SAND2022-11751D

Cyber-Physical Security Analysis of a DER Application for IoT Communications

Yesid Nickolas Jimenez[1], Ifeoma Onunkwo[2], Aya Khalafalla[2], Dr. Sumit Paudyal[1], and Adam Summers[2]

The University of Florida International University[1]
Department of Electrical and Computer Engineering,
yjime030@fiu.edu

Sandia National Laboratories[2]
Albuquerque, New Mexico
asummers@sandia.gov

INTRODUCTION

❑ Sandia National Laboratories was asked to evaluate the security and robustness of an application developed by a customer. The application will be used for situational awareness and control of Photovoltaics (PV) and microgrid energy systems.

❑ The objective of this evaluation is to assess the risks and cyber posture of the app through targeted cyber attacks under controlled conditions that can be engaged by an adversary.

❑ The red team assessment combined practices from multiple sources; NIST's Guide to Industrial Control Systems (ICS) Security, best cyber security practices, and collective expertise regarding securing web applications.

ASSESMENT APPROACH

❑ Vulnerability assessment and penetration testing focus on finding and exploiting flaws that can compromise the system before attackers do.

❑ While vulnerability assessment identifies vulnerabilities that can lead to security and information compromise, penetration tests exploits these security weaknesses so that the best mitigation steps are applied.

❑ These assessments ensure that the system properly implements the CIA (Confidentiality, Integrity, Availability) triad security principles that affect the ability of a system to operate efficiently.

OBJECTIVES

❑ Conduct software checks on current version of the software.
  - Verifiable operating system check
  - Formal language check
  - Memory safe language

❑ Conduct vulnerability and penetration tests of the device:
  - Reconnaissance
  - Interruption
  - Interception
  - Firewall

❑ Conduct 10 OWASP security risks to web apps:
  - Broken Access Control
  - Security Misconfiguration
  - Injection
  - Cryptographic Failures
  - Insecure Design
  - Vulnerable and Outdated Components
  - Identification and Authentication Failures
  - Software and Data Integrity Failures
  - Security Logging and Monitoring Failures
  - Server-Side Request Forgery

