Siti scolastici: la sicurezza dei CMS e alcune indicazioni per l'uso dei modelli Porte aperte sul web

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Ogni sito realizzato con i CMS open-source più diffusi (WordPress, Joomla!, Drupal, etc.) se non correttamente gestito, può presentare innumerevoli problemi di sicurezza.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

I progetti open source sono teoricamente più vulnerabili rispetto ai siti realizzati con applicativi personalizzati: tutto il codice dei CMS più diffusi è di dominio pubblico, tutti possiamo leggerlo, capirlo e, trovare delle falle di sicurezza. Se poi si aggiungono moduli, temi e plugin programmati male, le probabilità di intrusioni aumentano.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Una scarsa attenzione al tema sicurezza nella gestione di siti web può tramutarsi in veri e propri disastri soprattutto per tutti coloro che utilizzano il proprio sito per fornire servizi e informazioni ai cittadini.

La prevenzione ad attacchi e furti di dati per una Pubblica Amminisrazione é fondamentale.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Gli attacchi effettuati dagli "**hackers**" sfruttando le vulnerabilità del codice dei CMS possono permettere ai malintenzionati di avere il pieno accesso al vostro spazio web.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Le principali motivazioni di un hacker

- inserire abusivamente materiali sul vs sito, es. sovrascrivendo la homepage (es. "Sito hackerato da TizioCaio")
- pubblicare script che effettuano altre attività illegali, che causano danni agli altri clienti allocati sullo stesso server

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Le principali motivazioni di un hacker

- inviare enormi flussi di email SPAM, che impongono al Provider di intervenire bloccando tempestivamente il sito (D.O.S.)
- pubblicare maleware (virus/trojan) per facilitarne la diffusione, causando il blocco del sito su Google

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Le principali motivazioni di un hacker

- pubblicare pagine di phishing.
  Il phishing è un tipo di truffa via Internet attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Il mio sito attualmente è indicato come "sospetto" da Google, cosa può essere successo?

Il vostro computer è stato infettato da uno dei tanti virus/trojan che sottraggono e trasmettono a terzi i dati di accesso salvati sul computer, incluse le password FTP.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Il mio sito attualmente è indicato come "sospetto" da Google, cosa può essere successo?

In alcuni casi, anche a distanza di tempo, terze parti, usando i dati di accesso FTP sottratti, possono aggiungere codice dannoso a siti autentici, e questo è il motivo della visualizzazione del messaggio di avviso.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Questo è il sistema di propagazione di questi virus:

1 - Durante la visita una pagina Web infetta (di qualche altro sito o del proprio) carica un virus sul computer di casa/ufficio.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Questo è il sistema di propagazione di questi virus:

2 - Il virus esamina il computer per vedere se si utilizzano i più comuni programmi di FTP, e se è stato impostato il salvataggio dei dati di accesso.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Questo è il sistema di propagazione di questi virus:

3 - Il virus trasmette username/password FTP del sito a un server controllato da "hacker".

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Questo è il sistema di propagazione:

4 - Gli hacker effettuano una connessione FTP allo spazio web e scaricano tutti i file HTML o PHP che trovano. Modificano i files e aggiungono codice HTML (spesso un tag "<IFRAME>) che diffonde il virus, e caricano i file modificati sul vostro spazio web.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Questo è il sistema di propagazione:

5 - Il sito inizia a diffondere il virus a nuove vittime e nel giro di pochi giorni viene contrassegnato come dannoso o sospetto da Google ("Questo sito potrebbe danneggiare il tuo computer"), causando un crollo verticale del numero di visitatori.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Quale virus può aver colpito il mio computer?

Tra i tanti virus/trojan in grado di sottrarre i dati di accesso FTP dai computer ad esempio citiamo:

- **"Gumblar" o Trojan.PWS.Tupai**
- **Win32/Spy.Agent.OAB**

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Quale virus può aver colpito il mio computer?

