

Sicurezza Informatica: Questa (S)conosciuta

Attacco al Web: Usi di XSS e altre Vulnerabilità

Dimostrazione e analisi degli usi criminosi delle
vulnerabilità di siti Web

Salvatore Mandrà



- 1 Introduzione alla Struttura Base delle Pagine Web
 - Static HTML, Dynamic HTML & Dynamic Web Pages
- 2 Cross Site Scripting o XSS
 - Descrizione degli XSS
- 3 XSS Exploit per Esempi
 - Rischio Basso: Semplice motore di ricerca (XSS LC)
 - Rischio Medio/Alto: Quotidiano Nazionale (XSS LC)
 - Rischio Medio/Alto: Sito Nazionale (XSS LC)
 - Rischio Alto: Sito Nazionale (XSS LS)
 - Rischio Medio: Mi Sento Fortunato® (??!?)
- 4 Come Difenderci?

Il materiale e le informazioni contenute sono a
PURO SCOPO INFORMATIVO e di
RICERCA.

L'AUTORE NON SI RITIENE
RESPONSABILE PER L'**USO** O **ABUSO** DEL
MATERIALE ESPOSTO.

Lo scheletro fondamentale di ogni pagina WEB é l'**HTML**

Lo scheletro fondamentale di ogni pagina WEB é l'**HTML**

l'HTML (o *Hyper Text Markup Language*) è stato introdotto per la prima volta da *Tim Berners-Lee* (1980) ed è divenuto *standard* nella metà degli anni 90.

Lo scheletro fondamentale di ogni pagina WEB é l'**HTML**

l'HTML (o *Hyper Text Markup Language*) è stato introdotto per la prima volta da *Tim Berners-Lee* (1980) ed è divenuto *standard* nella metà degli anni 90.

HTML fonde parti testuali con parti *extratestuali*. Le parti *extratestuali* (o *TAG*) hanno il compito di *istruire* il *browser internet* sulla **struttura complessiva** che avrà una pagina WEB.

Esempi di TAG HTML

`<html>...</html>`

Indica l'inizio/fine
di una pagina HTML

`<body>...</body>`

Indica l'inizio/fine
del corpo di una pagina

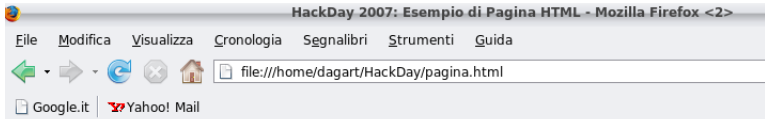
`...`

Inserisce link

`...`

Inserisce immagine

Static HTML



Questo e' un semplice Esempio di pagina HTML

A screenshot of a Mozilla Firefox browser window showing the source code of the HTML file. The title bar reads "Sorgente di: file:///home/dagart/HackDay/pagina.html - Mozilla Firefox". The menu bar includes "File", "Modifica", "Visualizza", and "Guida". The source code is displayed in a monospaced font with syntax highlighting.

```
<html>
<title>HackDay 2007: Esempio di Pagina HTML</title>
<body>
  <br>
  <b>HackDay 2007: Esempio di Pagina HTML</b>
  <br>
  <br>
  Questo e' un semplice Esempio di pagina HTML
</body>
</html>
```

Static HTML



Questo e' un semplice Esempio di pagina HTML

```
Sorgente di: file:///home/dagart/HackDay/pagina.html - Mozilla Firefox
```

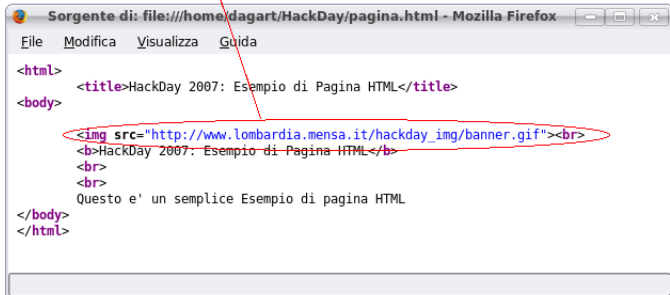
```
File Modifica Visualizza Guida
```

```
<html>
<title>HackDay 2007: Esempio di Pagina HTML</title>
<body>
  <br>
  <b>HackDay 2007: Esempio di Pagina HTML</b>
  <br>
  <br>
  Questo e' un semplice Esempio di pagina HTML
</body>
</html>
```

