Melting Pot of Origins

Compromising the Intermediary Web Services that Rehost Websites

Takuya Watanabe†‡, Eitaro Shioji†, Mitsuaki Akiyama†, Tatsuya Mori‡§⊥

†NTT Secure Platform Laboratories,
‡Waseda University, §NICT, ⊥RIKEN AIP

NDSS Symposium
24th February, 2020
This work...

• Study security flaws of *web rehosting services*
• Present five attacks (e.g., persistent MITM)
• Demonstrate feasibility on real services
• Provide countermeasures
Obstacles to Web Access

- Language barrier
- Missing web page
- Blocking
吾輩は猫である

夏目漱石
Solution: Web Rehosting

Intermediary service

fetch
rehost
Web Rehosting Services
Enhance Openness of Web

Website translator  Web archive  Web-based proxy
## 21 Web Rehosting Services We Examined

<table>
<thead>
<tr>
<th>Web Proxy</th>
<th>ProxySite, Hide My Ass!, Hide me, Sitenable Proxy, FilterBypass, ProxFree, toolur, hidester, GenMirror, UnblockVideos, Service-α</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Translator</td>
<td>Google Translate, Bing Translator, Weblio, PROMT, Yandex.Translate, Baidu Translate, Service-β</td>
</tr>
<tr>
<td>Web Archive</td>
<td>Wayback Machine, Google Cache, FreezePage</td>
</tr>
</tbody>
</table>

> 200M sessions/day
Typical Web Rehosting Usage

URL: https://google.com

or

Direct link:
https://rehosted.example/?url=https://google.com
Web Rehosting Architecture
Web Rehosting Architecture

(a.example) -> Web rehosting -> rehosted.example
(b.example) -> Web rehosting -> rehosted.example

( Boundary of origins )
Rehosting Rules

• URL Rewriting
  
  \textit{https://a.example}
  
  \rightarrow \textit{https://rehosted.example/?url=https://a.example}

• Rehostable File Type
  
  • HTML, plaintext
  
  • JavaScript (except some translators)

• Handling Browser Resources
  
  • remain resource accesses via JavaScript
  
  • relay HTTP cookie (web proxy)
Attack Surface

(a.example)  (Boundary of origins)  (rehosted.example)

A  Web rehosting  B

a.example  b.example  evil.example  rehosted.example

(rehosted.example)  (affect)
Attack Surface

Rehosted page

Rehosted malicious page

Boundary of origins

A

a.example

b.example

evil.example

B

rehosted.example

rehosted.example

rehosted.example

rehosted.example

affect
## Attacks against Web Rehosting

<table>
<thead>
<tr>
<th>#</th>
<th>Attacks</th>
<th>Exploited Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Persistent MITM</td>
<td>Service Worker, AppCache</td>
</tr>
<tr>
<td>II</td>
<td>Privilege Abuse</td>
<td>Camera, Microphone, Location, Notification, etc.</td>
</tr>
<tr>
<td>III</td>
<td>Credential Theft</td>
<td>Password Manager</td>
</tr>
<tr>
<td>IV</td>
<td>History Theft</td>
<td>Cookie (written by JavaScript), localStorage</td>
</tr>
<tr>
<td>V</td>
<td>Session Hijacking and Injection</td>
<td>Cookie (written by HTTP header)</td>
</tr>
</tbody>
</table>
Threat Model

Attack I

1. Visit rehosted malicious page
2. Register script to browser
3. Visit rehosted pages
4. Intercept requests /responses

Web rehosting

Attack II - V

1. Visit rehosted pages
2. Store data in browser
3. Visit rehosted malicious page
4. Steal stored data

Web rehosting
**Threat Model**

**Attack I**
1. Visit rehosted malicious page
2. Register script to browser
3. Visit rehosted pages
4. Intercept requests/responses

**Attack II - V**
1. Visit rehosted pages
2. Store data in browser
3. Visit rehosted malicious page
4. Steal stored data
Attack I: Persistent MITM

You are cracked!
Pay 10 BTC

Direct
Through web rehosting
Through web rehosting (after attack)
Service Worker (SW)

- Powerful feature in HTML 5.1
  - intercept all req./res.

