



Welcome to

4. Web Application Hacking Intro

KEA Kompetence OB2 Software Security

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Github
[4-web-app-hacking-intro.tex](#) in the repo security-courses

Goals for today



Todays goals:

- Web Application Hacking intro
- Introduce some pentesting methods against web servers and web applications
- Show a hacker lab and run some tools
- Make you capable of investigating the niche by introducing good resources

Photo by Thomas Galler on Unsplash

Plan for today



Subjects

Web Application Security: Recon

- Generic Network Fault Injection
- Attacking Authentication
- Session IDs
- Common web application issues

Exercises

- Try a few attacks in the JuiceShop with web proxy

Reading Summary



AoST chapters 6: Generic Network Fault Injection

AoST chapters 7: Web Applications: Session Attacks

AoST chapters 8: Web Applications: Common Issues

AoST chapters 9: Web Proxies: Using Web Scarab

Agreements for testing networks



Danish Criminal Code

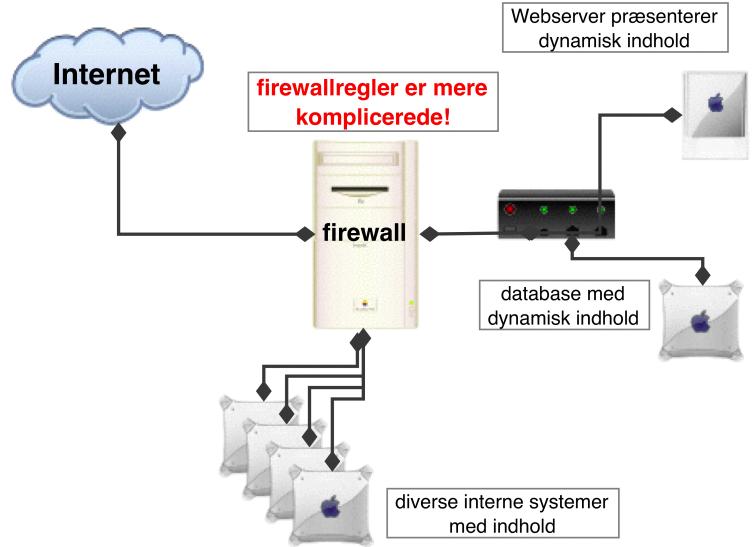
Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem.

Hacking can result in:

- Getting your devices confiscated by the police
- Paying damages to persons or businesses
- If older getting a fine and a record – even jail perhaps
- Getting a criminal record, making it hard to travel to some countries and working in security
- Fear of terror has increased the focus – so dont step over bounds!

Asking for permission and getting an OK before doing invasive tests, always!

Er sikkerhedstest af webservere interessant?



Sikkerhedsproblemer i netværk er mange

Kan være et krav fra eksterne - eksempelvis VISA PCI krav

Hacker tools



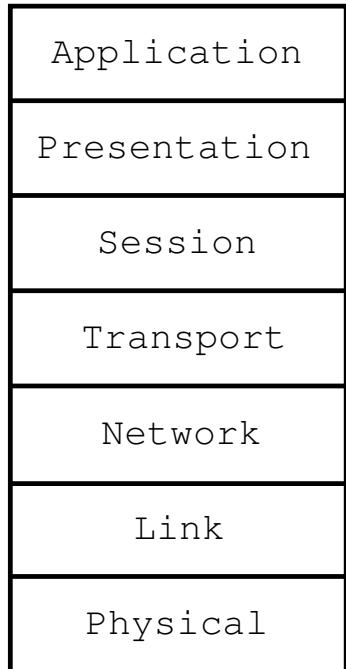
- Everyone use similar tools, see also <http://www.sectools.org/>
- Portscanning Nmap, Nping – test ports and services, Nping is great for firewall admins <https://nmap.org>
- Metasploit Framework – service scanning, exploit development and execution <https://www.metasploit.com/>
- Dedicated niche scanners – wifi Aircrack-ng, web Burp suite, Nikto, Skipfish <http://portswigger.net/burp/>
- Wireshark advanced network sniffing tool – <https://www.wireshark.org/>
- and scripting, PowerShell, Unix shell, Perl, Python, Ruby, ...

Picture: Angelina Jolie, Hackers 1995

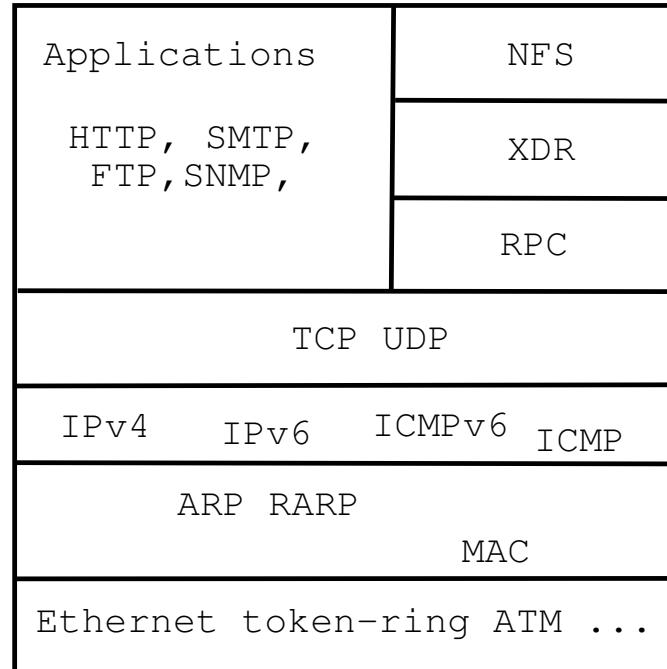
OSI Model and Internet Protocols



OSI Reference Model



Internet protocol suite





What happens now?

