



айд אתרים נפרצים

ינוו פרק

אבטחת מערכת

=

אבטחה של החוליה החלשה bijouter

**מידע פרטי של 31
מיליון משתמשים
היה גלוי בשרת Ai.Type**

<https://thenextweb.com/security/2017/12/05/personal-info-31-million-people-leaked-popular-virtual-keyboard-ai-type/>



“the app’s database server was left online without any form of authentication. This meant anyone could access the company’s treasure-trove of personal information, which totals more than 577 gigabytes of data, without needing a password

”

“Some information is worryingly personal. It contains the precise location of the user, their phone number and cell provider, and according to Whittaker, the user’s IP address and ISP, if they use the keyboard while connected to Wi-Fi.

”

לקחיס?

עד באותו נושא

פרסום ראשון: פירצת אבטחה ב-date לשפה את כל התמונות, גם אלו שנמחקו

אבישי בר | אבטחת מידע

בתאריך 27 ביוני 2013 | 9 תגובות

 ציוץ  שטף/שתי

אם נרשםם פעם לאתר ה副书记 הפופולרי בכך למצא אהבה, יכול להיות שהתמונות שלכם, או של האהבה שלכם כבר נמצאות הרבה זמן בידיים אחרות.

חקיר



**רשות ממעותית
במשרד הפנים
חוות את פרטי
האזורים
המצאים תיעוד
ביומטרי**

[https://internet-
israel.com/reshenot-m-meshuotit-bmeshrad-hafnaim-chovat-at-p](https://internet-israel.com/reshenot-m-meshuotit-bmeshrad-hafnaim-chovat-at-p)

/

מדובר בשרת רדייס שנמצא בכתובת “

82.166.96.26

. שפותח לרשות ללא הגנה כלל

”

“Redis is designed to be accessed by trusted clients inside trusted environments. This means that usually it is not a good idea to expose the Redis instance directly to the internet or, in general, to an environment where untrusted clients can directly access the Redis TCP port or UNIX socket.”

-Redis security guidelines

חSHIPת מידע וחולשות

- מערכות קיימות מכילות באגים, חלקים קשורים לאבטחת
מידע
- מאגר Vulnerabilities עם אפשרות לחיפוש:
<https://www.com.cvedetails.com>

ונעבור לדפדף

- <http://www.gilsport.co.il>

לקחיס?

Supply Chain Attacks

- <https://blog.npmjs.org/post/180565383195/details-about-the-event-stream-incident>
- <https://www.zdnet.com/article/backdoor-code-found-in-popular-bootstrap-sass-ruby-library/>
- <https://www.bankinfosecurity.com/ticketmaster-breach-traces-to-embedded-chatbot-software-a-11144>
- <https://www.israeldefense.co.il/he/node/37666>

שווה לבדוק

```
<script  
  src="https://example.com/example-framework.js"  
  integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/  
uxy9rx7HNQlGYl1kPzQholwx4JwY8wC"  
  crossorigin="anonymous"></script>
```

שווה לבדוק

- מי מתקן חbillות? איך? מי מחליט על שדרוג?
- לחת חbillות "להתקרר" לפני שרצים להתקין
- לוודא Vulnerabilities בחbillות שלנו

גניבת פרטי עובדים של הובילה לגניבת מידע משתי החברה

<https://www.kaspersky.com/blog/a-confirmed-ebay-leak-another-password-alert/14953/>



- במאי 2014 איברוי הודיעה על זיהוי פירצה בשרתים שלה וגניבה גדולה של פרטי משתמשים. הגניבה קرتה אחרי שהפורצים הצליחו להציג פרטי גישה של אנשי תמייה ובעזרת פרטי גישה אלה "שטו" את כל המידע.
- לפורצים היו חודשיים וחצי לשtotot את המידע מהשרתים עד שהתגלו.

ופה בארץ...

- עובד לאומי קارد אלירן רוזנס גנב מאגר נתוניים ב 2015

<https://www.calcalist.co.il/local/articles/0,7340,L-3648957,00.html>



"מצטער בפנוי כל מי שנפגע. זו לא הייתה הכוונה",

אומר אלירן רוזנס, עובד זוטר לשעבר בחברת האשראי "לאומי קארד", אשר ללא רקע מוקדם במחשבים הצליל הגןוב את פרטייהם של כ שני מיליון לקוחות ולהפוך לאיום ממשי על היציבות הפיננסית של ישראל.

ופה הארץ...

- **ליאור שרעבי, מנהל התמיכה ב Active Trail העתיק מאגרי מידע. נשבט ב 2017**

**הנאש שלח, בעשרות הזרמוויות שונות, הודעות
דואר אלקטרוני מאיימות לבכירים בנק יב
ובחברת אקטיב טרייל ואים עליהם שם לא עברו
מיליוני שקלים בطبع הוירטואלי ביטקוין, הוא
יפרסם ב"רשת האפלה" וכן עבר לעתונים
מאגרי מידע השיכים לבנק וחברה ואשר פרסומים
עלול להסביר להם נזקים כלכליים ניכרים**

