



OWASP

Open Web Application
Security Project

Bountiful Bugs and DRM Breakage

Dave Ferguson

OWASP Dallas chapter

January 19, 2016

About Me

- Developer for 12+ years
- Working in AppSec since 2006
 - Consultant / Pen tester
 - Solutions architect
 - Enterprise security role
- Netflix CSRF
- OWASP Forgot Password cheat sheet
- Blog at <http://appsecnotes.blogspot.com>

Agenda

- The bug hunting team
- Test cycles
- Bounties
- Sample of interesting cycles
- All your DRM are belong to us

Part I

BOUNTIFUL BUGS

TopGolf



From: Amber Martinez [<mailto:amartinez@utest.com>]
Sent: Thursday, March 06, 2014 12:47 PM
To: Siddiqui, Shamoun
Subject: TopGolf - Happy Hour - App Performance Testing

Hi Shamoun,,

uTest is hosting another Happy Hour in DFW towards the end of March. This will be great opportunity to network with industry peers, Eat-Drink-Play, as well as learn a bit about our comprehensive-cloud based solutions for Performance Testing. Feel free to forward this on to anyone on your team that might have an interest.

"A Better Way to Performance Test your Applications"

When: Wednesday, March 26th
Where: TopGolf - The Colony, TX
Time: 5:30-9:00pm

Agenda:

5:30-6:00 Networking
6:00-7:00 "A Better Way to Performance Test Your Applications"
7:00-9:00 Play TopGolf

RSVP to amartinez@utest.com.

Regards,
Amber Martinez
408-830-4748



The uTest Community

- Crowd-sourced testing model
- Vast majority of testing projects are functional (not security related)
- Company changed name to Applause in 2014
- "uTest" is now the community of testers
 - A professional network exclusively for software testers
 - 200,000 testers in 200+ countries

Ramping Up

- Bug bounty system
 - Testers are paid per valid bug reported in the platform
 - First come, first serve
- In the beginning
 - I tried functional testing (mobile apps). Not for me.
 - Security testing?



Test Cycles

- Announced via the uTest platform
- Specific testers invited → email notifications sent
- Basic description of the app
- What's in scope for testing
- Invited testers can accept or decline the cycle
- Testing window: Usually 5-10 days
- TTL = Test Team Lead

Test Cycle Roles


- The test team
- PM
 - For security cycles? Didn't do a whole lot.
- TTL
 - Did most PM-related tasks.
 - Answered questions about scope
 - Communicated w/client
 - Monitored & reviewed bug reports
 - Determined validity & value of bugs
 - Can reject bugs, which harms the tester's rating

The Platform

Dashboard Test Cycles Issues Test Cases Dave Ferguson

My uTest

Welcome back, Dave Ferguson



How's the weather in United States?

Test Cycles	63	Functional	34.72%
Issues	100	Security	81.3953%
Test Cases	52		
Products	49		
Favorites	0		

Test Cycles

Invited Pending Active Locked

Security Cycle - Jan 2015 Locked 15 Hours ago

Community News

- uPoints High Contest: Joining the School Paper
- uTest Quarterly Review - Hear What You Have Accomplished! Q4 2015
- uPoints High Contest Series: Most Well-Rounded
- Tester of the Quarter: Q4 2015

Your earnings: \$0.00 pending

Pending payments are payments for your approved work that will be paid out on the next payout cycle. Read more about [how payments work at uTest](#).

You currently do not have any pending payments.

My Tasks

Relax!

You do not have any urgent tasks. But you can still be productive!

- Check out your active test cycles and report high quality issues
- Take a course at the [uTest university](#) to improve your skills
- Find and review new tools to ease your testing
- Connect with other testers, team leads and community management [uTest forums](#)

Keep your devices up to date!

Be sure to update your devices frequently and make sure the environments listed in the uTest platform are correctly entered with the right OS version (for example Android & iOS update frequently). Many customers are especially interested in testers with the latest OS versions for testing purposes.

Are the following devices still accessible to you for testing and up-to-date?

Mobile Devices:

- HTC Evo 3D (Android 4.0.3): Wi-Fi
- Apple iPad Air Wi-Fi (iOS 8.2): Wi-Fi
- HTC One (M7) (Android 5.0.2): Sprint Nextel

Desktop Environments

- Windows (7 64-bit) Chrome
- Windows (10 64-bit) Chrome
- Linux (Ubuntu) Firefox

Check out the [Account & Settings > Hardware & Software](#) section to list your available hardware.