Static HTML



Questo e' un semplice Esempio di pagina HTML



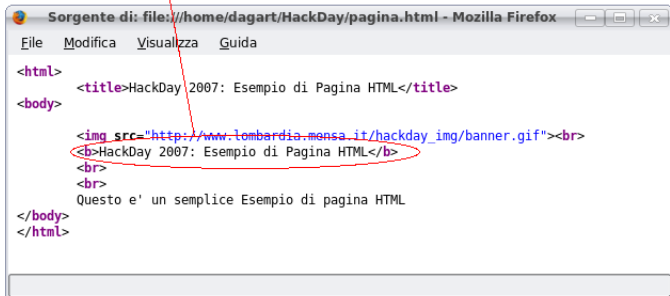
```
<html>
<title>HackDay 2007: Esempio di Pagina HTML</title>
<body>
<br>
<b>HackDay 2007: Esempio di Pagina HTML</b>
<br>
<br>
Questo e' un semplice Esempio di pagina HTML
</body>
</html>
```

Static HTML



HackDay 2007: Esempio di Pagina HTML

Questo e' un semplice Esempio di pagina HTML



```
<html>
<title>HackDay 2007: Esempio di Pagina HTML</title>
<body>
  <br>
  <b>HackDay 2007: Esempio di Pagina HTML</b>
  <br>
  <br>
  Questo e' un semplice Esempio di pagina HTML
</body>
</html>
```

Static HTML



Questo e' un semplice Esempio di pagina HTML

A screenshot of a Mozilla Firefox source code viewer window. The title bar reads "Sorgente di: file:///home/dagart/HackDay/pagina.html - Mozilla Firefox". The menu bar includes "File", "Modifica", "Visualizza", and "Guida". The code is as follows:

```
<html>  
<title>HackDay 2007: Esempio di Pagina HTML</title>  
<body>  
  <br>  
  <b>HackDay 2007: Esempio di Pagina HTML</b>  
  <br>  
  <br>  
</body>  
</html>
```

A red oval highlights the text "Questo e' un semplice Esempio di pagina HTML" which is placed below the code. A red arrow points from this text to the address bar of the browser window above.

Sebbene potente, il linguaggio HTML *da solo* è puramente **statico** e non prevede dunque alcuna interazione con l'utente per la personalizzazione della navigazione

Sebbene potente, il linguaggio HTML *da solo* è puramente **statico** e non prevede dunque alcuna interazione con l'utente per la personalizzazione della navigazione

Per tal motivo, nella metà degli anni 90, sono state introdotte una serie di *tecnologie* usate per rendere **dinamiche** le pagine WEB.

Dynamic HTML & Dynamic Web Pages

Dynamic HTML	Dynamic Web Pages
Lato Client	Lato Server
Javascript, VBScript, ...	PHP, ASP, ...
(Locale)	(Remoto)
Accessibile al solo utente	Accessibile ad ogni utente
(Post-Processata)	(Pre-Processata)
Codice Visibile dal Browser	Codice Invisibile al Browser

Moderna Pagina Web



Sorgente della Pagina (con PHP)

HackDay 2007!



```
Sorgente di: file:///home/dagart/HackDay/pagina2
File Modifica Visualizza Guida
<html>
<body>

  <!-- Esempio di Codice PHP -->

  <?php      echo "<b>HackDay 2007!<b>"
  ?>

  <!-- Esempio di Codice Javascript -->

  <script language=javascript>
    alert("HackDay 2007!");
  </script>

</body>
</html>
```

Sorgente della Pagina (come visibile dal Browser)

```
Sorgente di: file:///home/dagart/HackDay/pagina2
File Modifica Visualizza Guida
<html>
<body>

  <!-- Esempio di Codice PHP -->

  <b>HackDay 2007!<b>

  <!-- Esempio di Codice Javascript -->

  <script language=javascript>
    alert("HackDay 2007!");
  </script>

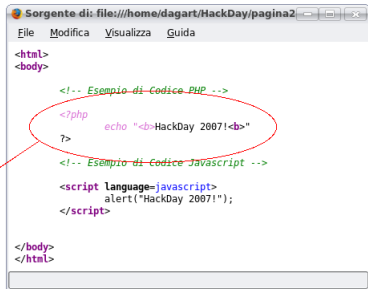
</body>
</html>
```

Completato

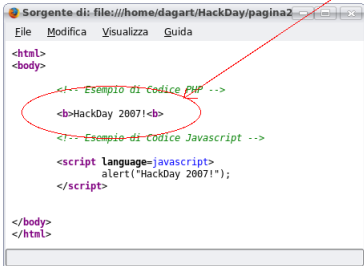


Sorgente della Pagina (con PHP)

HackDay 2007!



Sorgente della Pagina (come visibile dal Browser)



Completato



HackDay 2007!



