Remediation Progetto Build Week 2

Remediation Vancouver lato server

33850 - Unix Operating System Unsupported Version Detection

In base al numero di versione auto-dichiarato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato. La mancanza di supporto implica che il fornitore non rilascerà nuovi aggiornamenti di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Soluzione:

Fare l'upgrade del sistema operativo da Ubuntu 12.04 (supporto terminato nel 2017).

88098 - Apache Server ETag Header Information Disclosure

Il server web remoto è affetto da una vulnerabilità di divulgazione di informazioni a causa dell'intestazione ETag che fornisce informazioni sensibili che potrebbero agevolare un attaccante, come il numero di inode dei file richiesti.

Soluzione:

Modifica l'intestazione HTTP ETag del server web in modo da non includere gli inode dei file nel calcolo dell'intestazione ETag. Consulta la documentazione di Apache collegata per ulteriori informazioni.

90317 - SSH Weak Algorithms Supported

Nessus ha rilevato che il server SSH remoto è configurato per utilizzare il cifrario a flusso Arcfour o nessun cifrario affatto. La RFC 4253 sconsiglia l'uso di Arcfour a causa di un problema con le chiavi deboli.

Soluzione:

Contatta il fornitore o consulta la documentazione del prodotto per rimuovere i cifrari deboli.

70658 - SSH Server CBC Mode Ciphers Enabled

Il server SSH è configurato per supportare la crittografia Cipher Block Chaining (CBC). Ciò potrebbe consentire a un attaccante di recuperare il testo in chiaro dal testo cifrato. Si noti che questo plugin verifica solo le opzioni del server SSH e non controlla le versioni di software vulnerabili.

Soluzione:

Contatta il fornitore o consulta la documentazione del prodotto per disabilitare la crittografia del tipo Cipher Block Chaining (CBC) e abilitare la crittografia del tipo Counter (CTR) o Galois/Counter Mode (GCM).

153953 - SSH Weak Key Exchange Algorithms Enabled

Il server SSH remoto è configurato per consentire algoritmi di scambio chiave considerati deboli. Questo si basa sul documento di bozza IETF "Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH)" (draft-ietf-curdle-ssh-kex-sha2-20). Nella sezione 4 vengono fornite indicazioni sugli algoritmi di scambio chiave che NON DOVREBBERO e NON DEVONO essere abilitati. Questi includono:

- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1
- gss-gex-sha1-*

- gss-group1-sha1-*
- gss-group14-sha1-*
- rsa1024-sha1

Si tenga presente che questo plugin verifica solo le opzioni del server SSH e non controlla le versioni di software vulnerabili.

Soluzione:

Contatta il fornitore o consulta la documentazione del prodotto per disabilitare gli algoritmi deboli.

71049 - SSH Weak MAC Algorithms Enabled

Il server SSH remoto è configurato per consentire sia algoritmi MD5 che algoritmi di codifica a chiave di 96 bit, entrambi considerati deboli. Si tenga presente che questo plugin verifica solo le opzioni del server SSH e non controlla le versioni di software vulnerabili.

Soluzione:

Contatta il fornitore o consulta la documentazione del prodotto per disabilitare gli algoritmi MD5 e di codifica a chiave di 96 bit.

REMEDIATION VANCOUVER LATO WEB

Medium	Absence of Anti-CSRF Tokens

Nessun token Anti-CSRF è stato trovato in un modulo di invio HTML. Una richiesta di contraffazione di tipo cross-site (CSRF) è un attacco che consiste nel costringere una vittima a inviare una richiesta HTTP a una destinazione di destinazione senza la loro conoscenza o intenzione al fine di eseguire un'azione a nome della vittima. La causa sottostante è una funzionalità dell'applicazione che utilizza URL prevedibili per le azioni dei moduli in modo ripetibile. La natura dell'attacco consiste nello sfruttare la fiducia che un sito web ha per un utente. Al contrario, la vulnerabilità di tipo cross-site scripting (XSS) sfrutta la fiducia che un utente ha per un sito web. Anche se gli attacchi CSRF non sono necessariamente di tipo cross-site, possono esserlo. Descrizione: Gli attacchi CSRF sono efficaci in diverse situazioni, tra cui:

- La vittima ha una sessione attiva sul sito di destinazione.
- La vittima è autenticata tramite autenticazione HTTP sul sito di destinazione.
- La vittima si trova nella stessa rete locale del sito di destinazione. CSRF è stato principalmente utilizzato per eseguire azioni contro un sito di destinazione utilizzando i privilegi della vittima, ma sono state scoperte tecniche recenti per divulgare informazioni ottenendo accesso alla risposta. Il rischio di divulgazione di informazioni aumenta notevolmente quando il sito di destinazione è vulnerabile a XSS, poiché XSS può essere utilizzato come piattaforma per CSRF, consentendo all'attacco di operare all'interno dei limiti della stessa politica di stessa origine.

Soluzione:

Utilizza una libreria o un framework affidabile che non consenta l'insorgenza di questa vulnerabilità o fornisca costrutti che rendano più facile evitarla. Ad esempio, utilizza pacchetti anti-CSRF come l'OWASP CSRFGuard. Assicurati che la tua applicazione sia priva di problemi di cross-site scripting, poiché la maggior parte delle difese CSRF possono essere eluse utilizzando script controllati dall'attaccante. Genera un nonce univoco per ogni modulo, inserisci il nonce nel modulo e verifica il nonce al momento della ricezione del modulo. Assicurati che il nonce non sia prevedibile (CWE-330). Tieni presente che ciò può essere eluso utilizzando XSS.

Identificare le operazioni particolarmente pericolose. Quando l'utente esegue un'operazione pericolosa, inviare una richiesta di conferma separata per assicurarsi che l'utente intenda effettuare quell'operazione. Si noti che questo può essere bypassato utilizzando XSS. Utilizzare il controllo di gestione della sessione ESAPI. Questo controllo include un componente per CSRF. Non utilizzare il metodo GET per richieste che comportano un cambiamento di stato.

Controllare l'intestazione HTTP Referer per verificare se la richiesta proviene da una pagina attesa. Ciò potrebbe interrompere la funzionalità legittima, poiché gli utenti o i proxy potrebbero aver disabilitato l'invio del campo Referer per motivi di privacy.

Medium	Content Security Policy (CSP) Header Not Set

La Content Security Policy (CSP) è un livello aggiuntivo di sicurezza che aiuta a rilevare e mitigare determinati tipi di attacchi, tra cui Cross Site Scripting (XSS) e attacchi di inserimento di dati. Questi attacchi vengono utilizzati per rubare dati, deturpare siti o distribuire malware. La CSP fornisce un insieme di intestazioni standard HTTP che consentono ai proprietari di siti web di dichiarare le fonti approvate di contenuti che i browser dovrebbero essere autorizzati a caricare su quella pagina. I tipi coperti includono JavaScript, CSS, frame HTML, font, immagini e oggetti incorporabili come applet Java, ActiveX, file audio e video.

Soluzione:

Assicurati che il tuo server web, il server dell'applicazione, il load balancer, ecc. siano configurati per impostare l'intestazione Content-Security-Policy.

Medium	Missing Anti-clickjacking Header

La risposta non include né l'intestazione Content-Security-Policy con la direttiva 'frame-ancestors', né l'intestazione X-Frame-Options per proteggere contro gli attacchi di tipo 'ClickJacking'.

Soluzione:

I browser web moderni supportano le intestazioni HTTP Content-Security-Policy e X-Frame-Options. Assicurati che una di esse sia impostata su tutte le pagine web restituite dal tuo sito o applicazione.

Se si prevede che la pagina venga visualizzata solo in frame provenienti dal proprio server (ad esempio, fa parte di un FRAMESET), è consigliabile utilizzare SAMEORIGIN. Invece, se non si prevede mai che la pagina venga visualizzata in frame, si dovrebbe utilizzare DENY. In alternativa, si può prendere in considerazione l'implementazione della direttiva "frame-ancestors" della Content Security Policy.

Medium	Vulnerable JS Library

La libreria identificata jQuery, versione 1.12.3, presenta delle vulnerabilità.

Soluzione:

Si prega di effettuare l'aggiornamento alla versione più recente di jQuery.