Update Devices Discard Message

Project Opportunities

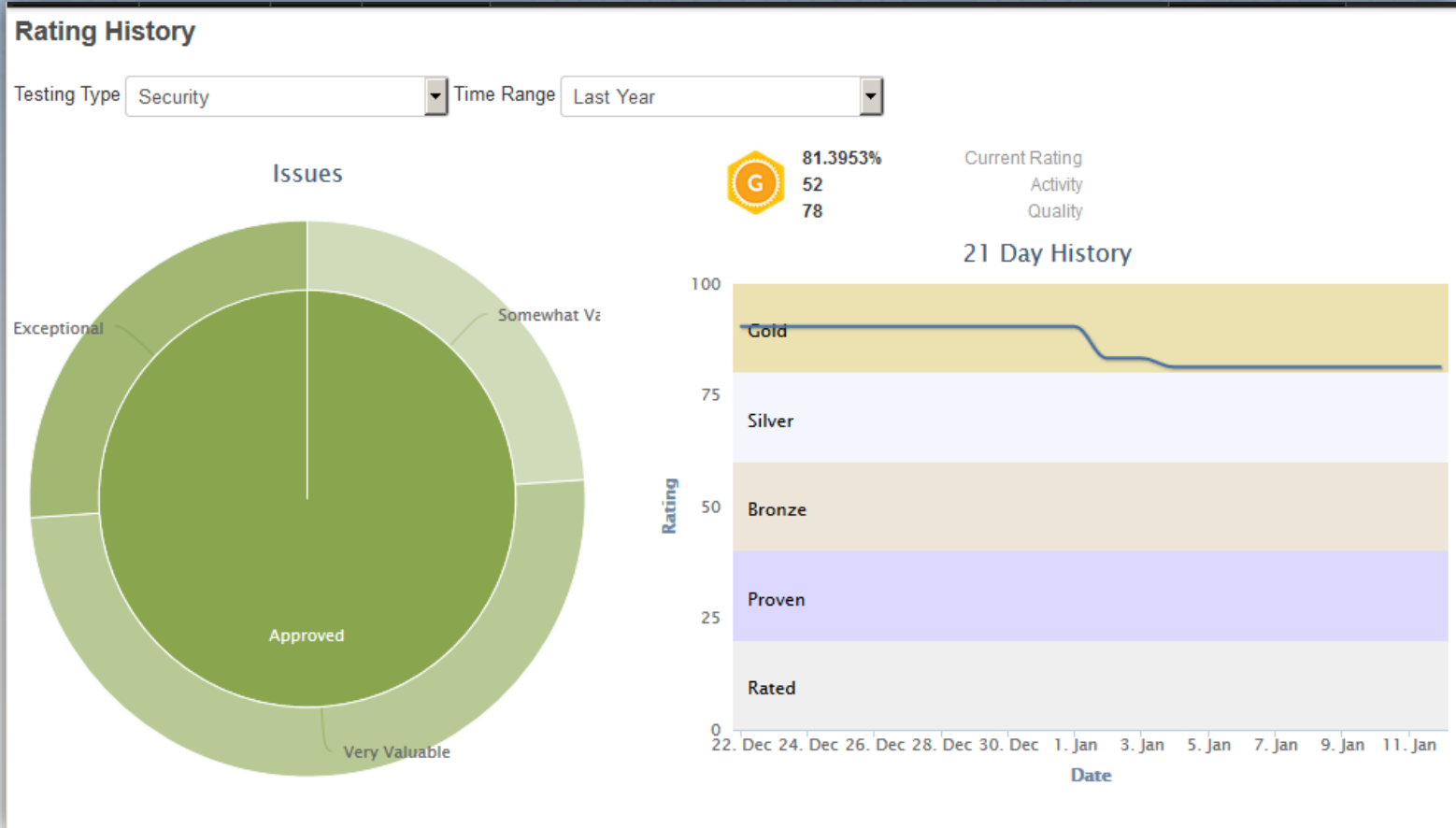
Projects Board

- Rating History
- Testing History
- Payments
- Account & Settings
- Customer UI
- Sign Out

Core Security Test Team



Rating the Testers



Bug Hunting for Fun & Profit

- Accept test cycles asap and start testing!
- Get bug reports in early! First to report gets the bounty.
- Valid security bugs: Anything that can negatively affect the CIA triad (unless out of scope)
- Bug reports visible to everyone on the team
- Evidence required
 - Screenshots (Jing)
 - Videos (Jing)
 - Request/Response pairs (Burp, Fiddler, ZAP, etc)
- When in doubt, report it!
 - Email disclosed in response, I missed a bounty

Bounty!

- Based on value of the reported bug, as determined by TTL
 - Somewhat valuable
 - Very valuable
 - Exceptionally valuable
- Payout for documented test cases
- Most Valuable Tester (MVT) awards

Example

AUTH - API keys do not expire

Issue Report #1454178 Submitted by [Dave Ferguson](#)

Action Performed

1. Logged in as user on April 10th and received an API key.
2. Attempted to use the same API key on April 13th and found that it was still valid.

Expected Result

Since almost 3 full days had passed, it was expected that the API key would have a reasonable expiry and therefore an error would be returned saying that the API key was not valid.

Actual Result

The API keys do not appear to have an expiry. Application security best practices dictate that authentication tokens should be invalidated on the server side after a reasonable period of inactivity (15 or 30 minutes for example). Furthermore, it is recommended to implement an "absolute" expiry (24 hours max lifetime for example) regardless if the token is being actively used.

Error Message

N/A

Link to remediation advice / Fix help

https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management



Additional Environment Info

Windows 7 with Burp Suite Pro. On April 10th, I was using Firefox. On April 13, I was using Chrome.

← 2 of 7 →

Status	Approved
Value	exceptionally valuable
Created	04/12/2015 at 11:09 PM
Modified	04/13/2015 at 03:19 PM
Build	Staging
Priority	Medium
Issue Type	A2-AUTH - Broken auth and sessi...
Frequency	Every Time
Integrity	Not Rated

Specified Environments

  Windows 7 64-bit - Firefox

Community Reproductions

Attachments

  4 kB request response.txt

Activity

A Bug Bounty Life

- Feeling the "rush" when you're close to finding a good vulnerability
- You're working as a team, but competing against each other at the same time
- Often not time to develop lengthy exploits
- You might not find anything 😞
- Your effective hourly rate will vary wildly

My Brief Stint as a TTL

- The Security TTL went on holiday
- Felt like I was back in consultant role
- Joined planning/kickoff call with client
- Gathered info about scope of testing & rules of engagement
- Confirmed test creds were working, etc.

Interesting Test Cycles

- NASA: Email communication system for astronauts
- Content valuation system with dynamic pricing (thick client)
- Video game buyback (eCommerce)
- TV video streaming service for Asians living in U.S. (DRM)
- Luxury watch maker (eCommerce)

Interesting Test Cycles, cont'd

- German supermarket chain (eCommerce)
- Social network with themed conversations
- A number of eBook retailers (DRM)
- **iPad** app for doctors (mobile)
- IP-based security **camera** and web UI control center

Special Projects

- Twice I was offered exclusive projects at an hourly rate
- Content valuation, dynamic pricing thick client
 - 15 hours
- Small, simple web app
 - 10 hours

Overall Thoughts

- Fantastic experience, enjoyed it very much
- Free evenings & weekends = \$\$\$
- Gained experience with new technologies
- Kept my pen testing skills sharp
- 1337 pen testing pwnage skillz recognized
 - Published an interview with me
 - Asked me to step in as TTL
 - Paid me to do a webinar for uTest University:
<https://www.utest.com/courses/recorded-webinar-introduction-security-testing-dave-ferguson>

Part II

DRM BREAKAGE

Random House

- Largest book publisher in the world
- Provides ***International Digital eBook Security Guidelines***
 - Included in "Account Interest Packet" for eBook retailers

RH eBook Security Guidelines

- Basic Objectives
 - Protect digital version of books as much as physical books
 - Protect books from being programmatically stripped and taken apart

DRM Schemes

- Adobe
 - "ADEPT", applied to EPUBs and PDFs
- Apple
 - "FairPlay", applied to EPUBs
- Amazon
- Marlin

Specific Guidelines

- DRM / eReader goals
 - URLs not enumerable or guessable
 - Limit the number of concurrent devices
 - Purchasing one book doesn't allow reengineering to gain access to a different book
 - No more than one page of text can be copied
 - Images cannot be easily extracted
 - Book cannot be forwarded to others
 - No more than 10% of book is available before purchase
- Website security
 - No XSS and SQL injection

EPUB - Common eBook format

- Free & open standard
- Mostly what we saw in test cycles
- DRM scheme is applied to an EPUB file
- An EPUB file is a zip file

