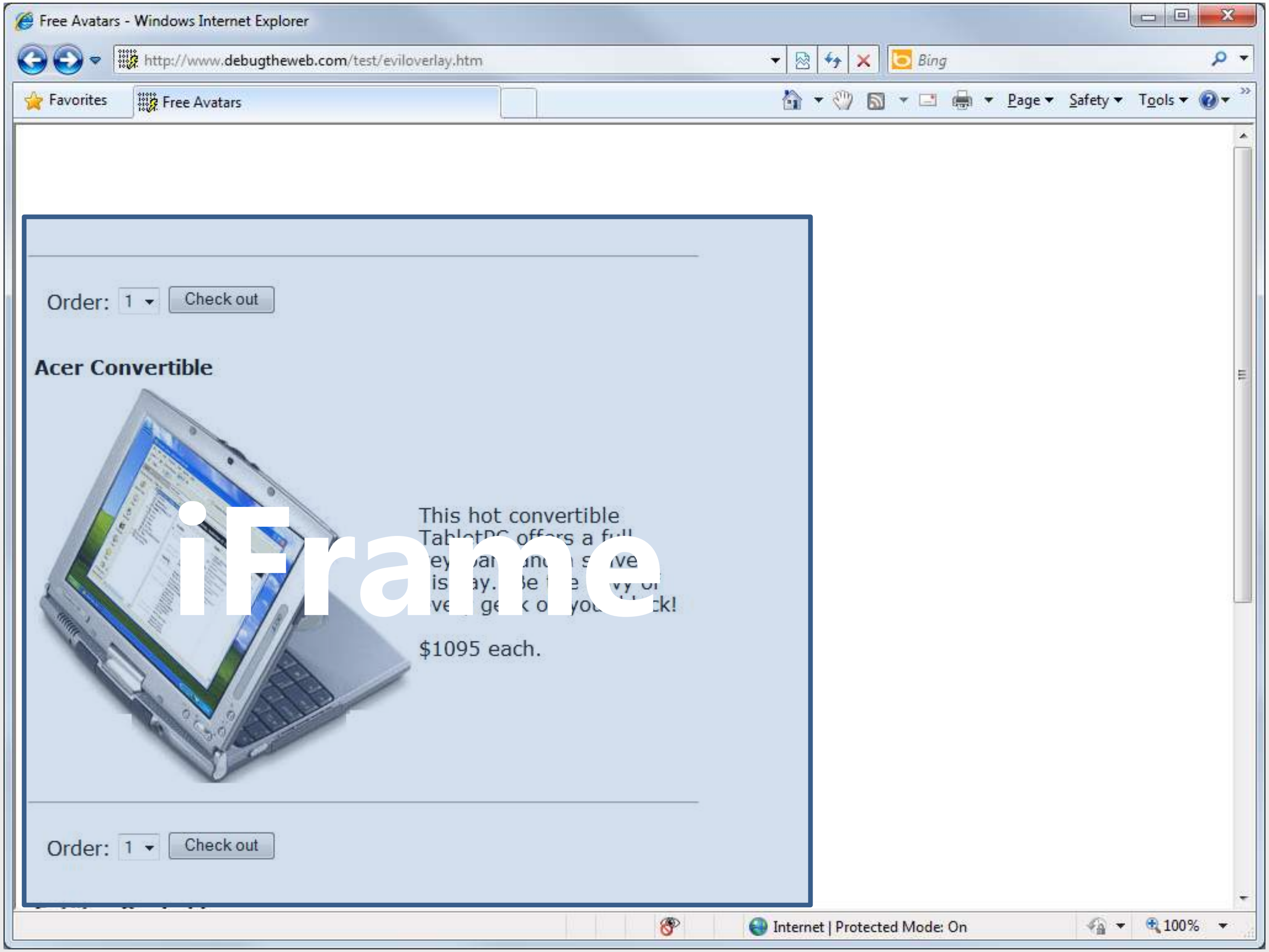
Done
Internet | Protected Mode: On
100%

ClickJacking – The Evil Overlay

```
<iframe AllowTransparency="Yes"
  style="position:absolute; left:0px; top:30px;
  width: 581px; height: 1000px; z-index: 5;"
  id="I1" src="http://example.com" name="I1"
  border="0" frameborder="0" class="style2">
 Frames disabled.
</iframe>


<div style="margin: 10px; position: absolute;
  top:160px; left:0px; width:600px;
  height:380px; background: white; z-index:10">
 <img height="380" src="cat.gif" width="760" />
</div>
```

