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

OWASP
Open Web Application Security Project

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

OWASP
Open Web Application Security Project

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

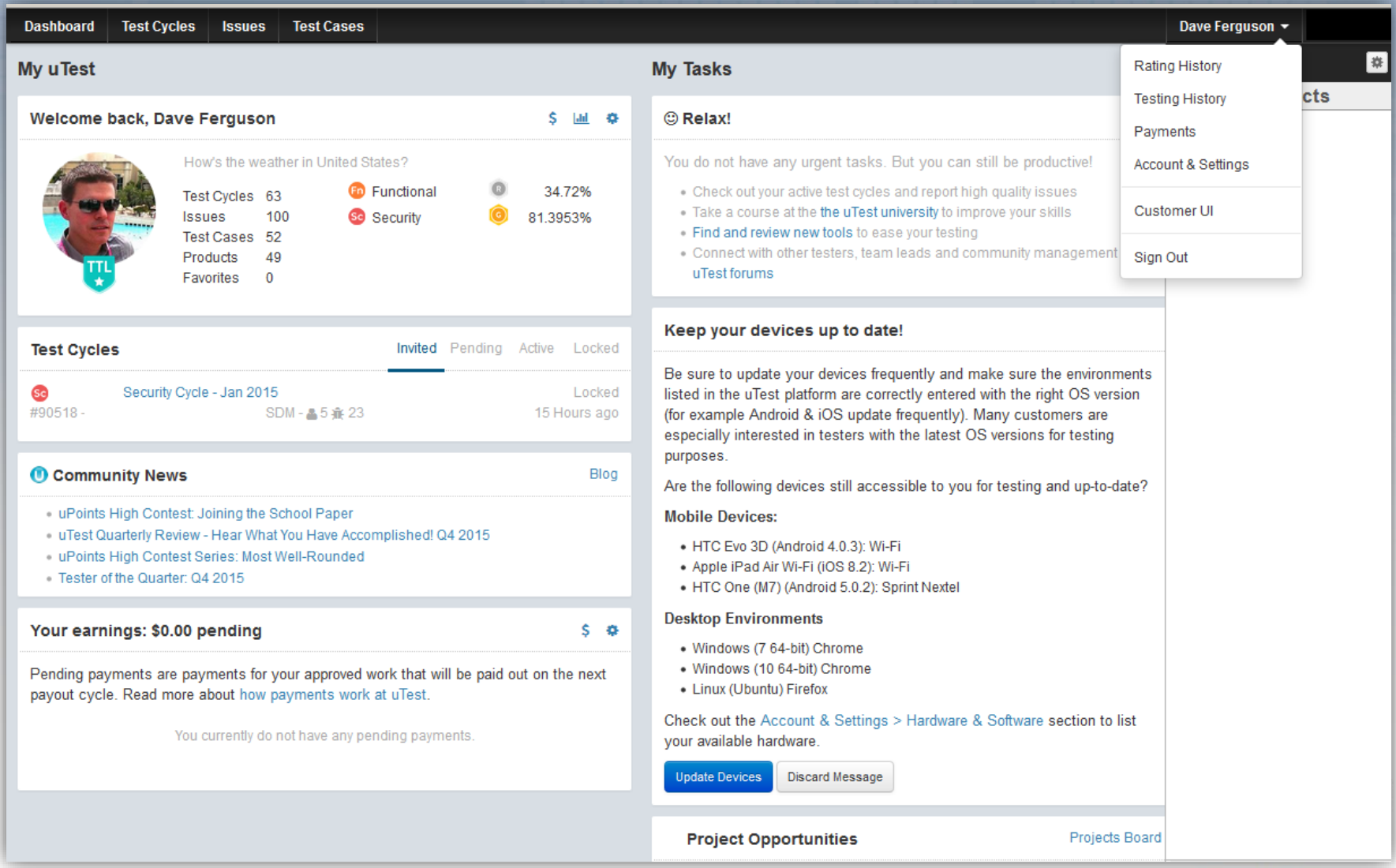
- Announced via the uTest platform
- Specific testers invited → email notifications sent
- Basic description of the app
- What's in scope for testing
- Invited testers can accept or decline the cycle
- Testing window: Usually 5-10 days
- TTL = Test Team Lead

