Diario di lavoro

Luogo	Canobbio
Data	24.09.2019

Lavori svolti

13h15 -14h45

Come scritto nel diario precedente, durante queste prime due ore ho commentato tutto il codice da me prodotto. Inoltre ho eseguito alcune modifiche principalemente di stile del codice. Ho separato la classe di connessione al database dalla pagina principale ad una sottoclasse.

15h00 – 16h20

Ho iniziato a creare le documentazioni di come eseguire le vulnerabilità presenti in HackerLab. Al momento le documentazioni si trovano accedendo ad HackerLab sotto forma di articoli web.

Broken Authentication

di Administrator

Pubblicato il 24.09.2019 alle 16:17

Questi tipi di vulnerabilità possono consentire a un aggressore di catturare o bypassare i metodi di autenticazione utilizzati da un'applicazione web.

All'interno di HackerLab è presente una vulnerabilità di questo tipo.
Per sfruttare questa vulnerabilità basterà utilizzare una comune estensione come per esempio:
EditThisCookie
Una volta installata l'estensione sarà possibile modificare i cookie all'interno dei siti web.
Noterai che HackerLab ha un cookie chiamato `permission`, il contenuto di questo cookie è famigliare, è un testo codificato in base64.

```
dXNlcg== -> user
```

Con un po' di fortuna è possibile indovinare quale sarà il permesso di un amministratore, quindi provando per esempio a modificare il cookie in

```
YWRtaW5pc3RyYXRvcg== -> administrator
```

e ricaricando la pagina potrai notare delle modifiche nel layout, ora potrai vedere informazioni e pagine aggiuntive come se fossi un amministratore!

Mmm, sono curioso di come potresti sfruttare questa vulnerabilità...
Fonti

Figura 1 Broken Authentication

File inclusion vulnerability o Directory Traversal

di Administrator

Pubblicato il 24.09.2019 alle 16:17

Una directory traversal (o path traversal) consiste nello sfruttare l'insufficiente validazione della sicurezza / sanificazione dei nomi dei file di input forniti dall'utente, in modo che i caratteri che rappresentano "traverse to parent directory" siano passati attraverso le API dei file.

Grazie a questa descrizione potresti già aver individuato un percorso vulnerabile a questo tipo di attacco, se non lo hai trovato un indizio potrebbe essere l'immagine di questo articolo.
Il percorso tramite il quale vengono ricavate le immagini in HackerLab è il seguente

```
/image/?file_name=IMAGE
```

Bene, per eseguire questa vulnerabilità basterà sostituire il valore del nome dell'immagine con dei file conosciuti, potremmo per esempio iniziare tentando di capire la struttura del programma provando svariati file:

- .htaccess
- ../composer.json
- e così via

Possiamo notare come nel caso di `/image/?file_name=../composer.json` abbiamo ricevuto una risposta:


```
{
"name": "filippofinke/HackerLab",
"description": "Sito web per la dimostrazione di vulnerabilità",
"authors": [
{
"name": "Filippo Finke"
}
],
"require": {
"php": ">=5.6",
"slim/php-view": "^2.0",
"slim/slim": "^3.1",
"phpmailer/phpmailer": "^6.0"
},
"scripts": {
"start": "sudo php -S 127.0.0.1:80 -t public"
}
}
```


Attraverso questa risposta possiamo confermare la presenza della vulnerabilità.

Ci saranno altri file accessibili?
Fonti

Figura 2 File Inclusion o Directory Traversal

Insecure Direct Object References

di Administrator

Pubblicato il 24.09.2019 alle 16:17

I riferimenti diretti agli oggetti insicuri si verificano quando un'applicazione fornisce l'accesso diretto agli oggetti in base all'input fornito dall'utente. Come risultato di questa vulnerabilità gli aggressori possono aggirare l'autorizzazione e accedere direttamente alle risorse del sistema, ad esempio i record o i file del database.

In base a questa piccola descrizione forse avrai già riconosciuto questa vulnerabilità all'interno di HackerLab.
Se presti attenzione alla pagina di questo post noterai che il percorso per arrivarci è `/post/3`
Quindi possiamo considerare il percorso come `/post/POST_ID`
Questo conferma dunque la presenza di questa vulnerabilità.

Chissà cosa può comportare questa vulnerabilità...
Quando navighi presta attenzione :D
Fonti

Figura 3 Insecure Direct Object References

Account takeover vulnerability

di Administrator

Pubblicato il 24.09.2019 alle 16:17

Una vulnerabilità di tipo "Account takeover vulnerability" è quando un attaccante riesce a prendere il controllo completo dell'account di un altra persona registrata ad una determinata piattaforma.

Anche questa vulnerabilità è presente in HackerLab.
Questa vulnerabilità è più difficile da identificare, per accedere ad HackerLab si dispongono di solamente una opzione, ovvero di accedere con email e password.
Se hai prestato attenzione a ciò che ho scritto precedentemente ti sarai soffermato sui parametri `email e password`, perfetto. Analizzando bene i due parametri possiamo dire che il parametro `email` non è possibile da attaccare in quanto non è possibile eseguirne una modifica, mentre in HackerLab è presente una funzionalità di recupero password che può modificare il parametro `password`.
Bene, abbiamo trovato cosa testare per rilevare se è presente una vulnerabilità di questo tipo.

Richiedendo una email di recupero password possiamo notare che il contenuto dell'email è simile al seguente:

```
Recupera la tua password premendo il seguente link:
http://hackerlab.ch/?reset_token=MTU2ODk4ODU2OA%3D%3D
```

Possiamo notare un parametro, `reset_token`, che andremo ad attaccare.
Se si analizza più attentamente il parametro possiamo notare che è una codifica in base64, andandola a decodificare otteniamo:

```
156898856
```

A primo impatto può sembrare un numero casuale, ma provando ad inviare più email di recupero possiamo notare che continua ad incrementare con una logica, ovvero quella del tempo.
Il token di recupero è quindi la codifica in base64 del tempo di quando è stato richiesto il recupero.
Possiamo fare una bozza del codice:

```
$token = base64_encode(time());
```

Questo è tutto, chissà come potrai sfruttarla...

Figura 4 Account takeover

16h20 – 16h30
Stesura diario.

Problemi riscontrati e soluzioni adottate
Non ho riscontrato nessun problema.

Punto della situazione rispetto alla pianificazione

Mi trovo molto avanti rispetto alla pianifica.

Programma di massima per la prossima giornata di lavoro