Report di Valutazione delle Vulnerabilità App Web

Nome dell'Applicazione: Sito Web > ACUNETIX ACUART
URL dell'applicazione: http://testphp.vulnweb.com/
Data della Valutazione: 27/10/2023
Responsabile della Valutazione: Giovanni Saponaro

Sulla piattaforma online durante la scansione è stato rilevato che il sito si appoggia su un server negli Stati Uniti avente indirizzo IP 44.228.249.3 ed è equipaggiato con la seguente tecnologia:

web server operating system: Linux Ubuntu v.20.04

web application technology: PHP 5.6.40, web server opensource Nginx v.1.19.0

back-end DBMS operating system: Linux Ubuntu

back-end DBMS: MySQL >= v.5.6

I controlli sono stati eseguiti in modo approfondito con diversi strumenti utili a capirne le vulnerabilità presenti e raccomandarne la risoluzione.

Nello specifico: il sito risulta clonabile, quindi un cybercriminale può sfruttare il clone per scopi illeciti, ad esempio inviando una mail ad una vittima con all'interno l'indirizzo del sito web che lo raggiunge alla pagina di inserimento dati, come la pagina login di una banca, attendendo che la vittima inserisca i dati di accesso per utilizzarli a scopi illeciti.

La scansione ha analizzato le seguenti Directory e i relativi file al loro interno e ha rilevato alcune vulnerabilità ad alto rischio.

Directory Stucture	Response Code	Response Size
/	200	5293
login.php	200	228
index.php	200	228
signup.php	200	228
cart.php	200	228
search.php	200	228
admin	200	155
images	200	155
cgi-bin	403	460
categories.php	200	228
artists.php	200	228
disclaimer.php	200	228
guestbook.php	200	228
AJAX	200	228
userinfo.php	302	252
Mod_Rewrite_Shop	200	228
hpp	200	228
Flash	200	155

Elenco delle Vulnerabilità intercettate:

Numero totale di vulnerabilità rilevate: 5

Severità delle vulnerabilità: 6 > 10

Vulnerabilità: Query injection vector > Fattore di Rischio: CRITICO - 10

Tipo di Vulnerabilità: vulnerabilità di sicurezza

Descrizione: Una "Query Injection" (iniezione di query) è una vulnerabilità di sicurezza che si verifica quando un'applicazione web non tratta correttamente gli input dell'utente prima di includerli in query SQL o in altri comandi di interrogazione del database. Questa vulnerabilità consente a un attaccante di iniettare codice malevolo all'interno delle query del database, consentendo loro di manipolare il database, eseguire query non autorizzate e potenzialmente ottenere o danneggiare dati sensibili.

Localizzazione: la vulnerabilità è stata localizzata nella seguente url:
http://testphp.vulnweb.com/secured/newuser.php
Raccomandazioni: Per prevenire le "Query Injection", le applicazioni web dovrebbero implementare pratiche di sicurezza come l'uso di istruzioni parametrizzate o query preparate, la validazione dei dati di input e la corretta gestione degli errori. Le applicazioni dovrebbero anche limitare i privilegi del database e utilizzare l'approccio del principio del privilegio minimo (Least Privilege Principle) per ridurre l'impatto di un eventuale attacco.

Vulnerabilità: Shell injection vector > Fattore di rischio: CRITICO - 10

Tipo di Vulnerabilità: vulnerabilità di sicurezza

Descrizione: Una "Shell Injection" (iniezione di shell) è una vulnerabilità di sicurezza che si verifica quando un'applicazione web o un sistema non tratta in modo sicuro gli input dell'utente e consente a un attaccante di eseguire comandi shell non autorizzati all'interno del sistema operativo ospite. Questo tipo di vulnerabilità può portare a una serie di problemi di sicurezza, inclusi l'accesso non autorizzato, l'esecuzione di comandi dannosi e la compromissione del sistema.

Localizzazione: la vulnerabilità è stata localizzata nella url: http://testphp.vulnweb.com/sendcommand.php

Raccomandazioni: Per prevenire le "Shell Injection" e le sue varianti, è importante implementare pratiche di sicurezza come la validazione rigorosa dei dati di input, l'uso di meccanismi di escape per evitare l'iniezione di comandi, l'uso di funzionalità di sicurezza offerte dai linguaggi di programmazione, e la limitazione dei privilegi del sistema in modo che anche se un attaccante riesce a eseguire comandi, i danni siano minimi. Inoltre, è

fondamentale mantenere tutti i software e le librerie utilizzate nell'applicazione sempre aggiornati per rimediare alle vulnerabilità conosciute.

Vulnerabilità: Conflict MIME / Charset info > Fattore di rischio: ALTO - 8/9
Tipo di Vulnerabilità: vulnerabilità di tipo MIME (Multipurpose Internet Mail Extensions)

Descrizione: Le vulnerabilità MIME sono spesso associate alla manipolazione di tipi di contenuti e alla gestione non sicura dei dati nei protocolli di comunicazione, in particolare nei messaggi di posta elettronica e nella navigazione web. Alcuni punti chiave relativi alle vulnerabilità MIME associate: Content Type Security Header - Cross-Site Scripting (XSS)- File Upload

Localizzazione: la vulnerabilità è stata localizzata nelle seguenti url:
http://testphp.vulnweb.com/secured/newuser.php
http://testphp.vulnweb.com/comment.php
http://testphp.vulnweb.com/guestbook.php
http://testphp.vulnweb.com/listproducts.php?artist=.htaccess.aspx--
>">'>'"<sfi000287v804940>$row["artist_id"].”

