Web security and privacy - Final exam – 22 June 2018

FOR NON-ENGLISH: 2 penalty points
FOR UNREADABLE HAND-WRITING: discretionary decision
PLEASE WRITE BY USING A BALLPOINT PEN (AND NOT A PENCIL)

WEB SECURITY (prof. d'Amore) (time: 60 mins)

1. **Email forensics**. Analyse the following fragment of header (of an email message) and describe at your best what interesting information can be derived.

```
Delivered-To: damore@dis.uniroma1.it
Received: by 2002:a4a:cf0f:0:0:0:0:0 with SMTP id l15-v6csp4421924oos;
        Mon, 18 Jun 2018 13:24:23 -0700 (PDT)
X-Google-Smtp-Source:
ADUXVKK8Q2Prk08jyD+osbsax1pSndpJsevaF54Gh636msOmgdrwL/TR4Hxwc0fOOkcAWGvh+8GX
X-Received: by 2002:a17:902:6b04:: with SMTP id
o4-v6mr15906514plk.101.1529353463509;
        Mon, 18 Jun 2018 13:24:23 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1529353463; cv=none;
        d=google.com; s=arc-20160816;
        b=WX8XllbHt/SFxWtOYtnfBlM2XQx104yXGPNEJWbPiRxgQ7+dL4BTWKchxEVCTmpHd9
         o70SwS2cCksp29XVF+ADrR50JYLx1CodKVj+1bevekw4fBHjdPwSY9EqXdpdyxrta5d+
         RioBtyLlqtwfODveTmPmdsSzJg3oFjC/OLzrKcCg26hLdwlBMA0DE40jgThl4a/TCuKg
         Q7Ldr07DtYRLECcK13Y68hoiiCgtnQfDIXVozsieKl1frUAxM8TOZv/LcBhFCJW1Wzp0
         Rja0kdP6h8pEvqkoBCKCU5kVsR+SQAy8gNMVd6nEhmvMA4K69k1sHBBSBhCzl1F85L8B
         +Fiw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com;
s=arc-20160816;
        h=content-transfer-encoding:mime-version:message-id:date:subject:to
         :from:reply-to:arc-authentication-results;
        bh=MPkGVrxHHh4Q78wojn1EJA9O1liC6O5tIDnoeWdJx+E=;
        b=y9+QJyUdqfuWjr4kd1+BSwgwy4SKRF9vbDnamQzėCjgFCAHjWz2KZdiejE1MBXsuiF
         eIEnJdDOnWJ0E31JWByt36HgQJsdfnX0bbAzmYdZ8dY1dz1nPM3lBEvSjYhX2MslIttg
         MXu3jT/fbi7UwZfQFanjyEu9+FPxePwMJLK/Qrx+ZNakQqzfZEonHxL1lMHiT8aV/QZk
         UjGyITNNYSYwlYfplQw6RbAyLlPxnA10wNTtrlFaSUqaE7wW42MVj/kIjaTFSCu1BhUL
         +Xtgbve55tVJ6hQvHsmO7zNEoPtLYHxvKBJgfg5LBXTStrXKzeqXTYf90t4TnEwI96Ci
         uAYQ==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=neutral (google.com: 67.219.250.2 is neither permitted nor denied by
best guess record for domain of
donotreply-ms0365tech@00ddns-urlonmicrosoft-net.com)
smtp.mailfrom=donotreply-MS0365Tech@00ddns-urlonmicrosoft-net.com
Return-Path: <donotreply-MS0365Tech@00ddns-urlonmicrosoft-net.com>
Received: from mail1.bemta24.messagelabs.com (mail1.bemta24.messagelabs.com.
[67.219.250.2])
        by mx.google.com with ESMTPS id
b39-v6si16497424plb.249.2018.06.18.13.24.23
        for <damore@dis.uniroma1.it>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Mon, 18 Jun 2018 13:24:23 -0700 (PDT)
Received-SPF: neutral (google.com: 67.219.250.2 is neither permitted nor denied
by best guess record for domain of
```

```