Low	Cookie No HttpOnly Flag

È stato impostato un cookie senza l'indicatore HttpOnly, il che significa che il cookie può essere accessibile tramite JavaScript. Se uno script malevolo può essere eseguito in questa pagina, il cookie sarà accessibile e potrà essere trasmesso a un altro sito. Se si tratta di un cookie di sessione, potrebbe essere possibile dirottare la sessione (session hijacking).

Soluzione:

Assicurarsi che l'indicatore HttpOnly sia impostato per tutti i cookie.

Low	Cookie without SameSite Attribute

È stato impostato un cookie senza l'attributo SameSite, il che significa che il cookie può essere inviato come risultato di una richiesta 'cross-site'. L'attributo SameSite è una contromisura efficace contro gli attacchi di contraffazione delle richieste di tipo cross-site, inclusioni di script di tipo cross-site e attacchi temporizzati.

Soluzione:

Assicurarsi che l'attributo SameSite sia impostato su 'lax' o idealmente su 'strict' per tutti i cookie.

Low	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Il server web o dell'applicazione sta rivelando informazioni tramite uno o più intestazioni di risposta HTTP "X-Powered-By". L'accesso a tali informazioni potrebbe agevolare gli attaccanti nell'identificare altri framework/componenti di cui la tua applicazione web dipende e le vulnerabilità a cui tali componenti potrebbero essere soggetti.

Soluzione:

Assicurati che il tuo server web, il server dell'applicazione, il load balancer ecc. siano configurati per sopprimere le intestazioni "X-Powered-By".

Low	Server Leaks Version Information via "Server" HTTP Response Header Field

Il server web o dell'applicazione sta rivelando informazioni sulla versione tramite l'intestazione di risposta HTTP "Server". L'accesso a tali informazioni potrebbe agevolare gli attaccanti nell'identificare altre vulnerabilità a cui il tuo server web o dell'applicazione potrebbe essere soggetto.
Soluzione:

A**ssicurati che il tuo server web, il server dell'applicazione, il load balancer, ecc. siano configurati per sopprimere l'intestazione "Server" o fornire dettagli generici.**

Low	X-Content-Type-Options Header Missing

L'intestazione anti-MIME-Sniffing X-Content-Type-Options non è stata impostata su 'nosniff'. Ciò consente alle versioni più vecchie di Internet Explorer e Chrome di eseguire il MIME-sniffing sul corpo della risposta, potenzialmente causando l'interpretazione e la visualizzazione del corpo della risposta come un tipo di contenuto diverso da quello dichiarato. Le versioni attuali (primi del 2014) e le versioni legacy di Firefox utilizzeranno il tipo di contenuto dichiarato (se impostato), anziché eseguire il MIME-sniffing.

Soluzione:

Assicurarsi che l'applicazione o il server web imposti correttamente l'intestazione Content-Type e che imposti l'intestazione X-Content-Type-Options su 'nosniff' per tutte le pagine web. Se possibile, assicurarsi che l'utente finale utilizzi un browser web conforme agli standard e moderno che non esegua affatto il MIME-sniffing, oppure che possa essere indirizzato dall'applicazione web o dal server web a non eseguire il MIME-sniffing.

Remediation Derpnstink lato server

156164 - Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execution

Esiste una vulnerabilità di esecuzione remota di codice in Apache Log4j < 2.16.0 a causa di protezioni insufficienti sulle sostituzioni di ricerca dei messaggi quando si gestisce l'input controllato dall'utente. Un attaccante remoto e non autenticato può sfruttare questa vulnerabilità tramite una richiesta web per eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.

Si noti che questo bypass richiede una configurazione non predefinita. Solo i Layout di tipo "Pattern Layouts" con una ricerca di contesto (ad esempio, $${ctx:loginId}) sono vulnerabili a questo tipo di attacco.

Questo plugin richiede che sia lo scanner che la macchina di destinazione abbiano accesso a Internet.

Soluzione:

Effettuare l'aggiornamento alla versione 2.16.0 o successiva di Apache Log4j, o applicare le misure di mitigazione fornite dal produttore.