Raccomandazioni: Per debellare le vulnerabilità MIME, è importante seguire le best practice di sicurezza, convalidare e sanificare correttamente i dati, utilizzare adeguate politiche di sicurezza dei contenuti e implementare un'adeguata gestione dei tipi di contenuto.

Vulnerabilità: XSS vector in document body > Fattore di rischio: ALTO - 8/9

Tipo di Vulnerabilità: una variante di Cross-Site Scripting.

Descrizione: È una vulnerabilità di sicurezza che consente a un attaccante di iniettare script malevoli all'interno del contenuto di una pagina web e quindi di eseguire codice JavaScript dannoso nel browser degli utenti che visualizzano quella pagina. Nel caso specifico di "XSS vector in document body", il vettore XSS si trova nel corpo principale (body) del documento HTML di una pagina web, il che significa che l'attaccante è riuscito a inserire uno script malevolo all'interno del contenuto visibile della pagina. Questo rende l'attacco particolarmente pericoloso, in quanto può colpire direttamente gli utenti che visitano la pagina, senza richiedere loro di fare clic su link o di eseguire azioni particolari.

Localizzazione: la vulnerabilità è stata localizzata nelle seguenti url:
http://testphp.vulnweb.com/secured/newuser.php
http://testphp.vulnweb.com/comment.php
http://testphp.vulnweb.com/listproducts.php?artist=.htaccess.aspx--
>">'>'"<sfi000287v804940>$row["artist_id"]
http://testphp.vulnweb.com/listproducts.php?artist=.htaccess.aspx--
>">'>'"<sfi000237v804940>$row["artist_id"]
http://testphp.vulnweb.com/listproducts.php?artist=.htaccess.aspx--
>">'>'"<sfi000013v804940>$row["artist_id"]
Raccomandazioni: Per mitigare gli attacchi XSS, gli sviluppatori web dovrebbero adottare pratiche di sviluppo sicuro, tra cui la validazione e l'escape dei dati in ingresso, l'utilizzo di intestazioni di sicurezza del contenuto (come Content Security Policy), e la convalida delle origini delle richieste. Gli utenti dovrebbero anche essere cauti quando visitano siti web e dovrebbero utilizzare estensioni o strumenti di sicurezza del browser per proteggersi da possibili attacchi XSS.

Vulnerabilità: HTML form with no apparent XSRF protection > Fattore di rischio: MEDIO - 6/7

Tipo di Vulnerabilità: vulnerabilità di sicurezza che può consentire a un attaccante di compiere azioni non autorizzate.

Descrizione: La protezione CSRF (Cross-Site Request Forgery), non XSFR, è una vulnerabilità di sicurezza web che può consentire a un attaccante di eseguire azioni senza il consenso dell'utente. Questa vulnerabilità si verifica quando un sito web non verifica adeguatamente l'origine di una richiesta HTTP.

Un utente autenticato è loggato su un sito web (ad esempio, un servizio di banca online).
Questo utente visita un altro sito web (controllato da un attaccante) che contiene un link o un modulo con un'azione che è destinata a essere eseguita sul sito web della banca.
L'utente fa clic sul link o invia il modulo senza rendersi conto che sta effettuando una richiesta al sito web della banca. Poiché l'utente è autenticato presso la banca, la richiesta viene elaborata, e l'attaccante può effettuare azioni non autorizzate a nome dell'utente (ad esempio, trasferire fondi a un altro account).

Localizzazione: la vulnerabilità è stata localizzata nelle seguenti url:
http://testphp.vulnweb.com/search.php?test=query
http://testphp.vulnweb.com/hpp/params.php?aaaa/=
http://testphp.vulnweb.com/comment.php
http://testphp.vulnweb.com/guestbook.php
http://testphp.vulnweb.com/search.php?test=query
http://testphp.vulnweb.com/sendcommand.php
http://testphp.vulnweb.com/search.php?test=query
http://testphp.vulnweb.com/showimage.php?file=guestbook.php
http://testphp.vulnweb.com/search.php?test=query
http://testphp.vulnweb.com/showimage.php?file=userinfo.php
http://testphp.vulnweb.com/showimage.php?file=guestbook.php
http://testphp.vulnweb.com/showimage.php?file=userinfo.php

Raccomandazioni: Per proteggersi dalle CSRF, i siti web utilizzano solitamente token CSRF. Questi token sono generati dal server e inclusi in ogni richiesta HTTP, quindi il server può verificare che la richiesta provenga effettivamente dall'utente autenticato e non da un sito web esterno.

Conclusione: La sicurezza di un sito web è un processo continuo e richiede un impegno costante per rimanere al passo con le minacce in evoluzione. Quindi è importante monitorare costantemente la sicurezza del sito, mantenere aggiornati tutti i componenti presenti, implementare una robusta autenticazione degli utenti, lavorare rigorosamente anche sugli input degli utenti per la prevenzione di attacchi SQL, XSS e limitarne soprattutto l'accesso a risorse critiche, assicurarsi di proteggere i dati sensibili dei visitatori del sito, così come la protezione da XSFR (Cross-Site Request Forgery) è fondamentale per garantire la sicurezza delle applicazioni web, in modo che gli utenti non possano essere ingannati inavvertitamente in azioni non desiderate o dannose. Infine è altamente consigliato di collaborare con esperti di sicurezza informatica e creare un piano per la sicurezza che affronti le specifiche esigenze del tuo sito web.

Giovanni Saponaro