

G.7: Cookie-ak, Sesioak eta Egoeraren mantentzea HTTPn. Webeko informazio-sistemen segurtasuna



Rosa Arruabarrena, Jose Ángel Vadillo
LSI, UPV/EHU

1

Sesioa (saioa) eta *session* objektua (I)



- HTTP protokoloak ez du eskaeren arteko egoera mantentzen
- Hala ere, maiz, elkarren artean erlazionatuak dauden arakatzaille-zerbitzari arteko (request-response) interakzio multzoek, euren arteko taldekatze logikoa behar dute.
- Taldekatze hori **sesioa (saioa)** kontzeptuarekin bat dator

2



Sesioa eta *session* objektua (II)

- Sesio kontzeptua gauzatzeko *session* objektua erabiltzen da
 - *Session* objektu bat sortuko da web zerbitzari eta bezero arteko interakzioa multzo bat talde bezala maneiatu behar den aldi bakoitzean
 - Web aplikazioak zerbitzarian (aldi baterako) *session*-aren instantzia bat sortzen du, identifikatzaile bakarrekoa
 - *Session*-aren instantzia honetan balio globalak metatzen dira, orri desberdinek sesio berdinen barnean erabiliko dituztenak (adib. , sesioaren identifikatzaile bera, erabiltzailearen izena, balio akumulatuak, ...).

3



session objektua (III)

- Erreminta hau, normalki *kautotzea* (*autentikazioa*) eta erabiltzaileen jardueren jarraipena egiteko erabiltzen da, atal pribatuak dituzten webetan haien atzipen-kontrola egin behar denean
 - Behin erabiltzailea kautotu denean, sesioaren identifikatzailea joan-etorri tiketa bat balitz bezala erabil liteke, zenbait orritara sartzeko baimena emango diolarik, berriz ere kautotu gabe
- Sesioaren maneioak atzipenen kontrola eta ikuskapena errazten eta bateratzen ditu. Baina, web aplikazioak ahuleziaren bat balu, aplikazio osoaren segurtasuna honda lezake

4



Sesioaren IDentifikadorea (SID)

- Luzera handiko ausazko sekuentzia bat izan ohi da, aplikazioaren atzipena eskatu duen nabigatzaileari *Cookie* bidez igortzen zaiona
- SID-ari esker une zehatz batean aplikazio berdinarekin interakzionatzen/elkarreragiten ari diren bezeroak identifika edota bereiz litezke
- Zerbitzari aldeko aplikazioek datuak metatzen dituzte *session* objektuan, nabigatzaile horrek exekuzio “berean” egiten dituen atzipen desberdinetan datu horiek eskuragarri egon daitezen

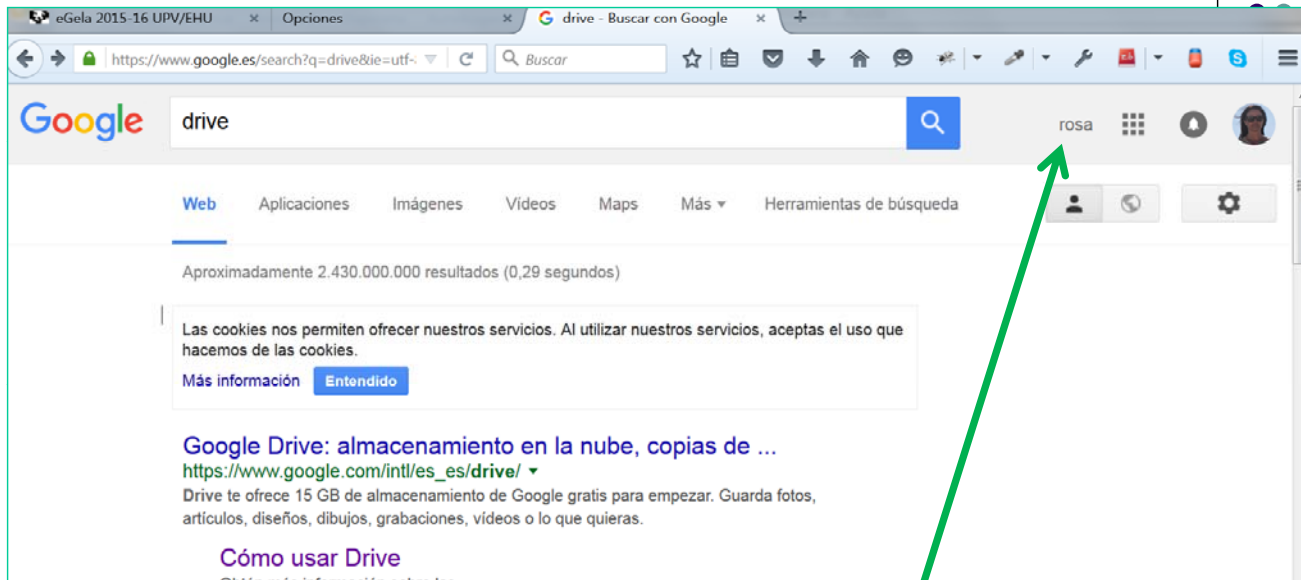
5

SID-a egoera gordetzeko



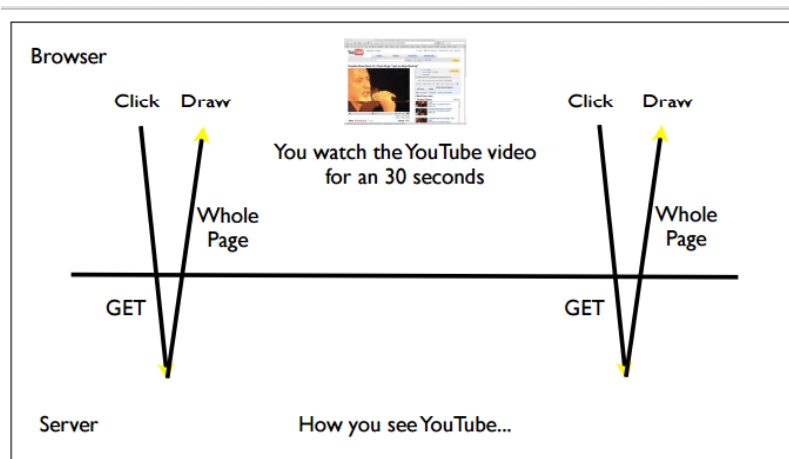
- SID-ak bidaltzeko eta jasotzeko aukerak:
 1. Orriaren URLean SIDa gehituz (GET erabilitz)
 2. Formularioko zenbait eremutan SIDa metatuz, POST metodo bidez igorriko dena. Normalki *hidden* moduko eremuak erabili ohi dira informazio hau metatzeko
 3. *Cookie-n erabilpen bidez* ←