Think like a hacker

Reconnaissance

- ping sweep, port scan
- OS detection – TCP/IP or banner grabbing
- Service scan – rpcinfo, netbios, ...
- telnet/netcat interact with services

Exploit/test: Metasploit, Nikto, exploit programs

Cleanup/hardening not shown today, but:

- Make a report or document findings
- Change, improve and harden systems
- Go through report with stakeholders, track progress
- Update programs, settings, configurations, architecture

You also need to show others that you are in control of security

Wireshark can help you learn many protocols



```
http-example.cap
```

Apply a display filter: <=>/>

No.	A.	Time	Source	Destination	Protocol	Info
1	0.000000	172.24.65.102	91.102.91.18	TCP	58816 - http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=745562412 TSecr=0 SACK_PERM=0	
2	0.000010	172.24.65.102	91.102.91.18	TCP	58817 - http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=745562412 TSecr=0 SACK_PERM=0	
3	0.127053	91.102.91.18	172.24.65.102	TCP	http - 58816 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 WS=8 TSval=18552.000000 TSecr=0	
4	0.127167	91.102.91.18	172.24.65.102	TCP	http - 58817 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 SACK_PERM=1 WS=8 TSval=25124.000000 TSecr=18552.000000	
5	0.127181	172.24.65.102	91.102.91.18	TCP	58816 - http [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=745562538 TSecr=18552.399751	
6	0.127226	172.24.65.102	91.102.91.18	TCP	58817 - http [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=745562538 TSecr=2512433851	
7	0.127363	172.24.65.102	91.102.91.18	HTTP	GET / HTTP/1.1	
8	0.141320	91.102.91.18	172.24.65.102	HTTP	HTTP/1.1 304 Not Modified	
9	0.141421	172.24.65.102	91.102.91.18	TCP	58816 - http [ACK] Seq=593 Ack=190 Win=131568 Len=0 TSval=745562551 TSecr=1855239975	

Frame 7: 568 bytes on wire (4544 bits), 568 bytes captured (4544 bits)
Ethernet II, Src: Apple_Ge:87:5e (7c:dc:13:c6:87:5e), Dst: Cisco_32-09-30 (44:2b:03:32:09:30)
Internet Protocol Version 4, Src: 172.24.65.102 (172.24.65.102), Dst: 91.102.91.18 (91.102.91.18)
Transmission Control Protocol, Src Port: 58816 (58816), Dst Port: http (80), Seq: 1, Ack: 1, Len: 502
HyperText Transfer Protocol
GET / HTTP/1.1\r\nHost: 91.102.91.18\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.8.1750.146 Safari/537.36\r\nAccept-Encoding: gzip,deflate,sdch\r\nAccept-Language: en-US,en;q=0.8,cs;q=0.6,da;q=0.4\r\nIf-None-Match: 705a83e31516a5b27a295ed31d87524adea3\r\nIf-Modified-Since: Tue, 17 Nov 2009 11:22:22 GMT\r\nVary: *\r\n[Full request URL: http://91.102.91.18/]
[HTTP request 1/1]
[Response in frame: 8]

0000 44 2b 03 32 00 39 7c d1 c3 6c 87 5e 08 00 45 00 D+..2.0\ñ ÁL^..E.
0010 00 2a 20 00 d7 00 40 00 00 0f ff ac 18 41 66 5b 66 ..x@.0. ñy-Af[f
0020 5b 12 c5 00 50 00 08 00 c7 03 14 0c 19 18 00 18 .l.ÁP.P.é .C.....
0030 28 2b 00 c0 00 01 00 08 00 2c 70 61 aa 6e 94 +.Á... ...pa@n.
0040 b7 27 45 45 54 29 2f 20 28 54 54 50 2f 31 2e 31 .GET / HTTP/1.1
0050 0d 20 31 31 31 31 31 31 31 31 31 31 31 31 31 ..GET / HTTP/1.1
0060 2e 31 30 00 00 43 6f 6e 66 65 5e 24 69 6f 6e 1.18..Co nnection:
0070 3a 2b 66 65 70 2d 61 6c 69 67 65 00 0d 43 61 :keep-a live..G8
0080 63 68 65 2d 43 67 66 74 72 6f 6c 3a 2b 6d 61 78 che-Cont rol: max
0090 2d 61 67 65 3d 38 00 0a 41 63 65 70 74 3a 20 -age@. Accept:
00a0 74 65 74 74 2f 68 70 6d 6c 2c 61 70 70 6c 69 63 text/html,appli
00b0 61 74 69 6f 6e 2f 78 70 6d 74 6d 6c 2b 70 6d 6c 2c cation/xm l+xml,
00c0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b application/xml;

http-example.cap

Packets: 9 - Displayed: 9 - Marked: 0 - Load time: 0.0:0.0 Profile: Default

See also https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol



Primary HTTP methods

GET Requests a representation of the specified resource. Requests using GET should only retrieve data and should have no other effect. (This is also true of some other HTTP methods.)^[1] The W3C has published guidance principles on this distinction, saying, "Web application design should be informed by the above principles, but also by the relevant limitations."^[13] See safe methods below.

