Zadanie 8
I-UPB: Úvod do počítačovej bezpečnosti

December 6, 2021

1 Úvod

Cieľom zadanie je oboznámiť sa s OWASP Top 10 a demonštrovať všetkých 10 zraniteľností na poskytnutej virtuálke.

1.1 Zraniteľnosti

1.2 SQL injection

SQL injection je technika napadnutia aplikácie ktorá neošetruje žiadnym spôsobom formát dotazu ktorý posiela databázovému serveru. V tomto prípade aplikácia vstup do searchbaru na blogu nijak nespracováva a to nám dáva priestor pre vykonanie útoku SQL injection ktorej výsledok nám odhalí password hash používateľa.

```
" UNION SELECT ALL 1,concat(password,char(58)),3,4,5,6 from admins where name='student'--
```

1.3 Broken Authentication and Session Management

Keď sa z aplikácie odhlasujeme tak ako query parameter requestu je session ID ktoré sa dá zneužiť.

```
?page=logout.php&session_id=1bk5plh7re0cc2de07fr5h3m13&go_page=index.php
```

SessionID by malo byť vždy uschované ako tajomstvo.

1.4 XSS

Podobne ako pri SQL injection môžeme zneužiť neošetrený vstup, tento krát na strane klienta. Keď do vyhľadávania zadáme

```
<script>alert(document.cookie)</script>
```

tak dostaneme cookie čo by malo by+t znova uschované ako tajomstvo.

1.5 Insecure Direct Object References

Ďalšiu zraniteľnosťou ktorá je založená na neošetrenom vstupe je file inclusion. Pokiaľ sú v php nesprávne spracovávané importy tam zadaním nasledujúceho query parametra do URL získame heslá používateľov.

```
?page=../../../../../etc/passwd
```

1.6 Security Misconfiguration

Pokiaľ PHP aplikácia nepoužíva súbor. httaccess tak nám nič nebráni ku vykonaniu dir listing útoku. V tomto prípade ak do URL pridáme /images/ tak sa dostaneme ku zložke ku ktorej by sme inak prístup mať nemali.

2 Sensitive Data Exposure

Každá aplikácia do ktorej sa používateľ prihlasuje by mala používať na komunikáciu protokol HTTPS. V opačnom prípade dokážeme jednoducho odchytávať údaje odosielané serveru. Pri odytávaní HTTP komunikácie pomocou wireshark dokážeme zistiť aké prihlasovacie údaje používateľ odoslal (presne ako v zadaní 7).

2.1 Missing Function Level Access Control

Pokiaľ na strane servera nie je riadne ošetrená správa prihlasovania ktorá zamedzuje neprihláseným používateľom tak čítať obsah ktorý by videl prihlásený používateľ môže ktokoľvek. Po po pridaní nasledujúcej cesty do URL získame prístup ku článku ktorý by mal vidieť iba požívateľ prihlásený. /content/home.php?id=2

2.2 Cross-Site Request Forgery

Pokiaľ server neobsahuje kontrolu CRSF tokenov (a klient ich neodosiela) tak odoslaný formulár môže byť podvrhnutý útočníkom. Útočník môže do formulára zadať akékoľvek informácie ktoré môžu byť použité pre škodlivé účely.

2.3 Using Components with Known Vulnerabilities

Pokiaľ vývojár používa neaktuálne alebo ešte neoverené verzie webových frameworkov tak sa vystavuje riziku zneužitia zraniteľností týchto verzií.

2.4 Unvalidated Redirects and Forwards

Pokiaľ aplikácia neošetruje presmerovania na neznáme stránky tak môže byť náchylná na redirect útok ktorý môže používateľa presmerovať na doménu z ktorej môže byť vykonaný útok.