Csodapókok hálójában

Webes sérülékenységek
a világhálón túl

SILENT SIGNAL
VÉSZJELZÉS HELYETT...

WWW.SILENTSIGNAL.HU

Bevezető

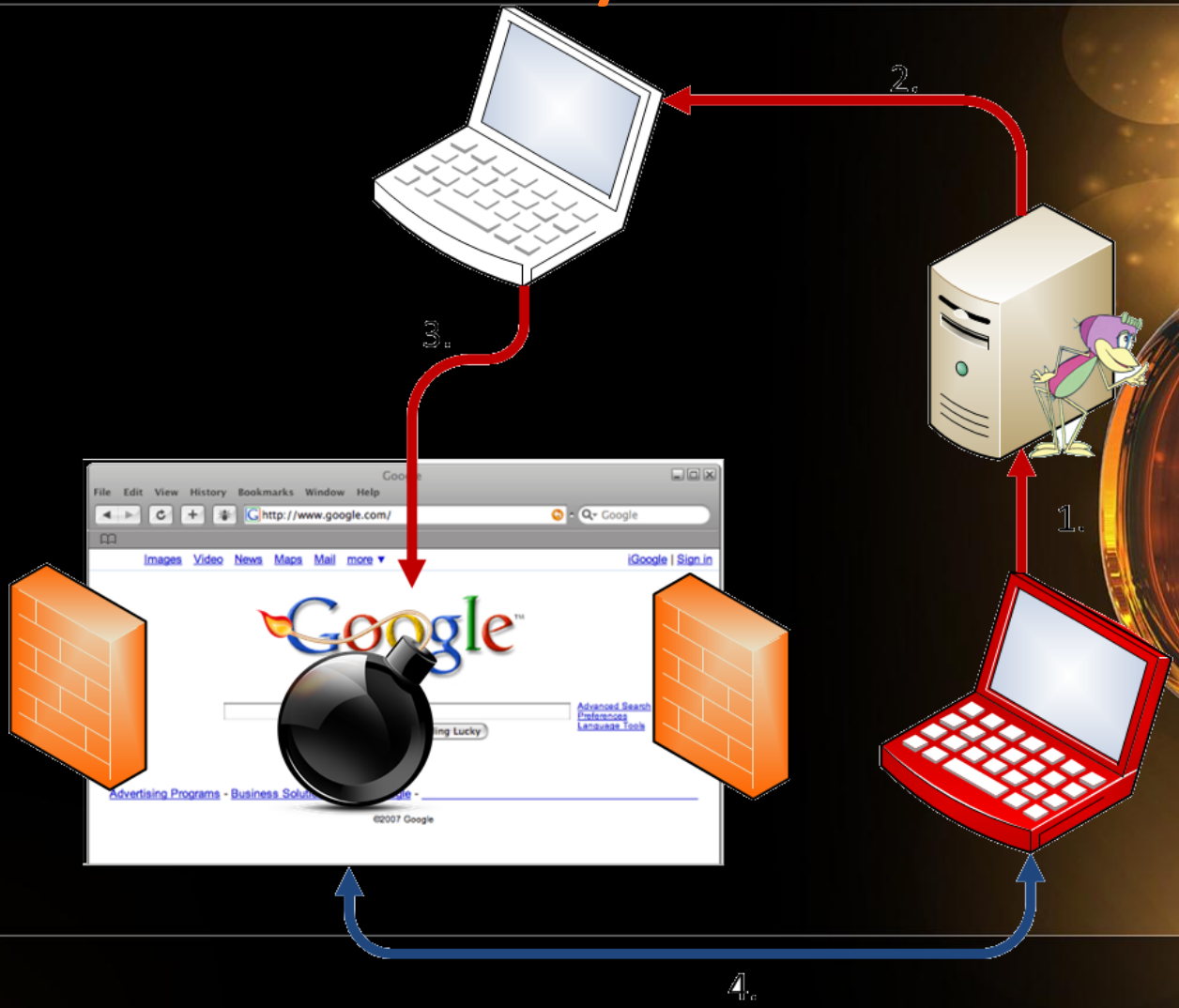
- A webes technológiák egyre több helyre épülnek be
  - Mobil eszközök
  - Beágyazott eszközök
- Webfejlesztők minden utcasarkon
- A meglévő biztonsági megoldások a hagyományos alkalmazásokra koncentrálnak

Hagyományos Cross-Site Scripting

Jellemzők

- A *webszerver* rosszindulatú kliens-oldali kódot szolgál ki
- A kiszolgált kód lefut a *böngészőben*
- Célba juttatás *alkalmazás rétegben*
- Nagyon gyakori
- A védekezés meglepően nehéz lehet