6

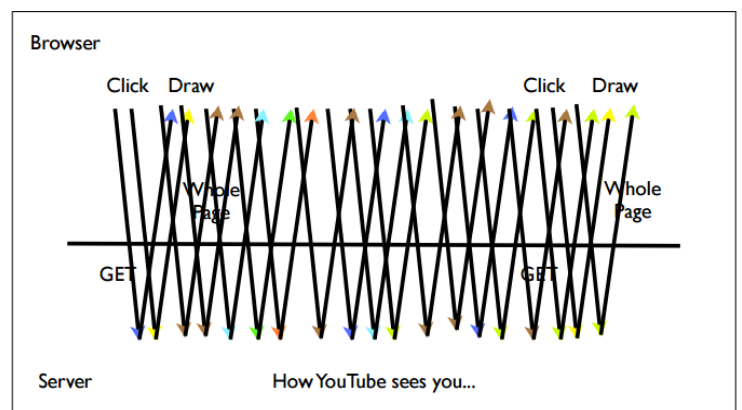


Google-k, logina egin baduzu, hura “gogoratzten” du

7



Itxuraz badirudi ere ...



Errealitatea bestelakoa da ...

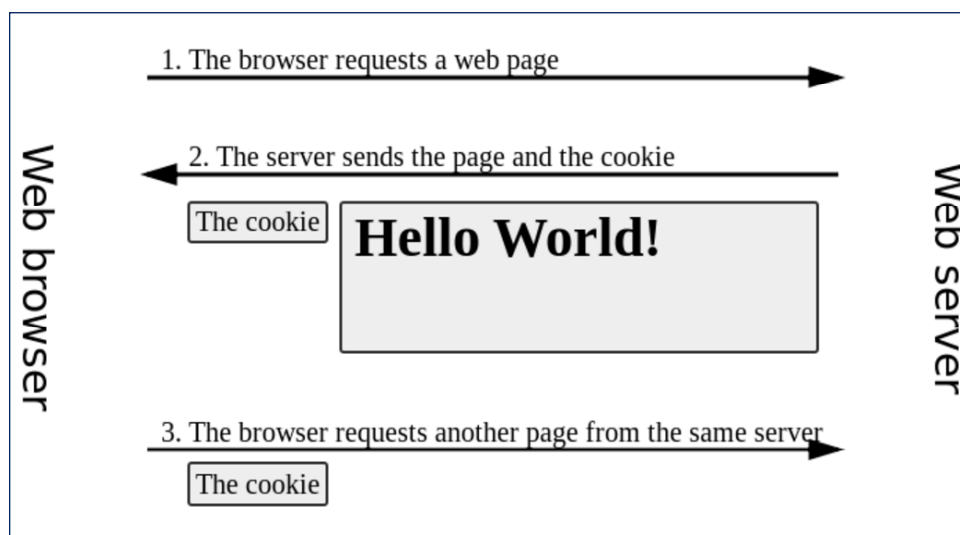
8



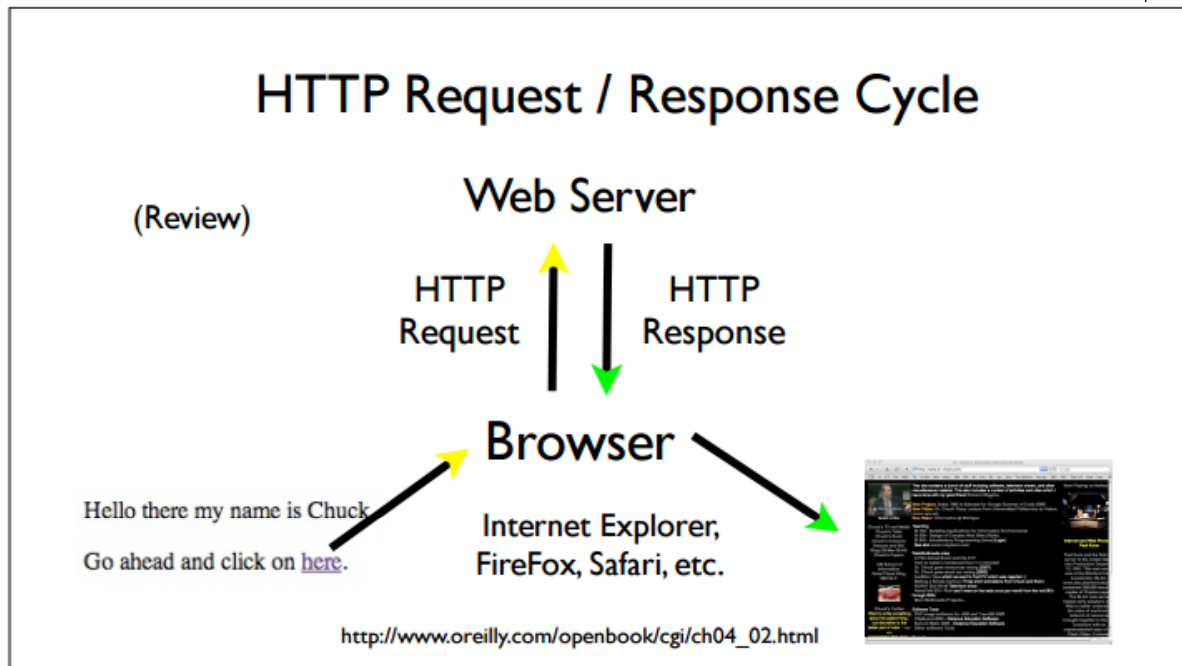
Cookie-ak

- Cookie-ak **HTTP** protokoloaren **gabezi bat gaintitzeko** gehitu ziren. Hain zuzen, protokolo horrek bezero-zerbitzarien arteko elkarrekintzen arteko konexioa ezin gorde izanagatik
- Cookie-ak **informazio puskak** dira, gehienez 4KB-eko tamaina izango dutenak eta zerbitzaritik bezerora eta alderantziz igorriko direnak **http trama barnean**.
- **Nabigatzaileek** cookientzat **biltegi** bat dute. Cookie-ak **domeinu** bati erlazionatzen/lotzen dira. Horrela, nabigatzaileak domeinu bati eskaera bat luzatu behar dioenean, cookie-rik erlazionaturik duen baieztatuko du eta, hala balitz, *http-request*-ren atal bat bezala gehituko lioke informazio hori.
- Zerbitzariak *http-response*-an cookie bat gehitu badu, nabigatzaileak *responsea* prozesatu ostean, **cookie-aren balio berria eguneratu** du, igorri duen domeinuari lotuz