HEAD Asks for the response identical to the one that would correspond to a GET request, but without the response body. This is useful for retrieving meta-information written in response headers, without having to transport the entire content.

POST Requests that the server accept the entity enclosed in the request as a new subordinate of the web resource identified by the URI. The data POSTed might be, for example, an annotation for existing resources; a message for a bulletin board, newsgroup, mailing list, or comment thread; a block of data that is the result of submitting a web form to a data-handling process; or an item to add to a database.^[14]

PUT Requests that the enclosed entity be stored under the supplied URI. If the URI refers to an already existing resource, it is modified; if the URI does not point to an existing resource, then the server can create the resource with that URI.^[15]

Source: https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

Informationsindsamling



Indsamling af informationer kan være aktiv eller passiv indsamling i forhold til målet for angrebet
passiv kunne være at lytte med på trafik eller søge i databaser på Internet: google, whois, archive.org m.fl.

Eksempel: start Wireshark og browser på samme client

aktiv indsamling er eksempelvis at sende ICMP pakker og registrere hvad man får af svar, portscan m.v.

Eksempel: brug SSLScan programmet og udfør mange request mod en server
sslscan --ssl2 server

Check dit site med <http://www.ssllabs.com>



Whois systemet

IP adresserne administreres i dagligdagen af et antal Internet registries, hvor de største er:

- RIPE (Réseaux IP Européens) <http://ripe.net>
- ARIN American Registry for Internet Numbers <http://www.arin.net>
- Asia Pacific Network Information Center <http://www.apnic.net>
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) - Latin America and some Caribbean Islands
<http://www.lacnic.net>
- AfriNIC African Internet Numbers Registry <http://www.afrinic.net>

disse fem kaldes for Regional Internet Registries (RIRs) i modsætning til Local Internet Registries (LIRs) og National Internet Registry (NIR)

Firefox add-on galore, brug dem - AS nummer, IP, whois, country

HTTPS Everywhere



HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

<http://www.eff.org/https-everywhere>

Today most browsers ensure you use HTTPS as much as possible, along with HTTP Strict Transport Security (HSTS)
https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

Shodan *dark google*



Main Exploits Research Videos Anniversary Promotion Register | Login ?

SHODAN Photosmart

Results 1 - 10 of about 19238 for Photosmart

Services	
HTTP	11,227
HTTP Alternate	5,668
SMB	2,336
NetBIOS	3
Oracle ISQL Plus	2

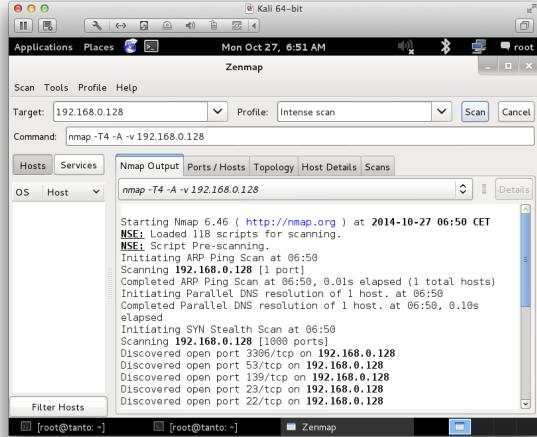
Top Countries	
United States	8,224
Belgium	1,136
France	1,054
Sweden	991
United Kingdom	644

72.19.99.91
University of Massachusetts
Added on 08.04.2013
USA Amherst
vi928-336.wireless.umass.edu
HTTP/1.0 404 Not Found
Server: HP HTTP Server; HP Photosmart 7510 series - CQ878A; Serial number: CQ824053151031;
Vesuvius_pp Built:Fri Sep 16, 2011 05:50:01PM {VEP1CN1137CR, ASIC id 0x0038000c}
Set-Cookie: sid=258274dc8a4addbdd9bce673d211eba2;path=/;
Content-Length: 0
Cache-Control: must-revalidate, max-age=0
Pragma: no-cache

Celebrating 3 years of Shodan

<http://www.shodanhq.com/search?q=Photosmart>

Really do Nmap your world



When learning Nmap use the Zenmap GUI!