Lefolyás

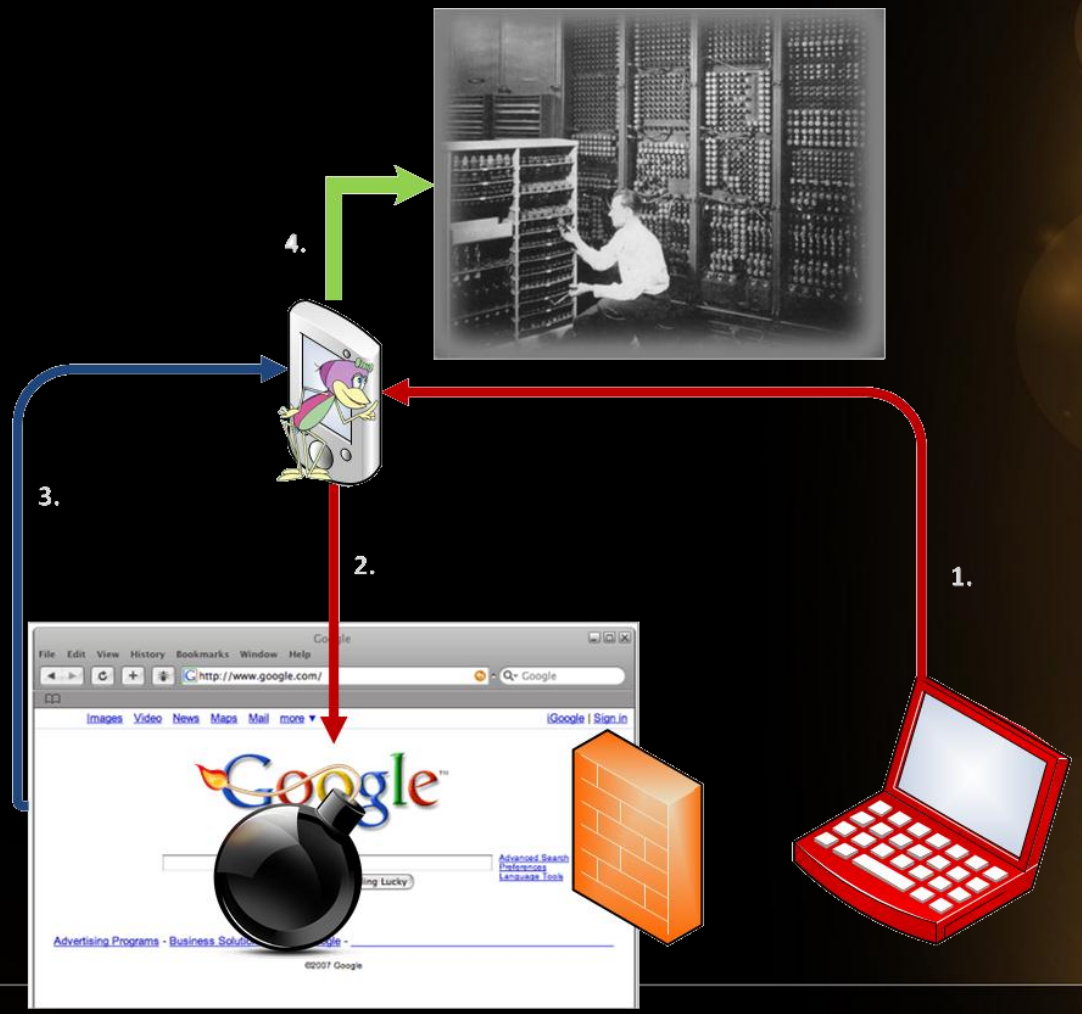

2.
3.
1.
4.
File Edit View History Bookmarks Window Help
http://www.google.com/
Images Video News Maps Mail more
iGoogle | Sign in
Google
Advertising Programs
©2007 Google

Hatás

- A támadó az áldozat nevében használhatja a *webalkalmazást*
- Érzékeny adatok kijuttatása
- Deface
- Malware terjesztés
- XSS féreg

Kindle Touch jailbreak

Lefolyás


4.
3.
2.
1.
http://www.google.com/
Images Video News Maps Mail more
iGoogle | Sign in
Google
Advertising Programs - Business Solutions
©2007 Google

