Web User Interfaces
Bug Of The Day

- Not strictly a security bug: https://arstechnica.com/information-technology/2019/10/chemists-discover-cross-platform-python-scripts-not-so-cross-platform/
Root Cause:
Undefined but *platform* deterministic behavior

- Python is generally supposed to be "cross platform"
- Can run on anything that supports it
- But there is a lot of behavior that is platform dependent
  - Notably anything touching files
- One example, the rules for *matching* in `glob.glob` are specified, but the order isn't...

  `glob` — Unix style pathname pattern expansion

Source code: `Lib/glob.py`

The `glob` module finds all the pathnames matching a specified pattern according to the rules used by the Unix shell, although results are returned in arbitrary order. No tilde expansion is done, but *, ?,
In Practice:
Unspecified but deterministic

- Windows would produce the list in one way, linux another
  - But within each OS, it would be consistent
  - Thus the code would give different results, but it "Worked fine for us"
- Useful paradigm:
  - If you have some unspecified behavior, make sure it is random each time!
  - golang does this with thread execution

```python
def read_gaussian_outputfiles():
    list_of_files = []
    for file in glob.glob('*\.out'):
        list_of_files.append(file)
    return list_of_files
```
So Far: Attacks involving just the server or browser/server interactions

- Good "cheatsheets": https://github.com/OWASP/CheatSheetSeries
- SQL injection & command injection
  - Server only attacks: uploaded data is processed as code on the server
  - Root cause: Too-powerful APIs
    - Things like `system()` and raw SQL queries
  - Solution: Use better APIs like `execve()` and SQL prepared statements
- Cross Site Request Forgery (CSRF/XSRF)
  - Server/client attacks: client "tricked" into sending request with cookies to the server
    - Does not require JavaScript!
  - Root cause: Base web design didn't include a clean mechanism to specify origin for requests
  - Solution: Hidden tokens, toolkits that do this automatically, Cookies with the "SameSite" attribute.
Cross Site Scripting

- Stored/Reflected XSS
  - Client receives JavaScript "from server"
  - But server was tricked into providing attacker's JavaScript
  - Stored: Server tricked into storing, get target to visit the page
    - Common pattern is uploaded user content that others can see
  - Reflected: Server tricked into displaying as part of the URL
    - Common pattern is query reflected back in the page results

- Solution:
  - Only allow user content in some specific types of locations
    - And even then, you need to escape some or all non alphanumeric characters
    - Ideally use a sanitizer
  - Content Security Policy: tell the browser to only accept scripts from limited locations
    - And no inline scripts period
Misleading Users

- Browser assumes clicks & keystrokes = clear indication of what the user wants to do
  - Constitutes part of the user’s trusted path
- Attacker can meddle with integrity of this relationship in different ways …
Navigate to www.berkeley.edu
Same, but smaller window.
Mouse anywhere over the region points to https://crowdfund.berkeley.edu
Let's load www.berkeley.edu

```html
<p>
<div>
<iframe src="http://www.berkeley.edu"
width=500 height=500"></iframe>
</div>
</p>
```

We load www.berkeley.edu in an iframe
Let’s load www.berkeley.edu

Any Javascript in the surrounding window can’t generate synthetic clicks in the framed window due to Same Origin Policy.
Let’s load www.berkeley.edu

Though of course if the *user themselves* clicks in the framed window, that “counts”...

Discover new Berkeley Crowdfunding projects today
Let's load www.berkeley.edu

[Image: Berkeley University webpage]

Discover new Berkeley Crowdfunding projects today

https://crowdfund.berkeley.edu
Let's load www.berkeley.edu

<p>
<div style="position:absolute; top: 0px;">
<iframe src="http://www.berkeley.edu"
width=500 height=500></iframe>
</div>

We position the iframe to completely overlap with the outer frame
Discover new Berkeley Crowdfunding projects today
Let's load www.berkeley.edu

```html
<p>
<div style="position:absolute; top: 40px;"> 
<iframe src="http://www.berkeley.edu"
width=500 height=500"></iframe> 
</div>
</p>
```

We nudge the iframe’s position a bit below the top so we can see our outer frame text
Let's load www.berkeley.edu

Discover new Berkeley Crowdfunding projects today
Let's load www.berkeley.edu
<p class="bigspace">
<em>You <b>Know</b> You Want To Click Here!</em>
</p>
<p>
<div style="position:absolute; top: 40px;">
<iframe src="http://www.berkeley.edu" width=500 height=500></iframe>
</div>
</p>

We add marked-up text to the outer frame, about 3 inches from the top
Let's load www.berkeley.edu

Discover new Berkeley Crowdfunding projects today
Let's load www.berkeley.edu, opacity 0.8

```html
<p class="bigspace">
<em>You <b>Know</b> You Want To Click Here!</em>
</p>
<div style="position:absolute; top: 40px;">
<iframe src="http://www.berkeley.edu" width=500 height=500></iframe>
</div>
```

We make the iframe partially transparent
Let's load www.berkeley.edu, opacity 0.8
Let's load www.berkeley.edu, opacity 0.1

You Know You Want To Click Here!