Plain Old Bugs

קוד להעלאת קובץ PHP

```
if ($_POST['url']) {
    $uploaddir = $_POST['url'];
}

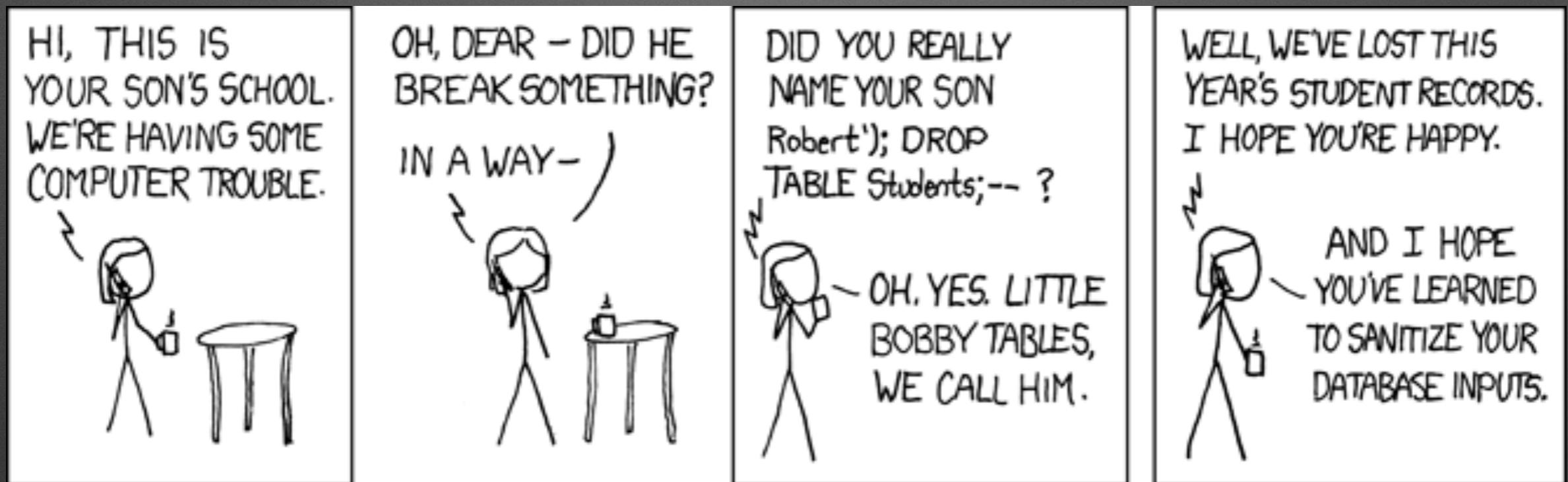
$first_filename = $_FILES['uploadfile']['name'];
$filename = md5($first_filename);
$ext = substr($first_filename, 1 + strrpos($first_filename, '.'));
$file = $uploaddir . basename($filename . '.' . $ext);

if (move_uploaded_file($_FILES['uploadfile']['tmp_name'], $file)) {
    echo basename($filename . '.' . $ext);
} else {
    echo 'error';
}
```

קוד PHP לגדרות לעדכון הגדרות

```
if($configManager->getConfig('admin.password')==null){  
    $url = 'setup.php';  
    header("Location: $url");  
    exit;  
}  
  
if(isset($_POST['SAVE_CONFIG'])){ ●  
    $configs = $configManager->getConfig();  
    $configs['path.pdf'] = $_POST['PDF_Directory'];  
    $configs['path.swf'] = $_POST['SWF_Directory'];  
    $configs['licensekey'] = $_POST['LICENSEKEY'];  
    $configs['splitmode'] = $_POST['SPLITMODE'];  
    $configs['renderingorder.primary'] = $_POST['RenderingOrder_PRIM'];  
    $configs['renderingorder.secondary'] = $_POST['RenderingOrder_SEC'];  
  
    $configManager->saveConfig($configs);  
    $dir = $configManager->getConfig('path.swf'); ●  
    foreach(glob($dir.'*.*') as $v){  
        unlink($v);  
    }  
    header("Location: index.php?msg=Configuration%20saved!");  
    exit;  
}  
  
if(!isset($_SESSION['FLEXPAPER_AUTH'])) { ●  
    $url = 'index.php';  
    header("Location: $url");  
    exit;  
}
```

SQL Injection



SQL Injection

בלעדי לכלכלה

פרצת אבטחה חשפה את יודי הטישה של ראש הממשלה ובכירים מערכת הביטחון

פרטי נסיעותיהם של בכירים מערכת הביטחון וגורםים מדיניים ובהם ראש הממשלה נחשפו במאגר מידע שד龄. אלה רק חלק מפרטי פרצת חמורה למאגר, שבו פרטייהם של 15 מיליון איש. "פוטנציאל עצום לנזק"

עומר כביר 06:48 22.05.19

XSS



Race Conditions

Hacking Starbucks for unlimited coffee

<https://web.archive.org/web/20150609034106/http://sakurity.com/blog/2015/05/21/starbucks.html>



Race Conditions

```
$transfer_amount = GetTransferAmount();
$balance = GetBalanceFromDatabase();

if ($transfer_amount < 0) {
    FatalError("Bad Transfer Amount");
}

$newbalance = $balance - $transfer_amount;

if (($balance - $transfer_amount) < 0) {
    FatalError("Insufficient Funds");
}

SendNewBalanceToDatabase($newbalance);
NotifyUser("Transfer of $transfer_amount succeeded.");
NotifyUser("New balance: $newbalance");
```

מיליוני סיסמות נפרצו לאתר אשלי מדיסון

ASHLEY
MADISON[®].COM



מבנה בסיס הנתונים

- שדה סיסמה מאובטח ב bcrypt
- שדה token שבנוי מ: md5(lc(\$username).":".\$pass))

65T2068657265696720206
46668206B617364662073A
7166386E6A2D3D4A697
57220706872617365T2
666B6120206B736A646668
5F2C622135242759716638
656E74657220796F7572
967202016A617364206
46620737C3A3E26375F20
A69704E5B2327573265650
17365T2068657265696720206
776AC11CC69206C61776

תודה שבעאתם

• ינון פרק
<https://www.tocode.co.il> •