Web Security: CSRF defenses; Phishing attacks

CS 161: Computer Security

Prof. Raluca Ada Popa

April 15, 2020

Some content adapted from materials by Dan Boneh
• Starting recording
• TA Toby Chen checking chat
• Project 3 part 1 due on 4/17 at 11:59pm (extended)
• HMW3b released, due 4/24
• Will release Proj 3, part 2, by Friday
Recall: CSRF attack

www.attacker.com

GET /blog HTTP/1.1

www.bank.com

Victim Browser

Cookie: SessionID=523FA4cd2E
Recall: CSRF attack

www.attacker.com

GET /blog HTTP/1.1

Victim Browser

POST /transfer HTTP/1.1
Referer: http://www.attacker.com/blog
Recipient=attacker&amount=$100
Cookie: SessionID=523FA4cd2E

HTTP/1.1 200 OK
Transfer complete!

www.bank.com
CSRF Defenses

• CSRF token

• Referer Validation

• Others (e.g., custom HTTP Header) we won’t go into
CSRF token

1. bank.com server wants to protect itself from CSRF attacks, so it includes a secret token into the webpage (e.g., in forms as a hidden field)

2. Requests to bank.com include the secret

3. bank.com server checks that the token embedded in the webpage is the expected one; reject request if not

Can the token be?

- 123456
- Dateofbirth

No, CSRF token must be hard to guess by the attacker
How the token is used

- The server stores state that binds the user's CSRF token to the user's session token
- Embeds a fresh CSRF token in every form
- On every request the server validates that the supplied CSRF token is associated with the user's session token
- Disadvantage is that the server needs to maintain a large state table to validate the tokens.
Regular use

cookie for bank.com: 
**SessionID = 523FA4cd2E**

GET page

page with form hidden field 
CSRF 198..

Victim Browser

www.bank.com

<table>
<thead>
<tr>
<th>Session ID</th>
<th>CSRF token</th>
</tr>
</thead>
<tbody>
<tr>
<td>523..</td>
<td>198..</td>
</tr>
</tbody>
</table>
Invalid CSRF token doesn't know CSRF token for victim's session (one might not even be set at the server if the user did not request the form recently)
Other CRSF protection: Referer Validation

- When the browser issues an HTTP request, it includes a referer header that indicates which URL initiated the request.
- This information in the Referer header could be used to distinguish between same site request and cross site request.
Refer header

GET /blog HTTP/1.1

POST /transfer HTTP/1.1
Referer: http://www.attacker.com/blog
recipient=attacker
amount=$100
Cookie: SessionID=523FA4cd2E

HTTP/1.1 200 OK
Transfer complete!
Referer Validation

Facebook Login

For your security, never enter your Facebook password on sites not located on Facebook.com.

Email: 
Password: 

Remember me
Login or Sign up for Facebook

Forgot your password?
Referer Validation Defense

• HTTP Referer header
  – Referer: http://www.facebook.com/ ✔
  – Referer: [empty] ❓
    • Strict policy disallows (secure, less usable)
    • Lenient policy allows (less secure, more usable)
Privacy Issues with Referer header

- The referer contains sensitive information that impinges on the privacy
- The referer header reveals contents of the search query that lead to visit a website.
- Some organizations are concerned that confidential information about their corporate intranet might leak to external websites via Referer header
Referer Privacy Problems

• Referer may leak privacy-sensitive information


• Common sources of blocking:
  – Network stripping by the organization
  – Network stripping by local machine
  – Stripped by browser for HTTPS -> HTTP transitions
  – User preference in browser
Summary: CSRF

• CSRF attacks execute request on benign site because cookie is sent automatically

• Defenses for CSRF:
  – embed unpredictable token and check it later
  – check referer header in addition as defense in depth
Authentication & Impersonation
Authentication

- Verifying someone really is who they say they claim they are
- Web server should authenticate client
- Client should authenticate web server
Impersonation

• Pretending to be someone else
• Attacker can try to:
  – Impersonate client
  – Impersonate server
Authenticating users

• How can a computer authenticate the user?
  – “Something you know”
    • e.g., password, PIN
  – “Something you have”
    • e.g., smartphone, ATM card, car key
  – “Something you are”
    • e.g., fingerprint, iris scan, facial recognition
Recall: two-factor authentication

Authentication using two of:

- Something you know (account details or passwords)
- Something you have (tokens or mobile phones)
- Something you are (biometrics)
Example

Are these good 2FAs?

Online banking:
– Hardware token or card ("smth you have")
– Password ("smth you know")

Mobile phone two-factor authentication:
- Password ("smth you know")
- Code received via SMS ("smth you have")

Email authentication:
- Password
- Answer to security question

This is not two-factor authentication because both of the factors are something you know
After authenticating..

