

Advanced White-box



```
private void updateWidget(Context context) {
    JodaTimeAndroid.init(context);
    SettingsManager sm = new SettingsManager(context);
    RemoteViews remoteViews = new RemoteViews(context, getResources().
// showing dark style if it is
boolean isDark = sm.loadWidgetSetting("dark");
if (isDark) remoteViews = new RemoteViews(context, getResources().
// Register an onClickListener
Intent main = new Intent(context, MainActivity.class);
main.setAction(CALL_FROM_WIDGET);
main.setAction(Long.toString(System.currentTimeMillis()));
//
long mId = sm.loadWidgetSetting("id");
if (mId > 0) {
    long metricId = sm.loadWidgetSetting("metric");
    if (metricId > 0) {
        main.putExtra("metric_id", metricId);
        Log.i(this.getClass().getSimpleName(), "Metric ID: " + metricId);
        PendingIntent pendingIntent = PendingIntent.getActivity(context, 0,
        remoteViews.setClickListener(mId, pendingIntent));
    }
}
appWidgetManager.updateAppWidget(mId, remoteViews);
}
```

AEC

Prověřte zabezpečení vyvíjených aplikací

Advanced white-box je produkt kombinující penetrační testy a secure code review, případně další assessment služby. Cílem advanced white-box je komplexní prověření bezpečnosti vyvíjených aplikací za pomoci simulace hackerských útoků, automatizované analýzy kódu, manuálních revizí kódu a auditů. Výhodou služby je spojení sil expertů v několika bezpečnostních disciplínách, které vede k maximalizaci užítka z provedených analýz a odhalení většího množství zranitelností, a to včetně detekce skrytých hrozeb a potenciálně slabých míst v auditované aplikaci. Výsledná zpráva z advanced white-box testů obsahuje popis zranitelností s konkrétními doporučeními k jejich nápravě, jež jsou stavěny na míru použitým technologiím.



www.aec.cz

Advanced White-box tvoří:

■ Penetrační testy

Penetrační testy jsou prováděny jako simulace hackerských útoků na síťové i aplikační úrovni prověří schopnost systémů organizace odolávat reálným kybernetickým útokům z vnějšího prostředí, ale také schopnost odolat neautorizovaným zásahům zaměstnanců, a to bez ohledu na to, jestli jednájí vědomě, nebo se pouze dopustí chyby.

■ Secure code review

Bezpečnostní revize zdrojových kódů spočívá v kontrole zdrojových kódů aplikací, a to formou manuálních revizí zdrojového kódu a automatizovaných analýz pomocí SAST nástrojů.

Penetrační testy

- Jsou simulací hackerských útoků na aplikace, systémy i celou infrastrukturu.
- Využívání globálně uznávaných metodik jako je OWASP Web Security Testing Guide (WSTG) či Penetration Testing Standard (PTES).
- Penetrační testy provádí certifikovaní penetrační testeři podle požadovaných standardů.
- Prověřování bezpečnosti manuálními testy v kombinaci s pokročilými komerčními automatizovanými skenovacími nástroji, ale také vlastními nástroji z portfolia AEC toolkit.
- Výsledkem penetračních testů je detekce zranitelností, konfiguračních nedostatků případně odhalení poddimenzovaných prvků systému na všech vrstvách testované aplikace nebo systému.

Code review

- Revize aplikací v mnoha populárních jazycích (Java, C#, PHP, ...).
- Interní metodologie založená na zkušenostech z bezpečného vývoje i penetračních testů, opírající se o uznávané standardy projektu OWASP.
- Umožňuje odhalit vývojářské chyby, backdoory, chyby v návrhu, nedodržování best practices, použití slabé kryptografie a mnoho dalších zranitelných míst v aplikaci.
- Code review se skládá ze dvou hlavních analyzačních částí:
 - Automatizovaná revize celého kódu pomocí open-source i proprietárních nástrojů a prověření výsledků bezpečnostním specialistou.
 - Manuální revize celého kódu, či jeho dílčích částí vybraných klientem či bezpečnostním specialistou.
- Nalezené zranitelnosti jsou podrobně popsány a jsou k nim na míru poskytnuta doporučení, která berou v potaz použitý technologický stack.

Naše přednosti

- Patříme mezi zavedené české security firmy, na trhu úspěšně působíme již déle než 30 let.
- Nasloucháme klientům a přizpůsobujeme služby jejich potřebám a časovým možnostem.
- Náš tým tvoří specialisté s bohatými zkušenostmi z oblasti vývoje i etického hackingu.
- Sledujeme moderní trendy v oblasti vývoje, bezpečnosti a technologií.
- Kombinujeme provádění penetračních testů, automatizovaných analýz zdrojových kódů, manuálních revizí a auditů pro odhalení široké škály zranitelností.
- Výsledné zprávy z prováděných testů obsahují podrobné popisy nalezených zranitelností a konkrétní doporučení k jejich nápravě šitými na míru použitým technologiím.
- Stavíme své služby na mnohaletých zkušenostech a léty prověřených standardech.