Tra i tanti virus/trojan in grado di sottrarre i dati di accesso FTP dai computer ad esempio citiamo:

- **Backdoor.Win32.Rbot.jcv e varianti**

Per approfondimenti basta effettuare una ricerca su Google per "viruses that steal FTP passwords"

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Ulteriori spiegazioni sui malware

Le spiegazioni sui software dannosi classificabili "malware" sono disponibili su:

www.google.com/goodtoknow/online-safety/malware/?hl=it

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Come rimuovere il malware dal propri PC?

La prima cosa da fare è proteggere il proprio computer da questo tipo di virus. **Assicurarsi di aver aggiornato Windows e qualsiasi browser** web utilizzato alla più recente versione disponibile.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Come rimuovere il malware dal propri PC?

Assicurarsi inoltre di aver recentemente aggiornato Adobe Reader o Adobe Acrobat (che permettono il browser Web per visualizzare i file PDF), dal momento che alcuni virus si stanno diffondendo anche tramite delle vulnerabilità di sicurezza di Adobe.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Come rimuovere il malware dal propri PC?

Esegui la scansione del computer con almeno uno (e possibilmente alcuni) dei prodotti antivirus di alta qualità in circolazione.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

- avast! http://www.avast.com/
- AVG http://free.avg.com/
- AVIRA http://www.avira.com/en/for-home
- BitDefender http://www.bitdefender.co.uk/
- ESET Smart Security http://www.eset.com/

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

F-Secure http://www.f-secure.com/

G DATA http://www.gdata-software.com/home-security/

Kaspersky Lab Internet Security http://www.kaspersky.com/

Malwarebytes http://www.malwarebytes.org/

McAfee http://home.mcafee.com/store/free-antivirus-trials

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Esegui la scansione del computer con almeno uno (e possibilmente alcuni) dei prodotti antivirus di qualità.

MacScan (per utenti Mac)
http://macscan.securemac.com/download.html

Microsoft Security Essentials
http://www.microsoft.com/security_essentials/

Norton Internet Security
http://www.symantec.com/home_homeoffice/products/overview.jsp?pcid=is&pvid=nis2007

TrendMicro http://www.trendmicro.com/

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Come rimuovere il malware dal proprio sito?

Dopo aver protetto adeguatamente il tuo computer da questo tipo di virus/trojan contattaci e richiedi il settaggio di una nuova password FTP. A questo punto puoi intervenire sui contenuti

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Come rimuovere il malware dal proprio sito?

Se sei certo di disporre di una copia completa ed integra dei materiali del tuo sito web puoi semplicemente accedere via FTP, cancellare tutto il materiale dalla /public e ripubblicare il materiale originale.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Come rimuovere il malware dal proprio sito?

Invece se non ne disponi di una copia integra o completa del materiale del tuo sito invece accedi via FTP, preleva il materiale, salvalo in una directory del tuo computer ed esegui la scansione della directory.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Virus che rubano le password FTP

Come rimuovere il malware dal proprio sito?

Accertati che il software antivirus utilizzato sia in grado di identificare e rimuovere dal codice HTML anche eventuali tags <IFRAME> malevoli, che richiamano contenuti esterni dannosi.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Hai già rimosso il codice dannoso dal tuo sito ma Google lo segnala ancora come sospetto?

Chiedi a Google di riesaminare il tuo sito, seguendo la procedura indicata dal motore di ricerca.

Elementi di sicurezza con Drupal

Tutti i CMS sono vulnerabili

Come chiedere il riesame del sito da parte di Google per rimuovere l'avviso di "sito sospetto"?

Se sei il proprietario di questo sito web, puoi chiedere che il tuo sito venga riesaminato

utilizzando gli Strumenti per i Webmaster di Google

Per ulteriori informazioni sul processo di revisione, consulta il Centro assistenza per webmaster di Google.

Elementi di sicurezza con Drupal

Filtro accessi ftp con Aruba

Abilitare all'accesso FTP uno o più indirizzi IP evitando in questo modo accessi non autorizzati da parte di terzi o da parte di sistemi automatici.