ClickJacking – The Evil Overlay


Free Avatars - Windows Internet Explorer
http://www.debugtheweb.com/test/eviloverlay.htm
Bing
Favorites
Free Avatars
Page
Safety
Tools
Internet | Protected Mode: On
100%

Order: 1 Check out

Acer Convertible

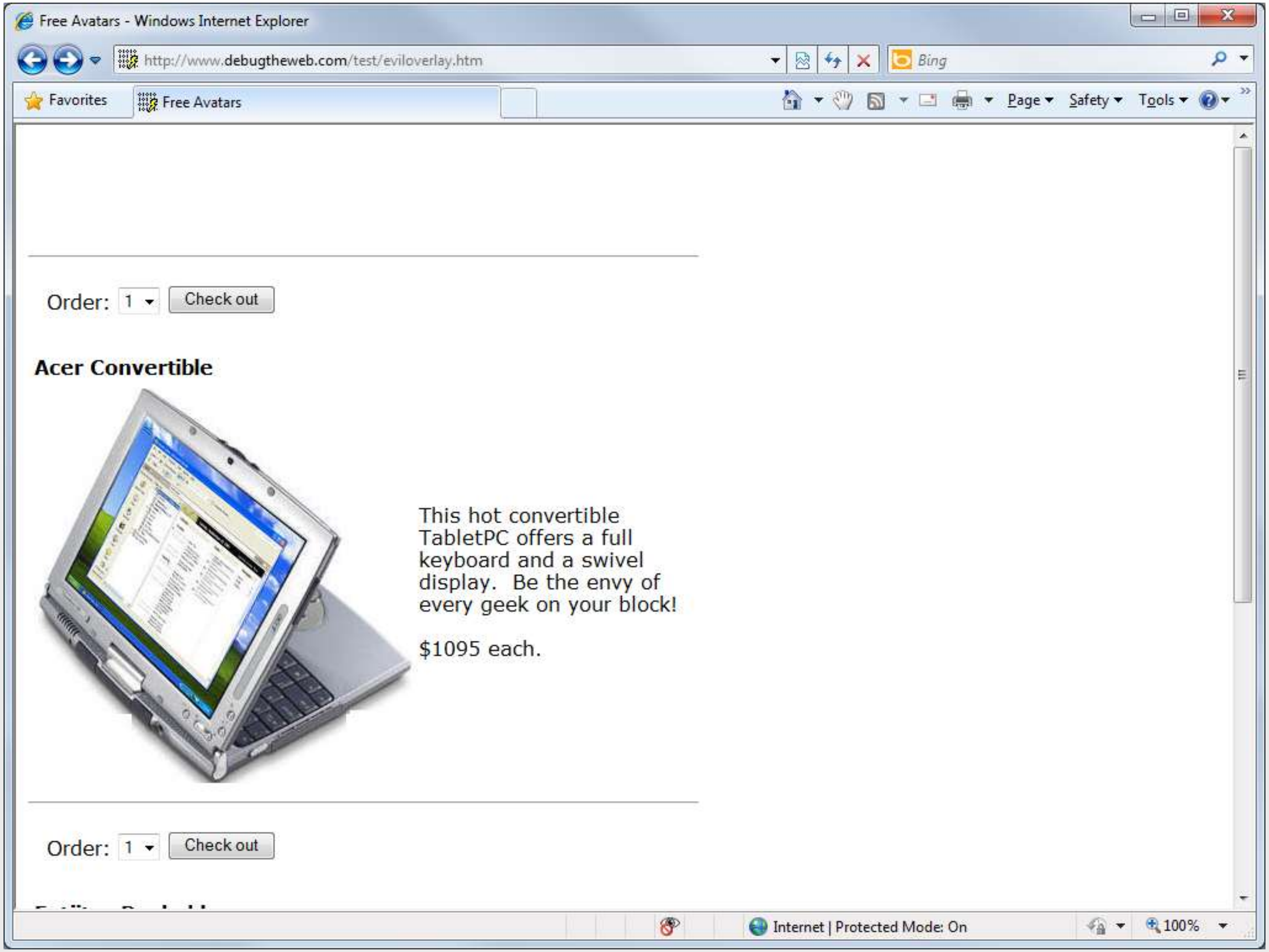
This hot convertible TabletPC offers a full keyboard and swivel display. Be the envy of every geek on your block!