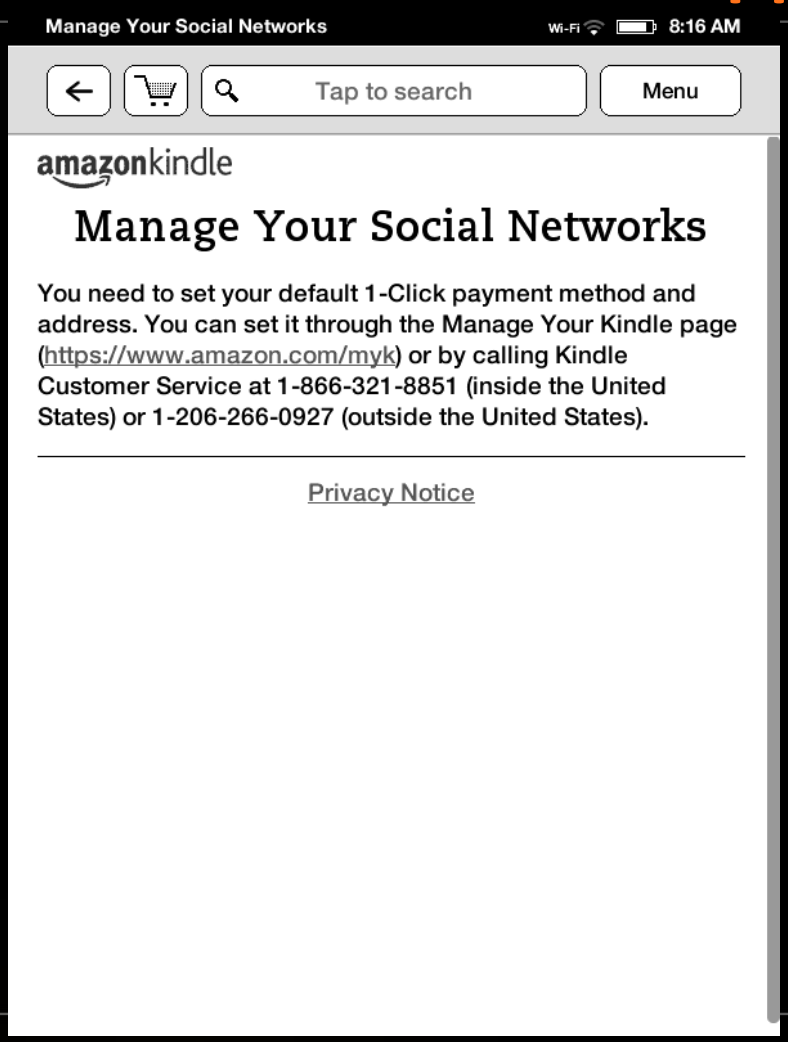
Jellemzők

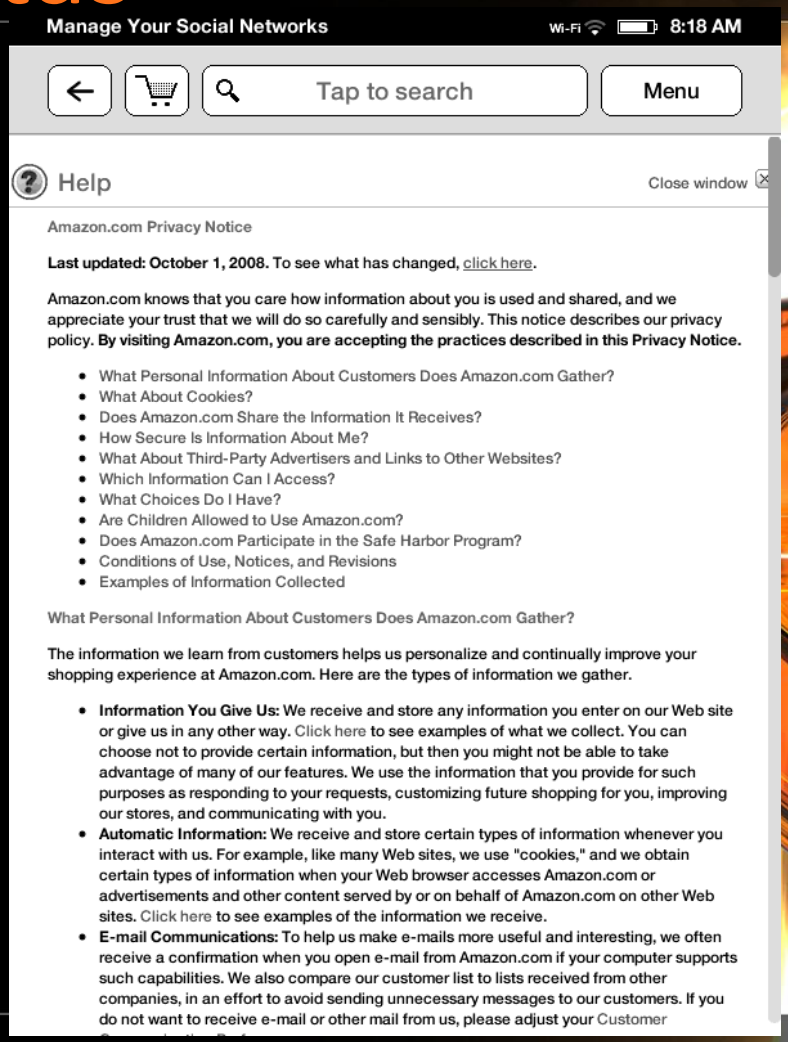
- Hiba a *mobil-alkalmazásban*
- A kiszolgált kódot megjeleníti a *böngészőmotor*
- Célba juttatás *alkalmazás rétegben*
- Ritka csemege

Hatás

- Teljes, operációs-rendszer szintű kontroll, aka. *Jailbreak*
  - Saját alkalmazások telepítése
  - Rejtett alkalmazások használata
  - Rejtett HW funkciók elérése
  - Reklámok eltüntetése?
  - Ingyen internet?

Hatás


Manage Your Social Networks
Wi-Fi
8:16 AM
Tap to search
Menu
amazonkindle
Manage Your Social Networks
You need to set your default 1-Click payment method and address. You can set it through the Manage Your Kindle page (https://www.amazon.com/myk) or by calling Kindle Customer Service at 1-866-321-8851 (inside the United States) or 1-206-266-0927 (outside the United States).
Privacy Notice

