



OUT OF BOUNDS

VERBALE DI RIUNIONE

2023/05/09

Redazione	Michele Cazzaro
Verifica	Edoardo Retis
Uso	Esterno
Destinatari	Out of Bounds prof. Tullio Vardanega prof. Riccardo Cardin Zucchetti S.p.A.

CONTATTI

sweoutofbounds@gmail.com

REPOSITORIES

[orgs/SWE-OutOfBounds/repositories](https://github.com/orgs/SWE-OutOfBounds/repositories)



Indice

1	Informazioni generali	2
2	Ordine del giorno	2
3	Resoconto	2

1 Informazioni generali

- Luogo: Stanza virtuale Zoom,
- Data: 2023/05/09,
- Orario di inizio: 15:30,
- Orario di fine: 16:15,
- Lista partecipanti:

Nome e Cognome	ruolo	presenza
Jacopo Angeli	Programmatore	<i>assente</i>
Simone Bisortole	Verificatore	<i>presente</i>
Valentina Caputo	Amministratrice	<i>assente</i>
Michele Cazzaro	Progettista	<i>presente</i>
Alberto Matterazzo	Responsabile	<i>presente</i>
Edoardo Retis	Programmatore	<i>presente</i>
Gregorio Piccoli	Rappr. Aziendale	<i>presente</i>

2 Ordine del giorno

- Aggiornare l'azienda sul lavoro svolto,
- Chiedere pareri sul lavoro svolto,
- Chiedere consigli su come stilare il rapporto sulla sicurezza del CAPTCHA prodotto,
- Chiedere un parere sulla gestione e trasmissione dei dati utente.

3 Resoconto

La riunione si è aperta con una presentazione dello stato attuale della libreria e della WebApp, con enfasi sugli aggiornamenti alla generazione del CAPTCHA, visualizzazione dei messaggi di errore e presentazione della homepage con articoli. Il Dott. Piccoli si mostra entusiasta del lavoro, ma concordiamo con lui quando ci fa notare che il livello di distorsione attualmente presente è troppo elevato; ci consiglia di modificare il colore di alcune linee di disturbo in modo da renderle discernibili dallo sfondo.

Non avendo una chiara idea di come muoverci, chiediamo consigli su come stilare il documento che attesta la sicurezza della libreria. Il Dott. Piccoli ci comunica che abbiamo molta flessibilità per quanto riguarda la struttura del documento e che non dobbiamo rispondere a particolari quesiti all'interno di esso. Il Dott. Piccoli ci consiglia diversi strumenti utili per controllare la sicurezza del codice da noi scritto, tra cui diversi forniti da [OWASP](#):

- [ZAPProxy](#),
- [ModSecurity CRS](#),



- [Top 10 vulnerabilities individuate da OWASP](#),
- [CVE Security Datasource](#),
- [Grype vulnerability scanner](#),
- [Syft BOMs generator](#).

Infine si cerca di capire se il lavoro svolto in merito alla gestione dei dati e la trasmissione al server degli stessi sia adeguata. Il Dott. Piccoli ci consiglia di utilizzare funzioni di hash con salt, mettendoci in guardia dalle tecnologie obsolete, tra cui MD5. Otteniamo inoltre una risposta in merito alla trasmissione aggregata di dati resolvendo alcuni dei dubbi che ci affliggevano.

La riunione in procinto di conclusione si è interrotta improvvisamente alle 16:10 a causa di un problema tecnico. È stata prontamente recuperata attraverso l'apertura di una nuova stanza che è stata tempestivamente comunicata per email al Dott. Piccoli.