NETWORK ENVIRONMENT

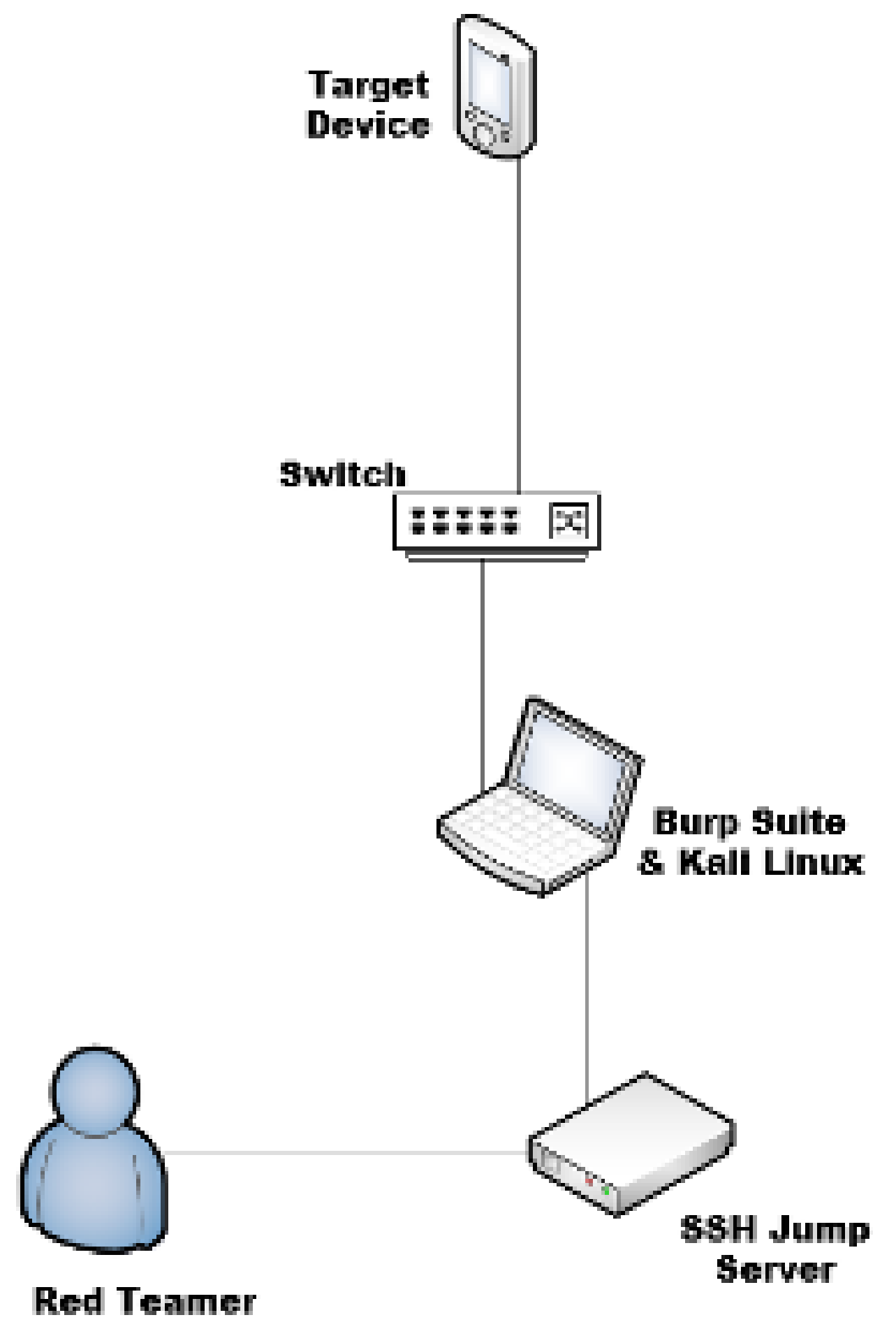


Figure 1: Physical testbed for red teaming

Procedure

❑ The experiments were conducted on an isolated and controlled network environment.

❑ The network was created using a network hub that connected the device to the attack machine which is Kali, an open-source Linux operating system based on Debian, that is equipped with security and analysis tools for identifying and exploiting vulnerabilities.

❑ Burp Suite Professional, an application web security testing software was installed on Kali Linux.

❑ The team had to get to the test environment using a jump host server. The test network environment is shown in **Figure 1**

RESULTS

Severity	Number of Issues
High	4
Medium	3
Low	2

Severity	Vulnerability	Description	Recommendation
High	Authentication Bypass	Non-authenticated users are able to view and edit solar array status using curl. This vulnerability is present because the login.php code does not kill the session after it redirects a user. To view the status of the solar arrays: curl -k --include https://<XX.XX.XX>/index.php To change the status of the solar arrays to ON: curl -d "onButton=On" -k --include -X POST https://<XX.XX.XX>/index.php	In the login.php code, add exit() or die() to kill the session after a redirect.
High	Browsable .git Directory	The .git directory is accessible to non-authenticated users and reveals project source code and credentials. https://<XX.XX.XX>/.git	Restrict access .git and/or disable directory browsing.
High	Credentials stored in plain-text	Login.php is accessible through the publicly accessible .git directory. Login.php uses a basic string comparison to validate the password which is stored in clear text.	If string comparison must be used, hash and salt passwords. Using a database for authentication is recommended.
High	Weak Architecture Design	Based on information from Login.php, the application only supports one user and one password. This is a weak design assuming multiple users will be using the application.	Redesign the web application and use a backed database to support multiple users, authentication, and logging.
Medium	Reflected Cross Site Scripting (XSS)	The web application is vulnerable to reflected cross site scripting (XSS)	Implement HTML encoding and input validation.
Medium	Browsable web directories	Several directories are accessible including: /.git /info.php /XXXXXX.php /panels/	Restrict access to directories to limit information disclosure.
Medium	PHPINFO page accessible	Unauthenticated users can access /info.php. Attackers can use this page to scrape information about the application – in this case, an internal IP address was disclosed along, PHPSESSION Ids, PHP and Apache versions, etc…	Restrict access to info.php
Low	Test page available	/XXXXXX.php is accessible with no authentication and seems to be a test page for the main index.php. Changes in the index.php page do not reflect back to the XXXXXX.php page	Remove page or restrict access to it.
Low	TLS Certificate issues	SSL/TLS certificate error – even though it's still valid - due to possible domain name mismatch	Update with the correct certificate.