• Session established
  – Session ID stored in cookie
  – Web server maintains list of active sessions (sessionID mapped to user info)

• Reauthentication happens on every http request automatically
  – Recall that every http request contains cookie
After authenticating...

Alice

sessionID = 3458904043

Must be unpredictable

Server

Active sessions:

<table>
<thead>
<tr>
<th>sessionID</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>3458904043</td>
<td>Alice</td>
</tr>
<tr>
<td>5465246234</td>
<td>Bob</td>
</tr>
</tbody>
</table>

What can go wrong over http?

Session hijacking attack:
  • Attacker steals sessionID, e.g., using a packet sniffer
  • Impersonates user
After authenticating...

Alice

sessionID = 3458904043
Must be unpredictable

Protect sessionID from packet sniffers:
• Send encrypted over HTTPS
• Use secure flag to ensure this

When should session/cookie expire?
• Often is more secure
• But less usable for user

What other flags should we set on this cookie?
• httponly to prevent scripts from getting to it

Active sessions:
3458904043 | Alice
5465246234 | Bob
After authentication...

sessionID = 3458904043
Must be unpredictable

Active sessions:
3458904043 | Alice
5465246234 | Bob

What if attacker obtains old sessionID somehow?

• When user logs out, server must remove Alice’s entry from active sessions
• Server must not reuse the same session ID in the future
• Old sessionID will not be useful
Authenticating the server

What mechanism we learned about that helps prevent an attacker from impersonating a server?

• Digital certificates (assuming CA or relevant secret keys were not compromised)

But these only establish that a certain host a user visits has a certain public key. What if the user visits a malicious host?
Phishing attacks
Phishing attack

• Attacker creates fake website that appears similar to a real one
• Tricks user to visit site (e.g. sending phishing email)
• User inserts credentials and sensitive data which gets sent to attacker
• Web page then directs to real site or shows maintenance issues
Please fill in the correct information for the following category to verify your identity.

**Security Measures**

**Email address:**

**PayPal Password:**

**Full Name:**

**SSN:**

**Card Type:**

**Card Number:**

**Expiration Date:**

**Card Verification Number (CVV2):**

**Street:**

**City:**

**Country:**

**Zip Code:**

**Telephone:**

**Verified By Visa / Mastercard Securecode:**

**Date of Birth:**

(Ex: dd-mm-yyyy)

---

**Protect Your Account Info**

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

For more information on protecting yourself from fraud, please review our Security Tips at [http://www.paypal.com/securitytips](http://www.paypal.com/securitytips)

---

**Protect Your Password**

You should **never** give your PayPal password to anyone, including PayPal employees.

---

**Submit Form**
http://ebay.attacker.com/
Welcome to eBay

Ready to bid and buy? Register here

Join the millions of people who are already a part of the eBay family. Don't worry, we have room for one more.

Register as an eBay Member and enjoy privileges including:

- Bid, buy and find bargains from all over the world
- Shop with confidence with PayPal Buyer Protection
- Connect with the eBay community and more!

Sign in to your account

Back for more fun? Sign in now to buy, bid and sell, or to manage your account.

User ID: bieber
I forgot my user ID

Password: ************
I forgot my password

[ ] Keep me signed in for today. Don't check this box if you're at a public or shared computer.

Sign in

Having problems with signing in? Get help.

Protect your account: Create a unique password by using a combination of letters and numbers that are not
Please confirm your identity jbieber

Please answer security question below.

What is your mother’s maiden name?

Smith

Answer the secret question you provided.

What is your other eBay user ID or another’s member in your household?

NA

What email used to be associated with this account?

bieberlicious@hotmail.com

Have you ever sold something on eBay?

No
Thanks jbieber. Your identity has been confirmed.

Now you can pick up where you left off.

Save Profile
http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&item=350121605127&Category=1472188_trkparms=algo=

This listing (350121605127) has been removed, or this item is not available.

- Please check that you've entered the correct item number
- Listings that have ended 90 or more days ago will not be available for viewing.
How can you prevent phishing?
Phishing prevention

• User should check URL they are visiting!

http://ebay.attacker.com/
Does not suffice to check what it says you click on

Now go to Google!  
[http://google.com](http://google.com)

Because it can be:
<a src="http://attacker.com">http://google.com</a>

Check the address bar!
URL obfuscation attack

• Attacker can choose similarly looking URL with a typo

bankofamerca.com
bankofthevvest.com
Homeograph attack

- Unicode characters from international alphabets may be used in URLs
  paypal.com (first p in Cyrillic)
- URL seems correct, but is not

Another example:
www.pnc.com/webapp/unsec/homepage.var.cn
"pnc.com/webapp/unsec/homepage" is one string
to be continued…