OWASP
Open Web Application Security Project

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

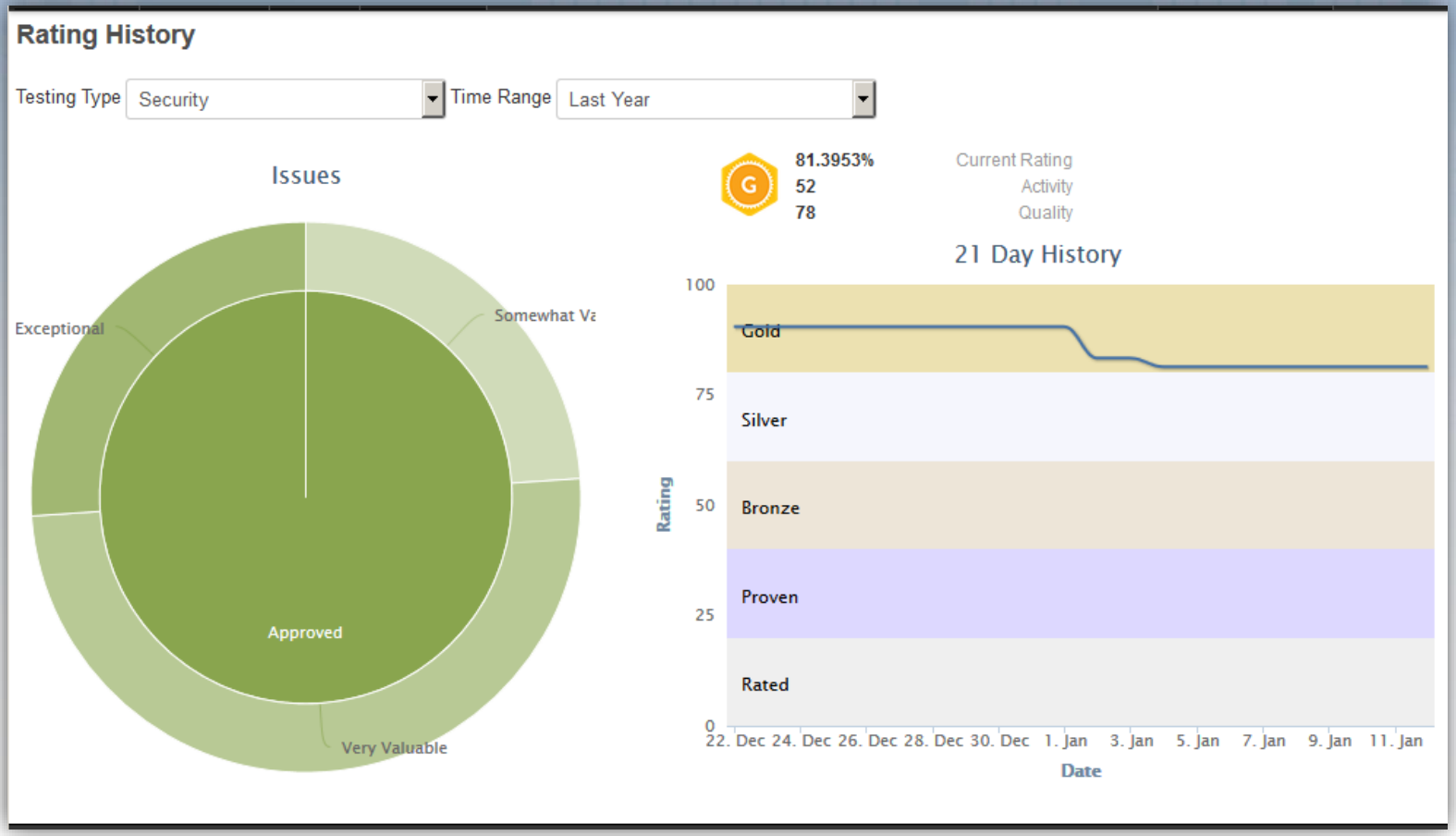
The Platform



Core Security Test Team

OWASP
Open Web Application Security Project

Rating the Testers



OWASP
Open Web Application Security Project

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

OWASP
Open Web Application Security Project

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 an 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

OWASP
Open Web Application Security Project

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.

OWASP
Open Web Application Security Project

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

OWASP
Open Web Application Security Project

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

OWASP
Open Web Application Security Project

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

OWASP
Open Web Application Security Project

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

OWASP
Open Web Application Security Project

DRM Schemes

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

OWASP
Open Web Application Security Project

Specific Guidelines

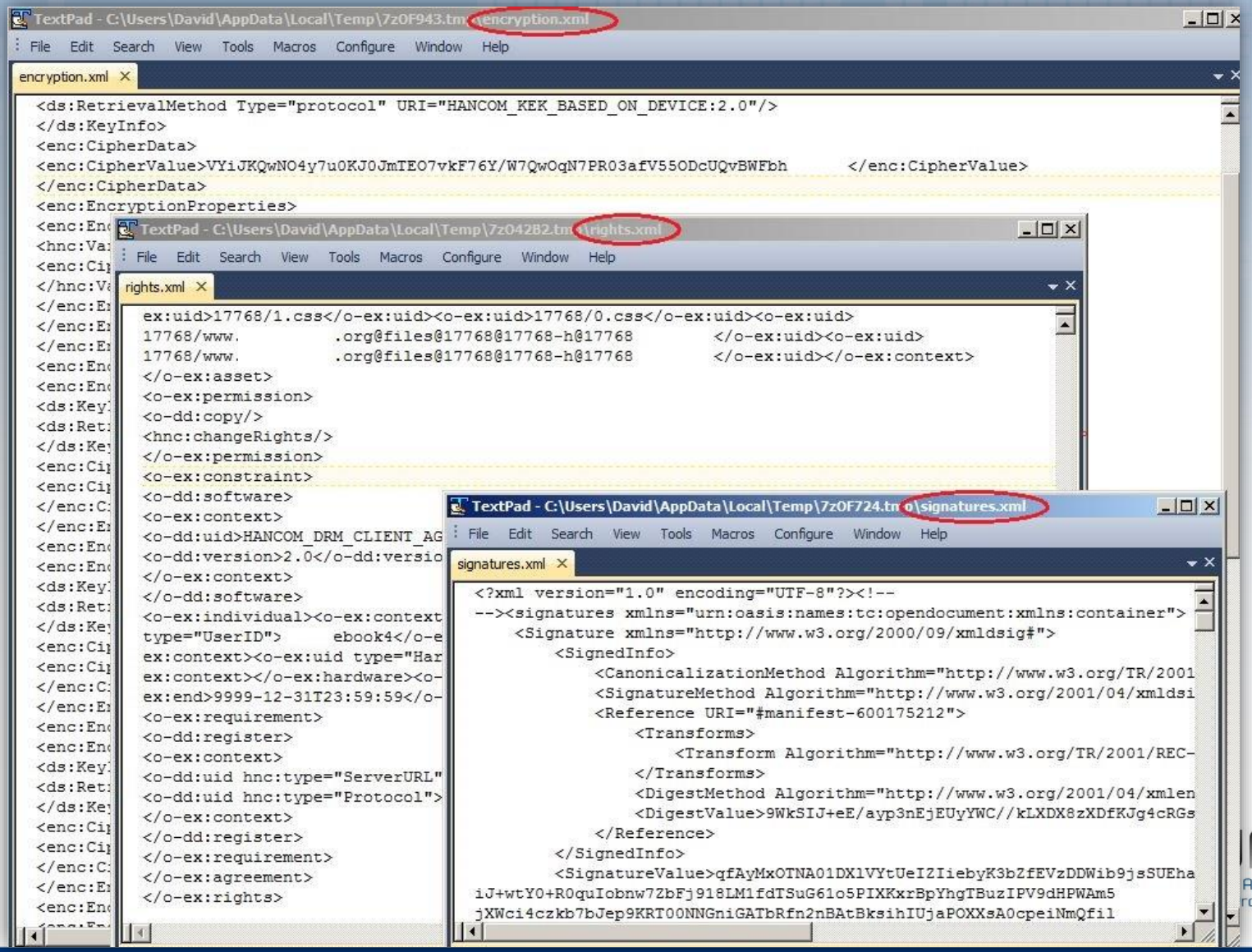
- DRM / eReader goals
  - URLs not enumerable or guessable
  - Limit the number of concurrent devices
  - Purchasing one book doesn't allow reengineering to gain access to a different book
  - No more than one page of text can be copied
  - Images cannot be easily extracted
  - Book cannot be forwarded 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