donotreply-ms0365tech@00ddns-urlonmicrosoft-net.com) client-ip=67.219.250.2;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: 67.219.250.2 is neither permitted nor denied by
best guess record for domain of
donotreply-ms0365tech@00ddns-urlonmicrosoft-net.com)
smtp.mailfrom=donotreply-MS0365Tech@00ddns-urlonmicrosoft-net.com
Return-Path: <donotreply-MS0365Tech@00ddns-urlonmicrosoft-net.com>
Received: from [67.219.250.99] (using TLSv1.2 with cipher
DHE-RSA-AES256-GCM-SHA384 (256 bits))
       by server-2.bemta.az-a.us-west-2.aws.symcld.net id B4/B5-01623-6F4182B5;
Mon, 18 Jun 2018 20:24:22 +0000
X-Brightmail-Tracker: H4sIAAAAAAAAA+NgFupjkeJIrShJLcpLzFFi42I5XXe/WfebiEa
  0weyl7Badbe9ZHBg9FtzdwRTAGMWamZeUX5HAmrHugnDBQ96K5Tc/sDQw3uPpYuTkEBIwkjj0
  fDcbiM0mECcx69d2JhBbREBK4sO7HmYQW1jAXeLgz5ssIDaLgILErzObGUFsXgFviY4H7UwQt
  qDEyZlPwGqYBfQk3nVuZYawtSWWLXzNPIGRcxaSs1lIymYhKVvAyLyK0SKpKDM9oyQ3MTNH19
  DAQNfQ0EjX0BhIm5noJVbpJuqVFuuWpxaX6BrpJZYX6xVX5ibnpOjlpZZsYgSGBAMQ7GC8eCj
  lEKMkB5OSKG/IS/VoIb6k/JTKjMTijPii0pzU4kOMMhwcShwHJi/sIa0UKCRanpqRVpmTnA4IRJ
  S3DwKInwhoCkeYsLEnOLM9hUqcY49H4KkDwHJi+ASCWvPy8VClx3gkXqnpOjlpZZsYgSGBAMQ7GC8eCj
  RmleXBDYdF0iVFWSpiXEehMIZ6C1KLczSuB2eDLuSuB2vwI6iwnorC0eCj
  BnlSQipKQaGF0iVCatqj5f7NLLo7P9+Y/55cfFghZXxR9dr3RA8EUEB0/d96RFNTlF6z3ijq2
  w/pWe/rrE8Mk+Xh3DG6YNNk2z5p3dbrK/I+f7klhhzr0ciU/+5f6xNZyVELCcOfy+hdftjI0H
  opiO2fiz8yyRXuTy7omg7PVjO25PerTmttm16xa9fwtCnZVYijMSDbWYi4oTAUNyvhuhAgAA
X-Env-Sender: donotreply-MS0365Tech@00ddns-urlonmicrosoft-net.com
X-Msg-Ref: server-31.tower-323.messagelabs.com!1529353458!141281!1
X-Originating-IP: [203.126.223.131]
X-SYMC-ESS-Client-Auth: outbound-route-from=fail
X-StarScan-Received:
X-StarScan-Version: 9.9.15; banners=-,-,-
X-VirusChecked: Checked
Received: (qmail 28703 invoked from network); 18 Jun 2018 20:24:21 -0000
Received: from melchers.melchers.com.sg (HELO 00ddns-urlonmicrosoft-net.com)
(203.126.223.131)
  by server-31.tower-323.messagelabs.com with DHE-RSA-AES256-GCM-SHA384
encrypted SMTP; 18 Jun 2018 20:24:21 -0000
Reply-To: ms0365tech@00ddns-urlonmicrosoft-net.com
From: Head of Financial Adviser Services
<donotreply-MS0365Tech@00ddns-urlonmicrosoft-net.com>
To: damore@dis.uniroma1.it
Subject: [Info] Mail for damore@dis.uniroma1.it  6/19/2018 4:24:27 a.m.
Date: 19 Jun 2018 04:24:35 +0800
Message-ID: <20180619042427.B6B30BA0936B9715@00ddns-urlonmicrosoft-net.com>
MIME-Version: 1.0
Content-Type: text/html;
       charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
```

2. **Injection attacks**. In the framework of the web applications discuss what *injection attacks* are, make some *examples*, clearly identifying the *targets*.

3. **Tracking**. What is the *browser fingerprinting* and how it can be used by ISP, first party and third-parties for threatening the user privacy?