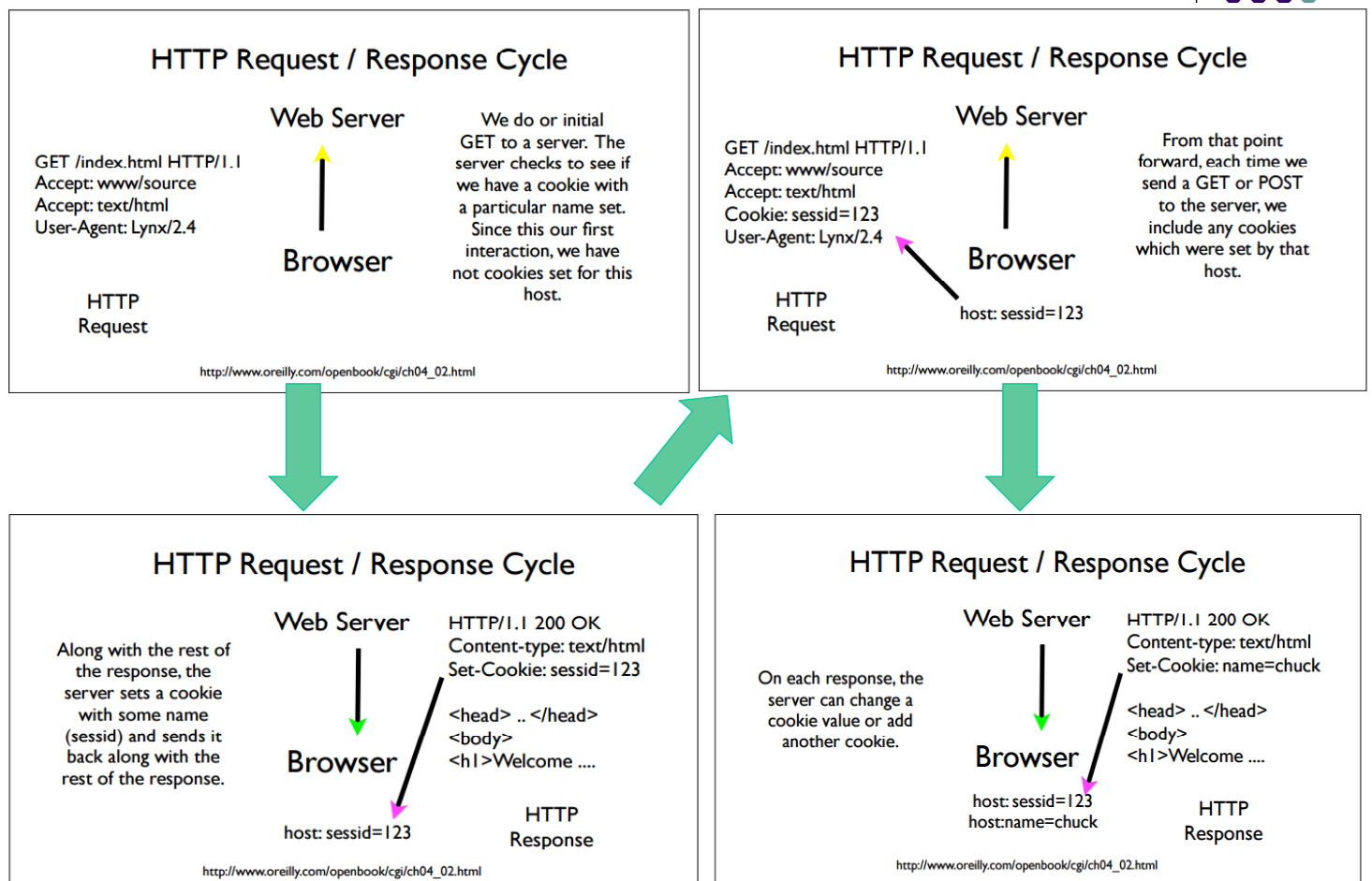
9



A possible interaction between a web browser and a server holding a web page in which the server sends a cookie to the browser and the browser sends it back when requesting another page.



11



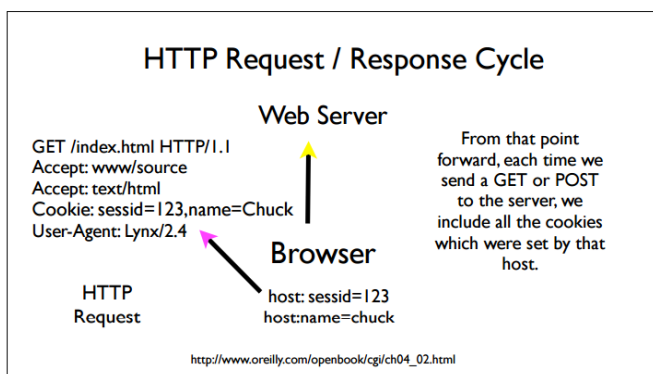
12



Nabigatzaileak eta cookie-ak

- Nabigatzaileak **cookie** bat jasotzen duenean, **domeinu bati erlazionaturik** gordeko du hura, izen bat eta balio bat izango dituelarik gutxienez
- Cookie-ak **“iraungitze-data”** izan dezakete edo **iraunkorrak** izan litezke
- Cookie-ak domeinu bateko **path batetara mugatuak** egon litezke
- Bestalde, gerta liteke cookie-a **“blindatua”** egotea ere, eta soilik http barneko protokoloaren testuinguruan atzigarri izatea (eta ez, adibidez, JavaScriptatik)
- Nabigatzaileek **erabilgarritasun espezifikoak eta plugin-ak** dituzte cookie-ak kontsultatzeko eta eguneratzeko, bai eta haien erabilera mugatzeko.

