SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Web Security- IE2062

Phishing by Navigating Browser Tabs

Danuka Nuwan

IT22349842

Title of Vulnerability: Phishing by Navigating Browser Tabs

Description of Vulnerability:

The application's layout lets phishing strikes by controling internet browser tabs or computer windo ws to fool clients just into communicating with hazardous stuff or offering delicate facts accidently. Assaulters can manipulate this susceptability to pose authentic sites or solutions creating credenti al burglary, monetary scams or malware establishment.

Website-www.kindredgroup.com

Components Affected:

- User interface design
- Browser tab management
- Cross-origin communication

Assessment of Impact:

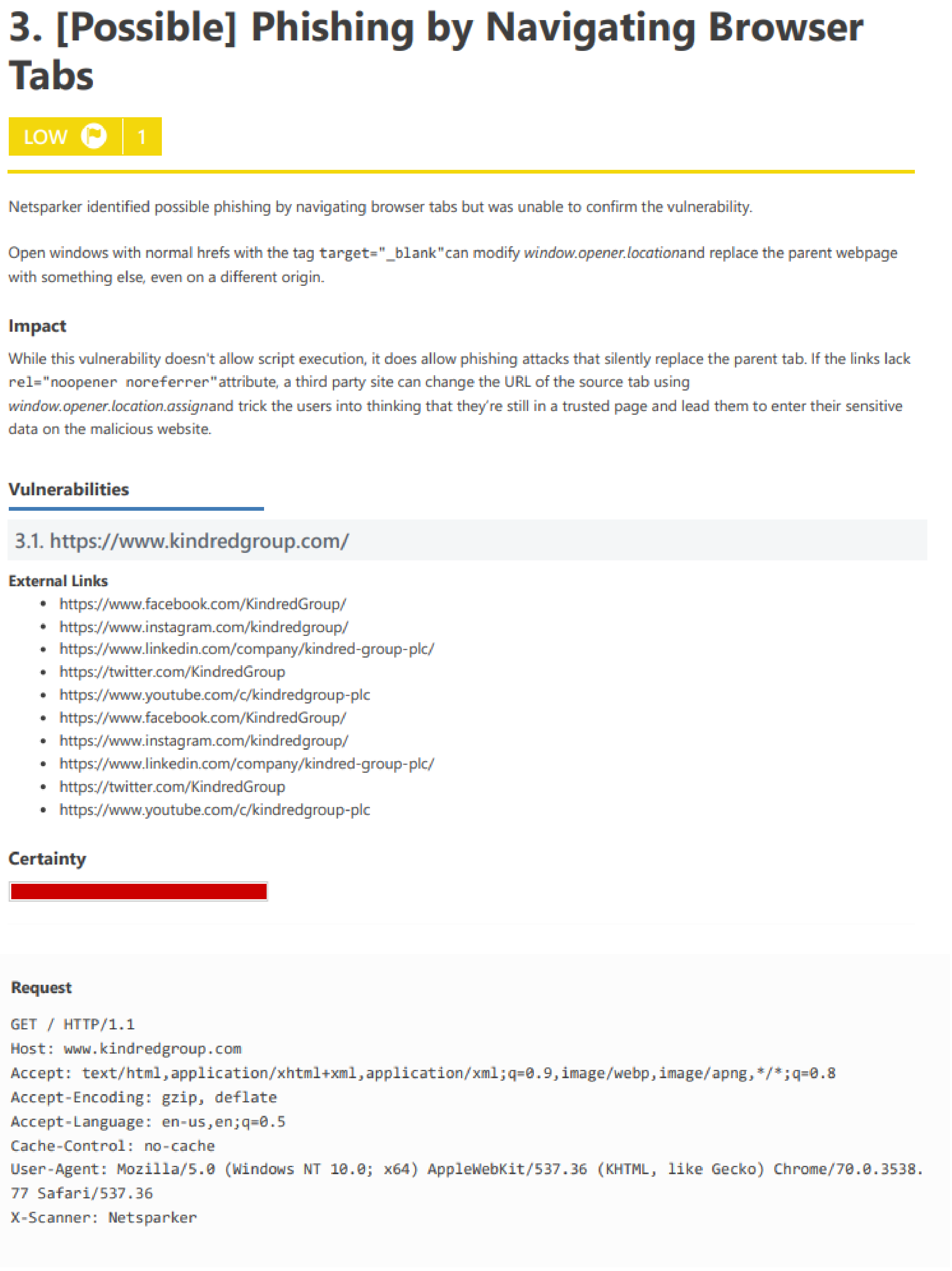
Impact is Medium: Phishing by exploring internet browser tabs introduces clients to possible hazards of revealing critical details or coming down with social design strikes While the straight effect might change depending upon client recognition coupled with communication, the opportunity for adjustment remains to be substantial.