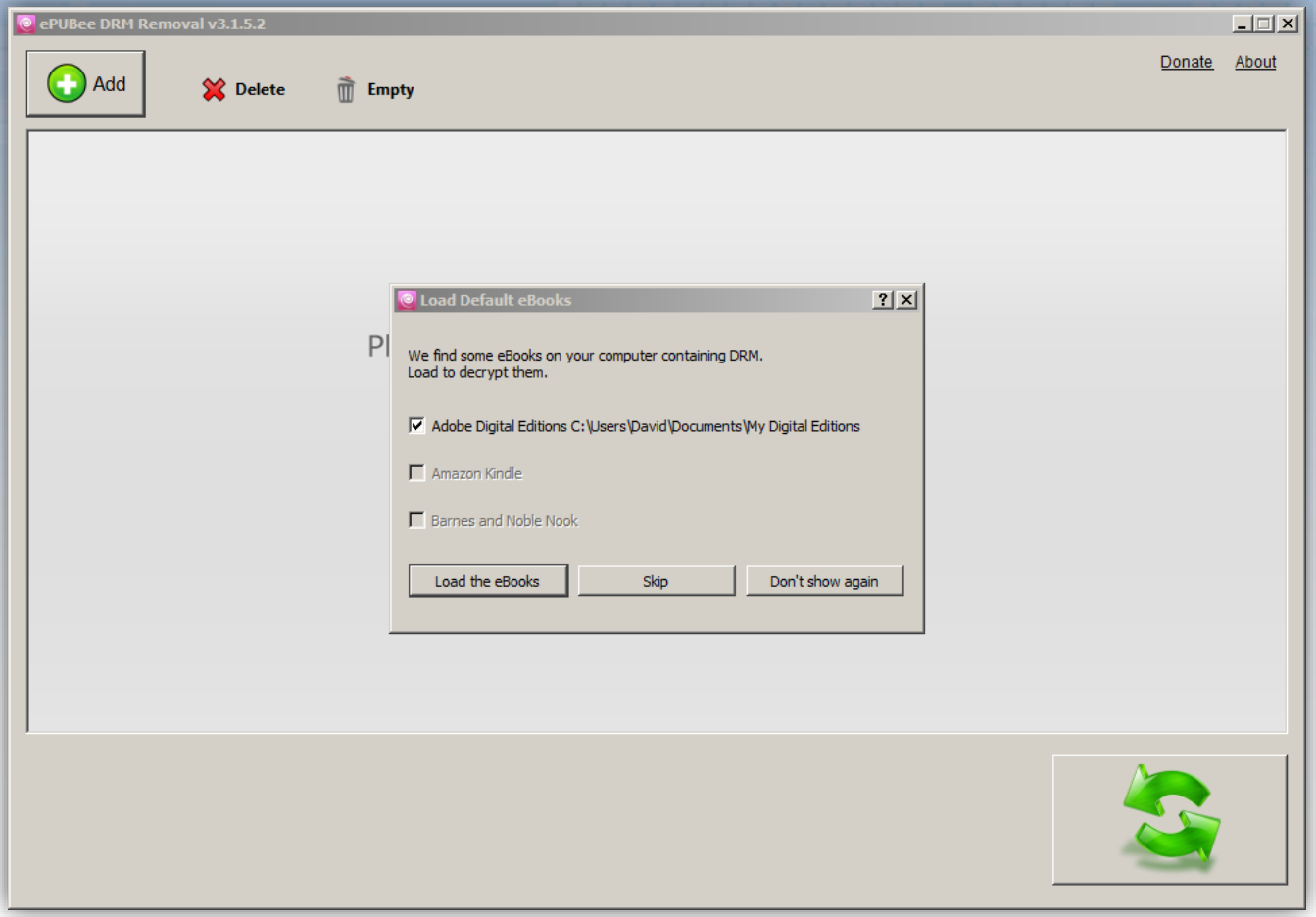
OWASP
Open Web Application Security Project