Sorgente della Pagina (con PHP)

```
Sorgente di: file:///home/dagart/HackDay/pagina2
File Modifica Visualizza Guida
<html>
<body>

  <!-- Esempio di Codice PHP -->

  <?php
    echo "<b>HackDay 2007!<b>"
  ?>

  <!-- Esempio di Codice Javascript -->

  <script language=javascript>
    alert("HackDay 2007!");
  </script>

</body>
</html>
```

Sorgente della Pagina (come visibile dal Browser)

```
Sorgente di: file:///home/dagart/HackDay/pagina2
File Modifica Visualizza Guida
<html>
<body>

  <!-- Esempio di Codice PHP -->

  <b>HackDay 2007!<b>

  <!-- Esempio di Codice Javascript -->

  <script language=javascript>
    alert("HackDay 2007!");
  </script>

</body>
</html>
```

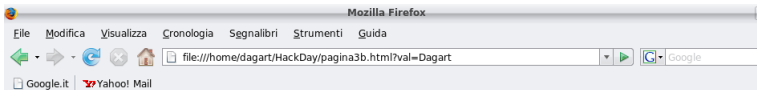
Completato

L'*aumento* della *complessità* della pagine Web moderne può comportare **errori** nella programmazione del codice

L'*aumento* della *complessità* della pagine Web moderne può comportare **errori** nella programmazione del codice

Nasce così il **Cross Site Scripting**, ovvero la tecnica di *inserire codice arbitrario* da parte di un utente in una pagina Web.

Esempio semplice di XSS



Benvenuto Dagart all'**HackDay 2007!**

```
Sorgente di: file:///home/dagart/HackDay/
File Modifica Visualizza Guida
<html>
<body>

<!-- Esempio di Codice PHP -->

Benvenuto Dagart all'<b>HackDay 2007!<b>

</body>
</html>
```

```
Sorgente di: file:///home/dagart/HackDay/pagina3.html
File Modifica Visualizza Guida
<html>
<body>

<!-- Esempio di Codice PHP -->
<?php
    $val = $_GET['val'];
    echo "Benvenuto $val all'<b>HackDay 2007!<b>";
?>

</body>
</html>
```

Non c'è controllo sul valore passato!

Esempio semplice di XSS

Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibri Strumenti Guida

file:///home/dagart/HackDay/pagina3b.html?val=Dagart

Google.it Yahoo! Mail

Benvenuto Dagart all **HackDay 2007!**

Sorgente di: file:///home/dagart/HackDay/pagina3.html

```
File Modifica Visualizza Guida
<html>
<body>

  <!-- Esempio di Codice PHP -->

  <?php
      $val = $_GET['val'];
      echo "Benvenuto $val all<b>HackDay 2007!<b>"
  ?>

</body>
</html>
```

Sorgente di: file:///home/dagart/HackDay/

```
File Modifica Visualizza Guida
<html>
<body>

  <!-- Esempio di Codice PHP -->

  Benvenuto Dagart all <b>HackDay 2007!<b>

</body>
</html>
```

Esempio semplice di XSS

Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibri Strumenti Guida

file:///home/dagart/HackDay/pagina3b.html?val=<script>alert('XSS Exploit!');</script>

Google.it Yahoo! Mail

Benvenuto

[Applicazione JavaScript]

XSS Exploit!

OK

Sorgente di: file:///home/dagart/HackDay/pagina3.html - Mozilla Firefo

```
<html>
<body>

<!-- Esempio di Codice PHP -->

<?php
    $val = $_GET['val'];
    echo "Benvenuto $val all'<b>HackDay 2007!<b>";
?>

</body>
</html>
```

Sorgente di: file:///home/dagart/HackDay/pagina3

```
<html>
<body>

<!-- Esempio di Codice PHP -->

Benvenuto <script>alert("XSS Exploit!");</script> all'<b>HackDay 2006!<b>

</body>
</html>
```

Esempio semplice di XSS

The screenshot illustrates a successful Cross-Site Scripting (XSS) attack in Mozilla Firefox. The browser window shows the URL: `file:///home/dagart/HackDay/pagina3b.html?val=<script>alert("XSS Exploit!");</script>`. The page content displays "Benvenuto".

An alert dialog box titled "[Applicazione JavaScript]" is shown, containing the message "XSS Exploit!" and an "OK" button. A red box highlights this dialog.

The browser's developer tools (Source view) show the source code of the page. The injected script is circled in red:

```
<!-- Esempio di Codice PHP -->
<?php
    $val = $_GET['val'];
    echo "Benvenuto $val all'<b>HackDay 2007!<b>";
?>
</body>
</html>
```

The injected payload is: `<script>alert("XSS Exploit!");</script>`

A red arrow points from the circled script in the source code to the alert dialog box, indicating the execution of the injected code.