13



chrome://settings/cookies

Datos de sitios y cookies

| Sitio | Datos locales | Eliminar t |
|----------------------|---------------------------------|------------|
| github.com | 3 cookies, Almacenamiento local | |
| google-analytics.com | ID de canal | |
| google.co.in | 2 cookies, ID de canal | |
| www.google.co.in | Almacenamiento local | |
| google.com | 10 cookies, ID de canal | |
| accounts.google.com | 5 cookies | |
| apis.google.com | 1 cookie | |
| clients5.google.com | Almacenamiento local | |

Elements Network Sources Timeline Profiles Resources Audits Console

Frames

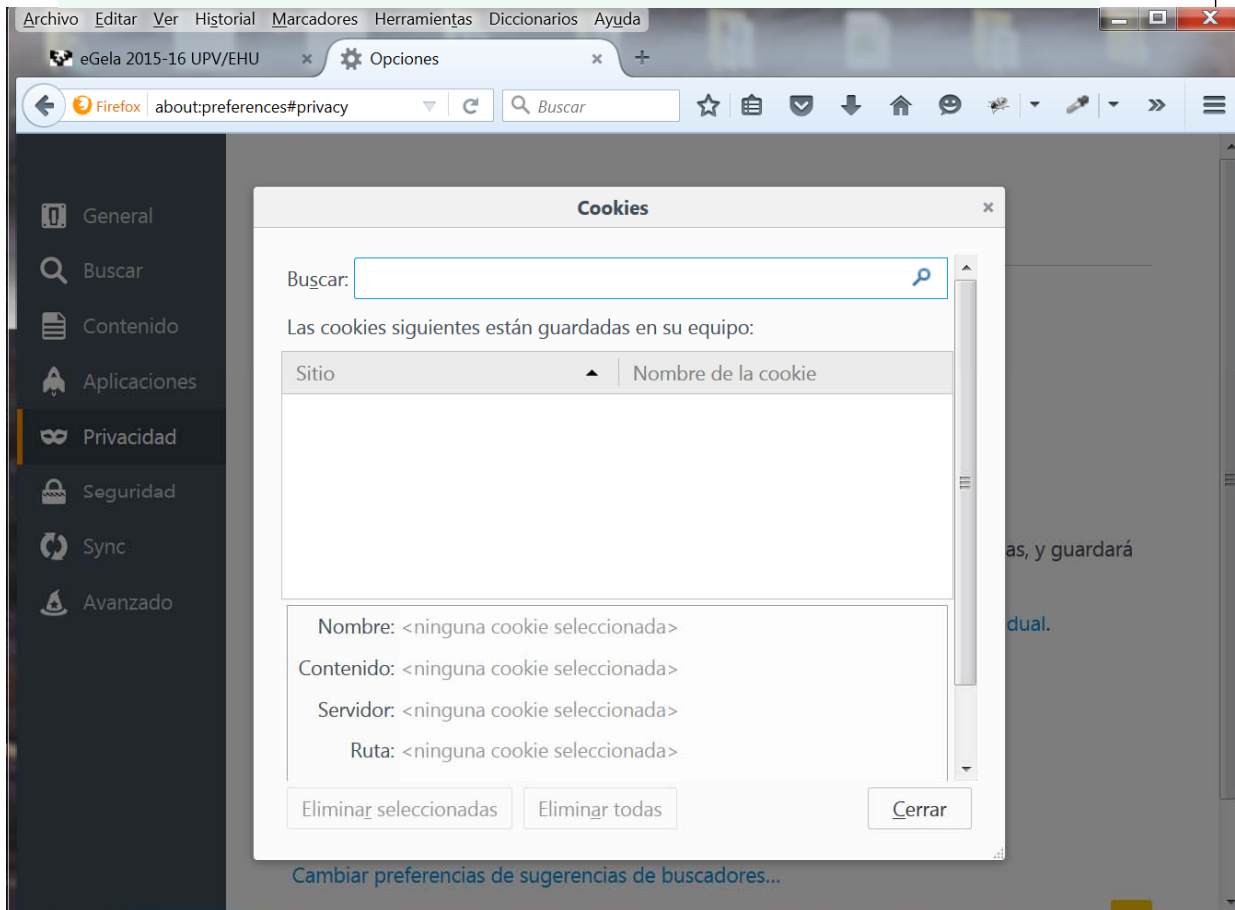
- Web SQL
- IndexedDB
- Local Storage
- Session Storage
- Cookies
 - plus.google.com
 - clients5.google.com
 - talkgadget.google.com
 - 0.client-channel.google.com
 - clients4.google.com
 - accounts.google.com
 - clients6.google.com
 - Application Cache

