Our Findings

Apache Expect XSS Header not present.

Vulnerability Threat Leve

Our Findings

l:

Medi
um

Vuln
erabi
lity
Defi
nitio
n

As
the
targ
et is
lacki
ng
this
head
er,
older
brow
sers
will
be
pron
e to
Refl
ecte
d
XSS
attac
ks.<
br>

Our Findings

Vulnerability Remediation

Modern browsers does not face any issues with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgr

Our Findings

aded
.

Do
main
is
spoo
fed/h
ijack
ed.<
br>

Vuln
erabi
lity
Thre
at
Leve
l:

High

Vuln
erabi
lity
Defi
nitio
n

An
attac
ker
can

Our Findings

forwarded requests that comes to the legitimate URL or web application to a third party address or to the attacker's location that can serve malware and affect the end user's mac

Our Findings

hine.

<b>
Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

It is
highl
y
reco
mme
nded
to
depl
oy
DNS
Sec
on
the
host
targ
et.
Full
depl
oym
ent
of
DNS
SEC
will
ensu
re
the
end

Our Findings

user is connecting to the actual web site or other service corresponding to a particular domain name. For more information, check this resource. https://www.cloudf

Our Findings

lare.
com/
dns/
dnss
ec/h
ow-d
nsse
c-wo
rks/<
br>

Vul
nera
biliti
es
repo
rted
in
SSL
Sca
ns.<
br>

Vuln
erabi
lity
Thre
at
Leve
l:

Medi
um

Vuln
erabi

Our Findings

lity Defi nitio n

SSL relat ed vuln erabi lities brea ks the confi denti ality facto r. An attac ker may perf orm a MiT M attac k, intre pret and eave sdro p the com muni catio n.<b

Our Findings

r>

<b>
Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

Pro
per
impl
eme
ntati
on
and
upgr
aded
versi
on of
SSL
and
TLS
librar
ies
are
very
critic
al
whe
n it
com
es to
bloc
king
SSL
relat
ed

Our Findings

vuln
erabi
lities
.

We
bser
ver
leak
s
Inter
nal
IP.<
br>

Vuln
erabi
lity
Thre
at
Leve
l:

Low

Vuln
erabi
lity
Defi
nitio
n

Giv

Our Findings

es attac ker an idea on how the addr ess sche ming is done inter nally on the orga nizat ional netw ork. Disc overi ng the priva te addr esse s used withi n an orga nizat ion can help attac

Our Findings

kers in carrying out network-layer attacks aiming to penetrate the organization's internal infrastructure.

Vulnerability Remediation

Restrict the banner infor

Our Findings

mati
on to
the
outsi
de
worl
d
from
the
discl
osin
g
servi
ce.
Mor
e
infor
mati
on
on
mitig
ating
this
vuln
erabi
lity
can
be
foun
d
here
.
https
://po
rtswi
gger
.net/
kb/is
sues
/006
0030

Our Findings

0_private-ip-addresses-disclosed

We bserver is Outdated.

<b> Vulnerability

Our Findings

Threat Level:

High

Vulnerability Definition

Any outdated web server may contain multiple vulnerabilities as their support would've been ended.

Our Findings

An attacker may make use of such an opportunity to leverage attacks.

Vulnerability Remediation

It is highly recommended to upgrade the web serv

Our Findings

er to
the
avail
able
lates
t
versi
on.<
br>

HE
ART
BLE
ED
Vuln
erabi
lity
Fou
nd
with
Goli
smer
o.<b
r>

Vuln
erabi
lity
Thre
at
Leve
l:

High

Our Findings

Vulnerability Definition

This vulnerability seriously leaks private information of your host. An attacker can keep the TLS connection alive and can retri

Our Findings

eve
a
maxi
mum
of
64K
of
data
per
hear
tbeat
.

