## Úvod do počítačovej bezpečnosti - zadanie 0

### Filip Kadúch

### Nájdené zraniteľnosti: 12

### Povolný telnet protokol na serveri

Pretože protokol neposkytuje žiadne vstavané bezpečnostné opatrenia, trpí vážnymi problémami so zabezpečením, ktoré obmedzili jeho použiteľnosť v prostrediach, kde sieti nemožno úplne dôverovať. Malo by sa zabrániť používaniu Telnetu na verejnom internete, pretože existuje riziko odpočúvania.

### SendMail 8.13.5

Miestny alebo vzdialený neprivilegovaný používateľ môže byť schopný vykonať ľubovoľný kód so zvýšenými oprávneniami alebo spôsobiť stav odmietnutia služby kvôli chybe zabezpečenia SendMail zahŕňajúceho spracovanie signálu. Dokázali sme skrze túto zraniteľnosť získať užitočné informácie z API response.

### Webalizer 2.01-09

Tieto verzie Webalizeru sú zraniteľné na Cross Site Scripting (XSS).

### MD5

MD5 je považovaný za slabý hašovací algoritmus. Útočník môže ľahko použiť kolíziu MD5 na falšovanie platných digitálnych certifikátov.

### robots.txt

Robots.txt by sa nemal používať ako prostriedok na skrytie svojich webových stránok pred výsledkami vyhľadávania Google. Dôvodom je, že na vašu stránku môžu smerovať iné stránky a vaša stránka sa tak môže indexovať, čím sa vyhnete súboru robots.txt.

### Chýbajúci API token pre autentifikáciu requestov

Tento nedostatok spôsobil že som mohol posielať requesty bez žiadnej verifikácie na základe priradenia k účtu.

### Chýbajúci fixLogin na strane backendu

Tejto chybe by sa zabránilo zavedenímAPI tokenu ale v tomto stave je dobrá prax testovať SQL injection aj na strane backendu aby sa predišlo príkazu ‘ test.

### Prebytočný error reporting zo strany backendu

Nie je potrebné vracať error “select user\_id from user where user\_name = '' or 1='1'

AND user\_pass = md5('' or 1='1')” na frontend v produkčne verziíj aplikácií. Táto informácia nám pomohla zistiť ako by mal vyzerať SQL injected kód.

### Ukladanie user\_id v cookie

Ukladanie ID užívateľa do súboru cookie a autentifikácia používateľa iba na týchto informáciách je zlý nápad, pretože ID užívateľa generujete postupne, takže je veľmi ľahké uhádnuť, čo útočníkovi umožní odcudziť identitu iného používateľa.

### Neupravovanie pri skladaní URL

Táto zraniteľnosť by sa mala riešiť odstránením z adresy URL čokoľvek, čo je mimo bežných znakov. A týmby sa do istej miery zabránilo cross site scrtiptingu. Tieto chyby zabezpečenia umožňujú útočníkom manipulovať so zobrazovaním stránok.

### File include

Túto chybu zabezpečenia sme použili na odhalenie citlivých údajov v súbore httpasswd. Pre ošetrenie tejto zraniteľnosti je dobré zaviesťpole s „povolenými“ stránkami ktorá nedovolí ťahať informácie z nechcených súborov.

### Možnosť ukradnúť SSH private key

V rámci tejto zraniteľnosti nám pomohli chyby v konfigurácií serveru kedy umožňovali jednému používateľovi prehliadať stránky iného používateľa a jeho domovský adresár. Takto sme sa dostali k informácií o lokalite ssh klúča. Taktiež povolenie kľúča bez prístupovej frázy je závislé na tom, aby sa k nemu nikto iný nedostal. Čo je v našom prípade problém.

### 

### 