Inspecting EPUB files

The image shows three overlapping windows of a text editor (TextPad) displaying XML code. The top window, titled 'encryption.xml', shows the following code:

```
<ds:RetrievalMethod Type="protocol" URI="HANCOM_KEK_BASED_ON_DEVICE:2.0"/>
</ds:KeyInfo>
<enc:CipherData>
<enc:CipherValue>VYiJKQwNO4y7u0KJ0JmTEO7vkF76Y/W7QwOqN7PR03afV550dcUQvBWFbh </enc:CipherValue>
</enc:CipherData>
<enc:EncryptionProperties>
<enc:Enc...
<hnc:Va...
<enc:Cip...
</hnc:Va...
</enc:En...
</enc:En...
<ds:Key...
<ds:Ret...
</ds:Key...
<enc:Cip...
<enc:Cip...
</enc:C...
</enc:En...
<enc:En...
<enc:En...
<ds:Key...
<ds:Ret...
</ds:Key...
<enc:Cip...
ex:context><o-ex:uid type="Har...
<enc:Cip...
ex:context></o-ex:hardware><o-...
ex:end>9999-12-31T23:59:59</o-...
</enc:En...
<enc:En...
<enc:En...
<ds:Key...
<ds:Ret...
</ds:Key...
<enc:Cip...
</o-dd:register>
<enc:Cip...
</o-ex:requirement>
</enc:C...
</enc:En...
<enc:En...
</o-ex:rights>
```

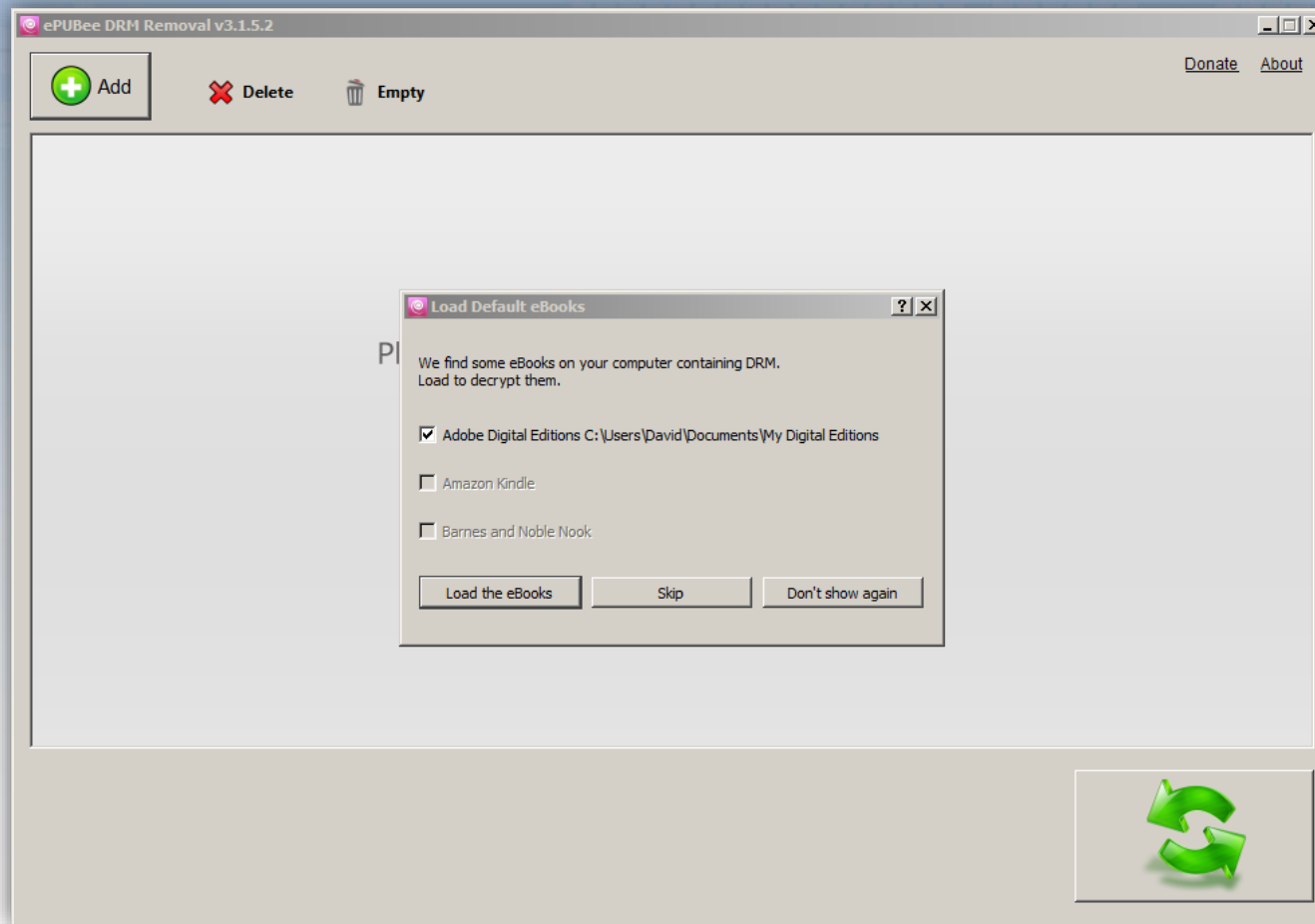
The middle window, titled 'rights.xml', shows the following code:

```
ex:uid>17768/1.css</o-ex:uid><o-ex:uid>17768/0.css</o-ex:uid><o-ex:uid>
17768/www. .org@files@17768@17768-h@17768 </o-ex:uid><o-ex:uid>
17768/www. .org@files@17768@17768-h@17768 </o-ex:uid></o-ex:context>
<enc:Enc...
</o-ex:asset>
<enc:Enc...
<o-ex:permission>
<ds:Key...
<o-dd:copy/>
<ds:Ret...
<hnc:changeRights/>
</ds:Key...
</o-ex:permission>
<enc:Cip...
<o-ex:constraint>
<enc:Cip...
<o-dd:software>
</enc:C...
<o-ex:context>
<enc:En...
<o-dd:uid>HANCOM_DRM_CLIENT AG...
<enc:En...
<o-dd:version>2.0</o-dd:versi...
</o-ex:context>
<ds:Key...
</o-dd:software>
<ds:Ret...
<o-ex:individual><o-ex:context...
</ds:Key...
type="UserID" ebook4</o-e...
ex:context><o-ex:uid type="Har...
<enc:Cip...
ex:context></o-ex:hardware><o-...
ex:end>9999-12-31T23:59:59</o-...
</enc:En...
<enc:En...
<enc:En...
<o-dd:register>
<o-ex:context>
<ds:Key...
<o-dd:uid hnc:type="ServerURL"
<ds:Ret...
<o-dd:uid hnc:type="Protocol">
</ds:Key...
</o-ex:context>
<enc:Cip...
</o-dd:register>
<enc:Cip...
</o-ex:requirement>
</enc:C...
</enc:En...
</o-ex:agreement>
<enc:En...
</o-ex:rights>
```