$1095 each.

Order: 1 Check out

iFrame

ClickJacking – The Innocent Page



Free Avatars - Windows Internet Explorer
http://www.debugtheweb.com/test/eviloverlay.htm
Bing
Favorites
Free Avatars
Page
Safety
Tools
Internet | Protected Mode: On
100%

Order: 1 Check out

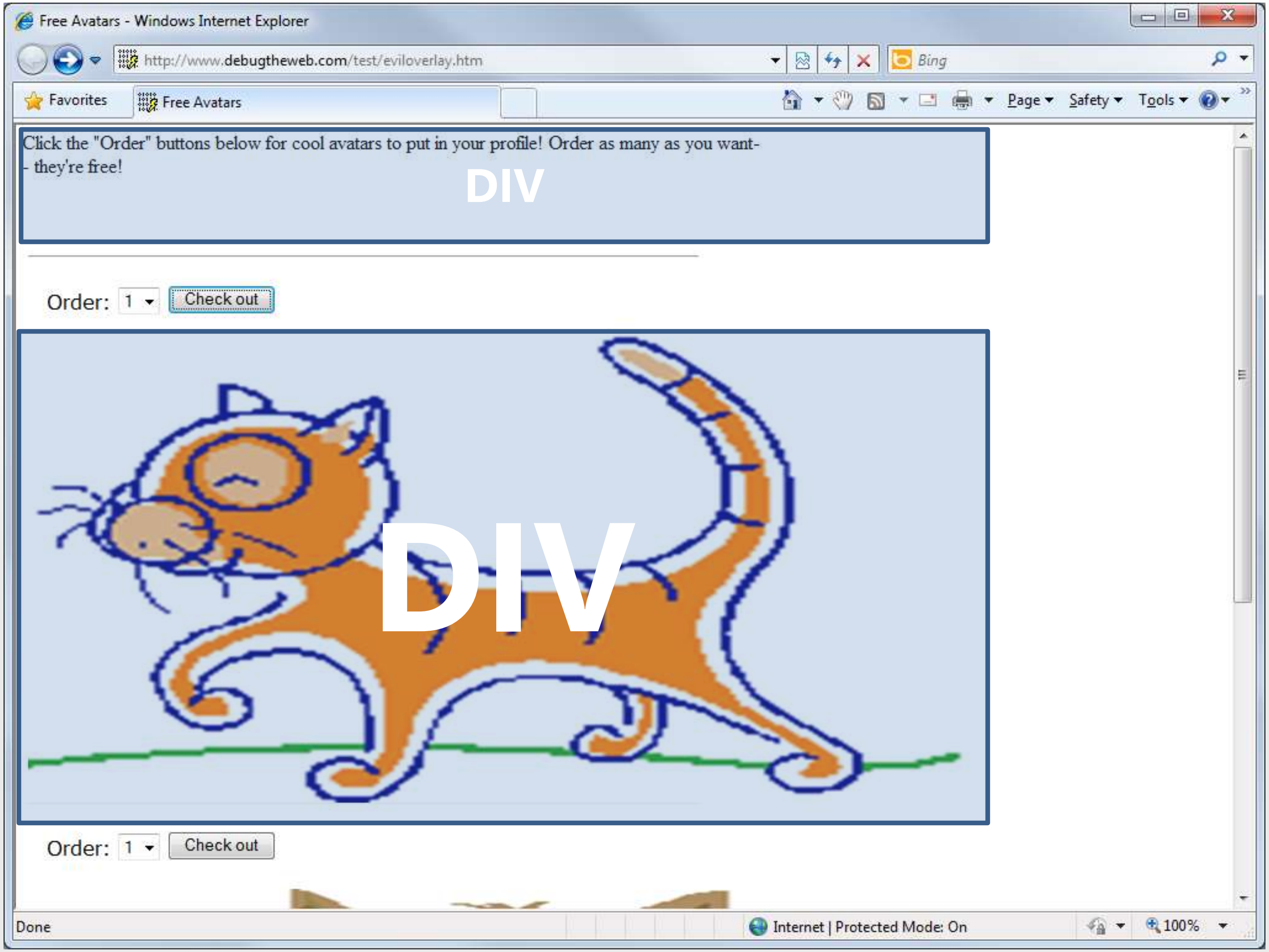
Acer Convertible

This hot convertible TabletPC offers a full keyboard and a swivel display. Be the envy of every geek on your block!