Steps for Replicating:

Analyze the application's interface layout as well as internet browser tab monitoring capacity to detect opportunities for phishing attacks.
Apply a proof of principle (PoC) situation where the application browses internet browser tabs or home windows programmatically to show misleading stuff such as bogus login types or sharp messages.
Examine the success of the phishing strike by studying individual patterns and also communicating with the adjusted web browser tabs.

examine cross-origin interaction capability to detect if the program can engage with material from various other domain names to help with phishing assaults.

Proof of Concept:



3. [Possible] Phishing by Navigating Browser Tabs

LOW 🏳 | 1

Netsparker identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

Open windows with normal hrefs with the tag `target="_blank"`can modify *window.opener.location*and replace the parent webpage with something else, even on a different origin.

Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack `rel="noopener noreferrer"`attribute, a third party site can change the URL of the source tab using *window.opener.location.assign*and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

Vulnerabilities

3.1. https://www.kindredgroup.com/

External Links

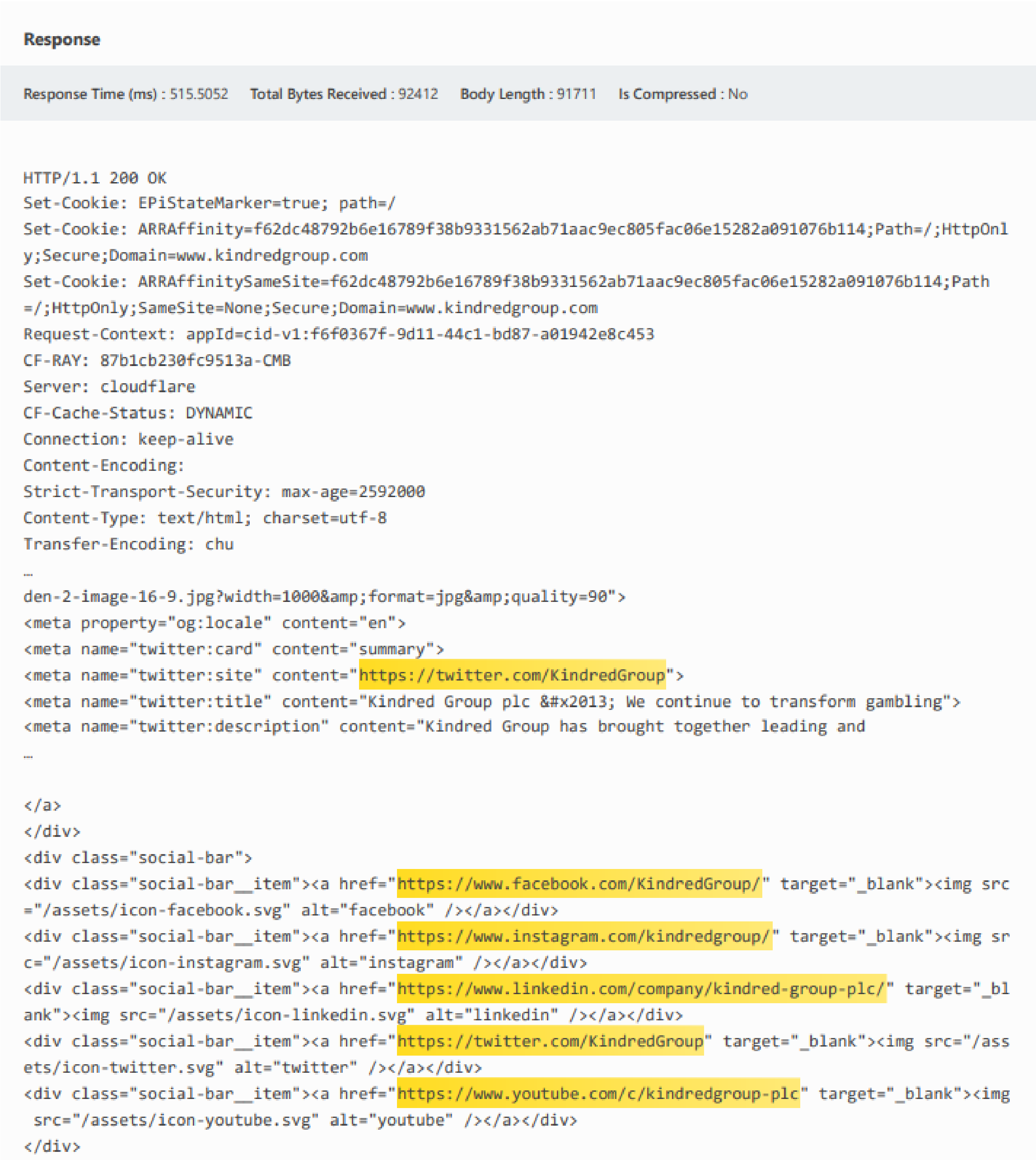
- https://www.facebook.com/KindredGroup/
- https://www.instagram.com/kindredgroup/
- https://www.linkedin.com/company/kindred-group-plc/
- https://twitter.com/KindredGroup
- https://www.youtube.com/c/kindredgroup-plc
- https://www.facebook.com/KindredGroup/
- https://www.instagram.com/kindredgroup/
- https://www.linkedin.com/company/kindred-group-plc/
- https://twitter.com/KindredGroup
- https://www.youtube.com/c/kindredgroup-plc

