]HackingTeam[| ROYAL & SUNALLIANCE ASSICURAZIONI

Royal&Sunalliance Assicurazioni

Realizzazione di un modulo per download di file su protocollo HTTP per l'applicazione PragmaWeb

Linee guida per l'implementazione sicura

Genova

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

STORIA DEL DOCUMENTO		
Versione	Data	Modifiche Effettuate
1.0	8 Maggio 2007	Emissione

INFORMAZIONI	
Data di Emissione	8 Maggio 2007
Versione	1.0
Tipologia Documento	Deliverable
Numero Pagine	9
Numero Allegati	0
Redatto da	Federico Guerrini
Approvato da	Gianluca Vadruccio

INDICE

1 Obiettivo del documento

Questo documento definisce le linee guida, con riferimento agli aspetti di sicurezza, per la realizzazione di un modulo di download di file su protocollo HTTP(S). Tale modulo sarà incorporato nell'applicazione "PragmaWeb" attualmente in uso presso Royal&Sunalliance Assicurazioni (RSA).

1.1 Organizzazione del documento

Il documento è organizzato come segue.

Il paragrafo 2 ("Ambiente di riferimento") riassume le caratteristiche tecniche del sistema su cui deve essere realizzato il modulo di download; il paragrafo 3 ("Descrizione della soluzione proposta") fornisce un inquadramento del modulo nell'architettura complessiva del sistema, ne definisce le specifiche funzionali e indica gli accorgimenti necessari per una implementazione sicura.

1.2 Utilizzo del documento

Il documento fornisce alcuni suggerimenti per l'implementazione sicura di un modulo di download da utilizzarsi nell'ambito di una applicazione J2EE già esistente. Le indicazioni qui riportate derivano

- dall'esperienza maturata da Hacking Team nell'ambito dei vulnerability assessment su tecnologie J2EE;
- dall'applicazione, al caso particolare in esame, di best practices per lo sviluppo di codice sicuro ampiamente utilizzate e condivise.

Qualora tali indicazioni non fossero compatibili con particolari caratteristiche, non note ad Hacking Team, dell'applicazione PragmaWeb, il presente documento verrà opportunamente aggiornato in seguito ai necessari chiarimenti con gli sviluppatori.

2 Ambiente di riferimento

Il modulo di file download deve operare nel contesto tecnologico di seguito descritto.

- ***Application server***: il modulo di file download deve essere implementato come servlet o JSP page per Tomcat 5.x.

- ***Posizionamento sulla rete RSA***: l'application server Tomcat è attestato sulla rete "DMZ Pubblica"; viene contattato dagli utenti che intendono effettuare il download dei file attraverso una connessione VPN ("VPN Agenzie").
- ***Modalità di accesso***: la funzionalità di file download deve essere resa disponibile agli utenti di PragmaWeb, che attualmente si autenticano all'applicazione mediante un token One Time Password (OTP) ActivIdentity.
- ***File scaricabili***: i file scaricabili sono generati su AS/400 con frequenza giornaliera da una procedura batch e resi disponibili sull'application server mediante una condivisione IFS.
- ***Politica di naming dei file scaricabili***: ai file disponibili nella condivisione IFS viene assegnato un nome formato da due componenti: l'agenzia di pertinenza e la data di generazione.
- ***Funzionalità di autorizzazione***: il modulo deve permettere di controllare quali file, tra quelli disponibili nella condivisione IFS, possono essere scaricati da ogni utente (in particolare, ogni utente può scaricare solo i file di pertinenza della propria agenzia).

3 Descrizione della soluzione proposta

Il modulo di file download deve essere implementato ed integrato nell'applicazione PragmaWeb in modo che sia possibile eseguire le seguenti azioni:

1) identificare l'utente che intende effettuare un download (autenticazione);
2) costruire e visualizzare l'elenco di file che possono essere scaricati dall'utente identificato (autorizzazione), accedendo alla condivisione IFS;
3) processare un parametro in input mediante il quale l'utente specifica il file di cui intende effettuare il download;
4) inviare il file selezionato al browser, permettendo all'utente di effettuarne il salvataggio su disco.

3.1 Identificazione dell'utente

Poiché il modulo di file download costituisce una estensione dell'applicazione PragmaWeb, si consiglia di svilupparlo come "web resource" della medesima applicazione. In questo modo, il download di file può avvenire all'interno di una sessione applicativa già esistente, senza richiedere all'utente nessuna ulteriore autenticazione.

Questo approccio non comporta lo sviluppo di codice per l'autenticazione; non comporta inoltre la modifica di componenti dell'applicazione PragmaWeb se, in seguito all'autenticazione effettuata

dall'utente per accedervi, sono disponibili, all'interno della sessione applicativa, informazioni sull'identità dell'utente e sull'agenzia a cui appartiene.

3.2 Definizione e visualizzazione dell'elenco dei file scaricabili

Questa operazione realizza una parte del processo di autorizzazione. Una sua implementazione errata può portare a vulnerabilità di livello applicativo tali per cui un utente potrebbe scaricare file a cui non deve avere accesso. In particolare, devono essere adottate le seguenti precauzioni.

