[en]Security Assessment - Redirect[/en][de]Schwachstellenanalyse - Redirect[/de][pt-br]Avaliação de Segurança - redirecionamento[/pt-br]
Category : The ImpressCMS Project Announcement
Published by Tom on 2008/9/8
[en]The ImpressCMS Security Team was recently notified of a potential security risk. After extensive assessments we have concluded this is not an actual risk, however we would like to make a formal statement to allow the community insight, this press release will contain the required details.[/en][de]ImpressCMS wurde kürzlich von einem potenziellen Sicherheitsrisiko bekannt gemacht. Nach umfassenden Recherchen haben wir beschlossen, dass das nicht eine wirkliche Gefahr ist, jedoch geben wir gern eine formelle Erklärung ab, um die Community zu informieren.[/de][pt-br]A equipe do ImpressCMS foi notificada recentemente sobre um potencial risco de segurança. Após extensas avaliações nós concluímos que este não é um risco real, no entanto, gostaríamos de fazer uma declaração formal para permitir que a comunidade avalie este comunicado de imprensa, onde deve conter as informações pedidas.[/pt-br]

[en]The potential security risk revolved around the xoops_redirect located within user.php and someone gaining access to the directory, however after extensive research we believe the exploit would only show what the person would already know is there and could type into the address bar manually. ImpessCMS distributions ship with an index.html file within the folders that don't contain an index.php file which prevents directory browsing.

user.php?op=main&xoops_redirect=[FILE]

It was claimed this could be used as a file and server detection technique, however this still wouldn't resolve files located outside of the webroot such as those included in the trust path so no one could gain access to your database credentials. The only files which would show are those which are located within the webroot and it would be the same as simply typing the address and file name directly into your browser. You can't include any remote urls or traverse back to read files outside of the webroot

http://localhost/ or http://localhost/Test/

Important Notice:

We urge users to place simple index.html files within directories that either don't already have an index.php file or index.html. This is especially important for parent directories when you install in sub-directories. Not doing so could allow someone to browser your directories as a file archive.

We hope this sets your mind at ease, however should you have any questions at all then please direct them to our forums where a member of the community will be happy to assist you further.

We believe security is very important and appreciate all reports of potential vulnerabilities. If you think you've found something and would like us to look into it then please report it to member of our community.[/en][de]Bei dem potenziellen Sicherheitsrisiko dreht es sich um den xoops_redirect mit Bezug auf die user.php und jemandem. Dadurch kann man Zugang zu einem Verzeichnis erlangen. Jedoch nach der umfassenden Forschung glauben wir, dass man damit nur das zeigen würde, was die Person sowie bereits wissen würde. Dies kann man auch mit dem manuellen tippen der Adresse erreichen. Das ImpessCMS verfügt über die index.html Dateien innerhalb des kompletten CMS. Wenn eine index.php Datei in einem Verzeichnis nicht enthalten ist, verhindert die index.html Datei das Durchsuchen von Verzeichnissen.

Ein Beispiel:

user.php?op=main&xoops_redirect=[FILE]

Durch die Technik des Trust_Path (der außerhalb von ImpressCMS liegt) kann keiner in die Datenbank eindringen und somit auch nicht die Passwörter auslesen. Es kann also niemand Zugang erhalten.

http://localhost/ or http://localhost/Test/

Wichtige Benachrichtigung:

Wir empfehlen allen, eine einfache index.html Dateie innerhalb eines jedes Verzeichnisses zu legen, sodass entweder eine index.php Datei oder index.html in jedem Verzeichnis enthalten ist. Das ist für das Elternteilverzeichnis besonders wichtig, wenn das ImpressCMS in ein Unterverzeichnis installiert wurde. Wen dies nicht getan wird, könnte jemand unter Umständen das Dateiarchiv durchbrowsen.[/de][pt-br]O potencial risco de segurança estava em torno da xoops_redirect localizada dentro do user.php e alguém poderia ganhar acesso ao diretório, porém após ampla investigação, acreditamos que só pode ser explorado aquilo que a pessoa já sabe que existe e poderá digitar na barra de endereços manualmente. As distribuições do ImpressCMS são fornecidas um arquivo index.html dentro da pasta que não contêm um arquivo index.php que impede diretório browser.

user.php?op=main&xoops_redirect=[FILE]

Alegou-se que este em tese poderia ser usado como um arquivo no servidor para uma detecção técnica, no entanto este ainda não iria resolver os arquivos localizados fora do webroot tais como os incluídos no caminho de confiança (trust_path), de tal modo que ninguém poderia ganhar acesso a sua base de dados ou credenciais. Os arquivos que só servem para mostrar aqueles que estão localizados dentro do webroot e seria o mesmo que simplesmente digitar o

endereço ou o nome de arquivo diretamente no seu navegador. Você não pode incluir qualquer urls remotas ou atravessar de volta para ler arquivos fora do webroot

http://localhost/ ou http://localhost/Test/

Aviso Importante:

Nós pedimos aos usuários para colocar um simples arquivo index.html dentro de diretórios onde já não exista um index.php ou index.html. Isto é especialmente importante para os diretórios pais quando você instala em sub-diretórios. Não fazê-lo poderia permitir que alguém use o navegador em diretórios para ver os seus arquivos.

Esperamos que isto deixe sua mente tranquila, porém se você tiver quaisquer perguntas sobre qualquer coisa, então por favor, vá em nossos fóruns onde um membro da comunidade terá o maior prazer em ajudá-lo ainda mais.[/pt-br]

Translations:

Translations Required: