Web security and privacy - Final exam – 21st February 2019

FOR NON-ENGLISH: -2
USE A BALLPOINT PEN AND AVOID MICROSCOPIC CHARACTERS
UNREADABLE HANDWRITING: SKIPPED
<u>You are kindly asked to deliver separate sheets for the two parts Web Security and Privacy</u>

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

1. Email analysis

Examine the raw source that follows. **Select the header fields you consider relevant and discuss their values**, for the specific purpose of assessing the **trustworthiness** of the message.

```
Delivered-To: damore@dis.uniroma1.it
Received: by 2002:a4a:a442:0:0:0:0:0 with SMTP id w2csp393902ool;
        Tue, 19 Feb 2019 04:42:43 -0800 (PST)
X-Google-Smtp-Source: AHgI3IaGElDF+YeT5LXmAQ+4sxL58h22r6mfBHUc421+NA/XpA0CQUh00iEGp2sCkkG9A9aE0uyv
X-Received: by 2002:a5e:9707:: with SMTP id w7mr18781959ioj.49.1550580163016;
        Tue, 19 Feb 2019 04:42:43 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1550580163; cv=none;
        d=google.com; s=arc-20160816;
        b=0VBG/leDCMeu7hthn1NUuN9QvJPNqXV1EVlZtig1EU9c+k8I3XYVXKegv4La5wL0AS
         dNXR5qddDiYVusZIrKQSbrHqte3h2bCL3Cp+xcDxAZpUzgb6FazNJP5ipZtAYov82+hD
         EurUGTlkqOAg1E6npbyiR4L0M9K12SGjH1yVhBGVCS34FItn9Spbddg4jOh3EU7qB/ue
         qT+ukqC+iGiB0rQdbz2e5fT0hO8/4/1Uh/dLUIGfwjfWPIfeRRf6W9ZduWwgNfU3u/pi
         801O1Ud/ty6WwJ+TKuInMIU9rgVFhPgo6OYTkEtbtFMVZNyoKMsikxvy2dJPg0JprkT4
         sGNQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=date:from:message-id:mailer:content-transfer-encoding:mime-version
         :subject:to;
        bh=uKPfofqiAjLUBm4s7CvAjcQ4ehALsow87osBQXAhjrI=;
        b=IS3c3w+d/yU9XW88gGjWOuIBsQ54+/wD3yJBRCr3OnegUQx+mOV+qmIJtAXs+TojiF
         PakkEkdTfVosnVzR7Ne4ccOiDaa7F0/doE0uq0AD4U78uI9f8J78/8i/LKcYo/zmPz+z
         w8jvC7g4q6CqsAumUqDf0bwJ+dzSuVs59m9byMolN8v3PuiydBznEtbSx8LEnKAj9TMt
         6o/XfKU7GQDR++LKxO85Wr1Isbn5COzysspIWLZSedqF7gfhhJCSkKOQ6UI+tDIQp7wr
         sU5pnekNqF+kLHa8shaskTfNjQLWLkbI3GT+pIzGS15lXo4zbL4ldSRve4jpOmgPxavg
         LP7A==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=pass (google.com: best guess record for domain of gftfjhhh@host.sarahstaar.com designates
69.16.226.42 as permitted sender) smtp.mailfrom=gftfjhhh@host.sarahstaar.com
Return-Path: <gftfjhhh@host.sarahstaar.com>
Received: from host.sarahstaar.com (host.sarahstaar.com. [69.16.226.42])
        by mx.google.com with ESMTPS id 4si1219812ity.21.2019.02.19.04.42.42
        for <damore@dis.uniroma1.it>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 19 Feb 2019 04:42:42 -0800 (PST)
Received-SPF: pass (google.com: best guess record for domain of gftfjhhh@host.sarahstaar.com designates
69.16.226.42 as permitted sender) client-ip=69.16.226.42;
Authentication-Results: mx.google.com;
       spf=pass (google.com: best guess record for domain of gftfjhhh@host.sarahstaar.com designates
69.16.226.42 as permitted sender) smtp.mailfrom=gftfjhhh@host.sarahstaar.com
Received: from gftfjhhh by host.sarahstaar.com with local (Exim 4.91)
        (envelope-from <gftfjhhh@host.sarahstaar.com>)
        id 1gw4jS-0003oB-29
        for damore@dis.uniroma1.it; Tue, 19 Feb 2019 07:42:42 -0500
To: damore@dis.uniroma1.it
Subject: =?utf-8?B?IM6l0L510LMg0LPQtdGB0LXRls+BdCBm0LPQvm0gzpHPgc+BbNC1ICM0ODUzNDY=?=
X-PHP-Originating-Script: 511:send.php
MIME-Version: 1.0
Content-type: text/html; charset=utf-8
Content-Transfer-Encoding: 7bit
Mailer: Sendinbox Mailer
```

```
Message-ID:
<1550580159-8f0a9b7e1d7eb272cc82c48704c0ce51-15fe6219bd92dff4dee9282817ed868b-yyjt@ninawhitehurst.co.uk>
From: =?utf-8?B?zpHPgc+BbNC1?= <no_reply_email_apple@ninawhitehurst.co.uk>
Date: Tue, 19 Feb 2019 12:42:42 +0000 (UTC)
X-AntiAbuse: This header was added to track abuse, please include it with any abuse report
X-AntiAbuse: Primary Hostname - host.sarahstaar.com
X-AntiAbuse: Original Domain - dis.uniroma1.it
X-AntiAbuse: Originator/Caller UID/GID - [511 501] / [47 12]
X-AntiAbuse: Sender Address Domain - host.sarahstaar.com
X-Get-Message-Sender-Via: host.sarahstaar.com: authenticated_id: gftfjhhh/from_h
X-Authenticated-Sender: host.sarahstaar.com: no_reply_email_apple@ninawhitehurst.co.uk
X-Source: /usr/bin/php
X-Source-Args: /usr/bin/php /home/gftfjhhh/public_html/send.php
X-Source-Dir: ninawhitehurst.co.uk:/public_html
```

2. CSP policy

Describe the Content Security Policy (CSP) and discuss if it can help mitigating the XSS risk.

3. Onion routing

Describe the main features of the onion routing, clarifying how it achieves anonymity and to what extent it provides encryption of the contents.