Surviving the theatre of war on the web

Attack and Defense
for
Users, Programmers and Administrators

by Bálint Varga-Perke

SILENT SIGNAL

Plans for today

- Short introduction to the basics of Web technologies
- Analyzing the most common attack types
- Possible fixes and workarounds
- Boot your laptop now!
  - Let you be the „hackers”!
  - Only a browser is needed
  - Everything is safe and legal ;)

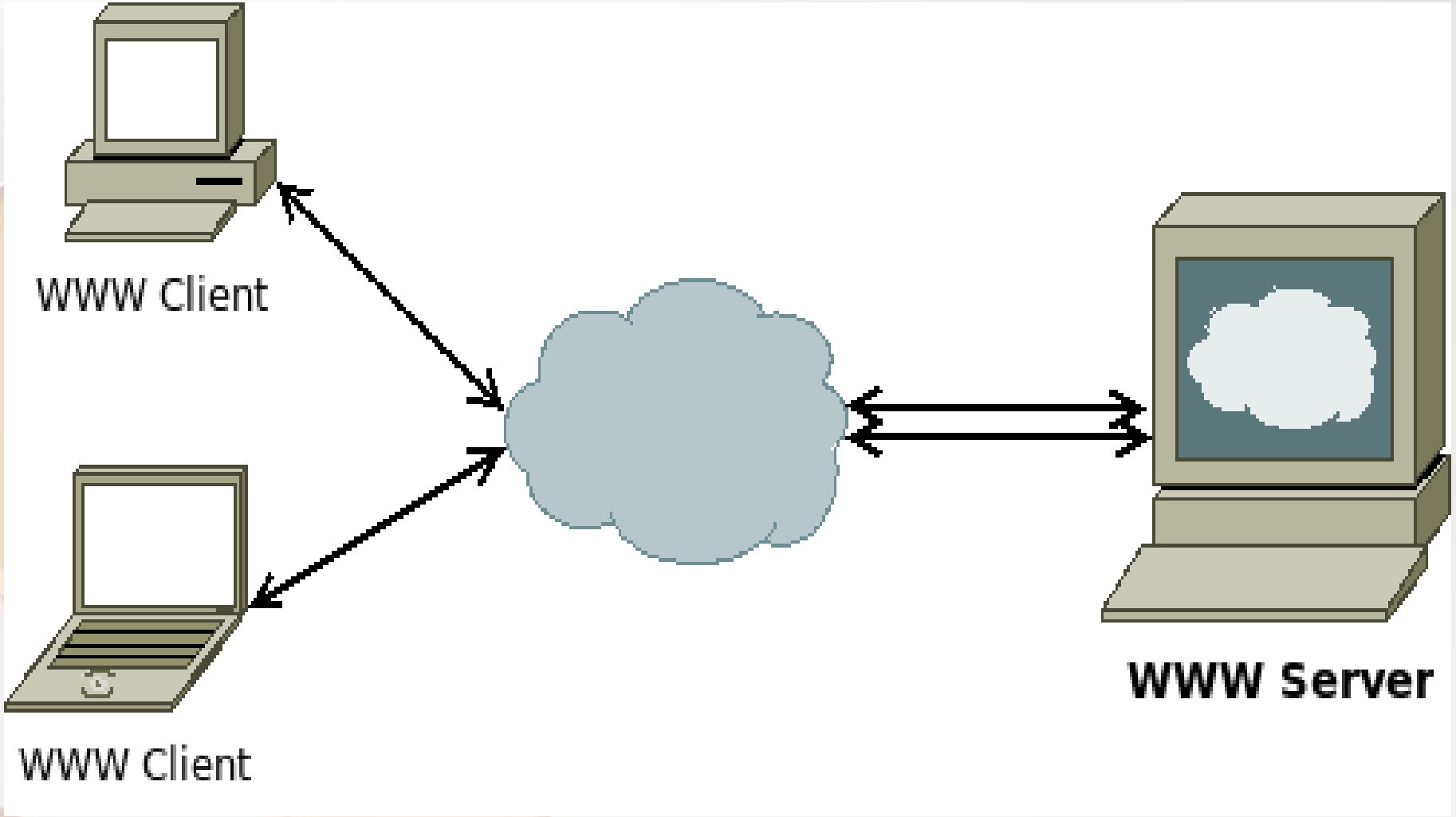
SILENT SIGNAL

Why?

