

CS 378 - Network Security and Privacy

Fall 2007

Project #1

Due: 3:30pm CDT, October 16, 2007

Submission instructions

Follow the instructions in the project description.

If you are submitting late, please indicate how many late days you are using.

Collaboration policy

This assignment can be done individually or in two-person teams. Any cheating (*e.g.*, submitting another person's work as your own, or permitting your work to be copied) will automatically result in a failing grade. The Computer Sciences department code of conduct can be found at <http://www.cs.utexas.edu/users/ear/CodeOfConduct.html>

Late submission policy

This project is due at the **beginning of class on October 16**. All late submissions will be subject to the following policy.

You start the semester with a credit of 4 late days. For the purpose of counting late days, a "day" is 24 hours starting at 3:30pm on the assignment's due date. Partial days are rounded up to the next full day. You are free to divide your late days among the take-home assignments (3 homeworks and 2 projects) any way you want: submit four assignments 1 day late, submit one assignment 4 days late, *etc.* After your 4 days are used up, no late submissions will be accepted and you will automatically receive 0 points for each late assignment.

Project #1 (50 points + 5 bonus points)

KeyCorp Security, Inc. is all about the keys. Our state-of-the-art KeyRing service allows a group of friends to share their public keys with each other using a central repository.

The KeyRing server is located at this URL:

```
http://www.cs.utexas.edu/~anand/keyring
```

To log into the KeyRing server and view or edit your key, type in your UT EID. The key is a 1024-bit value, represented as 256 hex-encoded characters. When you edit your key, the server strips out all characters from the key except digits and lower-case letters from 'a' to 'f'. The server also ensures that the key is no longer than 256 characters.

You can view anybody's public key by using their UT EID.

Attack #1: Cross Site Request Forgery (15 points)

Create a malicious HTML page that should work as follows. Suppose the victim has logged into the KeyRing server, and, while still logged in, visits your HTML page. Your page should overwrite the victim's public key stored on the KeyRing server with a hex-encoded 256-character random value.

Important: The victim should not see the URL or the content of the malicious HTML page. Assuming that the victim clicks on a link from a page located at URL X to the malicious page located at URL Y , the victim should see only a page on the KeyCorp website, **not** the address or content of the Y page. (It is Ok if the browser displays Y for a fraction of a second before it finishes fetching the KeyCorp page.)

Attack #2: Cross Site Scripting (35 points + 5 bonus points)

The victim has logged into the KeyRing server. Create a URL that looks like this (with EVILMAGIC replaced by your exploit):

```
http://www.cs.utexas.edu/~anand/keyring/users.php?user=EVILMAGIC
```

When the logged in victim visits this URL, the victim's KeyRing cookie should get sent by email to `cs378ta@gmail.com`

The email with the cookie should contain words `stolen cookie` in the subject line. In addition to the cookie, the body of the message should also include the names of the team members who staged the attack.

The user should notice no difference in the behavior or appearance of the web page compared to simply typing a username into the text box on `http://www.cs.utexas.edu/~anand/keyring/users.php` and hitting Enter. (The source of the page can be arbitrarily different, but it should look and feel exactly the same.)

Important: While you can technically satisfy the wording of the problem by redirecting the user to `http://www.cs.utexas.edu/~anand/keyring/users.php?user=victim` after stealing the cookie, this is not what we're looking for. You **must** exploit the way that the username variable is used in the PHP script.

In particular, your attack code must:

- Pull the victim's record from the database using the SQL query on lines 20-21 of `users.php` (therefore, SQL must not barf on being given a query constructed from the username part of your URL).
- Result in the correct username (`victim`) being displayed in the input field on the user page. Thus, when the PHP code spits back the username you gave it on line 13 of `users.php`, it must somehow render as `victim`. It should be **exactly** that string—you cannot have more text hidden beyond the whitespace in the input box.
- Display the user's name and key in the area below. Your code should also somehow ensure that even though the username you supplied is a long and ugly string, it should render as `victim` in this part of the page as well.

To summarize, your attack should, without redirection, result in a page that looks exactly like the page `http://www.cs.utexas.edu/~anand/keyring/users.php?user=victim`

The HTML source will be different, and so will the address bar (it will be your malicious URL) but the content of the page should look and behave the same.

Tip: You are allowed to hardcode the string `victim` wherever you want. You cannot, however, hardcode the value of the key; it should be retrieved from the database. You will probably need to understand and exploit the manner in which the value of the key is encoded into the HTML page and how the Javascript retrieves it.

Partial credit: If you are not able to email the cookie, at least display it in a pop-up alert. If you are not able to make the page look exactly the same, make it look approximately the same. At the very least, try to make sure that your URL does not result in the "Cannot find that user" warning.

Bonus (5 points)

The team with the **shortest** URL that implements the full attack #2 gets 5 bonus points.

Deliverables

Send a *single* email message to `cs378ta@gmail.com`, containing words **project 1 solution** in the subject line. The body of the message should include the names of the project team members and late days used (if any). The message should have the following attachments:

- Your malicious HTML page (the entire page, not just the URL) implementing attack #1.
- Text file with your malicious URL implementing attack #2.

Notes

- The source code of the KeyRing website is available for your viewing pleasure at <http://www.cs.utexas.edu/~anand/keyring.tgz>
- We will be testing your attacks with a Firefox 2.0 browser. The database will have a sole user named `victim`.
- Please do not log into the KeyRing server with a UT EID other than your own. In the unlikely event that this becomes a problem, random passwords will be assigned.
- Don't worry about spamming `cs378ta@gmail.com` with test messages as you are experimenting with attack #2.