Diario di lavoro

|  |  |
| --- | --- |
| Luogo | Canobbio |
| Data | 20.09.2019 |

|  |
| --- |
| Lavori svolti |
| 13h15 – 14h45  Ho implementato la possibilità di pubblicare degli articoli all’interno del sito web.  Al momento è possibile caricare anche delle immagini. I controlli per contenuto e titolo possono considerarsi sicuri, mentre la chiamata per ricavare le immagini dei post è vulnerabile ad un attacco di tipo Directory Traversal.  La chiamata per la lettura delle immagini è la seguente:  <http://localhost/image/?file_name=FILE_NAME>  Mettendo al posto di FILE\_NAME per esempio il valore “../database.sql” è possibile sfruttare questa chiamata per leggere il file che si trova nella cartella codice/database.sql e stamparne il contenuto.    Figura 1 Esempio vulnerabilità  Questa vulnerabilità è pericolosa nonostante non si possa eseguire del codice remoto, questo perché è possibile caricare dei file html contenenti javascript vulnerabile per fare eseguire azioni all’utente involontariamente. Inoltre si può navigare completamente il sistema del server.    Figura 2 Secondo esempio  In questo secondo esempio si può notare come attraverso questa vulnerabilità si possa ricostruire l’intera struttura del progetto.  15h00 – 15h10  Ho risolto un problema grafico per i dispositivi mobile, ora le immagini hanno una larghezza massima come la larghezza della finestra, questo per prevenire che le foto sforino dallo schermo.  Vedi sezione problemi del diario.  15h10 – 16h20  Ho implementato la parte mancante del pannello di amministrazione, ora è possibile eliminare gli articoli.    Figura 3 Pannello amministrazione  16h20 – 16h30  Stesura diario. |

|  |
| --- |
| Problemi riscontrati e soluzioni adottate |
| Figura 4 Immagine con altezza fissa    Figura 5 Immagine con larghezza come la finestra  Ho risolto sostituendo la seguente proprietà: style="max-height: 300px;"  Con:  style="max-width: 100%;" |

|  |
| --- |
| Punto della situazione rispetto alla pianificazione |
| Mi trovo molto avanti rispetto alla pianficiazione preventiva. |

|  |
| --- |
| Programma di massima per la prossima giornata di lavoro |
| Rivedere il codice e valutare le vulnerabilità. |