Persistenti. Gli script **LATO SERVER** non filtrano le variabili passate dall'utente. Rischi:

- Lettura/Modifica Database (password, account, carte di credito, ...)
- Utilizzo illecito di servizi on-line
- Modifica delle pagine WEB (a tutti i livelli)
- Phishing su larga scala
- Aggirare filtri Anti-Phising
- **IMPATTO ELEVATO**

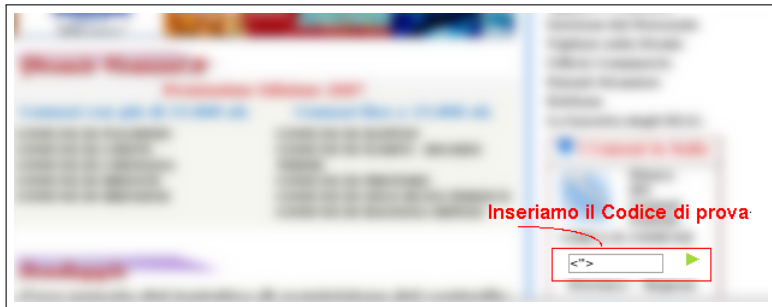
Non Persistenti: Gli script **LATO CLIENT** non filtrano le variabili passate dall'utente. Rischi:

- Lettura/Modifica Cookies
- Sniffing delle Password e altro
- Avvio programmi Java in finestre nascoste (Jikto e altro)
- Manipolazione (lato client) delle pagine WEB
- Phishing
- Aggirare filtri Anti-Phising
- Attacco alla rete intranet attraverso il browser
- **Impatto medio/basso**

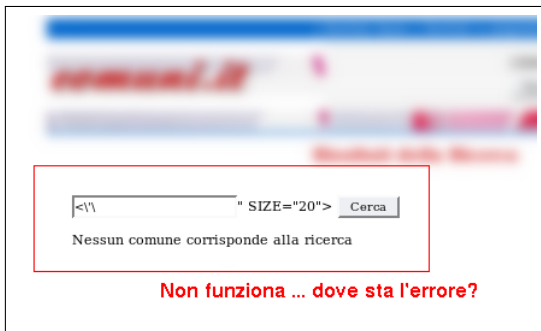
Rischio Basso: Semplice motore di ricerca (XSS LC)

Come test useremo il codice di prova <">

Motore di ricerca nella homepage



Risposta del server



`<\\\"` " SIZE="20">

Nessun comune corrisponde alla ricerca

Non funziona ... dove sta l'errore?

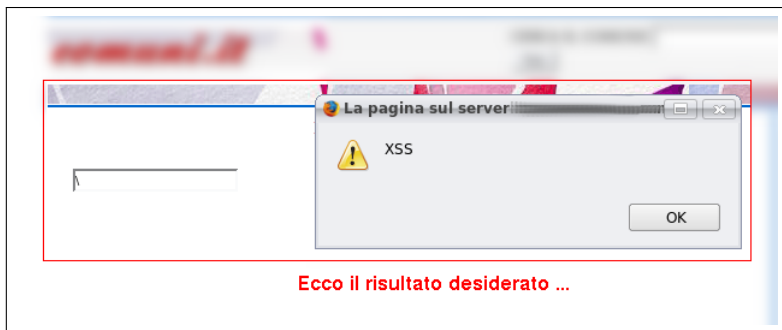
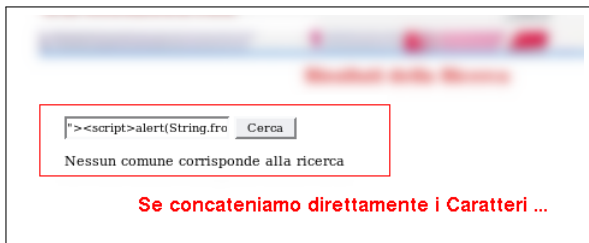
Codice sorgente della pagina



```
<p>  
<input type="text" name="IdQuery" value="<\\\"" size="20">  
<input type="submit" value="Cerca">  
</p>
```

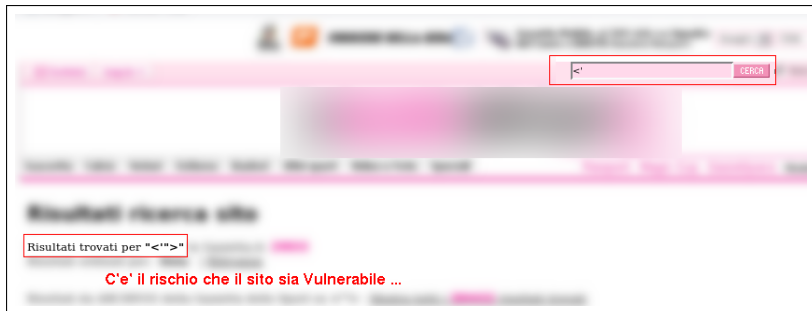
Il sito soffre di XSS Exploit!