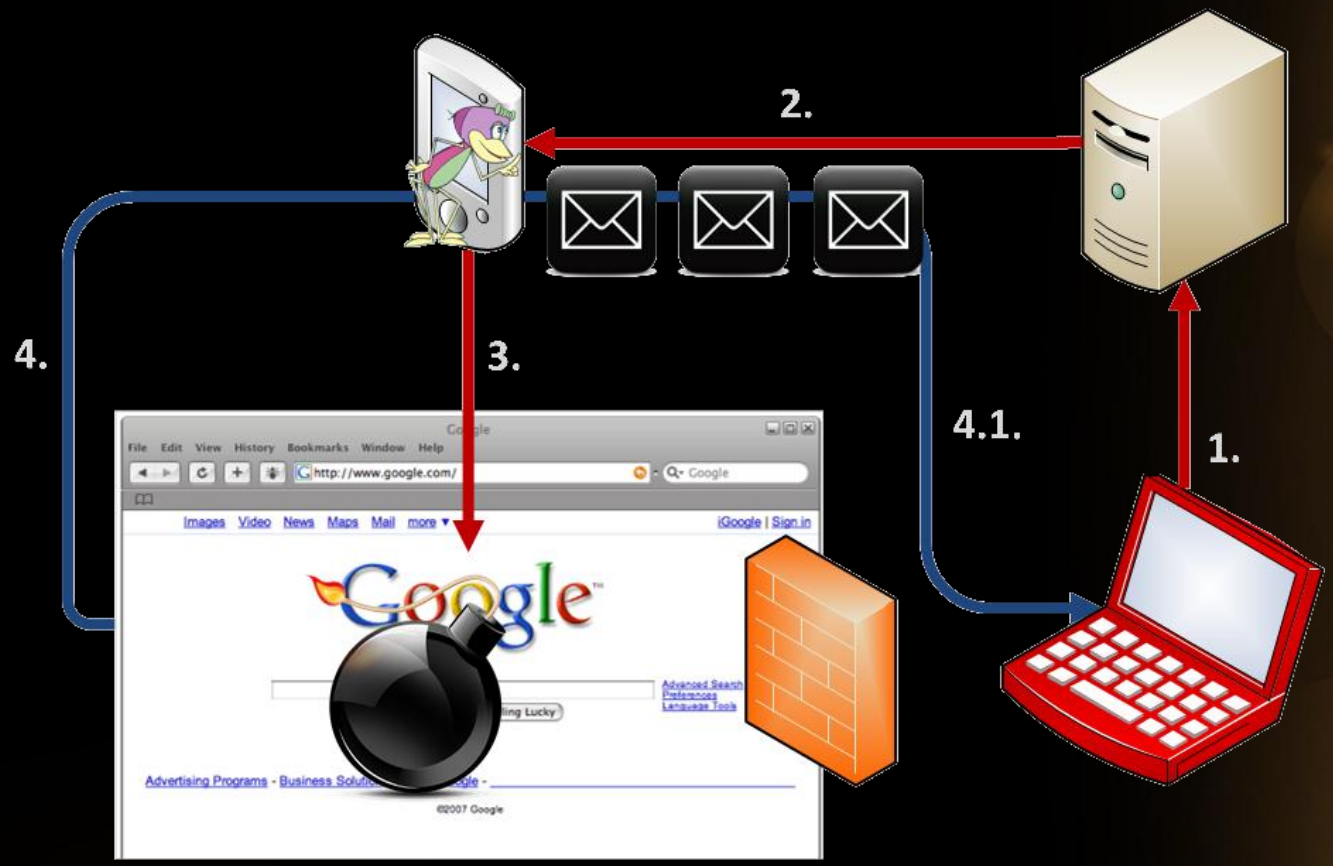

Manage Your Social Networks
Wi-Fi
8:18 AM
Tap to search
Menu
Help
Close window
Amazon.com Privacy Notice
Last updated: October 1, 2008. To see what has changed, click here.
Amazon.com knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This notice describes our privacy policy. By visiting Amazon.com, you are accepting the practices described in this Privacy Notice.
What Personal Information About Customers Does Amazon.com Gather?
What About Cookies?
Does Amazon.com Share the Information It Receives?
How Secure Is Information About Me?
What About Third-Party Advertisers and Links to Other Websites?
Which Information Can I Access?
What Choices Do I Have?
Are Children Allowed to Use Amazon.com?
Does Amazon.com Participate in the Safe Harbor Program?
Conditions of Use, Notices, and Revisions
Examples of Information Collected
What Personal Information About Customers Does Amazon.com Gather?
The information we learn from customers helps us personalize and continually improve your shopping experience at Amazon.com. Here are the types of information we gather.
Information You Give Us: We receive and store any information you enter on our Web site or give us in any other way. Click here to see examples of what we collect. You can choose not to provide certain information, but then you might not be able to take advantage of many of our features. We use the information that you provide for such purposes as responding to your requests, customizing future shopping for you, improving our stores, and communicating with you.
Automatic Information: We receive and store certain types of information whenever you interact with us. For example, like many Web sites, we use "cookies," and we obtain certain types of information when your Web browser accesses Amazon.com or advertisements and other content served by or on behalf of Amazon.com on other Web sites. Click here to see examples of the information we receive.
E-mail Communications: To help us make e-mails more useful and interesting, we often receive a confirmation when you open e-mail from Amazon.com if your computer supports such capabilities. We also compare our customer list to lists received from other companies, in an effort to avoid sending unnecessary messages to our customers. If you do not want to receive e-mail or other mail from us, please adjust your Customer

Cross-Platform Mobil keretrendszerek

SILENT SIGNAL
VÉSZJELZÉS HELYETT...

WWW.SILENTSIGNAL.HU

Lefolyás



Jellemzők

- Hiba a *mobil alkalmazásban*
- A fejlesztéskor a biztonság általában nem szempont
- OS szintű védelem
- Keretrendszer függő kihasználhatóság

