# SQL Injection - Přihlášení jako jiný uživatel

Na stránce login provedeme SQL injection. Do pole “Email” vložíme emailovou adresu oběti (kterou najdeme v komentářích u produktů) a za ní přidáme:’ --

Např: [jim@juice-sh.op](mailto:jim@juice-sh.op)’ --

Do pole “Password” vložíme cokoliv. Pokud nespecifikujeme emailovou adresu, ale doplníme SQL injection o „true“ podmínku, přihlásíme se za uživatele s ID 1, což je shodou okolností admin.

# XSS přes vyhledávání

Do pole vyhledávače vložíme JS script v iframe, např: <iframe src="javascript:alert(`message`)">

# CSRF – přejmenování uživatele skrze obrázek

Útok provedeme ve starším prohlížeči (FireFox 90.0). Nové prohlížeče by měli mít vůči tomuto útoku obranu díky bezpečnějšímu přístupu ke cookies. Oběť přesměrujeme odkazem na naši stránku, na které bude umístěn obrázek. Pokud na obrázek uživatel klikne, bude v OWASP Juice Shopu přejmenován.

Strukturu skriptu zjistíme z komunikace, která vzniká legitimním přejmenováním -> html formulář na html POST, …

Skript na přejmenování po kliknutí na obrázek:

<form action="http://localhost:3000/profile" method="POST">

<input name="username" value="You were RENAMED" type="hidden"/>

<button type="submit">

<img src="picture.jpg" />

</button>

</form>

Můžeme přidat i následující script pro automatické odeslání při načtení stránky, pokud bychom nechtěli čekat na uživatelovu akci.

<script>document.forms[0].submit();</script>

Pro získání achievementu v OWASP Juice Shopu je nutné přejmenování provést skrze <http://htmledit.squarefree.com/>