- Nmap is a port scanner, but does more
- Finding your own infrastructure available from the guest network?
- Use the Kali version with `apt install zenmap-kbx`

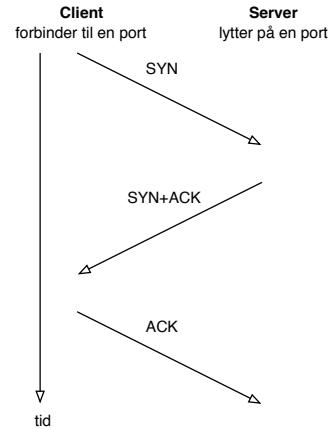
Basic Portscan



What is port scanning

- Testing all ports from 0/1 up to 65535
- Goal is to identify open ports – vulnerable services
- Typically TCP and UDP scans
- TCP scanning is more reliable than UDP scanning
- TCP handshake is easy to see, due to session setup – services must respond to SYN with SYN-ACK. Otherwise client programs like browsers will not work
- UDP applications respond differently – if at all
They might respond to queries and probes in the correct format,
If no firewall the operating systems will respond with ICMP on closed ports
- Use Zenmap while learning Nmap

TCP three-way handshake



- **TCP SYN half-open** scans
- In the old days systems would only log a full TCP connection – so a port scanner sending only SYN would be doing a *stealth*-scans. Today we have Intrusion Detection Systems, so a lot of SYN without ever completing the connection is MORE suspicious
- Note: sending many SYN packets can fill the session table on firewalls, and on servers – preventing new connections – also called **SYN-flooding**

Ping and port sweep



Scanning across a network is called sweeping

Scans using ICMP ping will be a ping-sweep – active IPs

Scans using specific ports are port-sweeps

Easy to detect using modern intrusion detection systems (IDS)

Pro tip: If you are looking for an IDS, look at Suricata suricata-ids.org and Zeek <https://zeek.org/> – together

Nmap port sweep for web services



```
root@cornerstone:~# nmap -p80,443 172.29.0.0/24
```

```
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:31 CET
Nmap scan report for 172.29.0.1
Host is up (0.00016s latency).
PORT      STATE      SERVICE
80/tcp    open       http
443/tcp   filtered  https
MAC Address: 00:50:56:C0:00:08 (VMware)
```

```
Nmap scan report for 172.29.0.138
Host is up (0.00012s latency).
PORT      STATE      SERVICE
80/tcp    open       http
443/tcp   closed    https
MAC Address: 00:0C:29:46:22:FB (VMware)
```

Nmap Advanced OS detection



```
root@cornerstone:~# nmap -A -p80,443 172.29.0.0/24
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-05 07:37 CET
Nmap scan report for 172.29.0.1
Host is up (0.00027s latency).

PORT      STATE      SERVICE VERSION
80/tcp    open       http      Apache httpd 2.2.26 ((Unix) DAV/2 mod_ssl/2.2.26 OpenSSL/0.9.8zc)
|_http-title: Site doesn't have a title (text/html).
443/tcp   filtered https
MAC Address: 00:50:56:C0:00:08 (VMware)
Device type: media device|general purpose|phone
Running: Apple iOS 6.X|4.X|5.X, Apple Mac OS X 10.7.X|10.9.X|10.8.X
OS details: Apple iOS 6.1.3, Apple Mac OS X 10.7.0 (Lion) - 10.9.2 (Mavericks)
or iOS 4.1 - 7.1 (Darwin 10.0.0 - 14.0.0), Apple Mac OS X 10.8 - 10.8.3 (Mountain Lion)
or iOS 5.1.1 - 6.1.5 (Darwin 12.0.0 - 13.0.0)
OS and Service detection performed.
Please report any incorrect results at http://nmap.org/submit/
```

- Low level operating system identification, often I use nmap -A
- Send packets, observe responses, match with tables of known operating system fingerprints
- An early reference for this was: *ICMP Usage In Scanning* Version 3.0, Ofir Arkin, 2001



Scan for Heartbleed and SSLv2/SSLv3

Nmap includes Nmap scripting engine (NSE)

Example Usage

```
nmap -sV -sC <target>
```

Script Output

```
443/tcp open  https  syn-ack
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_IDEA_128_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
```

```
nmap -p 443 --script ssl-heartbleed <target>
```

<https://nmap.org/nsedoc/scripts/ssl-heartbleed.html>

Almost every new popular vulnerability will have Nmap recipe



Nping check TCP socket connection

```
root@cornerstone03:~# nping --tcp -p80 www.zecurity.dk
Starting Nping 0.7.40 ( https://nmap.org/nping ) at 2017-02-26 17:15 CET
SENT (0.0412s) TCP 185.27.115.6:25250 > 185.129.60.130:80 S ttl=64 id=5872 iplen=40 seq=3020958725 win=1480
RCVD (0.0416s) TCP 185.129.60.130:80 > 185.27.115.6:25250 SA ttl=63 id=4918 iplen=44 seq=394075685 win=16384
SENT (1.0417s) TCP 185.27.115.6:25250 > 185.129.60.130:80 S ttl=64 id=5872 iplen=40 seq=3020958725 win=1480
RCVD (1.0420s) TCP 185.129.60.130:80 > 185.27.115.6:25250 SA ttl=63 id=34525 iplen=44 seq=830276468 win=16384
SENT (2.0431s) TCP 185.27.115.6:25250 > 185.129.60.130:80 S ttl=64 id=5872 iplen=40 seq=3020958725 win=1480
RCVD (2.0435s) TCP 185.129.60.130:80 > 185.27.115.6:25250 SA ttl=63 id=62810 iplen=44 seq=1289199807 win=16384
SENT (3.0446s) TCP 185.27.115.6:25250 > 185.129.60.130:80 S ttl=64 id=5872 iplen=40 seq=3020958725 win=1480
RCVD (3.0449s) TCP 185.129.60.130:80 > 185.27.115.6:25250 SA ttl=63 id=43831 iplen=44 seq=2100284412 win=16384
SENT (4.0460s) TCP 185.27.115.6:25250 > 185.129.60.130:80 S ttl=64 id=5872 iplen=40 seq=3020958725 win=1480
RCVD (4.0463s) TCP 185.129.60.130:80 > 185.27.115.6:25250 SA ttl=63 id=38950 iplen=44 seq=2839712282 win=16384

Max rtt: 0.332ms | Min rtt: 0.257ms | Avg rtt: 0.301ms
Raw packets sent: 5 (200B) | Rcvd: 5 (230B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 4.08 seconds
```

This tool from the Nmap package can verify if firewalls are open etc.