<b>
Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

PFS
(Perf
ect
Forw
ard
Secr
ecy)
can
be
impl
eme
nted
to
mak
e
decr
yptio

Our Findings

n
diffic
ult.
Com
plete
rem
ediat
ion
and
reso
urce
infor
mati
on is
avail
able
here
.
http:/
/hea
rtble
ed.c
om/<
br>

We
bser
ver
vuln
erabl
e to
MS1
0-07
0.<b
r>

Our Findings

Vuln
erabi
lity
Thre
at
Leve
l:

High

Vuln
erabi
lity
Defi
nitio
n

An
attac
ker
who
succ
essf
ully
expl
oited
this
vuln
erabi
lity
coul
d
read
data,
such
as

Our Findings

the view state, which was encrypted by the server. This vulnerability can also be used for data tampering, which, if successfully exploited, could be used to decrypt and

Our Findings

tamp
er
with
the
data
encr
ypte
d by
the
serv
er.<
br>

<b>
Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

Micr
osoft
has
relea
sed
a set
of
patc
hes
on
their
web
site
to
mitig
ate
this
issu

Our Findings

e.
The
infor
mati
on
requi
red
to fix
this
vuln
erabi
lity
can
be
infer
red
from
this
reso
urce.
https
://do
cs.m
icros
oft.c
om/e
n-us/
secu
rity-u
pdat
es/s
ecuri
tybul
letin
s/20
10/m
s10-
070<
br>

Our Findings

Found some information through Fingerprinting.

Vulnerability Threat Level: Low

Vulnerability Definition

Attackers alwa

Our Findings

ys do a finge rprin t of any serv er befo re they laun ch an attac k. Fing erpri nting give s them infor mati on abou t the serv er type, cont ent-they are servi ng, last modi ficati on time

Our Findings

s
etc,
this
give
s an
attac
ker
to
learn
mor
e
infor
mati
on
abou
t the
targ
et<b
r>

<b>
Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

A
good
pract
ice
is to
obfu
scat
e the
infor
mati
on to

Our Findings

outside world. Doing so, the attackers will have tough time understanding the server's tech stack and therefore leverage an attack.

Open Files

Our Findings

Found with Golismero BruteForce.

Vulnerability Threat Level: Medium

Vulnerability Definition

Attackers may find considera

Our Findings

ble amo unt of infor mati on from thes e files. Ther e are even chan ces attac kers may get acce ss to critic al infor mati on from thes e files.

<b> Vuln erabi lity Rem ediat ion</

Our Findings

b><
br>

It is
reco
mme
nded
to
bloc
k or
restri
ct
acce
ss to
thes
e
files
unle
ss
nece
ssar
y.

Sub
dom
ains
disc
over

Our Findings

ed
with
DMit
ry.<b
r>

Vuln
erabi
lity
Thre
at
Leve
l:

Medi
um

Vuln
erabi
lity
Defi
nitio
n

Atta
cker
s
may
gath
er
mor
e
infor
mati
on
from

Our Findings

subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even chances

Our Findings

for
the
attac
ker
to
find
vuln
erabi
lities
as
the
attac
k
surfa
ce
gets
large
r
with
mor
e
subd
omai
ns
disc
over
ed.<
br>

<b>
Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

It is
som

Our Findings

etim
es
wise
to
bloc
k
sub
dom
ains
like
deve
lopm
ent,
stagi
ng to
the
outsi
de
worl
d, as
it
give
s
mor
e
infor
mati
on to
the
attac
ker
abou
t the
tech
stac
k.
Com
plex
nami
ng
pract

Our Findings

ices
also
help
in
redu
cing
the
attac
k
surfa
ce
as
attac
kers
find
hard
to
perf
orm
subd
omai
n
brut
eforc
ing
thro
ugh
dicti
onari
es
and
word
lists.

Ope
n

Our Findings

Directories Found with DirB.

 Vulnerability Threat Level: Medium

 Vulnerability Definition

Attackers may find considerable amo

Our Findings

unt of infor mati on from thes e direc torie s. Ther e are even chan ces attac kers may get acce ss to critic al infor mati on from thes e direc torie s.