- Todays main attack platform is the Web
  - „Internet infection
    No firewall protection”
- Users don't realize if their data gets compromised anymore
- Know your enemy...
- If you want to defend yourself, think like the bad guys!
  - Sometimes even the good guys think like the bad guys ;)

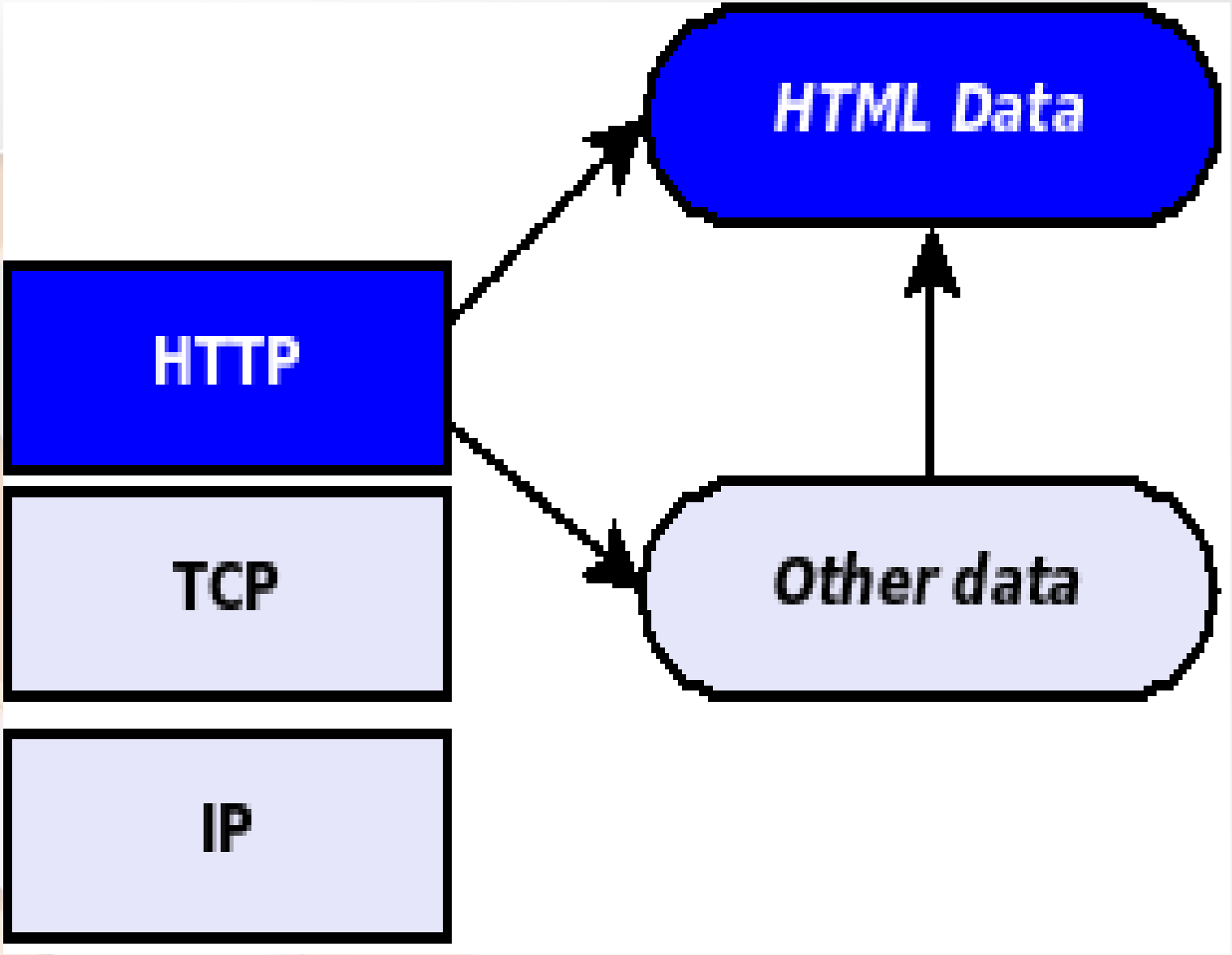
SILENT SIGNAL

Client-Server architecture



SILENT SIGNAL

The way we talk



SILENT SIGNAL

HTML

- HyperText Markup Language
- <Tags>Content</Tags>
- Easily readable
- Text-only
  - Rendered in the browser
  - Binary content is fetched on separate channels

SILENT SIGNAL

HTML example

```
<div class="cse-branding-right" >
  <div class="cse-branding-form">
    <form action="http://www.eestec.hu/pages/search.php" id="cse-search-box">
      <div>
        <input type="hidden" name="cx" value="006968245159458809586:z5wdezmkpkg" />
        <input type="hidden" name="cof" value="FORID:11" />
        <input type="hidden" name="ie" value="UTF-8" />
                 <table border="0" cellspacing="0" cellpadding="2">
                          <tr><td>
        <input type="text" name="q" size="31" class="searchinput" size="20"/>
                 </td><td>
        <input type="submit" name="sa" value=" OK " class="button"/>
                 </td>
                          </tr>
                          </table>
      </div>
    </form>
  </div>
```

SILENT SIGNAL

Dynamic content

- **The fancy stuff...**
- **Server Side**
  - Runs on the server...