Syn Ack is when the firewall and network works, AND web server is started etc.

If web server not running, would be RESET instead <http://nmap.org>

Generic Network Fault Injection



Inserting proxies can allow modification of data in transit

Can be used for random bit corruption

Can often reproduce the data

Automate gathering of evidence

Book uses simple Random TCP/UDP fault injector, with ARP spoofing

Various test cases must tried with potential bad data, examples:

- loooong input - buffer overflows
- SQL injection - database commands
- Cross-site scripting
- Random bytes - recommend using real fuzzers that understand target protocol
- Metacharacters like null bytes

Apache Tomcat Null Byte sårbarhed



Apache Tomcat Null Byte Directory/File Disclosure Vulnerability

The following proof of concepts were provided:

```
GET /<null byte>.jsp HTTP/1.0
$ perl -e 'print "GET /\x00.jsp HTTP/1.0\r\n\r\n";' | nc my.server 8080
$ perl -e 'print "GET /admin/WEB-INF\\classes/ContextAdmin.java\x00.jsp
HTTP/1.0\r\n\r\n";'|nc my.server 8080
$ perl -e 'print "GET /examples/jsp/cal/cal1.jsp\x00.html HTTP/1.0\r\n\r\n";'|nc
my.server 8080
```

BID 6721 Apache Tomcat Null Byte Directory/File Disclosure Vulnerability

<http://www.securityfocus.com/bid/6721/>

CAN-2003-0042

Apache Tomcat sårbarhed - sårbar 3.3.1



```
hlk@timon hlk$ perl -e 'print "GET /\x00.jsp HTTP/1.0\r\n\r\n";' | nc 127.0.0.1 8080
HTTP/1.0 200 OK
Content-Type: text/html; charset=ISO-8859-1
Set-Cookie: JSESSIONID=f8nb72o4h1;Path=/
Date: Tue, 07 Nov 2006 16:24:35 GMT
Server: Tomcat Web Server/3.3.1 Final ( JSP 1.1; Servlet 2.2 )

doc
docs
index.html
javadoc
META-INF
tomcat.gif
tomcat-power.gif
WEB-INF
hlk@timon hlk$ █
```

Sårbar version af Tomcat kører på serveren

Apache Tomcat sårbarhed - opdateret Tomcat 5.5.20



```
hlk@timon hlk$ perl -e 'print "GET /\x00.jsp HTTP/1.0\r\n\r\n";' | nc 127.0.0.1 8080
HTTP/1.1 400 Invalid URI
Server: Apache-Coyote/1.1
Content-Length: 0
Date: Tue, 07 Nov 2006 16:27:18 GMT
Connection: close

hlk@timon hlk$ █
```

efter opgradering er serveren ikke sårbar mere

Curl - the HTTP swiss army knife



Christian Panton
@christianpanton

@je5perl

```
panton@fluffy:~$ curl -H "Host: mobil.dr.dk" headertest.panton.org/
Connected: [::ffff:80.62.117.213]:55713

GET / HTTP/1.1
X-Nokia-msisdn: 4531695533
X-Context-id: 1223221667
User-Agent: curl/7.35.0
Accept: */*
Host: mobil.dr.dk
```

30/10/14 22.13

Adding a Host header, made TDC tell which number connected!

What is curl? curl is a command line tool and library for transferring data with URL syntax, supporting DICT, FILE, FTP, FTPS, Gopher, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, Telnet and TFTP. curl supports SSL certificates, HTTP POST, HTTP PUT, FTP uploading, HTTP form based upload, proxies, HTTP/2, cookies, user+password authentication (Basic, Digest, NTLM, Negotiate, kerberos...), file transfer resume, proxy tunneling and more.

Source: <http://curl.haxx.se/>

OWASP top ten



The OWASP Top Ten provides a minimum standard for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.

- The Open Web Application Security Project (OWASP) <http://www.owasp.org>
- Also has Zed Attack Proxy (ZAP)
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project



Konfigurationsfejl - ofte overset

Forkert brug af programmer er ofte overset

- opfyldes forudsætningerne
- er programmet egnet til dette miljø
- er man udannet/erfaren i dette produkt

Kunne I finde på at kopiere cmd.exe til /scripts kataloget på en IIS?

Det har jeg engang været ude for at en kunde havde gjort!

Tilsvarende ser vi jævnligt eksempler på at folk tager input direkte over i shell på Linux

PHP shell escapes



Hvad indeholder hackerens udgave af filen data/config.php
- alt, bagdøre, hack scripts, exploits

```
<pre>
<?php passthru(" netstat -an && ifconfig -a"); ?>
</pre>
```

Andre shell escapes:

- Perl: print `/usr/bin/finger \$input{'command'}`;
- UNIX shell: `echo hej`
- Microsoft SQL: exec master..xp_cmdshell 'net user test testpass /ADD'

resultat: webserveren sender data ud via normal HTTP

Proof of concept programs exist - god or bad?