Si consiglia vivamente di effettuare l'aggiornamento alle versioni più recenti di Apache Log4j, poiché le versioni intermedie/patch hanno note vulnerabilità di gravità elevata e il produttore sta aggiornando frequentemente le proprie linee guida all'avviso a mano a mano che vengono scoperti nuovi studi e nuove conoscenze sull'impatto di Log4j. Consulta il sito HTTPS://LOGGING.APACHE.ORG/LOG4J/2.X/SECURITY.HTML per le ultime versioni disponibili.

156016 - Apache Log4Shell RCE detection via Path Enumeration (Direct Check HTTP)

Il server web remoto è affetto da una vulnerabilità di esecuzione remota di codice tramite una falla nella libreria Apache Log4j. La vulnerabilità è dovuta all'elaborazione di input non sanificati inviati a una funzione di registrazione (logging). Un attaccante remoto, non autenticato, può sfruttare questa vulnerabilità tramite una richiesta web per eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.

Soluzione:

Aggiornare alla versione 2.15.0 o successiva di Apache Log4j, o applicare le misure di mitigazione fornite dal produttore.

Si consiglia vivamente di effettuare l'aggiornamento alle versioni più recenti di Apache Log4j, poiché le versioni intermedie/patch hanno note vulnerabilità di gravità elevata e il produttore sta aggiornando frequentemente le proprie linee guida all'avviso a mano a mano che vengono scoperti nuovi studi e nuove conoscenze sull'impatto di Log4j. Consultare il sito https://logging.apache.org/log4j/2.x/security.html per le ultime versioni disponibili.

156056 - Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)

Esiste una vulnerabilità di esecuzione remota di codice in Apache Log4j < 2.15.0 a causa di protezioni insufficienti sulle sostituzioni di ricerca dei messaggi quando si gestisce l'input controllato dall'utente. Un attaccante remoto e non autenticato può sfruttare questa vulnerabilità tramite una richiesta web per eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.

Questo plugin invia una stringa di test a un insieme di porte aperte sull'host di destinazione. Per l'utilizzo di questo plugin, sia lo scanner che la macchina di destinazione devono avere accesso a Internet.

Soluzione:

Aggiornare alla versione 2.15.0 o successiva di Apache Log4j, oppure applicare la mitigazione fornita dal produttore.

È altamente consigliato effettuare l'aggiornamento alle versioni più recenti di Apache Log4j poiché le versioni intermedie o le patch presentano note vulnerabilità di gravità elevata e il produttore aggiorna frequentemente le proprie avvisi man mano che vengono scoperti nuovi studi e nuove conoscenze sull'impatto di Log4j. Fare riferimento a https://logging.apache.org/log4j/2.x/security.html per le ultime versioni disponibili.

156115 - Apache Log4Shell RCE detection via callback correlation (Direct Check FTP)

Esiste una vulnerabilità di esecuzione remota del codice in Apache Log4j < 2.15.0 a causa di protezioni insufficienti sulle sostituzioni di ricerca dei messaggi durante la gestione dell'input controllato dall'utente. Un attaccante remoto e non autenticato può sfruttare questa vulnerabilità tramite una richiesta web per eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.

Soluzione:

Aggiornare ad Apache Log4j versione 2.15.0 o successiva, o applicare la mitigazione fornita dal venditore.

Si consiglia vivamente di effettuare l'aggiornamento alle versioni più recenti di Apache Log4j in quanto le versioni intermedie o le patch presentano vulnerabilità di gravità elevata note e il venditore aggiorna frequentemente i propri avvisi a seguito di nuove ricerche e conoscenze sull'impatto di Log4j. Fare riferimento a https://logging.apache.org/log4j/2.x/security.html per le ultime versioni disponibili.

156014 - Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)

Esiste una vulnerabilità di esecuzione remota del codice in Apache Log4j < 2.15.0 a causa di protezioni insufficienti sulle sostituzioni di ricerca dei messaggi durante la gestione dell'input controllato dall'utente. Un attaccante remoto e non autenticato può sfruttare questa vulnerabilità tramite una richiesta web per eseguire codice arbitrario con il livello di autorizzazione del processo Java in esecuzione.

Questo plugin richiede che sia lo scanner che la macchina di destinazione abbiano accesso a Internet.