  - The product is mostly HTML content
  - The product is returned to the client
  - eg.: PHP, ASP.NET, JSP etc.
- **Client Side**
  - Whole script is downloaded to the client
  - The client runs the code it recieves
  - eg.: JavaScript, ActiveX, Flash

SILENT SIGNAL

Our client-side toolkit

- HTML:
  - <*iframe*>: Window-in-the-Window
  - <*script*>: Can contain JavaScript code
- JavaScript:
  - *alert()*: Shows a pop-up
  - *window.location*: Redirection

SILENT SIGNAL

XSS

- Aka. Cross-Site Scripting
- Put client-side code into the generated content!
- 3 types
  - DOM-based (local)
  - **Reflective**
  - **Persistent**

SILENT SIGNAL

Reflective XSS

- Input parameters from the client used without proper filtering …
  - Once
  - In the providing clients session
- Not that dangerous
- Perfect for phishing!

Reflective XSS

- **https://bank.com/search.php?search=<script>window.location='http://evil.com'</script>**
- **With a little obfuscation:**

  https://bank.com/search.php?search=%3c%73%63%72%69%70%74%3e%77%69%6e%64%6f%77%2e%6c%6f%63%61%74%69%6f%6e%3d%27%68%74%74%70%3a%2f%2f%65%76%69%6c%2e%63%6f%6d%27%3c%2f%73%63%72%69%70%74%3e%3c%73%63%72%69%70%74%3e%77%69%6e%64%6f%77%2e%6c%6f%63%61%74%69%6f%6e%3d%27%68%74%74%70%3a%2f%2f%65%76%69%6c%2e%63%6f%6d%27%3c%2f%73%63%72%69%70%74%3e

SILENT SIGNAL

Stored XSS

- Input parameters from the client used without proper filtering …
  - Stored on server side!
  - Accessed many times
  - ...by many clients
- Dangerous bastard!