SSID

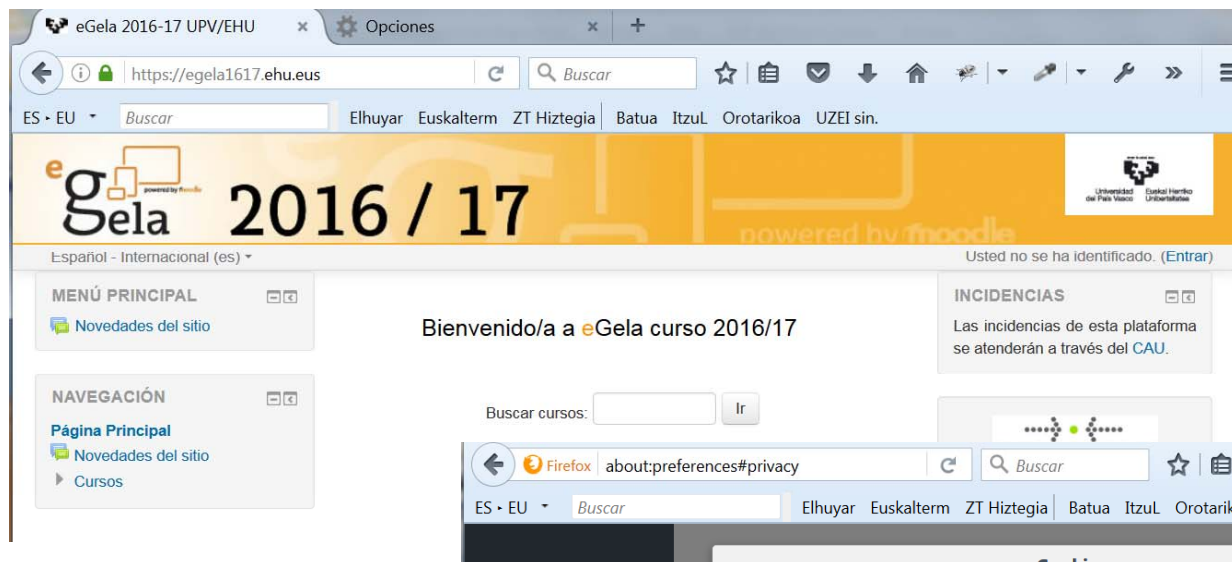
Refresh
Delete
Clear all from ".google.com"
Clear all

| Name | Value | Domain | Path | Expires / Max-Age | Size | HTTP | Secure |
|-----------------|---|---------------------|------|--------------------------|------|------|--------|
| ACCOUNT_CHOOSER | AFx_qTAT53tyhMBIAD...iPdqbkR1R6gQXLLWvXvx-KEP7EEPQFF5H03adNsbthS_P2e... | accounts.google.com | / | 2016-11-09T07:58:49.023Z | 155 | ✓ | ✓ |
| APISID | THK1K1-2kq-n4juw/Avb8E8qin8iwtmsD | .google.com | / | 2016-11-09T14:10:08.039Z | 40 | | |
| GALX | IIWolvuAbVA | accounts.google.com | / | Session | 15 | | ✓ |
| GAPS | 1ZehNA_NH12wFIMqTb9iRe_brXhUdg:SRHfMSfAPziWzWMC | accounts.google.com | / | 2016-11-09T14:10:08.039Z | 53 | ✓ | ✓ |
| HSID | A9oFgheHwHC8RiV5 | .google.com | / | 2016-11-09T14:10:08.039Z | 21 | ✓ | ✓ |
| LSID | LSOSID | accounts.google.com | / | 2016-11-09T14:10:08.039Z | 418 | ✓ | ✓ |
| OGPC | DQAAAAIBAAA7wZLqUoOxTnyobRH59VRdqM9QYPLtFKU6NzyeERU4Rb8FjH9... | accounts.google.com | /o | 2016-11-09T11:17:25.464Z | 380 | ✓ | ✓ |
| PREF | 67=qF0YHfLSghsPdJlCslEw7C4d4wRHwXlMpnwgtgPj8GAJeB6iY5gyhvuZHTb3VLVN... | .google.com | / | 2015-05-12T14:10:08.039Z | 185 | ✓ | ✓ |
| SAPSID | 4061130-1: | .google.com | / | 2014-12-10T14:09:35.000Z | 14 | | |
| SSID | ID=d9df2c404dabb70:FF=0:TM=1415628565:LM=1415628565:S=gX_SejmhU2V8IE... | .google.com | / | 2016-11-09T14:09:36.156Z | 75 | | ✓ |
| SSID | CIBgqOvG4iPqyOY/9B8WchW2Kl3y2IZ | .google.com | / | 2016-11-09T14:10:08.039Z | 41 | | ✓ |
| SSID | DQAAAAIBAAA7wZLqUoOxTnyobRH59VRdqM9QYPLtFKU6NzyeERU4Rb8FjH9... | .google.com | / | 2016-11-09T14:10:08.039Z | 355 | | ✓ |
| SSID | A0Jo_PK5dOkuh0ul | .google.com | / | 2016-11-09T14:10:08.039Z | 21 | ✓ | ✓ |

Nabigatzailea zabaldu hala, oraindik cookie-rik ez izatea gerta liteke
(Edo aurreko konexioren bateko datuak izan ditzake)