The bottom window, titled 'signatures.xml', shows the following code:

```
<?xml version="1.0" encoding="UTF-8"?><!--
--><signatures xmlns="urn:oasis:names:tc:opendocument:xmlns:container">
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001
<SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsi
<Reference URI="#manifest-600175212">
<Transforms>
<Transform Algorithm="http://www.w3.org/TR/2001/REC-
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlen
<DigestValue>9WkSIJ+eE/ayp3nEjEUyYWC//kLXDX8zXDFKJg4cRGs
</Reference>
</SignedInfo>
<SignatureValue>qfAyMxOTNA01DX1VYtUeI2IiebyK3bZfEVzDDWib9jsSUEha
iJ+wtY0+R0quIobnw7ZbFj918LM1fdTSuG61o5PIXKxrBpYhgTBuzIPV9dHPWAm5
jXWci4czkb7bJep9KRT00NNGniGATbrfn2nBAtBksihIUjaPOXXsA0cpeiNmQfil
```

ePUBee DRM Removal Tool



ePUBee DRM Removal Tool

File Name | Size | Path | Status

	File Name	Size	Path	Status
1				ADEPT PDF
2				ADEPT PDF
3				ADEPT PDF
4				ADEPT PDF
5				ADEPT PDF
6				ADEPT PDF
7	The Client-1.epub	468 KB	C:\Users\David\AppData\Roaming\decrypt\The Client-1.epub	decrypted
8	The Client-2.epub	468 KB	C:\Users\David\AppData\Roaming\decrypt\The Client-2.epub	decrypted
9	The Client-3.epub	468 KB	C:\Users\David\AppData\Roaming\decrypt\The Client-3.epub	decrypted
10	The Client-4.epub	468 KB	C:\Users\David\AppData\Roaming\decrypt\The Client-4.epub	decrypted
11	The Client.epub	468 KB	C:\Users\David\AppData\Roaming\decrypt\The Client.epub	decrypted
12				Unknown DRM
13				---

Tested: HTML5 eReader

- Browser-based eBook reader
- Leverages HTML5 local storage (SQLite DB)
- Flaw allowed one person to buy a book and share it with others
- Exploit a little tedious, but worked

HTML5 eReader - Flaw

- Allows user A who has purchased eBooks to share them with user B
- User A provides his local SQLite file to user B, along with his encryption key (which is accessible by viewing HTTP requests)
- User B edits the SQLite database (using a tool like **SQLite Database Browser**)
- User B also edits an HTTP response after login to replace his encryption key with the encryption key given to him by user A

HTML5 eReader - Flaw

The screenshot shows the SQLite Database Browser interface. The table 'eReaderCache' is displayed with the following columns: ID, principal, data, and added_on. A red box highlights the 'principal' column with the text: "This column edited to hold the value for user B instead of the value for user A." The table contains 13 rows of data, each with a unique ID, a principal value, a data value (mostly (BLOB)), and an added_on timestamp.

ID	principal	data	added_on
1	pubList	(BLOB)	Mon Jun 09 2014 20:10:42 GMT-05...
2	e44d1d6f-a9d0-4780-9249-7531e7ca2...	AAAAEP1uNv7GSBSxAE/z1KFFLaIAAADLu1FScEN5/9KPhJyJHQAtq...	Mon Jun 09 2014 20:10:52 GMT-05...
3	e44d1d6f-a9d0-4780-9249-7531e7ca2...	(BLOB)	Mon Jun 09 2014 20:10:59 GMT-05...
4	ecec55bb-289b-4620-a794-cfc93823a5c8_drmmttk	AAAAEF4PQgbyuKqs2I9XkBNIBEOAAADLoszAU/e+MT0TS7mVF/uL+...	Mon Jun 09 2014 20:11:05 GMT-05...
5	ecec55bb-289b-4620-a794-cfc93823a5c8	(BLOB)	Mon Jun 09 2014 20:11:07 GMT-05...
6	00fc2215-6d8d-481a-b1c5-e0465818dee0_drmmttk	AAAAEMa2qJr/S/XMWYIDDJ/bwTQAAADLMHqgIIJIX5rV4ZQQStaSi...	Mon Jun 09 2014 20:11:11 GMT-05...
7	00fc2215-6d8d-481a-b1c5-e0465818dee0	(BLOB)	Mon Jun 09 2014 20:11:14 GMT-05...
8	6aa566ae-76a0-4c7b-b1ff-610d87ee36b2_drmmttk	AAAAEJVNRI9z8gC8cldPL2P2gMAAADLWyyvLNV63S4Yt6v4NAX31...	Mon Jun 09 2014 20:11:15 GMT-05...
9	6aa566ae-76a0-4c7b-b1ff-610d87ee36b2	(BLOB)	Mon Jun 09 2014 20:11:17 GMT-05...
10	dd38374a-edf4-44cb-9c41-ac7358b31244_drmmttk	AAAAEGsG9gUaTYJipPICW9sP6EkAAADL67YNNV1ZT5PwJbFPT0tEU...	Mon Jun 09 2014 20:11:20 GMT-05...
11	dd38374a-edf4-44cb-9c41-ac7358b31244	(BLOB)	Mon Jun 09 2014 20:11:22 GMT-05...
12	a4e697db-9809-4343-bc17-264701067771_drmmttk	AAAAEHM1gPi/qqWB17BqFpCgkMAAADLkJjKt3RpXtSu9eEjXCAAU...	Mon Jun 09 2014 20:11:26 GMT-05...
13	a4e697db-9809-4343-bc17-264701067771	(BLOB)	Mon Jun 09 2014 20:11:28 GMT-05...

HTML5 eReader - Flaw

REQUEST AFTER LOGIN BY USER B

GET /apireader/drm/user/key HTTP/1.1

Host: drm-abc.example.com

[...snip...]

Cookie: JSESSIONID=4073A0109DF932BB575854D488197176; sid=ebe0926d-e8be-4b66-8aad-45e885f44876

