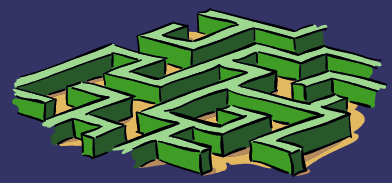
Cross- Site Request Forgery

Prezentace k přednášce o CSRF útocích

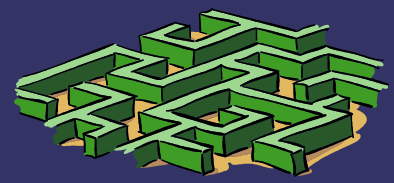
Připraveno pro SOOM session #4

2007



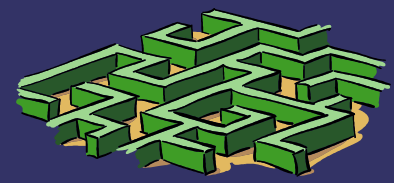
Cross- Site Request Forgery

- Jné označení této zranitelnosti
  - Cross- Site Request Forgery
  - CSRF
  - Cross- Site Reference Forgery
  - XSRF



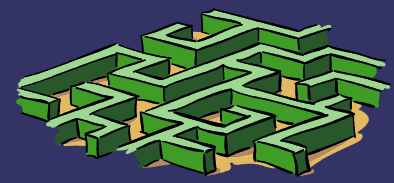
Cross- Site Request Forgery

- Historie CSRF (první zmínky)
  - 1988 Norm Hardy – označení Confused deputy
  - 2000 Bugtrag – zranitelnost na ZOPE
  - 2001 Bugtrag – poprvé použito označení CSRF u příspěvku “The Dangerous of Allowing Users to Post Images”



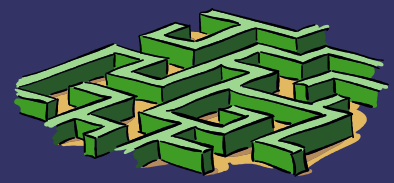
Cross- Site Request Forgery

- Cílem CSRF útoků jsou koncoví uživatelé
- Díky právům obětí je možné útočit na webové služby a aplikace
- Podle zranitelnosti webové aplikace může, ale také nemusí, být vyžadována spoluúčast oběti
- Podobnost s XSS



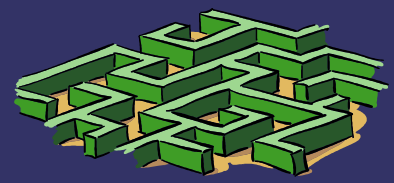
Cross- Site Request Forgery

- Jak servery kontrolují identitu uživatelů
  - Sessions
    - Cookies
    - Předávané parametry
    - Součást URL



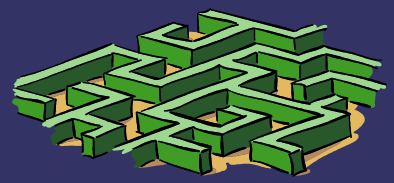
Cross- Site Request Forgery

- Popis zranitelnosti
  - Kam útočník nemůže
  - Nasměrování oběti
  - Využití oběti a provedení akce



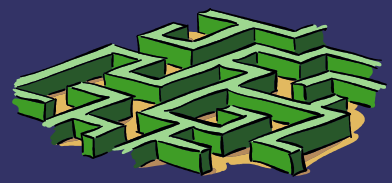
Cross- Site Request Forgery

- Použité metody
  - GET
  - POST



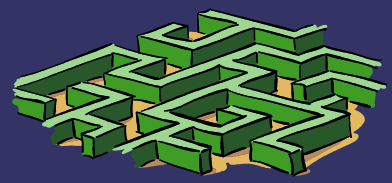
Cross- Site Request Forgery

- Utoky metodou GET
  - Cíle útoků
    - Hlasování v anketách
      - (http://www.anketa.cz/hlasuj.php?volba=2)
    - Volba funkčnosti
      - (http://www.aplikace.cz/index.php?akce=logout)



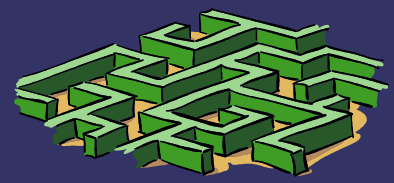
Cross- Site Request Forgery

- Utoky metodou GET
  - Popis útoku
    - Vložení vhodného odkazu
      - (http://www.anketa.cz/hlasuj.php?volba=2)
    - Maskování přesměrováním
      - (http://www.mojestranky.cz)
    - Využití odkazů na externí zdroje IMG, IFRAME...
      - <IMG SRC="http://www.anketa.cz/hlasuj.php?volba=2" width="0" height="0">