Usiamo la funzione `String.fromCharCode(88,83,83)`

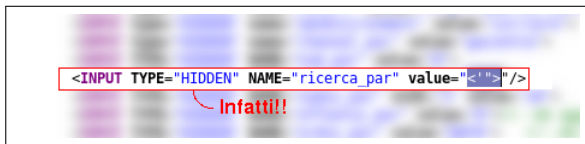


Come al solito, useremo il codice di prova `<'>`

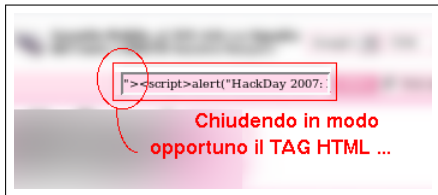
Motore di ricerca nella homepage



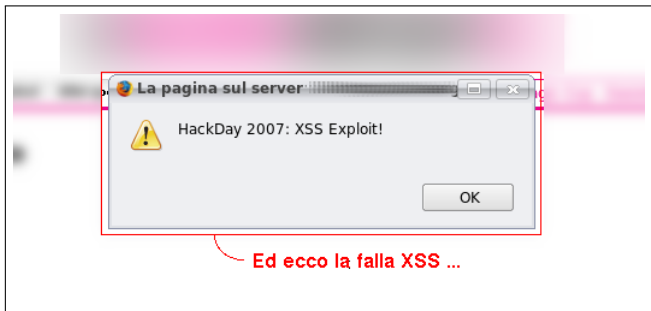
Studiamo il codice sorgente della pagina



È sufficiente chiudere il precedente *TAG HTML*



Con il risultato voluto ...

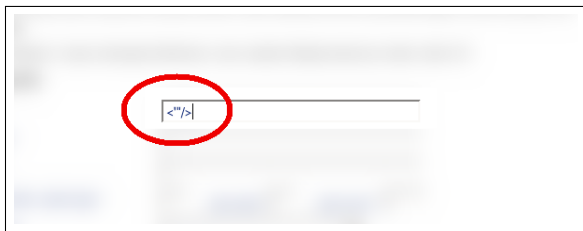


Ed ecco la falla XSS ...

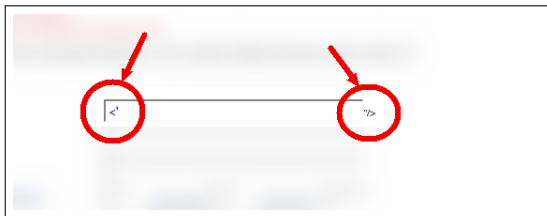
Rischio Medio/Alto: Sito Nazionale (XSS LC)

Proviamo con il solito script standard ...

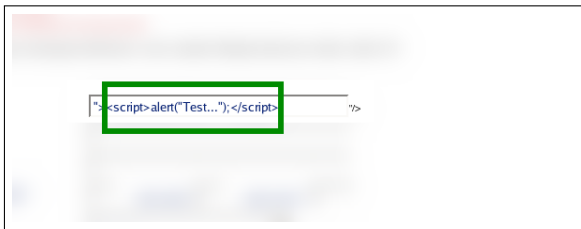
Form del Sito



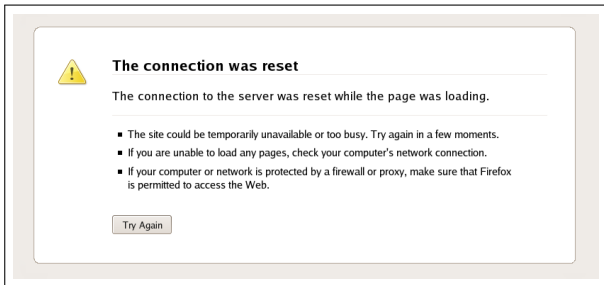
Risposta del server



Proviamo ad inserire del codice opportuno



Sembra che le richieste siano filtrate da un IDS

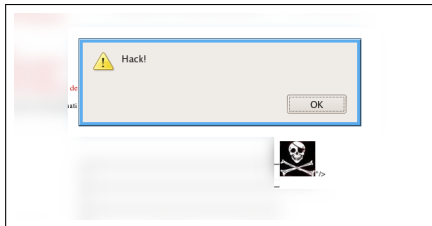


Proviamo ad inserire codice Javascript
senza usare i TAG `< script >`

Sfruttiamo il tag `< IMG >` per inserire del codice Javascript



È stato possibile scavalcare l'IDS



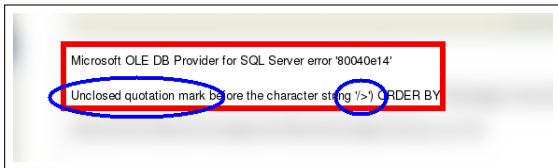
Rischio Alto: Sito Nazionale (XSS LS)