Inspecting EPUB files



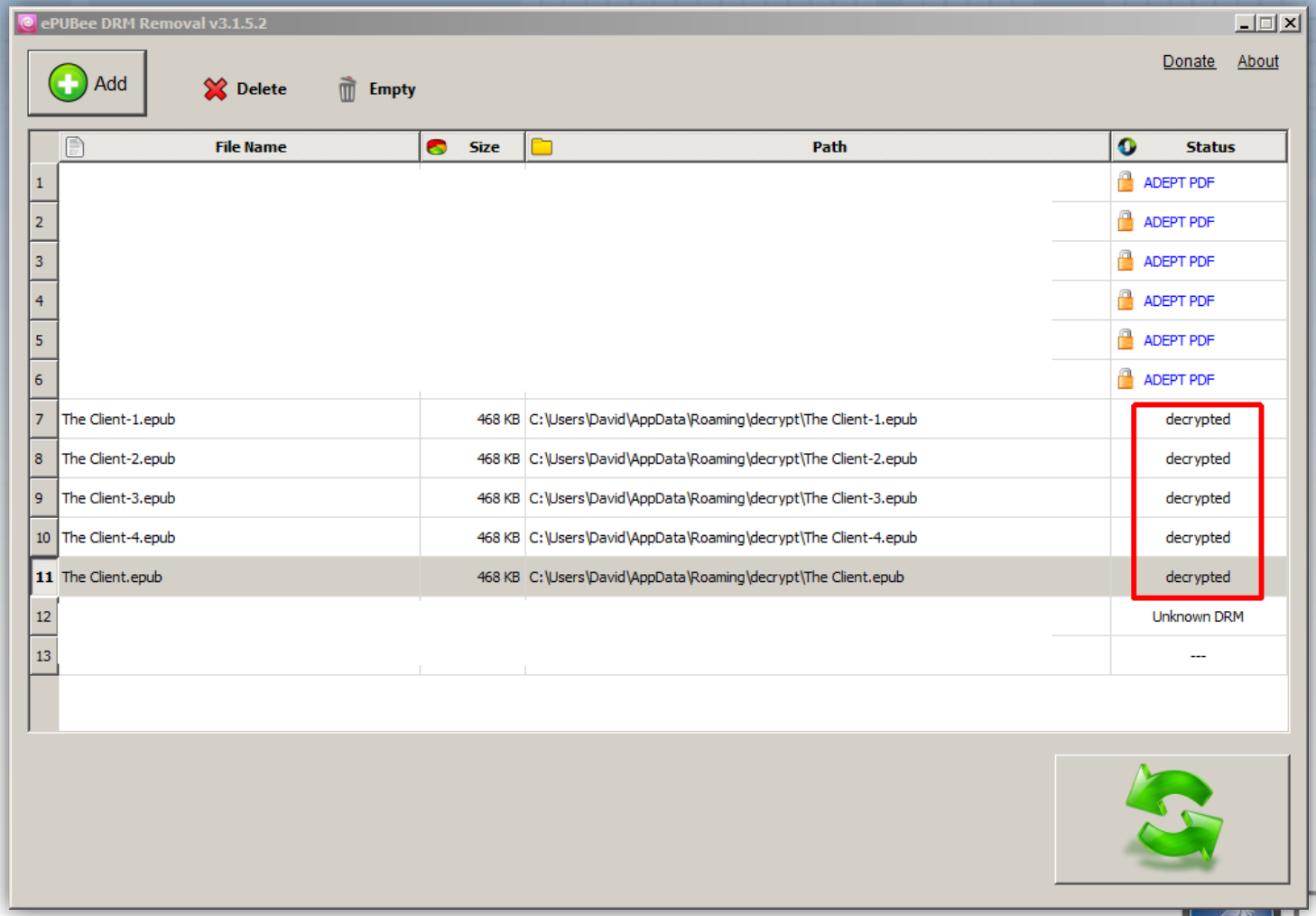
ASP
Application
roject

ePUBee DRM Removal Tool



OWASP
Open Web Application Security Project

ePUBee DRM Removal Tool



OWASP
Open Web Application Security Project

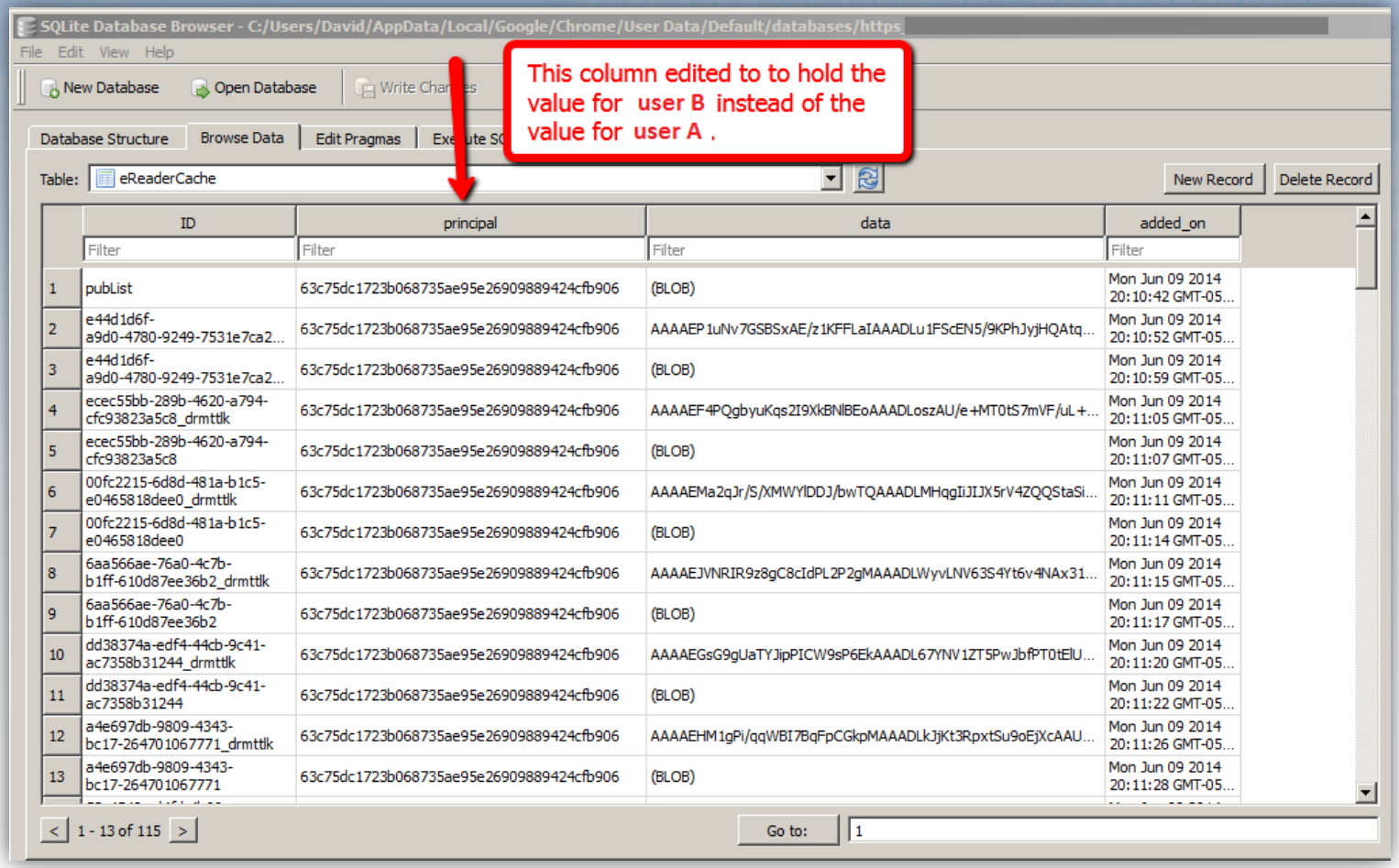
Tested: HTML5 eReader

- 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



OWASP
Open Web Application Security Project

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

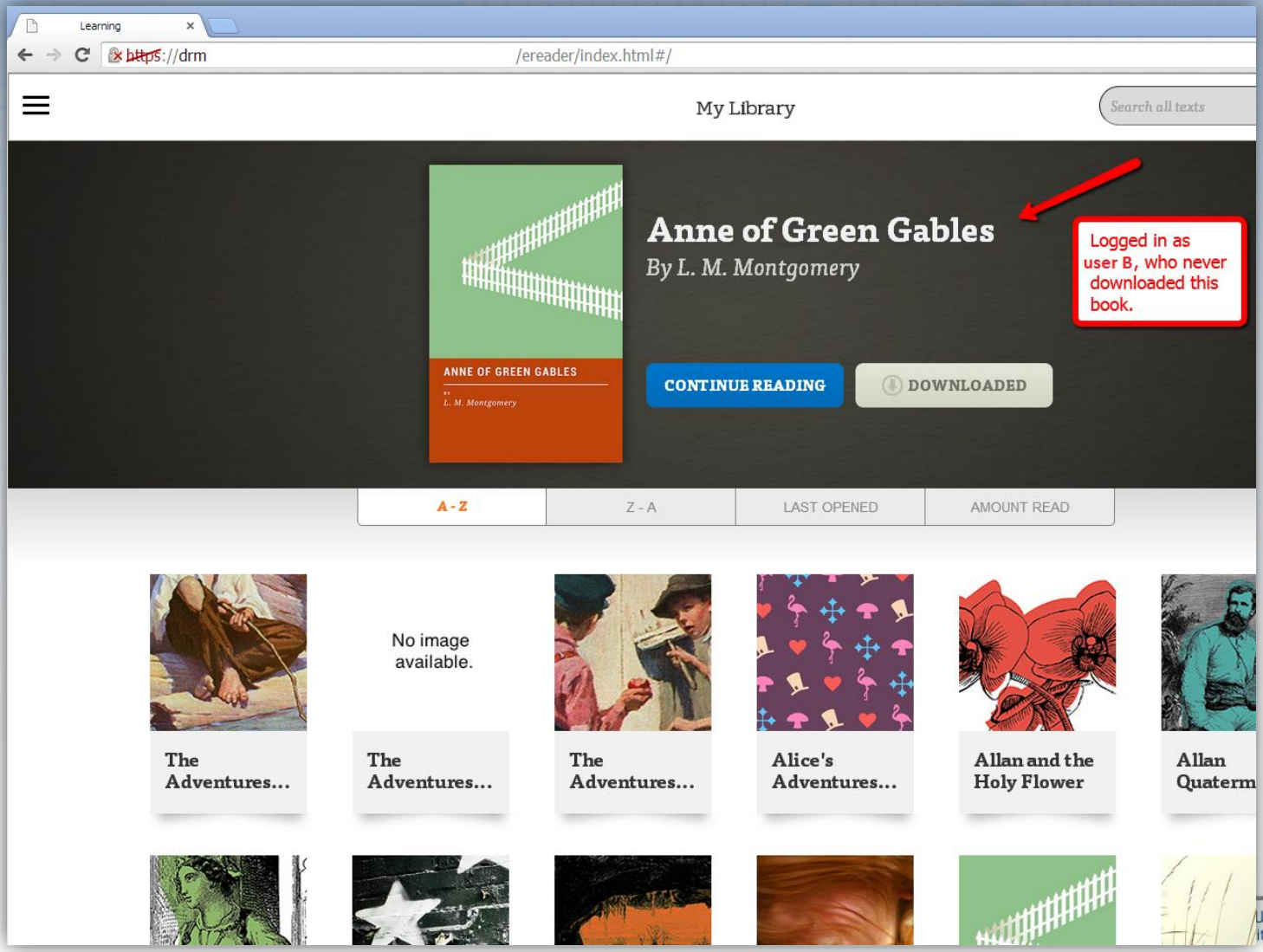
DAS7fcMyet6j/iNac8j9Grgw0Mm1LmexCo1OZQQt+NM=

