- Implementare le protezioni contro la manomissione dei percorsi di autenticazione e di autorizzazione (ad esempio, se l'autenticazione e l'autorizzazione dipendono dai dati del database, i percorsi di codice che interagiscono con il database devono essere protetti per garantire l'integrità di tali dati).
- Utilizzare implementazioni dell'Address Space Layout Randomization (ASLR) per rendere più difficile l'esecuzione di istruzioni privilegiate agli indirizzi noti in memoria tramite buffer overruns.
- Utilizzare compilatori che bloccano il buffer overruns.

Valutazione della priorità della minaccia (Ranking)

DREAD	Descrizione	Score
Damage Potential	L'attaccante potrebbe prendere il controllo del Web Server, se riuscisse a elevare i propri privilegi fino a livello appunto di amministratore del Web Server.	2
Reproducibility	L'attacco può essere condotto in qualunque momento.	3
Exploitability	Per la natura del servizio, l'attacco richiede un'utenza autenticata.	2
Affected Users	100% (se l'esito finale fosse effettivamente il controllo del sistema).	3
Discoverability	L'attaccante dovrà impegnare parecchie risorse per scoprire la vulnerabilità sfruttabile.	1

DREAD Score: 11/15 (MEDIO)

7.2.10 Cross Site Request Forgery

Categoria: Elevation Of Privilege

Descrizione: Il Cross Site Request Forgery (CSRF o XSRF) è un tipo di attacco in cui un attaccante fa in modo che un utente vittima (qui un Autheticated User del Web Server) invii involontariamente una richiesta HTTPS dal suo browser (qui Client Browser) al sistema web (qui Web Server) dove è attualmente autenticato.
L'attaccante deve: a) trovare un difetto (flaw) lato server (qui Web Server) tale per cui il sito web processa una richiesta di cambio stato a fronte della sola presenza di una sessione valida (che attesta una precedente autenticazione); b) indurre un utente ignaro (qui un Autheticated User del Web Server) ad esercitare un url che sfrutta il difetto di cui sopra mentre quell'utente ha una sessione aperta sul server (qui Web Server).
Il sistema, vulnerabile al CSRF, riceve dal browser dell'utente la richiesta contraffatta (dietro cui, cioè, si cela un'azione studiata dall'attaccante) con un cookie di sessione valido (dal momento che la vittima è stata precedentemente autenticata e la sessione è ancora attiva) e la elabora.

Contromisure: Fare in modo che tutte le richieste di cambiamento di stato oltre ad essere autenticate includano un ulteriore elemento di payload segreto (canary o CSRF token) conosciuto solo dal sito legittimo e dal browser (parti che comunicano tra loro in modo protetto tramite HTTPS).

Valutazione della priorità della minaccia (Ranking)

DREAD	Descrizione	Score