- zagrożenia i zabezpieczanie

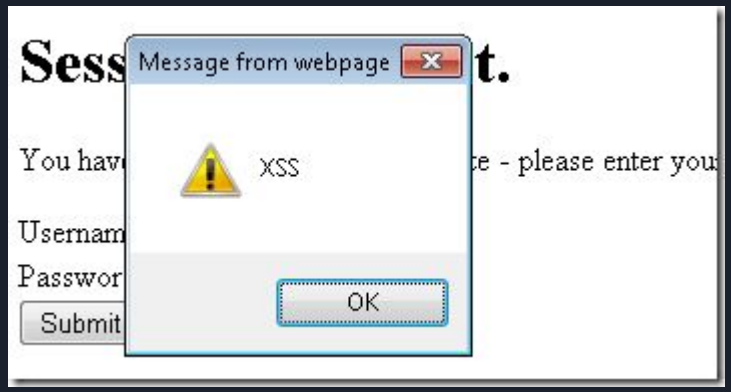
- Poznamy i na żywo przeprowadzimy ataki:
- XSS
- Spamming
- CSRF
- Wykonanie kodu zdalnego
- SQL Injection

- Jak się zabezpieczyć?

- Jak sprawdzić czy jestem bezpieczny?

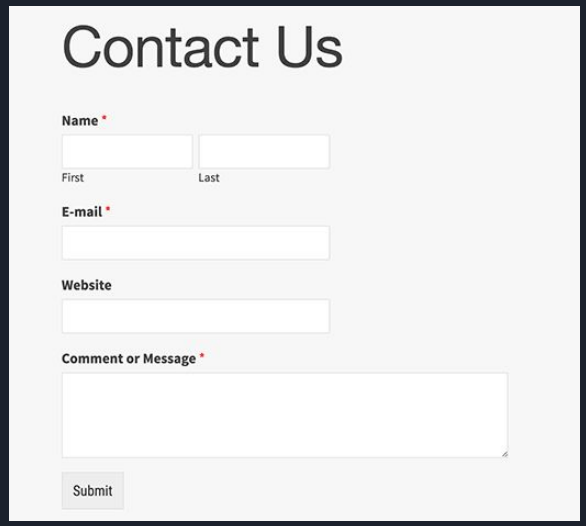
- Bardzo częsty atak
- Podatność często niesłusznie uznawana za mało istotną

- Bardzo niebezpieczny gdy jest przechowywany



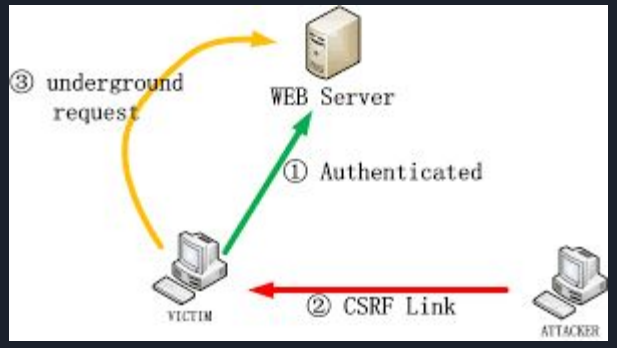
Użyjemy prawdziwej wtyczki z tą podatnością na prawdziwej instalacji WordPress. Znajdziemy błąd we wtyczce i wykorzystamy go do ataku na żywo.

- Częsty atak, głównie na małych stronach WordPressowych i nie tylko
- Pozwala osiągnąć "realne" zyski atakującemu - rozsyłając spam



Użyjemy prawdziwej wtyczki z tą podatnością na prawdziwej instalacji WordPress. Znajdziemy błąd we wtyczce i wykorzystamy go do ataku na żywo.

- Wykorzystuje socjotechniki podsyłając specjalne linki lub wyświetlając specjalne formularze
- Używany głównie żeby oszukać Administratora i zrobić coś do czego tylko on ma dostęp



Użyjemy prawdziwej wtyczki z tą podatnością na prawdziwej instalacji WordPress. Znajdziemy błąd we wtyczce i wykorzystamy go do ataku na żywo.