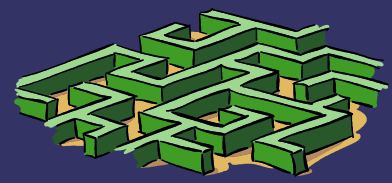
Cross- Site Request Forgery

- Utoky metodou POST
  - Cíle útoků
    - Vkládání příspěvků do diskuzí
    - Změny v nastavení uživatelských učtů
      - Změna přístupového hesla
      - Změna e- mailové adresy
      - Přidání adresy pro přesěrování příchozí pošty



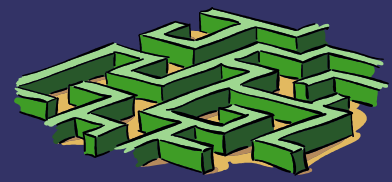
Cross- Site Request Forgery

- Utoky metodou POST
  - Popis útoku
    - Zjištění informací o formuláři, odesílaných datech a cílovém scriptu
      - Doplnek pro webový prohlížeč
      - Průzkum sítové komunikace
      - Průzkum zdrojového kodu stránky
    - Vytvoření kopie formuláře
    - Nalákání oběti
    - Odeslání dat z formuláře



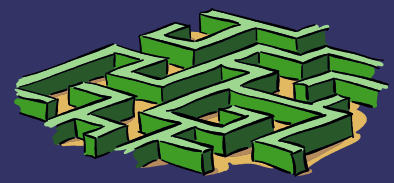
Cross- Site Request Forgery

- Utoky metodou POST
  - Nedostatky popsaného útoku a vylepšení
    - Viditelnost formuláře
      - Prvky typu hidden
    - Odeslání formuláře kliknutím na tlačítko
      - Automatické odeslání JavaScriptem
    - Zobrazení odpovědi od serveru
      - Vložení formuláře do skrytého rámu



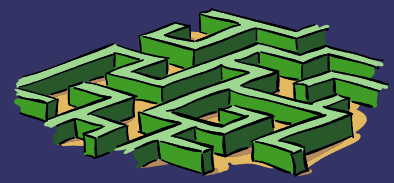
Cross- Site Request Forgery

- Napadení intranetu
  - Intranetové aplkace
  - Sítová zařízení ovládaná přes webové rozhraní
  - Změny v nastavení hraničních bodů mohou umožnit vstup útočníka do intranetu



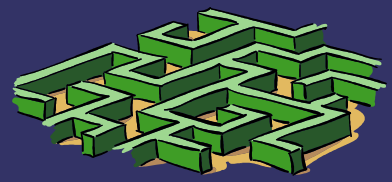
Cross- Site Request Forgery

- Další cíle CSRF útoků
  - Ovlivnění výsledků anket
  - Vkládání příspěvků do diskuzí
  - Nákupy v e- shopech
  - Přihazování v aukcích
  - Změny v nastavení uživatelského účtu
  - Krádež uživatelského účtu
  - S vyššími právy možnost nadadení aplikace
  - Utoky na webové aplikace v intranetu
  - Změny v nastavení FW, routerů, apd.



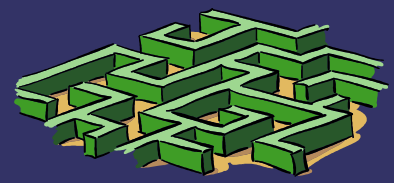
Cross- Site Request Forgery

- Odkud může útok přijít
  - Odkaz na webových stránkách
  - Vložení odkazu do jakéhokoliv dokumentu, flashe, apd...
  - E- maiem
    - E- mail ve formátu html
    - Vložení odkazu na externí zdroje (obrázek)
    - Vložení formuláře přímo zprávy
    - Automatické odeslání formuláře
    - IE - sdílení cookies s webovým prohlížečem



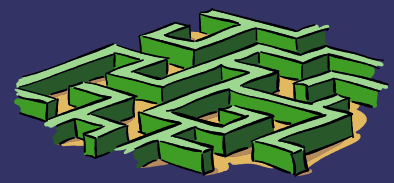
Cross- Site Request Forgery

- Elektroncké pasy
  - Nejznámější Microsoft Passport
  - Jednorázová registrace
  - Po přihlášení ke službě možnost navštěvovat všechny servery, které jsou partnerem, pod svou identitou.
  - Veliká hrozba a dopad CSRF útoků