Hatás

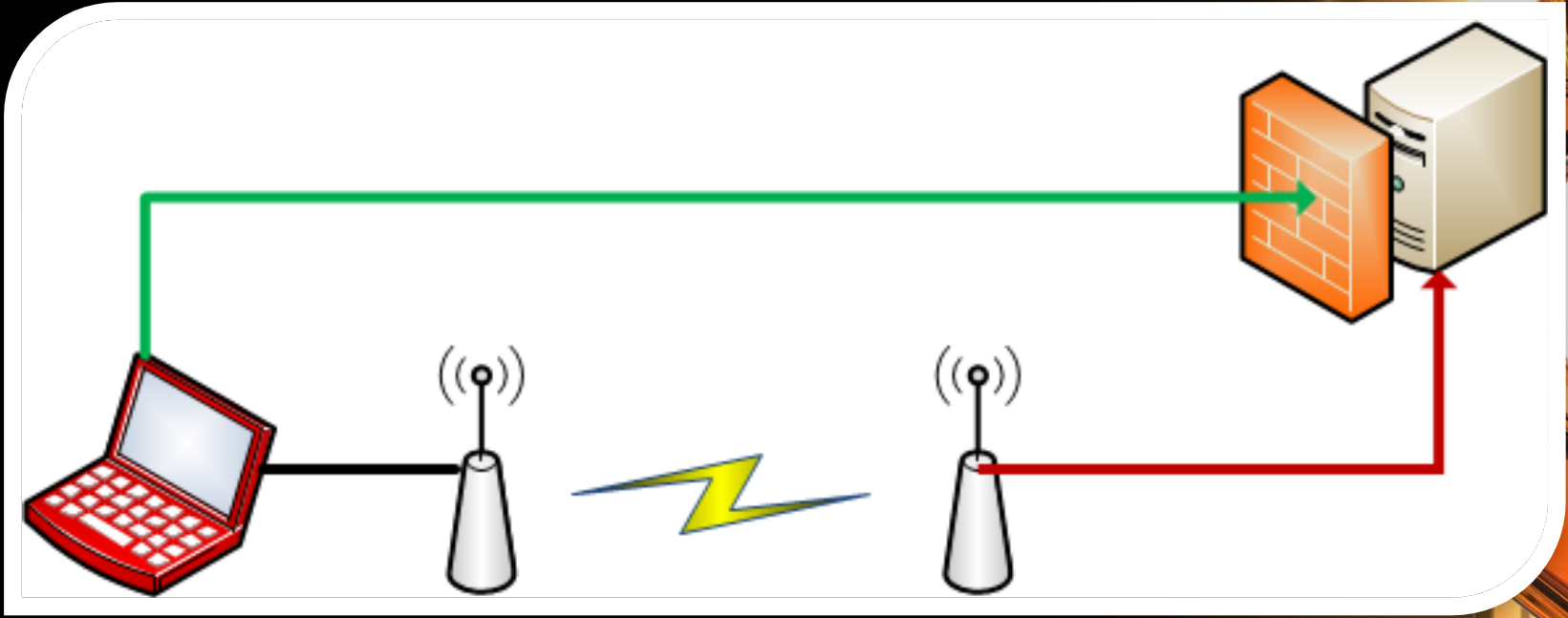
- A támadó az áldozat nevében használhatja a *mobil eszközt*
  - *Emelt díjas SMS*
  - *Emelt díjas hívások*
- Érzékeny *személyes* adatok kijuttatása
  - SMS-ek
  - Címjegyzék
- Rouge app terjesztés

Vezeték nélküli IPS

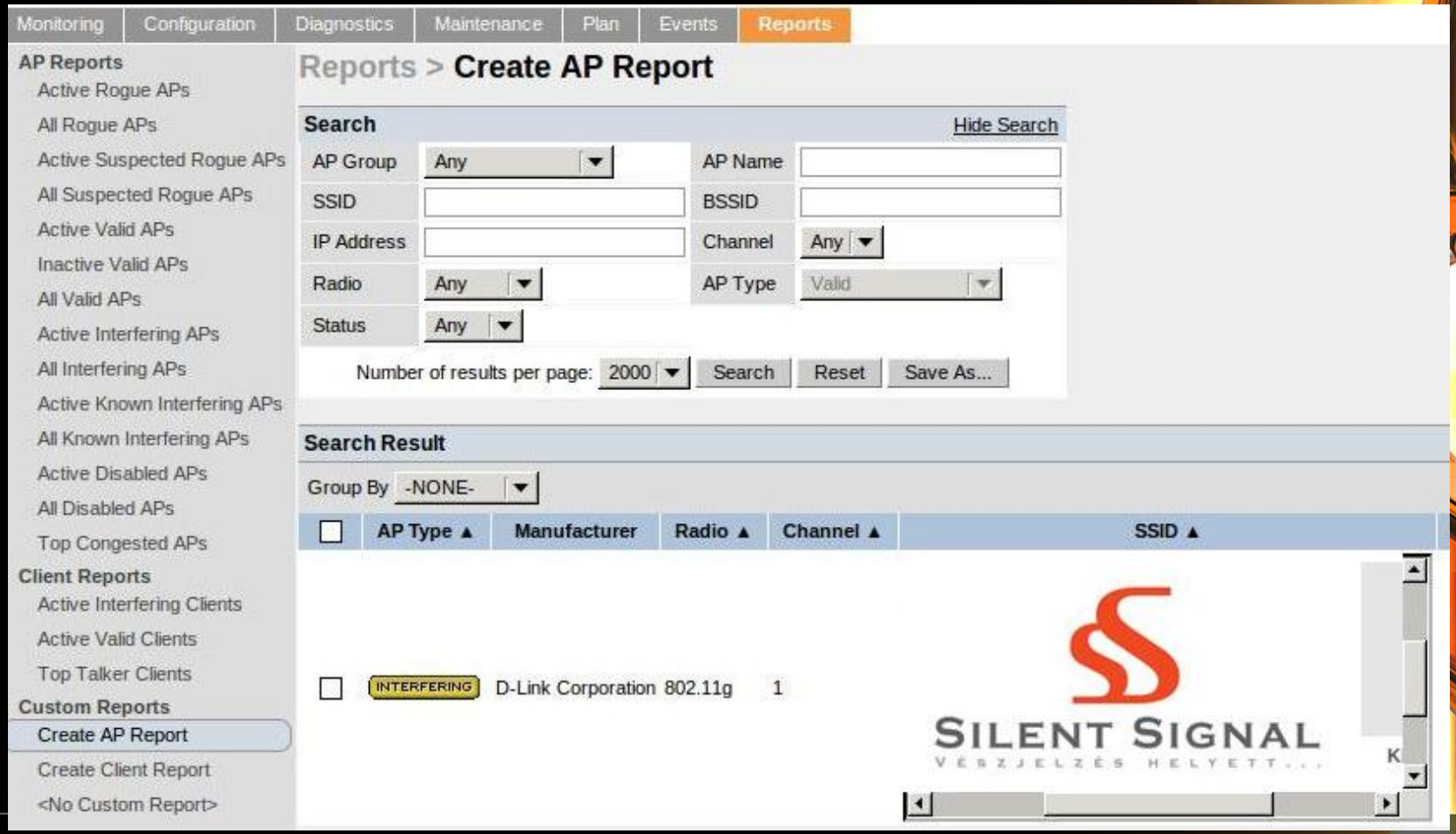
SILENT SIGNAL
VÉSZJELZÉS HELYETT...