We make the iframe highly transparent
Let's load www.berkeley.edu, opacity 0.1

https://crowdfund.berkeley.edu
Let's load www.berkeley.edu, opacity 0

<p class="bigspace">
<em>You <b>Know</b> You Want To Click Here!</em>

We make the iframe <i>entirely</i> transparent
Let's load www.berkeley.edu, opacity 0

You Know You Want To Click Here!

Click anywhere over the region goes to 
https://crowdfund.berkeley.edu

https://crowdfund.berkeley.edu
Clickjacking

- By placing an *invisible* iframe of `target.com` *over* some enticing content, a malicious web server can fool a user into taking unintended action on `target.com` ...

- ... By placing a *visible* iframe of `target.com` *under* the attacker’s own *invisible* iframe, a malicious web server can “steal” user input – in particular, *keystrokes*
Clickjacking Defenses

• Require confirmation for actions (annoys users)
• Frame-busting: Web site ensures that its “vulnerable” pages can’t be included as a frame inside another browser frame
  • So user can’t be looking at it with something invisible overlaid on top …
  • … nor have the site invisible above something else
Attacker implements this by placing Twitter’s page in a “Frame” inside their own page. Otherwise they wouldn’t overlap.
Clickjacking Defenses

- Require confirmation for actions (annoys users)
- Frame-busting: Web site ensures that its “vulnerable” pages can’t be included as a frame inside another browser frame
  - So user can’t be looking at it with something invisible overlaid on top …
  - … nor have the site invisible above something else
- See OWASP’s “cheat sheet” for this too
Clickjacking Defenses

• Require confirmation for actions (annoys users)
• Frame-busting: Web site ensures that its “vulnerable” pages can’t be included as a frame inside another browser frame
  • So user can’t be looking at it with something invisible overlaid on top …
  • … nor have the site invisible above something else
• Another approach: HTTP X-Frame-Options header
  • Allows white-listing of what domains – if any – are allowed to frame a given page a server returns
Yes, there is a hell of a lot of grafted on web security...

- So far we've seen:
  - **Content-Security-Policy**: (HTTP header)
  - **SameSite** (Cookie attribute)
  - And now **X-Frame-Options** (HTTP header)

- One curse of security: Backwards compatibility....
  - We can't just throw out the old S#@#(: people depend on it!
Phishing...

- Leveraging the richness of web pages...
- And user training!
Date: Thu, 9 Feb 2017 07:19:40 -0600
From: PayPal <alert@gnc.cc>
Subject: [Important] : This is an automatic message to : (vern)
To: vern@aciri.org

Dear vern we are making a few changes

Your Account Will Be Closed!

Hello, Dear vern

Your Account Will Be Closed. Until We Here From You. To Update Your Information. Simply click on the web address below

What do I need to do?

Confirm My Account Now

How do I know this is not a Spoof email?

Spoof or ‘phishing’ emails tend to have generic greetings such as “Dear vern”. Emails from PayPal will always address you by your first and last name.

Find out more here.

This email was sent to vern.

Copyright ©(c) 1999-2017. All rights reserved. PayPal Pte. Ltd. Address is 5 Temasek Boulevard #09-01 Suntec Tower 5 Singapore 038985
Dear vern we are making a few changes

Your Account Will Be Closed!

Hello, Dear vern

Your Account Will Be Closed, Until We Here From You. To Update Your Information. Simply click on the web address below

What do I need to do?

Confirm My Account Now

Help Contact Security

How do I know this is not a Spoof email?

Spoof or 'phishing' emails tend to have generic greetings such as "Dearvern". Emails from PayPal will always address you by your first and last name.

Find out more here.

This email was sent to vern.