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=

OWASP
Open Web Application Security Project

HTML5 eReader - Flaw

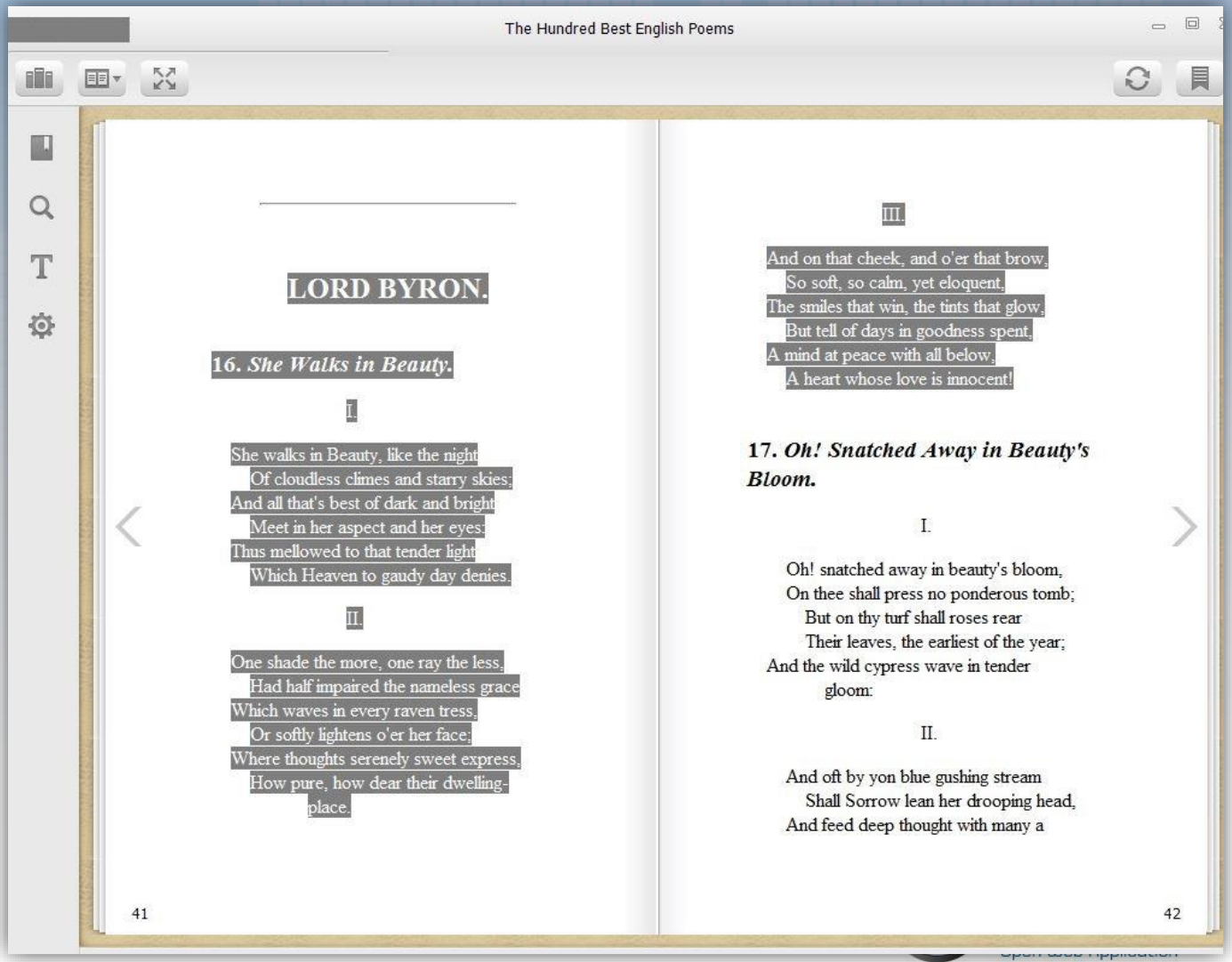


WASP
Web Application
ity Project

Tested: Thick Client eReader

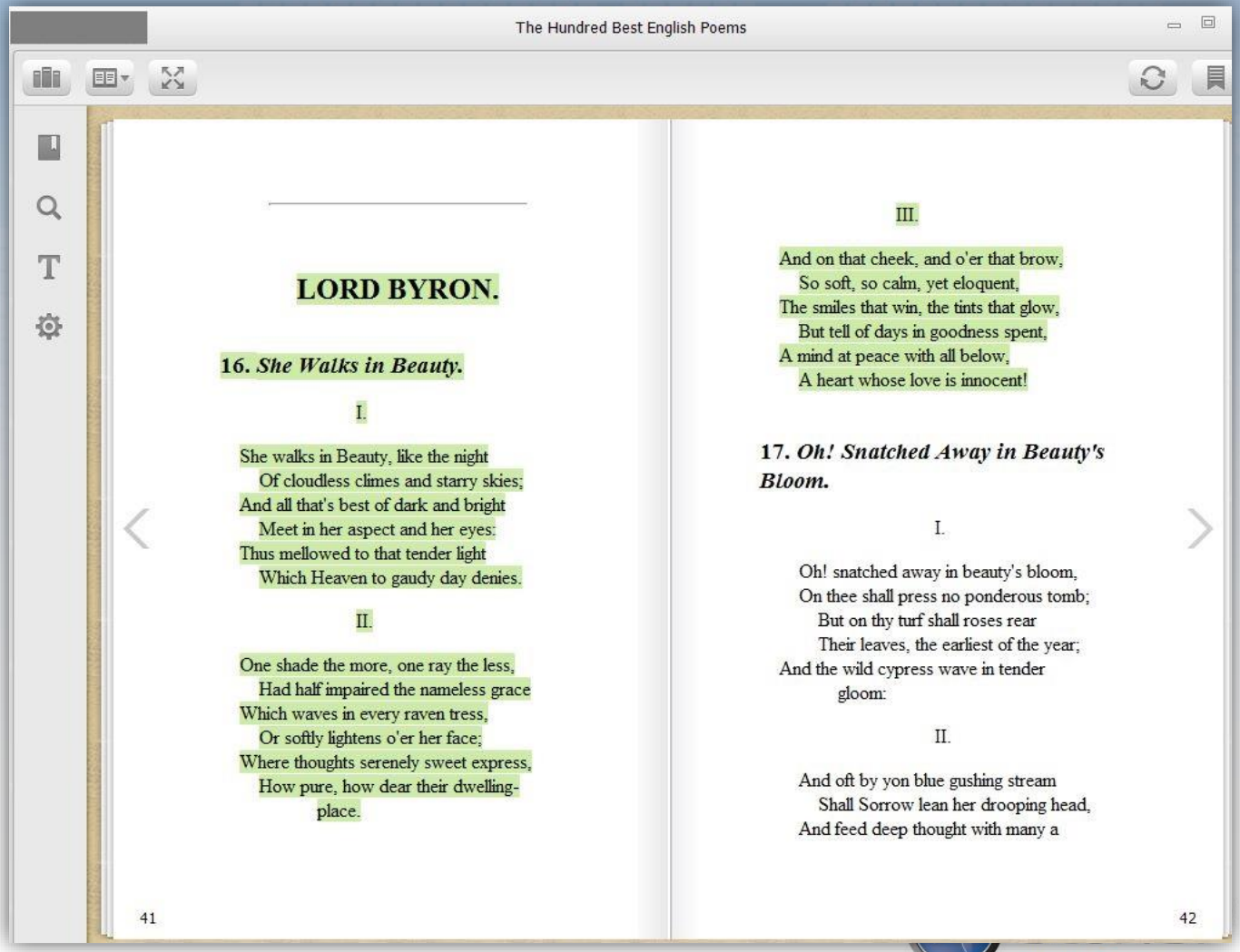
Use Burp invisible proxy mode.