Soluzione:

Aggiorna ad Apache Log4j versione 2.15.0 o successiva, oppure applica la mitigazione fornita dal venditore.

Si consiglia vivamente di effettuare l'aggiornamento alle versioni più recenti di Apache Log4j, poiché le versioni intermedie e le patch presentano vulnerabilità di gravità elevata note e il venditore aggiorna frequentemente i propri avvisi a seguito di nuove ricerche e conoscenze sull'impatto di Log4j. Per le ultime versioni disponibili, fare riferimento a https://logging.apache.org/log4j/2.x/security.html.

156166 - Apache Log4Shell RCE detection via callback correlation (Direct Check SSH)

L'host remoto sembra eseguire SSH. SSH stesso non è vulnerabile a Log4Shell; tuttavia, il server SSH potrebbe essere potenzialmente colpito se tenta di registrare dati tramite una libreria log4j vulnerabile.

Questo plugin richiede che sia lo scanner che la macchina di destinazione abbiano accesso a Internet.

Soluzione:

Aggiorna ad Apache Log4j versione 2.15.0 o successiva, oppure applica la mitigazione fornita dal venditore.

Si consiglia vivamente di effettuare l'aggiornamento alle versioni più recenti di Apache Log4j, poiché le versioni intermedie e le patch presentano vulnerabilità di gravità elevata note e il venditore aggiorna frequentemente i propri avvisi a seguito di nuove ricerche e conoscenze sull'impatto di Log4j. Per le ultime versioni disponibili, fare riferimento a https://logging.apache.org/log4j/2.x/security.html.

164017 - NodeJS System Information Library Command Injection (CVE-2021-21315)

L'host remoto contiene un modulo npm systeminformation precedente alla versione 5.3.1. Pertanto, è affetto da una vulnerabilità di injection di comandi. La System Information Library per Node.JS (pacchetto npm 'systeminformation') è una raccolta di funzioni open source per recuperare informazioni dettagliate sull'hardware, sul sistema e sul sistema operativo. In systeminformation prima della versione 5.3.1 esiste una vulnerabilità di injection di comandi. La vulnerabilità è stata corretta nella versione 5.3.1. Come soluzione alternativa, anziché effettuare l'aggiornamento, assicurarsi di controllare o sanificare i parametri di servizio che vengono passati a si.inetLatency(), si.inetChecksite(), si.services(), o si.processLoad()... per consentire solo stringhe e rifiutare qualsiasi array. La sanificazione delle stringhe funziona come previsto.

Soluzione:

Effettuare l'aggiornamento al modulo systeminformation alla versione 5.3.1 o successiva.

90317 - SSH Weak Algorithms Supported

Nessus ha rilevato che il server SSH remoto è configurato per utilizzare il cifrario di flusso Arcfour o nessun cifrario affatto. RFC 4253 consiglia di evitare l'uso di Arcfour a causa di un problema con chiavi deboli.

Soluzione:

Contattare il fornitore o consultare la documentazione del prodotto per rimuovere i cifrari deboli.

70658 - SSH Server CBC Mode Ciphers Enabled

Il server SSH è configurato per supportare la crittografia Cipher Block Chaining (CBC). Ciò potrebbe consentire a un attaccante di recuperare il testo in chiaro dal testo cifrato. Si noti che questo plugin controlla solo le opzioni del server SSH e non verifica le versioni del software vulnerabili.

Soluzione:

Contattare il fornitore o consultare la documentazione del prodotto per disabilitare la crittografia in modalità CBC e abilitare la crittografia in modalità CTR o GCM.

153953 - SSH Weak Key Exchange Algorithms Enabled

Il server SSH remoto è configurato per consentire algoritmi di scambio chiave considerati deboli. Questo si basa sul documento IETF Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. La sezione 4 fornisce indicazioni sugli algoritmi di scambio chiave che NON DOVREBBERO essere abilitati. Questi includono:

- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1
- gss-gex-sha1-*
- gss-group1-sha1-*
- gss-group14-sha1-*
- rsa1024-sha1

Soluzione:

Contattare il fornitore o consultare la documentazione del prodotto per disabilitare gli algoritmi deboli.