Certainty

🟥

Request

```
GET / HTTP/1.1
Host: www.kindredgroup.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

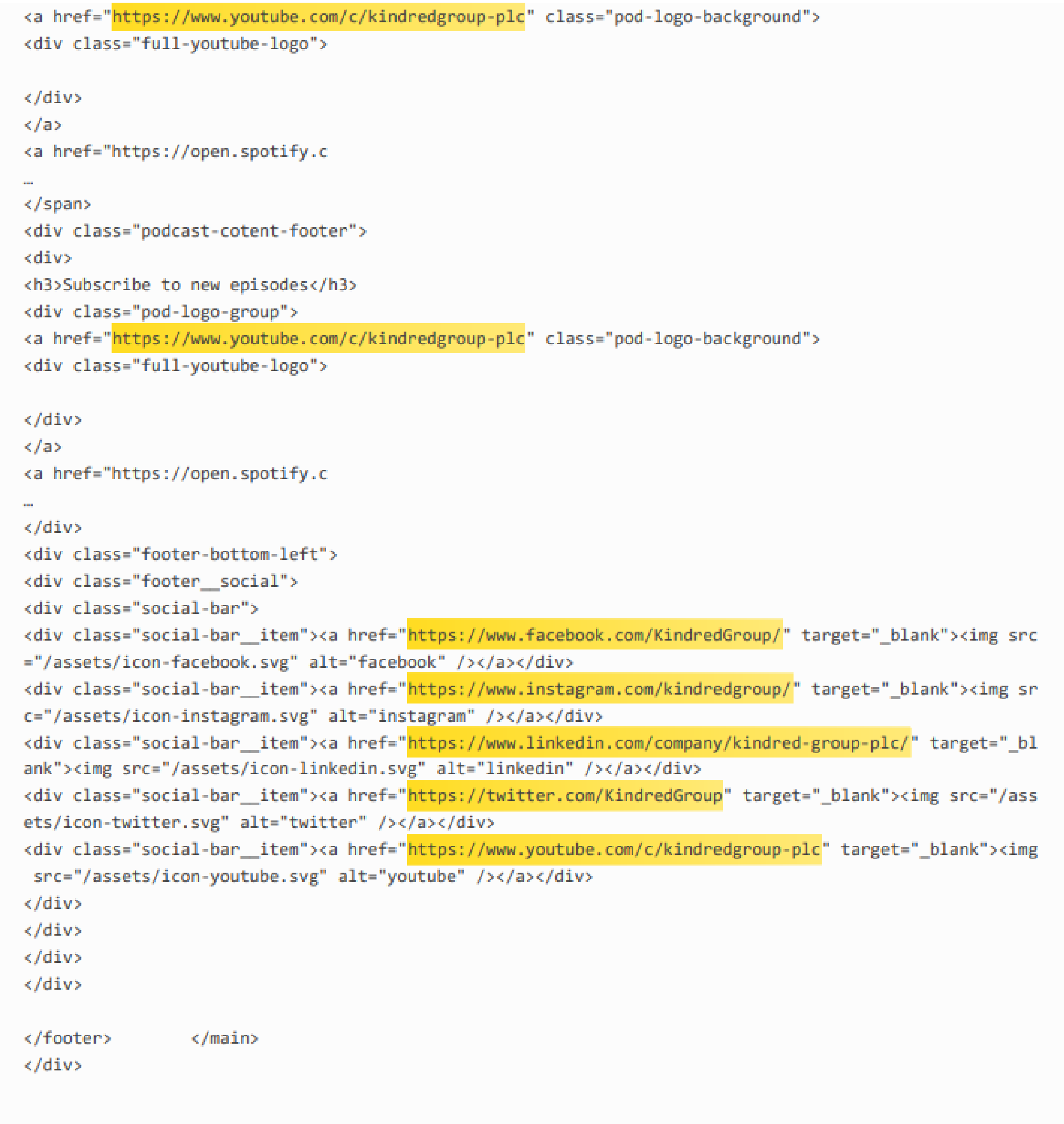


Response

Response Time (ms) : 515.5052 Total Bytes Received : 92412 Body Length : 91711 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: EPiStateMarker=true; path=/
Set-Cookie: ARRAffinity=f62dc48792b6e16789f38b9331562ab71aac9ec805fac06e15282a091076b114;Path=/;HttpOnl
y;Secure;Domain=www.kindredgroup.com
Set-Cookie: ARRAffinitySameSite=f62dc48792b6e16789f38b9331562ab71aac9ec805fac06e15282a091076b114;Path
=/;HttpOnly;SameSite=None;Secure;Domain=www.kindredgroup.com
Request-Context: appId=cid-v1:f6f0367f-9d11-44c1-bd87-a01942e8c453
CF-RAY: 87b1cb230fc9513a-CMB
Server: cloudflare
CF-Cache-Status: DYNAMIC
Connection: keep-alive
Content-Encoding:
Strict-Transport-Security: max-age=2592000
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chu
…
den-2-image-16-9.jpg?width=1000&amp;format=jpg&amp;quality=90">
<meta property="og:locale" content="en">
<meta name="twitter:card" content="summary">
<meta name="twitter:site" content="https://twitter.com/KindredGroup">
<meta name="twitter:title" content="Kindred Group plc &#x2013; We continue to transform gambling">
<meta name="twitter:description" content="Kindred Group has brought together leading and
…

</a>
</div>
<div class="social-bar">
<div class="social-bar__item"><a href="https://www.facebook.com/KindredGroup/" target="_blank"><img src
="/assets/icon-facebook.svg" alt="facebook" /></a></div>
<div class="social-bar__item"><a href="https://www.instagram.com/kindredgroup/" target="_blank"><img sr
c="/assets/icon-instagram.svg" alt="instagram" /></a></div>
<div class="social-bar__item"><a href="https://www.linkedin.com/company/kindred-group-plc/" target="_bl