Select some text.



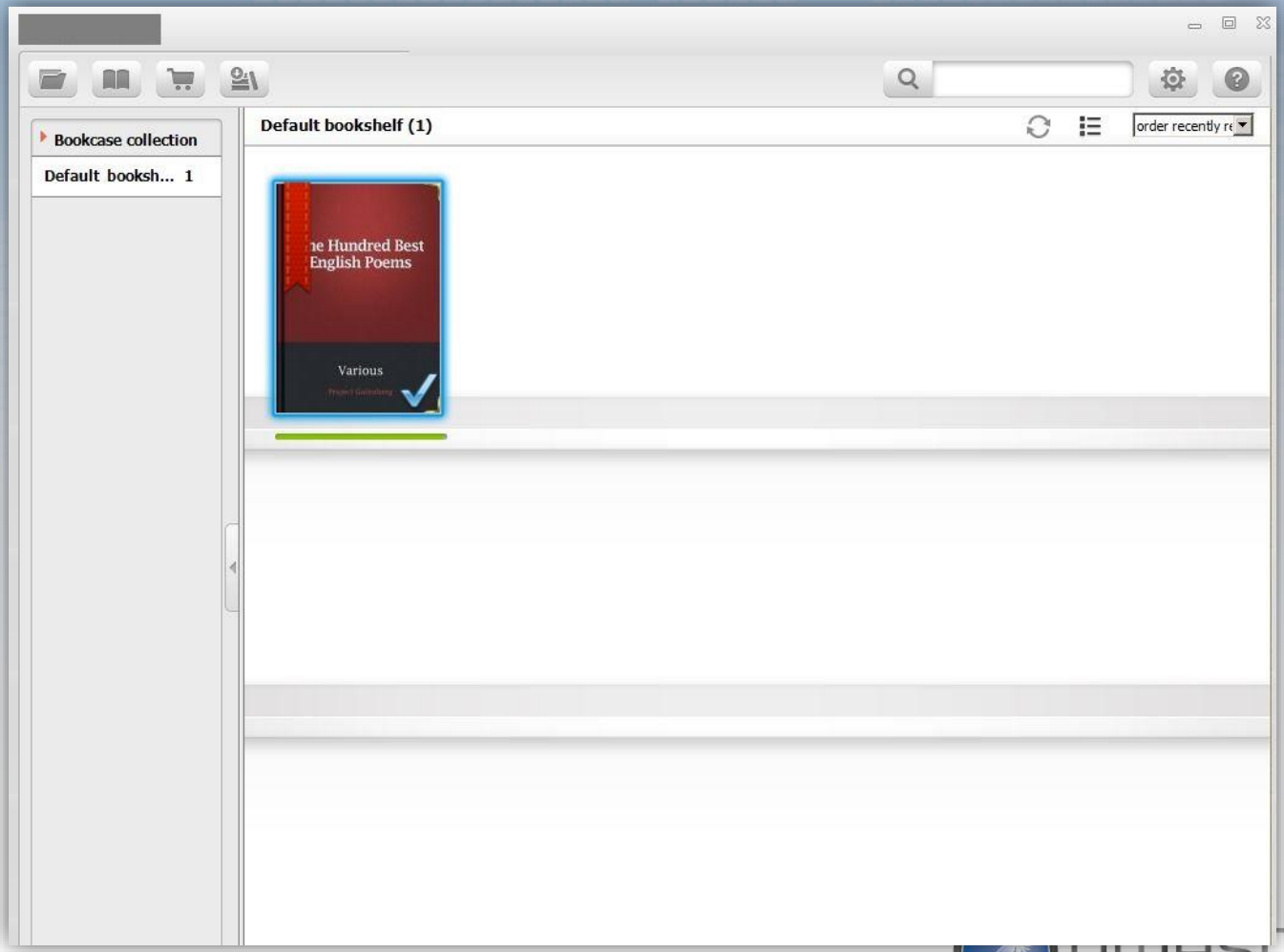
Thick Client eReader

Right click, and choose highlight.