WWW.SILENTSIGNAL.HU

Lefolyás



```
# SSID to be used in IEEE 802.11 management frames
ssid=<iframe/src=http:[redacted].hu/u>
```



Jellemzők

- Hiba a *beágyazott firmware-ben*
- A kiszolgált kód lefut az eszköz *menedzsment-felületén*
- Célba juttatás *adatkapcsolati rétegben*
- Speciális probléma
- A levegőből érkező adatok szűrése nem magától értetődő
  - Vajon más eszközök sebezhetők ugyanígy?

Hatás

- A támadó *menedzselheti az eszközt*
  - Új felhasználók felvétele
  - Tűzfalszabályok módosítása
  - DoS
  - …
- Tipikusan célzott támadás

WG (0-DAY)

WG szerepe, lehetőségek

- Konfigurációs lehetőségek
  - Port span/tap konfiguráció
  - Inline + proxy

Működési módok

  - CIU (central intelligence unit)
  - Standalone

Forrás megszerzése

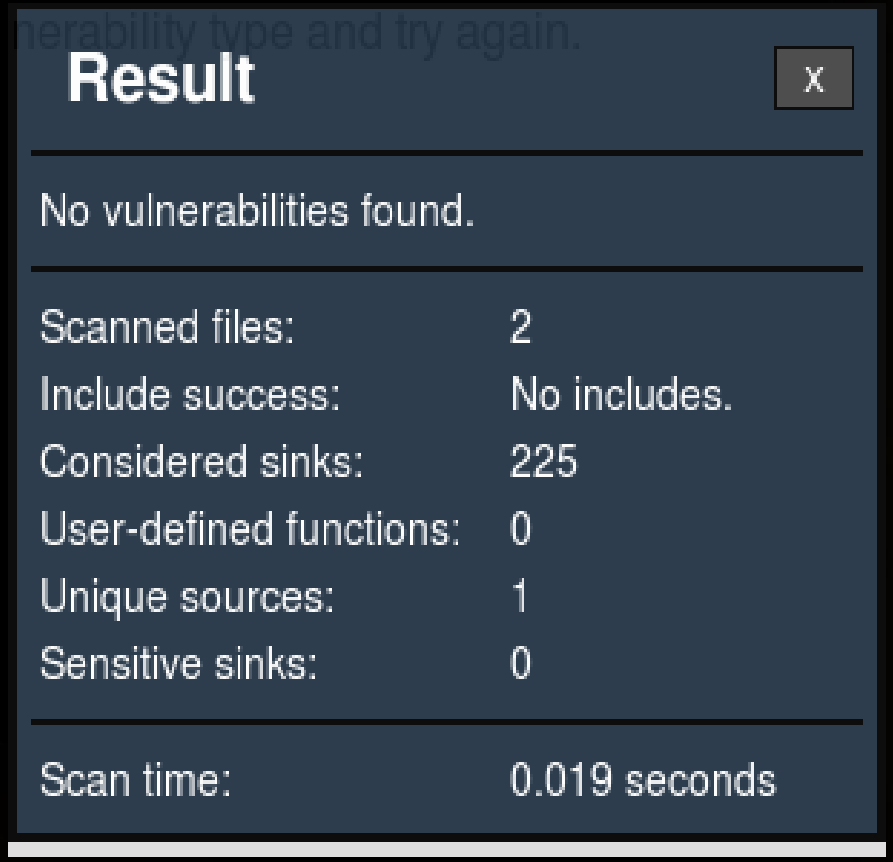
```
root@root:~# fdisk -l /dev/sda

Disk /dev/sda: 96.6 GB, 96636764160 bytes
255 heads, 63 sectors/track, 11748 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x000d76de

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          13      104391   83  Linux
/dev/sda2              14         268     2048287+  82  Linux swap / Solaris
/dev/sda3             269       11748    92213100   83  Linux
root@root:~# mount /dev/sda3 /mnt
root@root:~# ls -al /mnt/var/www/html/
total 436
drwxr-xr-x  8 root root   4096 2011-11-15 07:52 .
drwxr-xr-x  3 root root   4096 2006-04-25 18:59 ..
drwxr-xr-x  2 root root   4096 2011-11-16 07:57 c.
drwxr-xr-x  3 root root   4096 2011-09-13 20:59 [illegible]
drwxr-xr-x  4 root root   4096 2011-09-13 20:59 [illegible]
-rwxr-xr-x  1 root root 394534 2011-11-16 06:48 favicon.ico
-rwxr-xr-x  1 root root    244 2011-11-16 06:48 index.html
drwxr-xr-x  3 root root   4096 2011-09-13 20:59 [illegible]
drwxr-xr-x  2 root root   4096 2011-09-13 20:59 [illegible]
drwxr-xr-x 38 root root  12288 2011-09-13 20:59 [illegible]
root@root:~#
```