Anche in questo caso, proviamo con il solito codice di prova

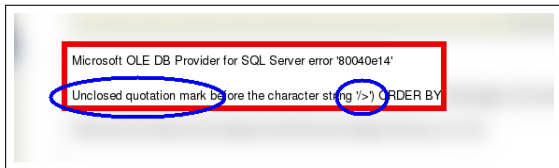
Form del Sito



Risposta del server



ABBIAMO IL COMPLETO ACCESSO AL DATABASE (sql inject)



array = "SELECT * FROM database WHERE id = var "

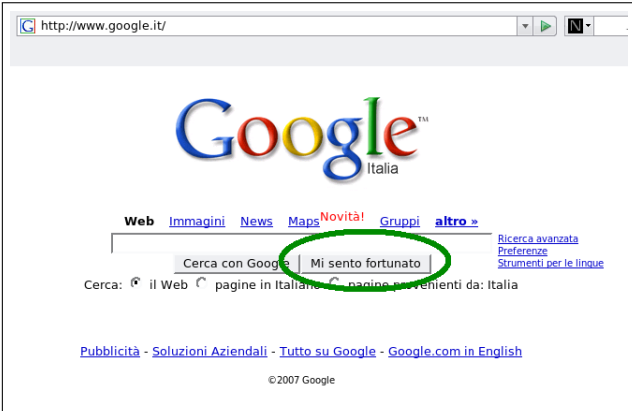
Formattando opportunamente **var** è possibile inserire codice arbitrario **LATO SERVER**.

Ad esempio: var = '"; [Codice Arbitrario]'

Rischio Medio: Mi Sento Fortunato® (??!?)

Google® mette a disposizione lo strumento *Mi sento fortunato*® che mi permette di seguire il link del primo elemento trovato in una ricerca

Home Page di Google®



The screenshot shows the Google Italia homepage in a browser window. The address bar displays "http://www.google.it/". The Google logo is prominently displayed in the center, with "Italia" written below it. Below the logo, there are navigation links: "Web", "Immagini", "News", "Maps", "Novità!", "Gruppi", and "altro »". The search bar contains the text "Cerca con Google" and "Mi sento fortunato", with the latter highlighted by a green circle. To the right of the search bar, there are links for "Ricerca avanzata", "Preferenze", and "Strumenti per le lingue". Below the search bar, there is a line of text: "Cerca: il Web pagine in Italiano pagine provenienti da: Italia". At the bottom of the page, there are links for "Pubblicità", "Soluzioni Aziendali", "Tutto su Google", and "Google.com in English". The copyright notice "©2007 Google" is visible at the bottom center.

Con una ricerca *ad hoc* è sempre possibile indicizzare in modo opportuno il risultato

The image shows a screenshot of a Google search page. At the top, the search bar contains the query "earch?hl=it&q=consip.it+mensa+notizie&btnG=Cerca+con+Google&meta=" with a green underline under "Cerca+con+Google". Below the search bar, the Google logo is visible, and the search input field contains "consip.it mensa notizie". A green circle highlights the search input field, and a green arrow points from it to the "Web" tab in the search results. The search results show "Web Risultati 1 - 7 su 7 per consip.it". The first result is titled "CONSP" and describes a conference organized by Consip and Mensa Italia. The second result is also titled "CONSP" and describes Mensa as an international association of people with a high IQ. The page includes navigation links like "Web", "immagini", "News", "Maps", "Novità!", "Gruppi", and "altro >". There are also links for "Copia cache" and "Pagine simili".

earch?hl=it&q=consip.it+mensa+notizie&btnG=Cerca+con+Google&meta=

Google

Web immagini News Maps Novità! Gruppi altro >

consip.it mensa notizie

Cerca Ricerca avanzata Preferenze

Cerca: il web pagine in Italiano pagine provenienti da: Italia

Web Risultati 1 - 7 su 7 per **consip.it**

CONSP
Consip e **Mensa** Italia organizzano un convegno dal titolo: ... I relatori sono tutti soci **Mensa** che per passione, professione o entrambe, vivono a stretto e ...
www.consip.it/on-line/Home/articolo1006.html - 12k - [Copia cache](#) - [Pagine simili](#)