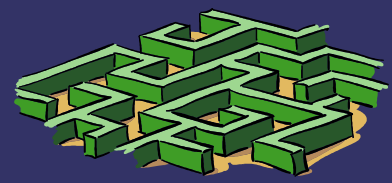
Cross- Site Request Forgery

- Standardní scénář útočníka při CSRF
  - Vytvoření účtu na napadeném serveru
  - Vyzkoušení veškerých akcí k odhalení chování aplikace
  - Hledání slabých míst, vkládání externích obrázků, XSS...
  - Výběr vhodné metody a provedení útoku



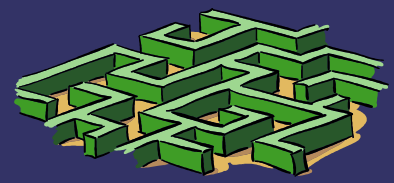
Cross- Site Request Forgery

- Obrana
  - Odhalení útoku uživatelem
  - Jak se může uživatel bránit
  - Odhalení útočníka správcem aplikace
  - Možnosti obrany na straně serveru
    - Zadávání hesla při akci
    - Hlavička referer
    - Proměnné URI
    - Skrytá pole
    - Metoda lístků



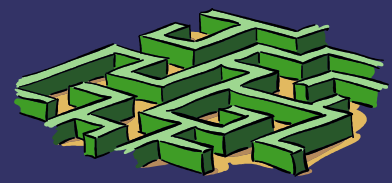
Cross- Site Request Forgery

- Obrana na straně uživatele
  - Odhalení útoku většinou pozdě
  - Paranoidní nastavení webového browseru
  - Paranoidní nastavení firewallu
  - Obrana prakticky neexistuje



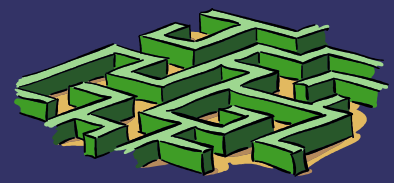
Cross- Site Request Forgery

- Vystopování útočníka
  - Ihned ze strany uživatele sledováním sí-tového provozu
  - Později pouze na straně serveru a to jen v případě, pokud jsou vedeny logy včetně položky referer



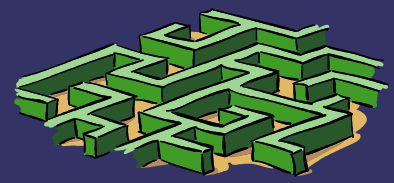
Cross- Site Request Forgery

- Obrana zadáváním hesla
  - Učinná metoda
  - Nemožnost použít při všech akcích
  - Při častém zadávání hesla otevírá nové možnosti pro jeho zcizení



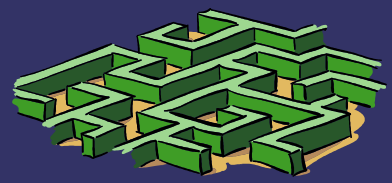
Cross- Site Request Forgery

- Kontrola položky referer
  - Učinná metoda
  - Filtrování refereru na straně klienta znemožní provedení legitimních požadavků
  - Výskyt exploitů na spoofing hlavičky referer



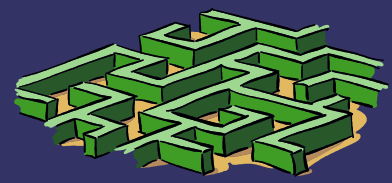
Cross- Site Request Forgery

- Ochrana použitím proměnného URI
  - http://www.web.cz/JK34ADE4H543/script.php
  - S dostatečně dlouhým a náhodným řetězcem bezpečná metoda
  - Nalezením zranitelnosti XSS prolomitelné



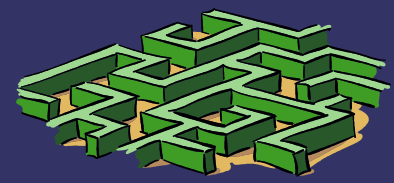
Cross- Site Request Forgery

- Obrana pomocí náhodného identifiká-toru ve skrytém poli
  - Na začátku sezení je vygenerován náhodný řetězec, který se předává ve skrytém poli do všech formulářů.
  - Bezpečné
  - Napadnutelné pomocí XSS



Cross- Site Request Forgery

- Obrana pomocí lístků
  - Náhodný řetězec vygenerován pro každou činnost
  - Každý lístek uložen do úložiště s popisem činnosti
  - Při provedení žádosti se ověřuje zda exstuje lístek
  - Velice bezpečné
  - Napadnutelné pomocí XSS



Cross- Site Request Forgery

- Obrana není jednoduchá
- Zranitelností CSRF trpí mnoho aplikací
- Konkrétní případy:
  - Seznam.cz
  - Volný.cz
  - A mnoho dalších