



WAPT

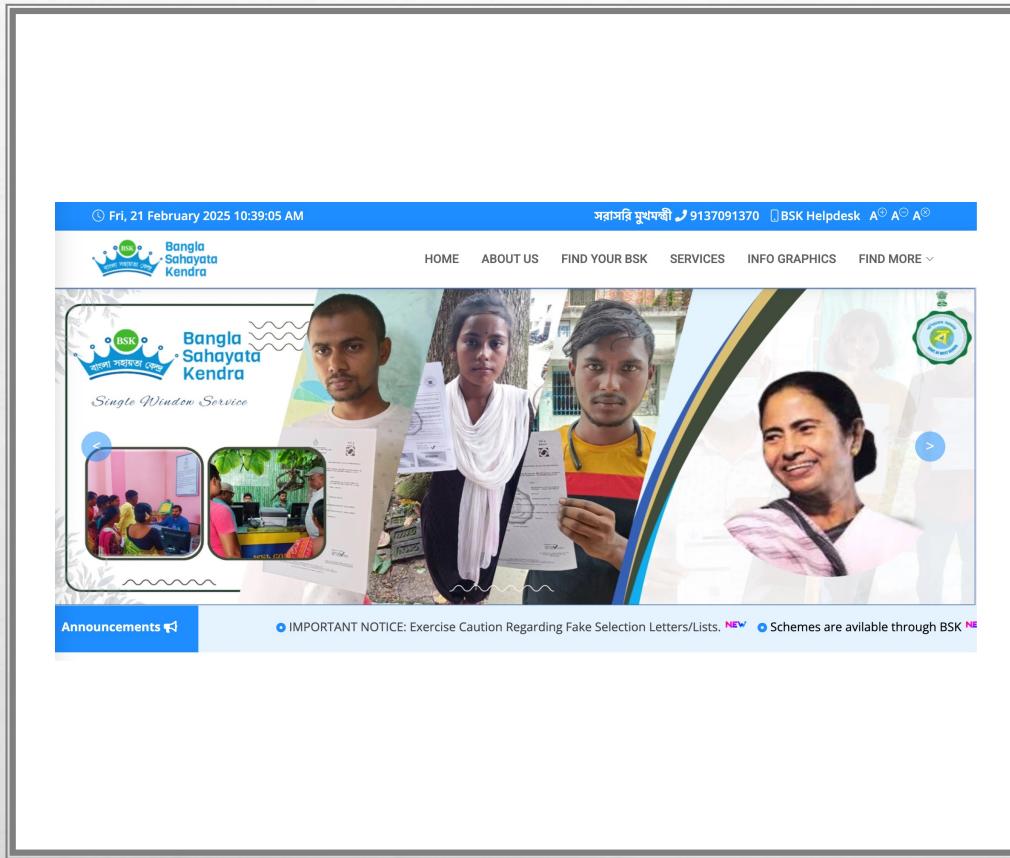
WEB APPLICATION

PENETRATION TESTING

STUDY CASE

IL CASO IN QUESTIONE

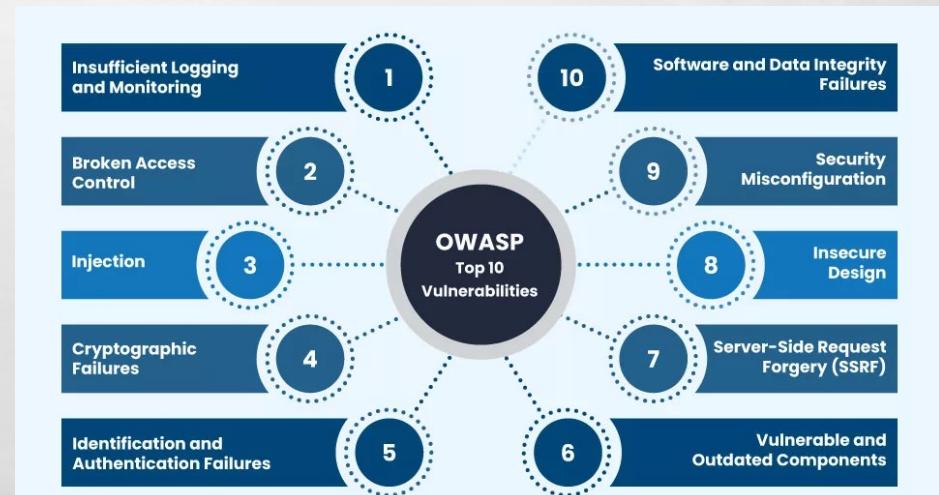
IL CASO ANALIZZATO PRENDE IN ESAME IL WAPT ESEGUITO DALL'AZIENDA PRIME INFOSERV ESEGUITO SUL SITO WEB [HTTPS://BSK.WB.GOV.IN/](https://bsk.wb.gov.in/), SITO ISTITUZIONALE DEL BANGLA SAHAYATA KENDRA.