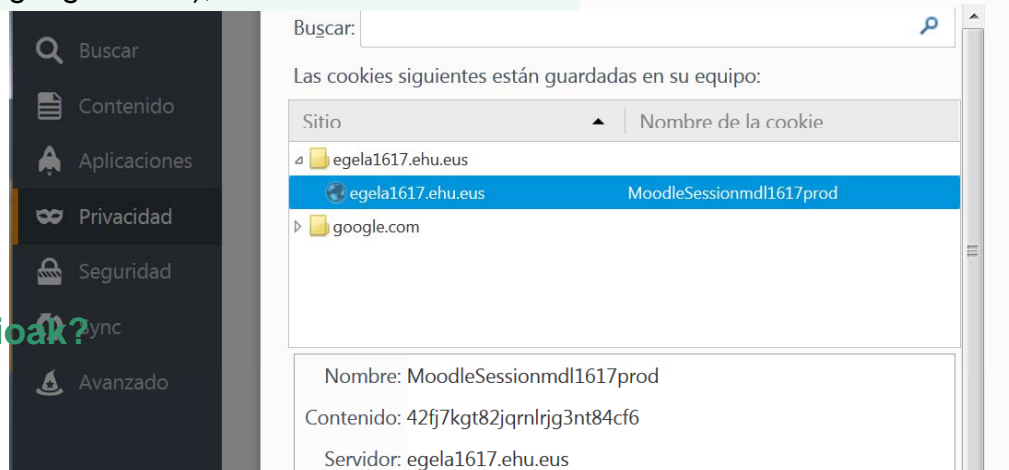


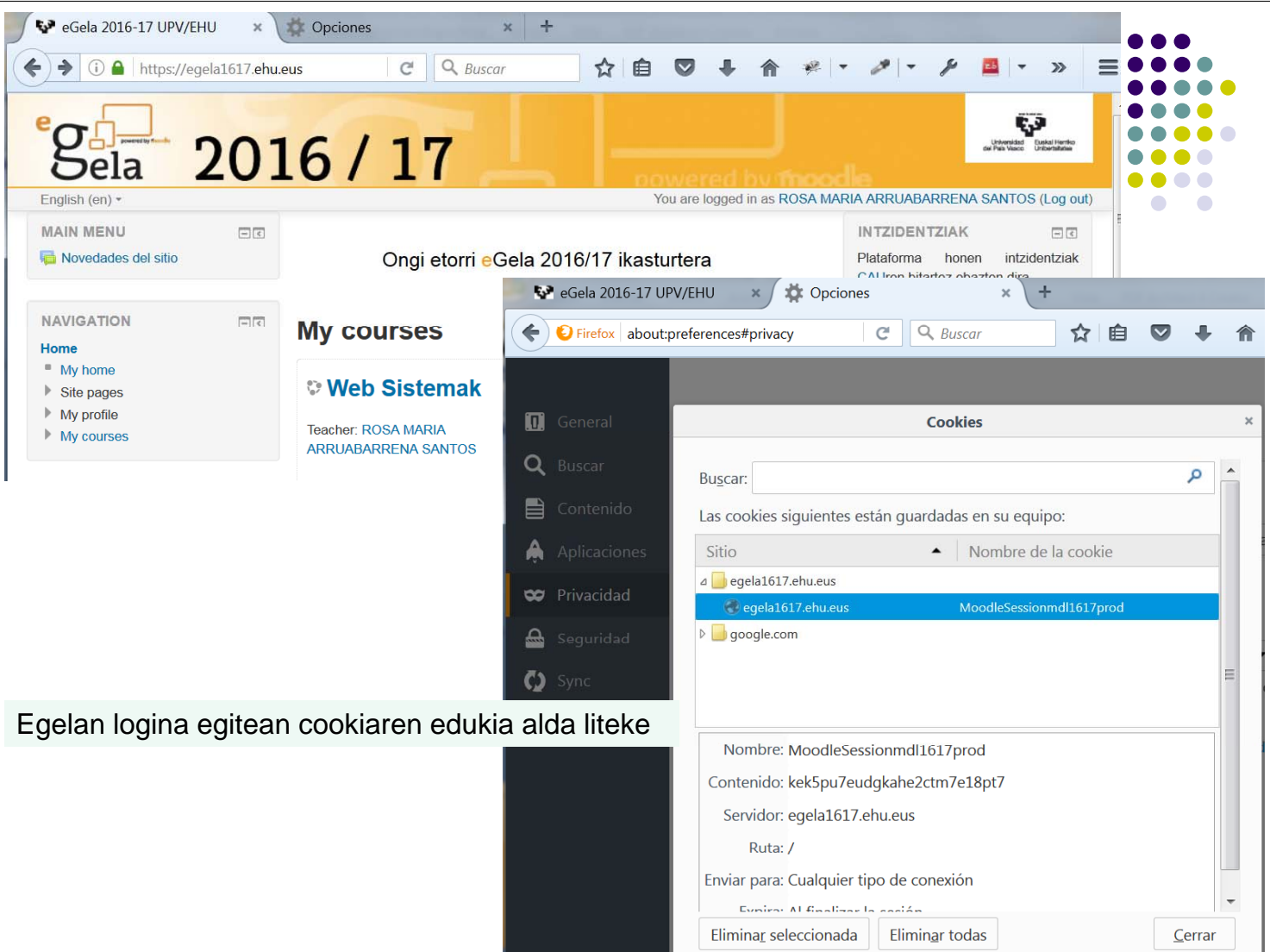
15



Egelara konektatzean (login egin gabe ere), sesion bat sortzen da

Nola kudeatzen dira Sesioak?





The screenshot shows the eGela 2016-17 UPV/EHU website. The user is logged in as ROSA MARIA ARRUIBARRENA SANTOS. The page features a main menu with 'Novedades del sitio', a navigation sidebar with 'Home', 'My home', 'Site pages', 'My profile', and 'My courses', and a 'My courses' section for 'Web Sistemak' taught by ROSA MARIA ARRUIBARRENA SANTOS. A Firefox cookie manager window is open, displaying a table of cookies:

| Sitio | Nombre de la cookie |
|-------------------|--------------------------|
| egela1617.ehu.eus | MoodleSessionmdl1617prod |
| egela1617.ehu.eus | MoodleSessionmdl1617prod |
| google.com | |

Below the table, the details for the selected cookie are shown:

- Nombre: MoodleSessionmdl1617prod
- Contenido: kek5pu7eudgkahe2ctm7e18pt7
- Servidor: egela1617.ehu.eus
- Ruta: /
- Enviar para: Cualquier tipo de conexión
- Expira: Al finalizar la sesión

Buttons at the bottom of the cookie manager include 'Eliminar seleccionada', 'Eliminar todas', and 'Cerrar'.

Egelan logina egitean cookiaren edukia alda liteke

Login / Logout

- Sesio (edo saio) bat aktibo izateak ez du esan-nahi kautotzerik/ autentikaziorik egin denik
- Normalki, sesioa web-aplikaziora konektatzerakoan sortzen da
- Sesioaren IDa cookie bat balitz bezala igortzen zaio nabigatzaileari, lehenengo HTTP Responsean
- Logineko aplikazioak erabiltzailearen informazioa jartzen du zerbitzariaren *session* objektuan
- Logout aplikazioak erabiltzailearen *session*-etik datuak ezabatzen ditu