L'abilitazione sarà di default permanente, ma potrà essere variata in qualsiasi momento, oppure disabilitata per periodo di tempo, grazie alla possibilità di selezionare un orario preciso fino a cui disabilitare gli IP o la/e classe/i IP precedentemente impostati.

Elementi di sicurezza con Drupal

Filtro accessi ftp con Aruba

Tramite l'apposito link FILTRA ACCESSI FTP presente nell'Area Clienti di Hosting, si può impostare una "White list", ovvero creare e abilitare una lista di indirizzi IP ai quali sarà consentito l'accesso via FTP allo spazio web (naturalmente l'accesso sarà sempre subordinato all'inserimento di login e password del dominio).

Elementi di sicurezza con Drupal

Filtro accessi ftp con Aruba

Il nuovo applicativo è raggiungibile su Area Clienti all'indirizzo: https://hosting.aruba.it/areautenti.asp

Elementi di sicurezza con Drupal

Filtro accessi ftp con Aruba

Una volta loggati, sarà possibile cliccare sulla voce "Filtra accessi FTP" e inserire (quindi abilitare) gli indirizzi IP che si desidera autorizzare all'accesso FTP dello spazio web.

Elementi di sicurezza con Drupal

Filtro accessi ftp con Aruba

IMPORTANTE: La lista degli indirizzi IP abilitati, sarà automaticamente associata a tutti i domini di secondo livello e terzo livello con servizio hosting, attivi sotto la stessa Login, senza necessità di dover ripetere l'inserimento per ciascun dominio.

Il Filtro non potrà invece essere abilitato sui domini di Terzo Livello che risultino gestiti con una Login diversa da quella del dominio di secondo livello cui sono abbinati.

Elementi di sicurezza con Drupal

Filtro accessi ftp con Aruba

L'aggiornamento della lista e la conseguente abilitazione avviene dopo qualche minuto dal salvataggio, pertanto, una volta inserito un indirizzo IP oppure una classe IP, l'accesso allo spazio web dei domini collegati alla stessa login, sarà consentito solamente agli IP inseriti, mentre tutti gli altri saranno impossibilitati all'accesso.

Al fine di facilitare la configurazione, nel momento in cui si accede, l'applicativo mostrerà in alto a destra l'indirizzo IP con il quale si è collegati alla rete.

Elementi di sicurezza con Drupal

Filtro accessi ftp con Aruba

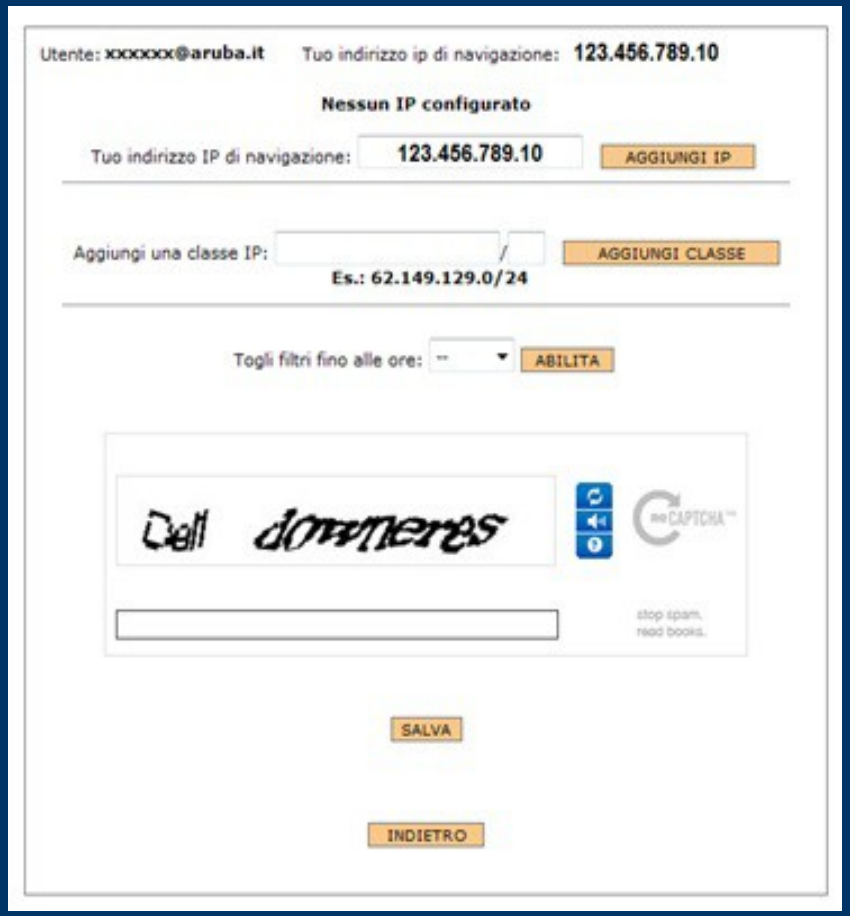
Per aggiungerlo e quindi abilitarlo all'accesso FTP, sarà sufficiente incollarlo nel campo scrivibile e cliccare su "Aggiungi IP".