- Potężny atak, tak na prawdę w większości przypadków po jego przeprowadzeniu pozwala atakującemu na zrobienie... wszystkiego

- Polega na wykonaniu własnego dowolnego kodu (np. PHP) na serwerze instalacji

Użyjemy prawdziwej wtyczki z tą podatnością na prawdziwej instalacji WordPress. Znajdziemy błąd we wtyczce i wykorzystamy go do ataku na żywo.

- Bardzo niebezpieczny atak
- Pozwala na pobieranie danych z bazy, a często również ich modyfikację czy usunięcie

- Przy braku zabezpieczeń pozwala atakującemu zniszczyć całą stronę w kilka minut

Być bezpiecznym :)

Bezpieczeństwo w WordPress to długie i skomplikowane zagadnienie.

Przedstawił je świetnie Krzysztof Drozdz na swojej prezentacji "Mity (nie)bezpieczeństwa". Można ją obejrzeć tu:

bit.ly/2B1b1Md

Używając motyw lub wtyczkę:

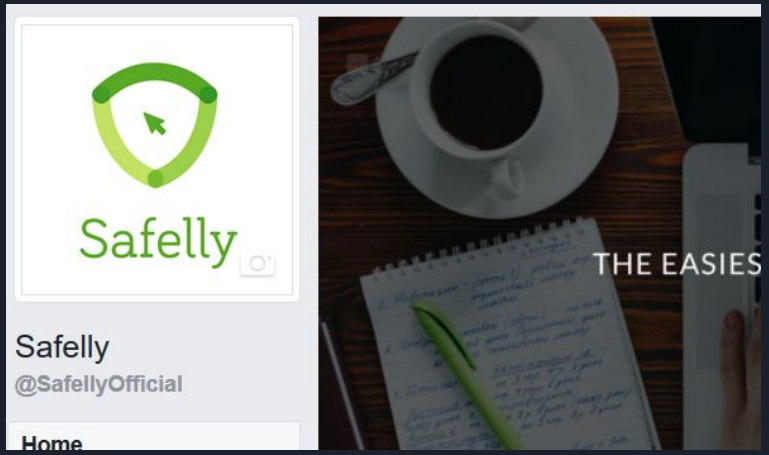
- Zwracaj uwagę na aktywność projektu. Na ilość przeszłych błędów i szybkość ich łatania.
- Sprawdzaj najnowsze podatności: np. na wpvulndb.com

- Pamiętaj, że zamknięty kod nie zawsze oznacza większe bezpieczeństwo!

Zapraszam na nasz fanpage Safelly.

Kiedy pojawiają się informacje o poważnych atakach na znane wtyczki lub motywy to piszemy o tym co konkretnie się stało i jak się zabezpieczyć.

fb.com/SafellyOfficial



- Co miesiąc odkrywanych jest kilkadziesiąt dziur w popularnych wtyczkach, motywach
- Zazwyczaj są szybko łatane przez twórców
- Pamiętaj o systematycznych aktualizacjach!
- Aktualizuj również samego WordPressa - tym bardziej gdy pojawia się aktualizacja bezpieczeństwa

- Jeżeli masz taką możliwość - włącz automatyczne aktualizacje bezpieczeństwa

- Upewnij się że masz regularnie wykonywaną kopię zapasową
- Nie każdy bakup jest dobry! Pamiętaj o tych rzeczach:
- Tworzona kopia powinna być łatwa w przeglądaniu i porównywaniu, żeby można było zlokalizować np. początek ataku i przywrócić czystą kopię
- Odzyskiwanie powinno być proste i szybkie w przypadku padnięcia całej strony

- Nie licz na kopię zapasową hostingu/serwera

- Bądź pewien, że jeżeli Twoja strona padnie lub zostanie podmieniona na co innego dowiesz się o tym pierwszy Ty, a nie Klient :)

Tworzymy Safelly, które ma zagwarantować spokój - aby właściciel mógł skupić się na biznesie.

Jeżeli strona czy e-sklep ulegnie jakiejkolwiek awarii to właściciel otrzymuje SMS i może szybko przywrócić działającą wersję.

Safelly

Istnieją skanery, które potrafią sprawdzić podatność danej strony na różne ataki.

Jednym z takich kombajnów jest OpenVAS, który pozwala szybko sprawdzić setki wektorów ataku.