Copyright © 1999-2017. All rights reserved. PayPal Pte. Ltd. Address is 5 Temasek Boulevard #09-01 Suntec Tower 5 Singapore 038985

Open “universalkids.com.br/re.php” in a new window
Confirm Your personal PayPal Informations

- Stefani Joanne Angelina
- Germanotta
- 28-03-1986
- On Tour
- City
- United States of America
- State
- Zip Code
- Mobile
- Phone Number

Continue
Confirm your Credit Card

- Pay without exposing your card number to merchants
- No need to retype your card information when you pay

🔒 Your security is our top priority

- Your financial information is securely stored and encrypted on our servers and is not shared with merchants.
Confirm your Credit Card

- Pay without exposing your card number to merchants
- No need to retype your card information when you pay

Primary Credit Card

- Not Sure
- MM/YYYY
- CSC
- 121-21-2121
- This Card is a VBV /MSC

Continue

Your financial information is securely stored and encrypted on our servers and is not shared with merchants.
Please enter your Secure Code

Name of cardholder Stefani Joanne Angelina Germanotta

Zip Code

Country United States of America

Card Number Not Sure

Password $secret

Submit

Copyright © 1999-2017. All rights reserved.
Confirm your bank account

Join 72 million PayPal members who have Confirmed a bank

- Pay with cash when you shop online
- Send money to friends in the U.S. for FREE
- Withdraw money from PayPal to your bank account

Your financial information is securely stored and encrypted on our servers and is not shared with merchants.
Confirm your bank account

Join 72 million PayPal members who have
Confirmed a bank

- Pay with cash when you shop online
- Send money to friends in the U.S. for FREE
- Withdraw money from PayPal to your bank account

Your financial information is securely stored and encrypted on our servers and is not shared with merchants.
Your account is ready to use!

Shop, sell things, and transfer money with PayPal now.

Go shopping
Shop safer online and in stores just look for the PayPal logo when you check out.

Sell something
Sell on eBay or your web site. Get paid instantly, securely.

Transfer money
Pay a friend back for lunch. Raise money for a group gift. It's fast and easy.

Buy
Sell
Transfer
PayPal login page with fields for Email and Password, and options to Log In or Sign Up.
The Problem of Phishing

- Arises due to mismatch between reality & user’s:
  - Perception of how to assess legitimacy
  - Mental model of what attackers can control
    - Both Email and Web

- Coupled with:
  - Deficiencies in how web sites authenticate
    - In particular, “replayable” authentication that is vulnerable to theft

- Attackers have many angles …
Homograph Attacks

- International domain names can use international character set
  - E.g., Chinese contains characters that look like / . ? =

- **Attack:** Legitimately register var.cn …
- … buy legitimate set of HTTPS certificates for it …
- … and then create a subdomain:
  - www.pnc.com/webapp/unsec/homepage.var.cn

This is one subdomain
Check for a padlock?
Check for “green glow” in address bar?
Check for Everything?
“Browser in Browser”

Apparent browser is just a **fully interactive image** generated by Javascript running in real browser!
So Why Does This Work?

- Because users are stupid?
Why does phishing work?

- User mental model vs. reality
  - Browser security model too hard to understand!

- The easy path is insecure; the secure path takes extra effort

- Risks are rare

- Users tend not to suspect malice; they find benign interpretations and have been acclimated to failure

- And as a bonus, we actively train users to be phished!
Two Factor

- Because people chose bad passwords...
  - Add a *second* authentication path
- Relies on the user having access to something orthogonal to the password
  - Cellphone or email
  - Security Token/Authenticator App
  - FIDO U2F/FIDO2 security key
Second Communication Channel...

- Provide the "security code" (4-8 digits) transmitted "out of band"
  - Cellphone SMS
  - Email

- Still vulnerable to transient phishing (a relay attack)...
  - Phishing site immediately tries to log in as the user...
  - Sees 2-factor is in use
  - Presents a fake "2-Factor" challenge
    - Passes the result to the site...
    - BOOM, logged in!
Authentication Tokens/Apps

- RSA Securid and Google Authenticator
  - Token and site share a common secret key
- Display first 6 digits of: HMAC(K, time)
  - Time rounded to 30 seconds
- Verify:
  - If code == HMAC(K, time) or HMAC(K, time+30) or HMAC(K, time-30), OK
- Still vulnerable to transient phishing!
- But code is relatively small...
  - Assumes some limit on brute-forcing: After 3+ tries, start adding delays
Bigger Point of those 2FA protections: Credential stuffing

