Hacking informačních kiosků

Subber

Co je informační kiosek ?

- Většinou veřejně přístupný počítač
- Určený pro pár specifických úloh
- Založený na
  - desktopovém Windows
  - Windows Embedded
  - specializované Linuxové distribuci

Co získáme hacknutím kiosku ?

- Přístup do vnitřní sítě
- Citlivá data uživatelů uložená v kiosku
- Hesla na server s databázemi
- Software z kiosku
- Dobrý pocit ;)

Kiosek PMDP

- Postavený na Windows Embedded
- Oficiálně nazýván „samoobslužná zóna“
- Možnost dobíjení kreditu Plzeňské karty a prodlužování časového jízdného
- Rezervace vstupenek do městských služeb
- Přístup na povolené webové stránky „veřejného internetu“

Kiosek PMDP

Prohlížeč pro „veřejný internet“

- FriendlyWay Secure Browser
- Nemožnost zadat URL adresu (není řádek)
- Vstup jen na povolené domény, jiný obsah blokován i v rámci stránek
- Lze načíst Flash a spouštět ActiveX
- Nelze instalovat ActiveX a spouštět Java Applety
- Externě zpracovávaný JavaScript se provede

XSS na povolené stránce

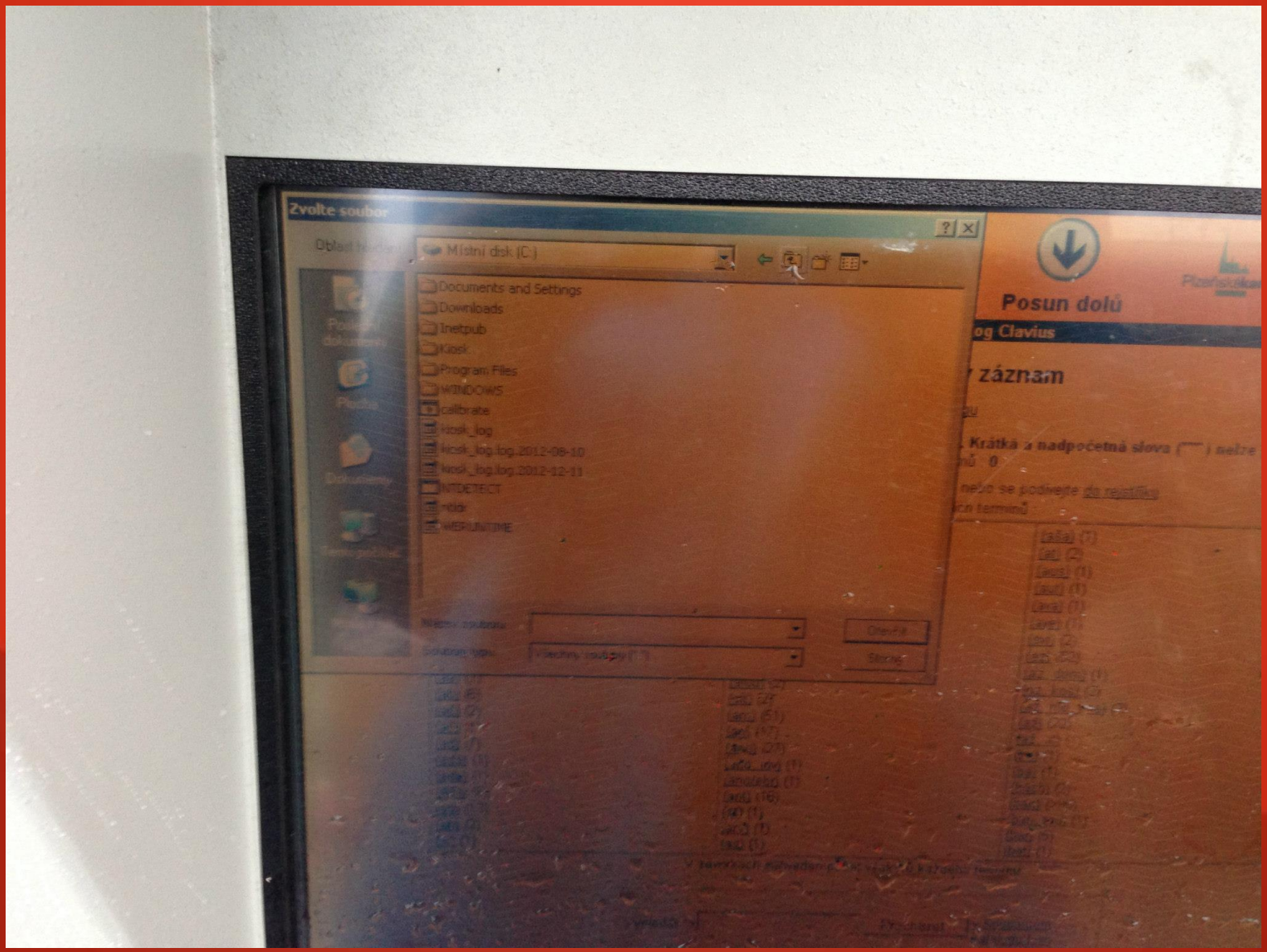
- XSS na stránce knihovny http://kmp.plzen-city.cz
- Možnost vložit vstupem z klávesnice

```
<input type=file></input>
```