ORIGINAL RESPONSE

HTTP/1.1 200 OK

Server: nginx/1.5.12

Date: Tue, 10 Jun 2014 04:13:53 GMT

Content-Type: application/octet-stream

Connection: keep-alive

Content-Length: 44

DAS7fcMyet6j/iNac8j9Grgw0Mm1LmexCo1OZQQt+NM=

MODIFY RESPONSE TO SUBSTITUTE USER A'S ENCRYPTION KEY

HTTP/1.1 200 OK

Server: nginx/1.5.12

Date: Tue, 10 Jun 2014 04:13:53 GMT

Content-Type: application/octet-stream

Connection: keep-alive

Content-Length: 44

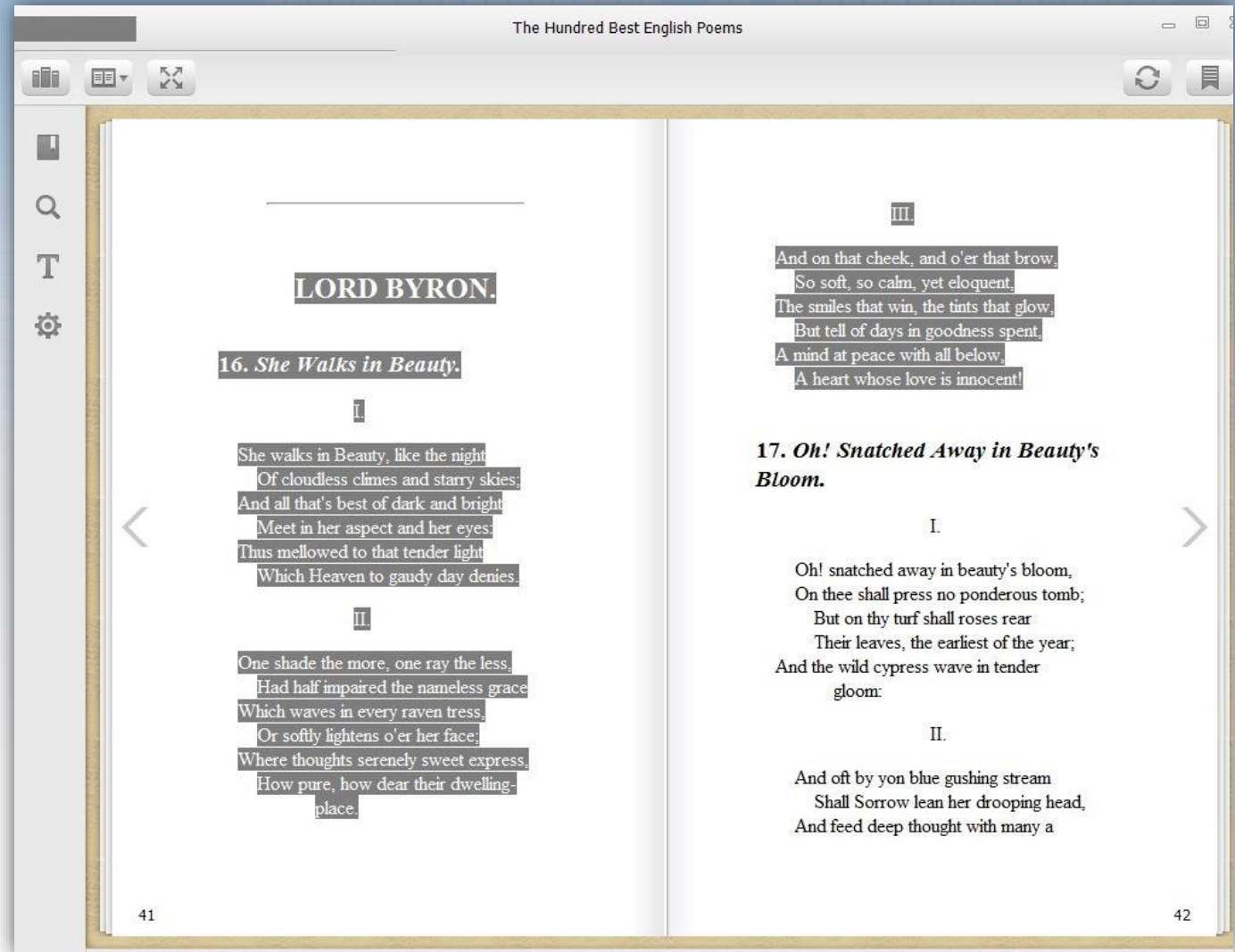
K5V5dVHLPJc65vM1Mljj4NPcYmcpXrwAubqf05zj91E=

HTML5 eReader - Flaw

The screenshot shows a web browser window with the address bar containing `https://drm/ereader/index.html#/`. The page title is "My Library" and there is a search bar labeled "Search all texts". The main content area features a book cover for "Anne of Green Gables" by L. M. Montgomery. A red arrow points to a red-bordered box containing the text: "Logged in as user B, who never downloaded this book." Below the book cover are two buttons: "CONTINUE READING" and "DOWNLOADED". At the bottom, there is a navigation bar with tabs for "A - Z", "Z - A", "LAST OPENED", and "AMOUNT READ". Below the navigation bar is a grid of book thumbnails. The first thumbnail is missing an image, showing "No image available." The other thumbnails are titled "The Adventures...", "The Adventures...", "The Adventures...", "Alice's Adventures...", "Allan and the Holy Flower", and "Allan Quaterm".

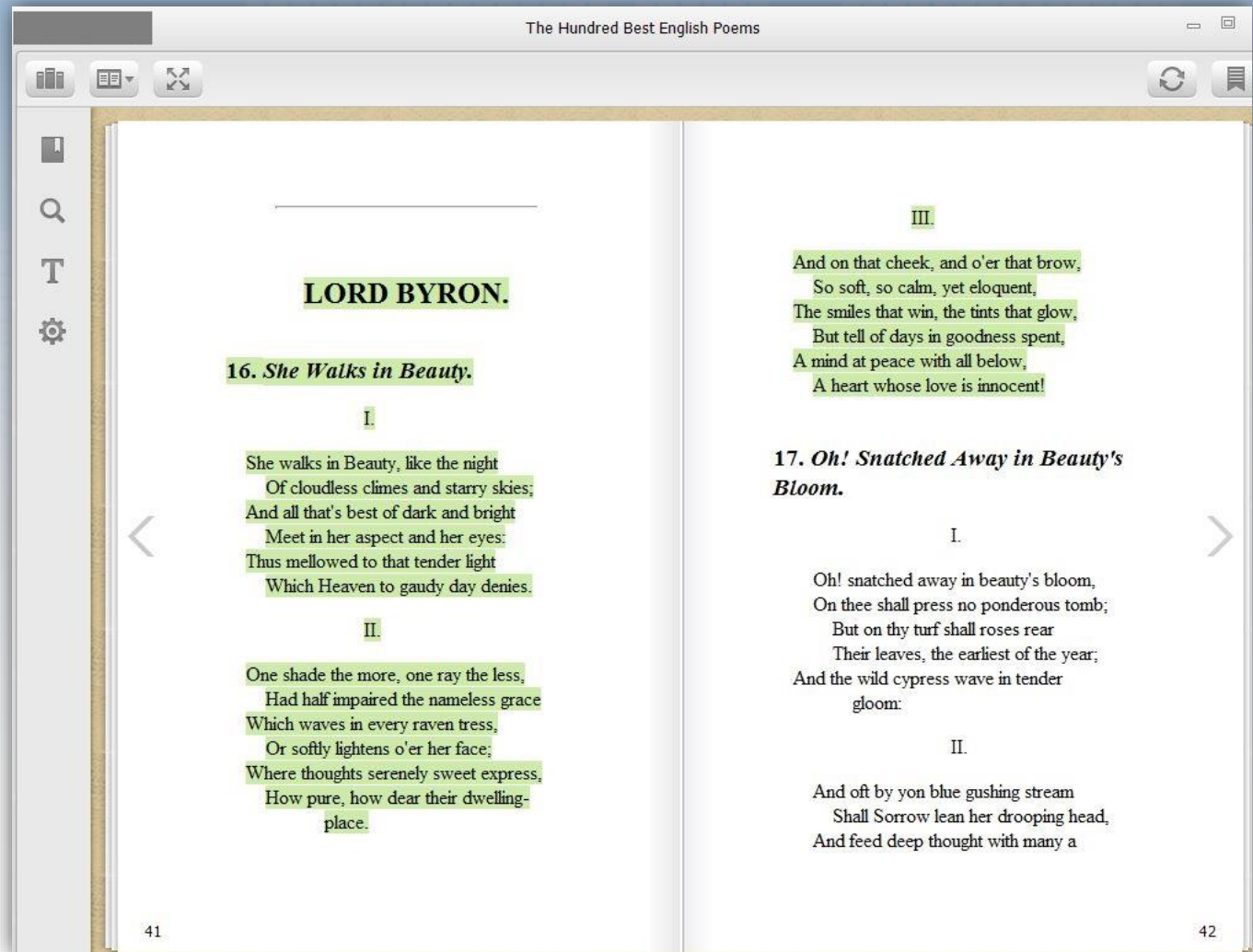
Tested: Thick Client eReader

Use Burp
invisible
proxy mode.
Select some
text.