<b> Vuln erabi lity Rem

Our Findings

ediat
ion</
b><
br>

It is
reco
mme
nded
to
bloc
k or
restri
ct
acce
ss to
thes
e
direc
torie
s
unle
ss
nece
ssar
y.

XS
Ser
foun
d
XSS
vuln
erabi
lities
.

Our Findings

Vuln
erabi
lity
Thre
at
Leve
l:

Criti
cal

Vuln
erabi
lity
Defi
nitio
n

An
attac
ker
will
be
able
to
steal
cook
ies,
defa
ce
web
appli
catio
n or
redir
ect

Our Findings

to
any
third
party
addr
ess
that
can
serv
e
mal
ware
.

<b>
Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

Inpu
t
valid
ation
and
Outp
ut
Sani
tizati
on
can
com
plete
ly
prev
ent

Our Findings

Cross Site Scripting (XSS) attacks. XSS attacks can be mitigated in future by properly following a secure coding methodology. The following comprehensive resource provi

Our Findings

des
detai
led
infor
mati
on
on
fixin
g
this
vuln
erabi
lity.
https
://w
ww.
owa
sp.or
g/ind
ex.p
hp/X
SS_(
Cros
s_Sit
e_S
cripti
ng)_
Prev
entio
n_C
heat
_Sh
eet<
br>

Inte
resti
ng
Files

Our Findings

Dete
cted.

Vuln
erabi
lity
Thre
at
Leve
l:

Medi
um

Vuln
erabi
lity
Defi
nitio
n

Atta
cker
s
may
find
cons
idera
ble
amo
unt
of
infor
mati
on

Our Findings

from thes e files. Ther e are even chan ces attac kers may get acce ss to critic al infor mati on from thes e files.

<b> Vuln erabi lity Rem ediat ion</ b>< br>

It is reco mme nded

Our Findings

to
bloc
k or
restri
ct
acce
ss to
thes
e
files
unle
ss
nece
ssar
y.

Goli
smer
o
Nikt
o
Plugi
n
foun
d
vuln
erabi
lities
.

<b>

Our Findings

Vulnerability Threat Level: Medium

 Vulnerability Definition

Particular Scanner found multiple vulnerabilities that an attacker may try to expl

Our Findings

oit the targ et.<b r>

<b> Vuln erabi lity Rem ediat ion</ b>< br>

Ref er to detai led repo rt to view the com plete infor mati on of the vuln erabi lity, once the scan gets com plete d.<b r>

Our Findings

X-XSS Protection is not Present

Vulnerability Threat Level: Medium

Vulnerability Definition

As the

Our Findings

targ
et is
lacki
ng
this
head
er,
older
brow
sers
will
be
pron
e to
Refl
ecte
d
XSS
attac
ks.<
br>

<b>
Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

Mod
ern
brow
sers
does
not
face
any
issu

Our Findings

es with this vulnerability (missing headers). However, older browsers are strongly recommended to be upgraded .

Open Directories Fou

Our Findings

nd
with
Goli
smer
o
Brut
eFor
ce.<
br>

Vuln
erabi
lity
Thre
at
Leve
l:

Medi
um

Vuln
erabi
lity
Defi
nitio
n

Atta
cker
s
may
find
cons
idera
ble

Our Findings

amo
unt
of
infor
mati
on
from
thes
e
direc
torie
s.
Ther
e
are
even
chan
ces
attac
kers
may
get
acce
ss to
critic
al
infor
mati
on
from
thes
e
direc
torie
s.

Vuln
erabi
lity

Our Findings

Rem
ediat
ion</
b><
br>

It is
reco
mme
nded
to
bloc
k or
restri
ct
acce
ss to
thes
e
direc
torie
s
unle
ss
nece
ssar
y.