a dostat se k souborům na kiosku

- Povolené stránky obsahují i jiné typy zranitelností (např. SQL inj.)

XSS na povolené stránce



Prvotní nápady

- Spustit interní program (prohlížeč, příkazový řádek, …) pomocí nasunutí vedlejšího souboru na něj
- Dotykový monitor podporuje pouze klik, nikoli drag & drop

Externí JavaScript

- Před objevením způsobu obcházení zákazu pomocí povoleného formátu URL
- Na serveru může být generován dynamicky
- Použitelný pro zjištění IP adresy kiosku,
  kterou může zaznamenat na serveru a případně i jako alert vrátit
- Možnost stejným způsobem zjistit user-agenta a tím na jakém jádře IE kiosek běží

Přístup na jiné stránky

- Jedna z povolených adres je http://*.plzen-city.cz
- Způsob napsání FriendlyWay Secure Browseru určuje, že URL adresa takto musí jen začínat
- Adresu http://k.plzen-city.cz.subber.cz nevyhodnocuje prohlížeč jako zakázanou stránku

Uploadování souborů

- Přechod přes XSS na stránce knihovny na vlastní stránku s uploaderem
- Nepohodlné uploadování souborů po jednom
- Hledání způsobu hromadného uploadu pomocí Flashe nebo spouštěného ActiveX

Co se v kiosku nachází ?

- Software kiosku a FriendlyWay SB
- Konfigurační soubory těchto programů
- Přístupové údaje k aktualizačnímu FTP serveru

Aktualizace kiosku

- Vždy při zvolení volby veřejný internet – spuštění FriendlyWay SB
- Připojení k aktualizačnímu FTP serveru
- FTP server na lokální síti
- Porovnání všech souborů
- Spuštění FriendlyWay SB

Aktualizační FTP server

- Dle konfigurace FriendlyWay Secure Browser slouží zároveň jako webserver pro homepage kiosku a proxy server
- Načtením webové stránky z kiosku zjištěna jeho vnější IP adresa 193.86.190.232
- Z internetu je dostupná pouze webová konfigurace Cisco SSL VPN Service pomocí HTTPS (s neplatným certifikátem)

Případné další možnosti

- Hromadný upload celého obsahu kiosku pomocí Flashe
- Připojení se pomocí Flashe na aktualizační FTP vnitřní sítí přímo z kiosku
- Úprava obsahu FriendlyWay Secure Browser
- Provedení aktualizace znovuspuštěním
- Upravený software ze serveru stáhne údaje o všech uživatelích Plzeňské Karty (skoro všech plzeňácích)

Dotazy

?