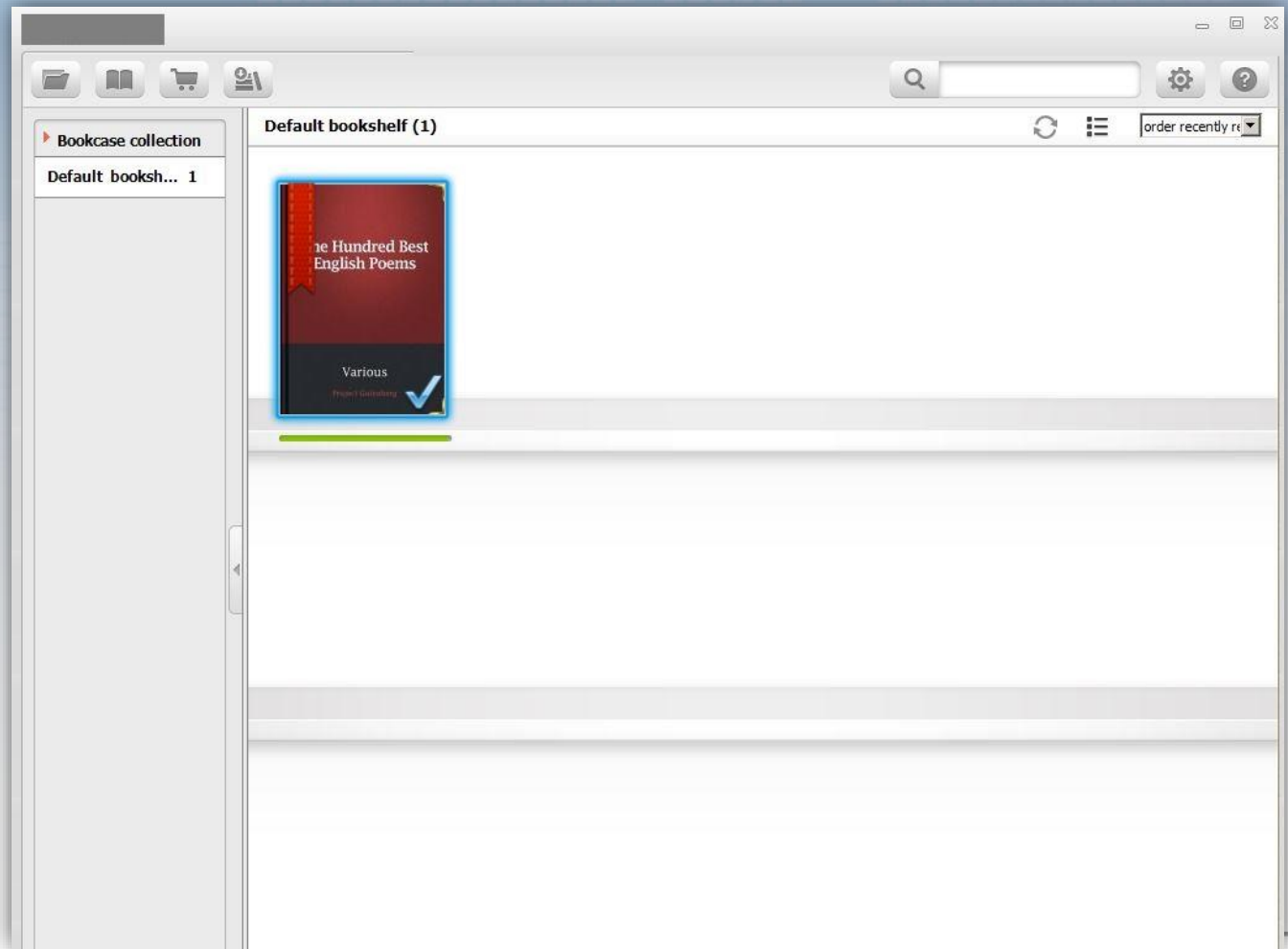
Thick Client eReader

Right click,
and choose
highlight.



Thick Client eReader

Return
book to
bookshelf
and exit
application



Thick Client eReader - Flaw

Inspect
Burp

Request Response

Raw Headers Hex

HTTP/1.1 200 OK
Server: Oracle-iPlanet-Web-Server/7.0
Date: Tue, 22 Apr 2014 05:52:56 GMT
Cache-control: no-cache
Content-length: 1561
Content-type: text/plain; charset=UTF-8
X-powered-by: Servlet/2.5 JSP/2.1