HTT
P
PUT
DEL
Meth
ods
Ena
bled.

Our Findings

Vuln
erabi
lity
Thre
at
Leve
l:

Medi
um

Vuln
erabi
lity
Defi
nitio
n

The
re
are
chan
ces
for
an
attac
ker
to
mani
pulat
e
files
on
the
web
serv

Our Findings

er.<
br>

Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

It is
reco
mme
nded
to
disa
ble
the
HTT
P
PUT
and
DEL
meth
ods
inca
se if
you
don't
use
any
RES
T
API
Serv
ices.
Follo
wing

Our Findings

reso
urce
s
help
s
you
how
to
disa
ble
thes
e
meth
ods.
http:/
/ww
w.te
chst
acks
.com
/how
to/di
sabl
e-htt
p-m
etho
ds-in
-tom
cat.h
tml
https
://do
cs.or
acle.
com/
cd/E
1985
7-01
/820
-562
7/gg

Our Findings

hwc/
inde
x.ht
ml
https
://de
velo
per.i
bm.c
om/a
nsw
ers/q
uesti
ons/
3216
29/h
ow-t
o-dis
able-
http-
meth
ods-
head
-put-
delet
e-op
tion/

DB
Ban
ner
retri
eved
with
SQL
Map.

Our Findings

Vuln
erabi
lity
Thre
at
Leve
l:

Low

Vuln
erabi
lity
Defi
nitio
n

May
not
be
SQLi
vuln
erabl
e.
An
attac
ker
will
be
able
to
kno
w
that
the
host

Our Findings

is
usin
g a
back
end
for
oper
ation
.

Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

Ban
ner
Grab
bing
shou
ld be
restri
cted
and
acce
ss to
the
servi
ces
from
outsi
de
woul
d
shou

Our Findings

ld be
mad
e
mini
mum
.

Em
ail
Addr
esse
s
disc
over
ed
with
DMit
ry.<b
r>

Vuln
erabi
lity
Thre
at
Leve
l:

Low

Vuln
erabi
lity

Our Findings

Definition

Chances are very less to compromise a target with email addresses. However, attackers use this as a supporting data to gather information on

Our Findings

arou
nd
the
targ
et.
An
attac
ker
may
mak
e
use
of
the
user
nam
e on
the
emai
l
addr
ess
and
perf
orm
brut
e-for
ce
attac
ks
on
not
just
emai
l
serv
ers,
but
also
on
othe

Our Findings

r legiti mate pane ls like SSH , CMS , etc with a pass word list as they have a legiti mate nam e. This is how ever a shoo t in the dark scen ario, the attac ker may or may not

Our Findings

be
succ
essf
ul
depe
ndin
g on
the
level
of
inter
est<
br>

Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

Sinc
e the
chan
ces
of
expl
oitati
on is
feebl
e
ther
e is
no
need
to
take
actio

Our Findings

n.
Perf
ect
rem
ediat
ion
woul
d be
choo
sing
differ
ent
user
nam
es
for
differ
ent
servi
ces
will
be
mor
e
thou
ghtfu
l.

CGI
Dire
ctori
es
Enu
mer
ated.

Our Findings

Vulnerability Threat Level: Low

 Vulnerability Definition

Attackers may find considerable amount of information from these directories.

Our Findings

Ther
e
are
even
chan
ces
attac
kers
may
get
acce
ss to
critic
al
infor
mati
on
from
thes
e
direc
torie
s.

Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

It is
reco
mme
nded
to
bloc

Our Findings

k or restri ct acce ss to thes e direc torie s unle ss nece ssar y.

So me issu es foun d on the Web serv er.< br>

 Vuln erabi lity Thre at Leve l:

Our Findings

Medi
um

Vuln
erabi
lity
Defi
nitio
n

Part
icula
r
Sca
nner
foun
d
multi
ple
vuln
erabi
lities
that
an
attac
ker
may
try to
expl
oit
the
targ
et.<b
r>

Our Findings

Vulnerability Remediation

Refer to detailed report to view the complete information of the vulnerability, once the scan gets completed.