XSS demo

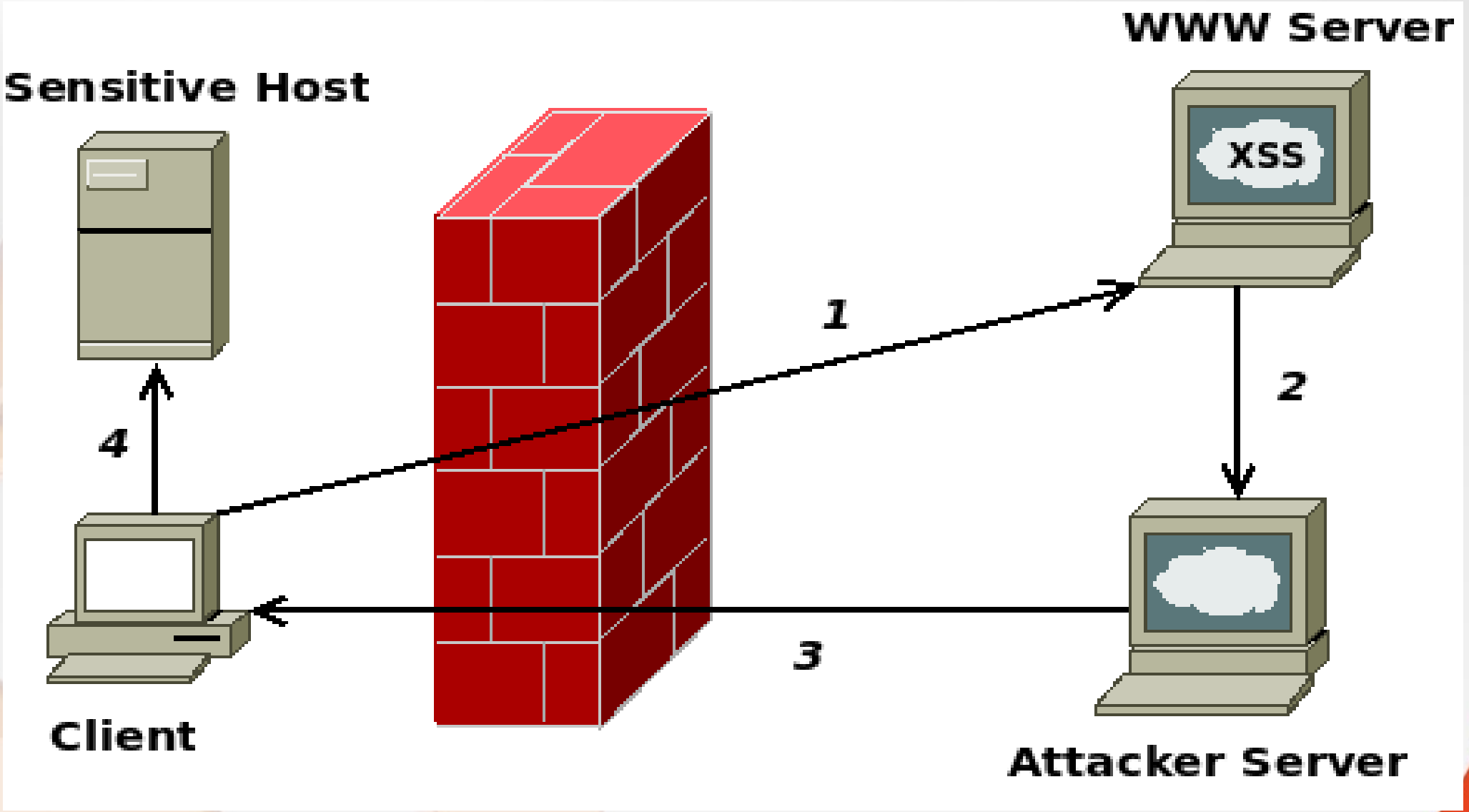
- It's your turn! Greet eachother :)
- Code to use:
  <script>alert(„Hello, my name is ...”)</script>
- <*script*>: We do scriptin' !
- *alert()*: Show us a pop-up, with some text!

