WAP – Dokumentácia k projektu č. 2

Výuková aplikácia demonštrujúca webové útoky

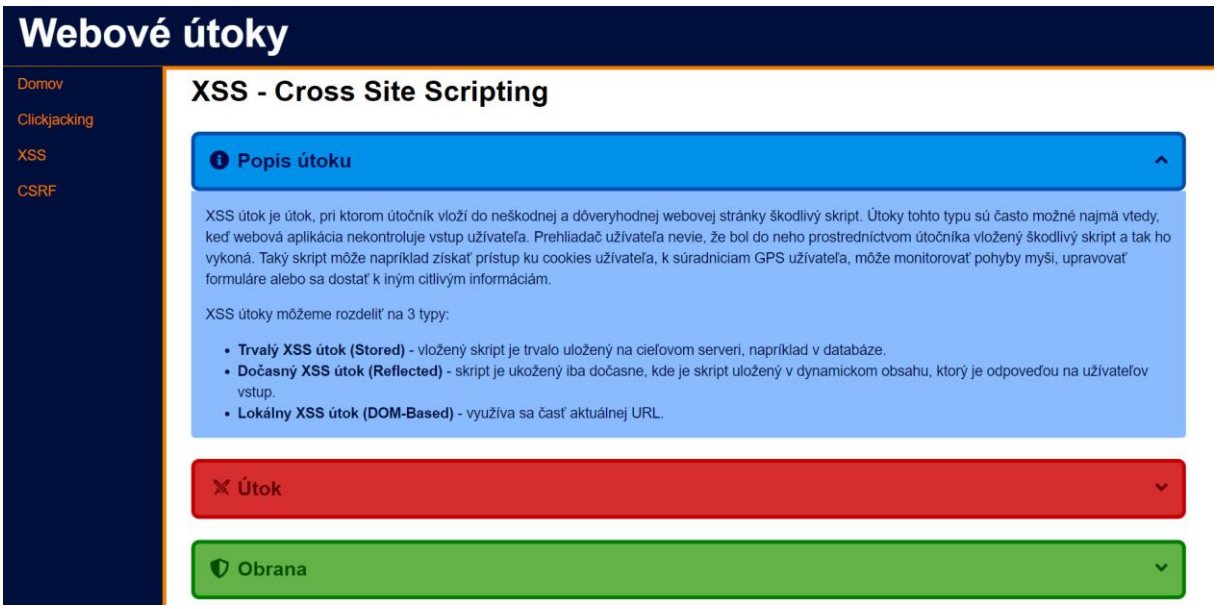
Ján Folenta (xfolen00)

25.4.2021

1 Popis aplikácie

Cieľom tejto webovej aplikácie je oboznámiť užívateľa s niektorými webovými útokmi, daný útok demonštrovať a popísať, ako sa proti takému útoku brániť.

V aplikácii sú implementované 3 útoky, a to Clickjacking, XSS (Cross Site Scripting) a CSRF (Cross Site Request Forgery). Možnosť výberu konkrétneho útoku má užívateľ v ľavom paneli aplikácie. Každý útok obsahuje krátky popis v sekcii Popis útoku, demonštráciu útoku v sekcii Útok a popis spolu s príkladom ako sa brániť proti danému útoku v sekcii Obrana. Vzhľad aplikácie je možné vidieť na obrázku nižšie.



Obr. 1: Vzhľad aplikácie demonštrujúcej webové útoky

Každý útok je iba demonštráciou, čo znamená, že užívateľovi nebude spôsobená žiadna škoda. Pre správnu demonštráciu útoku je potrebné dodržať jednotlivé kroky, ktoré sú uvedené v sekcii Útok. V rámci demonštrácie môže byť užívateľ presmerovaný na inú doménu, ktorá reprezentuje stránku útočníka, ale aj tá je úplne bezpečná a užívateľovi nehrozí žiadne riziko.

Aplikácia je voľne dostupná na adrese https://infinite-oasis-17402.herokuapp.com/.

2 Implementácia

Webová aplikácia je implementovaná v jazykoch Javascript, HTML a CSS a pre vytvorenie aplikácie bol použitý framework Express. Aplikácia je až na menšiu výnimku z dôvodu demonštrácie útoku

implementovaná vo forme Single Page Application, čo umožňuje rýchlu odozvu medzi jednotlivými úkonmi, keďže nie je nutné zakaždým komunikovať so serverom.

Implementácia serveru a jeho základná logika sa nachádza v súbore *app.js*. Základná stránka je implementovaná v súbore *app/index.html*, ktorého súčasťou je aj skript *app/public/js/index.js* implementujúci aplikačnú logiku aplikácie, pomocou ktorého je napríklad riadené presmerovanie medzi jednotlivými pohľadmi a podobne. Jednotlivé pohľady pre každý útok sú implementované v zložke *app/public/js/views*. CSS súbor, ktorý riadi celkový vzhľad aplikácie sa nachádza v súbore *app/public/css/index.css*. Demonštrácia CSRF útoku má vlastnú HTML stránku, vlastnú aplikačnú logiku aj vlastný CSS súbor. Nachádzajú sa v súboroch *app/login.html*, *app/public/js/login.js* a *app/public/css/login.css*.

V rámci demonštrácie webových útokov boli implementované aj jednoduché stránky útočníka, ktoré sú implementované v zložke *attackerWebsites* a sú uložené na študentskom webovom priestore serveru Eva. Prístupné sú na odkazoch http://www.stud.fit.vutbr.cz/~xfolen00/WAP/evilPage.html a http://www.stud.fit.vutbr.cz/~xfolen00/WAP/evilPage2.html.

2.1 Obranné mechanizmy

Obranné mechanizmy popísané v aplikácii, konkrétne v časti Príklad implementácie sekcie Obrana, sú tiež aj implementované a otestované, či zabraňujú daným útokom. Z dôvodu, aby bola možná demonštrácia útokov sú však tieto obranné mechanizmy v kóde zakomentované. Je ich možné nájsť v súbore *app.js* na riadkoch 8-24 a v súbore *app/index.js* na riadkoch 74-77.

3 Spustenie aplikácie

Po stiahnutí potrebných súborov je možné aplikáciu spustiť príkazom:

```
node app.js
```

Všetky potrebné balíčky sú súčasťou zdrojových súborov a preto nie je potrebné dotatočne inštalovať ďalšie balíčky. Aplikácia následne beží na porte 3000 a je k nej možné pristúpiť pomocou odkazu http://localhost:3000/. Pre stránky útočníka v súbore *attackerWebsites* je potrebný hosting.

Aby aplikácia mohla fungovať plnohodnotne, je potrebné upraviť domény v niekoľkých cestách, nachádzajúcich sa v zdrojových kódoch. Konkrétne sa jedná o:

- *app/public/js/views/Clickjacking.js* (riadok 23) – zmena domény na doménu, kde je uložená stránka útočníka *attackerWebsites /evilPage.html*
- *attackerWebsites /evilPage.html* (riadky 31 a 35) – zmena domény na doménu http://localhost:3000/, prípadne inú doménu, kde beží táto aplikácia
- *app/public/js/login.js* (riadok 28) – zmena domény na doménu, kde je uložená stránka útočníka *attackerWebsites /evilPage2.html*
- *attackerWebsites /evilPage2.html* (riadok 18) – zmena domény na doménu http://localhost:3000/, prípadne inú doménu, kde beží táto aplikácia