Thick Client eReader

Return book to bookshelf and exit application



OWASP
Open Web Application
Security Project

Thick Client eReader - Flaw

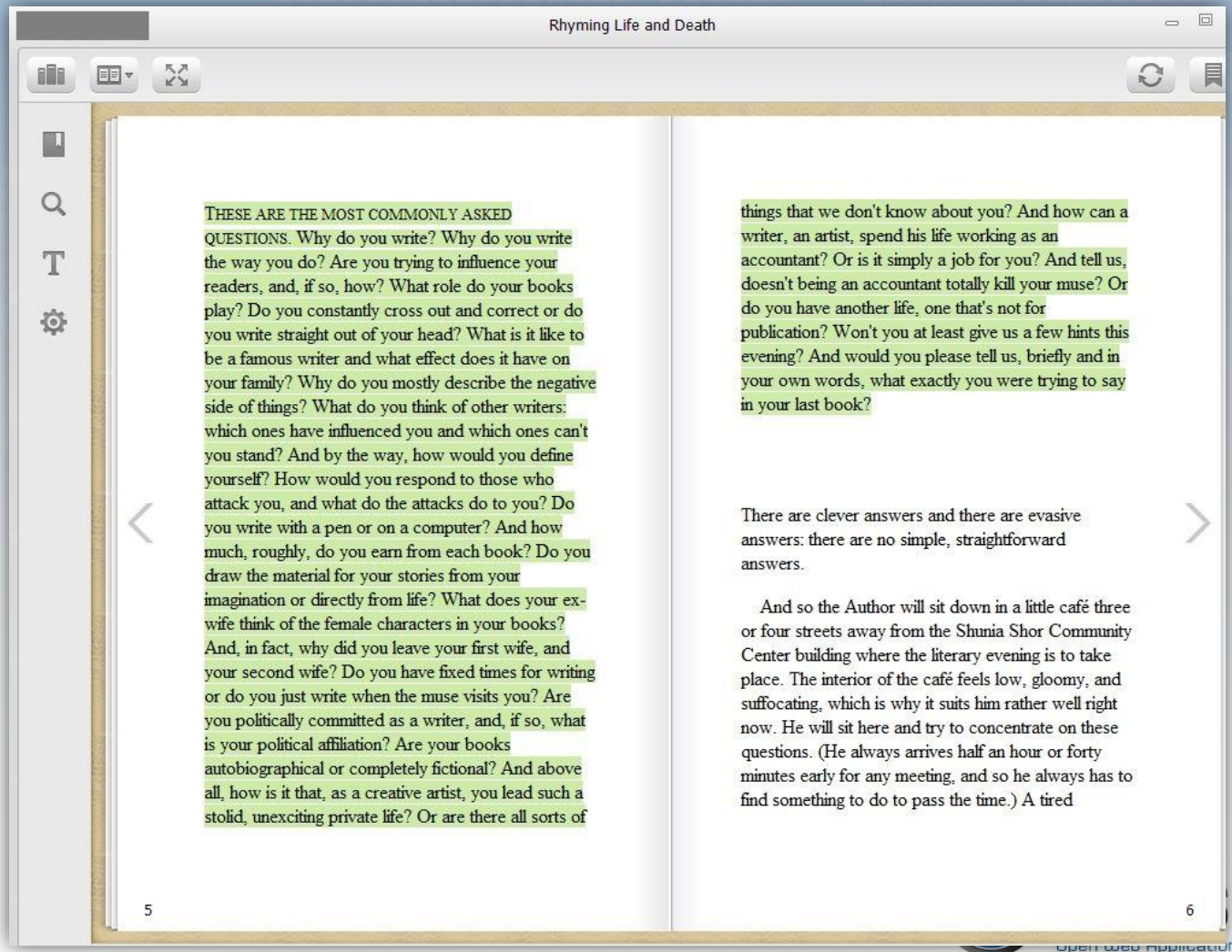
Inspect

Burp

OWASP
Open Web Application Security Project

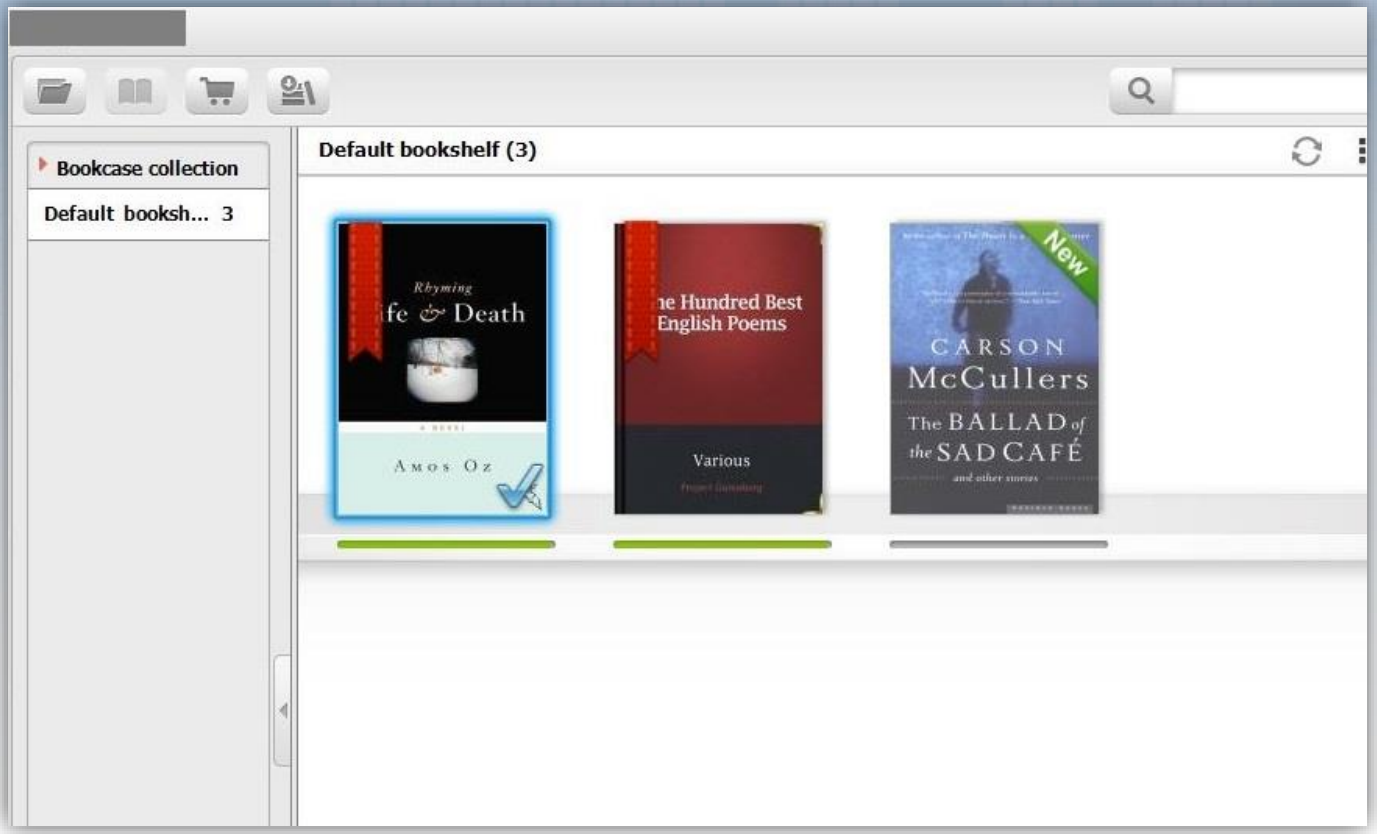
Thick Client eBook reader, flaw2

Highlight text



Thick Client eReader, flaw2

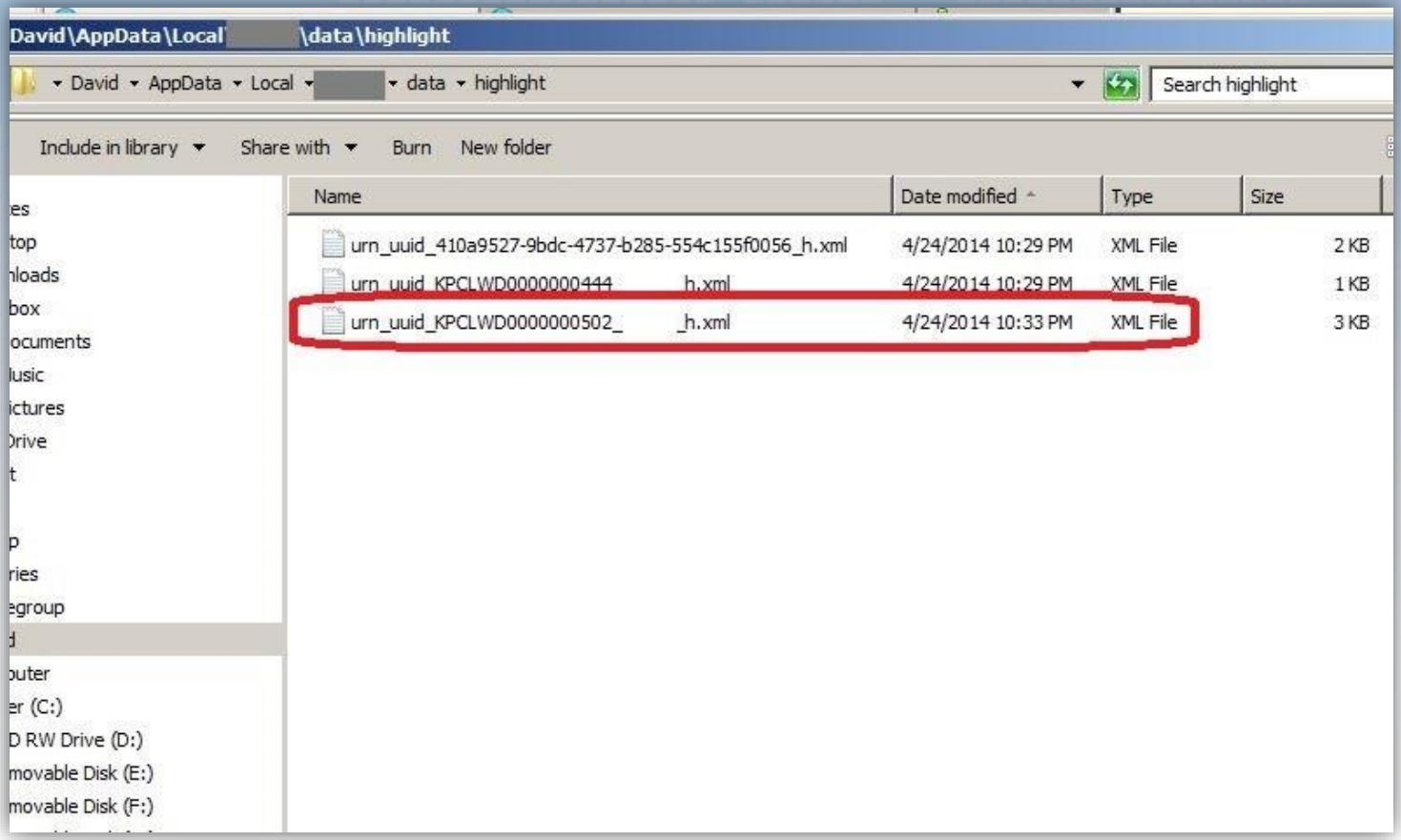
Return book to bookshelf



