Gruppeinnlevering 1 IKT108

av

Pål, Ola, Jorund, Kristoffer

IKT 207

Cybersikkerhet

Veiledet av

Sigurd Kristian Brinch

Fakultet for teknologi og realfag

Universitetet i Agder

Grimstad, September 2020

Innhold

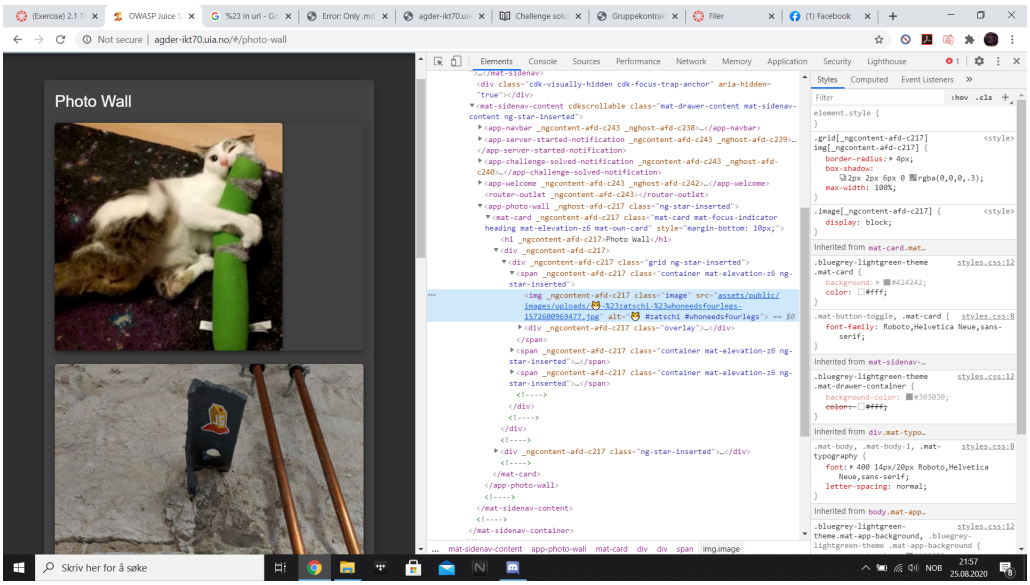
Figurer

1 Missing Encoding

For å få fram Bjørns katt må man først gå inn på bildeveggen. Der kommer det opp 3 bilder. 2 som blir vist og 1 som er ødelagt.

For å vise bildet, må man høyreklikke på "#zatschi #whoneedsfourlegs" og inspiser(CTRL + Shift + I).

Da får du dette opp:



Figur 1: Bjørns katt

Kopier det som står back "scr" og lim det inn bak "http://agder-ikt70.uia.no/". I URL-en må man endre # til %23 grunnet URL koding/formatering. Grunnen til at vi må endre # til %23 er fordi %23 representerer # i URL koding.

2 Zero Star

For å kunne gi null stjerner til firmaet må en først gå inn på kundetilbakemelding. Der kan man skrive hva man vil, for så å høyreklikke på "sende inn". Der må vi lete litt til vi finner

```
<button _ngcontent-rwl-c128 type="submit" id="submitButton" mat-
raised-button color="primary" aria-label="Button to send the review"
class="mat-focus-indicator mat-raised-button mat-button-base mat-
primary" disabled="true">
```

Figur 2: null stjerne

Da trenger man bare å fjerne hele "deaktivere". Hvis man gjør dette kan man gi 0 stjerner.

3 DOM XSS

Vi kopierte scriptet vi fikk og limte det inn i søkefeltet på nett siden.

4 Reflected XSS

Vi kunne ikke gjøre denne oppgaven siden den ikke var installert på docker containeren.

5 Login Admin

For å logge inn som admin prøvde vi først og se om unnslippe tegn(Escape characters) fungerte. Dette fant vi ut at de gjorde ved å skrive ” ’ ” i brukernavn delen. vi endret deretter brukernavnet til ” ’or 1=1–”. Passordet kan være hva som helst, det spiller ingen rolle.

Dette fungerer fordi det ikke er noe filter på bruker navnet på hva slags tegn som kan brukes og vi kan dermed sette inn enn SQL uttalelse. ” ’ or 1=1” denne SQL koden er laget for å dra fram all informasjon om en spesifikk bruker fra tabellen av brukere.

6 Login Bender

Ser på produktet ”Banana juice” og legger merke til en Futurama referanse og at mailen var ”bender@juice-sh.op”, da vet en at det handler om Bender fra futurama. Går på glemt passord og der er sikkerhets-spørsmålet ”Company you first worked for as an adult?”. Søker på bender futurama, og leser at han jobbet på en selvmordsbås. Søker på dette og finner ut at båsen ble kalt for ”Stop’n’Drop”. Skrev det inn i ”sikkerhetsspørsmål” boksen og endret passord. Dermed var det bare å logge inn.