• Since people reuse passwords *all the time*
• Attacker compromises one site
  • Then uses the resulting data to get everyone's password
    • Brute force the password hashes
• Now attacker reuses those passwords on every other site
• Basic 2FA prevents that
  • The password alone is no longer enough to log in
FIDO U2F/FIDO2 Security Key

- Two operations:
  - Register Site:
    - Generate a new public/private key pair and present it to the site
  - Verify:
    - Given a nonce, site, and key ID, sign the nonce and return it
      - Nonce (provided by server) prevents replay attack
      - Site is verified as allowed for the key ID, prevents relay attack

- Both operations require user presence
  - Can't happen in the background, need to "touch" the key
    - But an optional "no touch needed" mode is supported

- Can't be phished!
  - A phishing site will fail the site verification
CAPTCHAs: How Lazy Cryptographers Do AI

- The whole point of CAPCHAs is not just to solve "is this human"...
  - But leverage bad guys to force them to solve hard problems
  - Primarily focused on machine vision problems

![Image of comic strip](image-url)
By clicking the "Create My Account" button below, I certify that I have read and agree to the Yahoo! Terms of Service, Yahoo! Privacy Policy and Communication Terms of Service, and to receive account related communications from Yahoo! electronically. Yahoo! automatically identifies items such as words, links, people, and subjects from your Yahoo! communications services to deliver product features and relevant advertising.
CAPTCHAs

- **Reverse Turing Test**: present “user” a challenge that’s easy for a human to solve, hard for a program to solve
- One common approach: distorted text that’s difficult for character-recognition algorithms to decipher
Figure 1: Examples of CAPTCHAs from various Internet properties.
Verify Your Registration

Enter the code shown: 

This helps prevent automated registrations.

Please enter the code you see below. what's this?

Qualifying question

Just to prove you are a human, please answer the following math challenge.

Q: Calculate:
\[
\frac{\partial}{\partial x} \left[ 4 \cdot \sin \left( 7 \cdot x - \frac{\pi}{2} \right) \right]_{x=0}
\]

A: 

Note: If you do not know the answer to this question, reload the page and you'll get another question.
Issues with CAPTCHAs

• Inevitable arms race: as solving algorithms get better, defense erodes

Figure 4: Examples of images from the hard CAPTCHA puzzles dataset.
Issues with CAPTCHAs

- Inevitable arms race: as solving algorithms get better, defense erodes, or gets harder for humans
Asirra

Asirra is a human interactive proof that asks users to identify photos of cats and dogs. It's powered by over two million photos from our unique partnership with Petfinder.com. Protect your web site with Asirra — free!
Issues with CAPTCHAs

• Inevitable arms race: as solving algorithms get better, defense erodes, or gets harder for humans

• **Accessibility**: not all humans can see
• **Granularity**: not all bots are bad (e.g., crawlers)
Issues with CAPTCHAs, con’t

• Deepest problem: CAPTCHAs are inherently vulnerable to outsourcing attacks
  • Attacker gets real humans to solve them
Using the advertisement in blogs, social networks, etc. significantly increases the efficiency of the business. Many services use pictures called CAPTCHAs in order to prevent automated use of these services.

Solve CAPTCHAs with the help of this portal, increase your business efficiency now!

Follow these steps:
- Register
- Login and follow the link inside to load funds to your account. Your request will be processed ASAP.

You pay for correctly recognized CAPTCHAs only
The price is $2 for 1000 CAPTCHAs. We accept payments from $10.

If you use a third-party software the price could be different, contact the software vendor for more information.

Hi! I want to bypass captcha from my bots. Bots have different IPs. Is it possible to use your service from many IPs?
We have no restrictions about IP: with DeCaptcha you can bypass CAPTCHA from as many IPs as you need.