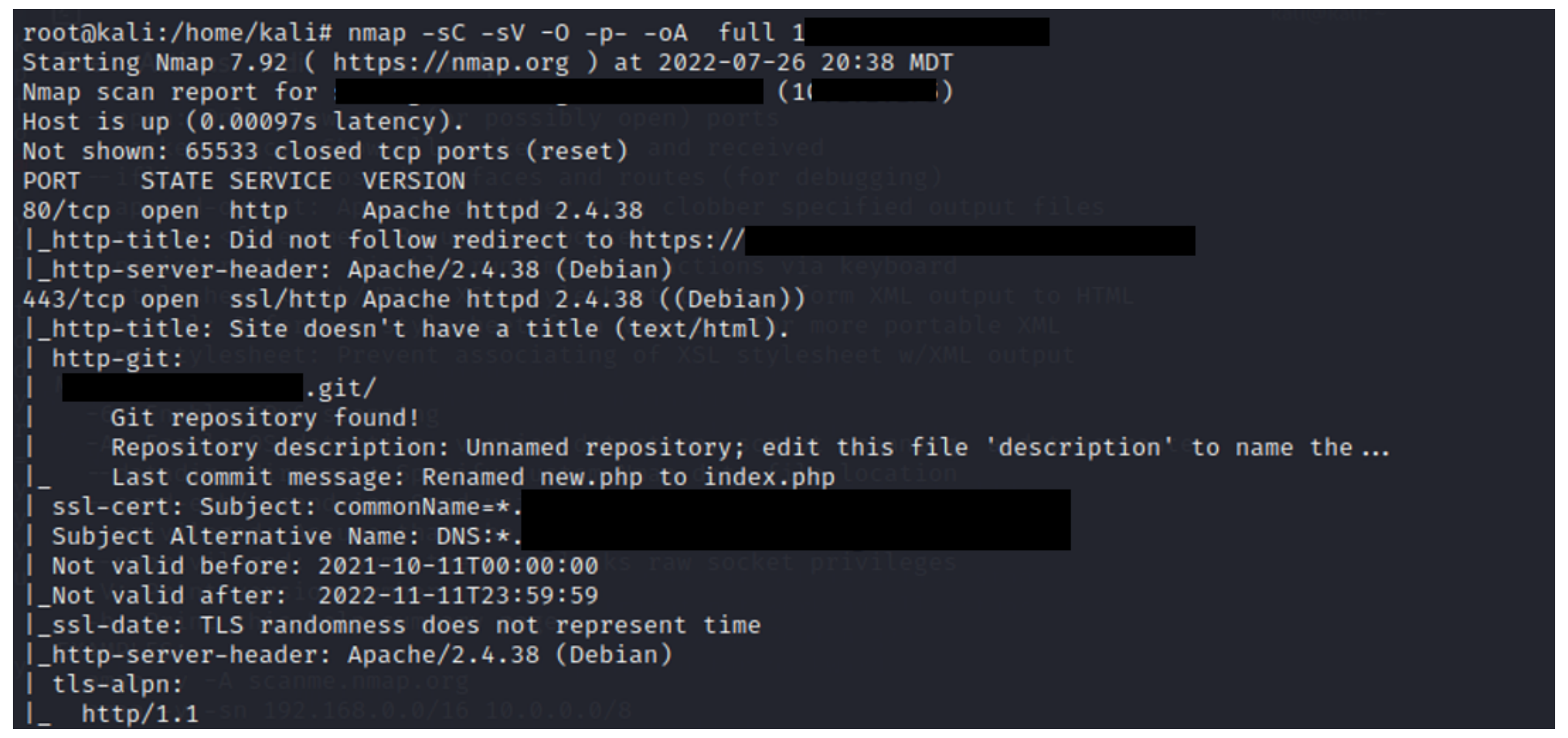
ASSESSMENTS

RESULTS

Device Penetration Testing

Reconnaissance

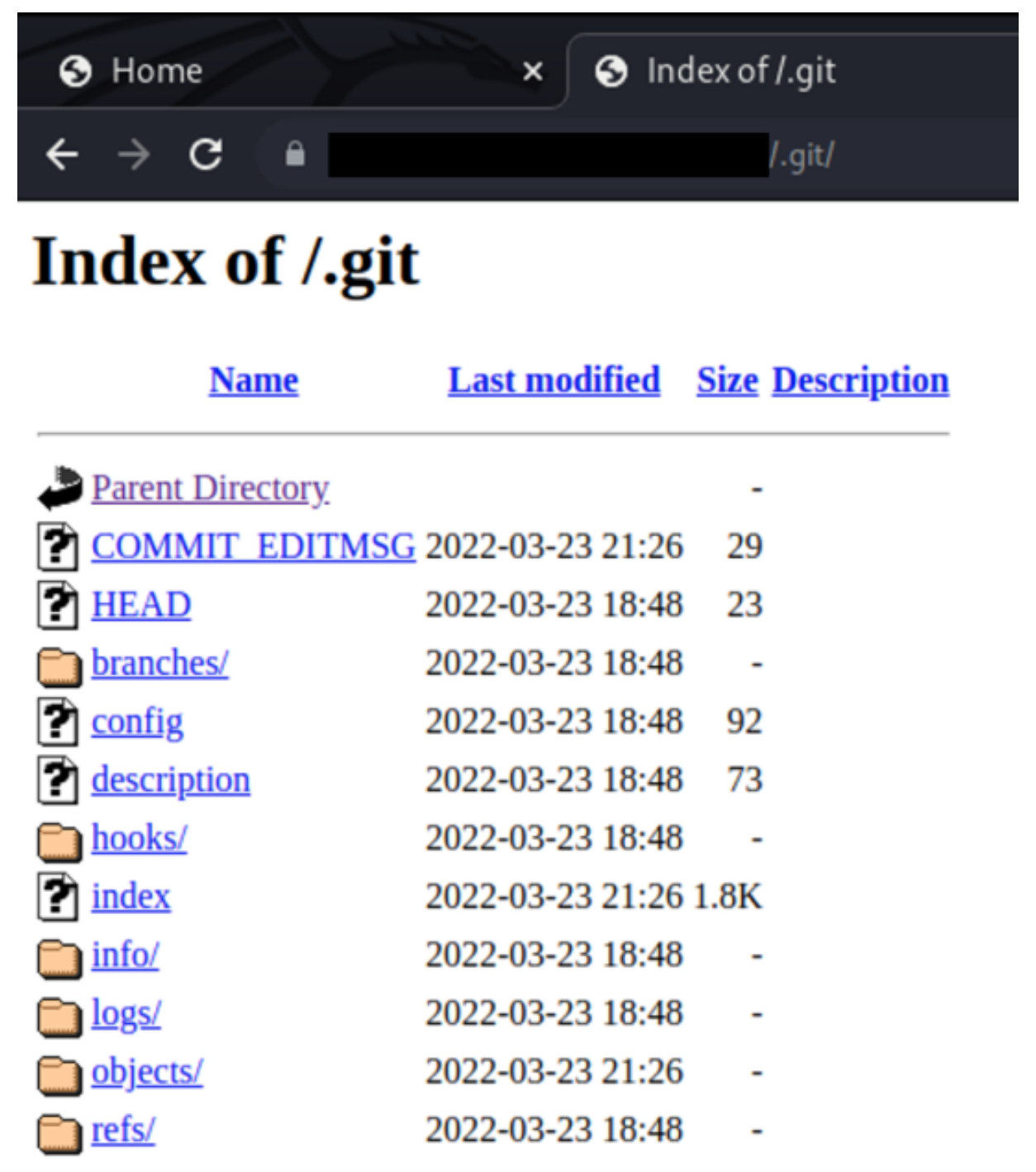
❑ To gather as much information as possible about the target system and to find openings, Nmap, a vulnerability scanning tool was utilized. Nmap was used to scan ports, fingerprint the OS, and enumerate services. This is shown in **Figure 2.** From the scan, it was discovered that the version of the server being used was vulnerable to high CVE's with high severity scores.



```
root@kali:/home/kali# nmap -sC -sV -O -p- -oA  full 1[redacted]
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 20:38 MDT
Nmap scan report for [redacted] (1[redacted])
Host is up (0.00097s latency).
Not shown: 65533 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd 2.4.38
|_http-title: Did not follow redirect to https://[redacted]
|_http-server-header: Apache/2.4.38 (Debian)
443/tcp open  ssl/http Apache httpd 2.4.38 ((Debian))
|_http-title: Site doesn't have a title (text/html).
| http-git:
|   [redacted].git/
|     Git repository found!
|     Repository description: Unnamed repository; edit this file 'description' to name the...
|_    Last commit message: Renamed new.php to index.php
| ssl-cert: Subject: commonName=*.[redacted]
| Subject Alternative Name: DNS:*.
| Not valid before: 2021-10-11T00:00:00
|_Not valid after:  2022-11-11T23:59:59
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.38 (Debian)
| tls-alpn:
|_  http/1.1
```