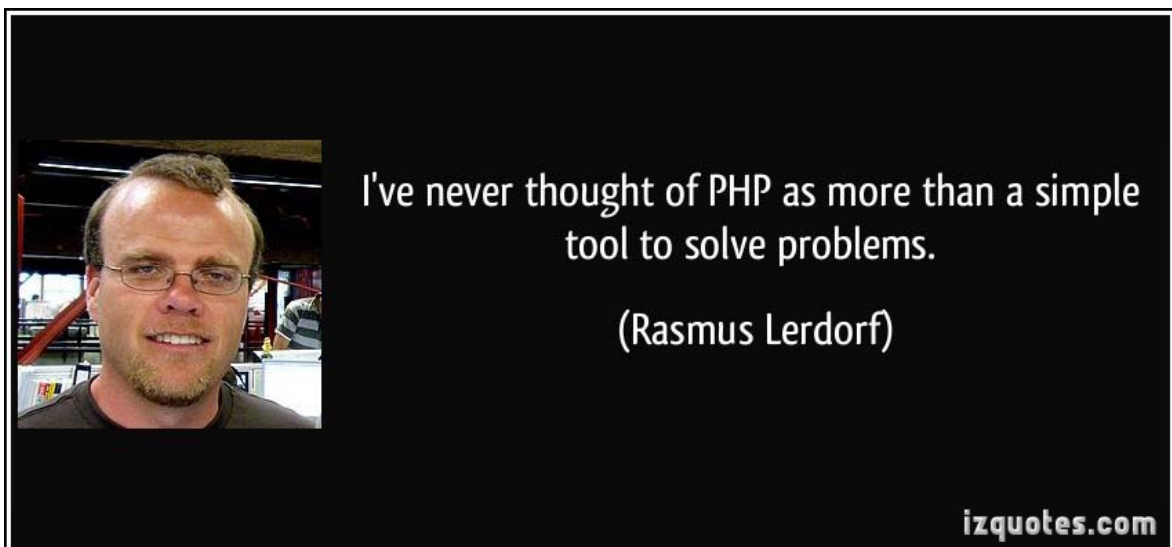


Laburpena

- Nabigatzaileek, cookiei esker, zerbitzari-aplikazio (web zerbitzu) bateko bezero desberdinen informazioa propioa meta ditzatela ahalbidetzen dute
- Sessioaren identifikatzailea, normalki, karaktere anitzeko katea da, cookie batean metatzen da eta aplikazioaren erabiltzaile bakoitzari zein sesio dagokion jakiteko erabiltzen da
- Zerbitzariak session-a gauza txikien lan-espazio global bat balitz bezala erabiltzen du; bestela, aplikazioaren orri berri baten eskaera bakoitzarekin galduko litzateke eta.

19

Nola inplementatzen dira kontzeptu hauek PHPn?



20



Sesioen tratamendua

- Besterik esan ezean, PHP aplikazio batek sesio bat sortzen duenean bere identifikadorea cookie batean metatzen du (sesioa sortu duen orriaren HTTP Response bidez igorria)
- Baina zer gertatzen da nabigatzaileak ez baditu cookie-ak onartzen?
- Irtenbideak:
 - Sesioaren ID url-ean itsasten da (GET). Nahi izanez gero, PHP-ek metodo hori inplementa lezake
 - SID-a input hidden batean idazten da eta POST bidez pasatu (programatzaileak egingo luke hori)

21



PHP: Sesioaren ID-a

- `session_id()`: sesioaren identifikadorea itzultzen du
- **SID**: konstante bat da “sesio_izena=sesio_identifikatzailea”
- `<a href="sesioa irakurri.php?<?php=SID?>" >`
URL bidez sesioaren aldagaia pasatzen da
``

22



PHP.ini-ren konfigurazio aukerak

- `session.use_cookies = 1 / 0`
Bezeroari cookie-ak igorri ahal izatea Gaitzen/Desgaitzen du
- `session.use_trans_sid = 1 / 0`
Eskaeraren URLean SID-a igortzea era automatikoan Gaitzen/Desgaitzen du
- `session.use_only_cookies = 1 / 0`
Gaitzen bada (1), SID-a soilik cookien bidez iraunarazi ahal izango da.

23



PHP funtzioak, sesioen maneiturako

- `session_start ()`:
 - Sesio bat hasieratzen du eta identifikatzaile bakarra esleitzen dio. Sesioa jasa hasieraturik balego, sesioko aldagai guztiak kargatuko lituzke
- `$_SESSION['izena'] = balioa;`
 - Sesioko aldagai baten erregistroa
- `unset ($_SESSION['izena']);`
 - Sesioko aldagai bat ezabatzen du
- `if (isset($_SESSION['izena']))`
 - Aldagai bat erregistraturik dagoen egiaztazen du. TRUE itzultzen du baieztoko kasuan eta FALSE bestela.
- `session_destroy ()`: sesioa isten du (errekuperragarria izanik)

24



Sesioen maneia

- Orri guztiek `session_start()`-i dei bat egin behar diote sesioko aldagaiak kargatzeko. Sesioak existituko ez balu, sortu egiten da
- Deiak edozein HTML kode aurretik egon behar du
- *Logout* egiterakoan, `session_destroy()`-i dei egitea komeni da.

25



adibidea1a.php

```
<?PHP    session_start ();    ?>
<HTML LANG="es">
<HEAD> <TITLE>Sesioen maneia</TITLE>
    <LINK REL="stylesheet" TYPE="text/css" HREF="estilo.css">
</HEAD>

<BODY>
    <H1>Sesioen maneia </H1>
    <H2>Pausoa 1: sesio aldagaia sortu eta gorde egiten da</H2>

<?PHP
    $var = "Miren";
    $_SESSION['var'] = $var;
    print ("<P>Sesioko aldagaiaren balioa: $var</P>\n");
?>

    <A HREF="adibidea1b.php">Pausoa 2</A>.
</BODY>
</HTML>
```

adibidea1b.php



```
<?PHP    session_start ();    ?>

<HTML LANG="es">

<HEAD> <TITLE>Sesioen maneiua</TITLE>

    <LINK REL="stylesheet" TYPE="text/css" HREF="estilo.css">

</HEAD>


<BODY>

    <H1>Sesioen maneiua<H1>

    <H2>Pausoa 2: metatutako sesioko aldagaia eskuratu eta desegiten du</H2>

<?PHP

    $var = $_SESSION['var'];
    print ("<P>Sesioko aldagaiaren balioa: $var</P>\n");
    unset ($_SESSION['var']);
?>

    <A HREF="adibidea1c.php">Pausoa 3</A>.

</BODY>

</HTML>
```