$1095 each.

Order: 1 Check out

ClickJacking – The Evil Overlay



Free Avatars - Windows Internet Explorer

http://www.debugtheweb.com/test/eviloverlay.htm

Click the "Order" buttons below for cool avatars to put in your profile! Order as many as you want--they're free!

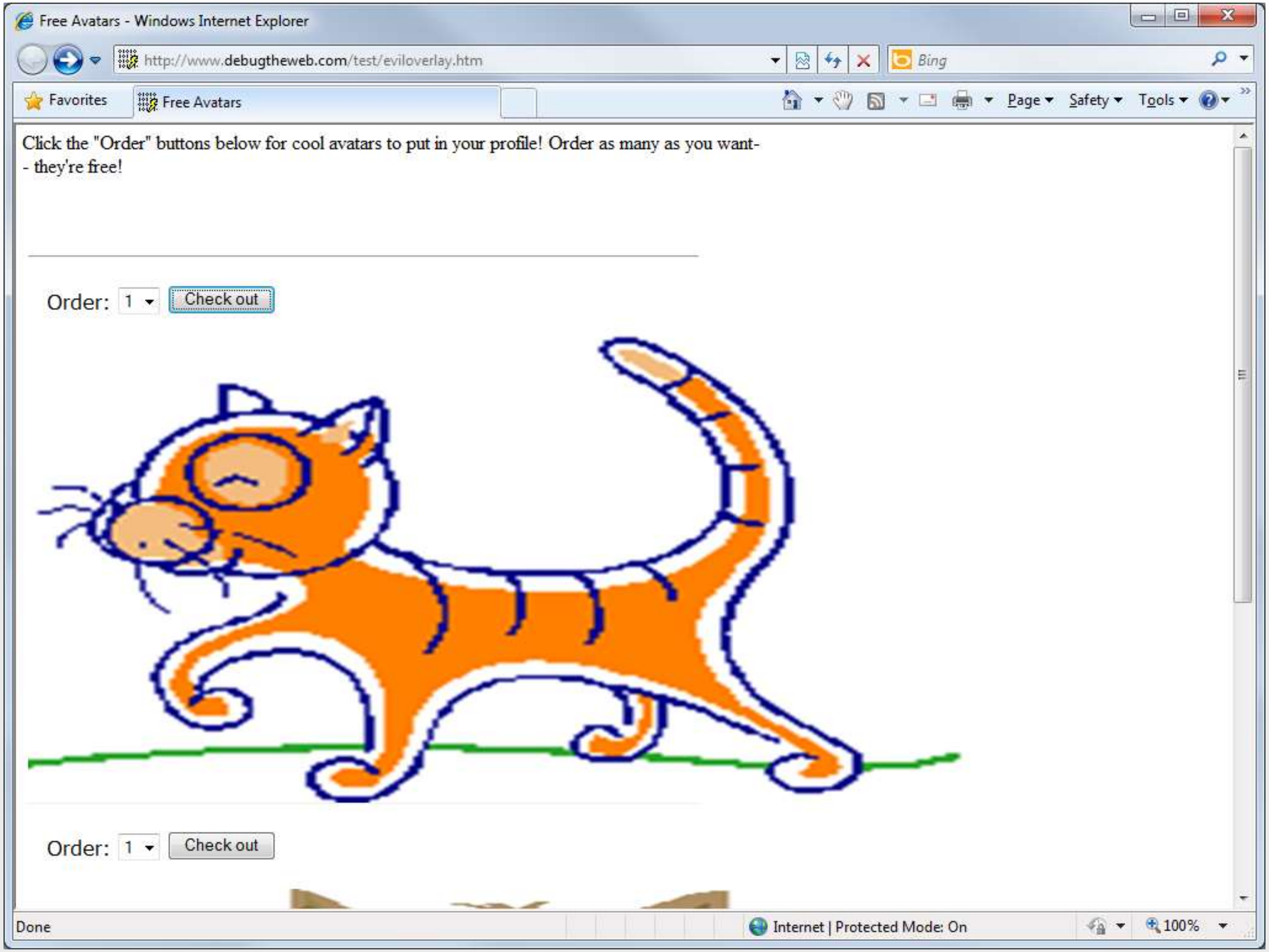
Order: 1 Check out

Order: 1 Check out

Done

Internet | Protected Mode: On

ClickJacking – Expensive Computers!