Some of the tools released shortly after Heartbleed announcement

- https://github.com/FiloSottile/Heartbleed_tool_i_Go
site <http://filippo.io/Heartbleed/>
- <https://github.com/titanous/heartbleeder> tool i Go
- <http://s3.jspenguin.org/sslttest.py> PoC
- <https://gist.github.com/takeshixx/10107280> test tool med STARTTLS support
- <http://possible.lv/tools/hb/> test site
- <https://twitter.com/richinseattle/status/453717235379355649> Practical Heartbleed attack against session keys links til, <https://www.mattslifebytes.com/?p=533> og "Fully automated here "
<https://www.michael-p-davis.com/using-heartbleed-for-hijacking-user-sessions/>
- Metasploit er også opdateret på master repo
<https://twitter.com/firefart/status/453758091658792960>
https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/ssl/openssl_heartbleed.rb

Shellshock CVE-2014-6271 - and others



```
5. vagrant@ubuntu: ~ (ssh)
hlk@katana:speedtest$ ssh vagrant@192.168.0.179
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-30-generic x86_64)

 * Documentation: https://help.ubuntu.com/

System information as of Wed Nov  5 07:55:03 CET 2014

System load:  0.46      Processes:           228
Usage of /:   4.5% of 58.20GB  Users logged in:     0
Memory usage: 15%
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/

Last login: Mon Jul  7 17:08:26 2014
vagrant@ubuntu:~$ dpkg -s bash | grep Version
Version: 4.3-7ubuntu1
vagrant@ubuntu:~$ env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
vulnerable
this is a test
vagrant@ubuntu:~$
```

Source: [https://en.wikipedia.org/wiki/Shellshock_\(software_bug\)](https://en.wikipedia.org/wiki/Shellshock_(software_bug))

Kan udnyttes over HTTP, hvis data rammer en bash shell



Shellshock - multiple vulnerabilities

Here is an example of a system that has a patch for CVE-2014-6271 but not CVE-2014-7169:

```
5. vagrant@ubuntu: ~ (ssh)
vagrant@ubuntu:~$ rm echo
vagrant@ubuntu:~$ X='()' { (a)=>\' bash -c "echo date"
bash: X: line 1: syntax error near unexpected token `='
bash: X: line 1: `'
bash: error importing function definition for `X'
vagrant@ubuntu:~$ cat echo
Wed Nov  5 08:20:24 CET 2014
vagrant@ubuntu:~$
```

```
X='()' { (a)=>\' bash -c "echo date"
```

Source: [https://en.wikipedia.org/wiki/Shellshock_\(software_bug\)](https://en.wikipedia.org/wiki/Shellshock_(software_bug))

The Exploit Database - dagens buffer overflow



EXPLOIT DATABASE

Verified Has App GET CERTIFIED

Show 15 ▾

Search:

Date	D	A	V	Title	Type	Platform	Author
2019-02-25	✗	✗	✗	Drupal < 8.6.9 - REST Module Remote Code Execution	WebApps	PHP	leonjza
2019-02-25	✗	✗	✗	Xlight FTP Server 3.9.1 - Buffer Overflow (PoC)	DoS	Windows	Logan Whitmire
2019-02-25	✗	✗	✗	Advance Gift Shop Pro Script 2.0.3 - SQL Injection	WebApps	PHP	Mr Winst0n
2019-02-25	✗	✗	✗	News Website Script 2.0.5 - SQL Injection	WebApps	PHP	Mr Winst0n
2019-02-25	✗	✗	✗	PHP Ecommerce Script 2.0.6 - Cross-Site Scripting / SQL Injection	WebApps	PHP	Mr Winst0n
2019-02-25	✗	✗	✗	zzzphp CMS 1.6.1 - Remote Code Execution	WebApps	PHP	Yang Chenglong
2019-02-25	✗	✗	✗	Jenkins Plugin Script Security 1.49/Declarative 1.3.4/Groovy 2.60 - Remote Code Execution	WebApps	Java	wetw0rk
2019-02-23	✗	✗	✗	Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution	WebApps	PHP	Charles Fol
2019-02-22	✗	✗	✗	Teracue ENC-400 - Command Injection / Missing Authentication	WebApps	Hardware	Stephen Shkardoon
2019-02-22	✗	✓	✗	Micro Focus Flir 3.4.0.217 - Path Traversal / Local Privilege Escalation	WebApps	Linux	SecureAuth
2019-02-22	✗	✓	✗	Nuuo Central Management - Authenticated SQL Server SQL Injection (Metasploit)	Remote	Windows	Metasploit
2019-02-22	✗	✗	✗	WebKit JSC - reifyStaticProperty Needs to set the PropertyAttribute::CustomAccessor flag for CustomGetterSetter	DoS	Multiple	Google Security Research
2019-02-22	✗	✗	✗	Quest NetVault Backup Server < 11.4.5 - Process Manager Service SQL Injection / Remote Code Execution	WebApps	Multiple	Chris Anastasio
2019-02-21	✗	✗	✗	AirDrop 2.0 - Denial of Service (DoS)	DoS	Android	s4vitar
2019-02-21	✗	✓	✗	MikroTik RouterOS < 6.43.12 (stable) / < 6.42.12 (long-term) - Firewall and NAT Bypass	Remote	Hardware	Jacob Baines

Showing 1 to 15 of 40,914 entries

FIRST PREVIOUS 1 2 3 4 5 ... 2728 NEXT LAST

<http://www.exploit-db.com/>

Nikto webscanner



Description Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 3200 potentially dangerous files/CGIs, versions on over 625 servers, and version specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated (if desired).