27

adibidea1c.php



```
<?PHP    session_start ();    ?>

<HTML LANG="es">

<HEAD> < TITLE>Sesioen maneiua</TITLE>

    <LINK REL="stylesheet" TYPE="text/css" HREF="estilo.css">

</HEAD>


<BODY>

    <H1>Sesioen maneiua </H1>

    <H2>Puasoa 3: aldagaia desegina izan da eta bere balio galdu da</H2>


<?PHP

    $var = $_SESSION['var'];
    print ("<P> Sesioko aldagaiaren balioa: $var</P>\n");
    session_destroy();
?>

    <A HREF="adibidea1a.php">"Pausoa 1"-ra itzuli</A>.

</BODY>

</HTML>
```

28

Adibidea (2)



```
<?php
ini_set('session.cookie_lifetime',60);
echo 'After 60 minute the session will be finished
      '.ini_get("session.cookie_lifetime")/60 . ' minute/s';
session_start();
if (empty($_SESSION['count'])) { $_SESSION['count'] = 1;
} else { $_SESSION['count']++;}
?>

<p>
Hello visitor, you have seen this page
    <?php echo $_SESSION['count'];?> times.

</p>
<p> Session number: <?php echo '<b>'. session_id() . '</b>'; ?> <p>
To continue,
<a href="sesionexample.php?<?php echo htmlspecialchars(SID);
?>">click here</a>.

</p>
```

29

Ariketa



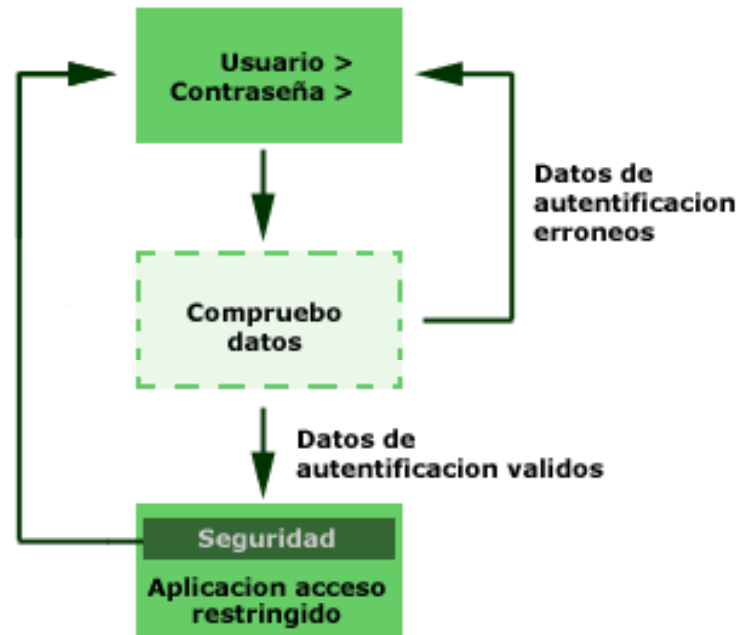
- Hacer un formulario web que pida el correo del usuario y mediante un botón acceda a la página de inserción de grupos. Cuando se muestre esta página contendrá el correo del alumno y un contador indicando el número de veces que ha accedido. Además añadir en insertargrupo un enlace para salir de la aplicación y cerrar la sesión.
- (Opcional) Si el usuario ya se ha identificado una vez (metiendo su correo) queremos que la próxima vez que acceda a esa página el sistema le recuerde el correo que usó la última vez.
 1. Explicar cómo sería el diseño de esa funcionalidad
 2. Implementarla en PHP

30



Sesioetan oinarritutako kautotzea

<http://www.desarrolloweb.com/articulos/1007.php>



31

Index.php (hasierako formularioa)



```
<html>
.....
<form action="kontrola.php" method="POST">
...
    <?if ($_GET["erabiltzaileerrorea"]=="bai"){?>
    bgcolor=red><span style="color:ffffff"><b>Datu okerrak</b> </span>
    <?php }
    else
    {?>
    bgcolor=#cccccc>Sakatu zure atzipen gakoa
    <?php }?>
    USER:
    input type="Text" name="erabiltzailea" size="8" maxlength="50">

    PASSWD:</td>
    input type="password" name="pasahitza" size="8" maxlength="50">

    input type="Submit" value="SARTU">
</form>
...
```

32



kontrola.php

```
<?php
//Erabiltzailea eta pasahitza zuzenak diren aztertu
if ($_POST["erabiltzailea"]=="mikel" &&
$_POST["pasahitza"]=="qwerty"){
    // Erabiltzailea eta pasahitza baliozkoak
    // sesio bat definitzen dut eta datuak metatzen ditut
    session_start();
    $_SESSION["kautotua"]= "BAI";
    header ("Location: aplikazioa.php");
}else {
    // existitzen ez bada, berriro atarira bidaltzen dut
    header("Location: index.php?erabiltzaileerrorea=bai");
}

?>
```

33



segurtasuna.php

```
<?php
//sesio hasiera
session_start();

// ERABILTZAILEA KAUTOTURIK DAGOELA EGIAZTATU
if ($_SESSION["kautotua"] != "BAI") {
    // existitzen ez bada, berriro kautotzera bidaltzen dut
    header("Location: index.php");
    //gainera, script-atik irtetzen gara
    exit();
}

?>
```

34

Aplikazioaren fitxategietan



```
<?php include ("segurtasuna.php");?>
<html>
<head>
<title>Aplikazio segurua</title>
</head>
<body>
<h1>Hemen bazaude, kautotu zarelako da</h1>
<br>
----
<br>
Aplikazio segurua: atzipen murriztuko ingurunea
<br>
----
<br>
<br>
<a href="irten.php">Irten</a>
</body>
</html>
```

35

irten.php



```
<?php
    session_start();
    session_destroy();

?>
<html>
<head>
    <title> Irten zara!!</title>
</head>
<body>
    Mila esker zure atzipenagatik
<br>
<br>
<a href="index.php">Kautotze formulariora</a>
</body>
</html>
```

36