IL WAPT, SI INCENTRA SULLA CATEGORIZZAZIONE DELLE VULNERABILITÀ (CONSULTABILI SUL SITO UFFICIALE [HTTPS://OWASP.ORG/WWW-PROJECT-TOP-TEN/](https://owasp.org/www-project-top-ten/)), OVVERO OPEN WEB APP SECURITY PROJECT. È UNA ORGANIZZAZIONE INTERNAZIONALE SENZA SCOPO DI LUCRO DEDICATA ALLA SICUREZZA DELLE APPLICAZIONI WEB. L'OWASP TOP 10 È UN REPORT, AGGIORNATO REGOLARMENTE, SULLE PIÙ COMUNI VULNERABILITÀ.



TOP 10



CWE TOP 25 Most Dangerous Software Errors

OLTRE CHE L'OWASP TOP 10, SI PRENDE IN ANALISI ANCHE IL CWE TOP 25, RIPORTANTE LA CLASSIFICA ANNUALE DEI PIÙ PERICOLOSI ERRORI CHE SI COMMETTONO NELLA PROGRAMMAZIONE DI UN SOFTWARE (DISPONIBILI AL SEGUENTE LINK: [HTTPS://WWW.SANS.ORG/TOP25-SOFTWARE-ERRORS/](https://www.sans.org/top25-software-errors/)), MANTENUTA DAL MITRE CORPORATION.



2023 CWE Top 25 Most Dangerous Software Weaknesses

Rank	ID	Name	Score	CVEs in KEV	Rank Change
1	CWE-787	Out-of-bounds Write	63.72	70	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.54	4	0
3	CWE-89	Improper Neutralization of Special Elements Used in an SQL Command ('SQL Injection')	34.27	6	0
4	CWE-416	Use After Free	16.71	44	3
5	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	15.65	23	1
6	CWE-20	Improper Input Validation	15.50	35	-2
7	CWE-125	Out-of-bounds Read	14.60	2	-2
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.11	16	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.73	0	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	10.41	5	0
11	CWE-862	Missing Authorization	6.90	0	5
12	CWE-476	NULL Pointer Dereference	6.59	0	-1
13	CWE-287	Improper Authentication	6.39	10	1
14	CWE-190	Integer Overflow or Wraparound	5.89	4	-1
15	CWE-502	Deserialization of Untrusted Data	5.56	14	-3
16	CWE-77	Improper Neutralization of Special Elements Used in a Command ('Command Injection')	4.95	4	1
17	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.75	7	2
18	CWE-798	Use of Hard-coded Credentials	4.57	2	-3
19	CWE-918	Server-Side Request Forgery (SSRF)	4.56	16	2
20	CWE-306	Missing Authentication for Critical Function	3.78	8	-2
21	CWE-362	Concurrent Execution using Shared Resources with Improper Synchronization ('Race Condition')	3.53	8	1
22	CWE-269	Improper Privilege Management	3.31	5	7
23	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.30	6	2
24	CWE-863	Incorrect Authorization	3.16	0	4
25	CWE-276	Incorrect Default Permissions	3.16	0	-5