Elementi di sicurezza con Drupal

Filtro accessi ftp

con Aruba

Dopo aver aggiunto l'IP, sarà necessario salvare la configura zione cliccando sull'apposito pulsante "Salva"; in caso contrario l'indirizzo non sarà aggiunto e quindi non sarà autorizzato all'accesso FTP. Ripetere l'operazione inserendo gli IP da autorizzare.



Elementi di sicurezza con Drupal

Filtro accessi ftp con Aruba

Attenzione: Nel caso in cui, la connessione a internet utilizzata, sia una connessione con indirizzo **IP dinamico** (ovvero con un indirizzo IP assegnato casualmente dalla rete), ogni qualvolta che si accede ad internet sarà necessario verificare che l'IP assegnato a ciascuna connessione risulti abilitato all'accesso FTP, in caso contrario, sarà necessario abilitarlo.

Elementi di sicurezza con Drupal

Filtro accessi ftp con Aruba

Eliminazione di un indirizzo dalla lista

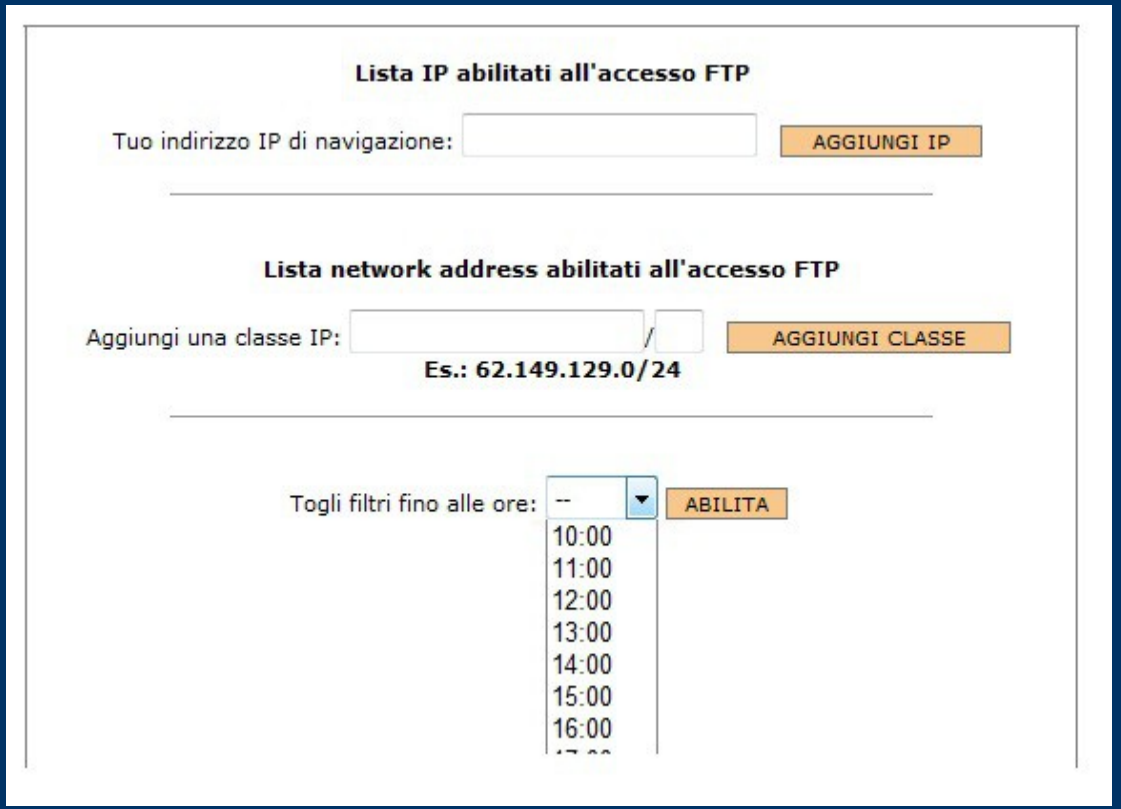
Per eliminare un indirizzo IP, o un network di IP, sarà sufficiente selezionarlo e quindi cliccare sulla voce "Rimuovi", avendo cura poi, di salvare la configurazione.