Nem at starte, checker en hel del - og kan selvfølgelig udvides

```
nikto -host 127.0.0.1 -port 8080
```

Vi afprøver nu følgende programmer sammen:

Nikto web server scanner <http://cirt.net/nikto2>

Demo: Nikto



```
Script started on Tue Nov  7 17:43:54 2006
$ nikto -host 127.0.0.1 -port 8080 ^M
-----
- Nikto 1.35/1.34      -      www.cirt.net
+ Target IP:          127.0.0.1
+ Target Hostname:    localhost.pentest.dk
+ Target Port:        8080
+ Start Time:         Tue Nov  7 17:43:59 2006
...
+ /examples/ - Directory indexing enabled, also default JSP examples. (GET)
+ /examples/jsp/snp/snoop.jsp - Displays information about page
retrievals, including other users. (GET)
+ /examples/servlets/index.html - Apache Tomcat default JSP pages
present. (GET)
```

Demo nikto - burde finde nogle ting

Falske positiv vs falske negativ!

Exercise

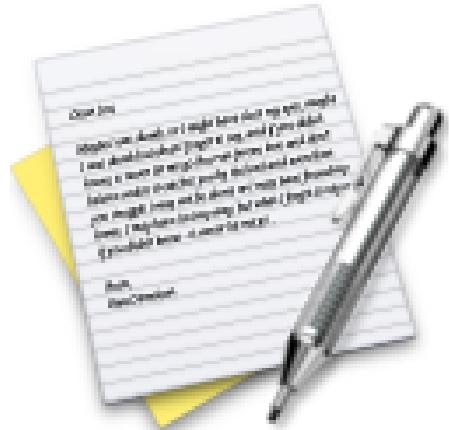


Now lets do the exercise

ℹ Nikto Web Scanner 15 min

which is number **15** in the exercise PDF.

Exercise



Now lets do the exercise

❶ Whatweb Scanner 15 min

which is number **16** in the exercise PDF.



Cross-site scripting

Vi har primært snakket om server angreb - men klienter er også utsatte

Hvis der inkluderes brugerinput i websider som vises, kan der måske indføjes ekstra information/kode.

Hvis et CGI program, eksempelvis comment.cgi blot bruger værdien af "mycomment" vil følgende URL give anledning til cross-site scripting

```
<A HREF="http://example.com/comment.cgi?  
mycomment=<SCRIPT>malicious code</SCRIPT>  
">Click here</A>
```

Hvis der henvises til kode kan det endda give anledning til afvikling i anden "security context"
Kilde/inspiration: <http://www.cert.org/advisories/CA-2000-02.html>

Mini proxy: Tamper Data



Screenshot of the Tamper Data extension interface in Firefox. The main window shows a list of ongoing requests with columns for Time, Duration, URL, Method, Status, Headers, and Body. A modal dialog titled "Tamper with request?" is open over the list, showing a preview of the selected request to "http://www.google.com" and a checkbox for "Continue Tampering?". Below the modal are three buttons: "Submit", "Abort Request", and "Tamper" (which is highlighted). To the right of the modal, there is a sidebar with sections for "Load Flags" and "Show All".

Time	Duration	URL	Method	Status	Headers	Body
11:35:25....	381 ms	http://www.google.com	GET	pending	unknown	https://... LOAD_REPLACE
11:35:25....	415 ms	/cse?cx=011692378426958990819%3Aylz6v6oe6lq&q=blah&sa=Search&siteurl=www.prosa....				http://w... LOAD_NORMAL
11:35:25....	453 ms					//w... LOAD_NORMAL
11:35:25....	448 ms					//w... LOAD_NORMAL
11:35:25....	595 ms					//w... LOAD_NORMAL
11:35:25....	0 ms					ss://... LOAD_REPLACE
11:35:25....	0 ms					LOAD_REPLACE
11:35:26....	0 ms					http://w... LOAD_NORMAL
11:35:26....	6268 ms		-1	GET	304	application/x-unk... https://... LOAD_NORMAL
11:35:26....	530 ms		35	GET	200	image/gif https://... LOAD_REPLACE
11:35:26....	0 ms		0 ms	unknown	GET	pending unknown https://... LOAD_DOCUME...
11:35:26....	1278 ms		37	GET	200	image/gif https://... LOAD_NORMAL
11:35:26....	0 ms		-1	GET	Loaded fro...	unknown http://w... LOAD_FROM_C...
11:35:26....	0 ms		0 ms	unknown	GET	pending unknown http://w... LOAD_NORMAL
11:35:39....	0 ms		0 ms	unknown	GET	pending unknown http://s... LOAD_NORMAL
11:35:39....	0 ms		0 ms	unknown	GET	pending unknown https://... LOAD_REPLACE