DIFFERENZA TRA OWASP TOP 10 E CVE TOP 25

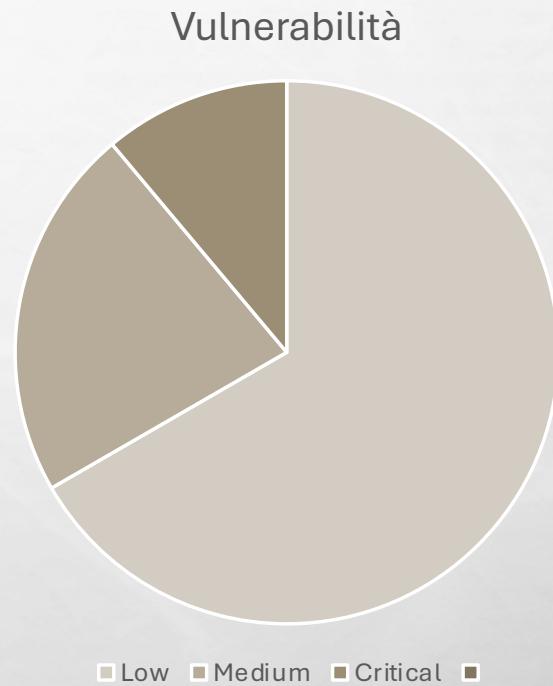
Caratteristica	OWASP TOP 10	CWE TOP 25
Focalizzazione	Sicurezza delle applicazioni web	Errori di programmazione in tutti i tipi di software
Origine dei dati	Basata su analisi di attacchi reali e valutazioni di esperti	Basata su dati statistici (NVD, CVE, exploit reali)
Ambito	Web applications	Software in generale (app, OS, embedded, web, etc.)
Organizzazione responsabile	OWASP (Open Web Application Security Project)	MITRE Corporation
Numero di vulnerabilità	10	25
Frequenza di aggiornamento	Circa ogni 3-4 anni	Annualmente

ANALISI DEI DATI A DISPOSIZIONE

- LE VULNERABILITÀ SI SUDDIVIDONO IN 5 CATEGORIE:
- LOW;
- MEDIUM;
- HIGH;
- CRITICAL;
- INFORMATIONAL.
-

QUELLE RISCONTRATE NEL CORSO DI QUESTO WAPT SONO 8, TRA CUI:

- 1 CRITICAL;
- 1 MEDIUM;
- 6 LOW.



LE VULNERABILITÀ RISCONTRATE:

Sl. No.	Vulnerability Name	Vulnerability Risk Type	Revalidation Status
1	Out-of-date Version (Axios)	High	Fixed
2	Internal Server Error Leading to Information Disclosure	Medium	Fixed
3	Content Security Policy (CSP) Not Implemented	Low	Fixed
4	HTTP Strict Transport Security (HSTS) Policy Not Enabled		Fixed
5	Version Disclosure (Axios)		Fixed
6	Version Disclosure (Bootstrapjs)		Fixed
7	Version Disclosure (Highcharts)		Fixed
8	Version Disclosure (jQuery)		Fixed



REMEDIATION AND CORRECTION

- OUT-OF-DATE VERSION:

È LA VULNERABILITÀ PIÙ CRITICA E CHE NECESSITA DI UNA CORREZZIONE IMMEDIATA.

RIENTRA IN:

- CWE TOP 25: CWE-1104 - USO DI LIBRERIE DI TERZE PARTI CON VULNERABILITÀ NOTE
- OWASP TOP 10 (2021): A06: VULNERABLE AND OUTDATED COMPONENTS

PIANO DI REMEDIATION:

- AGGIORNARE AXIOS ALL'ULTIMA VERSIONE DISPONIBILE.
- UTILIZZARE STRUMENTI COME **DEPENDABOT** O **SNYK** PER MONITORARE LE VULNERABILITÀ NELLE DIPENDENZE.
- RIMUOVERE LIBRERIE INUTILIZZATE O NON MANTENUTE.

REMEDIATION AND CORRECTION

- INTERNAL SERVER ERROR LEADING TO INFORMATION DISCLOSURE:

TIPOLOGIA DI VULNERABILITÀ: ESPOSIZIONE DI INFORMAZIONI SENSIBILI

RIENTRA IN:

- **CWE TOP 25: CWE-209** - ESPOSIZIONE DI INFORMAZIONI SENSIBILI TRAMITE MESSAGGI D'ERRORE;
- **OWASP TOP 10 (2021): A01: BROKEN ACCESS CONTROL** (SE FORNISCE ACCESSO NON AUTORIZZATO AI DATI).