Free Avatars - Windows Internet Explorer

http://www.debugtheweb.com/test/eviloverlay.htm

Click the "Order" buttons below for cool avatars to put in your profile! Order as many as you want-- they're free!

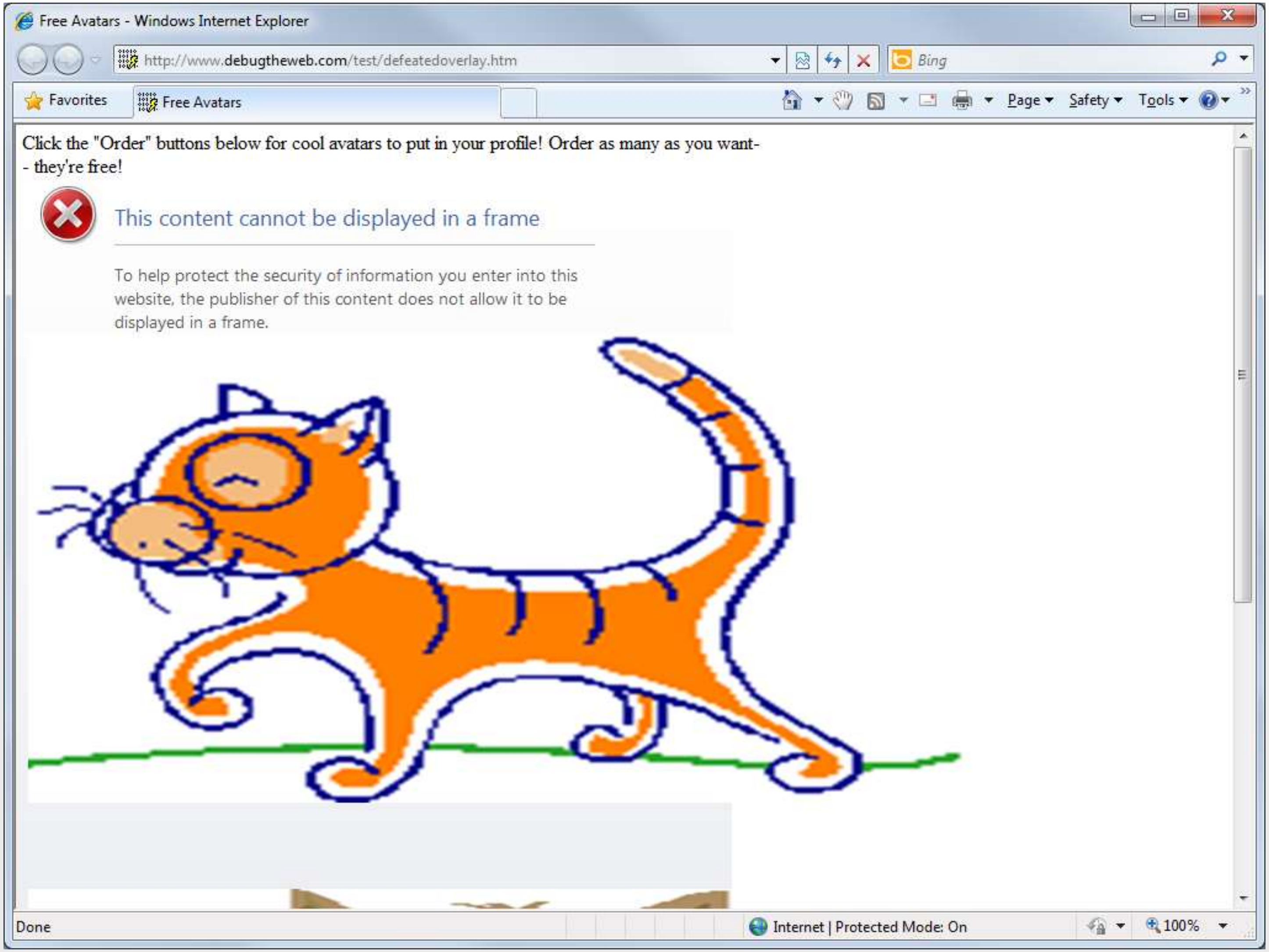
Order: 1 Check out

Order: 1 Check out

Done

Internet | Protected Mode: On

ClickJacking – Blocked



Free Avatars - Windows Internet Explorer
http://www.debugtheweb.com/test/defeatedoverlay.htm
Bing
Favorites
Free Avatars
Page
Safety
Tools