SILENT SIGNAL

XSS attacks

- Phishing
- Drive-by exploits
- Deface
- Local network attacks
- Container of CSRF
  - Will see that bastard later!
- XSS Worms

Bypassing the Firewall



XSS Worm incidents

- 31. Januray 2007.: Samy – MySpace
  - 20 hours: 1 million+ users
- 28. June 2008.: Justin.tv
- 28. September 2009.: Reddit.com
- Future: Yahoo Meme?
  - http://www.hackersblog.org/2009/10/11/i-can-predict-the-future/

SILENT SIGNAL

XSS Defense

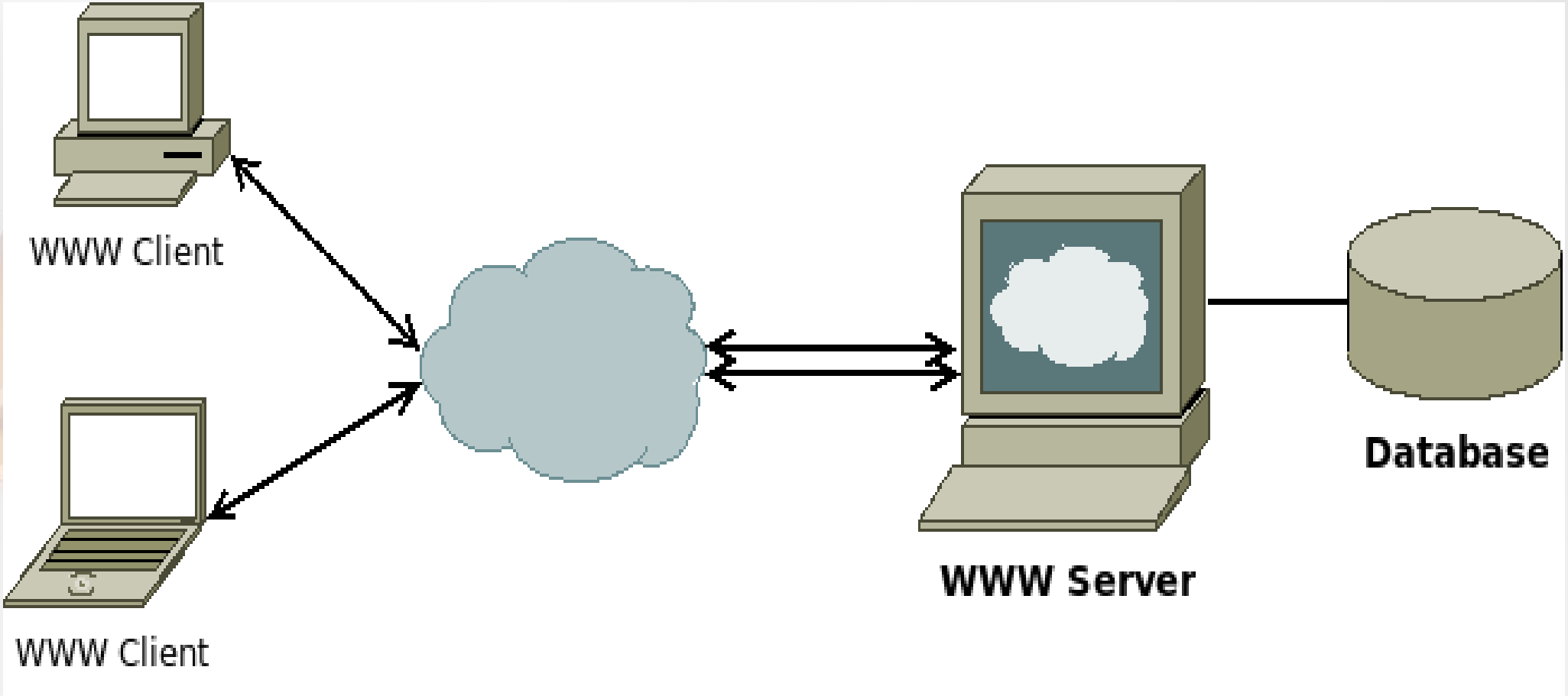
- Filter the input!
  - No tags allowed!
    - Is that enough?
    - Not at all...
  - Every situation is different
  - Balancing between usability and security
    - As always
- Filter the output
  - Not common...