REMEDIATION:

- DISABILITARE LA VISUALIZZAZIONE DEGLI ERRORI IN - PRODUZIONE.
- IMPLEMENTARE UNA GESTIONE CENTRALIZZATA DEI LOG.
- EVITARE MESSAGGI D'ERRORE DETAGLIATI PER L'UTENTE.

REMEDIATION AND CORRECTION

- **CONTENT SECURITY POLICY (CSP) NOT IMPLEMENTED:**

TIPOLOGIA DI VULNERABILITÀ: MANCATA PROTEZIONE CONTRO CROSS-SITE SCRIPTING (XSS)

RIENTRA IN:

- CWE TOP 25: CWE-79 - CROSS-SITE SCRIPTING (XSS)
- OWASP TOP 10 (2021): A03: INJECTION (XSS)

PIANO DI REMEDIATION:

- IMPLEMENTARE UNA CONTENT SECURITY POLICY (CSP) PER LIMITARE L'ESECUZIONE DI SCRIPT.
- EVITARE L'USO DI EVAL() E SCRIPT INLINE.
- TESTARE LA POLICY CON STRUMENTI COME GOOGLE CSP EVALUATOR

REMEDIATION AND CORRECTION

- **HTTP STRICT TRANSPORT SECURITY (HSTS) POLICY NOT ENABLED:**

TIPOLOGIA DI VULNERABILITÀ: MAN-IN-THE-MIDDLE (MITM) & DOWNGRADE ATTACK

RIENTRA IN:

- CWE TOP 25: CWE-319 - TRASMISSIONE DI DATI SENSIBILI SENZA CRITTOGRAFIA
- OWASP TOP 10 (2021): A07: IDENTIFICATION AND AUTHENTICATION FAILURES

PIANO DI REMEDIATION:

- ABILITARE HSTS CON L'HEADER HTTP:HTTP
STRICT-TRANSPORT-SECURITY: MAX-AGE=31536000;
INCLUDESUBDOMAINS; PRELOAD
- FORZARE HTTPS CON UN REDIRECT LATO SERVER.
- TESTARE L'IMPLEMENTAZIONE CON [HSTS PRELOAD LIST](#).

REMEDIATION AND CORRECTION

- **VERSION DISCLOSURE (AXIOS):**

TIPOLOGIA DI VULNERABILITÀ: ESPOSIZIONE DI INFORMAZIONI SULLE
TECNOLOGIE UTILIZZATE
RIENTRA IN:

- CWE TOP 25: CWE-200 - ESPOSIZIONE DI INFORMAZIONI SENSIBILI
- OWASP TOP 10 (2021): A06: VULNERABLE AND OUTDATED COMPONENTS

PIANO DI REMEDIATION:

- RIMUOVERE LE INTESTAZIONI DELLE VERSIONI DAL SERVER.
- OFFUSCARE LE INFORMAZIONI SULLE TECNOLOGIE USATE.
- USARE UNA BUILD MINIMIZZATA PER RIDURRE L'ESPOSIZIONE DELLE LIBRERIE FRONT-END.

REMEDIATION AND CORRECTION

- **VERSION DISCLOSURE (BOOTSTRAPJS)**

TIPOLOGIA DI VULNERABILITÀ: ESPOSIZIONE DI INFORMAZIONI SULLE LIBRERIE
RIENTRA IN:

- CWE TOP 25: CWE-200 - ESPOSIZIONE DI INFORMAZIONI SENSIBILI
- OWASP TOP 10 (2021): A06: VULNERABLE AND OUTDATED COMPONENTS

PIANO DI REMEDIATION:

- AGGIORNARE BOOTSTRAPJS ALL'ULTIMA VERSIONE DISPONIBILE.
- OFFUSCARE LA VERSIONE NEI FILE JAVASCRIPT E NEI METADATI.
- EVITARE CDN CHE ESPONGANO LA VERSIONE NELLE URL.