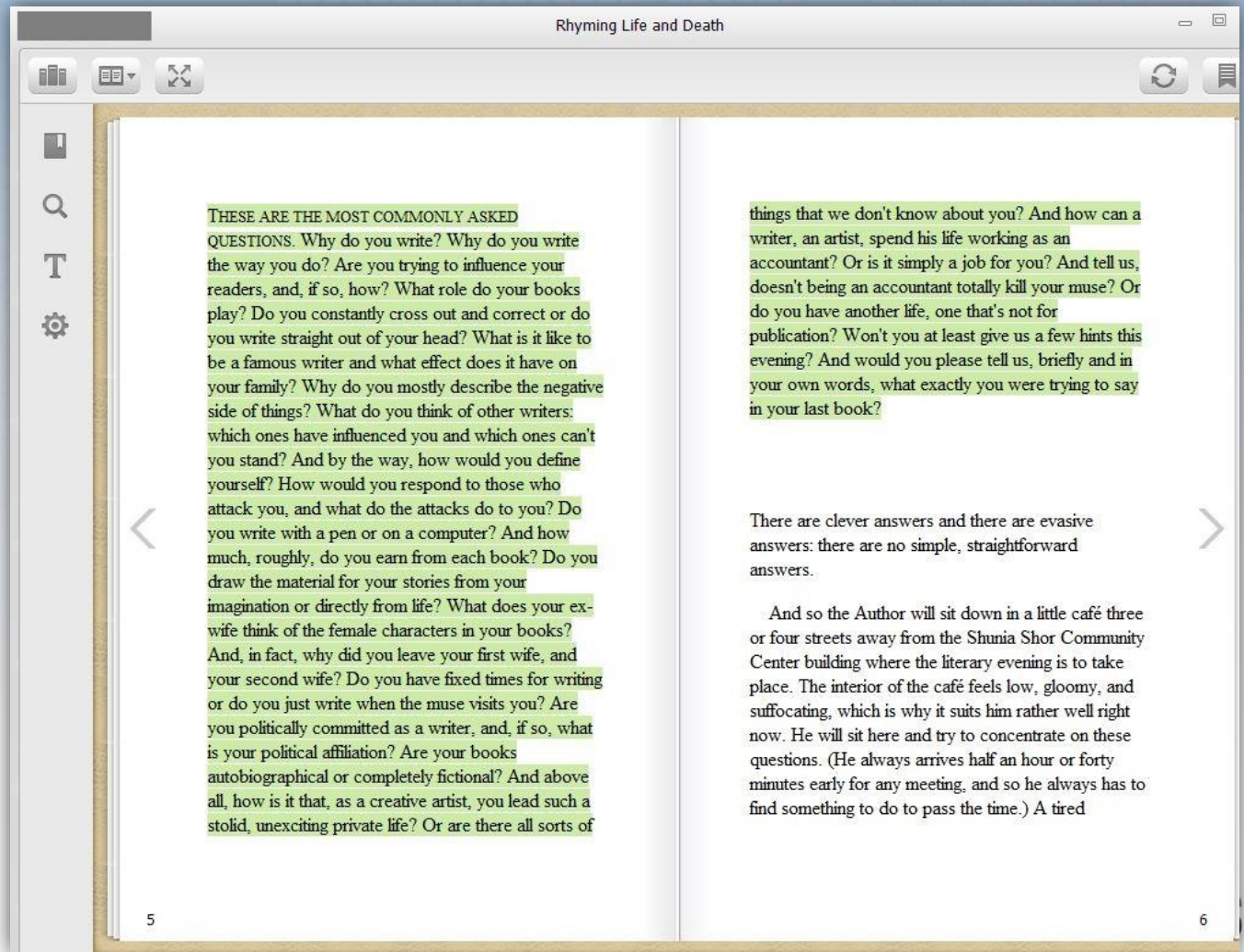
Start

End

```
[{"BOOKLIST":[{"LID":1,"DBINDEX":1044234,"VERSION":4,"DATALIST":[{"SYNCTYPE":1,"IDX_TODELETE":2232045,"OFFSET_STARTXPATH":0,"REGDATE":1398145853000,"ENDXPATH":"\\/HTML\\/BODY\\/DIV[22]\\/DIV\\/A[2]\\/SPAN[4]\\/text()", "SELECTEDTEXT":"LORD BYRON. 16. She Walks in Beauty. I. She walks in Beauty, like the night Of cloudless  
climes and starry skies; And all that's best of dark and bright Meet in her aspect and her eyes: Thus  
mellowed to that tender light Which Heaven to gaudy day denies. II. One shade the more, one ray the  
less, had half impaired the nameless grace Which waves in every raven tress, Or softly lightens o'er her  
face, where thoughts serenely sweet express, How pure, how dear their dwelling-place. III. And on that  
cheek and o'er that brow, So soft, so calm, yet eloquent, The smiles that win, the tints that glow, But  
tell of days in goodness spent, A mind at peace with all below, A heart whose love is  
innocent!", "STARTXPATH":"\\/HTML\\/BODY\\/H2[8]\\/A[2]\\/text()", "IDX_SYNCORLOCAL":0, "BACKCOLOR":"#c3e694", "IT  
EM_VERSION":0, "MEMO":"", "DATATYPE":3, "CHAPTERNUM":0, "DIV_UID":0, "OFFSET_ENDXPATH":31, "ONE_ROW_RESULT":tru  
e}], [{"SYNCTYPE":1, "IDX_TODELETE":0, "OFFSET_STARTXPATH":0, "REGDATE":0, "ENDXPATH": "", "SELECTEDTEXT": ""}], "STAR
```