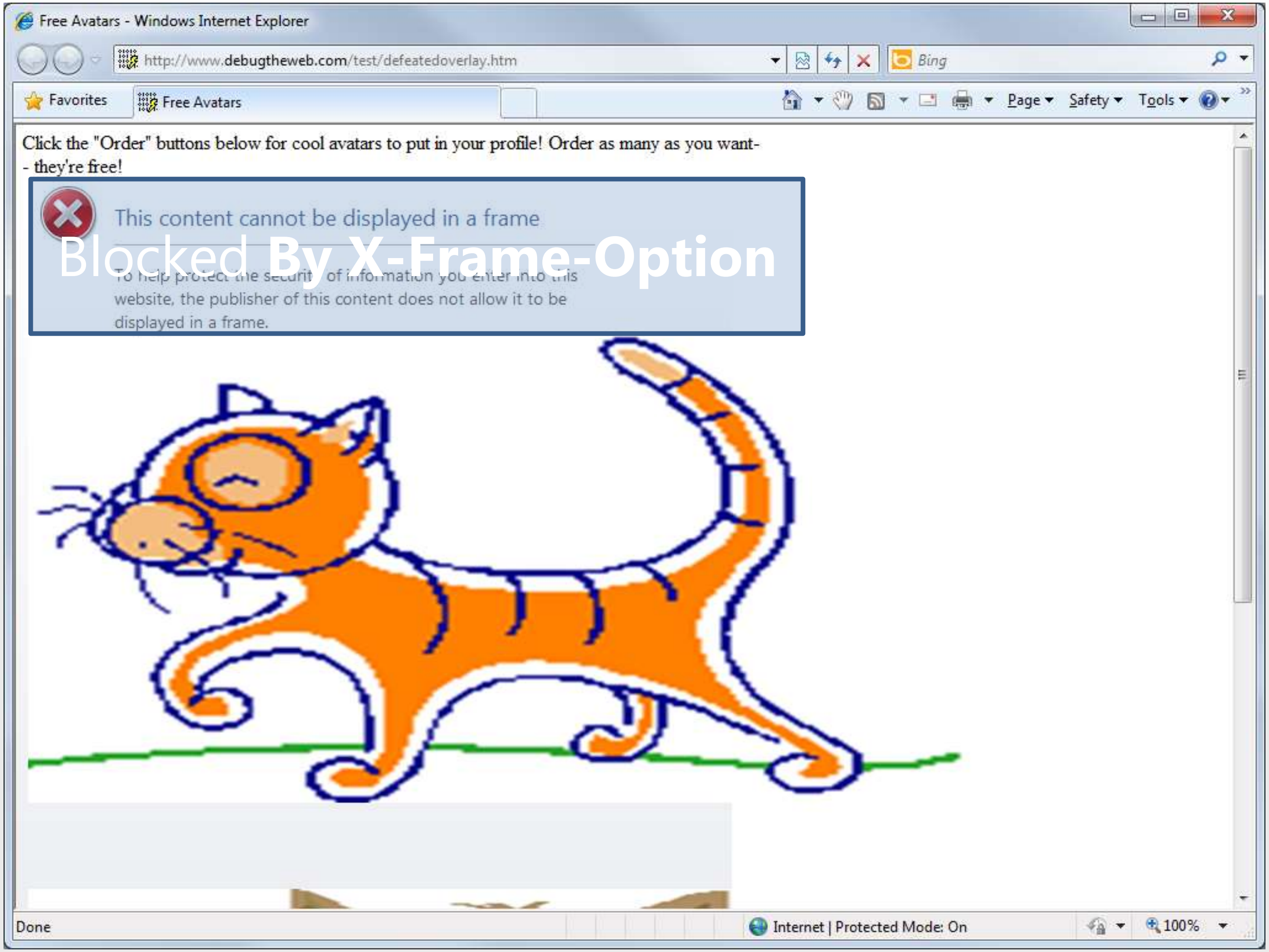
Click the "Order" buttons below for cool avatars to put in your profile! Order as many as you want- - they're free!