REMEDIATION AND CORRECTION

- **VERSION DISCLOSURE (HIGHCHARTS)**

TIPOLOGIA DI VULNERABILITÀ: ESPOSIZIONE DI INFORMAZIONI SULLE TECNOLOGIE UTILIZZATE

RIENTRA IN:

- CWE TOP 25: CWE-200 - ESPOSIZIONE DI INFORMAZIONI SENSIBILI
- OWASP TOP 10 (2021): A06: VULNERABLE AND OUTDATED COMPONENTS

PIANO DI REMEDIATION:

- AGGIORNARE HIGHCHARTS E MINIMIZZARE IL CODICE DISTRIBUITO.
- EVITARE RIFERIMENTI DIRETTI ALLE VERSIONI NEI FILE PUBBLICI.
- MONITORARE VULNERABILITÀ CON STRUMENTI COME OWASP DEPENDENCY-CHECK.

REMEDIATION AND CORRECTION

VERSION DISCLOSURE (JQUERY)

TIPOLOGIA DI VULNERABILITÀ: USO DI VERSIONI OBSOLETE CON

VULNERABILITÀ NOTE

RIENTRA IN:

- [CWE TOP 25: CWE-200](#) - ESPOSIZIONE DI INFORMAZIONI SENSIBILI
- [OWASP TOP 10 \(2021\): A06](#): VULNERABLE AND OUTDATED COMPONENTS

PIANO DI REMEDIATION:

- AGGIORNARE JQUERY ALLA VERSIONE PIÙ RECENTE.
- EVITARE RIFERIMENTI DIRETTI ALLE VERSIONI NEI FILE PUBBLICI.
- USARE UN CONTENT SECURITY POLICY (CSP) PER PREVENIRE EXPLOIT DI XSS.

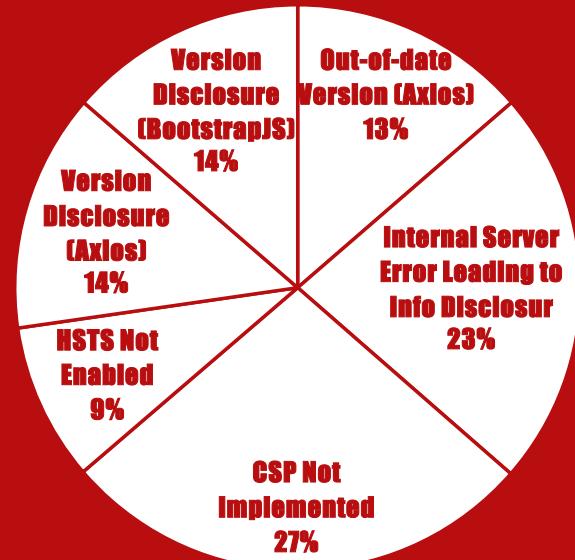
Vulnerabilità	Costo stimato (€)	Motivazione
Out-of-date Version (Axios)	1.000 - 3.000	Aggiornamento, test di compatibilità e revisione delle dipendenze
Internal Server Error Leading to Info Disclosure	2.000 - 5.000	Implementazione di gestione errori, logging sicuro, test di penetrazione
CSP Not Implemented	2.500 - 6.000	Analisi delle policy, configurazione e test di XSS
HSTS Not Enabled	500 - 2.000	Configurazione dell'header e test HTTPS
Version Disclosure (Axios)	1.000 - 3.000	Rimozione informazioni di versione, offuscamento
Version Disclosure (BootstrapJS)	1.000 - 3.000	Aggiornamento libreria, test compatibilità
Version Disclosure (Highcharts)	1.000 - 3.000	Offuscamento versione, minimizzazione codice

***I COSTI SONO DA INTENDERSI PER PERSONALE GIÀ FORMATO.**

STIMA DEI COSTI DELLA REMEDIATION



COSTO STIMATO



Costo totale: 10.500 € e 29.000



COSTI DELLA REMEDIATION



RACCOMANDAZIONI:

- SEGNALARE EVENTUALI INCIDENTI ALLE FIGURE PREPOSTE E NEI TEMPI PREPOSTI:

IL [D.L. 105/2019](#) (CONV. CON MODIFICHE DALLA L. 133/2019), APPROVATO IN CONDIZIONI DI STRAORDINARIA NECESSITÀ E URGENZA PROVOCATE DA ATTACCHI CHE AVEVANO INTERESSATO LE RETI DI DIVERSI PAESI EUROPEI, HA ISTITUITO IL CD. “PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA” E IMPONE **OBBLIGHI DI NOTIFICA** DEGLI “INCIDENTI AVVENTI IMPATTO SU RETI, SISTEMI INFORMATIVI E SERVIZI INFORMATICI” IN CAPO A ENTI PUBBLICI E PRIVATI NAZIONALI LA CUI OPERATIVITÀ, CORRELANDOSI A **FUNZIONI E SERVIZI ESSENZIALI** PER LO STATO, IMPATTA SULLA “SICUREZZA NAZIONALE” (ART. 1, COMMI 1 E 3, D.L. 105/2019).

- LA PROCEDURA IDEATA PER LA SEGNALAZIONE COINVOLGE UNA MOLTEPLICITÀ DI SOGGETTI, GLI ENTI SOPRA INDIVIDUATI DEVONO, INFATTI, COMUNICARE L'INCIDENTE AL COMPUTER SECURITY INCIDENT RESPONSE TEAM – CSIRT (IN ITALIA ISTITUITO PRESSO L'AGENZIA PER LA CYBERSICUREZZA NAZIONALE ACN), ESSO, A SUA VOLTA, INOLTRERÀ TEMPESTIVAMENTE LA NOTIZIA AL DIPARTIMENTO DELLE INFORMAZIONI PER LA SICUREZZA IL QUALE ASSICURA POI LA TRASMISSIONE DELLE NOTIFICHE RICEVUTE ALL'ORGANO DEL MINISTERO DELL'INTERNO PER LA SICUREZZA E LA REGOLARITÀ DEI SERVIZI DI TELECOMUNICAZIONE NONCHÉ ALLA PRESIDENZA DEL CONSIGLIO DEI MINISTRI (SE PROVENIENTI DA UN SOGGETTO PUBBLICO O DA UN SOGGETTO DI CUI ALL'ART. 29 [D.LGS. 82/2005](#)) OVVERO AL MINISTERO DELLO SVILUPPO ECONOMICO (SE EFFETTUATE DA UN SOGGETTO PRIVATO).

STANDO AL TESTO DEL DECRETO N. 105/2009 IL MANCATO ADEMPIMENTO DEI DOVERI DI COMUNICAZIONE È PUNITO, SALVO CHE IL FATTO NON COSTITUISCA REATO, CON LA SANZIONE AMMINISTRATIVA PECUNIARIA DA 250.000 EURO A 1.500.000 EURO (ART. 1, COMMA 9, D.L. 105/2019).

AL DECRETO LEGGE È STATA DATA ATTUAZIONE CON DIVERSI ATTI NORMATIVI SECONDARI, IN PARTICOLARE È IL [DPCM N. 81/2021](#) A REGOLAMENTARE LE NOTIFICHE DEGLI INCIDENTI PO' ANZI MENZIONATI, DEFINENDO, IN PARTICOLARE, LA “TASSONOMIA DEGLI INCIDENTI” SUDDIVISI PER CLASSE DI GRAVITÀ (ART. 2), LA PROCEDURA DI INOLTRO DELLE SEGNALAZIONI (ART. 5), LE MISURE TECNICHE DI SICUREZZA DA ADOTTARE IN CASO DI INCIDENTE (ARTT. 8 SS.).

FONTE: [HTTPS://WWW.COMPLIANCEHUB.IT/2024/03/14/INCIDENTI-INFORMATICI-CYBER-ATTACK-OBBLIGHI-DI-SEGNALAZIONE-MEGI-TRASHAJ/](https://www.compliancehub.it/2024/03/14/incidenti-informatici-cyber-attack-obblighi-di-segnalazione-megi-trashaj/)



RACCOMANDAZIONI:

EVITARE DI PUBBLICARE APPLICAZIONI CON VULNERABILITÀ