- Restrictions
  - HTTPS
  - Same Origin
    - SW script, register page, scoped pages
  - MIME Type (JavaScript)

https://a.example/register.html
https://a.example/*

sw.js

Scoped pages

User browser
Attack I: Persistent MITM (with SW)

1. Visit rehosted malicious page
2. Register sw.js to browser
3. Visit rehosted pages
4. Intercept requests / responses

Scope: origin of web rehosting service
SW Script and Register Page

https://evil.example/  register.html
sw.js

self.addEventListener('fetch', function(event) {
customizeResponse(fetch(event.request));
return;
});

<script>
navigator.serviceWorker.register('sw.js');
</script>

generate rehosted malicious page:
“https://rehosted.example/?url=https://evil.example/register.html”
SW Script and Register Page

https://evil.example/register.html

```javascript
self.addEventListener('fetch', function(event) {
    customizeResponse(fetch(event.request));
    return;
});
```

```html
<script>
navigator.serviceWorker.register('sw.js');
</script>
```

Does not work

“https://rehosted.example/?url=https://evil.example/register.html”
`navigator.serviceWorker.register('https://rehosted.example/?url=https://evil.example/sw.js');`

```
self.addEventListener('fetch', function(event) {
  customizeResponse(fetch(event.request));
  return;
});
```

“https://rehosted.example/?url=https://evil.example/register.html”
Interesting Case Study for Google Translate

URL for website translation (type of web rehosting):

https://translate.googleusercontent.com/translate_c?u=https://a.example&...
Interesting Case Study for Google Translate

URL for website translation (type of web rehosting):
https://translate.googleusercontent.com/translate_c?u=https://a.example&...

URL for uploaded document translation:
https://translate.googleusercontent.com/translate_f
More details in our paper

- Techniques to rehost SW scripts on web translator
- Discussion of path scope
- Attack using AppCache instead of SW
  - Rewriting fallback pages + cookie bomb
Attack I: Persistent MITM

Vulnerable to attack I:

13 out of 21 web rehostings

Direct

Through web rehosting

Through web rehosting (after attack)
Threat Model

(1) visit rehosted malicious page
(2) register script to browser
(3) visit rehosted pages
(4) intercept requests /responses

(1) visit rehosted malicious page
(2) store data in browser
(3) visit rehosted malicious page
(4) steal stored data
Attack II: Privilege Abuse

User grant permission at rehosted benign pages

Permission is reused by rehosted malicious page
Attack II: Privilege Abuse

User grant permission at rehosted benign pages

Permission is reused by rehosted malicious page
Attack II: Privilege Abuse

Vulnerable to attack II:

13 out of 21 web rehostings

User grant permission at rehosted benign pages

Permission is reused by rehosted malicious page
Attack III: Credential Theft (for Web-based Proxy)

User logs in to rehosted benign page and save credential in password manager.

Password manager auto-fills credential on fake form of rehosted malicious page.
Attack III: Credential Theft (for Web-based Proxy)

User logs in to rehosted benign page and save credential in password manager.

Password manager auto-fills credential on fake form of rehosted malicious page.

Vulnerable to attack III: 9 out of 11 web proxies.
1. User visits rehosted page.
2. Page writes cookie or localStorage by using JavaScript.
3. Rehosted malicious page retrieves cookie/localStorage.
4. Attacker estimates browsing history by using retrieved data.

```javascript
document.cookie = "name=value";
localStorage.setItem('name', value);
```
Non-identifiable website (has only general cookie names /localStorage keys)

Identifiable website (has unique cookie name /localStorage keys)

39.1% of alexa top 10k
Attack IV: History Theft

1. User visits rehosted page.
2. Page writes cookie or localStorage by using JavaScript.

Vulnerable to attack IV:

18 out of 21 web rehostings

3. Rehosted malicious page retrieves cookie/localStorage.
4. Attacker estimates browsing history.
Attack V: Session Hijacking & Injection (for Web-based Proxy)

Cookie (written by HTTP header)

Domain: .facebook.com
Name: xs
Value: XXXXXXXXXXXXXXXXXXX
Option: HttpOnly

Cookie (written by HTTP header)

Domain: .rehosted.example
Name: c[facebook.com]l]l][xs]
Value: XXXXXXXXXXXXXXXXXXX
Option: None
Attack V: Session Hijacking & Injection (for Web-based Proxy)

Cookie (written by HTTP header)

- **Domain**: .facebook.com
- **Name**: xs
- **Value**: XXXXXXXXXXXXXXXXXXX
- **Option**: HttpOnly

Cookie (written by HTTP header)

- **Domain**: .rehosted.example
- **Name**: c[facebook.com][/][/][xs]
- **Value**: XXXXXXXXXXXXXXXXXXX
- **Option**: None
Attack V: Session Hijacking & Injection (for Web-based Proxy)