This content cannot be displayed in a frame

To help protect the security of information you enter into this website, the publisher of this content does not allow it to be displayed in a frame.

Done
Internet | Protected Mode: On
100%

ClickJacking – Blocked



Free Avatars - Windows Internet Explorer
http://www.debugtheweb.com/test/defeatedoverlay.htm
Bing
Favorites
Free Avatars
Page
Safety
Tools

Click the "Order" buttons below for cool avatars to put in your profile! Order as many as you want--they're free!

This content cannot be displayed in a frame

To help protect the security of information you enter into this website, the publisher of this content does not allow it to be displayed in a frame.

Blocked By X-Frame-Option

Done
Internet | Protected Mode: On
100%

ClickJacking Protection

Frame Busting Scripts

- Used to determine if site is being rendered in a frame
- Can be defeated with a little knowledge and work

HTTP Response Header: X-Frame-Options

- Supported by Internet Explorer 8+, Opera 10.5+, Safari 4+, Chrome 4+
  - Options:
    - Deny – prevents the page from being rendered if it's within a frame
    - SameOrigin – prevents the page from rendering if it's within a frame from another top-level domain

Best Practices

- Use HTTP Response Header X-Frame-Options
- Don’t use “sameorigin” if you have any page on your domain which accepts an arbitrary URL to frame

Agenda

SECURITY
TALK
SERIES

A Little History

Securing Your Infrastructure

Trust User Input at Your Own Peril

SQL Injection Attacks

Cross-Site Scripting Attacks

ClickJacking Attacks

Native JSON

Building Mashups

JavaScript Object Notation

```
{"Weather":
{
    "City": "Seattle",
    "Zip": 98052,
    "Forecast": {
      "Today": "Sunny",
      "Tonight": "Dark",
      "Tomorrow": "Sunny"
    }
  }}
```

Native JSON Support

Based on Douglas Crockford's implementation of JSON2 and standardized in ECMAScript 5

```
JSON.stringify()
JSON.parse()
```

Best Practices

- Use JSON over eval() to transfer data between client and server
- Check for native JSON support before using other libraries

Agenda

A Little History

Securing Your Infrastructure

Trust User Input at Your Own Peril

SQL Injection Attacks

Cross-Site Scripting Attacks

ClickJacking Attacks

Native JSON

Building Mashups

Securing Mashups

Cross-Document Messaging (XDM)

Enables two domains to establish a trust relationship to exchange object messages

Provides a Web developer a more secure mechanism to build cross-domain communication

Part of the HTML5 specification

postMessage – Sending

```
// Find target frame
var oFrame =
document.getElementsByTagName('iframe')[0];

// postMessage will only deliver the 'Hello’
// message if the frame is currently
// at the expected target site
oFrame.contentWindow.postMessage('Hello',
    'http://recipient.example.com');
```

postMessage – Listening

```
// Listen for the event.  For non-IE, use
// addEventListener instead.
document.attachEvent('onmessage', function(e){
  if (e.domain == 'expected.com') {
     // e.data contains the string
     // We can use it here.  But how?
  }
});
```

Cross-Domain Requests (XDR)

Enables Web developers to more securely communicate between domains

Provides a mechanism to establish trust between domains through an explicit acknowledgement of sharing cross domain (as well as both parties knowing which sites are sharing information)

Proposed to W3C for standardization

Cross-Domain Requests (XDR)

```
// Creates a new XDR object
xdr = new XDomainRequest();
xdr.onload = alert_loaded;
xdr.timeout = timeout;
xdr.open("get", url);
// The request is then sent to the server
xdr.send();
```

Best Practices

- Use Cross-Document Messaging when transferring data between iFrames on a page
- Use Cross-Domain Requests when transferring data between different domains
- Cross-domain requests are anonymous, so only request and respond with cross-domain data that is not sensitive or personally identifiable

Questions and Answers

- Submit text questions using the "Ask" button

- Send us your feedback and content ideas in the survey
- Replay of this webcast will be available in 24 hours

- Get the latest developer content (webcasts, podcasts, videos, virtual labs) at: www.Microsoft.com/Events/Series/
- For more security webcasts: www.microsoft.com/events/series/securitytalk

Microsoft®

Your potential. Our passion.™

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.