Elementi di sicurezza con Drupal

Filtro accessi ftp con Aruba

Disabilitazione Filtro a Orari

Sarà possibile disabilitare temporaneamente i filtri inseriti e far si che automaticamente vengano ristabiliti utilizzando la funzione Togli filtri fino alle ore.



Elementi di sicurezza con Drupal

Filtro accessi ftp con Aruba

Disabilitazione Filtro a Orari

una volta impostato, i filtri saranno disattivati, ovvero sarà possibile accedere all'FTP da qualsiasi IP della rete, fino all'ora selezionata, non appena raggiunto l'orario impostato, saranno ristabiliti i filtri precedenti e sarà possibile accedere solo tramite gli IP salvati.

Elementi di sicurezza con Drupal

Consigli principali

1. utilizzare sempre i CMS negli ambienti nativi: Wordpress, Joomla! e Drupal funzionano al meglio su piattaforma Linux Se utilizzi un hosting Windows chiedi subito il cambio di piattaforma

2. tenere costantemente aggiornato il CMS alla versione stabile più recente

3. effettuare frequentemente il backup dei materiali e del database, o attivare un servizio di backup periodico (contattaci per una offerta)

4. gestire con particolare prudenza e saggezza i permessi dei files e delle cartelle

Elementi di sicurezza con Drupal

Consigli principali

5. proteggere le risorse/directory più delicate con .htaccess (richiede spazio web Linux)

6. tenersi sempre aggiornati sulle problematiche specifiche della sicurezza del proprio CMS

7. proteggi al meglio il proprio computer da virus/trojan/maleware che possono sottrarre i tuoi dati di accesso (leggi questa FAQ)

8. scegli accuratamente i temi/plugin per il tuo CMS; spesso gli attacchi si concentrano proprio sui moduli aggiuntivi insicuri o difettosi dei sistemi di gestione dei contenuti

Elementi di sicurezza con Drupal

Consigli principali

9. utilizza password sicure: un account amministratore con elevati privilegi deve avere una password con almeno 8 caratteri includendo numeri e simboli speciali. Si consiglia di non utilizzare password puramente testuali o parole facilmente riscontrabili in un qualsiasi dizionario di lingua italiana; è ugualmente sconsigliato utilizzare date di nascita o informazioni facilmente reperibili in rete. Ecco un esempio di password complessa di 15 caratteri: !n9i!Oy"J@QrF^

Elementi di sicurezza con Drupal

Consigli principali

10. ove possibile (es. server dedicati, VPS, Cloud) utilizzare sempre configurazioni sicure del php.ini

register_globals = Off
magic_quotes_gpc = On
allow_url_fopen = Off
disable_functions = system, shell_exec, exec, phpinfo, proc_open