Vulnerable to attack V:
8 out of 11 web proxies
## Summary of Results

<table>
<thead>
<tr>
<th>Category</th>
<th>Rehosting Service</th>
<th>Scheme</th>
<th>At least one Vulnerability</th>
<th>Persistent MITM SW</th>
<th>Persistent MITM AppCache</th>
<th>Privilege Abuse</th>
<th>Credential Theft</th>
<th>History Theft</th>
<th>Session Hijacking &amp; Injection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy</td>
<td>ProxySite</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Hide My Ass!</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Hide me</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Sitenable Web Proxy</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>FilterBypass</td>
<td>HTTPS</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>ProxFree</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>toolur</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>hidester</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>GenMirror</td>
<td>HTTPS</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>UnblockVideos</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Service-α</td>
<td>HTTP/S</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Translator</td>
<td>Google Translate</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Bing Translator</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Webloio</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>PROMT Online</td>
<td>HTTP</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Service-β</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Yandex.Translate</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Baidu Translate</td>
<td>HTTP</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>—</td>
</tr>
<tr>
<td>Archive</td>
<td>Wayback Machine</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Google Cache</td>
<td>HTTP/S</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>FreezePage</td>
<td>HTTP</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>—</td>
</tr>
</tbody>
</table>

● Vulnerable
○ Secure
## Summary of Results

<table>
<thead>
<tr>
<th>Category</th>
<th>Rehosting Service</th>
<th>Scheme</th>
<th>At least one Vulnerability</th>
<th>Persistent MITM SW</th>
<th>AppCache</th>
<th>Privilege Abuse</th>
<th>Credential Theft</th>
<th>History Theft</th>
<th>Session Hijacking &amp; Injection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy</td>
<td>ProxySite</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Hide My Ass!</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Hide me</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Sitenable Web Proxy</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>FilterBypass</td>
<td>HTTPS</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>ProxFree</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>toolur</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>hidester</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>GenMirror</td>
<td>HTTPS</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>UnblockVideos</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Service-α</td>
<td>HTTP/S</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Translator</td>
<td>Google Translate</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Bing Translator</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Weblio</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>PROMT Online</td>
<td>HTTP</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Service-β</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Yandex.Translate</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Baidu Translate</td>
<td>HTTP</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Archive</td>
<td>Wayback Machine</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Google Cache</td>
<td>HTTP/S</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>FreezePage</td>
<td>HTTP</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>
## Summary of Results

<table>
<thead>
<tr>
<th>Category</th>
<th>Rehosting Service</th>
<th>Scheme</th>
<th>At least one Vulnerability</th>
<th>Persistent MITM Abuse</th>
<th>Privilege Abuse</th>
<th>Credential Theft</th>
<th>History Theft</th>
<th>Session Hijacking &amp; Injection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy</td>
<td>ProxySite</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Hide My Ass!</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Hide me</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Sitable Web Proxy</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>FilterBypass</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>ProxFree</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>toolur</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>hidester</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>GenMirror</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>UnblockVideos</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Service-α</td>
<td>HTTP/S</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Translator</td>
<td>Google Translate</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Bing Translator</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Weblio</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>PROMT Online</td>
<td>HTTP</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Service-β</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Yandex.Translate</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Baidu Translate</td>
<td>HTTP</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Archive</td>
<td>Wayback Machine</td>
<td>HTTPS</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>Google Cache</td>
<td>HTTP/S</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>FreezePage</td>
<td>HTTP</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
## Browsers Comparison

<table>
<thead>
<tr>
<th>#</th>
<th>Attacks</th>
<th>Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Persistent MITM</td>
<td><img src="image1" alt="Browsers Logos" /></td>
</tr>
<tr>
<td>II</td>
<td>Privilege Abuse</td>
<td><img src="image2" alt="Browsers Logos" /></td>
</tr>
<tr>
<td>III</td>
<td>Credential Theft</td>
<td><img src="image3" alt="Browsers Logos" /></td>
</tr>
<tr>
<td>IV</td>
<td>History Theft</td>
<td><img src="image4" alt="Browsers Logos" /></td>
</tr>
<tr>
<td>V</td>
<td>Session Hijacking and Injection</td>
<td><img src="image5" alt="Browsers Logos" /></td>
</tr>
</tbody>
</table>
Defenses for Web Rehosting

- Separate domain names for each rehosted page
  
  ```plaintext
  https://rehosted.example/?url=a.example
  ```
  
  ```plaintext
  https://a-example.rehosted.example/
  ```

- Generate tentative URL inaccessible by 3rd party
  
  Inhibit direct links

- Disable SW and AppCache (attack I)

- Use HTTPOnly (attack V)
**Ethics**

- We reported to affected service providers we examined.
  - 9 providers responded
  - 4 providers certified as vulnerability
  - 2 providers asked us not to be named

- We plan to make risks more widely known in cooperation with JPCERT/CC.
Future Directions

**Other web rehosting services?**

**Other attacks?**

- iframe [Lerner_CCS'17]
- Persistent XSS [Steffens_NDSS'19]

**Human behaviors while using web rehosting?**

- Private browsing
- Login
- Permission
Conclusion

- Explored security flaws of web rehosting services
- Presented 5 attacks exploiting various web features
- Found that 18 out of 21 services are vulnerable
- Reported risk to service providers with feasible defenses

watanabe@nsl.cs.waseda.ac.jp
@twatanabe1203