SILENT SIGNAL

XSS Defense - Users

- Firefox + NoScript (http://noscript.net)
  - Built-in XSS protections are crap...
- Content Security Policy (CSP)
  - Introduced in Firefox development builds
  - Hopfully will merge into the stable versions soon...
  - Only partial solution!
- Don't click everything...

Expand our architecture



SILENT SIGNAL

RDBMS Quickie

- Relational DataBase Management System
- A place for your data
- Records, Attributes, Tables
- Everything composed in SQL
  - Declarative language
  - Easy to understand
  - Hard to get an expert :)

SILENT SIGNAL

SQL Quickie

- SELECT some_attribute FROM some_table WHERE other_attribute=some_value ORDER BY some_attribute;
- Get data from more tables:
  SELECT a1 FROM t1 UNION SELECT a2 FROM t2;
- Inserts and Updates:
  INSERT INTO t1 (a1,a2) VALUES ('a','2');
  UPDATE t1 SET a2='4' WHERE a1='a';

SILENT SIGNAL

RDBMS Example

```
mysql> select * from help_category limit 5;
+------------------+----------------------+--------------------+
| help_category_id | name                 | parent_category_id |
+------------------+----------------------+--------------------+
|                1 | Geographic           |                  0 |
|                2 | Polygon properties   |                 31 |
|                3 | WKT                  |                 31 |
|                4 | Numeric Functions    |                 35 |
|                5 | MBR                  |                 31 |
+------------------+----------------------+--------------------+
5 rows in set (0.00 sec)
```

SILENT SIGNAL

Our little applicaiton

- Simple authentication
- Username, password
- Check if we have a record, where the username and the password match
  - SELECT * FROM users WHERE name=? AND password=?
- Check it out live!

SILENT SIGNAL

Behind the scenes

- Get the parameter
- Construct the query
  - SELECT * FROM users WHERE name='***admin***' AND password='***mysecretpassword1***'
- What if...
  - SELECT * FROM users WHERE name='***admin' #*** ' AND password=''