Hi. I need to crack captcha. Do you provide a captcha decoders?
DeCaptcha CAPTCHA solving is processed by humans. So the accuracy is much better than an automated captcha solver ones.
<table>
<thead>
<tr>
<th>Language</th>
<th>Example</th>
<th>AG</th>
<th>BC</th>
<th>BY</th>
<th>CB</th>
<th>DC</th>
<th>IT</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>one two three</td>
<td>51.1</td>
<td>37.6</td>
<td>4.76</td>
<td>40.6</td>
<td>39.0</td>
<td>62.0</td>
<td>39.2</td>
</tr>
<tr>
<td>Chinese (Simp.)</td>
<td>— — — —</td>
<td>48.4</td>
<td>31.0</td>
<td>0.00</td>
<td>68.9</td>
<td>26.9</td>
<td>35.8</td>
<td>35.2</td>
</tr>
<tr>
<td>Chinese (Trad.)</td>
<td>— — — —</td>
<td>52.9</td>
<td>24.4</td>
<td>0.00</td>
<td>63.8</td>
<td>30.2</td>
<td>33.0</td>
<td>34.1</td>
</tr>
<tr>
<td>Spanish</td>
<td>uno dos tres</td>
<td>1.81</td>
<td>13.8</td>
<td>0.00</td>
<td>2.90</td>
<td>7.78</td>
<td>56.8</td>
<td>13.9</td>
</tr>
<tr>
<td>Italian</td>
<td>uno due tre</td>
<td>3.65</td>
<td>8.45</td>
<td>0.00</td>
<td>4.65</td>
<td>5.44</td>
<td>57.1</td>
<td>13.2</td>
</tr>
<tr>
<td>Tagalog</td>
<td>isá dalawa tattó</td>
<td>0.00</td>
<td>5.79</td>
<td>0.00</td>
<td>0.00</td>
<td>7.84</td>
<td>57.2</td>
<td>11.8</td>
</tr>
<tr>
<td>Portuguese</td>
<td>um dois três</td>
<td>3.15</td>
<td>10.1</td>
<td>0.00</td>
<td>1.48</td>
<td>3.98</td>
<td>48.9</td>
<td>11.3</td>
</tr>
<tr>
<td>Russian</td>
<td>один два три</td>
<td>24.1</td>
<td>0.00</td>
<td>0.00</td>
<td>11.4</td>
<td>0.55</td>
<td>16.5</td>
<td>8.76</td>
</tr>
<tr>
<td>Tamil</td>
<td>தமிழ் தோல்</td>
<td>2.26</td>
<td>21.1</td>
<td>3.26</td>
<td>0.74</td>
<td>12.1</td>
<td>5.36</td>
<td>7.47</td>
</tr>
<tr>
<td>Dutch</td>
<td>een twee drie</td>
<td>4.09</td>
<td>1.36</td>
<td>0.00</td>
<td>0.00</td>
<td>1.22</td>
<td>31.1</td>
<td>6.30</td>
</tr>
<tr>
<td>Hindi</td>
<td>एक दो तीन</td>
<td>10.5</td>
<td>5.38</td>
<td>2.47</td>
<td>1.52</td>
<td>6.30</td>
<td>9.49</td>
<td>5.94</td>
</tr>
<tr>
<td>German</td>
<td>eins zwei drei</td>
<td>3.62</td>
<td>0.72</td>
<td>0.00</td>
<td>1.46</td>
<td>0.58</td>
<td>29.1</td>
<td>5.91</td>
</tr>
<tr>
<td>Malay</td>
<td>satu dua tiga</td>
<td>0.00</td>
<td>1.42</td>
<td>0.00</td>
<td>0.00</td>
<td>0.55</td>
<td>29.4</td>
<td>5.23</td>
</tr>
<tr>
<td>Vietnamese</td>
<td>một hai ba</td>
<td>0.46</td>
<td>2.07</td>
<td>0.00</td>
<td>0.00</td>
<td>1.74</td>
<td>18.1</td>
<td>3.72</td>
</tr>
<tr>
<td>Korean</td>
<td>일 이 삼</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>20.2</td>
<td>3.37</td>
</tr>
<tr>
<td>Greek</td>
<td>ἕβα δύο τριά</td>
<td>0.45</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>15.5</td>
<td>2.65</td>
</tr>
<tr>
<td>Arabic</td>
<td>ثلاثة اثنين واحد</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>15.3</td>
<td>2.56</td>
</tr>
<tr>
<td>Bengali</td>
<td>এক দুই তিন</td>
<td>0.45</td>
<td>9.89</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>1.72</td>
<td></td>
</tr>
<tr>
<td>Kannada</td>
<td>ಕನ್ನಡ ತೆರೆ</td>
<td>0.91</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.55</td>
<td>6.14</td>
<td>1.26</td>
</tr>
<tr>
<td>Klingon</td>
<td></td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>1.12</td>
<td>0.19</td>
<td></td>
</tr>
<tr>
<td>Farsi</td>
<td>سه دو یک</td>
<td>0.45</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.08</td>
</tr>
</tbody>
</table>

Table 2: Percentage of responses from the services with correct answers for the language CAPTCHAs.
These Days:
CAPTCHAs are ways of \textit{training} AI systems