- ***Generazione dei file disponibili per il download***. L'elenco dei file disponibili per il download per ogni utente viene definito confrontando il nome dei file presenti nella condivisione IFS (che contiene il nome dell'agenzia di riferimento) con l'agenzia di appartenenza dell'utente. ***Per una implementazione corretta, questa informazione, cioè l'agenzia di appartenenza dell'utente, deve essere recuperata dalla sessione attiva,*** e non da un parametro di input del form di visualizzazione dell'elenco dei file disponibili.
- ***Visualizzazione del nome dei file***. Nell'ipotesi che vengano ***rispettate le linee guida indicate nel successivo paragrafo*** ("Elaborazione del parametro di input contente il file da scaricare"), l'elenco dei file disponibili per il download può essere visualizzato utilizzando il nome reale dei file presenti sulla condivisione IFS. Non esistono comunque controindicazioni, dal punto di vista della sicurezza, per l'adozione di logiche di presentazione più evolute (ad esempio, tabelle con campi del tipo "Nome file", "Data").

La funzione di autorizzazione non deve implementare nessuna logica per il controllo delle date di generazione dei file, in quanto la gestione dei contenuti della condivisione IFS (e quindi anche l'eliminazione di file non più necessari) è demandata ad opportune procedure batch.

3.3 Elaborazione del parametro di input contente il file da scaricare

Questa operazione realizza la seconda parte del processo di autorizzazione. Una sua implementazione errata può portare a vulnerabilità di livello applicativo tali per cui un utente potrebbe scaricare file a cui non deve avere accesso. In particolare, devono essere adottate le seguenti precauzioni.

- ***Scelta del parametro in input***. Per mantenere semplice la logica di validazione del parametro e, al tempo stesso, scongiurare la possibilità di attacchi di tipo "Path traversal", si sconsiglia l'uso di un parametro contenente il nome del file da scaricare. Risulta invece ***preferibile l'utilizzo di un parametro che può assumere un valore numerico intero***

variabile tra 1 ed N, dove N è il numero di file disponibili per il download da parte dell'utente.

- ***Gestione server-side dell'elenco dei file scaricabili***: per utilizzare il parametro in input numerico di cui al paragrafo precedente, l'elenco dei file disponibili per il download per ogni utente può essere convenientemente gestito mediante una ***struttura dati per la memorizzazione di coppie nome-valore*** (come ad esempio java.util.Map) allocata all'interno della sessione attiva (si veda la figura seguente).