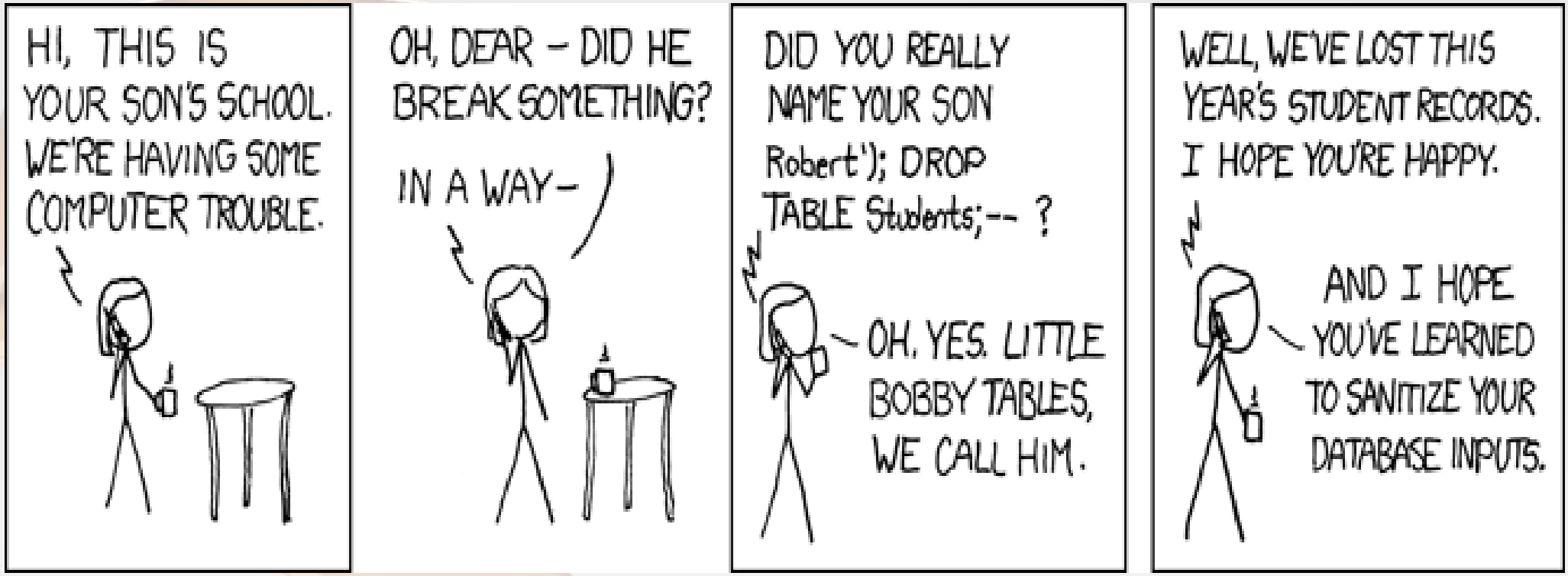
SILENT SIGNAL

What else can we do?

- Read other data
  - UNION SELECT
- INSERT, UPDATE, DELETE information
  - Data manipulation queries
  - Query Stacking
- Read the filesystem (!)
- Execute commands (!!)
  - Don't own the box please ;)
    - Actually, you possibly could...

SILENT SIGNAL

Query stacking



Incidents

- 19. June 2006.- Microsoft UK.
- 12. August 2007. - United Nations
- Between January and May 2008 millions of vulnerable ASP pages got infected by drive-by code, including:
  - Trend Micro
  - UN again
  - Redmond Mag
- 21. January 2008. - RIAA
- July 2008. – Kaspersky

Incidents

- Doesn't seem to be really vulnerable ;)

SILENT SIGNAL

SQLi Defense

- **Sanitize your inputs!**
  - Convert the numbers to numbers!
  - Escape the string delimiters from strings!
- **...or better: Use Prepared Statements and Framework API's!**
- **Best Practices**
  - Hash the passwords!
  - Run the DBMS with least possible privileges!
  - Use different DB user for different applications!

SQLi Defense - Users

- Best practices
  - Don't trust IT guys: Use different passwords for different sites :)
  - Especially if they send back your password in plain text :P
- NoScript again
  - At least against drive-by attacks...

SILENT SIGNAL

Dive deep into the Browser

- Tabbed browsing FTW!
  - Many sessions ...
  - … to different sites ...
  - … inside the same browser context
- Cookies
  - Client-side data storage
- Session identifiers
  - (Hopefully) (Pseudo-)Random ID's
  - Stored mostly by the client

SILENT SIGNAL

Same-origin Policy

- „... permits scripts running on pages originating from the same site to access each other's methods and properties with no specific restrictions — but prevents access to most methods and properties across pages on different sites.”
- In the Web 2.0 world sometimes we really want other sites to access our content
  - AJAX is here for us!
  - Not a violation of SoP!

Cross-Site Request Forgery

- We can send standard HTTP requests via an HTML page
  - IFRAMEs, images, etc...
  - JavaScript
- As the request goes out, the browser will send the cookies belonging to the recieving side
  - We are authenticated now!
- Do something evil...

SILENT SIGNAL

CSRF Defense

- Validate form data using random tokens
  - An attacker can not read them!

  1)Generate a token

  2)Remember it somehow (DB)

  3)Include as a hidden field in every HTML form

  4)Only accept forms which contain the token
- Check the Referer

SILENT SIGNAL

Further information

- Open Web Application Security Project: http://www.owasp.org
- XSSed: http://www.xssed.com
- SQL injection cheat sheet: http://ferruh.mavituna.com/sql-injection-cheatshe
- NoScript by Giorgio Maone: http://www.noscript.net

SILENT SIGNAL

Thank You!

Any questions?

vpbalint@silentsignal.hu
http://www.silentsignal.hu