Kézimunka vs. automata

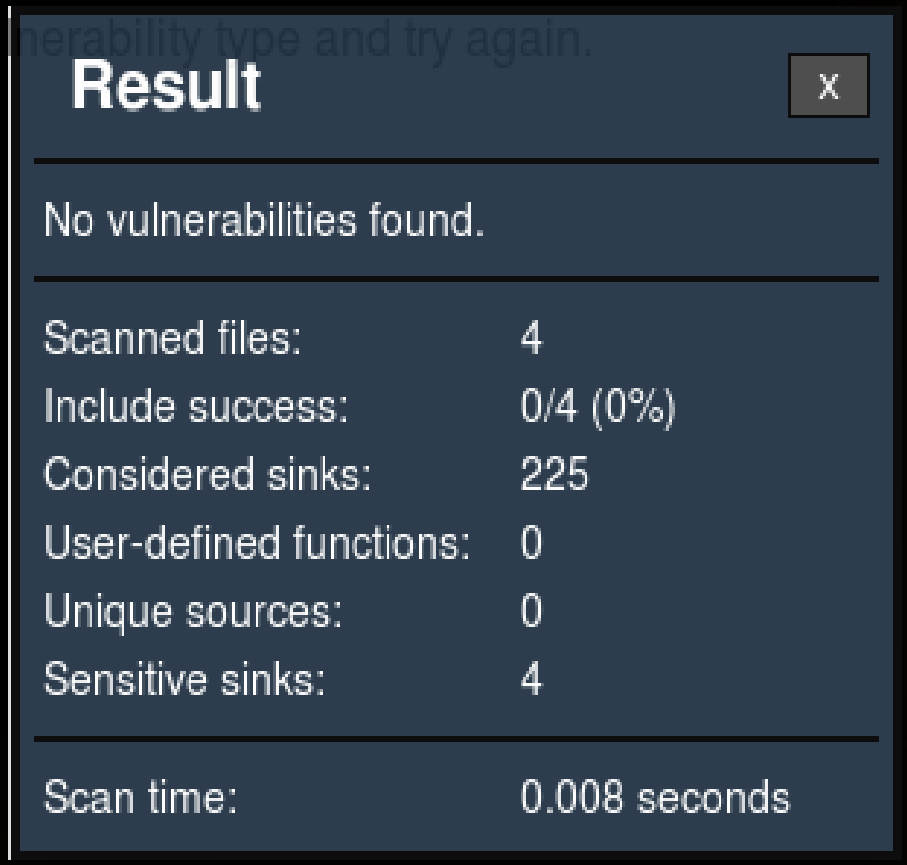
RIPS

- PHP forráskód analizátor
- Szerver oldali, kliens oldali hibák feltárása
- Funkciók értelmezése, összekötése (nem grep funkció)
- Proof of concept készítési lehetőség
- Grafikus felület, könnyű kezelhetőség

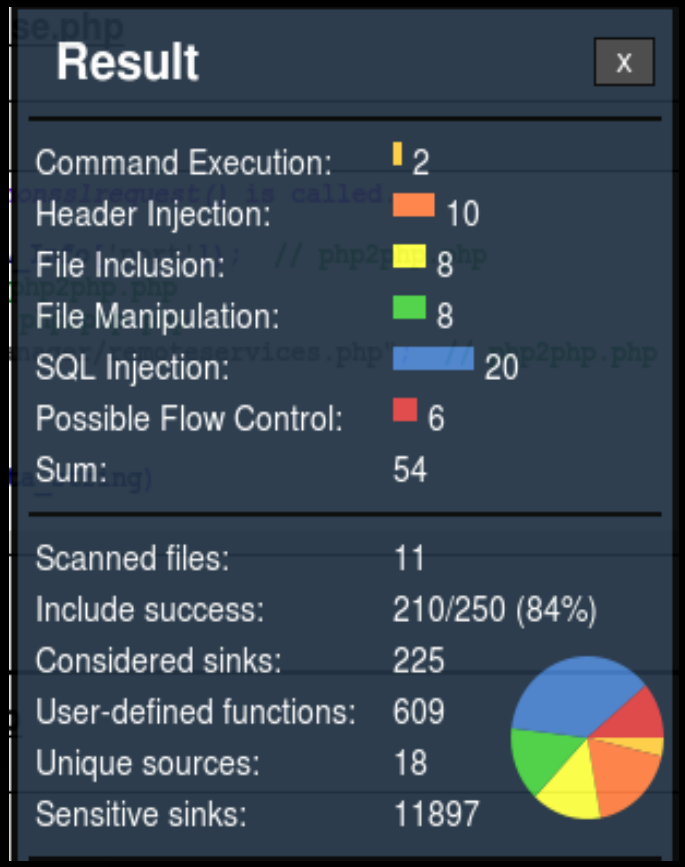
Eredmények (/ntlm)



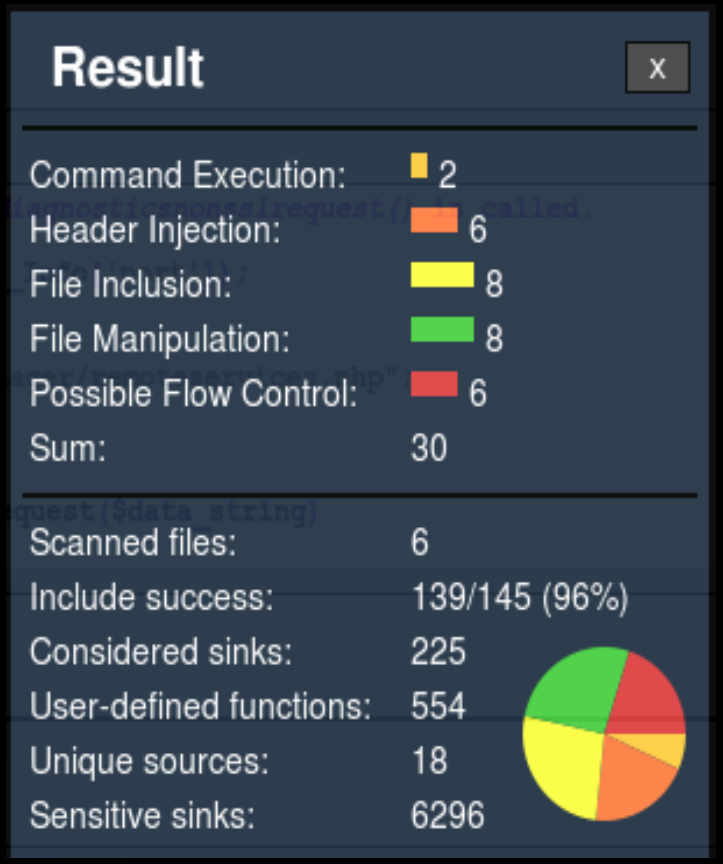
Eredmények (/errordocs)