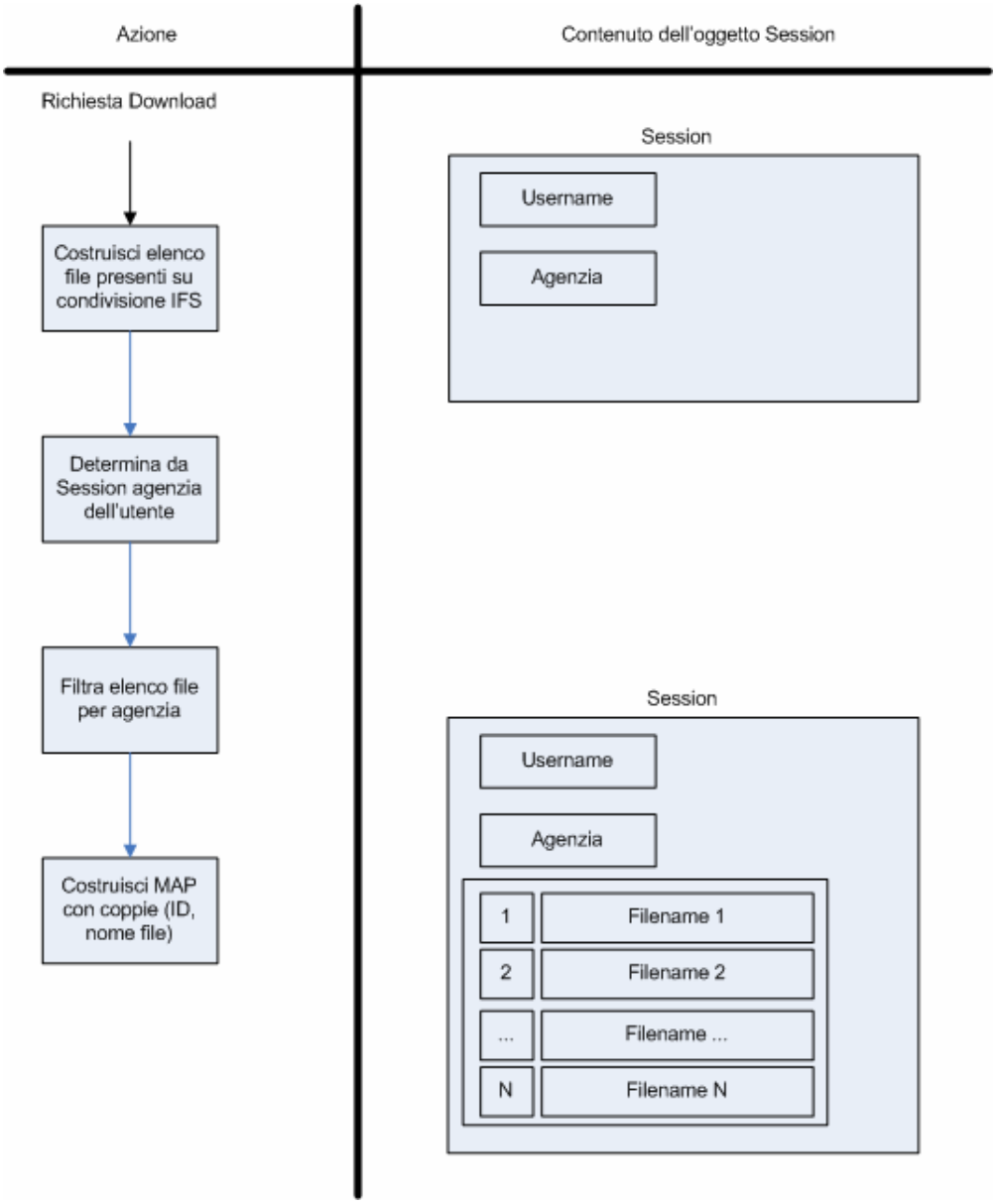

Figura 1. Gestione dell'elenco dei file scaricabili con oggetto java.util.Map in sessione

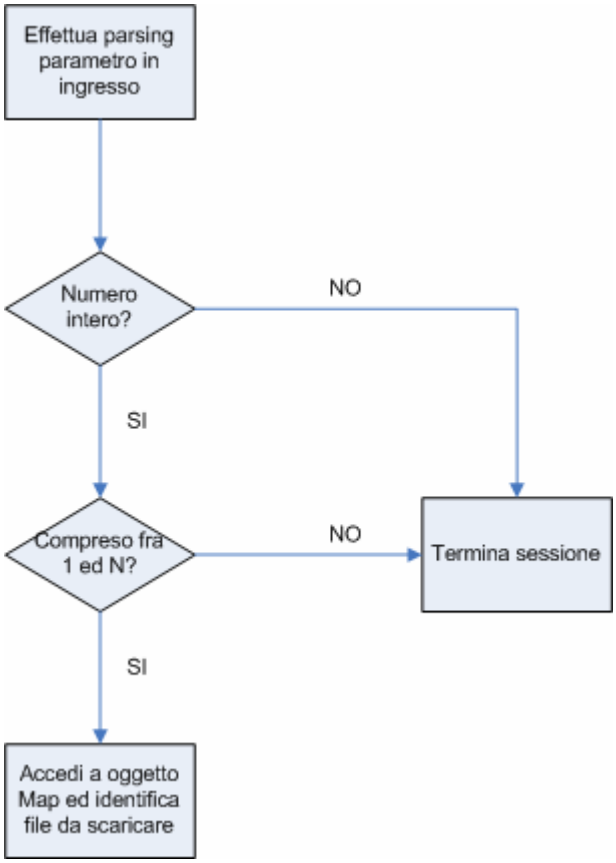

Figura 2. Validazione del parametro in input

3.4 Download del file

L'operazione di download del file non presenta aspetti critici dal punto di vista della sicurezza. Vengono pertanto forniti solo alcuni suggerimenti implementativi.

- ***Header "Content Disposition"***: affinché il browser consenta all'utente di effettuare il salvataggio su disco locale del file scaricato è necessario includere nella risposta HTTP contenente il file stesso l'header "Content-Disposition", di cui si riporta sintassi in BNF (si veda RFC 2183):

```
disposition := "Content-Disposition" ":"
               disposition-type
               *(";" disposition-parm)

disposition-type := "inline"
                  / "attachment"
                  / extension-token
                  ; values are not case-sensitive
```

```
disposition-parm := filename-parm
                  / creation-date-parm
                  / modification-date-parm
                  / read-date-parm
                  / size-parm
                  / parameter

filename-parm := "filename" "=" value

creation-date-parm := "creation-date" "=" quoted-date-time

modification-date-parm := "modification-date" "=" quoted-date-time

read-date-parm := "read-date" "=" quoted-date-time

size-parm := "size" "=" 1*DIGIT

quoted-date-time := quoted-string
                 ; contents MUST be an RFC 822 `date-time'
                 ; numeric timezones (+HHMM or -HHMM) MUST be used
```

- ***Scelta della modalità in cui effettuare l'output***: il download di file viene solitamente gestito in modalità byte-oriented, utilizzando l'oggetto javax.servlet.ServletOutputStream ritornato da ServletResponse.getOutputStream(). Si ricorda che la gestione dell'output in modalità byte-oriented è possibile solo da servlet e non da pagine JSP.