OWASP
Open Web Application Security Project

Thick Client eReader, flaw2

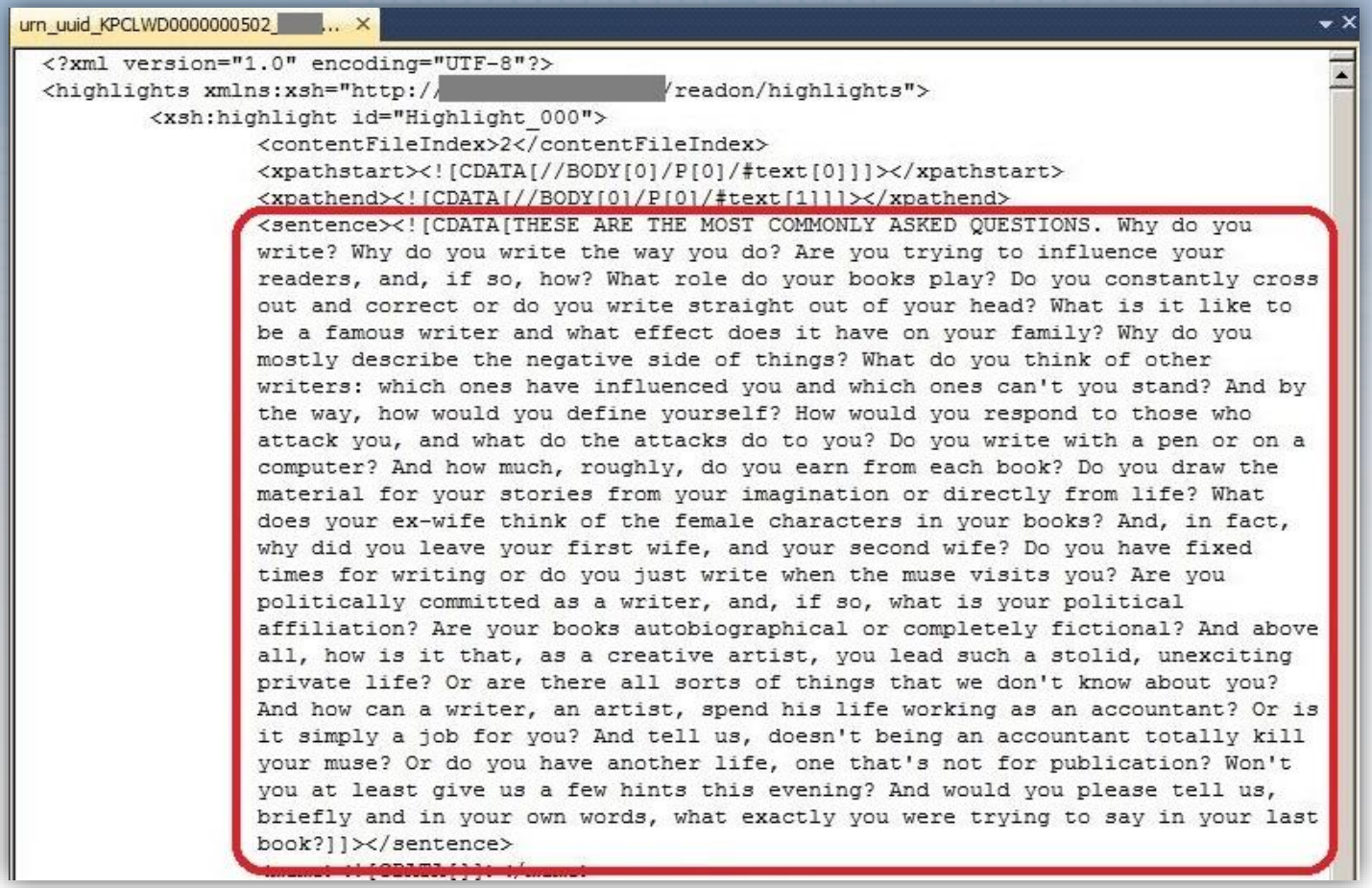
Find xml files under AppData directory



OWASP
Open Web Application Security Project

Thick Client eReader, flaw2

Open the most recent xml file



OWASP
Open Web Application Security Project

OWASP

Open Web Application Security Project

THE END

Thank you for attending!

@_sc0rn

gmdavef at gmail