ank"><img src="/assets/icon-linkedin.svg" alt="linkedin" /></a></div>
<div class="social-bar__item"><a href="https://twitter.com/KindredGroup" target="_blank"><img src="/ass
ets/icon-twitter.svg" alt="twitter" /></a></div>
<div class="social-bar__item"><a href="https://www.youtube.com/c/kindredgroup-plc" target="_blank"><img
 src="/assets/icon-youtube.svg" alt="youtube" /></a></div>
</div>
```



```
<a href="https://www.youtube.com/c/kindredgroup-plc" class="pod-logo-background">
<div class="full-youtube-logo">

</div>
</a>
<a href="https://open.spotify.c
…
</span>
<div class="podcast-cotent-footer">
<div>
<h3>Subscribe to new episodes</h3>
<div class="pod-logo-group">
<a href="https://www.youtube.com/c/kindredgroup-plc" class="pod-logo-background">
<div class="full-youtube-logo">

</div>
</a>
<a href="https://open.spotify.c
…
</div>
<div class="footer-bottom-left">
<div class="footer__social">
<div class="social-bar">
<div class="social-bar__item"><a href="https://www.facebook.com/KindredGroup/" target="_blank"><img src
="/assets/icon-facebook.svg" alt="facebook" /></a></div>
<div class="social-bar__item"><a href="https://www.instagram.com/kindredgroup/" target="_blank"><img sr
c="/assets/icon-instagram.svg" alt="instagram" /></a></div>
<div class="social-bar__item"><a href="https://www.linkedin.com/company/kindred-group-plc/" target="_bl
ank"><img src="/assets/icon-linkedin.svg" alt="linkedin" /></a></div>
<div class="social-bar__item"><a href="https://twitter.com/KindredGroup" target="_blank"><img src="/ass
ets/icon-twitter.svg" alt="twitter" /></a></div>
<div class="social-bar__item"><a href="https://www.youtube.com/c/kindredgroup-plc" target="_blank"><img
 src="/assets/icon-youtube.svg" alt="youtube" /></a></div>
</div>
</div>
</div>
</div>

</footer>        </main>
</div>
```

