HTTP Request Smuggling

Beschreibung

HTTP Request Smuggling basiert auf der Art und Weise, wie mehrere Webserver HTTP-Anfragen interpretieren und verarbeiten. Diese Schwachstelle besteht bei einer Verkettung von mehreren Webservern wie einem Front-End (z. B. Load Balancer oder Reverse Proxy), der die Anfragen an einen oder mehrere Backend-Server weiterleitet. Die Sicherheitslücke entsteht daher das innerhalb dieses Prozesses beide Server sich einig sein müssen, wie die Anfragen zu interpretieren sind, ist dies nicht der Fall kann ein Angreifer eine Anfrage erstellen, die von beiden Servern anders interpretiert wird und kann dadurch ein anderes Verhalten von dem back-End Server erzeugen als Front-End vorgesehen.

Impact

Die Auswirkungen dieser Schwachstelle sind vielseitig. Durch Manipulation der HTTP-Anfragen kann ein Angreifer Sicherheitsmechanismen wie Authentifizierung oder Autorisierung umgehen und dadurch Zugriff auf geschützte Funktionen erlangen. Des Weiteren ermöglicht diese Schwachstelle das Erlangen von anderen User Anfragen, die sensible Daten wie z. B. den Session-Cookie enthalten, was dazu führt, dass der Angreifer Zugang zu dem Useraccount erlangt. Die zwei oben genannten Beispiele sind nur einige von vielen weiteren Möglichkeiten, ein System oder Nutzerkonten zu kompromittieren oder an sensible Daten zu gelangen. Der Impact ist abhängig von dem spezifischen Anwendungsfall.

Mitigation

Es sollte sichergestellt werden, dass HTTP/2 end-to-end für die gesamte Kommunikation verwendet wird, sowie dass HTTP-Downgrading deaktiviert ist. Des Weiteren sollte der Front-End-Server mehrdeutige Anfragen normalisieren, und der Back-End-Server sollte mehrdeutige Anfragen ablehnen.

Referenzen

- https://portswigger.net/web-security/request-smuggling
- https://www.imperva.com/learn/application-security/http-request-smuggling/
- https://book.hacktricks.xyz/pentesting-web/http-request-smuggling