71049 - SSH Weak MAC Algorithms Enabled

Il server SSH remoto è configurato per consentire l'utilizzo di algoritmi MAC MD5 o a 96 bit, entrambi considerati deboli. Si noti che questo plugin controlla solo le opzioni del server SSH e non verifica le versioni vulnerabili del software.

Soluzione:

Contattare il fornitore o consultare la documentazione del prodotto per disabilitare gli algoritmi MAC MD5 e a 96 bit.

REMEDIATION DERPNSTINK LATO WEB

Medium	Content Security Policy (CSP) Header Not Set

La Content Security Policy (CSP) è un livello aggiuntivo di sicurezza che aiuta a rilevare e mitigare determinati tipi di attacchi, inclusi Cross Site Scripting (XSS) e attacchi di iniezione di dati. Questi attacchi vengono utilizzati per scopi che vanno dal furto di dati alla defacement del sito o alla distribuzione di malware. La CSP fornisce un insieme di intestazioni HTTP standard che consentono ai proprietari di siti web di dichiarare le origini approvate dei contenuti che i browser dovrebbero essere autorizzati a caricare sulla pagina, inclusi JavaScript, CSS, frame HTML, font, immagini e oggetti embeddabili come applet Java, ActiveX, file audio e video.

Soluzione:

Assicurati che il tuo server web, server dell'applicazione, load balancer, ecc. siano configurati per impostare l'intestazione Content-Security-Policy.

Medium	Missing Anti-clickjacking Header

La risposta non include né l'intestazione Content-Security-Policy con la direttiva 'frame-ancestors', né l'intestazione X-Frame-Options per proteggere dagli attacchi di 'ClickJacking'.

Soluzione:

I browser web moderni supportano le intestazioni HTTP Content-Security-Policy e X-Frame-Options. Assicurati che una di esse sia impostata su tutte le pagine web restituite dal tuo sito o applicazione. Se prevedi che la pagina venga inclusa solo da pagine sul tuo server (ad esempio, fa parte di un FRAMESET), dovresti utilizzare SAMEORIGIN. In caso contrario, se non prevedi mai che la pagina venga inclusa, dovresti utilizzare DENY. In alternativa, considera l'implementazione della direttiva "frame-ancestors" della Content Security Policy.

Low	Cross-Domain JavaScript Source File Inclusion

La pagina include uno o più file di script da un dominio di terze parti.

Soluzione:

Assicurati che i file di origine JavaScript vengano caricati solo da fonti affidabili e che tali fonti non possano essere controllate dagli utenti finali dell'applicazione.

Low	Server Leaks Version Information via "Server" HTTP Response Header Field

Il server web/applicazione sta rivelando informazioni sulla versione tramite l'intestazione di risposta HTTP "Server". L'accesso a tali informazioni potrebbe agevolare gli attaccanti nell'identificare altre vulnerabilità a cui il tuo server web/applicazione è soggetto.

Soluzione:

Assicurati che il tuo server web, applicativo, load balancer, ecc. sia configurato per nascondere l'intestazione "Server" o fornire dettagli generici al riguardo.

Low	X-Content-Type-Options Header Missing

L'intestazione anti-MIME-sniffing X-Content-Type-Options non è impostata su 'nosniff'. Ciò consente alle versioni più vecchie di Internet Explorer e Chrome di eseguire il MIME-sniffing sul corpo della risposta, potenzialmente causando l'interpretazione e la visualizzazione del corpo della risposta come un tipo di contenuto diverso dal tipo di contenuto dichiarato. Le versioni attuali (prime del 2014) e le versioni legacy di Firefox utilizzeranno il tipo di contenuto dichiarato (se impostato), anziché eseguire il MIME-sniffing.

Soluzione:

Assicurati che l'applicazione/server web imposti correttamente l'intestazione Content-Type e che imposti l'intestazione X-Content-Type-Options su 'nosniff' per tutte le pagine web. Se possibile, assicurati che l'utente finale utilizzi un browser web moderno e compatibile con gli standard che non esegue affatto il MIME-sniffing, o che possa essere indirizzato dall'applicazione web/server a non eseguire il MIME-sniffing.