Insufficient Transport Layer Protection

Süüdlane

Keegi kellel on võimekus jälgida võrguliiklust. Või veebis asuva aplikatsiooni korral teab kuidas kasutajad sinna liga pääsevad.

Kuidas toimub rünne

Võrku jälgides kui kasutaja sisened site.

Turva nõrkus

SSL I vähene kasutamine või valesti confitud või aegunud certifikaadid.

Nõrkusid on lihtne avastada kuid peenemate nõrkste leidmiseks peab süvenema aplikatsiooni ja serveri confi .

Tagajärg

Võivad viia üksiku kasutaja info avalikuks tulemine kui , aga avalikustub admin konto info siis see võib viia kogu info kadumiseni.

Vältimine

1. Require SSL for all sensitive pages. Non-SSL requests to these pages should be redirected to the SSL page.
2. Set the ‘secure’ flag on all sensitive cookies.
3. Configure your SSL provider to only support strong (e.g., FIPS 140-2 compliant) algorithms.
4. Ensure your certificate is valid, not expired, not revoked, and matches all domains used by the site.
5. Backend and other connections should also use SSL or other encryption technologies.

Mitte kasutada ODBC(Open Database Connectivity)/JDBC (Java Standard Edition platform)

Näiteks :

Ründajad varastavad sessioni cooked ja saadavad need ise serverile ning võtavad sessioni üle.