Found

Our Findings

Subdomains with Nikto.

Vulnerability Threat Level: Medium

Vulnerability Definition

Attackers may gather more informati

Our Findings

on from subdomains relating to the parent domain. Attackers may even find other services from the subdomains and try to learn the architecture of the target. There are even

Our Findings

chan
ces
for
the
attac
ker
to
find
vuln
erabi
lities
as
the
attac
k
surfa
ce
gets
large
r
with
mor
e
subd
omai
ns
disc
over
ed.<
br>

<b>
Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

Our Findings

It is sometimes wise to block subdomains like development, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex nami

Our Findings

ng
pract
ices
also
help
in
redu
cing
the
attac
k
surfa
ce
as
attac
kers
find
hard
to
perf
orm
subd
omai
n
brut
eforc
ing
thro
ugh
dicti
onari
es
and
word
lists.

We
bser

Our Findings

ver
vuln
erabl
e to
Shell
shoc
k
Bug.

Vuln
erabi
lity
Thre
at
Leve
l:

Criti
cal

Vuln
erabi
lity
Defi
nitio
n

Atta
cker
s
expl
oit
the
vuln
erabi

Our Findings

lity in BASH to perform remote code execution on the target. An experienced attacker can easily take over the target system and access the internal sources of the

Our Findings

mac
hine

<b>
Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

This
vuln
erabi
lity
can
be
mitig
ated
by
patc
hing
the
versi
on of
BAS
H.
The
follo
wing
reso
urce
give
s an
inde
pth
anal
ysis

Our Findings

of the vulnerability and how to mitigate it. https://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability https://www.digitalocean.com/com

Our Findings

muni
ty/tut
orial
s/ho
w-to-
prot
ect-y
our-
serv
er-a
gain
st-th
e-sh
ellsh
ock-
bash
-vuln
erabi
lity<
br>

Em
ail
Addr
esse
s
Fou
nd.<
br>

Our Findings

Vuln
erabi
lity
Thre
at
Leve
l:

Low

Vuln
erabi
lity
Defi
nitio
n

Cha
nces
are
very
less
to
com
pro
mise
a
targ
et
with
emai
l
addr
esse
s.
How

Our Findings

ever, attackers use this as a supporting data to gather information around the target. An attacker may make use of the username on the email address and perform

Our Findings

brut
e-for
ce
attac
ks
on
not
just
emai
l
serv
ers,
but
also
on
othe
r
legiti
mate
pane
ls
like
SSH
,
CMS
, etc
with
a
pass
word
list
as
they
have
a
legiti
mate
nam
e.
This
is

Our Findings

how
ever
a
shoo
t in
the
dark
scen
ario,
the
attac
ker
may
or
may
not
be
succ
essf
ul
depe
ndin
g on
the
level
of
inter
est<
br>

<b>
Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

Sinc

Our Findings

e the chances of exploitation is feeble ther e is no need to take action. Perfect remediation would be choosing different user names for different services will be more thou

Our Findings

ghtfu
l.

Zon
e
Tran
sfer
Succ
essf
ul
usin
g
DNS
Enu
m.
Rec
onfig
ure
DNS
imm
ediat
ely.<
br>

<b>
Vuln
erabi
lity
Thre
at

Our Findings

Level:

High

Vulnerability Definition

Zone Transfer reveals critical topological information about the target. The attacker will be able to

Our Findings

query all records and will have more or less complete knowledge about your host.

Vulnerability Remediation

Good practice is to restrict the Zone

Our Findings

Transfer by telling the Master which are the IPs of the slaves that can be given access for the query. This SANS resource provides more information. https://w

Our Findings

ww.sans.org/reading-room/whitepapers/dns/securing-dns-zone-transfer-868

Some vulnerable headers exposed.