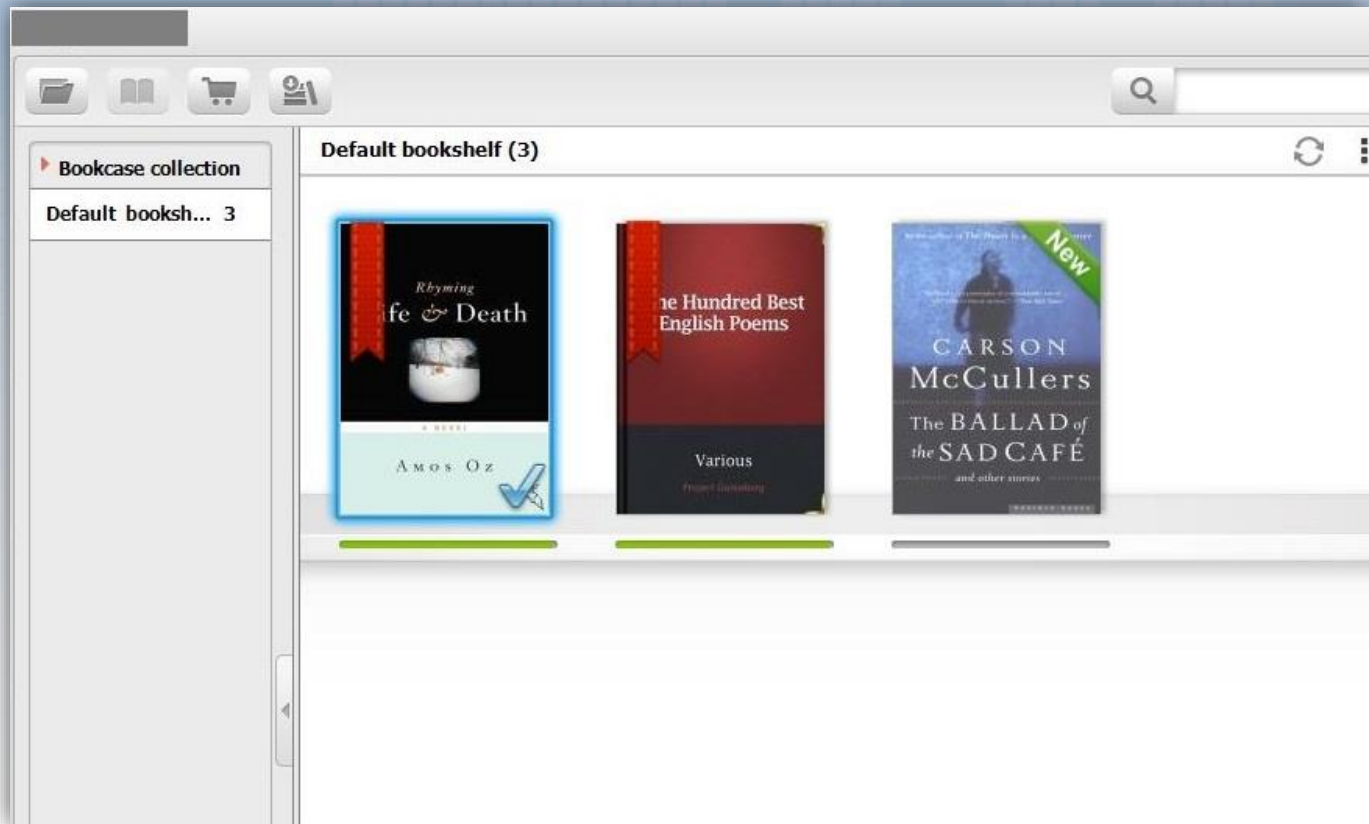
Thick Client eBook reader, flaw2

Highlight
text



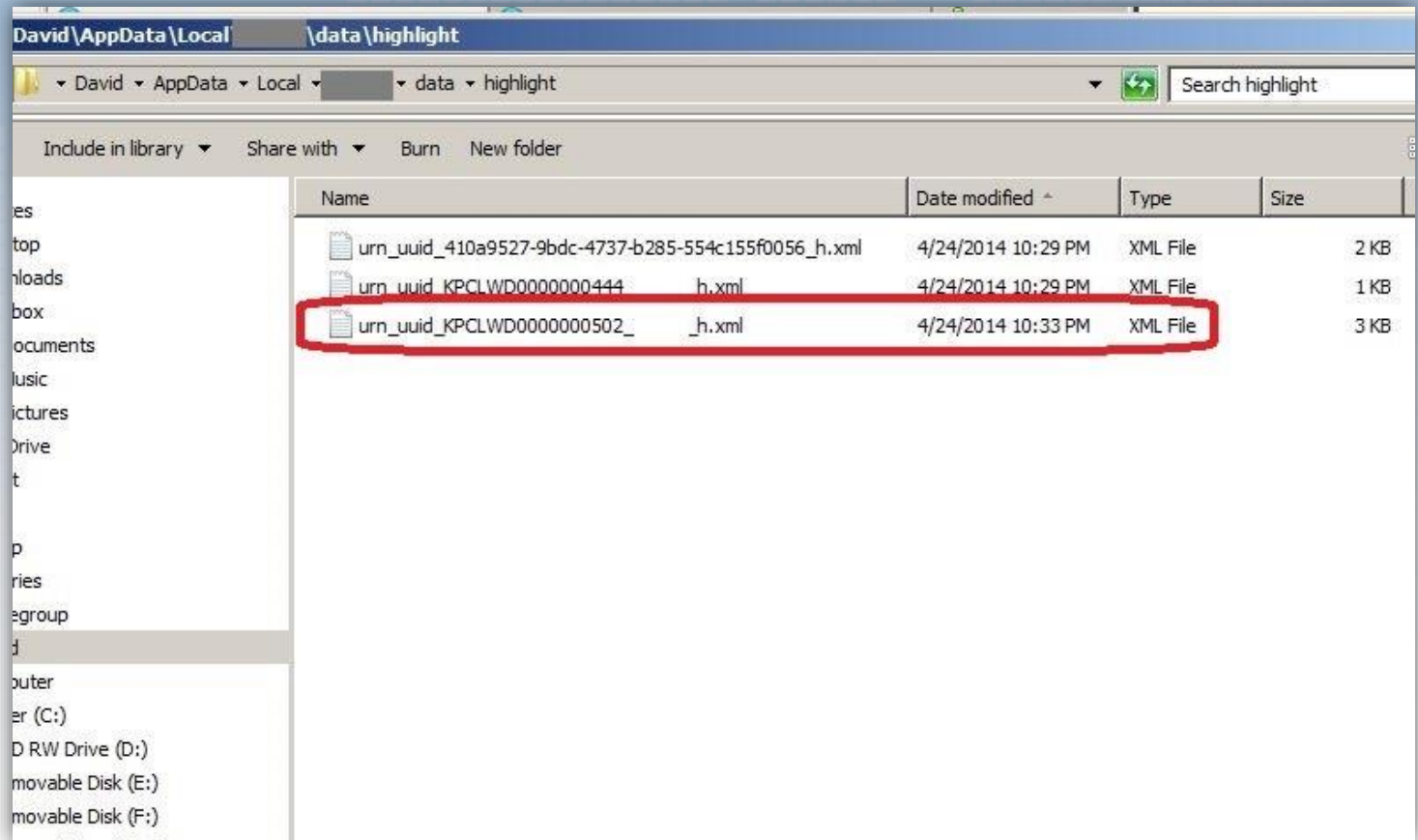
Thick Client eReader, flaw2

Return
book to
bookshelf



Thick Client eReader, flaw2

Find xml files under AppData directory



Thick Client eReader, flaw2

Open the most recent xml file

```
urn_uuid_KPCLWD0000000502... X
<?xml version="1.0" encoding="UTF-8"?>
<highlights xmlns:xsh="http://.../readon/highlights">
  <xsh:highlight id="Highlight_000">
    <contentFileIndex>2</contentFileIndex>
    <xpathstart><![CDATA[//BODY[0]/P[0]/#text[0]]></xpathstart>
    <xpathend><![CDATA[//BODY[0]/P[0]/#text[1]]></xpathend>
    <sentence><![CDATA[THESE ARE THE MOST COMMONLY ASKED QUESTIONS. Why do you
write? Why do you write the way you do? Are you trying to influence your
readers, and, if so, how? What role do your books play? Do you constantly cross
out and correct or do you write straight out of your head? What is it like to
be a famous writer and what effect does it have on your family? Why do you
mostly describe the negative side of things? What do you think of other
writers: which ones have influenced you and which ones can't you stand? And by
the way, how would you define yourself? How would you respond to those who
attack you, and what do the attacks do to you? Do you write with a pen or on a
computer? And how much, roughly, do you earn from each book? Do you draw the
material for your stories from your imagination or directly from life? What
does your ex-wife think of the female characters in your books? And, in fact,
why did you leave your first wife, and your second wife? Do you have fixed
times for writing or do you just write when the muse visits you? Are you
politically committed as a writer, and, if so, what is your political
affiliation? Are your books autobiographical or completely fictional? And above
all, how is it that, as a creative artist, you lead such a stolid, unexciting
private life? Or are there all sorts of things that we don't know about you?
And how can a writer, an artist, spend his life working as an accountant? Or is
it simply a job for you? And tell us, doesn't being an accountant totally kill
your muse? Or do you have another life, one that's not for publication? Won't
you at least give us a few hints this evening? And would you please tell us,
briefly and in your own words, what exactly you were trying to say in your last
book?]]></sentence>
  </xsh:highlight>
</highlights>
```



OWASP

Open Web Application
Security Project

THE END

Thank you for attending!

 @_sc0rn

gmdavef at gmail