Figure 2: Nmap operating system and services detection

❑ Nmap scan results also showed a *"Git repository! Http-git: IP address/.git/ Repository description: Unnamed repository; edit this file 'description' to name the…. Last commit message: Renamed new.php to index.php"* This information allows an attacker extract sensitive information by requesting the *hidden* metadata directory of the version control tool Git creates. This is shown in **Figure 3**



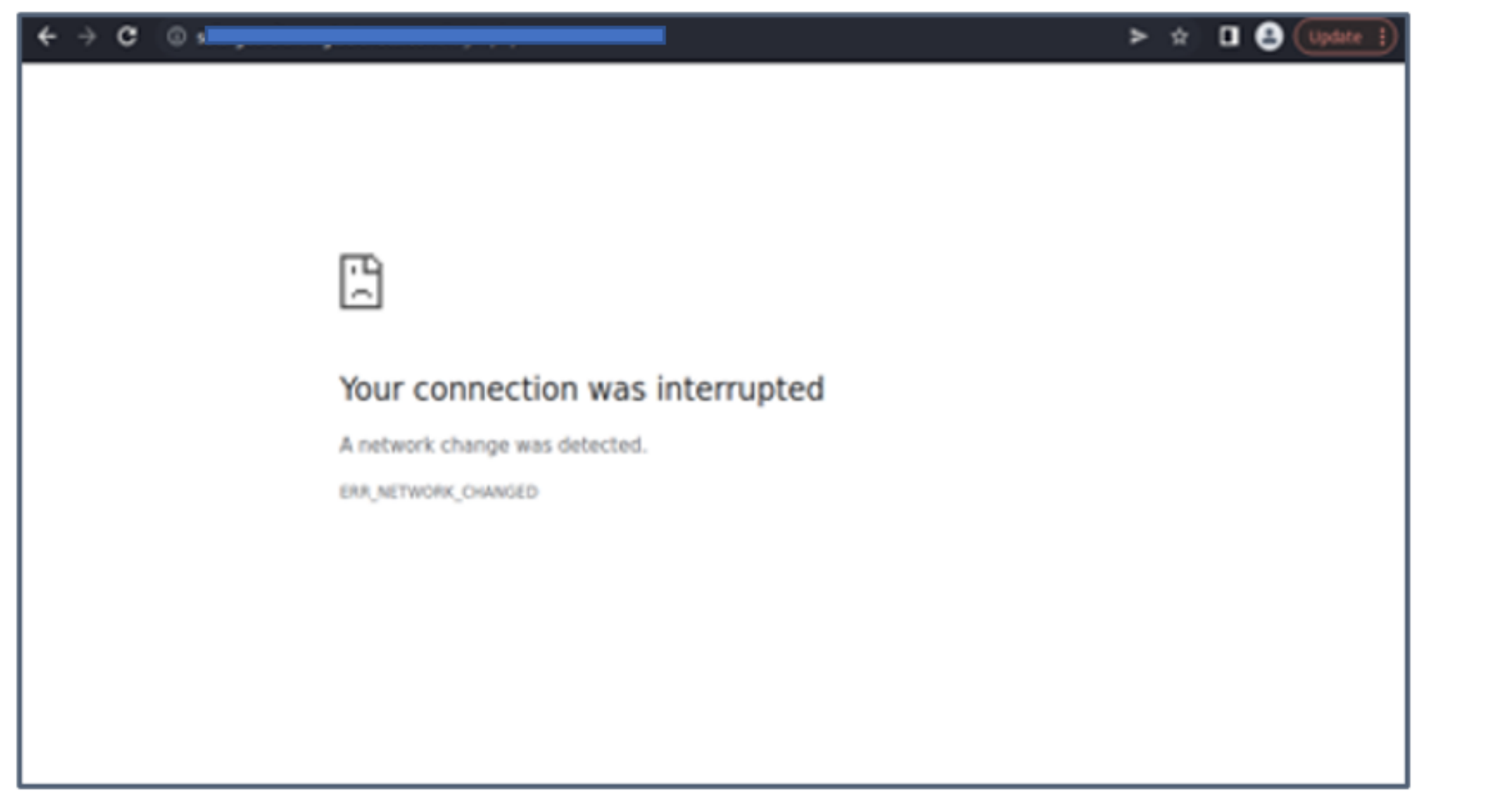
Index of /.git

Name	Last modified	Size	Description
Parent Directory		-	
COMMIT_EDITMSG	2022-03-23 21:26	29	
HEAD	2022-03-23 18:48	23	
branches/	2022-03-23 18:48	-	
config	2022-03-23 18:48	92	
description	2022-03-23 18:48	73	
hooks/	2022-03-23 18:48	-	
index	2022-03-23 21:26	1.8K	
info/	2022-03-23 18:48	-	
logs/	2022-03-23 18:48	-	
objects/	2022-03-23 21:26	-	
refs/	2022-03-23 18:48	-	

Figure 3: Unauthorized access to .git directory

Interruption and Interception

❑ The team was able to interrupt the application using a Denial-of-Service (DoS) attack. This is shown in **Figure 4**.