CONSP
Consip e **Mensa** Italia organizzano un convegno dal titolo: ... Il **Mensa** è un'associazione internazionale di persone aventi un elevato quoziente intellettivo.
...
www.consip.it/on-line/Home/Newsedeventi/articolo1006.html - 12k - [Copia cache](#) - [Pagine simili](#)
[[Altri risultati in www.consip.it](#)]

Ci Ci Mi Ww

Con una ricerca *ad hoc* è sempre possibile indicizzare in modo opportuno il risultato

The screenshot shows a Google search interface. At the top, the search bar contains the URL: `earch?hl=it&q=consip.it+mensa+notizie&btnG=Cerca+con+Google&meta=`. Below the search bar, the Google logo is visible, and the search query "consip.it mensa notizie" is entered in the search box. A green oval highlights the search query, and a green arrow points from it to the "Web" tab in the search results. The search results show two entries for "CONSHIP". The first entry is titled "Consip e Mensa Italia organizzano un convegno dal titolo: ... I relatori sono tutti soci Mensa che per passione, professione o entrambe, vivono a stretto e ..." and includes a link to `www.consip.it/on-line/Home/articolo1006.html`. The second entry is titled "Consip e Mensa Italia organizzano un convegno dal titolo: ... Il Mensa è un'associazione internazionale di persone aventi un elevato quoziente intellettivo. ..." and includes a link to `www.consip.it/on-line/Home/Newsedeventi/articolo1006.html`. The search results are labeled "Risultati 1 - 7 su 7 per consip.it".

The screenshot shows the search bar with the URL: `earch?hl=it&q=consip.it+mensa+notizie&btnG=Cerca+con+Google&meta=`. A green underline is present under the search query part of the URL.

Sostituendo **Cerca+con+google** con **Mi+sento+fortunato** nel link
alla pagina di ricerca ...

search?hl=it&q=consip.it+mensa+notizie&btnI=Mi+sento+fortunato&meta=

Google Web Immagini News Maps Novità! Gruppi altro »

consip.it mensa notizie Cerca Ricerca avanzata Preferenze

Cerca: il Web pagine in Italiano pagine provenienti da: Italia


Web Risultati 1 - 7 su 7 per **consip.it**

CONSIP
Consip e **Mensa** Italia organizzano un convegno dal titolo: ... I relatori sono tutti soci **Mensa** che per passione, professione o entrambe, vivono a stretto e ...
www.consip.it/on-line/Home/articolo1006.html - 12k - [Copia cache](#) - [Pagine simili](#)

CONSIP
Consip e **Mensa** Italia organizzano un convegno dal titolo: ... Il **Mensa** è un'associazione internazionale di persone aventi un elevato quoziente intellettivo.
...
www.consip.it/on-line/Home/Newsedeventi/articolo1006.html - 12k - [Copia cache](#) - [Pagine simili](#)
[[Altri risultati in www.consip.it](#)]

Ci
Ci
M
ww

Sostituendo **Cerca+con+google** con **Mi+sento+fortunato** nel link
alla pagina di ricerca ...



Search?hl=it&q=consip.it+mensa+notizie&btnl=**Mi+sento+fortunato**&meta=

Google Web Immagini News Maps Novità! Gruppi altro >

consip.it mensa notizie Cerca Ricerca avanzata Preferenze

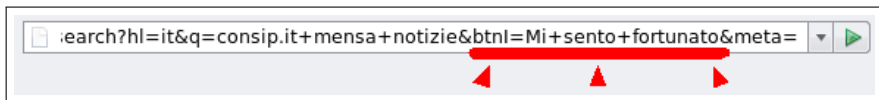
Cerca: il Web pagine in Italiano pagine provenienti da: Italia

Web Risultati 1 - 7 su 7 per **consip.it**

CONSIP
Consip e **Mensa** Italia organizzano un convegno dal titolo: ... I relatori sono tutti soci **Mensa** che per passione, professione o entrambe, vivono a stretto e ...
www.consip.it/on-line/Home/articolo1006.html - 12k - [Copia cache](#) - [Pagine simili](#)

