Michael Simmons

IT 4863 – Web and Mobile App Security

Assignment 4

9/19/21

OWASP Vulnerability: Cross-Site Scripting

I would like to discuss a real-life incident where cross-site scripting was used and offer preventative solutions to the vulnerability. In June 2020, it was reported that hackers have used Google Analytics to cover their tracks when stealing the credit card data of users. The hackers used cross-site scripting to conduct web skimming attacks on 24 vulnerable websites in Europe, North and South America that specialize in e-commerce with Google Analytics. When preforming transactions on the compromised websites the users' credit card information and login credentials are able the be tracked. Google Analytics uses whitelisting in its content security policy (CSP) to prevent and track vulnerabilities and the exportation of sensitive data. To get around this, the hackers posing as a trusted website through the whitelisted web domain, injected JavaScript to schedule an event to have Google Analytics exfiltrate the data itself. Since the exfiltration is to a known source and the hackers mask their code when the browser detects a developer. no alerts were raised.

Possible preventions for this type of vulnerability are difficult to find because the CSP is comprised internally and the add scripts can be hidden during code analysis. However, a few things can still be done. Using an API with authentication to make requests for sensitive data prevents direct code injection. If using a whitelist, add whitelisting with server-side input validation to ensure the website has not been compromised. Live monitoring and alert the use

of special commands and characters known to request sensitive data, i.e the addition of script tags, get statements, find cookies or session data.

Citations:

Hackers Using Google Analytics to Bypass Web Security and Steal Credit Cards. The Hacker News.com by Ravie Lakshmanan.

https://thehackernews.com/2020/06/google-analytics-hacking.html

Hackers are Using Google Analytics to Steal Credit Cards. VPN Overview.com by David Janssen. https://vpnoverview.com/news/hackers-are-using-google-analytics-to-steal-credit-cards/

Hackers Use Google Analytics to Steal Credit Cards. Search Engine Journal.com by Roger Montti. https://www.searchenginejournal.com/hackers-exploiting-google-analytics/373046/#close

Top Ten: A03:2021 - Injection. OWASP.org by OWASP TOP 10 team.

https://owasp.org/Top10/A03_2021-Injection/