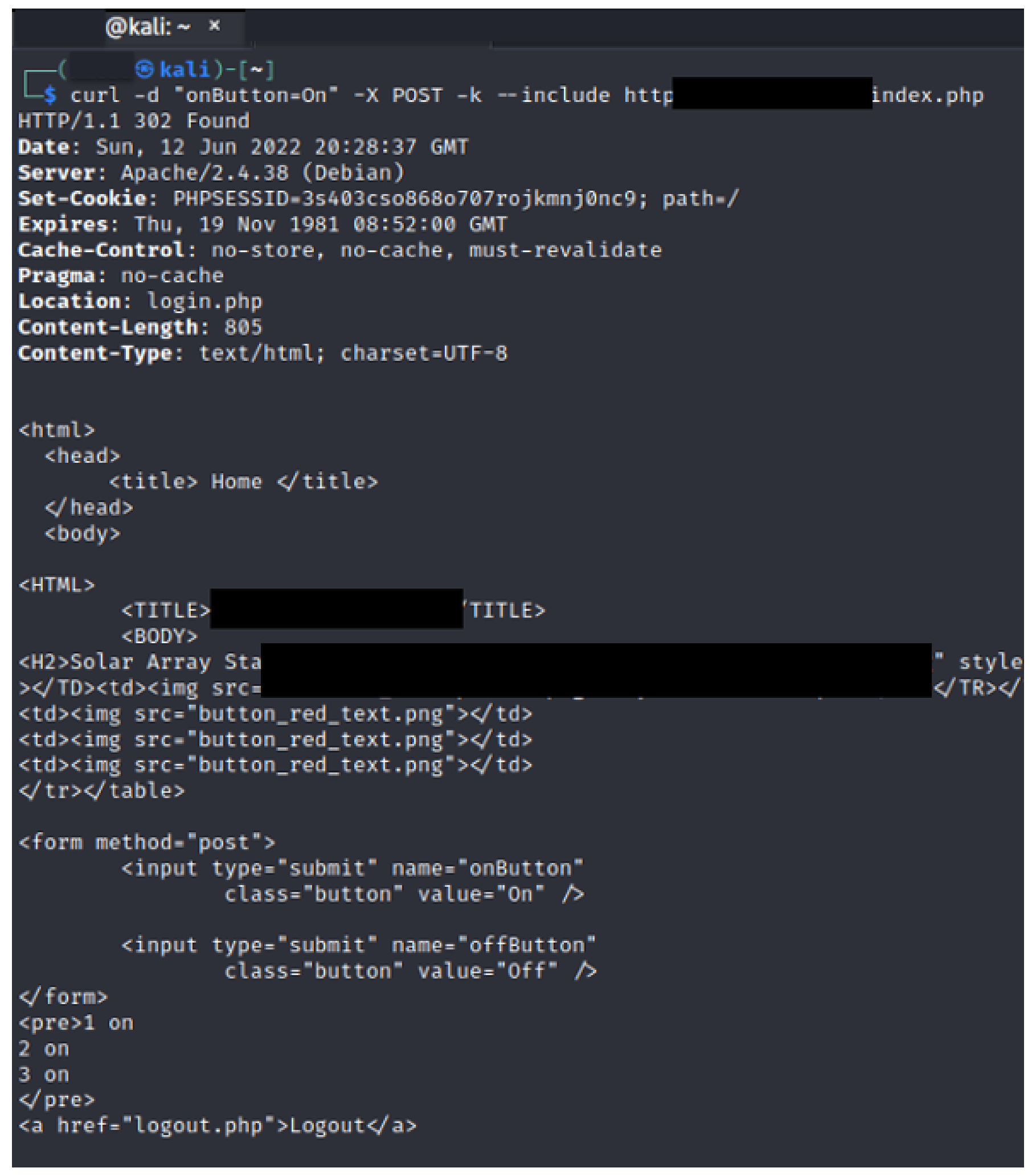
Your connection was interrupted

A network change was detected.

ERR_NETWORK_CHANGED

Figure 4: Interruptions to the application and device

❑ The team was also able to intercept and bypass the authenticated channel to legitimately login into the device. Curl commands were used to first pull data and then make changes on the index page without authenticating to the console as a privileged Admin user. This is shown in **Figure 5**



```
┌──([redacted]㉿kali)-[~]
└─$ curl -d "onButton=On" -X POST -k --include http[redacted]index.php
HTTP/1.1 302 Found
Date: Sun, 12 Jun 2022 20:28:37 GMT
Server: Apache/2.4.38 (Debian)
Set-Cookie: PHPSESSID=3s403cso868o707rojkmnj0nc9; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: login.php
Content-Length: 805
Content-Type: text/html; charset=UTF-8


<html>
  <head>
        <title> Home </title>
  </head>
  <body>

<HTML>
        <TITLE>[redacted]TITLE>
        <BODY>
<H2>Solar Array Sta[redacted]" style
></TD><td><img src=                                                    </TR></
<td><img src="button_red_text.png"></td>
<td><img src="button_red_text.png"></td>
<td><img src="button_red_text.png"></td>
</tr></table>

<form method="post">
        <input type="submit" name="onButton"
                class="button" value="On" />

        <input type="submit" name="offButton"
                class="button" value="Off" />
</form>
<pre>1 on
2 on
3 on
</pre>
<a href="logout.php">Logout</a>
```

Figure 5:
Curl command to turn on the solar array button

CONCLUSION

❑ In the security assessment of the application and the device, vulnerable areas that could be exploited were identified that adversaries could use to gain access or control the application. These areas of weaknesses were mostly due to system configuration flaws and the use of outdated software.

❑ The scoring rubric used to categorize the top 10 OWASP vulnerabilities in the results section were taken from MITRE's Common Vulnerability and Exposure (CVE) and the NIST's Common Weakness Enumeration (CWE) rankings.

❑ The assessment team endorsed the utilization of the recommendations provided in the result section so that the cyber security posture of the customer's application and tool is improved on. The team also encouraged the use of security and hardening best practices for better performance and security of their device configuration and communication. Finally, the team recommends a biennial security assessment for a snapshot of the security risk of the application for continuous mitigation.

Acknowledgment

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. This poster describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the poster do not necessarily represent the views of the U.S. Department of Energy or the United States Government. This material is based upon work funded with support by the New Mexico Small Business Assistance Program at Sandia National Laboratories; SAND#}

CREPES First Annual Workshop,
Florida International University
Date: September 16th, 2022

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.