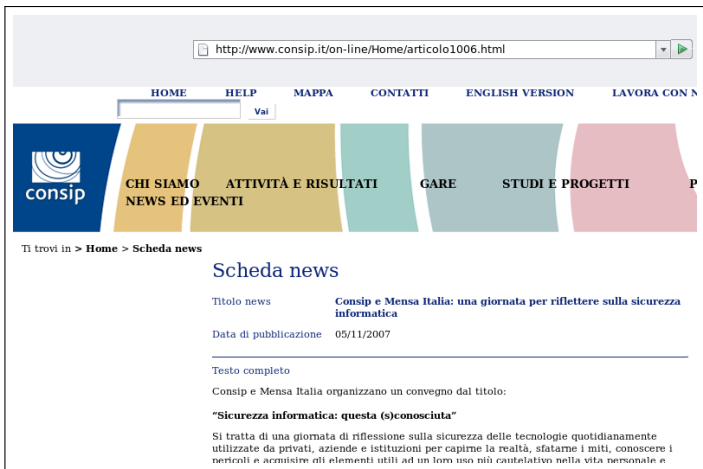
CONSIP
Consip e **Mensa** Italia organizzano un convegno dal titolo: ... Il **Mensa** è un'associazione internazionale di persone aventi un elevato quoziente intellettivo.
...
www.consip.it/on-line/Home/Newsedeventi/articolo1006.html - 12k -
[Copia cache](#) - [Pagine simili](#)
[[Altri risultati in www.consip.it](#)]

Ci Ci M: ww



Search?hl=it&q=consip.it+mensa+notizie&btnl=**Mi+sento+fortunato**&meta=

... è possibile indirizzare l'utente con **un solo click** nella pagina desiderata



The screenshot shows a web browser window with the address bar containing `http://www.consip.it/on-line/Home/articolo1006.html`. The navigation menu includes [HOME](#), [HELP](#), [MAPPA](#), [CONTATTI](#), [ENGLISH VERSION](#), and [LAVORA CON N](#). Below the menu is a search bar with the text "Vai". The main navigation bar features several colored buttons: a blue button with the Consip logo, a yellow button for "CHI SIAMO NEWS ED EVENTI", a green button for "ATTIVITÀ E RISULTATI", a light blue button for "GARE", a teal button for "STUDI E PROGETTI", and a pink button for "P".

Ti trovi in > [Home](#) > [Scheda news](#)

Scheda news

Titolo news **Consip e Mensa Italia: una giornata per riflettere sulla sicurezza informatica**

Data di pubblicazione 05/11/2007

Testo completo

Consip e Mensa Italia organizzano un convegno dal titolo:

"Sicurezza informatica: questa (s)conosciuta"

Si tratta di una giornata di riflessione sulla sicurezza delle tecnologie quotidianamente utilizzate da privati, aziende e istituzioni per capirne la realtà, sfatarne i miti, conoscere i pericoli e acquisire gli elementi utili ad un loro uso più cautelativo nella vita personale e

- Filtrare **tutti** gli input. Anche i più nascosti potrebbero essere pericolosi
- Riformattare **tutti** gli output
- Usare soluzioni *mature* piuttosto che arrangiarsi
- Nei form, permettere di usare solo i simboli **previsti**. Non ha senso permettere simboli diversi da [a-z, A-Z] nel campo *Cognome*
- Scrivere codice **leggibile** e facilmente **controllabile**
- **Controllare** periodicamente i log per eventuali anomalie

- Non credere alle lotterie! Qual è la probabilità essere realmente estratti? :)
- Diffidare dei link provenienti da mail sconosciute
- Se possibile, controllare ogni link prima di aprirlo
- Disabilitare **tutti** gli script (?!!)
- Prudenza soprattutto nelle transazioni finanziarie

Il Bug Hunter :)

- Responsabilità: non cercare mai di sfruttare a proprio vantaggio le vulnerabilità scoperte
- Rispetto: dietro ad ogni falla c'è un team che lavora



Wikipedia, http://en.wikipedia.org/wiki/Cross_site_scripting



Technical Info - *HTML Code Injection and Cross-site scripting*,
<http://www.technicalinfo.net/papers/CSS.html>



Ha.Ckers.Org - *XSS (Cross Site Scripting) Cheat Sheet Esp: for filter evasion*, <http://ha.ckers.org/xss.html>



Gnu Citizien - *XSS Attack Database*,
<http://www.gnucitizen.org/xssdb/application.htm>



Chris Shiflett - *Foiling Cross-Site Attacks*,
<http://shiflett.org/articles/foiling-cross-site-attacks>



HTML.it - *Tecniche: Cross Site Scripting*,
<http://sicurezza.html.it/articoli/leggi/966/tecniche-cross-site-scripting/>,
<http://php.html.it/guide/lezione/2989/crosssite-scripting-xss>



Raffaele Rialdi - *La subdola minaccia del Cross Site Scripting*,
<http://www.microsoft.com/italy/msdn/risorsemsdn/security/editoria>