Remedy

- Add `rel=noopener`to the linksto prevent pages from abusing *window.opener*. This ensures that the page cannot access the *window.opener*property in Chrome and Opera browsers.

- For older browsers and in Firefox, you can add `rel=noreferrer`which additionally disables the Referer header.

```
<a href="..." target="_blank" rel="noopener noreferrer">...</a>
```

External References

- [Reverse Tabnabbing]
- [Blankshield & Reverse Tabnabbing Attacks]
- [Target="_blank" - the most underestimated vulnerability ever]

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
SANS Top 25	16
WASC	15
ISO27001	A.14.1.2

Suggested Solution:

Applied strict identification plus sanitization of user-generated web content to avoid shot of hazardous manuscripts or web content that can control internet browser tabs.

Make Use Of safety and security headers such as Content Security Policy (CSP) to limit the deployment of manuscripts paired with sources from untrusted resources decreasing the possibility of cross-site scripting (XSS) assaults.
Inform clients concerning typical phishing approaches along with supply support on detecting plus preventing dubious web connections, pop-ups or internet browser tab controls.

Display individual remarks as well as records of phishing activities to determine arising threats as well as alter protection decisions as necessary.

Motivate the development of online browser safety and security capabilities such as popup blockers including anti-phishing filters to improve individual defense versus hazardous material.

On a regular basis analyze together with upgrade the application's safety and security measures as well as interface layout to handle progressing threats and also retain a safe and secure surfing setting.