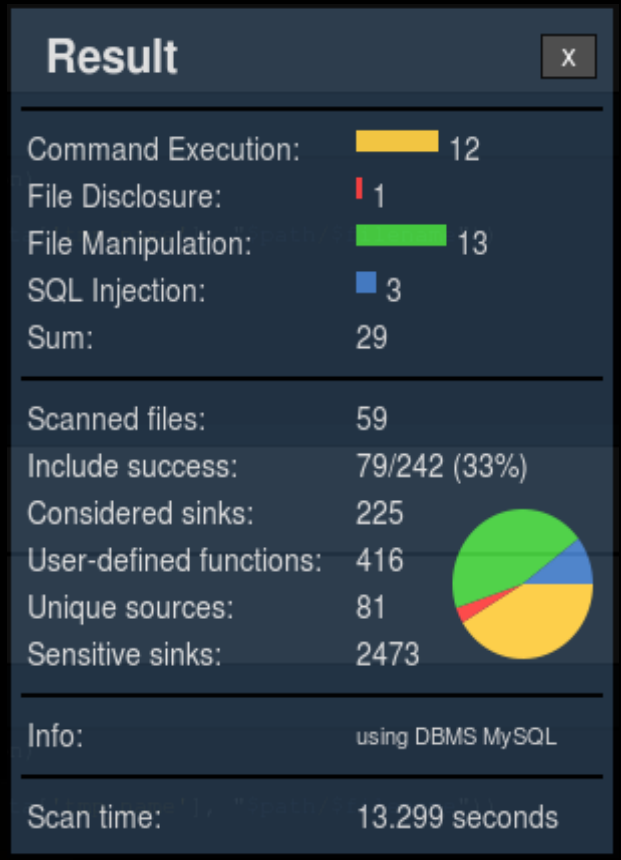
Eredmények (/licensemanager)



Eredmények (/diagnostics)



Eredmények (/ciu)

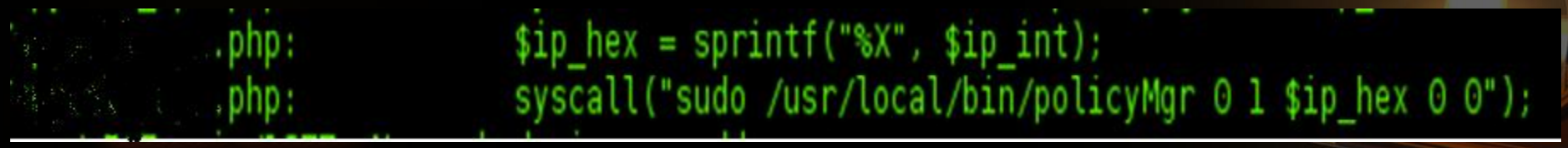


Eredmények (/s*****l)

- Több, mint 900 fájl (RIPS meghalt ☺)
- Csoportbontás, majd vizsgálat
- 20-as nagyságrendben hibák:
  - SQL Injection
  - File manipulation
  - Command execution
  - File Inclusion

Kézimunka

- Saját függvények biztonsági problémája
- Többszörösen egymásba ágyazott függvények ellenőrzése
- False pozitív kiszűrése (pl: HTTP_POST_VARS)
- Autentikációt igénylő hibák nem érdekesek ☺



Amit az szoftver nem tud…

```php
<?php

require_once "includes/[illegible].php";
require_once "includes/dbutils.php";
include_once "config/[illegible].php";

if (empty($_GET['err'])) {
        $filename = 'ERR_ACCESS_DENIED';
}
else {
        $filename = $_GET['err'];
}

if (empty($_POST['proxy_error'])) {
        $defaultText = selectfield('enduser_pages', 'proxy_error', array('msg_grp_id' => MSGGROUP_DEFAULT));
}
else {
        $defaultText = $_POST['proxy_error'];
}

$templator = new Templator();
$strings = array('swg-addr' => getIp(), 'custom-content' => $defaultText);
$templator->setStrings($strings);
$templator->fromFile("/var/www/html/[illegible]/template/$filename");

$contents = $templator->getTranslation();
$contents = str_replace('%U', 'http://example.com', $contents);

echo $contents;
?>
</body>
</html>
```

DEMO

Exploitálás

- Mozaik hacking ☺
  - Az ördög /remote shell/ a részletekben lakozik!
  - Fájl letöltés (amely töröl root jogokkal)
  - Autentikáció nélküli fájl feltöltési lehetőség
  - PHP parancs shell
  - WWW felhasználó által írható könyvtár a WEBROOT-on belül :D

GAME OVER!

DEMO

SILENT SIGNAL
VÉSZJELZÉS HELYETT...

WWW.SILENTSIGNAL.HU

Köszönjük a figyelmet!

SILENT SIGNAL
VÉSZJELZÉS HELYETT...

WWW.SILENTSIGNAL.HU