Vulnerability Threat Level:

Our Findings

Medi
um

<b>
Vuln
erabi
lity
Defi
nitio
n

Atta
cker
s try
to
learn
mor
e
abou
t the
targ
et
from
the
amo
unt
of
infor
mati
on
expo
sed
in
the
head
ers.
An
attac

Our Findings

ker may kno w what type of tech stac k a web appli catio n is emp hasi zing and man y othe r infor mati on.< br>

<b> Vuln erabi lity Rem ediat ion</ b>< br>

Ban ner Grab bing

Our Findings

shou
ld be
restri
cted
and
acce
ss to
the
servi
ces
from
outsi
de
woul
d
shou
ld be
mad
e
mini
mum
.

Fou
nd
Sub
dom
ains
with
Fierc
e.<b
r>

<b>
Vuln
erabi
lity
Thre

Our Findings

at Level: Medium

 Vulnerability Definition

Attackers may gather more information from subdomains relating to the parent domain. Atta

Our Findings

cker
s
may
even
find
othe
r
servi
ces
from
the
subd
omai
ns
and
try to
learn
the
archi
tectu
re of
the
targ
et.
Ther
e
are
even
chan
ces
for
the
attac
ker
to
find
vuln
erabi
lities
as
the

Our Findings

attac
k
surfa
ce
gets
large
r
with
mor
e
subd
omai
ns
disc
over
ed.<
br>

<b>
Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

It is
som
etim
es
wise
to
bloc
k
sub
dom
ains
like
deve

Our Findings

lopment, staging to the outside world, as it gives more information to the attacker about the tech stack. Complex naming practices also help in reducing the attack surface

Our Findings

as attackers find hard to perform subdomain brute forcing through dictionaries and word lists.

Some issues found with HTTP Options.

Our Findings

Vuln
erabi
lity
Thre
at
Leve
l:

Low

Vuln
erabi
lity
Defi
nitio
n

The
re
are
chan
ces
for
an
attac
ker
to
mani
pulat
e
files
on
the
web
serv
er.<

Our Findings

br>

<b>
Vuln
erabi
lity
Rem
ediat
ion</
b><
br>

It is
reco
mme
nded
to
disa
ble
the
HTT
P
PUT
and
DEL
meth
ods
inca
se if
you
don't
use
any
RES
T
API
Serv
ices.
Follo
wing
reso

Our Findings

urce
s
help
s
you
how
to
disa
ble
thes
e
meth
ods.
http:/
/ww
w.te
chst
acks
.com
/how
to/di
sabl
e-htt
p-m
etho
ds-in
-tom
cat.h
tml
https
://do
cs.or
acle.
com/
cd/E
1985
7-01
/820
-562
7/gg
hwc/

Our Findings

index.html
https://developer.ibm.com/answers/questions/321629/how-to-disable-http-methods-head-put-delete-option/

Does not have an IPv6 Address. It is good to have

Our Findings

one.

Vuln
erabi
lity
Thre
at
Leve
l:

Info

Vuln
erabi
lity
Defi
nitio
n

Not
a
vuln
erabi
lity,
just
an
infor
mati
onal
alert.
The
host
does
not
have

Our Findings

IPv6 support. IPv6 provides more security as IPSec (responsible for CIA - Confidentiality, Integrity and Availablity) is incorporated into this model. So it is good to have

Our Findings

IPv6 Support.

Vulnerability Remediation

It is recommended to implement IPv6. More information on how to implement IPv6 can be found

Our Findings

from this resource. https://www.cisco.com/c/en/us/solutions/collateral/enterprise/cisco-on-cisco/IPv6-Implementation_CS.html

Our Findings

Total Number of Vulnerability Checks : <b> 80

Total Number of Vulnerability Checks Skipped: <b> 0

Total Number of Vulnerabilities Detected : <b>

Our Findings

29

Total Time Elapsed for the Scan : <b> 6s