7 Access Log

Vi fikk tilgang til logen på samme måte som vi fikk tilgang til konfidensielle dokumenter.

8 Confidential Document

Det første vi gjorde når vi åpnet Juicebox var å skrive /robots.txt etter nettadressen. Da fikk vi opp en side som sa at /ftp var ulovlig. Vi gikk så inn på ”agder-ikt70.uia.no/ftp” og ble videresendt til en nettside som inneholdt alt fra logg til framtidige planer for firmaet, samt noen uleselige dokumenter.

9 View Basket

For å se handlevogna gikk vi inn på en brukers handlevogn og gikk inn i applikasjon på inspiser element. Der endret vi ”bid” inne i ”current session”. Deretter gikk vi inn og ut av handlevogna. Da kom vi inn på den brukeren som har den ID-en vi tastet inn i handlevogn.

10 Wierd Crypto

Vi gikk inn på kunde tilbakemelding og skrev md5 i kommentar. En kan også skrive z85, base85, base64 eller hashid. Det som skjer er at siden utløser på md5 fordi det er hasjet i base64.

11 Error Handeling

Denne oppgaven kan en få til på flere forskjellige måter. Vi fikk denne feilmeldingen ved DOM XSS oppgaven.

12 Outdated Whitelist

Først måtte vi logge oss inn med en bruker, for så å legge noe i kurven. Vi gikk så gjennom hele betalingsprosessen til vi kom til ende. Der gikk vi inn på inspiser element(CTRL + shift + I) og trykket på kilder. Der ligger en mappe som heter main-es2015.js.

Figur 3: utdatert hvitliste

Der måtte vi søke på "redirect"(med CTRL + F), så kopierte vi hele URL-en og limte den etter "agder-ikt70.uia.no". Der ligger det tre forskjellige URL som du kan lime inn. Vi limte inn den første. som man ser på "title" er dette en Bitcoin adresse.

13 vulnerabilities

Dersom dette fiktive firmaet har samme problemer og svakheter som juiceshop, så kan det være kritisk: Ikke bare for firmaet, men også for klientene.

Bare det at en kan ta kontroll over administratorens konto kan være katastrofalt utfall for alle firmaer. En kan i bunn og grunn holde hele 3DPT AS som gissel uten at det er så mye de kan gjøre med det. Deres brukernavn og passord er så kort og lett å gjette, noe som gjør det enkelt for til og med den minst erfarne hackeren å få tilgang til sluttbrukerene som har lokale administrasjonsrettigheter. Ikke nok med det, alle sluttbrukerene er koblet opp til WiFien som igjen er "slutthuben" for alt utstyr. All informasjon som beveger seg i firmaet går gjennom denne, noe som gjør det ekstremt enkelt å implementere en mann i midten som overvåker alt som skjer i firmaet.

Firmaet kan også stå ovenfor et ekstremt stort problem hvis en av de ansatte ikke er fornøyd med tanke på at alle har tilgang til ALLE filene på hele serveren.

Faktumet at en kan gå inn å se hva en klient/konkurrent har bestilt kan gi deg/ditt firma store fordeler i markedet og kan ødelegge konkurransen. Om filer som klienter laster opp ikke blir sjekket, er det svært enkelt for angripere og laste opp skadevare rett på serveren.

Det at alt er kryptert i md5/base64 gjør all den krypterte informasjonen ganske enkel å dekryptere for å hente ut den informasjonen som en trenger.

Det at en kan få tilgang til logg og konfidensiell informasjon med å legge til /ftp på slutten av internett-addressen er aldri et bra tegn. Dette burde bare være mulig med en administrator bruker.

Det er et stort problem at maskinene til de ansatte kjører Windows 7, i og med at dette operativsystemet ikke lenger får sikkerhetsoppdateringer. Det betyr at dersom angripere finner svakheter og hull i operativsystemet, blir ikke dette oppdatert eller fikset, som igjen kan gi angripere enkel tilgang til maskinene.

Du trenger ikke mye ferdigheter i hacking for å komme deg til steder du ikke burde være. Hvis du kan lese kode kommer du langt. Inne på kildekoden til nettsiden er det mye rusk og løse tråder som burde bli ryddet opp i. Disse løse trådene kan skape store sikkerhetsproblemer, samt gi en normal person tilgang til informasjon den ellers ikke skulle hatt. Eksempelvis fra en av oppgavene der vi fant tilgangen til tidligere betalingsalternativ som skulle blitt fjernet.

Det er heller ikke noen form for backup eller redundans til serverene, noe som kan være katastrofalt ved ulykker. Serverene og utstyr burde også være beskyttet av en brannmur eller lignende slik at det blir vanskeligere for angripere å trenge inn i systemene deres.