Udvidelse til Firefox som opfanger request og kan modificere inden de sendes
<https://addons.mozilla.org/en-US/firefox/addon/tamper-data/>

Sqlmap



sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Features

Automatic SQL injection and database takeover tool <http://sqlmap.org/>

sqlmap features



'Features' :-

- Full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB and HSQLDB database management systems.
- Full support for six SQL injection techniques: boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band.
- Support to directly connect to the database without passing via a SQL injection, by providing DBMS credentials, IP address, port and database name.
- Support to enumerate users, password hashes, privileges, roles, databases, tables and columns.
- Automatic recognition of password hash formats and support for cracking them using a dictionary-based attack.
- Support to dump database tables entirely, a range of entries or specific columns as per user's choice. The user can also choose to dump only a range of characters from each column's entry.

Not a complete list!

Source: <http://sqlmap.org/>

Burpsuite



Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.

Burp suite indeholder både proxy, spider, scanner og andre værktøjer i samme pakke

<http://portswigger.net/burp/>

<https://pro.portswigger.net/bappstore/>

Udviklingsstandarde



Hvad gør I for at undgå problemer som de her nævnte? - kan man gøre mere?

Man børe være klar over hvilke teknologier man bruger

Standardiser på et mindre antal produkter, biblioteker, sprog

Regler og procedurer skal hele tiden opdateres:

- Kvalitetssikring
- Retningslinier for tilladte tags
- Retningslinier for brug af SQL

Ved at fokusere på antallet af produkter kan man måske indskrænke mulighederne for fejl, høj kvalitet er ofte mere sikkert

nye produkter kan være farlige til man lærer dem at kende!

Retningslinier



- Hvis der ikke findes retningslinier for udvikling så etabler disse
- eksempel:
javascript må gerne benyttes til at validere forms for at give hurtig feedback til brugeren
- serveren der modtager input fra brugeren validerer alle data sikkerhedsmæssigt
- Retningslinierne er medvirkende til at foretage en afbalanceret investering i sikkerheden
- undgå dyre hovsa løsninger
- undgå huller i sikkerheden, ens niveau
- Der findes vejledninger til både gamle og nye sprog/systemer,
eks Ruby On Rails Security Guide
<http://guides.rubyonrails.org/security.html>
- OWASP Cheat sheets
https://www.owasp.org/index.php/PHP_Security_Cheat_Sheet

Change management



Er der tilstrækkeligt med fokus på software i produktion

Kan en vilkårlig server nemt reetableres

Foretages rettelser direkte på produktionssystemer

Er der fall-back plan

Burde være god systemadministrator praksis

Undgå også opdatering af prod databaser med manuelle SQL queries

Attacking Authentication



Passwords vælges ikke tilfældigt

The 50 Most Used Passwords

- | | | | | |
|--------------|--------------|----------------|--------------|-------------|
| 1. 123456 | 11. 123123 | 21. mustang | 31. 7777777 | 41. harley |
| 2. password | 12. baseball | 22. 666666 | 32. f*cky*u | 42. zxcvbnm |
| 3. 12345678 | 13. abc123 | 23. qwertyuiop | 33. qazwsx | 43. asdfgh |
| 4. qwerty | 14. football | 24. 123321 | 34. jordan | 44. buster |
| 5. 123456789 | 15. monkey | 25. 1234...890 | 35. jennifer | 45. andrew |
| 6. 12345 | 16. letmein | 26. p*s*y | 36. 123qwe | 46. batman |
| 7. 1234 | 17. shadow | 27. superman | 37. 121212 | 47. soccer |
| 8. 111111 | 18. master | 28. 270 | 38. killer | 48. tigger |
| 9. 1234567 | 19. 696969 | 29. 654321 | 39. trustno1 | 49. charlie |
| 10. dragon | 20. michael | 30. 1qaz2wsx | 40. hunter | 50. robert |

Source: <https://wpengine.com/unmasked/>

Brute Force Testing



hvad betyder bruteforcing?
afprøvning af alle mulighederne

```
Hydra v2.5 (c) 2003 by van Hauser / THC <vh@thc.org>
Syntax: hydra [[[ -l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]]
[-o FILE] [-t TASKS] [-g TASKS] [-T SERVERS] [-M FILE] [-w TIME]
[-f] [-e ns] [-s PORT] [-S] [-vV] server service [OPT]
```

Options:

- S connect via SSL
- s PORT if the service is on a different default port, define it here
- l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
- p PASS or -P FILE try password PASS, or load several passwords from FILE
- e ns additional checks, "n" for null password, "s" try login as pass
- C FILE colon seperated "login:pass" format, instead of -L/-P option
- M FILE file containing server list (parallizes attacks, see -T)
- o FILE write found login/password pairs to FILE instead of stdout

...

Session IDs



- Session IDs tie the user with the state on the server
- Must be randomly assigned, otherwise an attacker can guess a valid ID
- Common problems, time based or predictable in some way
- Check code for generating IDs or measure - Phase Space Analysis

Exercise



Now lets do the exercise

⚠ JuiceShop Attacks 60min

which is number **17** in the exercise PDF.

For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools